IBM WebSphere Application Server Network Deployment for Distributed Platforms, Version 8.0

Installing your application serving environment

Note

Before using this information, be sure to read the general information under “Notices” on page 367.

Compilation date: June 7, 2011

Contents

How to send your comments

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

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

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

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

Changes to serve you more quickly

Print sections directly from the information center navigation

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

To print a section of the information center navigation:

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

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

Under construction!

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

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

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

Chapter 1. What is new for installers

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

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

Follow these shortcuts to get started quickly with popular tasks.

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

Review the software and hardware prerequisites

Plan your installation of WebSphere® Application Server

Prepare your operating system for installation

Learn about installing the product

Chapter 3. Task overview: Installing

Use this high-level procedure to install and customize IBM® WebSphere Application Server.

Before you begin

Obtain the product code for distributed platforms.

About this task

Perform the following procedure to learn about and to create a running version of the product on your machine. Plan to read through the major topics in the Welcome, Learn about, and Product overview sections of the information center before beginning the installation.

If you are planning to migrate from an earlier version, you can install the WebSphere Application Server product before migrating.

Procedure

1. Review the installation solution diagrams to help you plan a design for your application serving topology.

   Use the diagrams to identify and select your installation path.
2. Prepare your operating platform for installation.
3. Install your WebSphere Application Server product.
4. Configure the product.

   You can use the Profile Management Tool or the manageprofiles command to configure application server runtime environments, called *profiles*.

   Create a cell. The cell includes a deployment manager profile and a federated application server profile.

   See the documentation on creating profiles for more information.
5. Optional: Consider migrating a previous installation to Version 8.0.

   You can migrate the configuration and applications from a previous installation of another version of WebSphere Application Server.

WebSphere Application Server Version 8 product offerings for supported operating systems

WebSphere Application Server Version 8 includes several related offerings.

Table 1. *WebSphere Application Server Version 8 product offerings for supported operating systems. The following table shows the WebSphere Application Server Version 8 product offerings for supported operating systems.*

Offering	Offering ID	Operating systems [1]	Description	Location					
				Product media	Passport Advantage® eImage (Non–z/OS systems only)	Shop ZSeries (z/OS systems only)	Entitled Software Support (ESS)	developer Works	eFD
Application Client for IBM WebSphere Application Server	com.ibm.websphere. APPCLIENT.v80	AIX®, HP-UX, IBM i, Linux, Solaris, Windows	Application Client for IBM WebSphere Application Server provides resources and clients to aid development of client applications for use with WebSphere Application Server. The Application Client provides a runtime framework for client applications either to run on the Application Client machine or to be distributed with client applications that are to run on other machines.	✓ [2]	✓				✓
Application Client for IBM WebSphere Application Server (ILAN)	com.ibm.websphere. APPCLIENTILAN.v80	AIX, HP-UX, IBM i, Linux, Solaris, Windows	Application Client for IBM WebSphere Application Server provides resources and clients to aid development of client applications for use with WebSphere Application Server. The Application Client provides a runtime framework for client applications either to run on the Application Client machine or to be distributed with client applications that are to run on other machines. This offering is a no-cost non-supported and non-warranted version of the product.					✓	
DMZ Secure Proxy Server for IBM WebSphere Application Server	com.ibm.websphere. NDDMZ.v80	AIX, HP-UX, IBM i, Linux, Solaris, Windows	DMZ Secure Proxy Server for IBM WebSphere Application Server provides enhanced security for WebSphere Application Server environments. This offering can be used to install a proxy server in the demilitarized zone (DMZ), while reducing the security risk of installing an application server in the DMZ to host a proxy server.	✓ [3]	✓				✓
DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS®	com.ibm.websphere. NDDMZ.zOS.v80	z/OS	DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS provides enhanced security for WebSphere Application Server for z/OS environments. This offering can be used to install a proxy server in the demilitarized zone (DMZ), while reducing the security risk of installing an application server in the DMZ to host a proxy server.			✓ [4]			
IBM HTTP Server for WebSphere Application Server	com.ibm.websphere. IHS.v80	AIX, HP-UX, Linux, Solaris, Windows	IBM HTTP Server for WebSphere Application Server provides advanced web server capabilities with consistent management and security in a WebSphere Application Server environment. IBM HTTP Server for WebSphere Application Server is based on Apache HTTP Server.	✓ [2]	✓				✓
IBM HTTP Server for WebSphere Application Server (ILAN)	com.ibm.websphere. IHSILAN.v80	AIX, HP-UX, Linux, Solaris, Windows	IBM HTTP Server for WebSphere Application Server provides advanced web server capabilities with consistent management and security in a WebSphere Application Server environment. IBM HTTP Server for WebSphere Application Server is based on Apache HTTP Server. This offering is a no-cost non-supported and non-warranted version of the product.					✓	
IBM HTTP Server for WebSphere Application Server for z/OS	com.ibm.websphere. IHS.zOS.v80	z/OS	IBM HTTP Server for WebSphere Application Server for z/OS provides advanced web server capabilities with consistent management and security in a WebSphere Application Server for z/OS environment. IBM HTTP Server for WebSphere Application Server z/OS is based on Apache HTTP Server.			✓ [4]			

Table 1. WebSphere Application Server Version 8 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8 product offerings for supported operating systems.

Offering	Offering ID	Operating systems [1]	Description	Location					
				Product media	Passport Advantage® eImage (Non–z/OS systems only)	Shop ZSeries (z/OS systems only)	Entitled Software Support (ESS)	developer Works	eFD
IBM Web Enablement for IBM i	com.ibm.websphere. WEBENAB.v80	IBM i	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. Web Enablement for IBM i offers an entitlement to WebSphere Application Server - Express®. WebSphere Application Server - Express delivers an affordable ready-to-go application foundation for smaller deployments of dynamic web applications which can be effortlessly migrated to more advanced versions of the WebSphere Application Server family as business needs change.				✓		
IBM WebSphere Application Server	com.ibm.websphere. BASE.v80	AIX, HP-UX, IBM i, Linux, Solaris, Windows	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server delivers the availability and security your business depends on while optimizing cost. This base edition of WebSphere Application Server is the foundation of the IBM WebSphere software platform.	✓[3]	✓				✓
IBM WebSphere Application Server Trial	com.ibm.websphere. BASETRIAL.v80	AIX, HP-UX, IBM i, Linux, Solaris, Windows	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server delivers the availability and security your business depends on while optimizing cost. This base edition of WebSphere Application Server is the foundation of the IBM WebSphere software platform. This offering is a no-cost trial version of the product.					✓	
IBM WebSphere Application Server - Express	com.ibm.websphere. EXPRESS.v80	AIX, HP-UX, IBM i, Linux, Solaris, Windows	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server - Express delivers an affordable ready-to-go application foundation for smaller deployments of dynamic web applications which can be effortlessly migrated to more advanced versions of the WebSphere Application Server family as business needs change.	✓[3]	✓				✓

Table 1. WebSphere Application Server Version 8 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8 product offerings for supported operating systems.

Offering	Offering ID	Operating systems [1]	Description	Location					
				Product media	Passport Advantage® eImage (Non–z/OS systems only)	Shop ZSeries (z/OS systems only)	Entitled Software Support (ESS)	developer Works	eFD
IBM WebSphere Application Server - Express Trial	com.ibm.websphere. EXPRESSTRIAL.v80	AIX, HP-UX, IBM i, Linux, Solaris, Windows	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server - Express delivers an affordable ready-to-go application foundation for smaller deployments of dynamic web applications which can be effortlessly migrated to more advanced versions of the WebSphere Application Server family as business needs change. This offering is a no-cost trial version of the product.					✓	
IBM WebSphere Application Server Community Edition		Linux, Windows	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. This community edition of WebSphere Application Server is a lightweight application server that is based on open source Apache Geronimo.					✓	
IBM WebSphere Application Server for Developers	com.ibm.websphere. DEVELOPERS.v80	AIX, HP-UX, IBM i, Linux, Solaris, Windows	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server for Developers delivers the efficient development and innovative features of WebSphere Application Server to help developers reduce testing effort and develop with confidence using a runtime environment that is identical to the production runtime environment their applications will eventually run on.	✓[3]	✓				✓
IBM WebSphere Application Server for Developers (ILAN)	com.ibm.websphere. DEVELOPERSILAN.v80	AIX, HP-UX, IBM i, Linux, Solaris, Windows	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server for Developers delivers the efficient development and innovative features of WebSphere Application Server to help developers reduce testing effort and develop with confidence using a runtime environment that is identical to the production runtime environment their applications will eventually run on. This offering is a no-cost non-supported and non-warranted version of the product.					✓	

Table 1. WebSphere Application Server Version 8 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8 product offerings for supported operating systems.

Offering	Offering ID	Operating systems [1]	Description	Location					
				Product media	Passport Advantage® eImage (Non–z/OS systems only)	Shop ZSeries (z/OS systems only)	Entitled Software Support (ESS)	developer Works	eFD
IBM WebSphere Application Server for z/OS	com.ibm.websphere. zOS.v80	z/OS	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server for z/OS delivers near-continuous availability, with advanced performance and management capabilities for mission-critical applications by leveraging the qualities of services of IBM System z® and z/OS.			✓ [4]			
IBM WebSphere Application Server Network Deployment	com.ibm.websphere. ND.v80	AIX, HP-UX, IBM i, Linux, Solaris, Windows	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server Network Deployment delivers near-continuous availability, with advanced performance and management capabilities for mission-critical applications.	✓ [3]	✓				✓
IBM WebSphere Application Server Network Deployment Trial	com.ibm.websphere. NDTRIAL.v80	AIX, HP-UX, IBM i, Linux, Solaris, Windows	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server Network Deployment delivers near-continuous availability, with advanced performance and management capabilities for mission-critical applications. This offering is a no-cost trial version of the product.					✓	
IBM WebSphere Edge Components: Caching Proxy	com.ibm.websphere. EDGECP.v80	AIX, HP-UX, Linux, Solaris, Windows, z/OS	WebSphere Edge Components: Caching Proxy offers efficiency and performance for WebSphere Application Server environments. This offering can satisfy multiple client requests for the same content directly from a local cache. This offering is stabilized and clients are encouraged to consider using the Proxy Server and DMZ Secure Proxy functionality provided with WebSphere Application Server Network Deployment and WebSphere Application Server for z/OS.						✓
IBM WebSphere Edge Components: Load Balancer for IPv4	com.ibm.websphere. EDGELBIPV4.v80	AIX, HP-UX, Linux, Solaris, Windows	WebSphere Edge Components: Load Balancer for IPv4 offers improved performance and scalability for WebSphere Application Server in IPv4 network environments and is not intended for IPv6 network environments. This offering provides an edge-of-network system that directs network traffic flow to reduce congestion and balance incoming requests to other servers and systems. This offering is stabilized and clients are encouraged to consider using the WebSphere Edge Components: Load Balancer for IPv4 and IPv6 offering.						✓

Table 1. WebSphere Application Server Version 8 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8 product offerings for supported operating systems.

Offering	Offering ID	Operating systems [1]	Description	Location					
				Product media	Passport Advantage® eImage (Non–z/OS systems only)	Shop ZSeries (z/OS systems only)	Entitled Software Support (ESS)	developer Works	eFD
IBM WebSphere Edge Components: Load Balancer for IPv4 and IPv6	com.ibm.websphere. EDGELBIPV4IPV6.v80	AIX, HP-UX, Linux, Solaris, Windows, z/OS	WebSphere Edge Components: Load Balancer for IPv4 and IPv6 offers improved performance and scalability for WebSphere Application Server in IPv4 or IPv6 network environments. This offering provides an edge-of-network system that directs network traffic flow to reduce congestion and balance incoming requests to other servers and systems.	✓[3]	✓	✓[4]			✓
Pluggable Application Client for IBM WebSphere Application Server	com.ibm.websphere. PLUGCLIENT.v80	Windows	Pluggable Application Client for IBM WebSphere Application Server provides a downloadable runtime environment for Java client applications to run with the Java Runtime Environment (JRE) on the Windows platforms. The Pluggable Application Client is deprecated. It is replaced by the standalone thin client, IBM Thin Client for EJB, available as part of the Application Client for IBM WebSphere Application Server offering.	✓[2]	✓				✓
Pluggable Application Client for IBM WebSphere Application Server (ILAN)	com.ibm.websphere. PLUGCLIENTILAN.v80	Windows	Pluggable Application Client for IBM WebSphere Application Server provides a downloadable runtime environment for Java client applications to run with the Java Runtime Environment (JRE) on the Windows platforms. The Pluggable Application Client is deprecated. It is replaced by the standalone thin client, IBM Thin Client for EJB, available as part of the Application Client for IBM WebSphere Application Server offering. This offering is a no-cost non-supported and non-warranted version of the product.					✓	
Web Server Plug-ins for IBM WebSphere Application Server	com.ibm.websphere. PLG.v80	AIX, HP-UX, IBM i, Linux, Solaris, Windows	Web Server Plug-ins for IBM WebSphere Application Server provides an optimized connection to route requests from a web server and WebSphere Application Server.	✓[2]	✓				✓
Web Server Plug-ins for IBM WebSphere Application Server (ILAN)	com.ibm.websphere. PLGILAN.v80	AIX, HP-UX, IBM i, Linux, Solaris, Windows	Web Server Plug-ins for IBM WebSphere Application Server provides an optimized connection to route requests from a web server and WebSphere Application Server. This offering is a no-cost non-supported and non-warranted version of the product.					✓	
Web Server Plug-ins for IBM WebSphere Application Server for z/OS	com.ibm.websphere. PLG.zOS.v80	z/OS	Web Server Plug-ins for IBM WebSphere Application Server for z/OS provides an optimized connection to route requests from a web server and WebSphere Application Server for z/OS.			✓[4]			

Table 1. WebSphere Application Server Version 8 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8 product offerings for supported operating systems.

Offering	Offering ID	Operating systems[1]	Description	Location					
				Product media	Passport Advantage® eImage (Non–z/OS systems only)	Shop ZSeries (z/OS systems only)	Entitled Software Support (ESS)	developer Works	eFD
WebSphere Customization Toolbox	com.ibm.websphere. WCT.v80	AIX, HP-UX, Linux, Solaris, Windows[5]	The WebSphere Customization Toolbox includes tools for customizing various parts of your WebSphere Application Server environment. For example, you can use the WebSphere Customization Toolbox graphical user interface (GUI) to launch the Web Server Plug-ins Configuration Tool to configure your web server plug-ins for any operating system on which the WebSphere Customization Toolbox can be installed. Launch the z/OS Profile Management Tool on a Windows or Linux operating system to generate jobs and instructions for creating profiles for WebSphere Application Server on z/OS systems, or launch the z/OS Migration Management Tool on a Windows or Linux operating system to generate definitions for migrating WebSphere Application Server for z/OS profiles. You can use the Remote Installation Tool for IBM i to install IBM Installation Manager or a WebSphere Application Server product offering from a Windows workstation to a remote target IBM i system.	✓[2, 3]	✓	✓			✓
WebSphere Customization Toolbox (ILAN)	com.ibm.websphere. WCTILAN.v80	AIX, HP-UX, Linux, Solaris, Windows[5]	The WebSphere Customization Toolbox includes tools for customizing various parts of your WebSphere Application Server environment. For example, you can use the WebSphere Customization Toolbox graphical user interface (GUI) to launch the Web Server Plug-ins Configuration Tool to configure your web server plug-ins for any operating system on which the WebSphere Customization Toolbox can be installed. Launch the z/OS Profile Management Tool on a Windows or Linux operating system to generate jobs and instructions for creating profiles for WebSphere Application Server on z/OS systems, or launch the z/OS Migration Management Tool on a Windows or Linux operating system to generate definitions for migrating WebSphere Application Server for z/OS profiles. You can use the Remote Installation Tool for IBM i to install IBM Installation Manager or a WebSphere Application Server product offering from a Windows workstation to a remote target IBM i system. This offering is a no-cost non-supported and non-warranted version of the toolbox.					✓	

Table 1. WebSphere Application Server Version 8 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8 product offerings for supported operating systems.

Offering	Offering ID	Operating systems [1]	Description	Location					
				Product media	Passport Advantage® eImage (Non–z/OS systems only)	Shop ZSeries (z/OS systems only)	Entitled Software Support (ESS)	developer Works	eFD

[1] See Supported hardware and software web page for the complete up-to-date listings on what is supported. If there is a conflict between the information provided in the information center and the information on the *Supported hardware and software* pages, the information at the website takes precedence. Prerequisites information in the information center is provided as a convenience only.

[2] Located on the Supplements disk in the physical media for non-Z/OS systems

[3] Located on its own disk in the physical media for non-Z/OS systems

[4] Installation Manager repositories in SMP/E format, available through CBPDO or ServerPac

[5] Platform-related notes:

- The Profile Management Tool (z/OS only) and z/OS Migration Management Tool that are contained in this toolbox, which create jobs to be run on z/OS systems, can be run on Intel-based Windows and Linux platforms only.
- The Web Server Plug-ins Configuration Tool that is contained in this toolbox can be run on AIX, HP-UX, Linux, Solaris, and Windows operating systems.
- The Remote Installation Tool for IBM i (the iRemoteInstall command) can be run on Windows operating systems only.

  A version of this utility that is current when the product is released is available also on the media or installation image.

Table 2. WebSphere Application Server Version 8 associated products. The following table shows the products associated with WebSphere Application Server Version 8.

Offering	Operating systems	Description	Location			
			Product media	Passport Advantage eImage (Non-z/OS systems only)	Shop ZSeries (z/OS systems only)	Web
IBM Business Solutions Version 5.2 (with WebSphere Application Server - Express only)	AIX, HP-UX, IBM i, Linux, Solaris, Windows	IBM Business Solutions contains a set of enterprise web applications built to run on the J2EE platform provided by IBM WebSphere Application Server for System i®. The applications provide integrated solutions to common business needs that work with your existing applications, server components, and enterprise data.	✓	✓		
IBM DB2® Workgroup Server Edition Limited Use Version 9.7	AIX, HP-UX, Linux, Solaris, Windows	DB2 Workgroup Server Edition is a scalable, full-fledged relational database for small to medium-sized businesses.	✓	✓		
IBM DB2 Enterprise Server Edition Limited Use for zlinux Version 9.7	zLinux	DB2 Enterprise Server Edition is database software capable of handling demanding workloads. Designed for large and mid-sized departmental servers, Enterprise Edition should be used for applications that require flexibility and scalability.				
IBM Installation Manager Version 1.4.3[1]	AIX, HP-UX, IBM i, Linux, Solaris, Windows, z/OS	IBM Installation Manager is a single installation program that can use remote or local software repositories to install, modify, or update new WebSphere Application Server products. It determines and shows available packages—including products, fix packs, interim fixes, and so on—checks prerequisites and interdependencies, and installs the selected packages. You also use Installation Manager to easily uninstall the packages that it installed.	✓	✓	✓ [2]	eFD
IBM Packaging Utility Version 1.4.3	AIX, HP-UX, Linux, Solaris, Windows [3]	IBM Packaging Utility is a program that is used to generate a new repository for packages, copy packages to a new repository, and delete packages that are no longer needed.				✓
IBM Rational® Agent Controller Version 8.3.3	AIX, Linux, zLinux, z/OS	IBM Rational Agent Controller is a daemon process that enables client applications to launch host processes and interact with agents that coexist within host processes.	✓	✓	✓	
IBM Rational Application Developer Standard Edition for WebSphere Application Server Version 8.0.3 Trial	AIX, HP-UX, IBM i, Linux, Solaris, Windows	IBM Rational Application Developer Standard Edition, the enterprise software development solution for Java and Java Enterprise Edition (Java EE), helps development teams deliver solutions for WebSphere Application Server. It includes support for feature packs and integrated test servers.	✓	✓		
IBM Assembly & Deploy Tools for WebSphere Administration Version 8.03	AIX, HP-UX, IBM i, Linux, Solaris, Windows	IBM Assembly and Deploy Tools for WebSphere Administration enable rapid assembly and deployment of applications to WebSphere Application Server environments. These tools replace the previously available IBM Rational Application Developer Assembly and Deploy function and are restricted to assembly and deployment usage only.	✓	✓		
IBM Support Assistant Agent Version 4.1.2	AIX, HP-UX, IBM i, Linux, Solaris, Windows, z/OS	IBM Support Assistant Agent is a software component running on a remote system for the purpose of providing problem determination services to the IBM Support Assistant Workbench. The Agent is an optional, separately installable software component that enables you to perform problem-solving activities on remote systems without leaving the Workbench.				✓
IBM Support Assistant Workbench Version 4.1.2	AIX, HP-UX, IBM i, Linux, Solaris, Windows, z/OS	IBM Support Assistant Workbench is a free serviceability workbench program that simplifies support and helps users resolve questions and problems with IBM software products.				✓
IBM Tivoli® Access Manager for e-business Version 6.1.1	AIX, HP-UX, Linux, Solaris, Windows, z/OS	IBM Tivoli Access Manager for e-business is a user authentication, authorization, and web SSO solution for executing security policies for web and application resources.	✓	✓	✓	
IBM Tivoli Composite Application Manager for WebSphere Application Server Version 7.2	AIX, HP-UX, IBM i, Linux, Solaris, Windows, z/OS	IBM Tivoli Composite Application Manager for WebSphere Application Server monitors the status of transactions in your application server farm. It also provides a complete history of performance and availability and a realtime Visualization Engine. You can use it to find the root cause of problems, troubleshoot them quickly, and enable capacity planning and sizing within a business context.	✓	✓	✓	
IBM Tivoli Directory Server Version 6.3	AIX, HP-UX, Linux, Solaris, Windows	IBM Tivoli Directory Server is an IBM implementation of the Lightweight Directory Access Protocol. IBM Tivoli Directory Server is a standards-compliant enterprise directory for corporate intranets and the Internet.	✓	✓		
IBM Tivoli Federated Identity Manager Version 6.2.2	AIX, HP-UX, Linux, Solaris, Windows	IBM Tivoli Federated Identity Manager offers secure information sharing between trusted parties with federated SSO and a security token service.				✓
IBM WebSphere Adapters Version 7.5	Various, depending on adapter	IBM WebSphere Adapters help accelerate business integration projects with rapidly deployable, enterprise ready connections based on best practices.	✓	✓	✓	
Mozilla Firefox for AIX Version 3.5.8 (64-bit only)	AIX	Mozilla Firefox for AIX is an open source web browser. It implements technologies like the Gecko layout engine and supports Wweb standards or draft standards like HTML, XHTML, XML, CSS, DOM, and more.	✓	✓		

[1] The WebSphere Application Server Version 8.0 packages for distributed and IBM i operating systems contain IBM Installation Manager Version 1.4.3.1.

[2] Installation Manager repositories in SMP/E format, available through CBPDO or ServerPac

[3] IBM i customers can build repositories using the IBM Packaging Utility on a Windows system.
trns: In WebSphere Application Server Version 8 and later, WorldType Fonts are not included with the product. If you require these fonts, change your applications to use newer fonts that are bundled with your operating system or obtain the Infoprint Fonts: WorldType Fonts for AFP Clients (Product 5648-E77).

Directory conventions

References in product information to *app_server_root*, *profile_root*, and other directories imply specific default directory locations. This topic describes the conventions in use for WebSphere Application Server.

Default product locations (distributed)

The following file paths are default locations. You can install the product and other components or create profiles in any directory where you have write access. Multiple installations of WebSphere Application Server Network Deployment products or components require multiple locations. Default values for installation actions by root and nonroot users are given. If no nonroot values are specified, then the default directory values are applicable to both root and nonroot users.

app_client_root

Table 3. Default installation root directories for the Application Client for IBM WebSphere Application Server.

This table shows the default installation root directories for the Application Client for IBM WebSphere Application Server.

User	Directory
Root	AIX `/usr/IBM/WebSphere/AppClient` (Java EE Application client only) HP-UX Linux Solaris `/opt/IBM/WebSphere/AppClient` (Java EE Application client only) Windows `C:\Program Files\IBM\WebSphere\AppClient`
Nonroot	AIX HP-UX Linux Solaris *user_home*`/IBM/WebSphere/AppClient` (Java EE Application client only) Windows `C:\IBM\WebSphere\AppClient`

app_server_root

Table 4. Default installation directories for WebSphere Application Server.

This table shows the default installation directories for WebSphere Application Server Network Deployment.

User	Directory
Root	AIX `/usr/IBM/WebSphere/AppServer` HP-UX Linux Solaris `/opt/IBM/WebSphere/AppServer` Windows `C:\Program Files\IBM\WebSphere\AppServer`
Nonroot	AIX HP-UX Linux Solaris *user_home*`/IBM/WebSphere/AppServer` Windows *user_home*`\IBM\WebSphere\AppServer`

component_root
: The component installation root directory is any installation root directory described in this topic. Some programs are for use across multiple components—in particular, the Web Server Plug-ins, the Application Client, and the IBM HTTP Server. All of these components are part of the product package.

gskit_root
: IBM Global Security Kit (GSKit) can now be installed by any user. GSKit is installed locally inside the installing product's directory structure and is no longer installed in a global location on the

target system. The following list shows the default installation root directory for Version 8 of the GSKit, where *product_root* is the root directory of the product that is installing GSKit, for example IBM HTTP Server or the web server plug-in.

AIX HP-UX Linux Solaris

`*product_root*/gsk8`

Windows

`*product_root*\gsk8`

profile_root

Table 5. Default profile directories.

This table shows the default directories for a profile named profile_name on each distributed operating system.

User	Directory
Root	AIX /usr/IBM/WebSphere/AppServer/profiles/*profile_name* HP-UX Linux Solaris /opt/IBM/WebSphere/AppServer/profiles/*profile_name* Windows C:\Program Files\IBM\WebSphere\AppServer\profiles\profile_name
Nonroot	AIX HP-UX Linux Solaris *user_home*/IBM/WebSphere/AppServer/profiles Windows *user_home*\IBM\WebSphere\AppServer\profiles

plugins_root

Table 6. Default installation root directories for the Web Server Plug-ins.

This table shows the default installation root directories for the Web Server Plug-ins for WebSphere Application Server.

User	Directory
Root	AIX /usr/IBM/WebSphere/Plugins HP-UX Linux Solaris /opt/IBM/WebSphere/Plugins Windows C:\Program Files\IBM\WebSphere\Plugins
Nonroot	AIX HP-UX Linux Solaris *user_home*/IBM/WebSphere/Plugins Windows C:\IBM\WebSphere\Plugins

wct_root

Table 7. Default installation root directories for the WebSphere Customization Toolbox.

This table shows the default installation root directories for the WebSphere Customization Toolbox.

User	Directory
Root	AIX /usr/IBM/WebSphere/Toolbox HP-UX Linux Solaris /opt/IBM/WebSphere/Toolbox Windows C:\Program Files\IBM\WebSphere\Toolbox

Table 7. Default installation root directories for the WebSphere Customization Toolbox (continued).

This table shows the default installation root directories for the WebSphere Customization Toolbox.

User	Directory
Nonroot	AIX HP-UX Linux Solaris `user_home/IBM/WebSphere/Toolbox` Windows `C:\IBM\WebSphere\Toolbox`

web_server_root

Table 8. Default installation root directories for the IBM HTTP Server.

This table shows the default installation root directories for the IBM HTTP Server.

User	Directory
Root	AIX `/usr/IBM/HTTPServer` HP-UX Linux Solaris `/opt/IBM/HTTPServer` Windows `C:\Program Files\IBM\HTTPServer`
Nonroot	AIX HP-UX Linux Solaris `user_home/IBM/HTTPServer` Windows `C:\IBM\HTTPServer`

Hardware and software requirements

The official statements of support for WebSphere Application Server products are provided online at the Supported hardware and software web page.

See Supported hardware and software web page for the complete up-to-date listings on what is supported. If there is a conflict between the information provided in the information center and the information on the Supported hardware and software pages, the information at the website takes precedence. Prerequisites information in the information center is provided as a convenience only.

Required disk space

Disk space requirements vary by operating system and hardware platform. See the following topics for information about required disk space and how to prepare your operating system for installation:

- AIX "Preparing AIX systems for installation" on page 47
- HP-UX "Preparing HP-UX systems for installation" on page 51
- Linux "Preparing Linux systems for installation" on page 56
- Solaris "Preparing Solaris systems for installation" on page 68
- Windows "Preparing Windows systems for installation" on page 71

Space is also required for the installable components in the secondary packet of the product package. Refer to the documentation for each installable component to determine exact space requirements.

Supported operating systems

As mentioned, the official statements of support for operating systems are on the Supported hardware and software website.

The installation programs for WebSphere Application Server products verify that a supported operating system is installed. The verification includes checking for required patches with the prerequisite checker.

Although the Installation Manager checks for prerequisite operating system patches, review the prerequisites on the Supported hardware and software web page if you have not already done so.

Always consult the Supported hardware and software website to determine whether your operating system is supported when you receive a message from the prerequisite checker. In some cases, the website will be more current than the prerequisite checker on a product image. For example, IBM often declares support for new versions of operating systems for a product that is already released. The prerequisite checker might issue a message when, in fact, a new version of an operating system is supported.

The website lists all supported operating systems and the operating system fixes and patches that you must install to have a compliant operating system.

Refer to the product documentation for non-IBM prerequisite and corequisite products, such as browsers, to learn how to migrate to supported versions.

Translated Languages

The WebSphere Application Server Version 8 distributed product is available in these native languages:

- Brazilian Portuguese
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- English
- French
- German
- Hungarian
- Italian
- Japanese
- Korean
- Polish
- Russian
- Spanish

Using the launchpad to start installations

The launchpad console is the starting point for installing IBM WebSphere Application Server Network Deployment.

Before you begin

- The launchpad is a web application. Before using the launchpad, you must have a supported web browser. The launchpad supports the following browsers:
  - AIX HP-UX Linux Solaris Mozilla Firefox Version 3.5 or later
  - Windows Internet Explorer Version 6.0 Service Pack 2 or later
- Install a supported web browser if one is not installed.
  - AIX HP-UX Linux Solaris Install a browser such as Mozilla Firefox. Download Firefox from the following location: http://www.mozilla.org/products/firefox/.
  - Windows Install a browser for the Windows operating system.
    - Download Internet Explorer from the following location: http://www.microsoft.com/windows/ie/default.mspx
    - Download Mozilla Firefox from the following location: http://www.mozilla.org/products/firefox/.

- AIX HP-UX Linux Solaris You must install the Bash shell package to use the launchpad application. Although the Bash shell must be installed, the Bash shell does not need to be used to run the launchpad.sh command. If you attempt to run the launchpad application from a DVD on the HP-UX, Linux, or Solaris operating systems without the Bash shell installed, the launchpad fails with an error message indicating that the Bash interpreter is not found. If you attempt to run the launchpad from any image on AIX, the launchpad fails with an error message indicating that the current browser is not supported. The Bash package for the AIX operating system is included in the IBM AIX Toolbox.

Examples of what the launchpad can do:

- The launchpad does support installing Installation Manager Version 1.4.3.1 in admin or non-admin (user) mode.
- The launchpad does support updating Installation Manager to Version 1.4.3.1 from an earlier version in admin or non-admin (user) mode.

Examples of what the launchpad cannot do:

- The launchpad does not support installing in group mode.
- The launchpad does not support installing or updating with a custom application data location.

Restriction: You cannot run the launchpad remotely to install a product. Only local use of the launchpad is supported.

About this task

The launchpad identifies components on the product disk or image that you can install (launch).

WebSphere Application Server is an integrated platform that contains an application server, a set of web development tools, a web server, and additional supporting software and documentation. The launchpad is a single point of reference for installing the entire application server environment. If you click a link that points to a product repository on another disk or image, you are prompted to insert that disk or browse to that image. For example, IBM HTTP Server, Web Server Plug-ins for IBM WebSphere Application Server, and Application Client for IBM WebSphere Application Server are on the supplements disk. If you click a link to launch those products, you must insert the supplements disk in the disk drive or point the installer to the product repositories to install the product from the launchpad.

Procedure

1. Start the launchpad.

   The launchpad program is available in the root directory of the product disk or the downloaded installation image. You can start the launchpad manually using a fully qualified command instead of changing directories to the disk and running the command locally from the root directory:

   - AIX HP-UX Linux Solaris Mount the disk drive if necessary. This procedure varies per platform. See “Mounting disk drives on operating systems such as AIX and Linux” on page 119.
   - Open a shell window and issue a fully qualified command to start the launchpad:
     - AIX HP-UX Linux Solaris `./launchpad.sh`
     - Windows `launchpad.bat`

   Tip: Windows If you need to navigate using the keyboard, use Mozilla Firefox as your web browser and start the launchpad with the following command:

```
launchpad_a11y.exe
```

Note: Windows Some Windows operating systems such as Windows 2003, Windows Vista, Windows Server 2008, and Windows 7 have implemented a more restrictive security policy that denies access to trusted files by non-trusted files or applications. When the launchpad application is run as a non-trusted program, you will receive JavaScript "Access is denied" errors that subsequently cause the application to hang. Because downloaded images are automatically blocked, unblock the files so that the launchpad can successfully access the files. Before you extract the image, right-click the image file and select **Properties** to open the Properties panel and locate the security section and click the **Unblock** button. You can now extract the image and run the launchpad application.

The launchpad opens in the language of the locale setting of the machine.

2. Use the launchpad to perform the following tasks.
   - View the Welcome page, and access links to the WebSphere Application Server Information Center and the IBM Education Assistant.
   - Launch Installation Manager installation, and access the IBM Installation Manager Information Center.
   - Download the latest version of IBM Packaging Utility, and access the IBM Packaging Utility Information Center.
   - Launch Installation Manager to install WebSphere Application Server Network Deployment
   - Launch Installation Manager to install DMZ Secure Proxy Server for IBM WebSphere Application Server.
   - Launch Installation Manager to install IBM HTTP Server
   - Launch Installation Manager to install Web Server Plug-ins for IBM WebSphere Application Server.
   - Launch Installation Manager to install the WebSphere Customization Toolbox.
   - Launch Installation Manager to install Application Clients.
   - Launch Installation Manager to install IBM WebSphere Edge Components: Load Balancer for IPv4 and IPv6.
   - Access the WebSphere Application Server Information Center for information on obtaining and installing IBM WebSphere Edge Components: Load Balancer for IPv4.
   - Access the WebSphere Application Server Information Center for information on obtaining and installing IBM WebSphere Edge Components: Caching Proxy.
   - Access the latest version of IBM Support Assistant.
   - Launch the installation for IBM Tivoli Composite Application Manager for WebSphere Application Server.
   - Access the latest version of the Tivoli Federated Identity Manager for WebSphere Application Server Network Deployment.
   - Launch Installation Manager to install IBM WebSphere Adapters Version 7.5.

Results

This procedure results in using the launchpad to start the installation and to access information through a browser.

Troubleshooting

If you can start the launchpad but clicking a link does not resolve to a page in the launchpad, you might have the wrong media in the disk drive. Check the validity of the media.

Use the following procedure to correct any error that is preventing the launchpad from displaying. Then, try to start the launchpad again:

1. If the product disk is no longer accessible, insert the disk.

2. AIX HP-UX Linux Solaris Mount the drive as necessary on platforms such as AIX or Linux.
3. Enable the JavaScript function in your browser.

   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**.
4. Restart the launchpad by issuing the following command:
   - AIX HP-UX Linux Solaris ./launchpad.sh
   - Windows launchpad.bat

If the launchpad links still do not work after following this procedure, launch the programs directly.

What to do next

Go to "Installing and uninstalling the product on distributed operating systems" on page 74 to continue installing your application serving environment.

Product version information

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

Run the historyInfo command to create a report about installed maintenance packages. The historyInfo command creates a report on the console.

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

This topic includes the following sections:
- "Product information files"
- "Reports"
- "Logs and backup directories locations" on page 21

Product information files

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

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

Reports

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

- Product version reports

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

    Lets you use parameters to create a version report on all supported platforms.

  - genVersionReport command

    Generates the `versionReport.html` report file in the `bin` directory on all supported platforms. The report includes the list of components and installed and uninstalled maintenance packages.

- Product history reports

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

  - historyInfo command

    Lets you use parameters to create a history report on all supported platforms.

  - genHistoryReport command

    Generates the `historyReport.html` report file in the `bin` directory on all supported platforms. The report includes the list of components and a history of installed and uninstalled maintenance packages.

Logs and backup directories locations

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

app_server_root **`/logs/update`**

Logs directory for product updates

app_server_root/**`properties/patches/backup`**

Backup directory for product updates

WebSphere Application Server products back up components before applying interim fixes.

Chapter 4. Planning the WebSphere Application Server product installation

This article introduces common installation scenarios for a WebSphere Application Server product.

Before you begin

Determine what components you want to use for your web serving environment. The installation scenarios can help you to understand the capabilities of your WebSphere Application Server product. Knowing what you can do with the product might influence how you install the product and other components.

About this task

The installation scenarios use topology diagrams and descriptions to show what components to install for a given topology. The scenarios also have installation steps that link to specific procedures for installing a component, running a command, or using a tool.

Review the scenarios to determine which topology best fits your needs. The diagrams and their accompanying procedures can serve as a roadmap for installing a similar topology.

Procedure

1. Review the installation scenarios for the WebSphere Application Server Network Deployment product, as described in “Planning to install WebSphere Application Server” on page 24.
2. Review the installation scenarios for the Web Server Plug-ins for WebSphere Application Server as described in the article "Selecting a web server topology diagram and roadmap".
3. Review the installation scenarios Application Client for IBM WebSphere Application Server as described in “Planning to install the Application Client for IBM WebSphere Application Server” on page 40.
4. Optional: Review interoperability and coexistence scenarios to know what is possible with the current version.

   WebSphere Application Server can interoperate with your other e-business systems, including other versions of WebSphere Application Server. *Interoperability* provides a communication mechanism for WebSphere Application Server nodes that are at different versions, running on separate machines. *Coexistence* describes multiple versions or instances running on the same machine at the same time.

   Interoperability support enhances migration scenarios with more configuration options. Interoperating is often more convenient or practical during the migration of a configuration from an earlier WebSphere Application Server version to a later one. Some machines can have the earlier product version and other machines can have the later version. An environment of machines and application components at different software version levels can involve both interoperability and coexistence.

   It is often impractical, or even physically impossible, to migrate all of the machines and applications within an enterprise at the same time. Understanding multiversion interoperability and coexistence is therefore an essential part of a migration between version levels. See the migration documentation for more information.
5. Optional: Consider performance when designing your network as described in the documentation for the performance topologies and Queing network.

Results

Following this procedure results in reviewing installation scenarios to identify specific steps to follow when installing more than one component.

What to do next

After determining an appropriate installation scenario, install the necessary components and configure the products for the system that you selected.

Planning to install WebSphere Application Server

Consider common installation scenarios for the product to determine how to install your application serving environment.

Before you begin

IBM WebSphere Application Server Network Deployment is an integrated platform that contains an application server, web development tools, a web server, and additional supporting software and documentation.

The installation of the application server product installs a shared set of core product files. Afterwards, you create at least one *profile*, which is a separate data partition that includes the files that define a runtime environment for an application server process, such as a deployment manager or an application server.

A running application server process can create, read, update, or delete the configuration files, data files, and log files in its profile. The application server process can access the core product files, which include command files and other shared product binary files. However, most core product or system files are updated only by installing fix packs, interim fixes, or products that extend the product.

After installation, you can create an *application server profile*, a *management profile*, a *cell set of profiles* that contains a deployment manager and a federated application server, or a *custom profile*. At least one profile must exist to have a functioning application server environment. You can use the Profile Management Tool or the manageprofiles command to create profiles.

You must first prepare your operating system for installation before installing any of the below topologies. See Chapter 5, “Preparing the operating system for product installation,” on page 47 for more information.

Note: It is suggested that you configure WebSphere Application Server Network Deployment with a single subnet for network traffic. You can use one Network interface card (NIC) on a physical machine or logical partition (LPAR). You can also reference a single domain name system (DNS) server in the network configuration for the physical machine or LPAR.

The following information describes scenarios for installing the product in various topologies on one or more machines. Two types of application server topologies are possible using the Network Deployment product.

Topologies for a standalone application server

Each standalone application server runs independently of other application servers.

The following application server topologies are described in this article.

- **Scenario 1:** Single-machine installation of a standalone application server
- **Scenario 2:** Single-machine installation of a standalone application server and a web server
- **Scenario 3:** Two-machine installation of a standalone application server and a web server
- **Scenario 4:** Two-machine installation of multiple standalone application servers and web servers
- **Scenario 5:** Flexible administration of a two-machine installation of multiple standalone application servers and web servers

Topologies for a managed group of application servers in a cell

A *cell* consists of one deployment manager and one or more federated application servers that are *managed nodes*. The deployment manager is the single point of administration for all of the managed nodes in the cell. The deployment manager maintains the configuration files for nodes that it manages and deploys applications to those managed nodes.

An application server can become a managed node in the following ways:

- By creating the cell with a federated node
- By federating the node within an application server profile into the cell
- By federating the node within a custom profile into the cell

Scenarios 6 - 10 assume that all nodes in a cell reside on a particular machine and operating system. However, this precise node assignment does not need to apply. The deployment manager node can exist on Machine A, other managed nodes (that have been federated into the deployment manager) can exist on differing machines and operating systems. Such a configured cell of differing machines or operating systems is called a `heterogeneous cell` and expands the possible topologies that you can consider for your network deployment.

The following topologies for a cell are described in this article.

- **Scenario 6:** Single-machine installation of a cell of application servers
- **Scenario 7:** Single-machine installation of a cell of application servers and a web server
- **Scenario 8:** Two-machine installation of a cell of application servers and a web server
- **Scenario 9:** Three-machine installation of a cell of application servers and a web server
- **Scenario 10:** Flexible administration of a four-machine installation of mixed runtime environments using the job manager

Topologies that include DMZ Secure Proxy Server for IBM WebSphere Application Server

DMZ Secure Proxy Server for IBM WebSphere Application Server delivers a high performance reverse proxy capability that can be used at the edge of the network to route, load balance, and improve response times for requests to web resources. Comapared to a web server, DMZ Secure Proxy Server for IBM WebSphere Application Server provides increased flexibility, improved integration with WebSphere systems management, improved workload balancing, and other enhancements. DMZ Secure Proxy Server for IBM WebSphere Application Server does not contain a web container and therefore does not have an administration console.

The product can be administered in a number of secure ways depending on various possible topologies.

- Administration with the wsadmin utility.

  This requires local access to the DMZ Secure Proxy Server for IBM WebSphere Application Server.
- Administration from an external web console.

  The product is configured through a profile on the deployment manager node, exported, and imported to the DMZ Secure Proxy Server for IBM WebSphere Application Server node.
- Flexible administration from a remote job manager.

  A secure proxy profile is deployed on the DMZ Secure Proxy Server for IBM WebSphere Application Server node and registered to an administrative agent on that same machine. The administrative agent is then registered to and managed by a remote job manager.

The second administrative topology for the DMZ Secure Proxy Server for IBM WebSphere Application Server is described in this article.

- **Scenario 11:** Remote administration of a DMZ Secure Proxy Server for IBM WebSphere Application Server from a deployment manager node

Some scenarios are more typical in production environments. For example, Scenario 1 supports a lighter workload than Scenario 3 or Scenario 4. However, Scenario 1 is a fully functional environment. Scenarios 3 - 5 are typical production environments for a standalone application server. Scenarios 9 is a typical production scenario for a simple cell environment.

Procedure

- **Scenario 1:** Install a standalone application server on a single machine.

  Install WebSphere Application Server Network Deployment by itself on a single machine, and create a standalone application server profile. Each standalone application server profile includes a server1 application server process. Each profile defines a separate standalone application server that has its own administrative interface.

  You can use the Profile Management Tool or the manageprofiles command to create profiles after installation.

  In this scenario, the application server uses its internal HTTP transport chain for communication instead of a using a separate web server (on a separate machine) to possibly offload some processing.

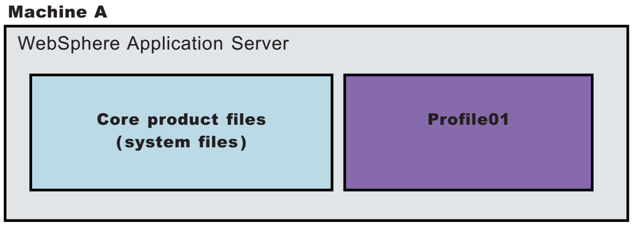

Machine A
WebSphere Application Server
Core product files (system files)
Profile01

Table 9. Installing a standalone application server on a single machine.

Complete these steps:

Step	Task
1	Install IBM Installation Manager.
2	Use Installation Manager to install WebSphere Application Server Network Deployment.
3	Use the Profile Management Tool or the manageprofiles command to create a standalone application server profile.

- **Scenario 2:** Install a standalone application server and a web server on a single machine.

  Installing a web server, such as IBM HTTP Server, on the same machine as the application server provides more configuration options. Installing a web server plug-in enables the web server to communicate with the application server. This installation scenario supports rigorous testing environments or production environments that do not require a firewall. However, this scenario is not a typical production environment. When everything is on one machine, neither the web server or the application server will run as fast as if they were on separate machines because they are both competing for the same CPU resources.

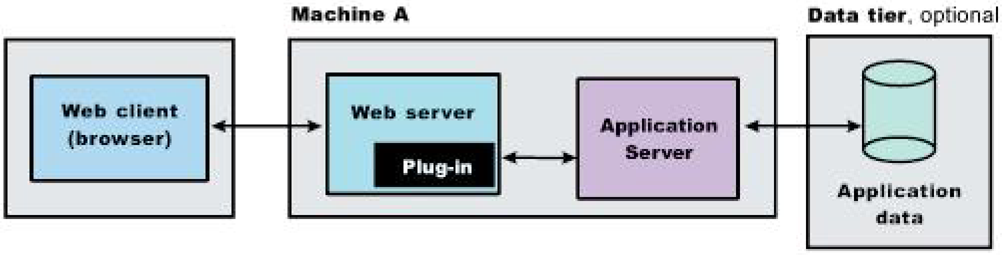


Table 10. Installing a standalone application server and a web server on a single machine.

Complete these steps:

Step	Task
1	Install IBM Installation Manager.

Table 10. Installing a standalone application server and a web server on a single machine (continued).

Complete these steps:

Step	Task
2	Use Installation Manager to install the following: • WebSphere Application Server Network Deployment • Web Server Plug-ins for WebSphere Application Server • WebSphere Customization Toolbox
3	Use the Profile Management Tool or the manageprofiles command to create a standalone application server profile.
4	Use Installation Manager to install IBM HTTP Server, or install another supported web server.
5	Open the WebSphere Customization Toolbox, and launch the Web Server Plug-ins Configuration Tool to configure the web server plug-in and create the web server definition. The web server definition is automatically created and configured during the configuration of the plug-in.

- **Scenario 3:** Install a standalone application server and a web server on separate machines.

  In the typical production environment, the application server on one machine communicates with a web server on a separate (remote) machine through the web server plug-in. After creating a profile and installing a dedicated web server, use the Web Server Plug-ins for WebSphere Application Server and Web Server Plug-ins Configuration Tool to install a plug-in and to update the web server configuration file. The Web server can then communicate with the application server. Optional firewalls can provide additional security for the application server machine.

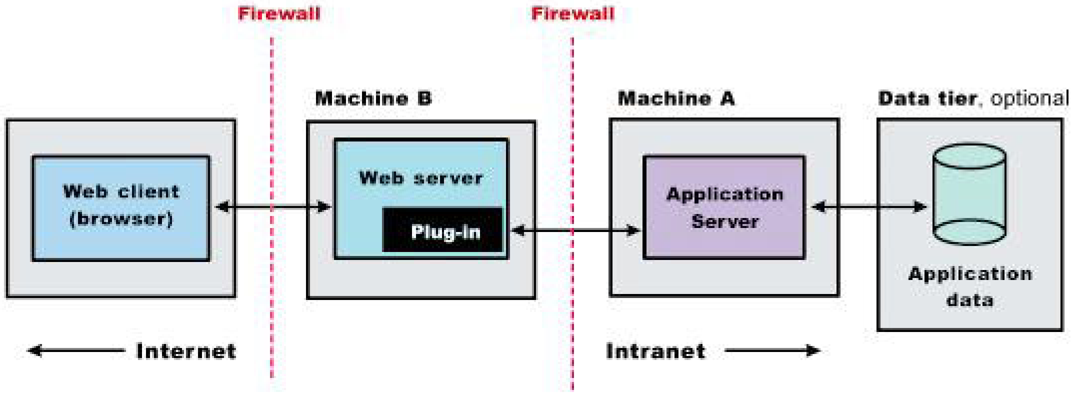


Table 11. Installing a standalone application server and a web server on separate machines.

Complete these steps:

Step	Machine	Task
1	A	Install IBM Installation Manager.
2	A	Use Installation Manager to install WebSphere Application Server Network Deployment.
3	A	Use the Profile Management Tool or the manageprofiles command to create a standalone application server profile.
4	B	Install IBM Installation Manager.
5	B	Use Installation Manager to install the following: • Web Server Plug-ins for WebSphere Application Server • WebSphere Customization Toolbox
6	B	Use Installation Manager to install IBM HTTP Server, or install another supported web server.
7	B	Open the WebSphere Customization Toolbox, and launch the Web Server Plug-ins Configuration Tool to configure the web server plug-in and create the web server definition. The script for creating and configuring the web server is created under the *plugins_root*/bin directory.

Table 11. Installing a standalone application server and a web server on separate machines (continued).

Complete these steps:

Step	Machine	Task
8	B	Copy the `configureweb_server_name` script to paste on Machine A. If one machine is running under an operating system such as AIX or Linux and the other machine is running under Windows, copy the script from the `plugins_root/bin/crossPlatformScripts` directory.
9	A	Paste the `configureweb_server_name` script from Machine B to the `profile_root/bin` directory on Machine A.
10	A	Start the application server.
11	A	Run the `configureweb_server_name` script on Machine A to create a web server definition in the administrative console.
12	A	Open the administrative console, and save the changed configuration.
13	B	Start the web server. AIX HP-UX Linux Solaris Source the `plugins_root/setupPluginCfg.sh` script for a Domino® Web Server before starting a Domino Web Server.
14	A	Propagate the `plugin-cfg.xml` file on Machine A from the application server to the web server using the administrative console. 1. Click **Servers** > **Web servers**. 2. On the web servers page, place a check mark beside the web server for which you want to propagate a plug-in, and click **Propagate Plug-in**. Web servers other than IBM HTTP Server require manual propagation.

- **Scenario 4:** Install multiple standalone application servers on one machine and one or more web servers on a separate machine.

  The Profile Management Tool or the manageprofiles command can create a deployment manager profile, an application server profile, or a custom profile. After creating a profile and installing a dedicated web server, use the Web Server Plug-ins for WebSphere Application Server and Web Server Plug-ins Configuration Tool to install a plug-in and to update the web server configuration file. The web server can then communicate with the application server. In this configuration, this process must be done for each profile and web server combination.

  This topology lets each profile have unique applications, configuration settings, data, and log files while sharing the same set of core product files. Creating multiple profiles creates multiple application server environments that you can dedicate to different purposes. For example, each application server on a website can serve a different application. In another example, each application server can be a separate test environment that you assign to a programmer or a development team.

  Another feature of having multiple profiles is enhanced serviceability. When a fix pack updates the system files, for example, all application servers begin using the updated core product files.

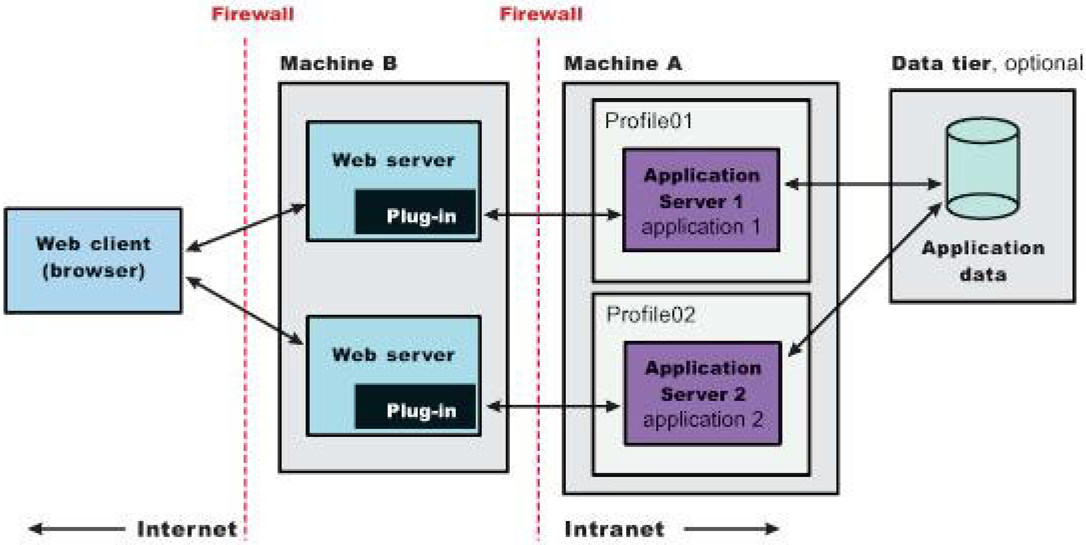


Table 12. Installing multiple standalone application servers on one machine and one or more web servers on a separate machine.

Complete these steps:

Step	Machine	Task
1	A	Install IBM Installation Manager.
2	A	Use Installation Manager to install WebSphere Application Server Network Deployment.
3	A	Use the Profile Management Tool or the manageprofiles command to create a standalone application server profile.
4	B	Install IBM Installation Manager.
5	B	Use Installation Manager to install the following: • Web Server Plug-ins for WebSphere Application Server • WebSphere Customization Toolbox
6	B	Use Installation Manager to install IBM HTTP Server, or install another supported web server.
7	B	Open the WebSphere Customization Toolbox, and launch the Web Server Plug-ins Configuration Tool to configure the web server plug-in and create the web server definition. The script for creating and configuring the web server is created under the `*plugins_root*/bin` directory.
8	B	Copy the `configure*web_server_name*` script to paste on Machine A. If one machine is running under an operating system such as AIX or Linux and the other machine is running under Windows, copy the script from the `*plugins_root*/bin/crossPlatformScripts` directory.
9	A	Paste the `configure*web_server_name*` script from Machine B to the `*profile_root*/bin` directory on Machine A.
10	A	Start the application server.
11	A	Run the `configure*web_server_name*` script on Machine A to create a web server definition in the administrative console.
12	A	Open the administrative console, and save the changed configuration.
13	B	Start the web server. AIX HP-UX Linux Solaris Source the `*plugins_root*/setupPluginCfg.sh` script for a Domino Web Server before starting a Domino Web Server.
14	A	Propagate the `plugin-cfg.xml` file on Machine A from the application server to the web server using the administrative console. 1. Click **Servers** > **Web servers**. 2. On the web servers page, place a check mark beside the web server for which you want to propagate a plug-in, and click **Propagate Plug-in**. Web servers other than IBM HTTP Server require manual propagation.
15	A	Create subsequent standalone application server profiles using the Profile Management Tool or the manageprofiles command on Machine A.
16	B	Install subsequent IBM HTTP Servers or other supported web servers on Machine B.

Table 12. Installing multiple standalone application servers on one machine and one or more web servers on a separate machine (continued).

Complete these steps:

Step	Machine	Task
17	A - B	Repeat steps 7through 14 to configure each additional web server on Machine B with each newly-added application server. Each application server profile is now directly associated with its own web server.

- **Scenario 5:** Install an administrative agent and multiple registered application servers and multiple web servers on separate machines.

  The application servers on one machine communicate with a web server on a separate (remote) machine through the web server plug-in. The application servers are registered with the administrative agent. The administrative agent provides a single location from which to administer the nodes registered to it. Optional firewalls can provide additional security for the application server machine.

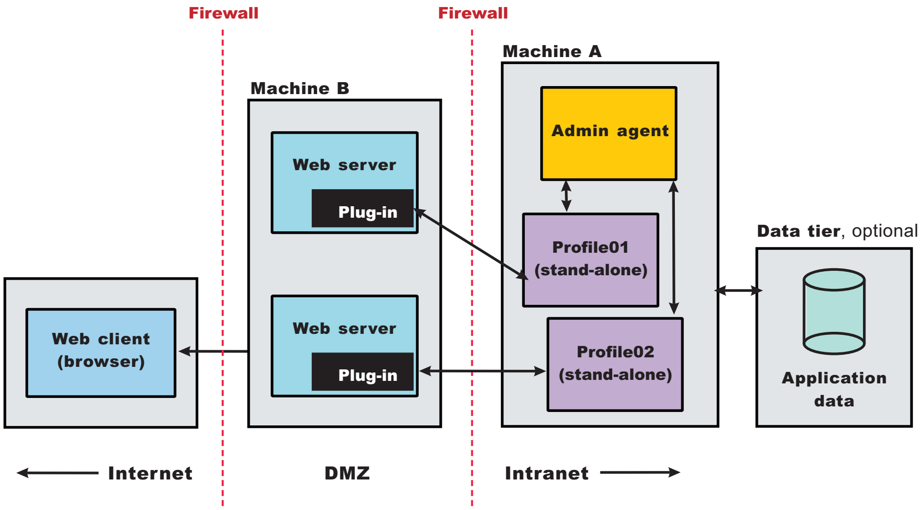


Table 13. Installing an administrative agent and multiple registered application servers and multiple web servers on separate machines.

Complete these steps:

Step	Machine	Task
1	A	Install IBM Installation Manager.
2	A	Use Installation Manager to install WebSphere Application Server Network Deployment.
3	A	Use the Profile Management Tool or the manageprofiles command to create a management profile of the administrative agent server type.
4	A	Use the Profile Management Tool or the manageprofiles command to create an application server profile.
5	A	Register the application server with the administrative agent by running the registerNode command in the bin directory of the administrative agent profile, `profile_root/bin`.
6	B	Install IBM Installation Manager.
7	B	Use Installation Manager to install the following: • Web Server Plug-ins for WebSphere Application Server • WebSphere Customization Toolbox
8	B	Use Installation Manager to install IBM HTTP Server, or install another supported web server.

Table 13. Installing an administrative agent and multiple registered application servers and multiple web servers on separate machines (continued).

Complete these steps:

Step	Machine	Task
9	B	Open the WebSphere Customization Toolbox, and launch the Web Server Plug-ins Configuration Tool to configure the web server plug-in and create the web server definition. The script for creating and configuring the web server is created under the `plugins_root/bin` directory.
10	B	Copy the `configureweb_server_name` script to paste on Machine A. If one machine is running under an operating system such as AIX or Linux and the other machine is running under Windows, copy the script from the `plugins_root/bin/crossPlatformScripts` directory.
11	A	Paste the `configureweb_server_name` script from Machine B to the `profile_root/bin` directory on Machine A.
12	A	Start the application server.
13	A	Run the `configureweb_server_name` script on Machine A to create a web server definition in the administrative console.
14	A	Open the administrative console, and save the changed configuration.
15	B	Start the web server. AIX HP-UX Linux Solaris Source the `plugins_root/setupPluginCfg.sh` script for a Domino Web Server before starting a Domino Web Server.
16	A	Propagate the `plugin-cfg.xml` file on Machine A from the application server to the web server using the administrative console. 1. Click **Servers** > **Web servers**. 2. On the web servers page, place a check mark beside the web server for which you want to propagate a plug-in, and click **Propagate Plug-in**. Web servers other than IBM HTTP Server require manual propagation.
17	A	Create subsequent application server profiles using the Profile Management Tool or the manageprofiles command on Machine A.
18	A	Register the new application server with the administrative agent by running the registerNode command in the bin directory of the administrative agent profile, `profile_root/bin`.
19	B	Install subsequent IBM HTTP Servers or other supported web servers on Machine B.
20	A - B	Repeat steps 9 through 16 to configure each additional web server on Machine B with each newly-added application server. Each application server profile is now directly associated with its own web server.

- **Scenario 6:** Install a cell of managed application servers on one machine.

  WebSphere Application Server Network Deployment can create a cell consisting of a deployment manager and one federated application server node on a single machine. After installation, create a cell set of profiles. You can use the Profile Management Tool or the manageprofiles command to create other standalone application server profiles or custom profiles. You can use the administrative interface of the deployment manager to federate the additional servers to the cell. The cell profile type is not recommended for production.

  Standalone application server profiles have their own administrative interface until you federate them into a deployment manager cell, at which point the administrative interface of the deployment manager controls the servers, which are at that point called *managed nodes*. Periodically the configuration and application files on a managed node are refreshed from the master copy of the files hosted on the deployment manager during *synchronization*. An application server profile has a default application server process called server1 and optionally might include the default application. A custom profile does not have a default server process nor does it have any applications.

  In a cell environment, only the managed nodes serve applications, not the deployment manager. The managed node in this scenario uses its internal HTTP transport chain for communication instead of a using a separate web server (on a separate machine) to possibly offload some processing.

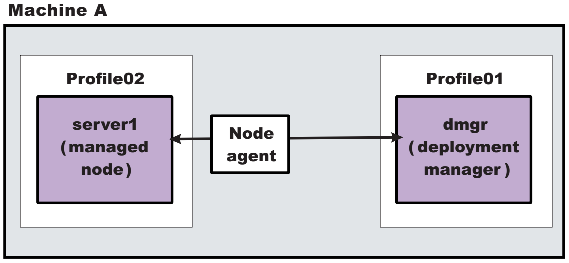


Table 14. Installing a cell of managed application servers on one machine.

Complete these steps:

Step	Task
1	Install IBM Installation Manager.
2	Use Installation Manager to install WebSphere Application Server Network Deployment.
3	Use the Profile Management Tool or the manageprofiles command to create a management profile of the deployment manager server type.
4	Use the Profile Management Tool or the manageprofiles command to create application server profiles.
5	Federate the application servers into the cell using the administrative console of the deployment manager. Click **System Administration > Nodes > Add Node**.
6	Start the deployment manager using its First steps console or by running the startManager command in the `bin` directory of the deployment manager profile, *profile_root*/`bin`.
7	Start the administrative console of the deployment manager using its First steps console.
8	Start the node agent process by running the startNode command in the `bin` directory of the application server profile, *profile_root*/`bin`.
9	Use the administrative console of the deployment manager to create and start application server processes. Click **Servers > Server Types > WebSphere application servers >** ***server_name***.

- **Scenario 7:** Install a cell of managed application servers and a web server on one machine.

  Installing a web server, such as IBM HTTP Server, on the same machine as the application server provides more configuration options. Installing a web server plug-in is required for the web server to communicate with the server in the managed node. This type of installation can support either rigorous testing in a cell environment or production environments that do not require a firewall.

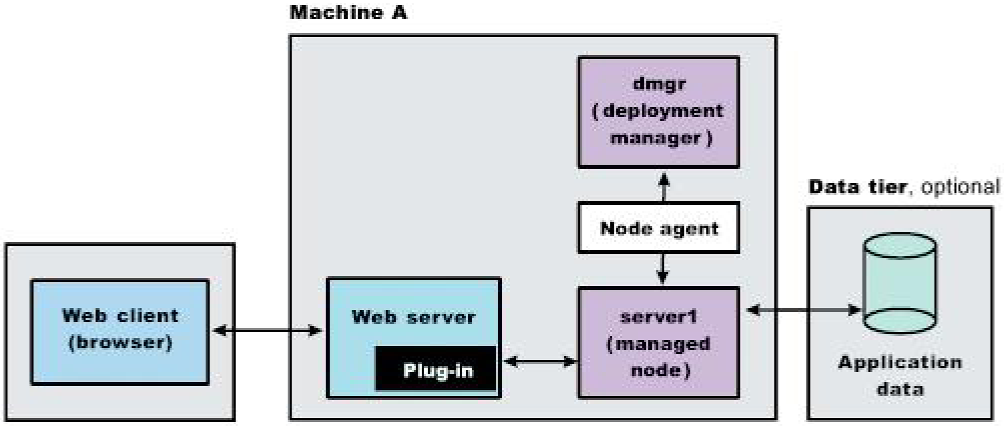


Table 15. Installing a cell of managed application servers and a web server on one machine.

Complete these steps:

Step	Task
1	Install IBM Installation Manager.
2	Use Installation Manager to install the following: • WebSphere Application Server Network Deployment • Web Server Plug-ins for WebSphere Application Server • WebSphere Customization Toolbox
3	Use the Profile Management Tool or the manageprofiles command to create a management profile of the deployment manager server type.
4	Use the Profile Management Tool or the manageprofiles command to create application server profiles.
5	Federate the application servers into the cell using the administrative console of the deployment manager. Click **System Administration** > **Nodes** > **Add Node**.
6	Start the deployment manager using its First steps console or by running the startManager command in the `bin` directory of the deployment manager profile, *`profile_root`*`/bin`.
7	Start the administrative console of the deployment manager using its First steps console.
8	Start the node agent process by running the startNode command in the `bin` directory of the application server profile, *`profile_root`*`/bin`.
9	Use the administrative console of the deployment manager to create and start application server processes. Click **Servers** > **Server Types** > **WebSphere application servers** > ***server_name***.
10	Use Installation Manager to install IBM HTTP Server, or install another supported web server.
11	Open the WebSphere Customization Toolbox, and launch the Web Server Plug-ins Configuration Tool to configure the web server plug-in and create the web server definition. The web server definition is automatically created and configured during the configuration of the plug-in.

- **Scenario 8:** Install a cell of managed application servers on one machine and a web server on a separate machine.

  In a typical production environment, a managed node in a cell communicates with a web server on a separate (remote) machine through the web server plug-in. An optional firewall can provide additional security for the application server machine.

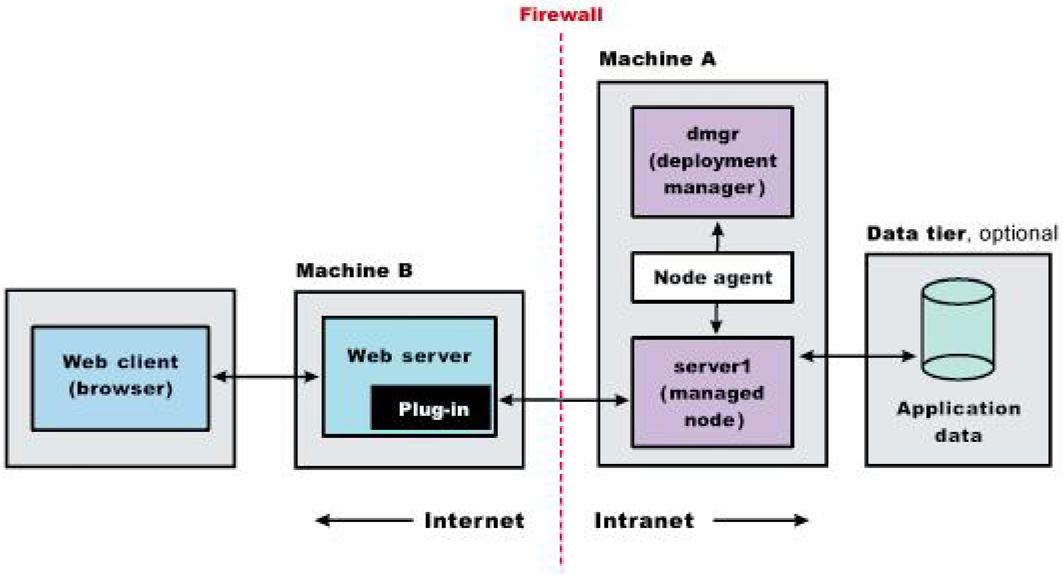


Table 16. Installing a cell of managed application servers on one machine and a web server on a separate machine.

Complete these steps:

Step	Machine	Task
1	A	Install IBM Installation Manager.
2	A	Use Installation Manager to install WebSphere Application Server Network Deployment.
3	A	Use the Profile Management Tool or the manageprofiles command to create a management profile of the deployment manager server type.
4	A	Use the Profile Management Tool or the manageprofiles command to create application server profiles.
5	A	Federate the application servers into the cell using the administrative console of the deployment manager. Click **System Administration > Nodes > Add Node**.
6	A	Start the deployment manager using its First steps console or by running the startManager command in the `bin` directory of the deployment manager profile, *`profile_root`*`/bin`.
7	A	Start the administrative console of the deployment manager using its First steps console.
8	A	Start the node agent process by running the startNode command in the `bin` directory of the application server profile, *`profile_root`*`/bin`.
9	A	Use the administrative console of the deployment manager to create and start application server processes. Click **Servers > Server Types > WebSphere application servers > *server_name*.**.
10	B	Install IBM Installation Manager.
11	B	Use Installation Manager to install the following: • Web Server Plug-ins for WebSphere Application Server • WebSphere Customization Toolbox
12	B	Use Installation Manager to install IBM HTTP Server, or install another supported web server.
13	B	Open the WebSphere Customization Toolbox, and launch the Web Server Plug-ins Configuration Tool to configure the web server plug-in and create the web server definition. The script for creating and configuring the web server is created under the *`plugins_root`*`/bin` directory.
14	B	Copy the `configure`*`web_server_name`* script to paste on Machine A. If one machine is running under an operating system such as AIX or Linux and the other machine is running under Windows, copy the script from the *`plugins_root`*`/bin/crossPlatformScripts` directory.
15	A	Paste the `configure`*`web_server_name`* script from Machine B to the *`profile_root`*`/bin` directory on Machine A.
16	A	Start the application server.
17	A	Run the `configure`*`web_server_name`* script on Machine A to create a web server definition in the administrative console.
18	A	Open the administrative console, and save the changed configuration.
19	B	Start the web server. AIX HP-UX Linux Solaris Source the *`plugins_root`*`/setupPluginCfg.sh` script for a Domino Web Server before starting a Domino Web Server.
20	A	Propagate the `plugin-cfg.xml` file on Machine A from the application server to the web server using the administrative console. 1. Click **Servers** > **Web servers**. 2. On the web servers page, place a check mark beside the web server for which you want to propagate a plug-in, and click **Propagate Plug-in**. Web servers other than IBM HTTP Server require manual propagation.

- **Scenario 9:** Install a deployment manager on one machine, multiple managed application server nodes on a second machine, and a web server on a third machine.

  The primary advantage of a cell over a standalone application server is its scalability. Managing a cell to keep it in proportion with workload levels is possible. In this scenario, managed nodes exist on Machine C. All of the managed nodes are federated into the same deployment manager. Depending on your needs, an application server in each managed node could serve the same or different applications.

  Machine A and Machine C represent both types of scaling, vertical and horizontal scaling:

  – *Vertical scaling* creates multiple managed nodes on the same physical machine.

  – *Horizontal scaling* creates cell members on multiple physical machines.

The managed nodes in this scenario communicate with the same web server. An alternative strategy, however, could have a dedicated web server for each managed node.

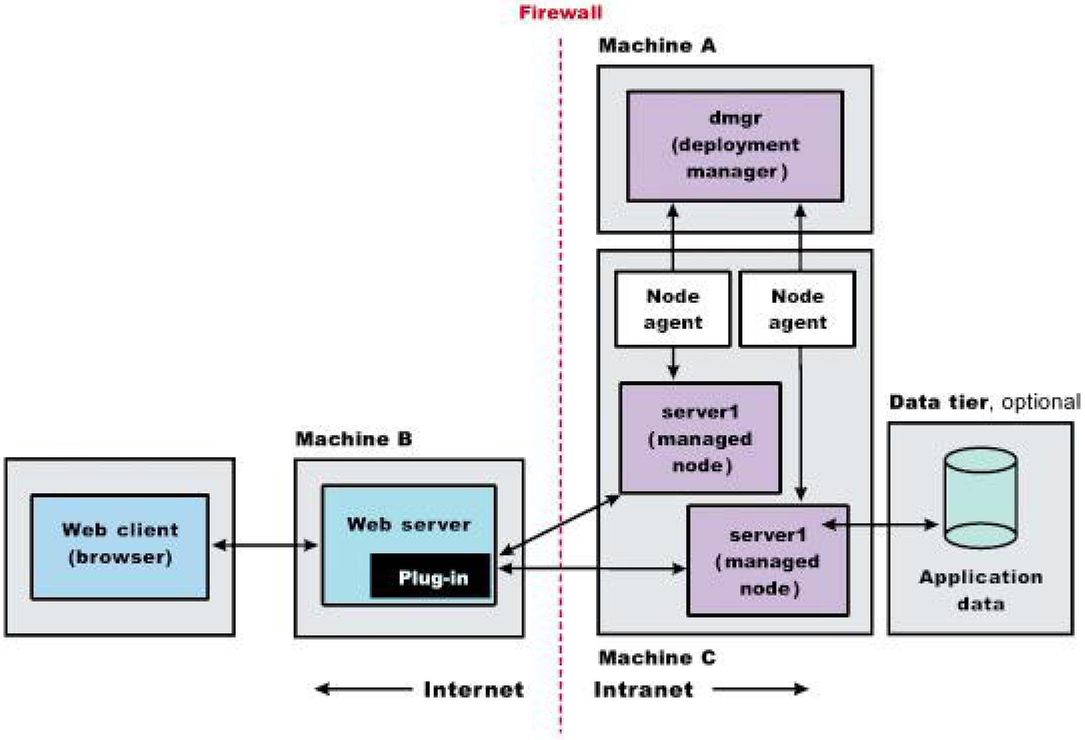


Table 17. Installing a deployment manager on one machine, multiple managed application server nodes on a second machine, and a web server on a third machine.

Complete these steps:

Step	Machine	Task
1	A	Install IBM Installation Manager.
2	A	Use Installation Manager to install WebSphere Application Server Network Deployment.
3	A	Use the Profile Management Tool or the manageprofiles command to create a management profile of the deployment manager server type.
4	A	Start the deployment manager using its First steps console or by running the startManager command in the `bin` directory of the deployment manager profile, *profile_root*/`bin`.
5	C	Install IBM Installation Manager.
6	C	Use Installation Manager to install WebSphere Application Server Network Deployment.
7	C	Use the Profile Management Tool or the manageprofiles command to create multiple application server profiles.
8	C	Start each application server using its First steps console or by running the startServer command in the `bin` directory of the application server profile, *profile_root*/`bin`.
9	A	On Machine A, add the application server nodes to the cell using the administrative console of the deployment manager. Click **System Administration > Nodes > Add Node**.
10	B	Install IBM Installation Manager.
11	B	Use Installation Manager to install the following: • Web Server Plug-ins for WebSphere Application Server • WebSphere Customization Toolbox
12	B	Use Installation Manager to install IBM HTTP Server, or install another supported web server.
13	B	Open the WebSphere Customization Toolbox, and launch the Web Server Plug-ins Configuration Tool to configure the web server plug-in and create the web server definition. The script for creating and configuring the web server is created under the *plugins_root*/`bin` directory.

Table 17. Installing a deployment manager on one machine, multiple managed application server nodes on a second machine, and a web server on a third machine (continued).

Complete these steps:

Step	Machine	Task
14	B	Copy the `configureweb_server_name` script to paste on Machine A. If one machine is running under an operating system such as AIX or Linux and the other machine is running under Windows, copy the script from the `plugins_root/bin/crossPlatformScripts` directory.
15	A	Paste the `configureweb_server_name` script from Machine B to the `profile_root/bin` directory on Machine A.
16	A	Run the `configureweb_server_name` script on Machine A to create a web server definition in the administrative console.
17	A	Open the administrative console and save the changed configuration.
18	B	Start the web server. AIX HP-UX Linux Solaris Source the `plugins_root/setupPluginCfg.sh` script for a Domino Web Server before starting a Domino Web Server.
19	A	Propagate the `plugin-cfg.xml` file on Machine A from the application server to the web server using the administrative console. 1. Click **Servers** > **Web servers**. 2. On the web servers page, place a check mark beside the web server for which you want to propagate a plug-in, and click **Propagate Plug-in**. Web servers other than IBM HTTP Server require manual propagation.

- **Scenario 10:** The job manager is part of an administrative process that allows you to flexibly manage multiple administrative agents, deployment managers, and standalone application servers. Nodes can be registered with one or more job managers. In contrast to a deployment manager, the job manager does not exclusively inherit the administrative functions of its registered nodes. Nodes that register with a job manager maintain their own administrative capabilities. Additionally, the nodes periodically poll the job managers to determine whether there are jobs posted there that require action. All registered nodes can still be managed separately from the job manager. The advantage to a job manager configuration is the ability to coordinate management actions across multiple varied environments.

  Install a deployment manager and a managed node on one machine, an administrative agent and multiple registered application server nodes on a second machine, a job manager on a third machine, and a web server on a fourth machine.

  The cell in machine A communicates with a web server, while machine C is an internal server that could be used for testing or some other purpose.

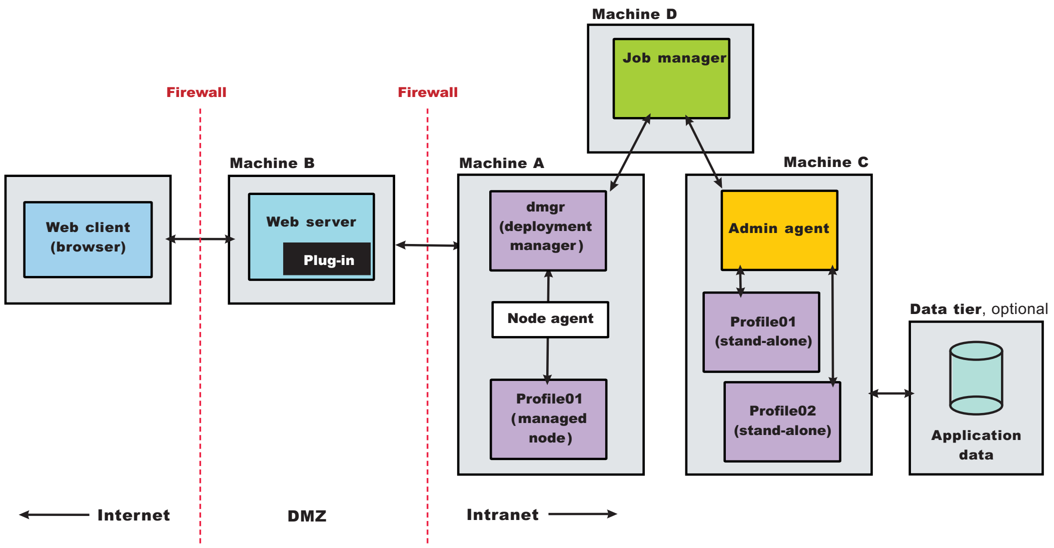


Table 18. Installing a deployment manager and a managed node on one machine, an administrative agent and multiple registered application server nodes on a second machine, a job manager on a third machine, and a web server on a fourth machine.

Complete these steps:

Step	Machine	Task
1	A	Install IBM Installation Manager.
2	A	Use Installation Manager to install WebSphere Application Server Network Deployment.
3	A	Use the Profile Management Tool or the manageprofiles command to create a management profile of the deployment manager server type.
4	A	Start the deployment manager using its First steps console or by running the startManager *profile_root* command in the `bin` directory of the deployment manager profile, `/bin`.
5	A	Use the Profile Management Tool or the manageprofiles command to create an application server profile.
6	A	Federate the application server into the cell using the administrative console of the deployment manager. Click **System Administration > Nodes > Add Node**.
7	C	Install IBM Installation Manager.
8	C	Use Installation Manager to install WebSphere Application Server Network Deployment.
9	C	Use the Profile Management Tool or the manageprofiles command to create a management profile of the administrative agent server type.
10	C	Use the Profile Management Tool or the manageprofiles command to create multiple application server profiles.
11	C	Register the standalone application servers with the administrative agent by running the registerNode command in the bin directory of the administrative agent profile, `*profile_root*/bin`.
12	D	Install IBM Installation Manager.
13	D	Use Installation Manager to install WebSphere Application Server Network Deployment.
14	D	Use the Profile Management Tool or the manageprofiles command to create a management profile of the job manager server type.

15	D	Register the administrative agent on Machine C and the deployment manager on Machine B with the job manager on Machine D by connecting to the wsadmin tool on the job manager and running the registerWithJobManager command in the AdminTask object.
		`AdminTask.registerWithJobManager('[-host myhost -conntype SOAP -port 8878`
		`-managedNodeName myhostNode01]')`
		Alternatively, you can register with the job manager using an administrative console. In the deployment manager console, click **System Administration > Deployment manager > Job manager**, select a deployment manager node, and click **Register with Job Manager**. In the administrative agent console, click **System Administration > Administrative agent > Nodes**, select one or more standalone nodes, and click **Register with Job Manager**. The deployment manager and standalone nodes that you register with the job manager become managed nodes of the job manager. The federated node, Profile01, on Machine A does not become a managed node of the job manager; it remains a federated node that is managed by the deployment manager.

16	B	Install IBM Installation Manager.
17	B	Use Installation Manager to install the following: • Web Server Plug-ins for WebSphere Application Server • WebSphere Customization Toolbox
18	B	Use Installation Manager to install IBM HTTP Server, or install another supported web server.
19	B	Open the WebSphere Customization Toolbox, and launch the Web Server Plug-ins Configuration Tool to configure the web server plug-in and create the web server definition. The script for creating and configuring the web server is created under the `*plugins_root*/bin` directory.
20	B	Copy the `configure*web_server_name*` script to paste on Machine A. If one machine is running under an operating system such as AIX or Linux and the other machine is running under Windows, copy the script from the `*plugins_root*/bin/crossPlatformScripts` directory.
21	A	Paste the `configure*web_server_name*` script from Machine B to the `*profile_root*/bin` directory on Machine A.
22	A	Run the `configure*web_server_name*` script on Machine A to create a web server definition in the administrative console.
23	A	Open the administrative console and save the changed configuration.
24	B	Start the web server. AIX HP-UX Linux Solaris Source the `*plugins_root*/setupPluginCfg.sh` script for a Domino Web Server before starting a Domino Web Server.

Table 18. Installing a deployment manager and a managed node on one machine, an administrative agent and multiple registered application server nodes on a second machine, a job manager on a third machine, and a web server on a fourth machine (continued).

Complete these steps:

Step	Machine	Task
25	A	Propagate the `plugin-cfg.xml` file on Machine A from the application server to the web server using the administrative console. 1. Click **Servers** > **Web servers**. 2. On the web servers page, place a check mark beside the web server for which you want to propagate a plug-in, and click **Propagate Plug-in**. Web servers other than IBM HTTP Server require manual propagation.

- **Scenario 11:** Install a deployment manager and one or more managed nodes on one machine and DMZ Secure Proxy Server for IBM WebSphere Application Server on a second machine. DMZ Secure Proxy Server for IBM WebSphere Application Server delivers a high performance reverse proxy capability that can be used at the edge of the network to route, load balance, and improve response times for requests to web resources.

  The most secure way to administer the DMZ Secure Proxy Server for IBM WebSphere Application Server is locally using wsadmin commands. The DMZ Secure Proxy Server for IBM WebSphere Application Server does not contain a web container and therefore does not have an administrative console. Local administration can only be done using the command line.

  Secure proxy server configurations can also be managed within a network deployment application server cell and then imported locally into the DMZ Secure Proxy Server for IBM WebSphere Application Server using wsadmin commands. The configurations are created and maintained inside the network deployment application server cell as configuration-only profiles. The profiles are registered with the administrative agent and are then managed using the administrative console. You configure the secure proxy server profile in the network deployment application server cell, export the configuration to a node in the DMZ, and import the configuration into the DMZ Secure Proxy Server for IBM WebSphere Application Server. You then repeat the process if any changes are made to the secure proxy server configuration.

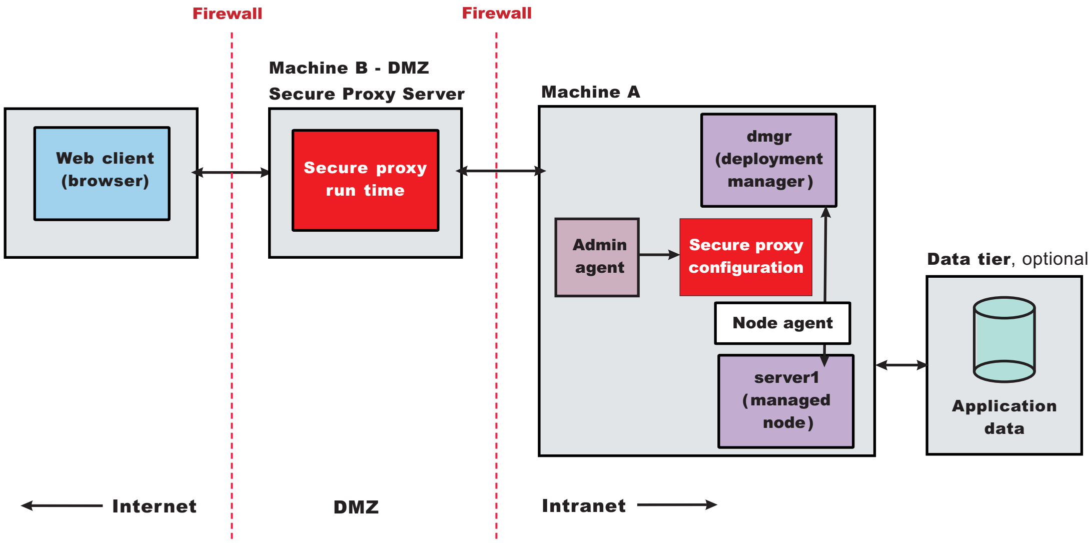


Table 19. Installing a deployment manager and one or more managed nodes on one machine and DMZ Secure Proxy Server for IBM WebSphere Application Server on a second machine.

Complete these steps:

Step	Machine	Task
1	A	Install IBM Installation Manager.

Table 19. Installing a deployment manager and one or more managed nodes on one machine and DMZ Secure Proxy Server for IBM WebSphere Application Server on a second machine (continued).

Complete these steps:

Step	Machine	Task
2	A	Use Installation Manager to install WebSphere Application Server Network Deployment.
3	A	Use the Profile Management Tool or the manageprofiles command to create a management profile of the deployment manager server type.
4	A	Start the deployment manager using its First steps console or by running the startManager *profile_root* command in the `bin` directory of the deployment manager profile, `/bin`.
5	A	Use the Profile Management Tool or the manageprofiles command to create application server profiles.
6	A	Federate the application servers into the cell using the administrative console of the deployment manager. Click **System Administration** > **Nodes** > **Add Node**.
7	A	Use the Profile Management Tool or the manageprofiles command to create a management profile of the administrative agent server type.
8	A	Start the administrative agent.
9	A	Use the Profile Management Tool or the manageprofiles command to create a secure proxy (configuration-only) profile.
10	A	Register the secure proxy (configuration-only) profile with the administrative agent by running the registerNode command in the bin directory of the administrative agent profile, *`profile_root`*`/bin`.
11	A	Restart the administrative agent.
12	A	When the administrative agent prompts you with a list of the nodes that it manages, select the node from the secure proxy (configuration-only) profile.
13	A	Create a secure proxy profile through the administrative console. Click **Servers** > **Server Types** > **WebSphere proxy servers** > **New**, and use the Proxy Server Creation wizard.

14	A	Export the server configuration by connecting to the wsadmin tool for the administrative agent and running the exportProxyServer command in the AdminTask object. Consider the following examples using Jython strings.
		Windows
		`AdminTask.exportProxyServer('[-archive c:\myProxyServer.ear -nodeName node1`
		`-serverName server1]')`
		AIX HP-UX Linux Solaris
		`AdminTask.exportProxyServer('[-archive /myProxyServer.ear -nodeName node1`
		`-serverName server1]')`

15	B	Install IBM Installation Manager.
16	B	Install the DMZ Secure Proxy Server for IBM WebSphere Application Server.
17	A	Transfer the server configuration file to Machine B using FTP.

18	B	Import the server configuration on Machine B by connecting to the wsadmin tool for the secure proxy and running the importProxyServer command in the AdminTask object. Consider the following examples using Jython strings.
		Windows
		`AdminTask.importProxyServer('[-archive c:\myProxyServer.ear -nodeName node1`
		`-serverInArchive server1 -deleteExistingServer true]')`
		AIX HP-UX Linux Solaris
		`AdminTask.importProxyServer('[-archive /myProxyServer.ear -nodeName node1`
		`-serverInArchive server1 -deleteExistingServer true]')`

Results

You have reviewed many of the most common installation scenarios to find a possible match for the topology that you intend to install.

What to do next

See the IBM HTTP Server, web server plug-in, and DMZ Secure Proxy Server for IBM WebSphere Application Server documentation for more information on installing those products.

Planning to install the Application Client for IBM WebSphere Application Server

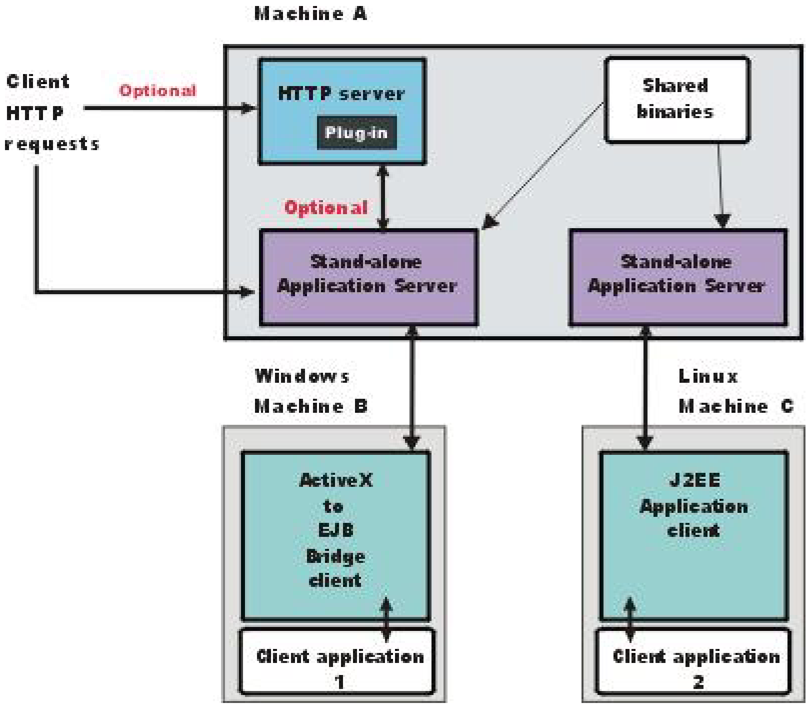
Examine typical topologies and uses for the Application Client for IBM WebSphere Application Server to determine how you might use this technology.

About this task

In a traditional client-server environment, the client requests a service and the server fulfills the request. Multiple clients use a single server. Clients can also access several different servers. This model persists for Java clients except that now these requests use a client runtime environment.

In this model, the client application requires a servlet to communicate with the enterprise bean, and the servlet must reside on the same machine as the application server.

The following graphic shows a topology for installing the Application Client and using client applications:



The example shows two types of application clients installed in a topology that uses client applications to access applications and data on Machine A:

- The ActiveX application client on Machine B is a Windows only client that uses the Java Native Interface (JNI) architecture to programmatically access the Java virtual machine (JVM) API. The JVM code exists in the same process space as the ActiveX application (Visual Basic, VBScript, or Active Server Pages (ASP) files) and remains attached to the process until that process terminates.
- The J2EE application client on Machine C is a Java application program that accesses enterprise beans, Java Database Connectivity (JDBC) APIs, and Java Message Service message queues. The application program must configure the execution environment of the Java EE application client and use the Java Naming and Directory Interface (JNDI) name space to access resources.

Use the following procedure as a example of installing the Application Client.

Procedure

1. Install IBM Installation Manager on Machine A.

2. Use Installation Manager to install the WebSphere Application Server product on Machine A to establish the core product files.
3. Use the Profile Management Tool or the manageprofiles command to create both standalone application server profiles.
4. Use the administrative console of each application server to deploy any user applications.
5. Use the administrative console of each application server to create a web server configuration for the web server.
6. Use the administrative console of each application server to regenerate each `plugin-cfg.xml` file in the local web server configuration.
7. Optional: Use Installation Manager to install IBM HTTP Server on Machine A.
8. Optional: Use Installation Manager to install WebSphere Customization Toolbox on Machine A.
9. Optional: Open the WebSphere Customization Toolbox, and launch the Web Server Plug-ins Configuration Tool to configure the web server plug-in and create the web server definition on Machine A.
10. Install the Application Client.

    The diagram shows two different types of application clients on two different operating systems. Although this example shows two application clients, you do not have to install two application clients to have a working system. Each application client is fully functional and works independently of the other.

    Optionally, install IBM Installation Manager and use it to install the Application Client on Machine B.

    Optionally, install IBM Installation Manager and use it to install the Application Client on Machine C.

Results

This article can help you plan runtime environments for client applications.

Example: Choosing a topology for better performance

Use this page to understand the advantages and disadvantages of various Workload Management topologies.

WebSphere Application Server provides various Workload Management (WLM) topologies. First, this topic describes a single-tier topology and a split-tier topology. Secondly, these two topologies are compared to show how the type of topology you choose can affect performance, security, and system flexibility.

The single-tier topology contains a cluster of WebSphere Application Servers. Each cluster member contains a web container and an Enterprise JavaBeans (EJB) container. The split-tier topology consists of a cluster of web container machines in front of a cluster of EJB container machines. The number of WebSphere Application Servers machines is the same in both topologies; the client driver, the Web server with plug-in, and the back end database are located on separate, dedicated machines.

The single-tier topology has an (the performance) advantage because the web container and EJB container are running in a single Java virtual machine (JVM). In this topology, with object request broker (ORB) pass by reference enabled, the EJB processing is done on the same thread as the web container processing. In the split-tier topology, the ORB pass by reference option is ignored because the web container and EJB container are in separate JVMs.

The split-tier topology enables web and EJB resources to be isolated and separately administered.

A lab experiment using a the Benchmark Sample for WebSphere (Trade3) and a cluster of 6 applications servers found that throughput of the single-tier topology was 10-20% higher than that of the split-tier topology. You can download the Benchmark sample for WebSphere (Trade3) from the following website:

http://www-306.ibm.com/software/webservers/appserv/was/performance.html

Queuing network

WebSphere Application Server contains interrelated components that must be harmoniously tuned to support the custom needs of your end-to-end e-business application. These adjustments help the system achieve maximum throughput while maintaining the overall stability of the system.

This group of interconnected components is known as a queuing network. These queues or components include the network, web server, web container, EJB container, data source, and possibly a connection manager to a custom back-end system. Each of these resources represents a queue of requests waiting to use that resource.

Various queue settings include the following. Consult the associated topics in the information center.

- IBM HTTP Server: MaxClients for operating systems such as AIX or Linux and ThreadsPerChild for Windows NT systems
- Web container: **Maximum size** , **MaxKeepAliveConnections**, and **MaxKeepAliveRequests**.
- **Tuning Object Request Brokers**.
- Data source **connection pooling** and **statement cache size** .

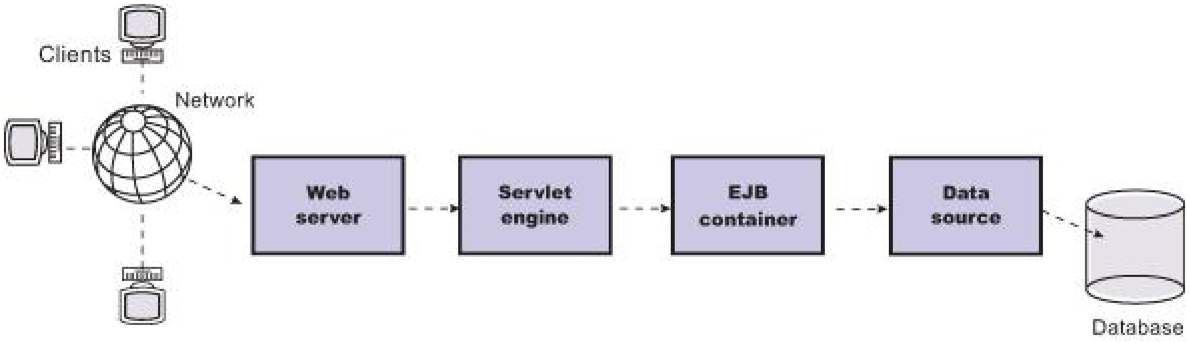


Figure Reference 1: WebSphere queuing network

Most of the queues that make up the queuing network are closed queues. A closed queue places a limit on the maximum number of requests present in the queue, while an open queue has no limit. A closed queue supports tight management of system resources. For example, the web container thread pool setting controls the size of the web container queue. If the average servlet running in a web container creates 10 MB of objects during each request, a value of 100 for thread pools limits the memory consumed by the web container to 1 GB.

In a closed queue, requests can be active or waiting. An active request is doing work or waiting for a response from a downstream queue. For example, an active request in the web server is doing work, such as retrieving static HTML, or waiting for a request to complete in the web container. A waiting request is waiting to become active. The request remains in the waiting state until one of the active requests leaves the queue.

All web servers supported by WebSphere Application Server are closed queues, as are WebSphere Application Server data sources. You can configure web containers as open or closed queues. In general, it is best to make them closed queues. EJB containers can be open or closed queues. If there are no threads available in the pool, a new one is created for the duration of the request.

If enterprise beans are called by servlets, the web container limits the number of total concurrent requests into an EJB container, because the web container also has a limit. The web container limits the number of total concurrent requests only if enterprise beans are called from the servlet thread of execution. Nothing prevents you from creating threads and bombarding the EJB container with requests. Therefore, servlets should not create their own work threads.

Queuing and clustering considerations

Cloning application servers to create a cluster can be a valuable asset in configuring highly scalable production environments, especially when the application is experiencing bottlenecks that are preventing full CPU utilization of symmetric multiprocessing (SMP) servers.

When adjusting the WebSphere Application Server system queues in clustered configurations, remember that when a server is added to a cluster, the server downstream receives twice the load.

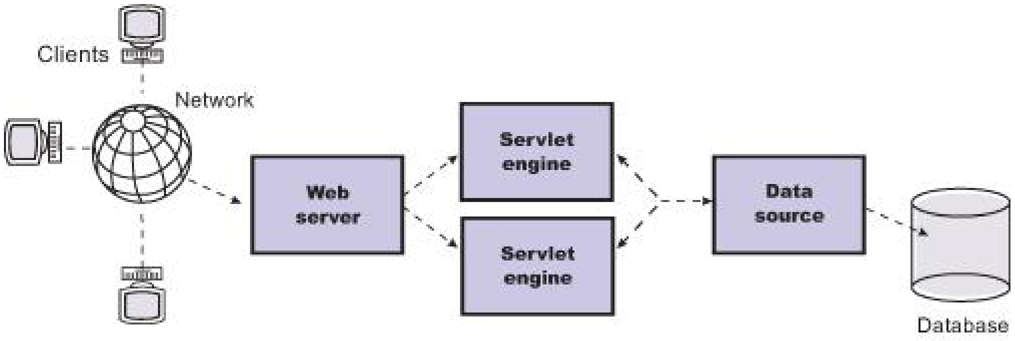


Figure Reference 1: Clustering and queuing

Two servlet engines are located between a web server and a data source. It is assumed that the web server, servlet engines and data source, but not the database, are all running on a single SMP server. Given these constraints, the following queue considerations must be made:

- Double the web server queue settings to ensure ample work is distributed to each web container.
- Reduce the web container thread pools to avoid saturating a system resource like CPU or another resource that the servlets are using.
- Reduce the data source to avoid saturating the database server.
- Reduce Java heap parameters for each instance of the application server. For versions of the Java virtual machine (JVM) shipped with WebSphere Application Server, it is crucial that the heap from all JVMs remain in physical memory. For example, if a cluster of four JVMs is running on a system, enough physical memory must be available for all four heaps.

Queue configuration best practices

A methodology exists for configuring the WebSphere Application Server queues. Moving the database server onto another machine or providing more powerful resources, for example a faster set of CPUs with more memory, can dramatically change the dynamics of your system.

There are four tips for queuing:

- **Minimize the number of requests in WebSphere Application Server queues**.

  In general, requests wait in the network in front of the web server, rather than waiting in WebSphere Application Server. This configuration only supports those requests that are ready for processing to enter the queuing network. Specify that the queues farthest upstream or closest to the client are slightly larger, and queues farther downstream or farthest from the client are progressively smaller.

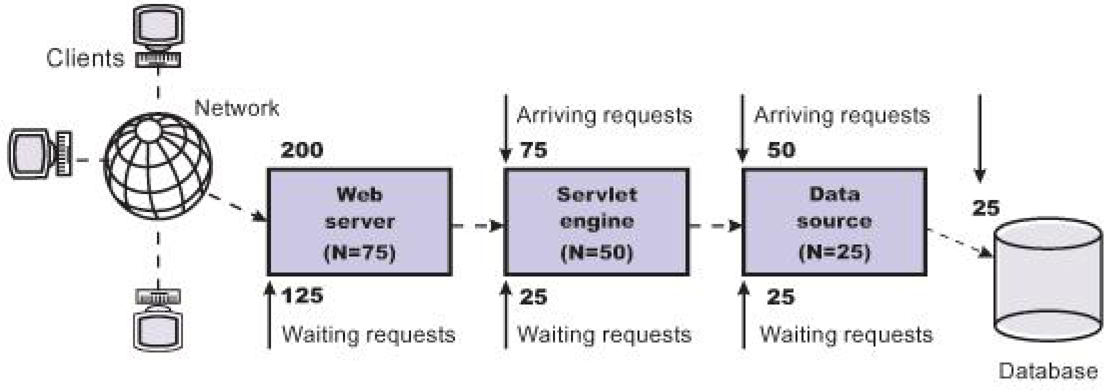


Figure Reference 1: Upstream queuing network

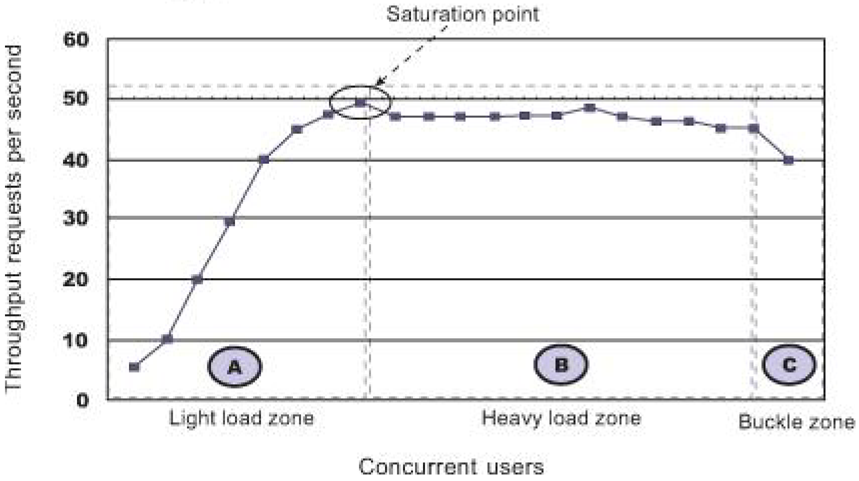
Queues in the queuing network become progressively smaller as work flows downstream. When 200 client requests arrive at the web server, 125 requests remain queued in the network because the web server is set to handle 75 concurrent clients. As the 75 requests pass from the web server to the web container, 25 requests remain queued in the web server and the remaining 50 are handled by the web container. This process progresses through the data source until 25 user requests arrive at the final destination, the database server. Because there is work waiting to enter a component at each point upstream, no component in this system must wait for work to arrive. The bulk of the requests wait in the network, outside of WebSphere Application Server. This type of configuration adds stability, because no component is overloaded.

You can then use the Edge Server to direct waiting users to other servers in a WebSphere Application Server cluster.

- **Draw throughput curves to determine when the system capabilities are maximized**.

  You can use a test case that represents the full spirit of the production application by either exercising all meaningful code paths or using the production application. Run a set of experiments to determine when the system capabilities are fully stressed or when it has reached the saturation point. Conduct these tests after most of the bottlenecks are removed from the application. The goal of these tests is to drive CPUs to near 100% utilization. For maximum concurrency through the system, start the initial baseline experiment with large queues. For example, start the first experiment with a queue size of 100 at each of the servers in the queuing network: Web server, web container and data source. Begin a series of experiments to plot a throughput curve, increasing the concurrent user load after each experiment. For example, perform experiments with one user, two users, five, 10, 25, 50, 100, 150 and 200 users. After each run, record the throughput requests per second, and response times in seconds per request. The curve resulting from the baseline experiments resembles the following typical throughput curve shown as follows:

Throughput curve



The WebSphere Application Server throughput is a function of the number of concurrent requests present in the total system. Section A, the light load zone, shows that the number of concurrent user requests increases, the throughput increases almost linearly with the number of requests. At light loads, concurrent requests face very little congestion within the WebSphere Application Server system queues. At some point, congestion starts to develop and throughput increases at a much lower rate until it reaches a saturation point that represents the maximum throughput value, as determined by some bottleneck in the WebSphere Application Server system. The most manageable type of bottleneck occurs when the WebSphere Application Server machine CPUs become fully utilized because adding CPUs or more powerful CPUs fixes the bottleneck.

In the heavy load zone or Section B, as the concurrent client load increases, throughput remains relatively constant. However, the response time increases proportionally to the user load. That is, if the user load is doubled in the heavy load zone, the response time doubles. At some point, represented by Section C, the buckle zone, one of the system components becomes exhausted. At this point, throughput starts to degrade. For example, the system might enter the buckle zone when the network connections at the web server exhaust the limits of the network adapter or if the requests exceed operating system limits for file handles.

If the saturation point is reached by driving CPU utilization close to 100%, you can move on to the next step. If the saturation CPU occurs before system utilization reaches 100%, it is likely that another bottleneck is being aggravated by the application. For example, the application might be creating Java objects causing excessive garbage collection bottlenecks in the Java code.

There are two ways to manage application bottlenecks: remove the bottleneck or clone the bottleneck. The best way to manage a bottleneck is to remove it. You can use a Java-based application profiler, such as Rational Application Developer, Performance Trace Data Visualizer (PTDV), Borland's Optimizeit, JProbe or Jinsight to examine overall object utilization.

- **Decrease queue sizes while moving downstream from the client**.

  The number of concurrent users at the throughput saturation point represents the maximum concurrency of the application. For example, if the application saturates WebSphere Application Server at 50 users, using 48 users might produce the best combination of throughput and response time. This value is called the Max Application Concurrency value. Max Application Concurrency becomes the preferred value for adjusting the WebSphere Application Server system queues. Remember, it is desirable for most users to wait in the network; therefore, queue sizes should decrease when moving downstream farther from the client. For example, given a Max Application Concurrency value of 48, start with system queues at the following values: Web server 75, web container 50, data source 45. Perform a set of additional experiments adjusting these values slightly higher and lower to find the best settings.

  To help determine the number of concurrent users, view the Servlet Engine Thread Pool and Concurrently Active Threads metric in the Tivoli Performance Viewer.

- **Adjust queue settings to correspond to access patterns**.

In many cases, only a fraction of the requests passing through one queue enters the next queue downstream. In a site with many static pages, a number of requests are fulfilled at the web server and are not passed to the web container. In this circumstance, the web server queue can be significantly larger than the web container queue. In the previous example, the web server queue was set to 75, rather than closer to the value of Max Application Concurrency. You can make similar adjustments when different components have different execution times.

For example, in an application that spends 90% of its time in a complex servlet and only 10% of its time making a short JDBC query, on average 10% of the servlets are using database connections at any time, so the database connection queue can be significantly smaller than the web container queue. Conversely, if the majority of servlet execution time is spent making a complex query to a database, consider increasing the queue values at both the web container and the data source. Always monitor the CPU and memory utilization for both the WebSphere Application Server and the database servers to verify that the CPU or memory are not saturating.

Chapter 5. Preparing the operating system for product installation

Prepare your operating platform before installing a WebSphere Application Server product.

About this task

Before installing the product, you must install the necessary prerequisites for your operating system. This will prepare your system for the installation. Use the links below to go to the procedure for your operating system.

Procedure

Prepare your operating system for installation.
Select the appropriate procedure:

- AIX “Preparing AIX systems for installation”
- HP-UX “Preparing HP-UX systems for installation” on page 51
- Linux “Preparing Linux systems for installation” on page 56
- Solaris “Preparing Solaris systems for installation” on page 68
- Windows “Preparing Windows systems for installation” on page 71

Results

Your operating system is configured for installation.

What to do next

Install the product as described in “Installing and uninstalling the product on distributed operating systems” on page 74.

Preparing AIX systems for installation

This topic describes how to prepare an AIX system for the installation of IBM WebSphere Application Server products.

Before you begin

The installation uses Installation Manager. You can use the graphical interface or use a response file in silent mode.

Note: WebSphere Application Server prevents users from installing to a non-empty directory. If WebSphere Application Server is installed to a directory with a `lost+found` subdirectory, you will be prompted to use an empty directory. If you still want to install to this directory, then you can delete the `lost+found` directory. However, the next time `fsck` is executed, the `lost+found` directory will be created. This should not have any effect on an existing installation; during uninstallation, however, this directory will not be removed.

Restrictions:

- There are known issues with using Cygwin/X to run Eclipse-based applications on remote AIX machines. This affects your use of the Profile Management Tool. With Cygwin/X on remote AIX, for example, a splash screen for the Profile Management Tool appears but the Profile Management Tool never actually comes up. For details of existing

Bugzilla reports on these issues, see the information at https://bugs.eclipse.org/bugs/show_bug.cgi?id=36806. If a different X server (such as Hummingbird Exceed®) is used, these problems do not occur.

- To run the Profile Management Tool or the Configuration Migration Tool after you have installed the 64-bit product on an AIX 64-bit system, you must have the GTK installed. If you do not have the GTK installed, you receive an error message similar to the following:

```
Eclipse:
 An error has occurred. See the log file
 /workspace/.metadata/.log.
```

To install the GTK, perform one of the following actions:

– Install Firefox 3.5.x as described later in this procedure.

– Install the following RPMs to install the current version of the GTK:

- atk-1.12.3-2.aix5.2.ppc.rpm
- cairo-1.8.8-1.aix5.2.ppc.rpm
- expat-2.0.1-1.aix5.2.ppc.rpm
- fontconfig-2.4.2-1.aix5.2.ppc.rpm
- freetype2-2.3.9-1.aix5.2.ppc.rpm
- gettext-0.10.40-6.aix5.1.ppc.rpm
- glib2-2.12.4-2.aix5.2.ppc.rpm
- gtk2-2.10.6-4.aix5.2.ppc.rpm
- libjpeg-6b-6.aix5.1.ppc.rpm
- libpng-1.2.32-2.aix5.2.ppc.rpm
- libtiff-3.8.2-1.aix5.2.ppc.rpm
- pango-1.14.5-4.aix5.2.ppc.rpm
- xcursor-1.1.7-3.aix5.2.ppc.rpm
- xft-2.1.6-5.aix5.1.ppc.rpm
- xrender-0.9.1-3.aix5.2.ppc.rpm
- zlib-1.2.3-3.aix5.1.ppc.rpm
- pixman-0.12.0-3.aix5.2.ppc.rpm

These RPMs can be found on the AIX Toolbox for Linux Applications website.

About this task

Preparing the operating system involves such changes as allocating disk space and installing patches to the operating system. IBM tests WebSphere Application Server products on each operating system platform. Such tests verify whether an operating system change is required for WebSphere Application Server products to run correctly. Without the required changes, WebSphere Application Server products do not run correctly.

Procedure

1. Log on to the operating system.

   You can log on as root or as a nonroot installer.

   Select a umask that allows the owner to read/write to the files, and allows others to access them according to the prevailing system policy. For root, a umask of 022 is recommended. For nonroot users a umask of 002 or 022 can be used, depending on whether the users share the group. To verify the umask setting, issue the following command:

```
umask
```

   To set the umask setting to 022, issue the following command:

```
umask 022
```

2. Stop all Java processes related to WebSphere Application Server on the machine where you are installing the product.
3. Stop any web server process such as the IBM HTTP Server.
4. The product contains IBM Software Development Kit (SDK) Version 6.
   - You must run AIX Version 6.1 or Version 7.1 for SDK 6 to operate properly.

     To test whether this Java SDK is supported on a specific System p® system, at the system prompt type:

```
lscfg -p | fgrep Architecture
```

     You should receive the reply: `Model Architecture: chrp`. Only Common Hardware Reference Platform (chrp) systems are supported.
   - The environment variable `LDR_CNTRL=MAXDATA` is not supported for 64-bit processes. Only use `LDR_CNTRL=MAXDATA` on 32-bit processes.

     Note: To show the value of this variable, use the following command:

```
echo $LDR_CNTRL
```

   - If you are using one of the supported non-UTF8 CJK locales, you must install one of the following file sets. The installation images are available on the AIX base discs; updates are available from the Fix Central website.
     - `X11.fnt.ucs.ttf` (for ja_JP or Ja_JP)
     - `X11.fnt.ucs.ttf_CN` (for zh_CN or Zh_CN)
     - `X11.fnt.ucs.ttf_KR` (for ko_KR)
     - `X11.fnt.ucs.ttf_TW` (for zh_TW or Zh_TW)
5. Use the System Management Interface Tool (SMIT) to display packages that are installed to determine whether you must update packages that are described in the following steps.
6. Download the most current version of the Info-ZIP product to avoid problems with zipped files.

   Although zipped files are primarily used in the service stream, prepare your AIX operating system by downloading a current version of the Info-ZIP package from the http://www.info-zip.org website.
7. Provide adequate disk space.

   The amount of disk space required varies with the number of features or products installed. If you are installing the product using Installation Manager, the installation summary panel indicates the approximate amount of disk space required based on the features and products that you have selected.Installing all features and products requires approximately 2 GB of disk space. This estimate includes the following products, components, and features:
   - Main application server product installation
   - Profiles
   - Sample applications
   - IBM HTTP Server
   - Web Server Plug-ins
   - Application Client for WebSphere Application Server

   With the JFS file system on AIX, you can allocate expansion space for directories. If Installation Manager does not have enough space, it issues a system call for more space that increases the space allocation dynamically.

   If you plan to migrate applications and the configuration from a previous version, verify that the application objects have enough disk space. As a rough guideline, plan for space equal to 110 percent of the size of the applications.
8. Unmount file systems with broken links to avoid java.lang.NullPointerException errors.

   Unmount file systems with broken links before installing.

   Installation can fail when broken links exist to file systems.

Use the df -k command to check for broken links to file systems. Look for file systems that list blank values in the *1024-blocks size* column. Columns with a value of "-" (dash) are not a problem. The following example shows a problem with the /dev/lv00 file system:

```
>  df -k
Filesystem    1024-blocks      Free %Used    Iused %Iused Mounted on
/dev/hd4          1048576    447924   58%     2497     1% /
/dev/hd3          4259840   2835816   34%      484     1% /tmp
/proc                   -         -    -         -     -  /proc
/dev/lv01         2097152    229276   90%     3982     1% /storage
/dev/lv00
/dev/hd2          2097152    458632   79%    42910     9% /usr
iw031864:/cdrom/db2_v72_eee_aix32_sbcs
```

The /proc file system is not a problem. The iw031864:/cdrom/db2_v72_eee_aix32_sbcs file system is a definite problem. The /dev/lv00 file system is also a likely problem. Use one of the following commands to solve this problem:

```
>  umount /cdrom/db2_v72_eee_aix32_sbcs
>  umount /cdrom
```

Start the installation again. If the problem continues, unmount any file systems that have blank values, such as the /dev/lv00 file system in the example. If you cannot solve the problem by unmounting file systems with broken links, reboot the machine and start the installation again.

9. Verify that prerequisites and corequisites are at the required release levels.

   Although Installation Manager checks for prerequisite operating system patches, review the prerequisites on the Supported hardware and software website if you have not already done so.

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

10. Verify the system cp command when using emacs or other freeware.

    If you have emacs or other freeware installed on your operating system, verify that the system cp command is used.

    a. Type the following command prompt before running the installation program for the WebSphere Application Server product.

```
which cp
```

    b. Remove the freeware directory from your PATH if the resulting directory output includes freeware. For example, assume that the output is similar to the following message: .../freeware/bin/cp. If so, remove the directory from the PATH.

    c. Install the WebSphere Application Server product.

    d. Add the freeware directory back to the PATH.

    If you install with a cp command that is part of a freeware package, the installation might appear to complete successfully, but the Java 2 SDK that the product installs might have missing files in the *app_server_root*/java directory.

    Missing files can destroy required symbolic links. If you remove the freeware cp command from the PATH, you can install the application server product successfully.

11. Verify that the Java SDK on the installation image disk is functioning correctly if you created your own disk.

    For example, you might have downloaded an installation image from Passport Advantage, or you might have copied an installation image onto a backup disk. In either case, perform the following steps to verify that the disk contains a valid Java software development kit (SDK).

    a. Change directories to the /JDK/jre.pak/repository/package.java.jre/java/jre/bin directory on the product disk. For example:

```
cd /JDK/jre.pak/repository/package.java.jre/java/jre/bin
```

    b. Verify the Java version. Type the following command:

```
./java -version
```

    The command completes successfully with no errors when the SDK is intact.

12. Optional: Install the Mozilla Firefox browser if it is not already installed.

    Follow the instructions for installing Firefox Version 3.5.x or above on AIX.

a. Download the latest supported version of Mozilla Firefox (3.5.x or later) for AIX.

   Download Mozilla for AIX from the following location: Web browsers for AIX.

   Download the installp imag,e and install it from the SMIT.

13. Optional: Export the location of the supported browser.

    Export the location of the supported browser using a command that identifies the actual location of the browser.

    If the Mozilla Firefox package is in the `bin/firefox` directory, for example, use the following command to export BROWSER=/usr/bin/firefox:

```
EXPORT BROWSER=/usr/bin/firefox
```

14. Optional: Prepare a Workload Partition (WPAR).

    If you are going to install the product on a WPAR on AIX Version 6.1, you must make sure that the WPAR has private and writable versions of the `/usr` and `/opt` file systems. If you do not have this type of WPAR, create a new WPAR using the following steps:

    a. Choose a name for the WPAR that maps to an IP address for your network, or add an entry for the new WPAR in the `/etc/hosts` file. Make sure you know the subnet IP address as well.

    b. Use the following command to create the WPAR:

```
mkwpar -n <wpar_name> -h <host_name> -N netmask=<A.B.C.D> address=<A.B.C.D> -r -l
```

Note: The `-l` parameter creates private and writable versions of the `/usr` and `/opt` file systems.

Results

This procedure results in preparing the operating system for installing the product.

What to do next

For optimal performance, tune the Java environment for your operating system. For more information, see the Java tuning information for your specific AIX operating system version.

After verifying prerequisites, verifying the product disk, and setting your installation goals, you can start installing. Use one of the following installation procedures:

- Perform an installation using the graphical user interface.

  See “Installing the product on distributed operating systems using the GUI” on page 78.
- Perform a silent installation.

  See “Installing the product on distributed operating systems silently” on page 84.
- Install additional features on an existing product.

  See “Installing and removing features on distributed operating systems” on page 96.

Preparing HP-UX systems for installation

This topic describes how to prepare an HP-UX system for the installation of IBM WebSphere Application Server products.

Before you begin

The installation uses Installation Manager. You can use the graphical interface or use a response file in silent mode.

Restriction: There are known issues with using Cygwin/X to run Eclipse-based applications on remote HP-UX machines. This affects your use of the Profile Management Tool. With Cygwin/X on remote HP-UX, for example, the Profile Management Tool's welcome panel appears but no keyboard or mouse input is accepted. For details of existing Bugzilla reports on these issues, see the information at https://bugs.eclipse.org/bugs/show_bug.cgi?id=97808. If a different X server (such as Hummingbird Exceed®) is used, these problems do not occur.

About this task

Preparing the operating system involves such changes as allocating disk space and installing patches to the operating system. IBM tests WebSphere Application Server products on each operating system platform. Such tests verify whether an operating system change is required for WebSphere Application Server products to run correctly. Without the required changes, WebSphere Application Server products do not run correctly.

Procedure

1. Log on to the operating system.

   You can log on as root or as a nonroot installer.

   Select a umask that allows the owner to read/write to the files, and allows others to access them according to the prevailing system policy. For root, a umask of 022 is recommended. For nonroot users a umask of 002 or 022 can be used, depending on whether the users share the group. To verify the umask setting, issue the following command:

```
umask
```

   To set the umask setting to 022, issue the following command:

```
umask 022
```

2. Optional: Download and install the Mozilla Firefox web browser.

   If you do not have the Mozilla web browser, download and install the browser from Web Browsers for HP-UX.
3. Optional: Export the location of the supported browser.

   Export the location of the supported browser using a command that identifies the actual location of the browser.

   If the Mozilla Firefox package is in the `/opt/bin/firefox` directory, for example, use the following command:

```
export BROWSER=/opt/bin/firefox
```

4. Stop all Java processes related to WebSphere Application Server on the machine where you are installing the product.
5. Stop any web server process such as the IBM HTTP Server.
6. Provide adequate disk space.

   The amount of disk space required varies with the number of features or products installed. If you are installing the product using Installation Manager, the installation summary panel indicates the approximate amount of disk space required based on the features and products you have selected.Installing all features and products requires approximately 2 GB of disk space. This estimate includes the following products, components, and features:
   - Main application server product installation
   - Profiles
   - Sample applications
   - IBM HTTP Server
   - Web Server Plug-ins
   - Application Client for WebSphere Application Server

   If you plan to migrate applications and the configuration from a previous version, verify that the application objects have enough disk space. As a rough guideline, plan for space equal to 110 percent of the size of the applications.
7. Set kernel values to support Application Server.

   Several HP-UX kernel values are typically too small for the product.

To set kernel parameters, perform the following steps:

a. Log into the host machine as root.

b. Determine the physical memory, which you must know to avoid setting certain kernel parameters above the physical capacity:

   1) Start the HP-UX System Administration Manager (SAM) utility with the /usr/sbin/sam command.

   2) Select **Performance Monitors > System Properties > Memory**.

   3) Note the value for Physical Memory and click **OK**.

   4) Exit from the SAM utility.

c. Set the maxfiles and maxfiles_lim parameters to at least `4096`. The following table recommends 8000 and 8196, respectively. You must first edit the `/usr/conf/master.d/core-hpux` file, so the SAM utility can set values greater than 2048:

   1) Open the `/usr/conf/master.d/core-hpux` file in a text editor.

   2) Change the line," *range maxfiles<=2048" to "*range maxfiles<=60000"

   3) Change the line, "*range maxfiles_lim<=2048" to "*range maxfiles_lim<=60000"

   4) Save and close the file. Old values might be stored in the `/var/sam/boot.config` file. Force the SAM utility to create a new `boot.config` file:

      a) Move the existing version of the `/var/sam/boot.config` file to another location, such as the `/tmp` directory.

      b) Start the SAM utility.

      c) Select **Kernel Configuration** > **Configurable Parameters**. When the Kernel Configuration window opens, a new `boot.config` file exists.

         Alternatively, rebuild the `boot.config` file with the following command:

```
# /usr/sam/lbin/getkinfo -b
```

d. Set new kernel parameter values:

   1) Start the SAM utility.

   2) Click **Kernel Configuration > Configurable Parameters**.

   3) For each of the parameters in the following table, perform this procedure:

      a) Highlight the parameter to change.

      b) Click **Actions > Modify Configurable Parameter**.

      c) Type the new value in the **Formula/Value** field.

      d) Click **OK**.

Table 20. Typical kernel settings for running WebSphere Application Server.

Change typical kernel settings for running WebSphere Application Server in the order shown in the following table:

Parameter	Value
swchunk	8192
shmmni	8192 (Change this one before shmseg)
shmseg	512
maxdsiz	3221225472
maxdsiz_64bit	64424509440
maxfiles_lim	10000 (Change this one before maxfiles)
maxfiles	8192
semume	512
semmsl	3072

Table 20. Typical kernel settings for running WebSphere Application Server (continued).

Change typical kernel settings for running WebSphere Application Server in the order shown in the following table:

Parameter	Value
msgssz (removed and replaced by msgmbs in HP-UX 11.31)	512 (Change this one before msgmax)
nkthread	10000
max_thread_proc	4096
nproc	8192 (Change this one before maxuprc)
maxuprc	4096
ninode	8110
msgtql	13107 (Change this one before msgmap)
msgseg (removed and replaced by msgmbs in HP-UX 11.31)	32767 (Change this one before msgmap and msgmax)
msgmap (removed in HP-UX 11.31)	13109
msgmnb	65535 (0x10000) (Change this one before msgmax)
msgmnb	131070 (when running multiple profiles on the same system)
msgmax (removed in HP-UX 11.31)	65535 (0x10000)
msgmax (removed in HP-UX 11.31)	131070 (when running multiple profiles on the same system)
msgmbs (added and replaced msgssz and msgseg in HP-UX 11.31)	8
msgmni	4634
semmns	11586
semmni	8192
semmnu	8180
shmmax	185513715302
STRMSGSZ	65535
dbc_max_pct	10
nstrpty	60

When WebSphere Application Server and IBM DB2 are on the same machine, some kernel values are higher than those shown in the preceding table.

See the Recommended HP-UX kernel configuration parameters for DB2 V8 web page for more information.

e. Click **Actions > Process New Kernel**.

f. Click **Yes** on the information window to confirm your decision to restart the machine.

Follow the on-screen instructions to restart your machine and to enable the new settings.

g. If you plan to redirect displays to non-HP machines, do the following before installing:

1) Issue the following command to obtain information on all the public locales that are accessible to your application:

```
# locale -a
```

2) Choose a value for your system from the output that is displayed and set the LANG environment variable to this value. Here is an example command that sets the value of LANG to en_US.iso88591

```
# export LANG=en_US.iso88591
```

8. Verify that prerequisites and corequisites are at the required release levels.

   Although Installation Manager checks for prerequisite operating system patches, review the prerequisites on the Supported hardware and software website if you have not done so already. Refer to the documentation for non-IBM prerequisite and corequisite products to learn how to migrate to their supported versions.

   - If you encounter the following error in the system out or installation log during the installation, you are missing a required linker patch:

```
/usr/lib/dld.sl: Can't find path for shared library: libjli.sl
```

Table 21. Linker patches.

Apply the following linker patch for your operating system version:

Operating system version	Patch
HP 11.23:	PHSS_37201
HP 11.31:	PHSS_37202

9. Verify the system cp command when using emacs or other freeware.

   If you have emacs or other freeware installed on your operating system, verify that the system cp command is used.

   a. Type the following command prompt before running the installation program for the WebSphere Application Server product.

```
which cp
```

   b. Remove the `freeware` directory from your PATH if the resulting directory output includes `freeware`. For example, assume that the output is similar to the following message: `.../freeware/bin/cp`. If so, remove the directory from the PATH.

   c. Install the WebSphere Application Server product.

   d. Add the `freeware` directory back to the PATH.

   If you install with a cp command that is part of a freeware package, the installation might appear to complete successfully, but the Java 2 SDK that the product installs might have missing files in the *app_server_root*/`java` directory.

   Missing files can destroy required symbolic links. If you remove the freeware cp command from the PATH, you can install the application server product successfully.

10. Verify that the Java SDK on the installation image disk is functioning correctly if you created your own disk.

    For example, you might have downloaded an installation image from Passport Advantage, or you might have copied an installation image onto a backup disk. In either case, perform the following steps to verify that the disk contains a valid Java software development kit (SDK).

    a. Change directories to the `/JDK/jre.pak/repository/package.java.jre/java/jre/bin` directory on the product disk. For example:

```
cd /JDK/jre.pak/repository/package.java.jre/java/jre/bin
```

    b. Verify the Java version. Type the following command:

```
./java -version
```

    The command completes successfully with no errors when the SDK is intact.

Results

This procedure results in preparing the operating system for installing the product.

What to do next

After verifying prerequisites, verifying the product disk, and setting your installation goals, you can start installing. Use one of the following links to open the installation procedure that you require.

- Perform an installation using the graphical user interface.

  See "Installing the product on distributed operating systems using the GUI" on page 78.
- Perform a silent installation.

  See "Installing the product on distributed operating systems silently" on page 84.
- Install additional features on an existing product.

  See "Installing and removing features on distributed operating systems" on page 96.

Preparing Linux systems for installation

This topic describes how to prepare a Linux system for installing WebSphere Application Server.

Before you begin

The installation uses Installation Manager. You can use the graphical interface or use a response file in silent mode.

On the SUSE Linux Enterprise Server Version 10 operating system, the xorg-x11-libs package exists by default. This package contains the following libraries, which are required to properly operate WebSphere Application Server:

- libXp
- libXmu
- libXtst

For more information on this package, see the Novell website.

Note: Ensure that the default shell for your Linux operating system is `/bin/bash`. Use the following command to ensure that your default shell is *bash* and not *dash*:

```
$ readlink /bin/sh
```

If the result of the command is *dash*, consult your operating system documentation for the steps to properly switch to *bash* as the default shell. Failure to use the *bash* shell can result in errors and hang situations during the profile creation process.

About this task

Preparing the operating system involves such changes as allocating disk space and installing patches to the operating system. IBM tests WebSphere Application Server products on each operating system platform. Such tests verify whether an operating system change is required for WebSphere Application Server products to run correctly. Without the required changes, WebSphere Application Server products do not run correctly.

While this topic lists many steps that are common to all Linux distributions, specific Linux distributions might require additional steps. Complete all common steps, as well as any additional steps that are required for your distribution. If your distribution is not listed in this topic, but is supported by WebSphere Application Server, check for any post-release technical notes that are available for your operating system at the product support site at http://www.ibm.com/software/webservers/appserv/was/support/. If a technical note is not available for your distribution, additional steps might not be required.

When additional steps are required, it is typically because a default installation of the distribution does not provide required libraries or operating system features. If you install WebSphere Application Server on a customized Linux installation that has installed packages that differ significantly from the packages provided by a default installation of the distribution, ensure that your customized installation has the packages required for WebSphere Application Server to run. WebSphere Application Server does not maintain lists of the packages required for each Linux distribution or for updates to each distribution.

For WebSphere Application Server to run adequately, your Linux installation must have the following items:

- Kernel and C runtime library
- Current® and all compatibility versions of the C++ runtime library
- X Windows libraries and runtime
- GTK runtime libraries

Procedure

1. Log on to the operating system.

   You can log on as root or as a nonroot installer.

   Select a umask that allows the owner to read/write to the files, and allows others to access them according to the prevailing system policy. For root, a umask of 022 is recommended. For nonroot users a umask of 002 or 022 can be used, depending on whether the users share the group. To verify the umask setting, issue the following command:

```
umask
```

   To set the umask setting to 022, issue the following command:

```
umask 022
```

2. Download and install the Mozilla Firefox web browser.

   If you do not have the Firefox browser, download and install the browser from http://www.mozilla.org/products/firefox/.

   Note: It might be necessary to run `>firefox &url` from directories other than the one where Firefox is installed, so ensure that Firefox is in the path. You can add a symbolic link to the Firefox directory by entering:

   ```
   >ln -s /locationToFirefox/firefox firefox
   ```

3. Optional: Export the location of the supported browser.

   Export the location of the supported browser using a command that identifies the actual location of the browser.

   If the Mozilla Firefox package is in the `/opt/bin/firefox` directory, for example, use the following command:

```
export BROWSER=/opt/bin/firefox
```

4. Stop all Java processes related to WebSphere Application Server on the machine where you are installing the product.
5. Stop any web server process such as the IBM HTTP Server.
6. Provide adequate disk space.

   The amount of disk space required varies with the number of features or products installed. If you are installing the product using Installation Manager, the installation summary panel indicates the approximate amount of disk space required based on the features and products that you have selected.Installing all features and products requires approximately 2 GB of disk space. This estimate includes the following products, components, and features:

   - Main application server product installation
   - Profiles
   - Sample applications
   - IBM HTTP Server
   - Web Server Plug-ins
   - Application Client for WebSphere Application Server

If you plan to migrate applications and the configuration from a previous version, verify that the application objects have enough disk space. As a rough guideline, plan for space equal to 110 percent of the size of the applications.

7. Verify that prerequisites and corequisites are at the required release levels.

   Although Installation Manager checks for prerequisite operating system patches, review the prerequisites on the Supported hardware and software website if you have not done so already.

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

8. Increase the ulimit setting in the bash command shell profile to prevent addNode and importWasprofile problems.

   The addNode command script can fail when adding a node, or the importWasprofile command can fail when importing a configuration archive.

   Set a higher ulimit setting for the kernel in the bash shell profile script, which is loaded at login time for the session.

   Set the ulimit on your Linux command shells by adding the command to your shell profile script. The shell profile script is usually found under your home directory:

   a. `cd ~`
   b. `vi .bashrc`
   c. `ulimit -n 8192`

9. Restore the original copy of the `etc/issue` file if the file is modified.

   Installation Manager uses the file to verify the version of the operating system. If you cannot restore the original version, ignore the Operating System Level Check message about the operating system being unsupported. The installation can continue successfully despite the warning.

10. Verify the system cp command when using emacs or other freeware.

    If you have emacs or other freeware installed on your operating system, verify that the system cp command is used.

    a. Type the following command prompt before running the installation program for the WebSphere Application Server product.

```
which cp
```

    b. Remove the `freeware` directory from your PATH if the resulting directory output includes `freeware`. For example, assume that the output is similar to the following message: `.../freeware/bin/cp`. If so, remove the directory from the PATH.
    c. Install the WebSphere Application Server product.
    d. Add the `freeware` directory back to the PATH.

    If you install with a cp command that is part of a freeware package, the installation might appear to complete successfully, but the Java 2 SDK that the product installs might have missing files in the *app_server_root*/`java` directory.

    Missing files can destroy required symbolic links. If you remove the freeware cp command from the PATH, you can install the application server product successfully.

11. Complete any distribution-specific set up.

    Complete the steps for your distribution:

    - “Preparing Asianux Server 3 for installation” on page 59
    - “Preparing Red Hat Enterprise Linux 5 for installation” on page 61
    - “Preparing Red Hat Enterprise Linux 6 for installation” on page 63
    - “Preparing SUSE Linux Enterprise Server 10 for installation” on page 66
    - “Preparing SUSE Linux Enterprise Server 11 for installation” on page 66

    If you are using a supported distribution other than those listed above, examine the WebSphere Application Server support site for any technical notes that are published for your distribution. If technical notes have been published, apply the fixes.

12. Grant a non-root installer ID the correct file permissions to create menu entries in Gnome and KDE.

    Before the installation, the root user can grant write permission to the non-root installer for the `/etc/xdg/menus/applications-merged` directory. Then, Installation Manager creates the menu entries during the non-root installation.

    Otherwise, you must run scripts to create and remove the menu entries while WebSphere Application Server Network Deployment is installed.

Results

This procedure results in preparing the operating system for installing the product.

What to do next

After verifying prerequisites, verifying the product disk, and setting your installation goals, you can start installing. Use one of the following links to open the installation procedure that you require.

- Perform an installation using the graphical user interface.

  See "Installing the product on distributed operating systems using the GUI" on page 78.
- Perform a silent installation.

  See "Installing the product on distributed operating systems silently" on page 84.
- Install additional features on an existing product.

  See "Installing and removing features on distributed operating systems" on page 96.

Preparing Asianux Server 3 for installation

You must complete additional steps to prepare an Asianux Server 3 system for a WebSphere Application Server installation.

Before you begin

Complete steps 1-10 in "Preparing Linux systems for installation" on page 56. Those steps are common to any Linux system.

Note: The RedCastle security service is not supported with WebSphere Application Server.

About this task

In addition to the common steps required for installing any Linux system, a few system-specific steps are required for Asianux Server 3.

Verify that the prerequisite packages are installed. A Linux package registration limitation prevents the prerequisites checker program from examining prerequisite packages on Linux systems. For more information, see "Installing and verifying Linux packages" on page 67.

Procedure

1. Install packages for all hardware platforms.

   Install the following packages on any hardware platform:

   compat-libstdc++-33-3.2.3-61

   Required for C++ runtime compatibility. Used by such components as GSKit, the Java 2 Software Development Kit (SDK), and the Web Server Plug-ins.

   compat-db-4.2.52-5.1

   Required by IBM HTTP Server. Some of the modules use the libraries that exist within this package.

ksh-20080202-14
Required by IBM HTTP Server.

gtk2-2.10.4-20
Required by IBM Installation Manager.

gtk2-engines-2.8.0-3
Required by IBM Installation Manager.

libXp-1.0.0-8
Required by the Java 2 SDK to provide printing functions for graphical user interfaces. Without this package, Swing-based applications and AWT-based applications, such as InstallShield for Multiplatforms (ISMP), cannot instantiate.

libXmu-1.0.2-5

libXtst-1.0.1-3.1

pam-0.99.6.2-4

rpm-build-4.4.2.3-9
Required by ISMP to properly register products within the RPM database.

elfutils-0.137

elfutils-libs-0.137

libXft-2.1.10-1.1
Required to install the application server using a user interface.

libstdc++-4.1.2-48

These packages are part of the Asianux Server 3 operating system, but might not be installed by default. Also, you can install a later release of any of these packages.

2. Select packages for hardware platforms that can run both 32-bit and 64-bit applications. If you are running 64-bit Asianux Server 3 operating system, then you must install both the 32-bit and 64-bit versions of the following packages.

   Hardware platforms that can run both 32-bit and 64-bit applications include Opteron and EM64T for the Asianux Server 3 operating system in terms of applicability to WebSphere Application Server. There are situations in which you might have 64-bit runtime support on these platforms only. However, various applications that are included with WebSphere Application Server Version 6.1 products and packages also require the 32-bit runtime support. Therefore, you must install the 32-bit runtime support.

   Install the following required 32-bit packages by selecting to customize the packages during the Asianux Server 3 installation. Or, customize packages on an existing system by issuing the appropriate system software configuration commands.

   Platforms that support both 32-bit and 64-bit applications require both the 32-bit and 64-bit versions of the following packages:
   - compat-libstdc++-33-3.2.3-61
   - compat-db-4.2.52-5.1
   - gtk2-2.10.4-20
   - gtk2-engines-2.8.0-3
   - libstdc++-4.1.2-48
   - libXft-2.1.10-1.1
   - libXp-1.0.0-8
   - libXmu-1.0.2-5
   - libXtst-1.0.1-3.1
   - pam-0.99.6.2-4

   Run the rpm -qa | grep *package_name* command to verify that you have both versions of each package. Substitute the name of each package for the *package_name* variable.

Installed packages are displayed in the reply to the command. If you do not get two replies for each package, you have only one version of the package installed. You must then install the missing package.

3. Install additional packages for specific platforms.

   In addition to the packages that are common to all platforms, install the following package on hardware platforms that can run both 32-bit and 64-bit applications before installing WebSphere Application Server products and packages.

   x86 platforms and Opteron or EM64T platforms: compat-libstdc++-296-2.96-138
   The compat-libstdc++ package is required for C++ runtime compatibility. The package is used by such components as GSKit, the Java 2 SDK, and the Web Server Plug-ins.

Results

If you do not install all the required packages, the Installation wizard cannot start. Error messages indicate missing libraries, the inability to load graphical interfaces, or other errors that occur during the installation.

What to do next

After you complete the steps in this topic, proceed to the final step in “Preparing Linux systems for installation” on page 56.

Preparing Red Hat Enterprise Linux 5 for installation

You must complete additional steps to prepare a Red Hat Enterprise Linux Version 5 system for a WebSphere Application Server installation.

Before you begin

Complete all steps in “Preparing Linux systems for installation” on page 56. Those steps are common to any Linux system.

About this task

In addition to the common steps required for installing any Linux system, a few system specific steps are required for Red Hat Enterprise Linux Version 5.

Verify that the prerequisite packages are installed. A Linux package registration limitation prevents the prerequisites checker program from examining prerequisite packages on Linux systems. See “Installing and verifying Linux packages” on page 67 for more information.

You should consider the following points if you have enabled Security-Enhanced Linux (SELinux) on your Red Hat Enterprise Linux Version 5 operating system.

- If SELinux is enabled and enforced while you are installing the product from the CD, then you must mount the CD with the following option:

  ```
  -o context=system_u:object_r:textrel_shlib_t
  ```
- If you enable SELinux after installing the product while SELinux was disabled, then the file labels will be reset when the system is rebooted. In this case, you must run the relabel_linux.sh script located in *app_server_root*/`properties/install/script/` to relabel the product runtime files. Note that running the relabel_linux.sh command is not necessary if you made security mode changes with the command setenforce, which does not required a system reboot.

Procedure

1. Install packages for all hardware platforms.

   Install the following packages on any hardware platform:

compat-libstdc++-33-3.2.3-61
Required for C++ runtime compatibility. Used by such components as GSKit, the Java 2 Software Development Kit (SDK), and the Web Server Plug-ins.

compat-db-4.2.52-5.1
Required by IBM HTTP Server Some of the modules use the libraries contained within this package.

ksh-20080202-14
Required by IBM HTTP Server.

gtk2-2.10.4-20
Required by IBM Installation Manager.

gtk2-engines-2.8.0-3
Required by IBM Installation Manager.

libXp-1.0.0-8
Required by the Java 2 SDK to provide printing functions for graphical user interfaces. Without this package, Swing-based applications and AWT-based applications, such as InstallShield for Multiplatforms (ISMP), cannot instantiate.

libXmu-1.0.2-5

libXtst-1.0.1-3.1

pam-0.99.6.2-3.26.el5

rpm-build-4.4.2-37.*architecture*.el5 or later
Required by ISMP to properly register products within the RPM database.

elfutils-0.125-3.el5

elfutils-libs-0.125-3.el5

libXft-2.1.10-1.1
Required to install the application server using a user interface.

libstdc++-4.1.2-48

These packages are part of the Red Hat Enterprise Linux 5 operating system, but might not installed by default. You can also install a later release of any of these packages if Red Hat provides new packages as errata.

2. Select packages for hardware platforms that are capable of running both 32-bit and 64-bit applications.

   Hardware platforms capable of running both 32-bit and 64-bit applications include Opteron, EM64T, iSeries®, pSeries® (PowerPC®), and zSeries® (64-bit) machines.

   By default, RHEL 5 only installs 64-bit runtime support on these platforms. However, various applications included with WebSphere Application Server Version 8.x products and packages also require the 32-bit runtime support. Therefore, you must install the 32-bit runtime support.

   Install the following required 32-bit packages by selecting to customize the packages during the RHEL 5 installation. Or, customize packages on an existing RHEL 5 system by issuing the `system-config-packages` command from a graphical terminal.

   Install the Compatibility Architecture Support under the System category. Optionally install the Compatibility Architecture Development Support under the Development category if you intend to build C or C++ libraries for use with both 32-bit and 64-bit applications.

   Platforms that support both 32-bit and 64-bit applications require both the 32-bit and 64-bit versions of the following packages:

   - compat-libstdc++-33-3.2.3-61
   - compat-db-4.2.52-5.1
   - gtk2-2.10.4-20
   - gtk2-engines-2.8.0-3

- libstdc++-4.1.2-48
- libXft-2.1.10-1.1
- libXp-1.0.0-8
- libXmu-1.0.2-5
- libXtst-1.0.1-3.1
- pam-0.99.6.2-3.26.el5

Run the `rpm -qa | grep` *`package_name`* command to verify that you have both versions of each package. Substitute the name of each package for the *package_name* variable.

Installed packages are displayed in the reply to the command. If you do not get two replies for each package, you have only one version of the package installed. You must then install the missing package.

3. Install additional packages for specific platforms.

   In addition to the packages that are common to all platforms, install the following packages on hardware platforms capable of running both 32-bit and 64-bit applications before installing WebSphere Application Server products and packages.

   x86 platforms and Opteron or EM64T platforms: compat-libstdc++-296-2.96-138
   The compat-libstdc++ package is required for C++ runtime compatibility. The package is used by such components as GSKit, the Java 2 SDK, and the Web Server Plug-ins.

   z/Series platforms: compat-libstdc++-295-2.95.3-85
   The compat-libstdc++ package is required for C++ runtime compatibility. The package is used by such components as GSKit, the Java 2 SDK, and the Web Server Plug-ins.

   Install both the 32-bit version and the 64-bit version of the package on 64-bit z/Series hardware platforms.

Results

If you do not install all of the required packages, the installation will not perform as intended. Error messages indicate missing libraries, the inability to load graphical interfaces, or other errors that occur during the installation.

What to do next

After you complete the steps in this topic, proceed to "What to do next" in “Preparing Linux systems for installation” on page 56.

Preparing Red Hat Enterprise Linux 6 for installation

You must complete additional steps to prepare a Red Hat Enterprise Linux Version 6 system for a WebSphere Application Server installation.

Before you begin

Complete all steps in “Preparing Linux systems for installation” on page 56. Those steps are common to any Linux system.

About this task

In addition to the common steps required for installing any Linux system, a few system-specific steps are required for Red Hat Enterprise Linux Version 6.

Verify that the prerequisite packages are installed. A Linux package registration limitation prevents the prerequisites checker program from examining prerequisite packages on Linux systems. See “Installing and verifying Linux packages” on page 67 for more information.

You should consider the following points if you have enabled Security-Enhanced Linux (SELinux) on your Red Hat Enterprise Linux Version 6 operating system.

- If SELinux is enabled and enforced while you are installing the product from the disk, you must mount the disk with the following option:

  ```
  -o context=system_u:object_r:textrel_shlib_t
  ```

- If you enable SELinux after installing the product while SELinux was disabled, the file labels will be reset when the system is rebooted. In this case, you must run the `relabel_linux.sh` script located in *app_server_root*`/properties/install/script/` to relabel the product runtime files. Note that running the `relabel_linux.sh` command is not necessary if you made security mode changes with the command setenforce, which does not require a system reboot.

Procedure

1. Install packages for all hardware platforms.

   Install the following packages on any hardware platform:

   compat-libstdc++-33-3.2.3-69
   Required for C++ runtime compatibility; used by such components as GSKit, the Java 2 Software Development Kit (SDK) and the Web Server Plug-ins

   compat-db-4.6.21-15
   Required by IBM HTTP Server; some of the modules use the libraries contained within this package

   ksh-20100621-2
   Required by IBM HTTP Server

   gtk2-2.18.9-4
   Required by the IBM Installation Manager

   gtk2-engines-2.18.4-5
   Required by the IBM Installation Manager

   libXp-1.0.0-15.1
   Required by the Java 2 SDK to provide printing functions for graphical user interfaces

   Without this package, Swing-based applications and AWT-based applications, such as InstallShield for Multiplatforms (ISMP), cannot instantiate.

   libXmu-1.0.5-1

   libXtst-1.0.99.2-3

   pam-1.1.1-4

   rpm-build-4.8.0-12
   Required by ISMP to properly register products within the RPM database

   elfutils-0.148-1

   elfutils-libs-0.148-1

   libXft-2.1.13-4.1
   Required to install the application server using a user interface.

   libstdc++-4.4.4-13

   These packages are part of the Red Hat Enterprise Linux 6 operating system, but they might not installed by default. You can also install a later release of any of these packages if Red Hat provides new packages as errata.

2. Install packages for hardware platforms that are capable of running both 32-bit and 64-bit applications.

   Hardware platforms capable of running both 32-bit and 64-bit applications include Opteron, EM64T, IBM i, pSeries (PowerPC), and zSeries (64-bit) machines.

By default, RHEL 6 only installs 64-bit runtime support on these platforms. However, various applications included with WebSphere Application Server Version 8 products and packages also require the 32-bit runtime support. Therefore, you must install the 32-bit runtime support.

Install the following required 32-bit packages by selecting to customize the packages during the RHEL 6 installation or by installing the packages later through the appropriate rpm or yum commands.

Install the Compatibility Architecture Support under the System category. Optionally, install the Compatibility Architecture Development Support under the Development category if you intend to build C or C++ libraries for use with both 32-bit and 64-bit applications.

Platforms that support both 32-bit and 64-bit applications require both the 32-bit and 64-bit versions of the following packages:

- compat-libstdc++-33-3.2.3-69
- compat-db-4.6.21-15
- libstdc++-4.4.4-13
- libXp-1.0.0-15.1
- libXmu-1.0.5-1
- libXtst-1.0.99.2-3
- pam-1.1.1-4
- libXft-2.1.13-4.1
- gtk2-2.18.9-4
- gtk2-engines-2.18.4-5

Run the `rpm -qa | grep` *`package_name`* command to verify that you have both versions of each package. Substitute the name of each package for the *package_name* variable.

Installed packages are displayed in the reply to the command. If you do not get two replies for each package, you have only one version of the package installed. You must then install the missing package.

3. Install packages on specific hardware platforms capable of running both 32-bit and 64-bit applications.

   In addition to the packages that are common to all platforms, install the following packages on hardware platforms capable of running both 32-bit and 64-bit applications before installing WebSphere Application Server products and packages.

   x86 platforms and Opteron or EM64T platforms:
   compat-libstdc++- 296-2.96-144

   The compat-libstdc++ package is required for C++ runtime compatibility. The package is used by such components as GSKit, the Java SDK, and the Web Server Plug-ins.

   z/Series platforms:
   compat-libstdc++-295-2.95.3-86

   The compat-libstdc++ package is required for C++ runtime compatibility. The package is used by such components as GSKit, the Java SDK, and the Web Server Plug-ins.

   Install both the 31-bit version and the 64-bit version of the package on 64-bit z/Series hardware platforms.

4. If you plan to install WebSphere Application Server on a system with a 32-bit JDK, make sure that any corresponding libraries are installed.

Results

If you do not install all of the required packages, the installation will not perform as intended. Error messages indicate missing libraries, the inability to load graphical interfaces, or other errors that occur during the installation.

What to do next

After you complete the steps in this topic, proceed to "What to do next" in “Preparing Linux systems for installation” on page 56.

Preparing SUSE Linux Enterprise Server 10 for installation

You might have to complete additional steps to prepare a SUSE Linux Enterprise Server Version 10 system for a WebSphere Application Server installation.

Before you begin

Complete all steps in “Preparing Linux systems for installation” on page 56. Those steps are common to any Linux system.

Procedure

Verify that the appropriate library package or packages exist on your SUSE Linux Enterprise Server Version 10 operating system.
For the 32-bit SUSE Linux Enterprise Server Version 10 operating system, the xorg-x11-libs package is required before installing and using WebSphere Application Server. This package contains the following libraries:

- libXp
- libXmu
- libXtst

For the 64-bit SUSE Linux Enterprise Server Version 10 operating system, both the xorg-x11-libs package and the xorg-x11-libs-32bit package are required before installing and using WebSphere Application Server.
For more information on these packages, see the Novell website.

What to do next

After you complete the steps in this topic, proceed to "What to do next" in “Preparing Linux systems for installation” on page 56.

Preparing SUSE Linux Enterprise Server 11 for installation

You might have to complete additional steps to prepare a SUSE Linux Enterprise Server Version 11 system for a WebSphere Application Server installation.

Before you begin

Complete all steps in “Preparing Linux systems for installation” on page 56. Those steps are common to any Linux system.

Procedure

Verify that the appropriate library package or packages exist on your SUSE Linux Enterprise Server Version 11 operating system.
For the 32-bit SUSE Linux Enterprise Server Version 11 operating system, the xorg-x11-libs package is required before installing and using WebSphere Application Server. This package contains the following libraries:

- libXp
- libXmu
- libXtst

For the 64-bit SUSE Linux Enterprise Server Version 11 operating system, both the xorg-x11-libs package and the xorg-x11-libs-32bit package are required before installing and using WebSphere Application Server.
For more information on these packages, see the Novell website.

What to do next

After you complete the steps in this topic, proceed to "What to do next" in “Preparing Linux systems for installation” on page 56.

Installing and verifying Linux packages

This topic describes how to query a Linux system to verify that a package is installed. The topic also describes how to install a missing package from an operating system CD.

Before you begin

Install the Linux operating system before using this procedure.

About this task

Use the following procedure to install and verify prerequisite libraries (packages) that WebSphere Application Server products require on Linux systems.

Assume that your Linux operating system requires the compat-libstdc++-33-3.2.3-47.3 package and that there are two versions of the package. One version is for 32-bit platforms and the other is for 64-bit platforms. This procedure shows how to query the operating system to see if the packages are installed, find the missing packages on the operating system disk, and install the packages.

This example uses Red Hat Enterprise Linux (RHEL) on a PowerPC 64-bit hardware platform. The example assumes that RHEL requires both the 32-bit version and the 64-bit version of the compat-libstdc++-33-3.2.3-47.3 package.

Procedure

1. Query the operating system to determine if the packages are already installed.

```
rpm -qa | grep compat-libstdc++-33-3.2.3-
```

   In this example, the operating system did not find any matching packages so a blank line is displayed.

   You can also search without the grep argument to see an explicit message about the file:

```
rpm -q compat-libstdc++-33-3.2.3-
```

   The operating system returns the following message:

```
package compat-libstdc++-33-3.2.3- is not installed
```

2. Find all related packages on the operating system media to get the fully qualified locations.

   This example assumes that the operating system media is a CD mounted at *mount_directory*.

```
find mount_directory -name compat-libstdc++-33-3.2.3-*
```

   In this example, the operating system finds two matching package names. One package is the 32-bit version, and the other is the 64-bit version.

```
mount_directory/Server/compat-libstdc++-33-3.2.3-47.3.ppc.rpm
mount_directory/Server/compat-libstdc++-33-3.2.3-47.3.ppc64.rpm
```

3. Install the first missing package:

```
rpm -ivh mount_directory/Server/compat-libstdc++-33-3.2.3-47.3.ppc.rpm
```

4. Install the second missing package:

```
rpm -ivh mount_directory/Server/compat-libstdc++-33-3.2.3-47.3.ppc64.rpm
```

5. Optional: **Alternative method to find and install packages in one command:** Use the following command to find packages and to install all packages that are found.

Find the packages as described in the earlier step to verify that the following command installs only the packages that you intend to install.

```
find mount_directory -name compat-libstdc++-33-3.2.3-* | xargs rpm -ivh
```

This single command installs both packages.

6. Optional: **Alternative command to update existing packages:** Use the following command to find and install missing packages or to find and update existing packages:

```
find /mount_directory -name compat-libstdc++-33-3.2.3-* | xargs rpm -Uvh
```

This single command installs a package when the package is not installed. This command updates a package to a newer version when the package is installed.

What to do next

Required packages vary by operating system. See "Preparing Linux systems for installation" on page 56 for a list of required packages for each Linux operating system.

Preparing Solaris systems for installation

This topic describes how to prepare Solaris systems for the installation of IBM WebSphere Application Server products.

Before you begin

The installation uses Installation Manager. You can use the graphical interface or use a response file in silent mode.

Restriction: There are known issues with using Cygwin/X to run Eclipse-based applications on remote Solaris machines. This affects your use of the Profile Management Yool. With Cygwin/X on remote Solaris, for example, the Profile Management Tool welcome panel appears but no keyboard or mouse input is accepted. For details of existing Bugzilla reports on these issues, see the information at https://bugs.eclipse.org/bugs/show_bug.cgi?id=97808. If a different X server (such as Hummingbird Exceed®) is used, these problems do not occur.

About this task

Preparing the operating system involves such changes as allocating disk space and installing patches to the operating system. IBM tests WebSphere Application Server products on each operating system platform. Such tests verify whether an operating system change is required for WebSphere Application Server products to run correctly. Without the required changes, WebSphere Application Server products do not run correctly.

Procedure

1. Log on to the operating system.

   You can log on as root or as a nonroot installer.

   Select a umask that allows the owner to read/write to the files, and allows others to access them according to the prevailing system policy. For root, a umask of 022 is recommended. For nonroot users a umask of 002 or 022 can be used, depending on whether the users share the group. To verify the umask setting, issue the following command:

```
umask
```

   To set the umask setting to 022, issue the following command:

```
umask 022
```

2. Make sure that you select the **Entire Group** option on the **Select Solaris Software Group** panel when you set up your system.
3. Optional: Download and install the Mozilla Firefox web browser.

If you do not have the Mozilla web browser, download and install the browser from http://www.mozilla.org/products/firefox.

4. Optional: Export the location of the supported browser.

   Export the location of the supported browser using a command that identifies the actual location of the browser.

   If the Mozilla Firefox package is in the `/opt/bin/firefox` directory, for example, use the following command:

```
export BROWSER=/opt/bin/firefox
```

5. Optional: Configure Hummingbird Exceed to disable Automatic Font Substitution.

   Font changes occur when using the Hummingbird Exceed package and invoke the Profile Management Tool. When you use the Hummingbird Exceed package to connect to a machine running the Solaris operating system, and then invoke the Profile Management Tool, some font sizes and styles display differently than when doing the same operation from the native Solaris display.

   The font sizes and style changes are based on the font selections in the bundled Java SE Runtime Environment 6 (JRE 6).

   To prevent the various font changes, configure Hummingbird Exceed to disable Automatic Font Substitution:

   a. From the Hummingbird Exceed user interface, click **Xconfig** > **Font** > **Font Database** > **Disable (Automatic Font Substitution)**.

   b. Click **OK**.

   c. Restart the Hummingbird Exceed package.

6. Stop all Java processes related to WebSphere Application Server on the machine where you are installing the product.

7. Stop any web server process such as the IBM HTTP Server.

8. Provide adequate disk space.

   The amount of disk space required varies with the number of features or products installed. If you are installing the product using Installation Manager, the installation summary panel indicates the approximate amount of disk space required based on the features and products you have selected.Installing all features and products requires approximately 2 GB of disk space. This estimate includes the following products, components, and features:

   - Main application server product installation
   - Profiles
   - Sample applications
   - IBM HTTP Server
   - Web Server Plug-ins
   - Application Client for WebSphere Application Server

   If you plan to migrate applications and the configuration from a previous version, verify that the application objects have enough disk space. As a rough guideline, plan for space equal to 110 percent of the size of the applications.

9. Set kernel values to support Application Server. Several Solaris kernel values are typically too small.

   The instructions in this step apply to the Solaris SPARC (32-bit and 64-bit) operating system only. For Solaris x64 processor-based systems, see How to Get Started with IBM WebSphere Application Server on Solaris 10 and Zones. The article was written for Solaris 10 on SPARC but the principles apply equally to x64.

   Before installing, review the machine configuration:

```
sysdef -i
```

   The kernel values are set in the `/etc/system` file, as shown in the following example.

```
set shmsys:shminfo_shmmax = 4294967295
set shmsys:shminfo_shmseg = 1024
set shmsys:shminfo_shmmni = 1024
set semsys:seminfo_semaem = 16384
set semsys:seminfo_semmni = 1024
set semsys:seminfo_semmap = 1026
set semsys:seminfo_semmns = 16384
set semsys:seminfo_semmsl = 100
set semsys:seminfo_semopm = 100
set semsys:seminfo_semmnu = 2048
set semsys:seminfo_semume = 256
set msgsys:msginfo_msgmap = 1026
set msgsys:msginfo_msgmax = 65535
set rlim_fd_cur=1024
```

You can change kernel values by editing the `/etc/system` file then rebooting the operating system. For more information about setting up the Solaris system, see the Sun Microsystems documentation. For example, the Solaris Tunable Parameters Reference Manual.

10. Verify that prerequisites and corequisites are at the required release levels.

    Although Installation Manager checks for prerequisite operating system patches, review the prerequisites on the Supported hardware and software website if you have not done so already. Refer to the documentation for non-IBM prerequisite and corequisite products to learn how to migrate to their supported versions.

    Note: If your Solaris system does not have sufficient available memory as specified on the supported hardware and software website, you might experience a prerequisite error during installation: "A supported operating system architecture was not detected". If you proceed to the end of the installation, you might also see the following insufficient disk space error:

```
java.io.IOException: Cannot run program "sh": error=12, Not enough space
        at java.lang.ProcessBuilder.start(ProcessBuilder.java:459)
        at java.lang.Runtime.exec(Runtime.java:593)
        at java.lang.Runtime.exec(Runtime.java:466)
```

Free up additional memory on the machine and retry the installation.

11. Verify the system cp command when using emacs or other freeware.

    If you have emacs or other freeware installed on your operating system, verify that the system cp command is used.

    a. Type the following command prompt before running the installation program for the WebSphere Application Server product.

```
which cp
```

    b. Remove the `freeware` directory from your PATH if the resulting directory output includes `freeware`. For example, assume that the output is similar to the following message: `.../freeware/bin/cp`. If so, remove the directory from the PATH.
    c. Install the WebSphere Application Server product.
    d. Add the `freeware` directory back to the PATH.

    If you install with a cp command that is part of a freeware package, the installation might appear to complete successfully, but the Java 2 SDK that the product installs might have missing files in the *app_server_root*/`java` directory.

    Missing files can destroy required symbolic links. If you remove the freeware cp command from the PATH, you can install the application server product successfully.

12. Verify that the Java SDK on the installation image disk is functioning correctly if you created your own disk.

    For example, you might have downloaded an installation image from Passport Advantage, or you might have copied an installation image onto a backup disk. In either case, perform the following steps to verify that the disk contains a valid Java software development kit (SDK).

    a. Change directories to the `/JDK/jre.pak/repository/package.java.jre/java/jre/bin` directory on the product disk. For example:

```
cd /JDK/jre.pak/repository/package.java.jre/java/jre/bin
```

    b. Verify the Java version. Type the following command:

```
./java -version
```

The command completes successfully with no errors when the SDK is intact.

Results

This procedure results in preparing the operating system for installing the product.

What to do next

After verifying prerequisites, verifying the product disk, and setting your installation goals, you can start installing. Use one of the following links to open the installation procedure that you require.

- Perform an installation using the graphical user interface.

  See “Installing the product on distributed operating systems using the GUI” on page 78.
- Perform a silent installation.

  See “Installing the product on distributed operating systems silently” on page 84.
- Install additional features on an existing product.

  See “Installing and removing features on distributed operating systems” on page 96.

Preparing Windows systems for installation

This topic describes how to prepare your Windows systems for the installation of IBM WebSphere Application Server products.

Before you begin

The installation uses Installation Manager. You can use the graphical interface or use a response file in silent mode.

About this task

Preparing the operating system involves such changes as allocating disk space and installing patches to the operating system. IBM tests WebSphere Application Server products on each operating system platform. Such tests verify whether an operating system change is required for WebSphere Application Server products to run correctly. Without the required changes, WebSphere Application Server products do not run correctly.

Procedure

1. Log on to a user ID that belongs to the administrator group.

   Log on as a member of the administrator group to successfully install the product. You cannot create Windows services from a user ID that does not belong to the administrator group. The creation of Windows services requires the user to have the advanced user rights *Act as part of the operating system* and *Log on as a service*.

   During the procedure, you can assign another ID or the one you are using to install as the user who will log on the Windows service. That user requires the advanced user right: *Log on as a service*.

   However, if you do not have this advanced user right or if the user ID that is to log on the Windows service does not have the advanced user right, Installation Manager assigns the advanced right to the user.
2. Optional: Download and install a web browser.

   If your system does not have a default browser or the browser has been corrupted or installed incorrectly, then you might experience errors when trying to open various links in the installation panels.
3. Stop all Java processes related to WebSphere Application Server on the machine where you are installing the product.
4. Stop any web server process such as the IBM HTTP Server.
5. Stop all instances of the `process_spawner.exe` program.

6. Provide adequate disk space.

   The amount of disk space required varies with the number of features or products installed. If you are installing the product using Installation Manager, the installation summary panel indicates the approximate amount of disk space required based on the features and products you have selected.Installing all features and products requires approximately 2 GB of disk space. This estimate includes the following products, components, and features:

   - Main application server product installation
   - Profiles
   - Sample applications
   - IBM HTTP Server
   - Web Server Plug-ins
   - Application Client for WebSphere Application Server

   If you plan to migrate applications and the configuration from a previous version, verify that the application objects have enough disk space. As a rough guideline, plan for space equal to 110 percent of the size of the applications.

7. Verify that prerequisites and corequisites are at the required release levels.

   Although Installation Manager checks for prerequisite operating system patches, review the prerequisites on the Supported hardware and software website if you have not done so already.

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

Results

This procedure results in preparing the operating system for installing the product.

What to do next

After verifying prerequisites, verifying the product disk, and setting your installation goals, you can start installing. Use one of the following links to open the installation procedure that you require.

- Perform an installation using the graphical user interface.

  See “Installing the product on distributed operating systems using the GUI” on page 78.
- Perform a silent installation.

  See “Installing the product on distributed operating systems silently” on page 84.
- Install additional features on an existing product.

  See “Installing and removing features on distributed operating systems” on page 96.

Chapter 6. Installing the product

Install the application server product on AIX, HP-UX, Linux, Solaris, or Windows operating systems.

Before you begin

Before you use the installation tools, prepare for installation and to learn about installation options. Also read the hardware and software requirements on the Supported hardware and software website.

Use the launchpad to launch each installation procedure. Read “Using the launchpad to start installations” on page 17 for more information.

About this task

Use the information in this article to learn about the types of installation available. This article has links to more detailed installation topics.

You can install a product using the Installation Manager GUI or silent mode. Installation Manager performs the following actions:

- Automatically checks prerequisites
- Looks for a previous WebSphere Application Server installation to determine whether to let you add features to the product binaries or to install a new set of product binaries
- Looks for a previous installation to determine whether to let you upgrade from a trial installation to the real product
- Installs the necessary product binaries

Procedure

1. Plan your installation as described in Chapter 4, “Planning the WebSphere Application Server product installation,” on page 23.
2. Prepare your operating platform for installation as described in Chapter 5, “Preparing the operating system for product installation,” on page 47.
3. Review the roadmap for installing the Network Deployment product as described in “Roadmap: Installing the Network Deployment product” on page 111.
4. Install the product and any optional components.
   - Install Application Client for IBM WebSphere Application Server.

     Application Client for IBM WebSphere Application Server provides resources and clients to aid development of client applications for use with WebSphere Application Server.

     You do not need to install the Application Client for IBM WebSphere Application Server unless an application that you are deploying was designed to run as a client application.
   - Install DMZ Secure Proxy Server for IBM WebSphere Application Server.

     Use DMZ Secure Proxy Server for IBM WebSphere Application Server 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.
   - Install IBM HTTP Server for WebSphere Application Server.

     IBM HTTP Server is a web server based on the Apache HTTP Server developed by the Apache Software Foundation (ASF). This product provides advanced web server capabilities and a consistent cross-platform build of the Apache HTTP Server.

     After installing a WebSphere Application Server product, you can use the application server to serve applications over the Internet. It is not necessary to install the IBM HTTP Server or another web server.

The installation solution diagrams in Chapter 4, “Planning the WebSphere Application Server product installation,” on page 23 show the components that are present in different types of environments.

- Install the Web Server Plug-ins for IBM WebSphere Application Server.

  If you install the IBM HTTP Server or another web server, you must then install a binary module for the web server to enable it to communicate with WebSphere Application Server products.

  After installing a web server plug-in, you can use the Web Server Plug-ins Configuration Tool to create a new element in the application server configuration called a *web server definition*. You can then manage applications for the web server using the administrative console.

- Install the WebSphere Customization Toolbox.

  The WebSphere Customization Toolbox includes tools for customizing various parts of your WebSphere Application Server environment. For example, you can use the WebSphere Customization Toolbox graphical user interface (GUI) to launch the Web Server Plug-ins Configuration Tool to configure your web server plug-ins for any operating system on which the WebSphere Customization Toolbox can be installed.

  Install the z/OS Profile Management Tool on a Windows or Linux operating system to generate jobs and instructions for creating profiles for WebSphere Application Server on z/OS systems, or install the z/OS Migration Management Tool on a Windows or Linux operating system to generate definitions for migrating WebSphere Application Server for z/OS profiles.

Installing and uninstalling the product on distributed operating systems

IBM Installation Manager is a common installer for many IBM software products that you use to install this version of WebSphere Application Server.

Before you begin

Note: WebSphere Application Server Version 8.0 is the first full version to be installed by Installation Manager rather than by the programs based on InstallShield MultiPlatform (ISMP) that are used to install, update, and uninstall previous versions. Installation Manager is a single installation program that can use remote or local software flat-file repositories to install, modify, or update new WebSphere Application Server products. It determines and shows available packages—including products, fix packs, interim fixes, and so on—checks prerequisites and interdependencies, and installs the selected packages. You also use Installation Manager to easily uninstall the packages that it installed.

Overview of IBM Installation Manager: IBM Installation Manager is a general-purpose software installation and update tool that runs on a range of computer systems. Installation Manager can be invoked through a graphical user interface (GUI) or a command-line interface. You can also create response files in XML and use them to direct the performance of Installation Manager tasks in silent mode.

For more information on using Installation Manager, read the IBM Installation Manager Information Center.

Packages and package groups: Each software product that can be installed with Installation Manager is referred to as a "package." An installed package has a product level and an installation location. A package group consists of all of the products that are installed at a single location.

Installation Manager modes: IBM Installation Manager can be installed in one of the following three modes:

- In admin mode, the Installation Manager is installed from an administrator or a root ID and can be invoked by any administrator or root user.
- In nonAdmin mode (also called "user mode"), the Installation Manager can be invoked only by the user that installed it.

- AIX HP-UX Linux Solaris In group mode, the Installation Manager can be invoked by any user ID that is connected to the default group of the user that installed it.

  This does not mean that two people can use the single instance of IBM Installation Manager at the same time.

How many Installation Managers do you need: You only need to run Installation Manager on those systems on which you install or update product code. You normally need only one Installation Manager on a system because one Installation Manager can keep track of any number of product installations.

Getting the Installation Manager installation kit: IBM Installation Manager comes in the form of an installation kit, which contains a set of Installation Manager binaries and a flat-file repository for the Installation Manager product. The installation kit is only used for setup and maintenance of the Installation Manager .

Installing Installation Manager: When the installation kit is available on your system, you can install Installation Manager. Installation Manager consists of a set of binaries that are copied from the installation kit and a set of runtime data that describe the products that have been installed by this particular Installation Manager. Before installing Installation Manager, you must decide in which mode the Installation Manager will run as well as where the binaries and runtime data—called "agent data" or "appdata"—will reside. Then, you issue the Installation Manager installc, userinstc, or groupinstc command from the appropriate user ID to install Installation Manager.

Accessing product repositories: All software materials that will be installed with IBM Installation Manager are stored in flat-file repositories. Each repository contains program objects and metadata for one or more packages—that is, software products at a particular level. Repositories can also contain product maintenance, such as fix packs and ifixes. Whenever you install a new product, you can choose from any of the available product levels in any accessible repository.

Installing the product: After you have installed Installation Manager and have access to all necessary product repositories, you can use Installation Manager command-line commands or response files to perform the actual product installations. When you install a product, you provide the package name, optionally the product level to be installed, the product location, and any other optional properties. For example, some products have optional features that you can select at installation time or a list of optional supported language packs from which you can select.

Working with installed products: You can use Installation Manager commands to list installed products and product levels. You can also obtain this information for installed copies of WebSphere Application Server Version 8 products by issuing the versionInfo command from the product file system. You can use Installation Manager commands or response files to install a new product level, roll back to a previous level, or modify the product by adding or removing optional features or language packs.

Restrictions:

- Do not use the same response files that are used with WebSphere Application Server Version 7.0 or earlier to install or uninstall Version 8.0 silently. Use response files that are based on Installation Manager to install, update, or uninstall Version 8.0 and later.
- Solaris The Installation Manager GUI is not supported on Solaris 10 x64 systems. Perform the following actions to install or uninstall the product on these systems:
  - Use the Installation Manager GUI on a supported system to record a response file that will allow you to install or uninstall WebSphere Application Server Version 8.0 silently.
  - Edit the recorded response file if necessary.
  - Use the response file to install or uninstall WebSphere Application Server Version 8.0 silently on your system.

- Linux For any Linux system that is enabled for Security Enhanced Linux (SELinux), such as Red Hat Enterprise Linux Version 5 or SUSE Linux Enterprise Server Version 11, you must identify the Java shared libraries in the Installation Manager installation image to the system. Also, you must identify the Java shared libraries in the Installation Manager installation after it has been installed. For example:

```
chcon -R -t texrel_shlib_t ${IM_Image}/jre_5.0.3.sr8a_20080811b/jre/bin
chcon -R -t texrel_shlib_t ${IM_Install_root}/eclipse/jre_5.0.3.sr8a_20080811b/jre/bin
```

- Windows If a non-administrator installs WebSphere Application Server Version 8 on a Windows Vista, Windows 7, or Windows Server 2008 operating system into the `Program Files` or `Program Files (x86)` directory with User Account Control (UAC) enabled, WebSphere Application Server will not function correctly.

  UAC is an access-control mechanism that allows non-administrative users to install a software product into the `Program Files` or `Program Files (x86)` directory; but it then prohibits any write access to that directory after the installation has completed. WebSphere Application Server requires write access in the *app_server_root* directory in order to function correctly.

  To resolve this issue, perform one of the following actions:

  – Install WAS into a directory other than `Program Files` or `Program Files (x86)`.

    For example:

```
C:\IBM\WebSphere\AppServer
```

  – Disable UAC.

- When you install WebSphere Application Server Version 8.0 using Installation Manager with local repositories, the installation takes a significantly longer amount of time if you use the `repository.zip` file directly without extracting it.

  Before you install WebSphere Application Server Version 8.0 using Installation Manager with local repositories, extract the `repository.zip` file to a location on your local system and add that location to your Installation Manager preferences.

- Installation Manager console mode, which is included in Installation Manager Version 1.4.3 and later, does not work with WebSphere Application Server Version 8.0 offerings.

Important: Do not transfer the content of a repository in non-binary mode and do not convert any content on extraction.

Note: In addition to the GUI and silent methods described in this information, you can also use Installation Manager to manage installation using the the Installation Manager imcl installation command. For information on using Installation Manager using this method, read the IBM Installation Manager Information Center.

About this task

Perform one of these procedures to install or uninstall the product using Installation Manager.

Procedure

- "Installing the product on distributed operating systems using the GUI" on page 78
- "Installing the product on distributed operating systems silently" on page 84
- "Uninstalling the product from distributed operating systems using the GUI" on page 104
- "Uninstalling the product from distributed operating systems silently" on page 105

Results

Notes on logging and tracing:

- An easy way to view the logs is to open Installation Manager and go to **File > View Log**. An individual log file can be opened by selecting it in the table and then clicking the **Open log file** icon.

- Logs are located in the `logs` directory of Installation Manager's application data location. For example:
  - Windows **Administrative installation:**

```
C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
```

  - Windows **Non-administrative installation:**

```
C:\Documents and Settings\user_name\Application Data\IBM\Installation Manager
```

  - AIX HP-UX Linux Solaris **Administrative installation:**

```
/var/IBM/InstallationManager
```

  - AIX HP-UX Linux Solaris **Non-administrative installation:**

```
user_home/var/ibm/InstallationManager
```

- The main log files are time-stamped XML files in the `logs` directory, and they can be viewed using any standard web browser.
- The `log.properties` file in the `logs` directory specifies the level of logging or tracing that Installation Manager uses. To turn on tracing for the WebSphere Application Server plug-ins, for example, create a `log.properties` file with the following content:

```
com.ibm.ws=DEBUG
com.ibm.cic.agent.core.Engine=DEBUG
global=DEBUG
```

  Restart Installation Manager as necessary, and Installation Manager outputs traces for the WebSphere Application Server plug-ins.

Notes on troubleshooting:

- HP-UX By default, some HP-UX systems are configured to not use DNS to resolve host names. This could result in Installation Manager not being able to connect to an external repository.

  You can ping the repository, but nslookup does not return anything.

  Work with your system administrator to configure your machine to use DNS, or use the IP address of the repository.
- In some cases, you might need to bypass existing checking mechanisms in Installation Manager.
  - On some network file systems, disk space might not be reported correctly at times; and you might need to bypass disk-space checking and proceed with your installation.

    To disable disk-space checking, specify the following system property in the `config.ini` file in *`IM_install_root`*`/eclipse/configuration` and restart Installation Manager:

```
cic.override.disk.space=sizeunit
```

    where *size* is a positive integer and *unit* is blank for bytes, k for kilo, m for megabytes, or g for gigabytes. For example:

```
cic.override.disk.space=120 (120 bytes)
cic.override.disk.space=130k (130 kilobytes)
cic.override.disk.space=140m (140 megabytes)
cic.override.disk.space=150g (150 gigabytes)
cic.override.disk.space=true
```

    Installation Manager will report a disk-space size of Long.MAX_VALUE. Instead of displaying a very large amount of available disk space, N/A is displayed.
  - To bypass operating-system prerequisite checking, add `disableOSPrereqChecking=true` to the `config.ini` file in *`IM_install_root`*`/eclipse/configuration` and restart Installation Manager.

  If you need to use any of these bypass methods, contact IBM Support for assistance in developing a solution that does not involve bypassing the Installation Manager checking mechanisms.
- Installation Manager might display a warning message during the uninstallation process.

  Uninstalling WebSphere Application Server Version 8.0 using Installation Manager requires that the data repositories remain valid and available.
- For more information on using Installation Manager, read the IBM Installation Manager Information Center.

Read the release notes to learn more about the latest version of Installation Manager. To access the release notes, complete the following task:

- Windows Click **Start > Programs > IBM Installation Manager > Release Notes**.
- AIX HP-UX Linux Solaris Go to the documentation subdirectory in the directory where Installation Manager is installed, and open the `readme.html` file.

Note on version and history information: The versionInfo and historyInfo commands return version and history information based on all of the installation, uninstallation, update, and rollback activities performed on the system.

trns: Beginning with WebSphere Application Server Version 8.0, you cannot use the installation registry utility (the installRegistryUtils command) to list installed products and packages. Use the Installation Manager imcl command to list installed products and packages for WebSphere Application Server Version 8.0 and later. See the IBM Installation Manager Information Center for information on using this command.

Installing the product on distributed operating systems using the GUI

You can use the Installation Manager GUI to install WebSphere Application Server Version 8.0.

Before you begin

Install Installation Manager:

1. Perform one of the following procedures:
   - If you want to use the Installation Manager that is included with this product, perform the following actions:
     a. Obtain the necessary files from the physical media or the web.

        There are three basic options for obtaining and installing Installation Manager and the product.

        - **Access the physical media, and use local installation**

          You can access Installation Manager and the product repositories on the product media. You can install Installation Manager on your system and use it to install the product from the product repositories on the media.
        - **Download the files from the IBM Passport Advantage site, and use local installation**

          Licensed customers can download Installation Manager as well as the necessary product repositories from the Passport Advantage site. You can then install Installation Manager on your system and use it to install the product from the repositories.
        - **Download a file from the Installation Manager website, and use web-based installation**

          You can download and unpack a compressed file containing Installation Manager from the IBM Installation Manager website. You can then install Installation Manager on your local system and use it to install the product from the web-based repository located at

```
http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v80
```

Tip: This live repository is accessed by using Passport Advantage authentication. After you have installed Installation Manager, you can set the Passport Advantage preference to connect to the live repositories. To set Passport Advantage preferences, follow this procedure:

1) Open Installation Manager.
2) Open the Passport Advantage preferences page by selecting **File > Preferences > Passport Advantage**.
3) Select **Connect to Passport Advantage** to connect to the Passport Advantage repository.

   The Password Required dialog box opens.

4) Enter a user name and password for Passport Advantage.

5) **Optional:** Select **Save password** to save the user name and password credentials.

   If you do not save the user name and password credentials, you are prompted for these credentials each time you access Passport Advantage.

6) Click **OK** to close the Password Required dialog box.

7) Click **OK** to close the Preferences window.

For more information on setting your Installation Manager preferences, see the IBM Installation Manager Information Center.

b. Change to the location containing the Installation Manager installation files, and run one of the following commands:

Administrative installation:

- Windows `install.exe`
- AIX HP-UX Linux Solaris `./install`

Non-administrative installation:

- Windows `userinst.exe`
- AIX HP-UX Linux Solaris `./userinst`

Group-mode installation:

AIX HP-UX Linux Solaris `./groupinst`

Notes on group mode:

- Group mode allows multiple users to use a single instance of IBM Installation Manager to manage software packages.

  This does not mean that two people can use the single instance of IBM Installation Manager at the same time.
- Windows Group mode is not available on Windows operating systems.
- If you do not install Installation Manager using group mode, you will not be able to use group mode to manage any of the products that you install later using this Installation Manager.
- Make sure that you change the installation location from the default location in the current user's home directory to a location that is accessible by all users in the group.
- Set up your groups, permissions, and environment variables as described in the Group mode road maps in the IBM Installation Manager Information Center before installing in group mode.
- For more information on using group mode, read the Group mode road maps in the IBM Installation Manager Information Center.

The installer opens an **Install Packages** window.

c. Make sure that the Installation Manager package is selected, and click **Next**.

d. Accept the terms in the license agreements, and click **Next**.

   The program creates the directory for your installation.

e. Click **Next**.

   f. Review the summary information, and click **Install**.
      - If the installation is successful, the program displays a message indicating that installation is successful.
      - If the installation is not successful, click **View Log File** to troubleshoot the problem.
- If you already have a version of Installation Manager installed on your system and you want to use it to install and maintain the product, obtain the necessary product files from the physical media or the web.

  There are three basic options for installing the product.

  - **Access the physical media, and use local installation**

    You can access the product repositories on the product media. Use your existing Installation Manager to install the product from the product repositories on the media.
  - **Download the files from the Passport Advantage site, and use local installation**

    Licensed customers can download the necessary product repositories from the Passport Advantage site. You can then use your existing Installation Manager to install the product from the repositories.
  - **Access the live repositories, and use web-based installation**

    You can install Installation Manager on your local system and use it to install the product from the web-based repository located at

```
http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v80
```

    Tip: This live repository is accessed by using Passport Advantage authentication. After you have installed Installation Manager, you can set the Passport Advantage preference to connect to the live repositories. To set Passport Advantage preferences, follow this procedure:

    a. Open Installation Manager.

    b. Open the Passport Advantage preferences page by selecting **File > Preferences > Passport Advantage**.

    c. Select **Connect to Passport Advantage** to connect to the Passport Advantage repository.

       The Password Required dialog box opens.

    d. Enter a user name and password for Passport Advantage.

    e. **Optional:** Select **Save password** to save the user name and password credentials.

       If you do not save the user name and password credentials, you are prompted for these credentials each time you access Passport Advantage.

    f. Click **OK** to close the Password Required dialog box.

    g. Click **OK** to close the Preferences window.

    For more information on setting your Installation Manager preferences, see the IBM Installation Manager Information Center.

2. Add the product repository to your Installation Manager preferences.

   a. Start Installation Manager.

   b. In the top menu, click **File > Preferences**.

   c. Select **Repositories**.

   d. Perform the following actions:

      1) Click **Add Repository**.

      2) Enter the path to the `repository.config` file in the location containing the repository files.

         For example:

         - Windows `C:\repositories\`*`product_name`*`\local-repositories`
         - AIX HP-UX Linux Solaris `/var/repositories/`*`product_name`*`/local-repositories`

or

http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v80

3) Click **OK**.

e. Deselect any locations listed in the Repositories window that you will not be using.

f. Click **Apply**.

g. Click **OK**.

h. Click **File > Exit** to close Installation Manager.

About this task

Tip: By default, Installation Manager saves earlier versions of a package to roll back to if you experience issues later. When Installation Manager rolls back a package to a previous version, the current version of the files are uninstalled and the earlier versions are reinstalled. If you choose not to save the files for rollback, you can prevent the files from being saved or delete them after they are saved. To set your rollback preferences, perform the following actions before installing a package:

1. Launch Installation Manager.
2. Open the Rollback preferences window by selecting **File > Preferences > Files for Rollback**.
3. Select or clear the **Save files for rollback** option to save or to stop saving a copy of files that are required to roll back packages on your computer.

   You can remove any files that have already been saved by clicking **Delete Saved Files**. If you delete the files and you need to roll back a package later, you must connect to a repository or insert the media to obtain the required files for the previous version of the package.
4. Click **OK** to save your rollback preferences.

For more information on setting your Installation Manager preferences, see the IBM Installation Manager Information Center.

Perform this procedure to use the Installation Manager GUI to install the product.

Procedure

1. Start Installation Manager.

   Tip: AIX HP-UX Linux Solaris You can start Installation Manager in group mode with the ./IBMIM command.
   - Group mode allows multiple users to use a single instance of IBM Installation Manager to manage software packages.
   - For more information on using group mode, read the Group mode road maps in the IBM Installation Manager Information Center.
2. Click **Install**.

   Note: If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.

   Installation Manager searches its defined repositories for available packages.
3. Perform the following actions.

   a. Select **IBM WebSphere Application Server Network Deployment** and the appropriate version.

   Note: If you are installing the trial version of this product, select **IBM WebSphere Application Server Network Deployment (Trial Version)**.

   If you already have the product installed on a WebSphere Application Server installation on your system, a message displays indicating that the product is already installed. To create another installation of the product in another location, click **Continue**.

   b. Click **Next**.

Note: If you try to install a newer level of the product with a previous version of Installation Manager, Installation Manager might prompt you to update to the latest level of Installation Manager when it connects to the repository. Update to the newer version before you continue if you are prompted to do so. Read the IBM Installation Manager Information Center for information about automatic updates.

4. Accept the terms in the license agreements, and click **Next**.
5. Specify the installation root directory for the product binaries, which are also referred to as the core product files or system files.

   The panel also displays the shared resources directory and disk-space information.

   Note: The first time that you install a package using Installation Manager, specify the shared resources directory. The shared resources directory is where installation artifacts are located that can be used by one or more package groups. Use your largest drive for this installation. You cannot change the directory location until after you uninstall all packages.

   Restrictions:

   - Deleting the default target location and leaving an installation-directory field empty prevents you from continuing.
   - Do not use symbolic links as the destination directory.

     Symbolic links are not supported.
   - Do not use a semicolon in the directory name.

     WebSphere Application Server cannot install properly if the target directory includes a semicolon.

     Windows A semicolon is the character used to construct the class path on Windows systems.
   - Windows The maximum path length on the Windows Server 2008, Windows Vista, and Windows 7 operating systems is 60 characters.
6. Click **Next**.
7. Select the languages for which translated content should be installed.

   English is always selected.
8. Click **Next**.
9. Select the features that you want to install.

   Choose from the following features:

   - EJBDeploy tool for pre-EJB 3.0 modules

     This option installs the EJBDeploy tool for pre-EJB 3.0 modules.

     trns: The EJBDeploy tool was installed automatically with the product in WebSphere Application Server Version 7 and earlier. It is now an optional feature.

     Before you deploy applications on the server, you must run the EJBDeploy tool on applications that contain EJB modules that are based on specifications prior to EJB 3.0. Running the EJBDeploy tool generates deployment code for enterprise beans in the application. Beginning with the EJB 3.0 specification, the EJBDeploy tool is no longer required because WebSphere Application Server uses a new feature called "JITDeploy", which automatically generates code when the application starts.

     Tip: You can run the Installation Manager later to modify this installation and add or remove this feature.
   - Standalone thin clients, resource adapters, and embeddable containers

     IBM thin clients and resource adapters provide a set of clients and resource adapters for a variety of technologies, such as JAX-WS, JAX-RPC, JAX-RS, XML, EJB, JPA, JMS, and more. An embeddable container runs in a standalone Java Platform, Standard Edition environment. For example, you can use the embeddable EJB container to run enterprise beans outside the application server.

- Standalone thin clients and resource adapters

  This option installs the IBM standalone thin clients and resource adapters.

  IBM thin clients provide a set of clients for a variety of technologies, such as JAX-WS, JAX-RPC, JAX-RS, XML, EJB, JPA, JMS, and more. IBM resource adapters provide the resource adapters for JMS.
- Embeddable EJB container

  This option installs the embeddable EJB container.

  The embeddable EJB container is a Java Archive (JAR) file that you can use to run enterprise beans in a standalone Java Platform, Standard Edition environment. You can run enterprise beans using this embeddable container outside the application server. The embeddable EJB container is a part of the EJB 3.1 specification and is primarily used for unit testing enterprise beans business logic.

Tip: You can run the Installation Manager later to modify this installation and add or remove these features.

- Sample applications

  This option installs the sample applications for learning and demonstration environments.

  The samples include both source code files and integrated enterprise applications that demonstrate some of the latest Java (TM) Platform, Enterprise Edition (Java EE) and WebSphere technologies. The samples are recommended for installation to learning and demonstration environments, such as development environments. However, they are not recommended for installation to production application server environments.

  Tip: You can run the Installation Manager later to modify this installation and add or remove this feature.
- AIX Linux Solaris Windows IBM Software Development Kit

  This option allows you to choose between a 32-bit and 64-bit Software Development Kit.

  Notes:
  - This option displays only if you are installing on a 64-bit system.
  - This does not apply to Solaris x86 64-bit systems.
  - You must select one of the two options.
  - You cannot modify this installation later and change this selection.

10. Click **Next**.
11. Review the summary information, and click **Install**.
    - If the installation is successful, the program displays a message indicating that installation is successful.

      Note: The program might also display important post-installation instructions as well.
    - If the installation is not successful, click **View Log File** to troubleshoot the problem.
12. Select which tool you want to start when this installation is finished.
    - Select **Profile Management Tool to create a profile** if you want to open the full Profile Management Tool and create a new profile when this installation is finished.
    - Select **Profile Management Tool to create an application server profile for a development environment** if you want to create an application server profile with settings appropriate for a development environment when this installation is finished.

Note: The development settings are appropriate for a development environment where frequent application updates are performed and system resources are at a minimum. Do not use the development settings for production servers.

- Select **None** if you do not want to create a new profile when this installation is finished.

Restriction: The option to launch the Profile Management Tool is only available when a version of WebSphere Application Server containing the Profile Management Tool is installed.

13. Click **Finish**.
14. Click **File > Exit** to close Installation Manager.

What to do next

You can create a standalone application server profile, management profile, managed (custom) profile, cell profile, or secure proxy profile using the Profile Management Tool or the manageprofiles command.

Tip: Installation Manager optionally can search for updates to itself whenever the Install Packages, Modify Packages, or Update Packages page is opened from the Start page as well as when clicking **Check for Other Versions and Extensions** on the Install Packages page. To enable this option, perform the following actions:

1. Start Installation Manager.
2. In the top menu, click **File > Preferences**.
3. Select **Updates**.
4. Select **Search for Installation Manager updates**.
5. Click **Apply**.
6. Click **OK**.

Do not enable this option if you do not have access to the service repository.

Installing the product on distributed operating systems silently

You can use Installation Manager to install WebSphere Application Server Version 8.0 silently.

Before you begin

Install Installation Manager on each of the systems onto which you want to install the product.

1. Perform one of the following procedures:
   - If you want to use the Installation Manager that is included with this product, perform the following actions:
     a. Obtain the necessary files from the physical media or the web.

        There are three basic options for obtaining and installing Installation Manager and the product.

        – **Access the physical media, and use local installation**

          You can access Installation Manager and the product repositories on the product media. You can install Installation Manager on your system and use it to install the product from the product repositories on the media.

        – **Download the files from the Passport Advantage site, and use local installation**

          Licensed customers can download Installation Manager as well as the necessary product repositories from the Passport Advantage site. You can then install Installation Manager on your system and use it to install the product from the repositories.

        – **Download a file from the Installation Manager website, and use web-based installation**

          You can download and unpack a compressed file containing Installation Manager from the IBM Installation Manager website. You can then install Installation Manager on your local system and use it to install the product from the web-based repository located at http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v80

b. Change to the location containing the Installation Manager installation files, and run one of the following commands to install Installation Manager silently:

   Administrative installation:

   - Windows `installc.exe -acceptLicense -log` *`log_file_path_and_name`*
   - AIX HP-UX Linux Solaris `./installc -acceptLicense -log` *`log_file_path_and_name`*

   Non-administrative installation:

   - Windows `userinstc.exe -acceptLicense -log` *`log_file_path_and_name`*
   - AIX HP-UX Linux Solaris `./userinstc -acceptLicense -log` *`log_file_path_and_name`*

   Group-mode installation:

   AIX HP-UX Linux Solaris `./groupinstc -acceptLicense -dataLocation` *`application_data_location`* `-log` *`log_file_path_and_name`*

   Notes on group mode:

   - Group mode allows multiple users to use a single instance of IBM Installation Manager to manage software packages.

     This does not mean that two people can use the single instance of IBM Installation Manager at the same time.
   - Windows Group mode is not available on Windows operating systems.
   - If you do not install Installation Manager using group mode, you will not be able to use group mode to manage any of the products that you install later using this Installation Manager.
   - Make sure that you change the installation location from the default location in the current user's home directory to a location that is accessible by all users in the group.
   - Set up your groups, permissions, and environment variables as described in the Group mode road maps in the IBM Installation Manager Information Center before installing in group mode.
   - For more information on using group mode, read the Group mode road maps in the IBM Installation Manager Information Center.

- If you already have a version of Installation Manager installed on your system and you want to use it to install and maintain the product, obtain the necessary product files from the physical media or the web.

  There are three basic options for installing the product.

  - **Access the physical media, and use local installation**

    You can access the product repositories on the product media. Use your existing Installation Manager to install the product from the product repositories on the media.
  - **Download the files from the Passport Advantage site, and use local installation**

    Licensed customers can download the necessary product repositories from the Passport Advantage site. You can then use your existing Installation Manager to install the product from the repositories.
  - **Access the live repositories, and use web-based installation**

    You can install Installation Manager on your local system and use it to install the product from the web-based repository located at

```
http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v80
```

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

2. Add the product repository to your Installation Manager preferences.
   a. Start Installation Manager.
   b. In the top menu, click **File > Preferences**.
   c. Select **Repositories**.
   d. Perform the following actions:
      1) Click **Add Repository**.
      2) Enter the path to the `repository.config` file in the location containing the repository files.

         For example:

         - Windows `C:\repositories\`*`product_name`*`\local-repositories`
         - AIX HP-UX Linux Solaris `/var/repositories/`*`product_name`*`/local-repositories`

         or

```
http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v80
```

      3) Click **OK**.
   e. Deselect any locations listed in the Repositories window that you will not be using.
   f. Click **Apply**.
   g. Click **OK**.
   h. Click **File > Exit** to close Installation Manager.

About this task

Using Installation Manager, you can work with response files to install the product silently in a variety of ways. You can record a response file using the GUI as described in the following procedure, or you can generate a new response file by hand or by taking an example and modifying it.

Procedure

1. Optional: **Record a response file to install the product:** On one of your systems, perform the following actions to record a response file that will install the product.
   a. From a command line, change to the eclipse subdirectory in the directory where you installed Installation Manager.
   b. Start Installation Manager from the command line using the -record option.

      For example:

      - Windows **Administrator or non-administrator:**

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"
  -record C:\temp\install_response_file.xml
```

      - AIX HP-UX Linux Solaris **Administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry
  -record /var/temp/install_response_file.xml
```

      - AIX HP-UX Linux Solaris **Non-administrator:**

```
./IBMIM -skipInstall user_home/var/temp/imRegistry
  -record user_home/var/temp/install_response_file.xml
```

      Tip: When you record a new response file, you can specify the -skipInstall parameter. Using this parameter has the following benefits:

      - No files are actually installed, and this speeds up the recording.
      - If you use a temporary data location with the -skipInstall parameter, Installation Manager writes the installation registry to the specified data location while recording. When you start

Installation Manager again without the -skipInstall parameter, you then can use your response file to install against the real installation registry.

The -skipInstall operation should not be used on the actual agent data location used by Installation Manager. This is unsupported. Use a clean writable location, and re-use that location for future recording sessions.

For more information, read the IBM Installation Manager Information Center.

c. Add the appropriate repositories to your Installation Manager preferences.
   1) In the top menu, click **File > Preferences**.
   2) Select **Repositories**.
   3) Perform the following actions for each repository:
      a) Click **Add Repository**.
      b) Enter the path to the `repository.config` file in the remote web-based repository or the local directory into which you unpacked the repository files.

         For example:

         - Remote repositories:

```
https://downloads.mycorp.com:8080/WAS_80_repository
```

         or

```
http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v80
```

         - Local repositories:
           - Windows `C:\repositories\was80\local-repositories`
           - AIX HP-UX Linux Solaris `/var/repositories/was80/local-repositories`

      c) Click **OK**.
   4) Click **Apply**.
   5) Click **OK**.

d. Click **Install**.

   Note: If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.

   Installation Manager searches its defined repositories for available packages.

e. Perform the following actions.
   1) Select **IBM WebSphere Application Server Network Deployment** and the appropriate version.

      Note: If you are installing the trial version of this product, select **IBM WebSphere Application Server Network Deployment (Trial Version)**.

      If you already have the product installed on a WebSphere Application Server installation on your system, a message displays indicating that the product is already installed. To create another installation of the product in another location, click **Continue**.
   2) Click **Next**.

f. Accept the terms in the license agreements, and click **Next**.

g. Specify the installation root directory for the product binaries, which are also referred to as the core product files or system files.

   The panel also displays the shared resources directory and disk-space information.

   Note: The first time that you install a package using Installation Manager, specify the shared resources directory. The shared resources directory is where installation artifacts are located that can be used by one or more package groups. Use your largest drive for this installation. You cannot change the directory location until after you uninstall all packages.

Restrictions:

- Deleting the default target location and leaving an installation-directory field empty prevents you from continuing.
- Do not use symbolic links as the destination directory.

  Symbolic links are not supported.
- Do not use a semicolon in the directory name.

  WebSphere Application Server cannot install properly if the target directory includes a semicolon.

  Windows A semicolon is the character used to construct the class path on Windows systems.
- Windows The maximum path length on the Windows Server 2008, Windows Vista, and Windows 7 operating systems is 60 characters.

h. Click **Next**.

i. Select the languages for which translated content should be installed.

English is always selected.

j. Click **Next**.

k. Select the features that you want to install.

Choose from the following features:

- EJBDeploy tool for pre-EJB 3.0 modules

  This option installs the EJBDeploy tool for pre-EJB 3.0 modules.

  trns: The EJBDeploy tool was installed automatically with the product in WebSphere Application Server Version 7 and earlier. It is now an optional feature.

  Before you deploy applications on the server, you must run the EJBDeploy tool on applications that contain EJB modules that are based on specifications prior to EJB 3.0. Running the EJBDeploy tool generates deployment code for enterprise beans in the application. Beginning with the EJB 3.0 specification, the EJBDeploy tool is no longer required because WebSphere Application Server uses a new feature called "JITDeploy", which automatically generates code when the application starts.

  Tip: You can run the Installation Manager later to modify this installation and add or remove this feature.
- Standalone thin clients, resource adapters, and embeddable containers

  IBM thin clients and resource adapters provide a set of clients and resource adapters for a variety of technologies, such as JAX-WS, JAX-RPC, JAX-RS, XML, EJB, JPA, JMS, and more. An embeddable container runs in a standalone Java Platform, Standard Edition environment. For example, you can use the embeddable EJB container to run enterprise beans outside the application server.

  – Standalone thin clients and resource adapters

    This option installs the IBM standalone thin clients and resource adapters.

    IBM thin clients provide a set of clients for a variety of technologies, such as JAX-WS, JAX-RPC, JAX-RS, XML, EJB, JPA, JMS, and more. IBM resource adapters provide the resource adapters for JMS.

  – Embeddable EJB container

    This option installs the embeddable EJB container.

    The embeddable EJB container is a Java Archive (JAR) file that you can use to run enterprise beans in a standalone Java Platform, Standard Edition environment. You can run enterprise beans using this embeddable container outside the application server. The embeddable EJB container is a part of the EJB 3.1 specification and is primarily used for unit testing enterprise beans business logic.

Tip: You can run the Installation Manager later to modify this installation and add or remove these features.

- Sample applications

  This option installs the sample applications for learning and demonstration environments.

  The samples include both source code files and integrated enterprise applications that demonstrate some of the latest Java (TM) Platform, Enterprise Edition (Java EE) and WebSphere technologies. The samples are recommended for installation to learning and demonstration environments, such as development environments. However, they are not recommended for installation to production application server environments.

  Tip: You can run the Installation Manager later to modify this installation and add or remove this feature.

- AIX Linux Solaris Windows IBM Software Development Kit

  This option allows you to choose between a 32-bit and 64-bit Software Development Kit.

  Notes:

  – This option displays only if you are installing on a 64-bit system.

  – This does not apply to Solaris x86 64-bit systems.

  – You must select one of the two options.

  – You cannot modify this installation later and change this selection.

l. Click **Next**.

m. Review the summary information, and click **Install**.

- If the installation is successful, the program displays a message indicating that installation is successful.

  Note: The program might also display important post-installation instructions as well.

- If the installation is not successful, click **View Log File** to troubleshoot the problem.

n. Click **Finish**.

o. Click **File > Exit** to close Installation Manager.

p. Optional: If you are using an authenticated remote repository, create a keyring file for silent installation.

Note: In a keyring file, you can store credentials for URLs that require authentication, such as your remote repositories.

1) From a command line, change to the eclipse subdirectory in the directory where you installed Installation Manager.

2) Start Installation Manager from the command line using the -record option.

   For example:

   - Windows **Administrator or non-administrator:**

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"
  -keyring C:\IM\im.keyring
  -record C:\temp\keyring_response_file.xml
```

   - AIX HP-UX Linux Solaris **Administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry
  -keyring /var/IM/im.keyring
  -record /var/temp/keyring_response_file.xml
```

   - AIX HP-UX Linux Solaris **Non-administrator:**

```
./IBMIM -skipInstall user_home/var/temp/imRegistry
  -keyring user_home/var/IM/im.keyring
  -record user_home/var/temp/keyring_response_file.xml
```

3) When a window opens that requests your credentials for the authenticated remote repository, enter the correct credentials and **save** them.

4) Click **File > Exit** to close Installation Manager.

For more information, read the IBM Installation Manager Information Center.

2. **Use the response files to install the product silently:**

a. Optional: **Use the response file to install the keyring file silently:** Go to a command line on each of the systems on which you want to install the product, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and install the keyring file silently.

For example:

- Windows **Administrator or non-administrator:**

```
imcl.exe -acceptLicense
  input C:\temp\keyring_response_file.xml
  -log C:\temp\keyring_log.xml
```

- AIX HP-UX Linux Solaris **Administrator:**

```
./imcl -acceptLicense
  input /var/temp/keyring_response_file.xml
  -log /var/temp/keyring_log.xml
```

- AIX HP-UX Linux Solaris **Non-administrator:**

```
./imcl -acceptLicense
  input user_home/var/temp/keyring_response_file.xml
  -log user_home/var/temp/keyring_log.xml
```

For more information on keyring files, read the IBM Installation Manager Information Center.

b. **Use the response file to install the product silently:** Go to a command line on each of the systems on which you want to install the product, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and install the product silently.

For example:

- Windows **Administrator or non-administrator:**

```
imcl.exe -acceptLicense
  input C:\temp\install_response_file.xml
  -log C:\temp\install_log.xml
  -keyring C:\IM\im.keyring
```

- AIX HP-UX Linux Solaris **Administrator:**

```
./imcl -acceptLicense
  input /var/temp/install_response_file.xml
  -log /var/temp/install_log.xml
  -keyring /var/IM/im.keyring
```

- AIX HP-UX Linux Solaris **Non-administrator:**

```
./imcl -acceptLicense
  input user_home/var/temp/install_response_file.xml
  -log user_home/var/temp/install_log.xml
  -keyring user_home/var/IM/im.keyring
```

Notes:

- The relevant terms and conditions, notices, and other information are provided in the license-agreement files in the `lafiles` or *`product_name`*`/lafiles` subdirectory of the installation image or repository for this product.
- The program might write important post-installation instructions to standard output.

Read the IBM Installation Manager Information Center for more information.

Example

Windows The following is an example of a response file for silently installing the product.

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright ######################################################
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2011.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
######################################################################## -->

<!-- ##### Frequently Asked Questions ####################################
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
#     Installation Manager Information Center can be found at:
#     http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
#   Windows = IBMIM.exe -record c:\temp\responsefiles\WASv8.install.Win32.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#   Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv8.install.RHEL64.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse\tools subdirectory in the directory where you installed
# Installation Manager:
#
#   Windows = imcl.exe -acceptLicense -showProgress
#     input <response_file_path_and_name> -log <log_file_path_and_name>
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
#   Windows = imcl.exe -acceptLicense -showProgress
#     input c:\temp\responsefile\WASv8.install.Win32.xml
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input /home/user/responsefile/WASv8.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
#     license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help:  IBMIM -help
#
# Question 3. How do I store and pass credentials to repositories that
# require authentication?
# Answer 3. Installation Manager uses a key ring file to store encrypted
# credentials for authenticating with repositories. Follow this two-step
# process for creating and using a key ring file with Installation Manager.
#
# First, create a key ring file with your credentials by starting
# Installation Manager from the command line under eclipse subdirectory
# with the keyring parameter.
# Use the optional password parameter to password protect your file.
#
#   Windows = IBMIM.exe -keyring <path and file name> -password <password>
#   Linux, UNIX, IBM i and z/OS = ./IBMIM -keyring <path and file name>
#                                 -password <password>
#
# Installation Manager will start in graphical mode. Verify that the
# repositories to which you need to authenticate are included in the
# preferences, File / Preferences / Repositories. If they are not
# listed, then click Add Repositories to add the URL or UNC path.
# Installation Manager will prompt for your credentials. If the repository
# is already in the list, then any attempt to access the repository location,
# such as clicking the Test Connections button, will also prompt for your
# credentials. Enter the correct credential and check the Save password
# checkbox. The credentials are saved to the key ring file you specified.
#
# Second, when you start a silent installation, run imcl under eclipse/tools
# subdirectory, and provide Installation Manager with the location of the key
# ring file and the password if the file is protected. For example:
#
#   Windows = imcl.exe -acceptLicense -showProgress
#     input <path and file name of response file>
#     -keyring <path and name of key ring file> -password <password>
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input <path and file name of response file>
#     -keyring <path and name of key ring file> -password <password>
#
######################################################################## -->

<!-- ##### Agent Input ###############################################
#
# Note that the "acceptLicense" attribute has been deprecated.
# Use "-acceptLicense" command line option to accept license agreements.
```

```
#
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the installation finishes.
#
# Valid values for clean:
#      true = only use the repositories and other preferences that are
#           specified in the response file.
#      false = use the repositories and other preferences that are
#           specified in the response file and Installation Manager.
#
# Valid values for temporary:
#      true = repositories and other preferences specified in the
#           response file do not persist in Installation Manager.
#      false = repositories and other preferences specified in the
#           response file persist in Installation Manager.
#
####################################################################### -->

<agent-input clean="true" temporary="true">

<!-- ##### Repositories ###################################################
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#
####################################################################### -->

<server>
    <!-- ##### IBM WebSphere Live Update Repositories ####################
     # These repositories contain WebSphere Application Server offerings,
     # and updates for those offerings
     #
     # To use the secure repository (https), you must have an IBM ID,
     # which can be obtained by registering at: http://www.ibm.com/account
     # or your Passport Advantage account.
     #
     # And, you must use a key ring file with your response file.
     ################################################################## -->
    <repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v80" />
    <!-- <repository location="https://www.ibm.com/software/rational/repositorymanager/repositories/websphere" /> -->

    <!-- ##### Custom Repositories ######################################
     # Uncomment and update the repository location key below
     # to specify URLs or UNC paths to any intranet repositories
     # and directory paths to local repositories to use.
     ################################################################## -->
    <!-- <repository location='https:\\w3.mycompany.com\repositories\'/> -->
    <!-- <repository location='/home/user/repositories/websphere/'/> -->

    <!-- ##### Local Repositories #######################################
     # Uncomment and update the following line when using a local
     # repository located on your own machine to install a
     # WebSphere Application Server offering.
     ############################################################# -->
    <!-- <repository location='insert the full directory path inside single quotes'/> -->
</server>

<!-- ##### Install Packages ###############################################
#
# Install Command
#
# Use the install command to inform Installation Manager of the
# installation packages to install.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
#    false = indicates not to modify an existing install by adding
#            or removing features.
#    true = indicates to modify an existing install by adding or
#           removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be installed. The offering listed must be present in
# at least one of the repositories listed earlier. The example
# command below contains the offering ID for the Network Deployment
# edition of WebSphere Application Server.
#
# The version attribute is optional. If a version number is provided,
# then the offering will be installed at the version level specified
# as long as it is available in the repositories. If the version
# attribute is not provided, then the default behavior is to install
# the latest version available in the repositories. The version number
# can be found in the repository.xml file in the repositories.
# For example, <offering ... version='8.0.0.20110617_2222'>.
#
# The profile attribute is required and typically is unique to the
# offering. If modifying or updating an existing installation, the
# profile attribute must match the profile ID of the targeted installation
# of WebSphere Application Server.
#
# The features attribute is optional. Offerings always have at least
# one feature; a required core feature which is installed regardless
# of whether it is explicitly specified. If other feature names
# are provided, then only those features will be installed.
# Features must be comma delimited without spaces.
#
# The feature values for WebSphere Application Server include:
#  ejbdeploy,thinclient,embeddablecontainer,samples,
#  com.ibm.sdk.6_32bit,com.ibm.sdk.6_64bit
#
# On 32-bit machines, the 32-bit sdk feature will be install
# automatically even if it is not specified in the response file.
#
# On 64-bit machines, one and only one of the Software Development
# Kit features (SDK) must be specified.
#
# The installFixes attribute indicates whether fixes available in
# repositories are installed with the product. By default, all
# available fixes will be installed with the offering.
#
# Valid values for installFixes:
#      none = do not install available fixes with the offering.
#      recommended = installs all available recommended fixes with the offering.
#      all = installs all available fixes with the offering.
#
# Interim fixes for offerings also can be installed while they
# are being installed by including the offering ID for the interim
# fix and specifying the profile ID. A commented out example is
# provided in the install command below.
#
# Installation Manager supports installing multiple offerings at once.
# Additional offerings can be included in the install command,
# with each offering requiring its own offering ID, version, profile value,
# and feature values.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# The eclipseLocation data key should use the same directory path to
# WebSphere Application Server as the installationLocation attribute.
#
# Include data keys for product specific profile properties.
# For instance, additional translations can be specified by including
# the cic.selector.nl data key and the language codes as values for
# the translations to install.
#
#  Language code values: cs,de,en,es,fr,hu,it,ja,ko,pl,pt_BR,ro,ru,zh,zh_HK,zh_TW
#
###################################################################### -->

<install modify='false'>
<offering id='com.ibm.websphere.ND.v80'
 profile='IBM WebSphere Application Server Network Deployment V8.0'
 features='core.feature,ejbdeploy,thinclient,embeddablecontainer,com.ibm.sdk.6_32bit' installFixes='none'/>
<!-- <offering id='PM12345_WAS80' profile='IBM WebSphere Application Server Network Deployment V8.0'/> -->
</install>

<profile id='IBM WebSphere Application Server Network Deployment V8.0'
 installLocation='C:\Program Files\IBM\WebSphere\AppServer'>
<data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.nl' value='en'/>
</profile>

<!-- ##### Shared Data Location ##########################################
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared'/>
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
#     true = store downloaded artifacts in the shared data location
#     false = remove downloaded artifacts from the shared data location
#
###################################################################### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
-->


<!-- ##### Preferences Settings ###########################################
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
###################################################################### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
 -->

</agent-input>
```

Important: AIX Linux Solaris Windows If you are installing on a 64-bit system, you must include one of the options for an IBM Software Development Kit.

- If you want to use the 32-bit IBM Software Development Kit, include `com.ibm.sdk.6_32bit` as a feature in the response file.

  For example:

```
<offering profile='IBM WebSphere Application Server Network Deployment V8.0'
    features='core.feature,com.ibm.sdk.6_32bit' id='com.ibm.websphere.ND.v80'/>
```

- If you want to use the 64-bit IBM Software Development Kit, include `com.ibm.sdk.6_64bit` as a feature in the response file.

  For example:

```
<offering profile='IBM WebSphere Application Server Network Deployment V8.0'
    features='core.feature,com.ibm.sdk.6_64bit' id='com.ibm.websphere.ND.v80'/>
```

Follow these guidelines:

- Include this feature only if you are installing on a 64-bit system; do not include it if you are installing on a 32-bit system.
- This does not apply to Solaris x86 64-bit systems.
- You must include one of the two options if you are installing on a 64-bit system.
- You cannot modify this installation later and change the selection.

Tip: To disable remote searches for updates in the response file, set the following preferences to false:

- offering.service.repositories.areUsed

  Used for searching remote repositories for updates to installed offerings
- com.ibm.cic.common.core.preferences.searchForUpdates

  Used for searching for updates to Installation Manager

For example:

```
<preference value='false' name='offering.service.repositories.areUsed'/>
<preference value='false' name='com.ibm.cic.common.core.preferences.searchForUpdates'/>
```

You can find more details on silent preference keys in the IBM Installation Manager Information Center.

Here are some examples of changes that you could make to manipulate this response file to perform alternative actions.

- To install multiple copies of this product, specify a different installation location and a new package group for each installation. For example, to install a second copy of the product into the `C:\Program Files\IBM\WebSphere\AppServer_2` directory and create the `IBM WebSphere Application Server Network Deployment V8.0_2` package group:
  1. Replace

```
<profile id='IBM WebSphere Application Server Network Deployment V8.0'
  installLocation='C:\Program Files\IBM\WebSphere\AppServer'>
```

  with

```
<profile id='IBM WebSphere Application Server Network Deployment V8.0_2
  installLocation='C:\Program Files\IBM\WebSphere\AppServer_2
```

  2. Replace

```
<data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\AppServer'/>
```

  with

```
<data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\AppServer_2'/>
```

  3. Replace

```
<offering id='com.ibm.websphere.ND.v80'
  profile='IBM WebSphere Application Server Network Deployment V8.0'
  features='core.feature,com.ibm.sdk.6_32bit,ejbdeploy,thinclient,embeddablecontainer' installFixes='none'/>
```

  with

```
<offering id='com.ibm.websphere.ND.v80'
  profile='IBM WebSphere Application Server Network Deployment V8.0_2'
  features='core.feature,com.ibm.sdk.6_32bit,ejbdeploy,thinclient,embeddablecontainer' installFixes='none'/>
```

- To add the optional features, add each desired feature in the offering as an entry in a comma-separated list. For example, to install all of the optional features (except for the optional IBM Software Development Kit on 64-bit systems):

Replace

```
<offering id='com.ibm.websphere.ND.v80'
  profile='IBM WebSphere Application Server Network Deployment V8.0'
  features='core.feature' installFixes='none'/>
```

with

```
<offering id='com.ibm.websphere.ND.v80'
  profile='IBM WebSphere Application Server Network Deployment V8.0'
  features='core.feature,samples,ejbdeploy,thinclient,embeddablecontainer' installFixes='none'/>
```

where `samples` indicates the sample applications feature, `thinclient` indicates the standalone thin clients and resource adapters, `embeddablecontainer` indicates the embeddable EJB container, and `ejbdeploy` indicates the EJBDeploy tool for pre-EJB 3.0 modules.

- Installation Manager can save earlier versions of a package to roll back to if you experience issues later. When Installation Manager rolls back a package to a previous version, the current version of the files are uninstalled and the earlier versions are reinstalled. If you choose not to save the files for rollback, you can prevent the files from being saved by changing the following preference in your response file:

```
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
```

to this:

```
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='false'/>
```

For more information on setting your Installation Manager preferences, see the IBM Installation Manager Information Center.

What to do next

You can create a standalone application server profile, management profile, managed (custom) profile, cell profile, or secure proxy profile using the Profile Management Tool or the manageprofiles command.

Installing and removing features on distributed operating systems

You can use Installation Manager to install and remove a product feature.

Before you begin

Make sure that your Installation Manager preferences are pointing to the appropriate web-based or local repositories containing the product.

About this task

Perform this procedure to use Installation Manager to install or remove a feature.

Note: Like other Installation Manager operations, you can invoke a modification from a silent response file. You can record this response file using the GUI and Installation Manager's record mode, or you can manually create or modify a response file to suit your needs.

Procedure

1. Stop all servers and applications on the WebSphere Application Server installation that is being modified.
2. Start Installation Manager.
3. Click **Modify**.
4. Select the package group to modify.
5. Click **Next**.

Note: If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.

6. Expand **IBM WebSphere Application Server Network Deployment**.
7. Check the appropriate checkbox to install a feature, or clear the appropriate checkbox to remove a feature if you already have it installed.
   - EJBDeploy tool for pre-EJB 3.0 modules

     This option installs the EJBDeploy tool for pre-EJB 3.0 modules.

     trns: The EJBDeploy tool was installed automatically with the product in WebSphere Application Server Version 7 and earlier. It is now an optional feature.

     Before you deploy applications on the server, you must run the EJBDeploy tool on applications that contain EJB modules that are based on specifications prior to EJB 3.0. Running the EJBDeploy tool generates deployment code for enterprise beans in the application. Beginning with the EJB 3.0 specification, the EJBDeploy tool is no longer required because WebSphere Application Server uses a new feature called "JITDeploy", which automatically generates code when the application starts.
   - Standalone thin clients, resource adapters, and embeddable containers

     IBM thin clients and resource adapters provide a set of clients and resource adapters for a variety of technologies, such as JAX-WS, JAX-RPC, JAX-RS, XML, EJB, JPA, JMS, and more. An embeddable container runs in a standalone Java Platform, Standard Edition environment. For example, you can use the embeddable EJB container to run enterprise beans outside the application server.
     - Standalone thin clients and resource adapters

       This option installs the IBM standalone thin clients and resource adapters.

       IBM thin clients provide a set of clients for a variety of technologies, such as JAX-WS, JAX-RPC, JAX-RS, XML, EJB, JPA, JMS, and more. IBM resource adapters provide the resource adapters for JMS.
     - Embeddable EJB container

       This option installs the embeddable EJB container.

       The embeddable EJB container is a Java Archive (JAR) file that you can use to run enterprise beans in a standalone Java Platform, Standard Edition environment. You can run enterprise beans using this embeddable container outside the application server. The embeddable EJB container is a part of the EJB 3.1 specification and is primarily used for unit testing enterprise beans business logic.
   - Sample applications

     This option installs the sample applications for learning and demonstration environments.

     The samples include both source code files and integrated enterprise applications that demonstrate some of the latest Java (TM) Platform, Enterprise Edition (Java EE) and WebSphere technologies. The samples are recommended for installation to learning and demonstration environments, such as development environments. However, they are not recommended for installation to production application server environments.
8. Click **Next**.
9. Review the summary information, and click **Modify**.
   - If the modification is successful, the program displays a message indicating that installation is successful.
   - If the modification is not successful, click **View Log File** to troubleshoot the problem.
10. Click **Finish**.
11. Click **File > Exit** to close Installation Manager.

Example

Like other Installation Manager operations, you can invoke a modification from a silent response file. You can record this response file using the GUI and Installation Manager's record mode, or you can manually create or modify a response file to suit your needs. In the following list, the optional feature offering names are enclosed in parentheses:

- EJBDeploy tool for pre-EJB 3.0 modules (`ejbdeploy`)
- Standalone thin clients, resource adapters, and embeddable containers
  - Standalone thin clients and resource adapters (`thinclient`)
  - Embeddable EJB container (`embeddablecontainer`)
- Sample applications (`samples`)

Windows Here is an example of a response file for modifying the features in an installation:

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright ######################################################
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2011.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
####################################################################### -->

<!-- ##### Frequently Asked Questions #####################################
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
#     Installation Manager Information Center can be found at:
#     http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
#   Windows = IBMIM.exe -record c:\temp\responsefiles\WASv8.install.Win32.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#   Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv8.install.RHEL64.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse\tools subdirectory in the directory where you installed
# Installation Manager:
#
#   Windows = imcl.exe -acceptLicense -showProgress
#     input <response_file_path_and_name> -log <log_file_path_and_name>
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
#   Windows = imcl.exe -acceptLicense -showProgress
#     input c:\temp\responsefile\WASv8.install.Win32.xml
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input /home/user/responsefile/WASv8.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
#     license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help:  IBMIM -help
#
# Question 3. How do I store and pass credentials to repositories that
# require authentication?
# Answer 3. Installation Manager uses a key ring file to store encrypted
# credentials for authenticating with repositories. Follow this two-step
# process for creating and using a key ring file with Installation Manager.
#
# First, create a key ring file with your credentials by starting
# Installation Manager from the command line under eclipse subdirectory
# with the keyring parameter.
# Use the optional password parameter to password protect your file.
#
#   Windows = IBMIM.exe -keyring <path and file name> -password <password>
#   Linux, UNIX, IBM i and z/OS = ./IBMIM -keyring <path and file name>
#                                 -password <password>
#
# Installation Manager will start in graphical mode. Verify that the
# repositories to which you need to authenticate are included in the
# preferences, File / Preferences / Repositories. If they are not
# listed, then click Add Repositories to add the URL or UNC path.
# Installation Manager will prompt for your credentials. If the repository
# is already in the list, then any attempt to access the repository location,
# such as clicking the Test Connections button, will also prompt for your
# credentials. Enter the correct credential and check the Save password
# checkbox. The credentials are saved to the key ring file you specified.
#
# Second, when you start a silent installation, run imcl under eclipse/tools
# subdirectory, and provide Installation Manager with the location of the key
# ring file and the password if the file is protected. For example:
#
#   Windows = imcl.exe -acceptLicense -showProgress
#     input <path and file name of response file>
#     -keyring <path and name of key ring file> -password <password>
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input <path and file name of response file>
#     -keyring <path and name of key ring file> -password <password>
#
####################################################################### -->

<!-- ##### Agent Input ###############################################
#
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the installation finishes.
#
# Valid values for clean:
#      true = only use the repositories and other preferences that are
#           specified in the response file.
#      false = use the repositories and other preferences that are
#           specified in the response file and Installation Manager.
#
# Valid values for temporary:
#      true = repositories and other preferences specified in the
#           response file do not persist in Installation Manager.
#      false = repositories and other preferences specified in the
#           response file persist in Installation Manager.
#
####################################################################### -->

<agent-input clean='true' temporary='true'>

<!-- ##### Repositories ####################################################
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#
####################################################################### -->

<server>
    <!-- ##### IBM WebSphere Live Update Repositories ###################
     # These repositories contain WebSphere Application Server offerings,
     # and updates for those offerings
     #
     # To use the secure repository (https), you must have an IBM ID,
     # which can be obtained by registering at: http://www.ibm.com/account
     # or your Passport Advantage account.
     #
     # And, you must use a key ring file with your response file.
     ################################################################## -->
    <repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v80" />
    <!-- <repository location="https://www.ibm.com/software/rational/repositorymanager/repositories/websphere" /> -->

    <!-- ##### Custom Repositories ########################################
     # Uncomment and update the repository location key below
     # to specify URLs or UNC paths to any intranet repositories
     # and directory paths to local repositories to use.
     ################################################################## -->
    <!-- <repository location='https:\\w3.mycompany.com\repositories\'/> -->
    <!-- <repository location='/home/user/repositories/websphere/'/> -->
    <!-- ##### Local Repositories ########################################
     # Uncomment and update the following line when using a local
     # repository located on your own machine to install a
     # WebSphere Application Server offering.
     ############################################################# -->
    <!-- <repository location='insert the full directory path inside single quotes'/> -->
</server>

<!-- ##### Modify Packages ###############################################
#
# Install and Uninstall Commands
#
# Use the install and uninstall commands to inform Installation Manager
# of the installation packages to install or uninstall.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
#    false = indicates not to modify an existing install by adding
#            or removing features.
#    true = indicates to modify an existing install by adding or
#           removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be installed. The offering listed must be present in
# at least one of the repositories listed earlier. The example
# command below contains the offering ID for the Network Deployment
# edition of WebSphere Application Server.
#
# The version attribute is optional. If a version number is provided,
# then the offering will be installed or uninstalled at the version level
# specified as long as it is available in the repositories. If the version
# attribute is not provided, then the default behavior is to install or
# uninstall the latest version available in the repositories. The version
# number can be found in the repository.xml file in the repositories.
# For example, <offering ... version='8.0.0.20110617_2222'>.
#
# The profile attribute is required and typically is unique to the
# offering. If modifying or updating an existing installation, the
# profile attribute must match the profile ID of the targeted installation
# of WebSphere Application Server.
#
# The features attribute is optional. Offerings always have at least
# one feature; a required core feature which is installed regardless
# of whether it is explicitly specified. If other feature names
# are provided, then only those features will be installed.
# Features must be comma delimited without spaces.
#
# The feature values for WebSphere Application Server include:
#  ejbdeploy,thinclient,embeddablecontainer,samples,
#  com.ibm.sdk.6_32bit,com.ibm.sdk.6_64bit
#
# In the example that follows, the samples feature is being added
# and the thinclient, ejbdeploy, and embeddablecontainer features
# are being removed from the specified offering.
#
# Neither the core.feature nor the Software Development Kit (SDK)
# feature can be removed because they are required features.
#
# The installFixes attribute indicates whether fixes available in
# repositories are installed with the product. By default, all
# available fixes will be installed with the offering.
#
# Valid values for installFixes:
#      none = do not install available fixes with the offering.
#      recommended = installs all available recommended fixes with the offering.
#      all = installs all available fixes with the offering.
#
# Installation Manager supports modifying multiple offerings at once.
# Additional offerings can be included in the install and uninstall commands,
# with each offering requiring its own offering ID, version, profile value,
# and feature values.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# The eclipseLocation data key should use the same directory path to
# WebSphere Application Server as the installationLocation attribute.
#
# Include data keys for product specific profile properties.
# For instance, additional translations can be specified by including
# the cic.selector.nl data key and the language codes as values for
# the translations to install.
#
#  Language code values: cs,de,en,es,fr,hu,it,ja,ko,pl,pt_BR,ro,ru,zh,zh_HK,zh_TW
#
######################################################################## -->

<install modify='true'>
<offering id='com.ibm.websphere.ND.v80'
 profile='IBM WebSphere Application Server Network Deployment V8.0'
 features='samples'/>
</install>

<uninstall modify='true'>
<offering id='com.ibm.websphere.ND.v80'
 profile='IBM WebSphere Application Server Network Deployment V8.0'
 features='thinclient,ejbdeploy,embeddablecontainer'/>
</uninstall>

<profile id='IBM WebSphere Application Server Network Deployment V8.0'
 installLocation='C:\Program Files\IBM\WebSphere\AppServer'>
<data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.nl' value='en'/>
</profile>

<!-- ##### Shared Data Location ############################################
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared'/>
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
#     true = store downloaded artifacts in the shared data location
#     false = remove downloaded artifacts from the shared data location
#
######################################################################## -->

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
-->

<!-- ##### Preferences Settings ############################################
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
######################################################################## -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
```

```
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
 -->

</agent-input>
```

Updating the product on distributed operating systems

You can use Installation Manager to update this product to a later version.

Before you begin

Make sure that your Installation Manager preferences are pointing to Web-based or local repositories that contain the appropriate updates for the product.

About this task

Perform this procedure to use Installation Manager to update this product.

Procedure

1. Stop all servers and applications on the WebSphere Application Server installation that is being updated.
2. Start Installation Manager.
3. Click **Update**.
4. Select the package group to update.
5. Click **Next**.

   Note: If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.
6. Select the version to which you want to update under **IBM WebSphere Application Server Network Deployment**.
7. Click **Next**.
8. Accept the terms in the license agreements, and click **Next**.
9. Review the summary information, and click **Update**.
   - If the installation is successful, the program displays a message indicating that installation is successful.
   - If the installation is not successful, click **View Log File** to troubleshoot the problem.
10. Click **Finish**.
11. Click **File > Exit** to close Installation Manager.

Rolling back the product on distributed operating systems

You can use Installation Manager to roll back this product to an earlier version.

Before you begin

Make sure that your Installation Manager preferences are pointing to Web-based or local repositories that contain the appropriate earlier version of the product.

About this task

Perform this procedure to use Installation Manager to roll back this product to an earlier version.

Procedure

1. Stop all servers on the WebSphere Application Server installation that is being modified.
2. Start Installation Manager.
3. Click **Roll Back**.
4. Select the package group to roll back.
5. Click **Next**.

   Note: If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.
6. Select the version to which you want to roll back under **IBM WebSphere Application Server Network Deployment**.
7. Click **Next**.
8. Review the summary information, and click **Roll Back**.
   - If the roll back is successful, the program displays a message indicating that the roll back is successful.
   - If the roll back is not successful, click **View Log File** to troubleshoot the problem.
9. Click **Finish**.
10. Click **File > Exit** to close Installation Manager.

Upgrading the product on distributed operating systems

You can use Installation Manager to upgrade WebSphere Application Server Version 8.0 from the trial to the full product.

Before you begin

- The installation that you want to upgrade must be at the WebSphere Application Server Version 8.0.0.0 level.
  - If you originally installed Version 8.0.0.0 and then added any fix packs to your existing trial installation, you must use Installation Manager to roll back to Version 8.0.0.0 before upgrading.
  - If you installed your existing trial installation at a level later than Version 8.0.0.0, you must uninstall your existing edition and install the full product to which you want to upgrade.
- Make sure that your Installation Manager preferences are pointing to Web-based or local repositories that contain the appropriate upgrades for the product.

About this task

Perform this procedure to use Installation Manager to upgrade from the trial to the full product.

Procedure

1. Stop all servers and applications on the WebSphere Application Server installation that is being upgraded.
2. Start Installation Manager.
3. Click **Install**.

   Note: If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.

   Installation Manager searches its defined repositories for available packages.

4. Select **Application Server Network Deployment** and the appropriate version, and click **Next**.
5. Accept the terms in the license agreements, and click **Next**.
6. Complete the following actions.
   a. Select **Use the existing package group**.
   b. Select the package group of the product that you want to upgrade.

      Important: If you select an existing group that cannot be upgraded to the product that you are currently installing, an error will occur.

   c. Click **Next**.

   Important: Installation Manager defaults to installing a new offering. To upgrade your existing installation, you must select the existing package group.
7. Select any features that you want to install, and click **Next**.

   Tip: You can run the Installation Manager later to modify this installation and add or remove features.
8. Review the summary information, and click **Install**.
   - If the upgrade is successful, the program displays a message indicating that installation is successful.

     Note: The program might also display important post-installation instructions as well.
   - If the installation is not successful, click **View Log File** to troubleshoot the problem.
9. Select which tool you want to start when this upgrade is finished.
   - Select **Profile Management Tool to create a profile** if you want to open the full Profile Management Tool and create a new profile when this installation is finished.
   - Select **Profile Management Tool to create an application server profile for a development environment** if you want to create an application server profile with settings appropriate for a development environment when this installation is finished.

     Note: The development settings are appropriate for a development environment where frequent application updates are performed and system resources are at a minimum. Do not use the development settings for production servers.
   - Select **None** if you do not want to create a new profile when this installation is finished.

   Restriction: The option to launch the Profile Management Tool is only available when a version of WebSphere Application Server containing the Profile Management Tool is installed.
10. Click **Finish**.
11. Click **File** > **Exit** to close Installation Manager.

Uninstalling the product from distributed operating systems using the GUI

Use the Installation Manager GUI to uninstall the product.

Procedure

1. Uninstall the product.
   a. Stop all servers and applications on the WebSphere Application Server installation that contains the product.
   b. Start Installation Manager.
   c. Click **Uninstall**.
   d. In the **Uninstall Packages** window, perform the following actions.

1) Select **IBM WebSphere Application Server Network Deployment** and the appropriate version.

   Note: If you are uninstalling the trial version of this product, select **IBM WebSphere Application Server Network Deployment (Trial Version)**.

2) Click **Next**.

e. Review the summary information.

f. Click **Uninstall**.

- If the uninstallation is successful, the program displays a message that indicates success.
- If the uninstallation is not successful, click **View log** to troubleshoot the problem.

g. Click **Finish**.

h. Click **File > Exit** to close Installation Manager.

2. Optional: Uninstall IBM Installation Manager.

   Important: Before you can uninstall IBM Installation Manager, you must uninstall all of the packages that were installed by Installation Manager.

   Read Uninstalling Installation Manager in the Installation Manager information center for information about performing this procedure.

Uninstalling the product from distributed operating systems silently

You can use Installation Manager to uninstall this product silently.

Before you begin

Optional: Perform or record the installation of Installation Manager and installation of the product to a temporary installation registry on one of your systems so that you can use this temporary registry to record the uninstallation without using the standard registry where Installation Manager is installed.

Read the following for more information:

- "Installing the product on distributed operating systems using the GUI" on page 78
- "Installing the product on distributed operating systems silently" on page 84

About this task

Using Installation Manager, you can work with response files to uninstall the product silently in a variety of ways. You can record a response file using the GUI as described in the following procedure, or you can generate a new response file by hand or by taking an example and modifying it.

Procedure

1. Stop all servers and applications on the WebSphere Application Server installations that contain the product.
2. Optional: **Record a response file to uninstall the product:** On one of your systems, perform the following actions to record a response file that will uninstall the product:

   a. From a command line, change to the eclipse subdirectory in the directory where you installed Installation Manager.

   b. Start Installation Manager from the command line using the -record option.

   For example:

   - Windows **Administrator or non-administrator:**

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"
  -record C:\temp\uninstall_response_file.xml
```

- AIX HP-UX Linux Solaris **Administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry
  -record /var/temp/uninstall_response_file.xml
```

- AIX HP-UX Linux Solaris **Non-administrator:**

```
./IBMIM -skipInstall user_home/var/temp/imRegistry
  -record user_home/var/temp/uninstall_response_file.xml
```

Tip: If you choose to use the -skipInstall parameter with a temporary installation registry created as described in "Before you begin," Installation Manager uses the temporary installation registry while recording the response file. It is important to note that when the -skipInstall parameter is specified, no product packages are installed or uninstalled. All of the actions that you perform in Installation Manager simply update the installation data that is stored in the specified temporary registry. After the response file is generated, it can be used to uninstall the product, removing the product files and updating the standard installation registry.

The -skipInstall operation should not be used on the actual agent data location used by Installation Manager. This is unsupported. Use a clean writable location, and re-use that location for future recording sessions.

For more information, read the IBM Installation Manager Information Center.

c. Click **Uninstall**.

d. In the **Uninstall Packages** window, perform the following actions.

1) Select **IBM WebSphere Application Server Network Deployment** and the appropriate version.

Note: If you are uninstalling the trial version of this product, select **IBM WebSphere Application Server Network Deployment (Trial Version)**.

2) Click **Next**.

e. Review the summary information.

f. Click **Uninstall**.

- If the uninstallation is successful, the program displays a message that indicates success.
- If the uninstallation is not successful, click **View log** to troubleshoot the problem.

g. Click **Finish**.

h. Click **File > Exit** to close Installation Manager.

3. **Use the response file to uninstall the product silently:** From a command line on each of the systems from which you want to uninstall the product, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager and use the response file that you created to silently uninstall the product.

For example:

- Windows **Administrator or non-administrator:**

```
imcl.exe
  input C:\temp\uninstall_response_file.xml
  -log C:\temp\uninstall_log.xml
```

- AIX HP-UX Linux Solaris **Administrator:**

```
./imcl
  input /var/temp/uninstall_response_file.xml
  -log /var/temp/uninstall_log.xml
```

- AIX HP-UX Linux Solaris **Non-administrator:**

```
./imcl
  input user_home/var/temp/uninstall_response_file.xml
  -log user_home/var/temp/uninstall_log.xml
```

Go to the IBM Installation Manager Information Center for more information.

4. Optional: Uninstall IBM Installation Manager.

Important: Before you can uninstall IBM Installation Manager, you must uninstall all of the packages that were installed by Installation Manager.

Read the IBM Installation Manager Information Center for information about using the uninstall script to perform this procedure.

Windows

Example

The following is an example of a response file for silently uninstalling the product.

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright #######################################################
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2011.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
######################################################################## -->

<!-- ##### Frequently Asked Questions ######################################
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
#     Installation Manager Information Center can be found at:
#     http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
#   Windows = IBMIM.exe -record c:\temp\responsefiles\WASv8.install.Win32.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#   Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv8.install.RHEL64.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse\tools subdirectory in the directory where you installed
# Installation Manager:
#
#   Windows = imcl.exe -acceptLicense -showProgress
#     input <response_file_path_and_name> -log <log_file_path_and_name>
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
#   Windows = imcl.exe -acceptLicense -showProgress
#     input c:\temp\responsefile\WASv8.install.Win32.xml
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input /home/user/responsefile/WASv8.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
#     license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help:  IBMIM -help
#
######################################################################## -->

<!-- ##### Agent Input ##############################################
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the uninstall finishes.
#
# Valid values for clean:
#      true = only use the repositories and other preferences that are
#           specified in the response file.
#      false = use the repositories and other preferences that are
#           specified in the response file and Installation Manager.
#
# Valid values for temporary:
#      true = repositories and other preferences specified in the
#           response file do not persist in Installation Manager.
#      false = repositories and other preferences specified in the
#           response file persist in Installation Manager.
#
####################################################################### -->

<agent-input clean='true' temporary='true'>

<!-- ##### Repositories ###################################################
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#
####################################################################### -->

<server>
    <!-- ##### IBM WebSphere Live Update Repositories ####################
     # These repositories contain WebSphere Application Server offerings,
     # and updates for those offerings
     #
     # To use the secure repository (https), you must have an IBM ID,
     # which can be obtained by registering at: http://www.ibm.com/account
     # or your Passport Advantage account.
     #
     # And, you must use a key ring file with your response file.
     ################################################################## -->
    <repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v80" />
    <!-- <repository location="https://www.ibm.com/software/rational/repositorymanager/repositories/websphere" /> -->

    <!-- ##### Custom Repositories #######################################
     # Uncomment and update the repository location key below
     # to specify URLs or UNC paths to any intranet repositories
     # and directory paths to local repositories to use.
     ################################################################## -->
    <!-- <repository location='https:\\w3.mycompany.com\repositories\'/> -->
    <!-- <repository location='/home/user/repositories/websphere/'/> -->

    <!-- ##### Local Repositories ########################################
     # Uncomment and update the following line when using a local
     # repository located on your own machine to install a
     # WebSphere Application Server offering.
     ############################################################# -->
    <!-- <repository location='insert the full directory path inside single quotes'/> -->
</server>

<!-- ##### Uninstall Packages ############################################
#
# Uninstall Command
#
# Use the uninstall command to inform Installation Manager of the
# installation packages to uninstall.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
#    false = indicates not to modify an existing install by adding
#            or removing features.
#    true = indicates to modify an existing install by adding or
#           removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be uninstalled. The example command below contains the
# offering ID for WebSphere Application Server Network Deployment edition.
#
# The version attribute is optional. If a version number is provided,
# then the offering will be uninstalled at the version level specified
# If the version attribute is not provided, then the default behavior is
# to uninstall the latest version. The version number can be found in
# the repository.xml file in the repositories.
# For example, <offering ... version='8.0.0.20110617_2222'>.
#
# The profile attribute is required and must match the package group
# name for the offering to be uninstalled.
#
# The features attribute is optional. If there is no feature attribute,
# then all features are uninstalled. If features are specified, then
# only those features will be uninstalled.
# Features must be comma delimited without spaces.
#
# The feature values for WebSphere Application Server include:
#  ejbdeploy,thinclient,embeddablecontainer,samples,
#  com.ibm.sdk.6_32bit,com.ibm.sdk.6_64bit
```

```
#
# Installation Manager supports uninstalling multiple offerings at once.
# Additional offerings can be included in the uninstall command,
# with each offering requiring its own offering ID, version, profile value,
# and feature values.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# The eclipseLocation data key should use the same directory path to
# WebSphere Application Server as the installationLocation attribute.
#
# Include data keys for product specific profile properties.
# For instance, additional translations can be specified by including
# the cic.selector.nl data key and the language codes as values for
# the translations to install.
#
#  Language code values: cs,de,en,es,fr,hu,it,ja,ko,pl,pt_BR,ro,ru,zh,zh_HK,zh_TW
#
####################################################################### -->

<uninstall modify='false'>
<offering id='com.ibm.websphere.ND.v80'
 profile='IBM WebSphere Application Server Network Deployment V8.0'
 features='core.feature,ejbdeploy,thinclient,embeddablecontainer,samples,com.ibm.sdk.6_32bit'/>
</uninstall>

<profile id='IBM WebSphere Application Server Network Deployment V8.0'
 installLocation='C:\Program Files\IBM\WebSphere\AppServer'>
<data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.nl' value='cs,de,en,es,fr,hu,it,ja,ko,pl,pt_BR,ro,ru,zh,zh_HK,zh_TW'/>
</profile>

<!-- ##### Shared Data Location ###########################################
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared'/>
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
#     true = store downloaded artifacts in the shared data location
#     false = remove downloaded artifacts from the shared data location
#
####################################################################### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
-->

<!-- ##### Preferences Settings ###########################################
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
####################################################################### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
 -->

</agent-input>
```

Verifying the installation

You can verify successful installation of the product using the capabilities of IBM Installation Manager.

About this task

WebSphere Application Server Version 7 and earlier had an installation verification utility, the installver command, that would verify checksums of installed files against a bill of materials that was shipped with the product. In WebSphere Application Server Version 8.0 and later, where the installation is based on the Installation Manager rather than on InstallShield MultiPlatform (ISMP), the installver command is replaced by the verification capabilities of the Installation Manager.

Procedure

- To verify installation of the product, you can use Installation Manager to find the product in the list of installed packages.

  Perform one of the following actions:

  – Change the directory to the `eclipse/tools` subdirectory of the Installation Manager binaries location and run this command:

    AIX HP-UX Linux Solaris

```
./imcl listInstalledPackages
```

    Windows

```
imcl listInstalledPackages
```

    This will display a list indicating which packages this Installation Manager has installed. For example:

```
com.ibm.websphere.ND.v80_8.0.0.20110203_0234
```

  – Launch the Installation Manager GUI, and verify the installation by going to **File -> View Installed Packages**.

- If an installation was successful, the `installed.xml` file should contain a location element for the installed product.

  For example, the following file:

  AIX HP-UX Solaris Linux

```
installation_manager_root/properties/version/installed.xml
```

Windows

```
installation_manager_root\properties\version\installed.xml
```

should contain something like this:

AIX HP-UX Solaris Linux

```
<location id="IBM WebSphere Application Server V8.0" kind="product"
path="/opt/IBM/WebSphere/AppServer"> ..... </location>
```

Windows

```
<location id="IBM WebSphere Application Server V8.0" kind="product"
path="C:\Program Files\IBM\WebSphere\AppServer"> ..... </location>
```

- If you used the Installation Manager -log option during installation, you can verify that the resulting log file does not contain any errors.

  If you used the following command to install the product silently for example:

  AIX HP-UX Solaris Linux

  ```
  ./imcl -acceptLicense
    input /var/temp/install_response_file.xml
    -log /var/temp/install_log.xml
    -keyring /var/IM/im.keyring
  ```

  Windows

  ```
  imcl.exe -acceptLicense
    input C:\temp\install_response_file.xml
    -log C:\temp\install_log.xml
    -keyring C:\IM\im.keyring
  ```

  and the installation was successful, the `install_log.xml` file should contain something like this:

  ```
  <?xml version="1.0" encoding="UTF-8"?>
  <result>
  </result>
  ```

Roadmap: Installing the Network Deployment product

Install IBM WebSphere Application Server Network Deployment from the product media or from an installation image that you can download from the Passport Advantage site.

Before you begin

See Chapter 6, "Installing the product," on page 73 for information about installing any of the products in the WebSphere Application Server family of products.

About this task

This article provides an overview of installing the WebSphere Application Server Network Deployment product.

The Installation Manager product performs the installation. You can install from a graphical interface or from the command line using a response file.

At a high-level view, the steps for installing and configuring the Network Deployment product are:

1. Install the Network Deployment product.
2. Use the Profile Management Tool or the manageprofiles command to create the profiles that your topology needs.

   You can create the following profiles:

   - Application server profile
   - Management profile
   - Cell profile

- Custom profile
- Secure proxy server

Procedure

1. Review typical installation scenarios for the product.
2. Install the product and create a Network Deployment cell.

   The steps for installing the Network Deployment product and creating a deployment manager are as follows:

   a. Prepare the operating system.

   b. Access the product disk or a downloaded installation image.

   c. Install the product.

   d. Create a Network Deployment environment.

      A cell has a deployment manager with a federated application server.

      A deployment manager has only the deployment manager profile. To work with applications deployed on an application server that is part of a Network Deployment cell, you must create an application server profile and federate it after installing the Network Deployment product.
3. Create an additional application server profile for a Network Deployment cell.

   The steps for creating an application server profile are:

   a. Use the Profile Management Tool or the manageprofiles command to create an application server profile.

   b. Open the First steps console and start the application server, or start the application server from the command line:

      1) Change to the *profile_root*/bin directory.
         - AIX HP-UX Linux Solaris cd *profile_root*/bin
         - Windows cd *profile_root*\bin

      2) Start the application server with the startServer command.
         - AIX HP-UX Linux Solaris ./startServer.sh
         - Windows startServer.bat

   c. Federate the application server into the cell through the administrative console (**System Administration** > **Nodes** > **Add Node**) or with the addnode command in the *profile_root*/bin directory.

   To access applications deployed on the application server from a deployment manager, you must federate the application server. To federate the application server, add the application server as a managed node of the deployment manager.

Results

The Network Deployment product is installed on a single machine and you can start the deployment manager and the standalone application server.

What to do next

After installing and verifying, the next step is to use the product. Start the application server or the deployment manager, node agent, and federated application server to use the administrative console to deploy an existing application.

Getting the latest information: The information center always has the most current information. The information center displays in the language of your machine locale if possible.

Access the information center for a WebSphere Application Server product from the WebSphere Application Server library page.

Installing in group mode

You can use IBM Installation Manager group mode to allow multiple users to use a single instance of Installation Manager to manage software packages.

About this task

- Group mode allows multiple users to use a single instance of IBM Installation Manager to manage software packages.

  This does not mean that two people can use the single instance of IBM Installation Manager at the same time.
- Group mode is not available on Windows or IBM i operating systems.
- If you do not install Installation Manager using group mode, you will not be able to use group mode to manage any of the products that you install later using this Installation Manager.
- Make sure that you change the installation location from the default location in the current user's home directory to a location that is accessible by all users in the group.
- Set up your groups, permissions, and environment variables as described in the Group mode road maps in the IBM Installation Manager Information Center before installing in group mode.
- For more information on using group mode, read the Group mode road maps in the IBM Installation Manager Information Center.

Procedure

1. Create a group.

   For example:

```
wasadmin
```

2. Create multiple user IDs.

   For example:

```
installadmin
imuser
```

3. Make the group that you created the primary group for the user IDs that you created.
4. Make sure that the umask for all IDs is 002.

   See the IBM Installation Manager Information Center for alternatives if for some reason you cannot set the umask.
5. Create a file system where all the of the products will be installed.

   For example:

```
/WASProducts
```

6. Give access to this file system to all of the user IDs that you created.
7. Using one of the user IDs that you created, install Installation Manager in group mode to the file system that you created.

   Use `installadmin`, for example, to install Installation Manager in group mode using the GUI:

```
groupinst -dataLocation /WASProducts/IMAppData
```

8. Using one of the user IDs that you created, start Installation Manager and install a WebSphere Application Server product to the file system that you created.

   Use `installadmin`, for example, to install the trial edition of the Network Deployment product in:

```
/WASProducts/WASV8/NDTRIAL
```

   with the Samples option.
9. Exit Installation Manager.

10. Using one of the other user IDs that you created, you can maintain the product installation.

    Use `imuser`, for example, to update the trial edition of the Network Deployment product with additional optional features, remove options, or add fixpacks.

    a. As root user ID,

       - For WebSphere Application Server only, change to *app_server_root*/`instutils` and run the following command:

```
chutils -setowner=imuser
```

       - For all other products, run the following command:

```
chown -R imuser app_server_root
```

    b. Start Installation Manager under the `imuser` user ID, and perform any necessary changes to the installation.

Non-root installations

Non-root users can install WebSphere Application Server Network Deployment in both silent and interactive mode for full product installations and removals, incremental feature installations, and edition upgrades. The term *non-root* implies an installer on an operating system such as AIX or Linux, but it also means a non-administrator group installer on a Windows system.

For existing installations, the root or non-root installer who owns the currently installed files is the only user who can perform subsequent installation or removal operations on that installation except under one of the following conditions:

- Installation Manager and the product were installed in group mode.
- The owner reassigns ownership of the appropriate directories and files to another user.

The set of post-installation operations that are subject to this rule includes installing a feature, upgrading a trial or from Express to the base product, installing maintenance, and uninstalling the product.

- "Installation considerations"
- "Setting permissions" on page 115
- "Private GSKit installation" on page 115
- "Non-root limitations" on page 115
- Windows "Uninstallation considerations" on page 117

Installation considerations

There are various considerations that you must examine if you want to install as a non-root user.

- **Non-root installations apply to all of the WebSphere software components in the product package**

  Non-root installers can install all of the components, including the following:

  - Application Client for IBM WebSphere Application Server
  - DMZ Secure Proxy Server for IBM WebSphere Application Server
  - IBM HTTP Server for WebSphere Application Server
  - IBM WebSphere Application Server
  - Pluggable Application Client for IBM WebSphere Application Server
  - Web Server Plug-ins for IBM WebSphere Application Server
  - WebSphere Customization Toolbox

- **Non-root installations install an operational product**

  If some portion of an installation requires root privileges, Installation Manager provides an option so that the non-root installer can install an operational product without enabling the privileged option whenever possible.

- **Installation Manager identifies root-only options**

  Installation Manager clearly identifies privileged options by disabling such options in the interface of the non-root installer.
- **Default installation locations are within your home directory**

  Default installation locations are within the home directory of the non-root installer to verify a writable disk space. Installation Manager verifies that specified disk locations are writable.

Setting permissions

Note: You can use the chutils utility to change ownership to another user for the file system after installation for future operations on that product.

Certain subsequent installation operations (SIOs) on the application server can be attempted and performed by other users, whether root or non-root. SIOs include installing features, edition upgrades, and fix packs.

See "Setting file permissions" on page 117 for more information.

Restriction: Windows The permissions features are not available on Windows operating systems.

Private GSKit installation

Note: Installing IBM HTTP Server and the Web Server Plug-ins installs a private copy of IBM Global Security Kit (GSKit), which allows both root and non-root users to enable SSL support.

The GSKit package is installed to the `gsk8` directory within the installing product's root directory.

The private copy of GSKit is maintained through GSKit update packages delivered in IBM HTTP Server and web server plug-in fix packs.

Solaris If you are using zones on the Solaris operating system, you can use the private GSKit without a zone-writable `/usr` directory.

Non-root limitations

There are some limitations and differences when installing as a non-root user as opposed to a root user.

- **Local web server plug-in installation**

  When the web server plug-in and the application server are installed on the same machine (local installation scenario), non-root installation for the plug-in component is only supported if the application server was also installed by the same non-root user. Otherwise, the web server configuration scripts fail to run against the application server installation.
- AIX HP-UX Linux Solaris **Home directories**

  You cannot successfully complete certain post-installation tasks if the installing non-root user does not have a home directory defined. Any user installing and using the product must have a valid home directory.
- **Port value assignment**

  Profile creation avoids port value conflicts by examining port values in use by other WebSphere Application Server installations. Multiple non-root installers diminish the ability to detect and avoid port value conflicts. WebSphere Application Server installations are visible to the installer ID only, because the non-root installations do not register globally. If the root user performs all WebSphere Application Server installations, the problem is avoided.
- **Operating system registration**

- AIX HP-UX Linux Solaris Packages installed by a non-root installer cannot register using the native operating system mechanisms, such as Red Hat Package Manager (RPM) on Linux.

  WebSphere software registers in the WebSphere Application Server installation registry file and the `vpd.properties` file. All installable components are fully functional despite the lack of native registration.
- Windows Registry entries are on a non-administrator per user basis instead of registering the software for the entire machine, which occurs when an administrator user installs.

- **Installation visibility**

  The non-root installer cannot register software packages natively. The installation registers installed components in the WebSphere Application Server installation registry file. The file is in the home directory of the non-root installer as opposed to being a globally shared resource available to all users.

  In case a non-root user is granted access or visibility to share installation information with a root or administrator user, all installation information cannot be accessed in certain scenarios. If the non-root or non-administrator user has previously installed WebSphere Application Server before increased access rights are granted, the scope of the installation registry will still be local instead of global.

  However, if the non-root or non-administrator user has not installed WebSphere Application Server before and access is upgraded, it becomes possible to access global installation information generated by a root or admin user.
- Windows **Adaptive Fast Path Architecture (AFPA) limitations**

  FRCA/AFPA has been deprecated starting with V7.0 and its use is discouraged. There is no support for Windows Vista, Windows 2008, or any later Windows operating systems.

  AFPA is a software architecture that dramatically improves the efficiency, and therefore the capacity, of web servers and other network servers by caching static files.

  AFPA is a Windows kernel-level device driver within the IBM HTTP Server. AFPA provides caching of static files served from IBM HTTP Server. AFPA is recommended for very high-volume static-file web sites only.

  Dynamic web pages, such as those generated by WebSphere Application Server, are not usually cacheable. Most application servers should not enable AFPA.
  - A Windows kernel-level device driver cannot install from a non-administrator installer. Windows requires administrator group privileges when installing device drivers.
- **Edge Components**

  Edge requires root privileges because of its native installation mechanisms.
- Windows **Java Web Start**

  The Application Client supports Java Web Start (JWS) on all supported platforms. Particularly on a Windows system, the Application Client requires administrator access in order to configure JWS properly, by updating Windows native registry entries with some JWS-specific entries.

  Non-administrator installers cannot register the update, which provides less than full support for JWS. For example, a JWS application cannot launch from the Internet Explorer or Mozilla Firefox browser.

  JWS is not an installable feature for the Client and cannot be separately installed by an administrator installer. The installation program lists JWS as one of the non-administrator limitations on Windows systems.
- Windows **Windows services limitations**
  - The non-root installer cannot create Windows services for any of the WebSphere Application Server processes, including the application server, node agent, deployment manager, IBM HTTP Server, or IBM Administration Server.
  - An administrator installer can create the service after installation using the WASService command.
- **Menu limitations**
  - Windows **Start menu entries**

    Entries in the menu are for the non-root installer, but they are not available to all users.

    If an administrator installs the product and then non-root users create profiles, the non-administrators can see their shortcuts.

  - Linux **Gnome and KDE menu entries**

    Entries in the menus are for the non-root installer instead of being applicable to all users.

    Normally, menu items are only visible to the installing user. If you want to allow other users who create profiles to see menu items for their profiles, they must have access to a copy of the base `WebSphere#.menu` file. All profile shortcuts are visible to all users who have access to the base `WebSphere#.menu` file. Copy this file into either the `/etc/xdg/menus/applications-merged` directory (for all users) or the user's `$HOME/.config/menus/applications-merged` directory. Make sure there are no conflicts between the menu file names in the `/etc/xdg/menus/applications-merged` directory and any user's `$HOME/.config/menus/applications-merged` directory.

- AIX HP-UX Linux Solaris **chutils command**

  The chutils command should be run by a root user.

Windows Uninstallation considerations

Uninstalling as an administrator: If an administrator user uninstalls an application server that is owned by another user, all registry entries for all application server instances owned by the administrator are also be removed. You should uninstall any non-root application server with the owning non-administrator user if possible.

Setting file permissions

When installation is initially performed, the resulting installation is owned by a single user or group. You can change file ownership and permissions after installation using the chutils command.

Restriction: Windows The set-permissions feature is not currently available on Windows operating systems.

Verifying file permissions

Installation Manager reports an error when the user does not have appropriate system permissions.

Setting file ownership and permissions with the chutils command

You can use the chutils command to set the file ownership and permissions for an entire installation to an owner or group that differs from the user that performed the initial installation. The main benefit is the ability to have the initial installation performed by one user and then have different users perform supported operations such as feature installations, edition upgrades, maintenance installations (such as fix packs or refresh packs), and feature-pack installations.

The command can be used for the following:

- Add or remove the ability of other non-root users to update the installation
- Transfer all file ownership of the installation to another user
- Reestablish consistent file permissions for the entire installation

The command can edit the following ownership and permissions:

- File owner
- File group
- Owner permissions

  You can only change owner permissions to the default values set during installation using the -setmod reset parameter.

- Group permissions

  You can elevate group permissions to match the owner permissions using the -setmod *grp2owner* parameter.
- Others permissions

  You can only change others, or "world," permissions to the default values set during installation through the `-setmod` parameter.

For more information on using the chutils command, read “chutils command.”

Troubleshooting

- Directory existence errors

  If you have not yet created a profile after installing the application server and you run the chutils command, then you might experience a profile-related directory error like the following:

```
INFO: (Jul 17, 2008 16:16:35) Initializing permission utility...
INFO: (Jul 17, 2008 16:16:35) Executing commands...
INFO: (Jul 17, 2008 16:16:47) The directory does not exist: /data/WebSphere/AppServer/instutils/../properties/fsdb
INFO: (Jul 17, 2008 16:16:58) The permission utility has completed successfully.
```

  Because the overall process is successful, this message can be safely ignored in this situation.
- AIX HP-UX Linux Solaris Menus and shortcuts

  Existing menus and shortcuts are not transferred after application server-owning users or groups are modified with the chutils command. You must manually recreate the menu items and shortcuts for the new owner of the application server installation. You might need to recreate the following menu items and shortcuts:
  - Profiles
  - Information center
  - Configuration Migration Tool
  - Online support
  - Profile Management Tool

chutils command

You can use the chutils command to set the file ownership and permissions for an entire installation to an owner or group that differs from the user that performed the initial installation.

trns: The chutils command delivered with WebSphere Application Server Version 8 and later has a behavior that is different from the behavior of the chutils command delivered with WebSphere Application Server Version 7 and earlier.

Considerations and limitations:

- The chutils command delivered with WebSphere Application Server Version 8 and later will not work for WebSphere Application Server Version 7 and earlier installations; and the chutils command delivered with WebSphere Application Server Version 7 and earlier will not work for WebSphere Application Server Version 8 and later installations.
- Windows The chutils command is not available on Windows operating systems.
- The chutils command should be run by a root user.
- The chutils command can be run using multiple options at once.
- You cannot use the chutils command to modify permissions for directories that are parents of of *app_server_root*.

If *app_server_root* is in User A's home directory and the root user uses chutils to change the ownership of *app_server_root* to User B, for example, *app_server_root* might still be inaccessible to User B because it is still a subdirectory of User A's home directory.

- You cannot use the chutils command to modify permissions for owner or world, although group permissions can be elevated to match owner permissions.

Location

The chutils command is located in the following directory:

```
app_server_root/instutils
```

Syntax

The chutils command syntax is as follows:

```
chutils.sh
  -installlocation=installation_directory
  -setowner=user_name
  -setgroup=group_name
  -setmod=[reset | grp2owner | patchperm]
  -help
  -debug
```

Parameters

The following options are available for the chutils command:

-installlocation=*installation_directory*
Specifies the absolute path to the installation root directory

This parameter is optional. It defaults to the current installation location, *app_server_root*.

-setowner=*user_name*
Sets the owner for each file and directory

-setgroup=*group_name*
Sets the group for each file and directory

-setmod=[reset | *grp2owner* | **patchperm]**
Sets the permissions on the files and directories

- `reset`

  Resets the owner, group, and other permissions to the default value of 755
- *grp2owner*

  Sets the group permission to match the owner permissions
- `patchperm`

  Does nothing in WebSphere Application Server Version 8 and later

-help
Displays the help

-debug
Displays additional runtime information

Mounting disk drives on operating systems such as AIX and Linux

Some operating systems such as AIX or Linux require you to mount the drive before you can access data on the product disk.

Before you begin

Insert the product disk into the drive before mounting the drive.

Note: You may experience errors if you install from a mounted ISO file created using a WebSphere Application Server product disk. Mount the drive that contains an official product disk or a product disk that was created from a licensed downloaded compressed file.

About this task

Use these procedures to mount the product disks for WebSphere Application Server.

Procedure

- AIX Mounting the DVD-ROM on AIX

  To mount the DVD-ROM on AIX using the System Management Interface Tool (SMIT), perform the following steps:

  1. Log in as a user with root authority.
  2. Insert the DVD-ROM in the drive.
  3. Create a DVD-ROM mount point by entering the `mkdir -p /cdrom` command, where `cdrom` represents the DVD-ROM mount point directory.
  4. Allocate a DVD-ROM file system using SMIT by entering the smit storage command.
  5. After SMIT starts, click **System Storage Management (Physical & Logical Storage)** > **File Systems** > **Add / Change / Show / Delete File Systems** > **CDROM File Systems** > **Add a CDROM File System**.
  6. In the Add a CDROM File System window:
     - Enter a device name for your DVD-ROM file system in the **DEVICE Name** field. Device names for DVD-ROM file systems must be unique. If there is a duplicate device name, you may need to delete a previously-defined DVD-ROM file system or use another name for your directory. The example uses `/dev/cd0` as the device name.
     - Enter the DVD-ROM mount point directory in the **MOUNT POINT** window. In our example, the mount point directory is `/cdrom`.
     - In the **Mount AUTOMATICALLY at system restart** field, select `yes` to enable automatic mounting of the file system.
     - Click **OK** to close the window, then click **Cancel** three times to exit SMIT.
  7. Next, mount the DVD-ROM file system by entering the smit mountfs command.
  8. In the Mount a File System window:
     - Enter the device name for this DVD-ROM file system in the **FILE SYSTEM name** field. In our example, the device name is `/dev/cd0`.
     - Enter the DVD-ROM mount point in the **Directory over which to mount** field. In our example, the mount point is /cdrom.
     - Enter `cdrfs` in the **Type of Filesystem** field. To view the other kinds of file systems you can mount, click List.
     - In the **Mount as READ-ONLY system** field, select `yes`.
     - Accept the remaining default values and click **OK** to close the window.

     Your DVD-ROM file system is now mounted. To view the contents of the DVD-ROM, place the disk in the drive and enter the cd /cdrom command where *cdrom* is the DVD-ROM mount point directory.

- HP-UX Mounting the DVD-ROM on HP-UX Because WebSphere Application Server contains several files with long file names, the mount command can fail. The following steps let you mount successfully your WebSphere Application Server product DVD-ROM on the HP-UX platform:

  1. Log in as a user with root authority.

2. In the `/etc` directory, add the following line to the `pfs_fstab` file:

```
/dev/dsk/c0t2d0 mount_point pfs-rrip ro,hard
```

   where *mount_point* represents the mount point of the DVD-ROM.

3. Start the *pfs* daemon by entering the following commands (if they are not already running):

```
/usr/sbin/pfs_mountd &
/usr/sbin/pfsd 4 &
```

4. Insert the DVD-ROM in the drive and enter the following commands:

```
mkdir /cdrom
/usr/sbin/pfs_mount /cdrom
```

   The */cdrom* variable represents the mount point of the DVD-ROM.

5. Log out.

- Linux Mounting the DVD-ROM on Linux To mount the DVD-ROM on Linux:

1. Log in as a user with root authority.
2. Insert the DVD-ROM in the drive and enter the following command:

```
mount -t iso9660 -o ro /dev/cdrom /cdrom
```

   The */cdrom* variable represents the mount point of the DVD-ROM.

   Note: If you have enabled and enforced Security-Enhanced Linux (SELinux) on your Red Hat Enterprise Linux Version 5 operating system while you are installing the product from the CD, then you must mount the CD with the following option. For more information see Preparing Red Hat Enterprise Linux 5 for installation.

```
-o context=system_u:object_r:textrel_shlib_t
```

3. Log out.

   Some window managers can automatically mount your DVD-ROM for you. Consult your system documentation for more information.

- Solaris Mounting the DVD-ROM on Solaris To mount the DVD-ROM on Solaris:

1. Log in as a user with root authority.
2. Insert the DVD-ROM into the drive.
3. If the Volume Manager is not running on your system, enter the following commands to mount the DVD-ROM:

```
mkdir -p /cdrom/unnamed_cdrom
mount -F hsfs -o ro /dev/dsk/c0t6d0s2 /cdrom/unnamed_cdrom
```

   The */cdrom/unnamed_cdrom* variable represents the DVD-ROM mount directory and the `/dev/dsk/c0t6d0s2` represents the DVD-ROM drive device.

   If you are mounting the DVD-ROM drive from a remote system using NFS, the DVD-ROM file system on the remote machine must be exported with root access. You must also mount that file system with root access on the local machine.

   If the Volume Manager (vold) is running on your system, the DVD-ROM is automatically mounted as:

```
/cdrom/unnamed_cdrom
```

4. Log out.

What to do next

Return to the installation procedure to continue.

Using the post-installer after updating or rolling back to a different service level

For z/OS systems, service that is applied to WebSphere Application Server occasionally requires corresponding changes to be made to the configuration file systems for existing application serving environments that were configured at a lower service level. For distributed operating systems, service that is applied to WebSphere Application Server occasionally requires corresponding changes to be made to the profile directory for existing application-serving environments that were created at a lower service level.

About this task

Most of these post-maintenance or post-installation updates can be performed automatically. This is done by the post-installer.

The WebSphere Application Server post-installer is a set of scripts that can be used to:

- Run configuration actions by Installation Manager at installation or uninstallation time
- Automatically detect the application or removal of fixpacks, and run any necessary configuration actions

The post-installation process is performed at the node level and must run against each node's WebSphere Application Server home directory after maintenance is applied to the product datasets and HFS and before the node is started. For more information about the post-installer and how to use it to apply or back out service to the configuration HFS, see "Completing post-installation tasks after updating or rolling back to a different service level."

Procedure

Perform the post-installation process in ether of two ways.

- Automatically by the post-installer

  A console message is displayed whenever the post-installation detects service to be applied. In some cases, some post-installation steps might still have to be performed manually. The post-installer will detect these situations and refuse to start the server.
- Manually

  You can run the post-installer yourself against each node's WebSphere Application Server home directory after installing maintenance and before starting the nodes.

Completing post-installation tasks after updating or rolling back to a different service level

This article describes post-installation tasks that you complete after applying a new service level.

About this task

The post-installation functionality includes actions that are performed at the following times:

- At installation time

  Installation Manager calls the post-installer for any non-profile related configuration actions using `positnstall.sh` or `positnstall.bat`. You can see a mention of the post-installer in the installation log.

  Installation manager considers the post-installation step a nonfatal one; therefore, it does not roll back the installation if the post-installer returns FAIL or PARTIAL SUCCESS. Installation manager will display `The packages are installed with warnings` at the end of the installation. If the post-installation action fails, run *app_server_root*`/bin/postinstall.sh` or *app_server_root*`/bin/postinstall.bat` with the following parameters (on one line):

```
-WS_CMT_CONF_DIR app_server_root/properties/postinstall/
-MASTER_ACTION_REGISTRY app_server_root/properties/postinstall/masterRegistry.xml
-SUB_ACTION_REGISTRY app_server_root/properties/postinstall/cacheRegistry.xml
-WS_PI_ACTION_REGISTRY_EXTENSION app_server_root/properties/postinstall/registryExtension.xml
-WS_CMT_LOG_HOME app_server_root/logs/postinstall/
-POSTINSTALL_LOG_FILE app_server_root/logs/postinstall/postinstall.log
```

Note: Application Client for IBM WebSphere Application Server and IBM HTTP Server for WebSphere Application Server also use the post-installer at installation time. If the post-installer fails, the installation completes with warnings just like for WebSphere Application Server and recovery is very similar. Simply replace `app_server_root` in the example with `app_client_root` or `IHS_root`.

- At server-startup time

  The `runConfigActions.sh` or `runConfigActions.bat` script runs before server startup. This script runs all the necessary configuration actions for all product fix packs and interim fixes that are installed in `app_server_root`.

  – If the script returns RC=0 (SUCCESS) or RC=2 (PARTIAL SUCCESS), the server starts.

  – If the script returns RC=1 (FAIL), the server does not start.

  If the `runConfigActions` script returns FAIL or PARTIAL SUCCESS, complete the following actions:

  1. Read the logs.

     The logs are in the following locations:

     Overall log for all products installed
     `profile_root/properties/service/productDir/runConfigActions.log`

     Log specific to WebSphere Application Server
     `profile_root/properties/service/productDir/WebSphere/logs/postinstall.log`

     Configuration-manager log specific to a run of the post-installer for WebSphere Application Server
     `profile_root/properties/service/productDir/WebSphere/logs/postinstallerConfigActionstimestamp.log`

     Log specific to a stack product or feature pack
     `profile_root/properties/service/productDir/product_name/logs/postinstall.log`

     Configuration-manager log specific to a run of the post-installer for a stack product or feature pack
     `profile_root/properties/service/productDir/product_name/logs/postinstallerConfigActionstimestamp.log`

     Log specific to an interim fix for a stack product or feature pack
     `profile_root/properties/service/productDir/product_name/iFixes/interim_fix_name/logs/postinstall.log`

     Configuration-manager log specific to a run of the post-installer for an interim fix for a stack product or feature pack
     `profile_root/properties/service/productDir/product_name/iFixes/interim_fix_name/logs/postinstallerConfigActionstimestamp.log`

  2. Fix any problems.

  3. Start the server again, or run `profile_root/bin/runConfigActions.sh` or `profile_root/bin/runConfigActions.bat`.

     The user running the script must have enough authority to update the profile—in other words, enough authority to start the server.

This applies to all platforms as well as any feature pack, interim fix, or stack product that requires post-installation tasks at server startup.

Procedure

- Run the post-installer automatically.

  This is running under the authority of the WebSphere Admin ID.
- Run the post-installer manually.

Cleaning your system after uninstalling the product

The uninstallation program leaves some files that can prevent you from reinstalling into the original directory. Delete files and registry entries to clean the machine so that you can reinstall into any directory. If you are not planning to reinstall the product, you do not have to clean your system.

About this task

You can reinstall the product 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.

Run one of the following procedures to produce a clean system.

Procedure

- AIX “Cleaning your AIX system after uninstalling the product”
- HP-UX “Cleaning your HP-UX system after uninstalling the product” on page 126
- Linux “Cleaning your Linux system after uninstalling the product” on page 127
- Solaris “Cleaning your Solaris system after uninstalling the product” on page 128
- Windows “Cleaning your Windows system after uninstalling the product” on page 129

Results

This procedure produces a clean system. A clean system has no evidence of a previously deleted installation.

Cleaning your AIX system after uninstalling the product

Uninstall a WebSphere Application Server product from an AIX system by running Installation Manager and then performing manual steps to remove log files and registry entries that can prevent you from reinstalling the product into the original directory. If you are not planning to reinstall, you do not have to clean your system.

Before you begin

The uninstallation program removes all profiles by default, including all of the configuration data and applications in each profile. Before you start the uninstallation procedure, back up the `config` folder, the `installableApps` folder, and the `installedApps` folder of each profile if necessary.

Determine the installation root directory for the product so that you remove the correct product and produce a clean system.

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 a WebSphere Application Server product. A clean system lets you reinstall the product into the original directory without coexistence.

Table 22. Default directories.

Default directories are shown in the following planning table:

Identifier	Default Directory
app_server_root	`/usr/IBM/WebSphere/AppServer`
profile_root	`/usr/IBM/WebSphere/AppServer/profiles`
plugins_root	`/usr/IBM/WebSphere/Plugins`

Installation Manager and the Profile Management Tool provide an override for your own locations for root directories.

Perform the following procedure to produce a clean system.

Procedure

1. Log on with the same user ID that was used to install the product.
2. Use Installation Manager to uninstall the Web Server Plug-ins.

   If a web server is configured to run with the application server, uninstall the plug-ins to remove the configuration from the web server.
3. Use the kill command to stop all Java processes that are running.

   If running Java processes are not related to WebSphere Application Server products and it is not possible to stop them, stop all WebSphere Application Server product-related processes. Use the following command to determine all processes that are running:

```
ps -ef | grep java
```

   Stop all WebSphere Application Server-related processes with the kill command.

```
kill -9 java_pid_1 java_pid_2...java_pid_n
```

4. Use Installation Manager to uninstall the product.
   - "Uninstalling the product from distributed operating systems using the GUI" on page 104
   - "Uninstalling the product from distributed operating systems silently" on page 105
5. Change directories to the `/usr/IBM` directory or the equivalent top directory of your installation.
6. Type `rm -rf` *`app_server_root`* to remove WebSphere Application Server directories in the *app_server_root* directory. Do not remove installation root directories for products that you intend to keep. Remove all of the profile directories as well.

Results

This procedure results in having a clean system. You can reinstall into the same directories now. A clean system has no trace of a previously deleted installation.

What to do next

Go to Chapter 3, "Task overview: Installing," on page 5 to begin planning a new installation.

Cleaning your HP-UX system after uninstalling the product

Uninstall a WebSphere Application Server product from an HP-UX system by running Installation Manager and then performing manual steps to remove log files and registry entries that can prevent you from reinstalling the product into the original directory. If you are not planning to reinstall, you do not have to clean your system.

Before you begin

The uninstallation program removes all profiles by default, including all of the configuration data and applications in each profile. Before you start the uninstallation procedure, back up the `config` folder, the `installableApps` folder, and the `installedApps` folder of each profile if necessary.

Determine the installation root directory for the product so that you remove the correct product and produce a clean system.

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 a WebSphere Application Server product. A clean system lets you reinstall the product into the original directory without coexistence.

Table 23. Default directories.

Default directories are shown in the following planning table:

Identifier	Default Directory
app_server_root	`/opt/IBM/WebSphere/AppServer`
profile_root	`/opt/IBM/WebSphere/AppServer/profiles`
plugins_root	`/opt/IBM/WebSphere/Plugins`

Installation Manager and the Profile Management Tool provide an override for your own locations for root directories.

Perform the following procedure to produce a clean system.

Procedure

1. Log on with the same user ID that was used to install the product.
2. Use Installation Manager to uninstall the Web Server Plug-ins.

   If a web server is configured to run with the application server, uninstall the plug-ins to remove the configuration from the web server.
3. Use the kill command to stop all Java processes that are running.

   If running Java processes are not related to WebSphere Application Server products and it is not possible to stop them, stop all WebSphere Application Server product-related processes. Use the following command to determine all processes that are running:

```
ps -ef | grep java
```

   Stop all WebSphere Application Server-related processes with the kill command.

```
kill -9 java_pid_1 java_pid_2...java_pid_n
```

4. Use Installation Manager to uninstall the product.
   - “Uninstalling the product from distributed operating systems using the GUI” on page 104
   - “Uninstalling the product from distributed operating systems silently” on page 105

5. Type `rm -rf app_server_root` to remove WebSphere Application Server directories in the *app_server_root* directory. Do not remove installation root directories for products that you intend to keep. Remove all of the profile directories as well.

Results

This procedure results in having a clean system. You can reinstall into the same directories now. A clean system has no trace of a previously deleted installation.

What to do next

Go to Chapter 3, “Task overview: Installing,” on page 5 to begin planning a new installation.

Cleaning your Linux system after uninstalling the product

Uninstall a WebSphere Application Server product from a Linux system by running Installation Manager and then performing manual steps to remove log files and registry entries that can prevent you from reinstalling the product into the original directory. If you are not planning to reinstall, you do not have to clean your system.

Before you begin

The uninstallation program removes all profiles by default, including all of the configuration data and applications in each profile. Before you start the uninstallation procedure, back up the `config` folder, the `installableApps` folder, and the `installedApps` folder of each profile if necessary.

Determine the installation root directory for the product so that you remove the correct product and produce a clean system.

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 a WebSphere Application Server product. A clean system lets you reinstall the product into the original directory without coexistence.

Table 24. Default directories.

Default directories are shown in the following planning table:

Identifier	**Default Directory**
app_server_root	`/opt/IBM/WebSphere/AppServer`
profile_root	`/opt/IBM/WebSphere/AppServer/profiles`
plugins_root	`/opt/IBM/WebSphere/Plugins`

Installation Manager and the Profile Management Tool provide an override for your own locations for root directories.

Perform the following procedure to produce a clean system.

Procedure

1. Log on with the same user ID that was used to install the product.
2. Use Installation Manager to uninstall the Web Server Plug-ins.

   If a web server is configured to run with the application server, uninstall the plug-ins to remove the configuration from the web server.
3. Use the kill command to stop all Java processes that are running.

If running Java processes are not related to WebSphere Application Server products and it is not possible to stop them, stop all WebSphere Application Server product-related processes. Use the following command to determine all processes that are running:

```
ps -ef | grep java
```

Stop all WebSphere Application Server-related processes with the kill command.

```
kill -9 java_pid_1 java_pid_2...java_pid_n
```

4. Use Installation Manager to uninstall the product.
   - "Uninstalling the product from distributed operating systems using the GUI" on page 104
   - "Uninstalling the product from distributed operating systems silently" on page 105
5. Type `rm -rf` *app_server_root* to remove WebSphere Application Server directories in the *app_server_root* directory. Do not remove installation root directories for products that you intend to keep. Remove all of the profile directories as well.

Results

This procedure results in having a clean system. You can reinstall into the same directories now. A clean system has no trace of a previously deleted installation.

What to do next

Go to Chapter 3, "Task overview: Installing," on page 5 to begin planning a new installation.

Cleaning your Solaris system after uninstalling the product

Install a WebSphere Application Server product from a Solaris system by running Installation Manager and then performing manual steps to remove log files and registry entries that can prevent you from reinstalling the product into the original directory. If you are not planning to reinstall, you do not have to clean your system.

Before you begin

The uninstallation program removes all profiles by default, including all of the configuration data and applications in each profile. Before you start the uninstallation procedure, back up the `config` folder, the `installableApps` folder, and the `installedApps` folder of each profile if necessary.

Determine the installation root directory for the product so that you remove the correct product and produce a clean system.

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 a WebSphere Application Server product. A clean system lets you reinstall the product into the original directory without coexistence.

Table 25. Default directories.

Default directories are shown in the following planning table:

Identifier	Default Directory
app_server_root	`/opt/IBM/WebSphere/AppServer`
profile_root	`/opt/IBM/WebSphere/AppServer/profiles`
plugins_root	`/opt/IBM/WebSphere/Plugins`

Installation Manager and the Profile Management Tool provide an override for your own locations for root directories.

Perform the following procedure to produce a clean system.

Procedure

1. Log on with the same user ID that was used to install the product.
2. Use Installation Manager to uninstall the Web Server Plug-ins.

   If a web server is configured to run with the application server, uninstall the plug-ins to remove the configuration from the web server.
3. Use the kill command to stop all Java processes that are running.

   If running Java processes are not related to WebSphere Application Server products and it is not possible to stop them, stop all WebSphere Application Server product-related processes. Use the following command to determine all processes that are running:

```
ps -ef | grep java
```

   Stop all WebSphere Application Server-related processes with the kill command.

```
kill -9 java_pid_1 java_pid_2...java_pid_n
```

4. Use Installation Manager to uninstall the product.
   - “Uninstalling the product from distributed operating systems using the GUI” on page 104
   - “Uninstalling the product from distributed operating systems silently” on page 105
5. Type `rm -rf` *`app_server_root`* to remove WebSphere Application Server directories in the *app_server_root* directory. Do not remove installation root directories for products that you intend to keep. Remove all of the profile directories as well.

Results

This procedure results in having a clean system. You can reinstall into the same directories now. A clean system has no trace of a previously deleted installation.

What to do next

Go to Chapter 3, “Task overview: Installing,” on page 5 to begin planning a new installation.

Cleaning your Windows system after uninstalling the product

Uninstall a WebSphere Application Server product from a Windows system by running Installation Manager and then performing manual steps to remove log files and registry entries that can prevent you from reinstalling the product into the original directory. If you are not planning to reinstall, you do not have to clean your system.

Before you begin

The uninstallation program removes all profiles by default, including all of the configuration data and applications in each profile. Before you start the uninstallation procedure, back up the `config` folder, the `installableApps` folder, and the `installedApps` folder of each profile if necessary.

Determine the installation root directory for the product so that you remove the correct product and produce a clean system.

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 a WebSphere Application Server product. A clean system lets you reinstall the product into the original directory without coexistence.

Table 26. Default directories.

Default directories are shown in the following planning table:

Identifier	**Default Directory**
app_server_root	`C:\Program Files\IBM\WebSphere\AppServer`
profile_root	`C:\Program Files\IBM\WebSphere\AppServer\profiles`
plugins_root	`C:\Program Files\IBM\WebSphere\Plugins`

Installation Manager and the Profile Management Tool provide an override for your own locations for root directories.

Perform the following procedure to produce a clean system.

Procedure

1. Log on with the same user ID that was used to install the product.
2. Use Installation Manager to uninstall the Web Server Plug-ins.

   If a web server is configured to run with the application server, uninstall the plug-ins to remove the configuration from the web server.
3. Stop any browsers and any Java processes related to WebSphere Application Server products.
4. Remove the application server service from the operating system.

   Stop the `IBM WebSphere Application Server V8.0 -` *`nodename`* service using the Windows Services panel, or run the WASService -stop command located in the *app_server_root*/`bin` directory. Then run the WASService -remove command to remove the service from the operating system.
5. Use Installation Manager to uninstall the product.
   - “Uninstalling the product from distributed operating systems using the GUI” on page 104
   - “Uninstalling the product from distributed operating systems silently” on page 105
6. Delete the installation root directory for the product that you are uninstalling.
7. Locate all of the profile directories and delete the directories if they were located outside of the *app_server_root* directory and were not deleted in the previous step.

Results

This procedure results in having a clean system. You can reinstall into the same directories now. A clean system has no trace of a previously deleted installation.

What to do next

Go to Chapter 3, “Task overview: Installing,” on page 5 to begin planning a new installation.

Chapter 7. Configuring the product after installation

Use the Profile Management Tool in the WebSphere Customization Toolbox to create a profile, and use the First steps console to test and verify your WebSphere Application Server environment.

Before you begin

Install the product.

Procedure

1. Start the Profile Management Tool to create a new profile.

   Tip: At the end of product installation, select **Profile Management Tool** if you want to open the Profile Management Tool when the installation is finished.

2. Start the First steps console for your server.

   Tip: At the end of profile creation, select **Launch the First steps console** if you want to open the First steps console for the profile when profile creation is finished. This First steps console belongs to the profile that you just created. Each profile has its own First steps console.

   The First steps console is an easy way to start using the product. The console provides access to the administrative console, WebSphere Customization Toolbox, installation verification test, and other activities.

   See the description of the “firststeps command” on page 221 for more information.

3. Click **Installation verification** on the First steps console.

   The installation verification test starts the server process and runs several tests to verify that the process can start without errors.

   See “Using the installation verification tool” on page 226 for more information.

4. Click **WebSphere Customization Toolbox** on the First steps console and use its tools to create a new profile or migrate a profile from an earlier version.

   You can create multiple servers on your system.

5. Use the administrative console to federate an application server into a deployment manager cell.

   If both server processes are running, use the administrative console of the deployment manager to add the application server node into the cell.

   Point your browser at `http://localhost:9060/ibm/console`, for example, to start the administrative console. Or start it from the First steps console of the deployment manager profile.

   Note: Vista Windows 7 If you are installing the product on these operating systems, then 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.

   Log in and click **System administration** > **Nodes** > **Add Node** and follow the wizard to add the node into the cell. You can use `localhost` for the Host field if both processes are on the same machine. The SOAP port for the application server node is 8880 unless you changed the port during profile creation.

   If the deployment manager is running, you can use the addNode command instead.

6. Optional: Click **WebSphere Customization Toolbox** on the First steps console and use the **Profile Management Tool** to create a custom profile.

   Verify that the deployment manager is running. The Profile Management Tool can federate the custom node for you if the deployment manager is running.

   Supply the host name and the SOAP port for the deployment manager while creating the custom profile.

Choose to federate the custom node into the deployment manager cell. A custom profile must be part of a cell.

Use the deployment manager to customize the node at your leisure. Add servers, add clusters, and install applications on the node for example.

Results

This procedure results in configuring and testing the application server environment.

What to do next

See Chapter 4, “Planning the WebSphere Application Server product installation,” on page 23 for diagrams of topologies that you can create using the Profile Management Tool.

Managing profiles on non-z/OS operating systems

You can create and delete profiles, which are sets of files that define the runtime environment. At least one profile must exist to run the product.

Before you begin

This task assumes a basic familiarity with the **manageprofiles** command, the Profile Management Tool, system commands, and profile concepts.

About this task

Typically, you create a profile after you install the product. Depending on which WebSphere Application Server product you have, you might create additional profiles.

You can create profiles using the Profile Management Tool or the **manageprofiles** command.

For the WebSphere Application Server, Network Deployment product, you can create any combination of profiles.

Linux HP-UX Solaris AIX Non-root users can create their own profiles so that they can manage their own application servers. Typically, non-root users manage application servers for development purposes.

You can delete profiles through the manageprofiles command or by other means if necessary. You might delete a profile if the configuration that you specified in the profile is not what you want.

Perform any of the following tasks to manage profiles.

Procedure

- Create profiles using the Profile Management Tool.
- Create profiles using the manageprofiles command.
- Delete profiles.

Results

You might have created or deleted a profile depending on the tasks that you completed.

What to do next

Depending on the action that you completed, you can start a server or proceed to other tasks such as deploying an application.

Profile concepts

A profile defines the runtime environment. The profile includes all the files that the server processes in the runtime environment and that you can change.

You can create a runtime environment either through the **manageprofiles** command or the Profile Management Tool graphical user interface. You can use the Profile Management Tool to enter most of the parameters that are described in this topic. Some parameters, however, require you to use the **manageprofiles** command. You must use the **manageprofiles** command to delete a profile, for instance, because the Profile Management Tool does not provide a deletion function. You can use either the Profile Management Tool or the **manageprofiles** command to create a cell profile. The Profile Management Tool creates the cell in a single step, whereas the **manageprofiles** command requires two separate invocations.

Core product files

The core product files are the shared product binary files, which are shared by all profiles.

The directory structure for the product has the following two major divisions of files in the installation root directory for the product:

- The core product files are shared product binary files that do not change unless you install a refresh pack, a fix pack, or an interim fix. Some log information is also updated.

  The following list shows default installation locations for root users on supported platforms:

  - AIX `/usr/IBM/WebSphere/AppServer`
  - Linux HP-UX Solaris `/opt/IBM/WebSphere/AppServer`
  - Windows `C:\Program Files\IBM\WebSphere\AppServer`
- The *app_server_root*/`profiles` directory is the default directory for creating profiles.

When you want binary files at different service levels, you must use a separate installation of the product for each service level.

The configuration for every defined application server process is within the `profiles` directory unless you specify a new directory when you create a profile. These files change as often as you create a new profile, reconfigure an existing profile, or delete a profile.

Each of the folders except for the `profiles` directory and a few others such as the `logs` directory and the `properties` directory do not change, unless you install service fixes. The `profiles` directory, however, changes each time you add, change, or delete a profile. The `profiles` directory is the default repository for profiles. However, you can put a profile anywhere on the machine or system, provided enough disk space is available.

If you create a profile in another existing folder in the installation root directory, then a risk exists that the profile might be affected by the installation of a service fix that applies maintenance to the folder. Use a directory outside of the installation root directory when using a directory other than the `profiles` directory for creating profiles.

Why and when to create a profile

The **manageprofiles** command-line tool defines each profile for the product.

Run the Profile Management Tool or the **manageprofiles** command each time that you want to create a profile. A need for more than one profile on a machine is common.

Administration is greatly enhanced when using profiles instead of multiple product installations. Not only is disk space saved, but updating the product is simplified when you maintain a single set of product core files. Also, creating new profiles is more efficient and less prone to error than full product installations, allowing a developer to create separate profiles of the product for development and testing.

You can run the Profile Management Tool or the command-line tool to create a new profile on the same machine as an existing profile. Define unique characteristics, such as profile name and node name, for the new profile. Each profile shares all runtime scripts, libraries, the Java SE Runtime Environment 6 (JRE 6) environment, and other core product files.

Profile types

Templates for each profile are located in the `*app_server_root*/profileTemplates` directory.

Multiple directories exist within this directory, which correspond to different profile types and vary with the type of product that is installed. The directories are the paths that you indicate while using the **manageprofiles** command with the -templatePath option. You can also specify profile templates that exist outside the `profileTemplates` directory, if you have any.

See the -templatePath parameter description in the **manageprofiles** command topic for more information.

The **manageprofiles** command in the WebSphere Application Server, Network Deployment product can create the following types of profiles:

Management profile with a deployment manager server

The basic function of the deployment manager is to deploy applications to a cell of application servers, which it manages. Each application server that belongs to the cell is a *managed node*.

You can create the management profile with a deployment manager server using the Profile Management Tool or the **manageprofiles** command. If you create the profile with the **manageprofiles** command, specify *app_server_root*/profileTemplates/management for the -templatePath parameter and DEPLOYMENT_MANAGER for the -serverType parameter.

Management profile with an administrative agent server

The basic function of the administrative agent is to provide a single interface to administer multiple unfederated application servers.

You can create the profile using the Profile Management Tool or the **manageprofiles** command. If you create the profile with the **manageprofiles** command, specify *app_server_root*/profileTemplates/management for the -templatePath parameter and ADMIN_AGENT for the -serverType parameter to create this type of management profile.

Management profile with a job manager server

The basic function of the job manager is to provide a single console to administer multiple base servers, multiple deployment managers, and do asynchronous job submission.

You can create the profile using the Profile Management Tool or the **manageprofiles** command. If you create the profile with the **manageprofiles** command, specify *app_server_root*/profileTemplates/management for the -templatePath parameter and JOB_MANAGER for the -serverType parameter to create this type of management profile.

Application server profile

Use the application server to make applications available to the Internet or to an intranet.

An important product feature is the ability to scale up a standalone application server profile by adding the application server node into a deployment manager cell. Multiple application server processes in a cell can deploy an application that is in demand. You can also remove an application server node from a cell to return the node to the status of a standalone application server.

Each standalone application server can optionally have its own administrative console application, which you use to manage the application server. You can also use the wsadmin scripting facility to perform every function that is available in the administrative console application.

No node agent process is available for a standalone application server node unless you decide to add the application server node to a deployment manager cell. Adding the application server node to a cell is known as *federation*. Federation changes the standalone application server node into a managed node. You use the administrative console of the deployment manager to manage the node. If you remove the node from the deployment manager cell, then use the administrative console and the scripting interface of the standalone application server node to manage the process.

You can create the profile using the Profile Management Tool or the **manageprofiles** command. If you create the profile with the **manageprofiles** command, specify `app_server_root/profileTemplates/default` for the -templatePath parameter to create this type of profile.

Cell profile

Use the cell profile to make applications available to the Internet or to an intranet under the management of the deployment manager.

Creation of a cell profile generates a deployment manager and a federated node in one iteration through the Profile Management Tool. The result is a fully functional cell on a given system.

To create a cell profile using the **manageprofiles** command, you must create two portions of the profile: the cell deployment manager portion and the cell node portion. Additionally, you can have only one cell deployment manager and one cell node associated with each other when you create a cell. The initial cell profile that you create with the **manageprofiles** command is equivalent to the cell profile you create with the Profile Management Tool. After you create the initial cell profile, you can create custom profiles or standalone profiles and federate the profiles into the deployment manager.

On the **manageprofiles** command, specify `app_server_root/profileTemplates/cell/dmgr` for the -templatePath parameter for the deployment manager and `app_server_root/profileTemplates/cell/default` for the -templatePath parameter for the cell node.

After you create the two portions that make up the cell profile, you have a deployment manager and federated node. The federated node contains an application server and the default application, which contains the snoop servlet, the HitCount application, and the HelloHTML servlet.

Custom profile

Use the custom profile, which belongs to a deployment manager cell, to make applications available to the Internet or to an intranet under the management of the deployment manager.

The deployment manager converts a custom profile to a managed node by adding the node into the cell. The deployment manager also converts an application server node into a managed node when you add an application server node into a cell. When either node is added to a cell, the node becomes a managed node. The node agent process is then instantiated on the managed node. The node agent acts on behalf of the deployment manager to control application server processes on the managed node. The node agent can start or stop application servers, for example.

A deployment manager can create multiple application servers on a managed node so long as the node agent process is running. Processes on the managed node can include cluster members that the deployment manager uses to balance the workload for heavily used applications.

Use the administrative console of the deployment manager to control all of the nodes that the deployment manager manages. You can also use the wsadmin scripting facility of the deployment manager to control any of the managed nodes. A custom profile does not have its own administrative console or scripting interface. You cannot manage the node directly with the wsadmin scripting facility.

A custom profile does not include default applications or a default server like the application server profile includes. A custom profile is an empty node. Add the node to the deployment manager cell. Then, you can use the administrative interface of the deployment manager to customize the managed node by creating clusters and application servers.

You can create the profile using the Profile Management Tool or the **manageprofiles** command. If you create the profile with the **manageprofiles** command, specify `*app_server_root*/profileTemplates/managed` for the -templatePath parameter to create this type of profile.

Secure proxy profile
Use the secure proxy server to take requests from the Internet and forward them to application servers. The secure proxy server resides in the DMZ.

Default profiles

Profiles use the concept of a default profile when more than one profile exists. The default profile is set to be the default target for scripts that do not specify a profile. You can use the -profileName parameter with most of the scripts to enable the scripts to act on a profile other than the default profile.

The default profile name is *<profile_type><profile_number>*:

- *<profile_type>* is a value of `AppSrv`, `Dmgr`, `Custom`, `AdminAgent`, `JobMgr`, or `SecureProxySrv`.
- *<profile_number>* is a sequential number that is used to create a unique profile name

Addressing a profile in a multiprofile environment: When multiple profiles exist on a machine, certain commands require that you specify the -profileName parameter if the profile is not the default profile. In those cases, it might be easier to use the commands that are in the `bin` directory of each profile. When you issue one of these commands within the `bin` directory of a profile, the command acts on that profile unless the -profileName parameter specifies a different profile.

Security policy for application server profiles

In environments where you plan to have multiple standalone application servers, the security policy of each application server profile is independent of the others. Changes to the security policy in one application server profile are not synchronized with the other profiles.

Installed file set

You decide where to install the files that define a profile.

The default location is in the `profiles` directory in the installation root directory. You can change the location on the Profile Management Tool or in a parameter when using the command-line tool. For example, assume that you create two profiles on a Linux platform with host name devhost1. The profile directories resemble the following example if you do not relocate them:

```
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01
/opt/IBM/WebSphere/AppServer/profiles/AppSrv02
```

You can specify a different directory, such as `/opt/profiles` for the profile directory using the **manageprofiles** command. For example:

```
manageprofiles.sh
   -profileName AppSrv01
   -profilePath /opt/profiles

manageprofiles.sh
   -profileName AppSrv02
   -profilePath /opt/profiles
```

Then the profile directories resemble the directories shown in the following example:

```
/opt/profiles/AppSrv01
/opt/profiles/AppSrv02
```

The following directories exist within a typical profile. This example assumes that the profile, AppSrv01, exists:

- *app_server_root*/profiles/AppSrv01/bin
- *app_server_root*/profiles/AppSrv01/config
- *app_server_root*/profiles/AppSrv01/configuration
- *app_server_root*/profiles/AppSrv01/etc
- *app_server_root*/profiles/AppSrv01/firststeps
- *app_server_root*/profiles/AppSrv01/installableApps
- *app_server_root*/profiles/AppSrv01/installedApps
- *app_server_root*/profiles/AppSrv01/installedConnectors
- *app_server_root*/profiles/AppSrv01/installedFilters
- *app_server_root*/profiles/AppSrv01/logs
- *app_server_root*/profiles/AppSrv01/properties
- *app_server_root*/profiles/AppSrv01/temp
- *app_server_root*/profiles/AppSrv01/wstemp

Profiles: File-system requirements

A minimum amount of space must be available in the directory where you create a profile.

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

Table 27. Space requirements.

This table shows space requirements for various profiles and server types.

Profile or server type	Space required
Application server	200 MB
Deployment manager	30 MB
Administrative agent	30 MB
Job manager	30 MB
Custom	10 MB
Cell	230 MB
Secure proxy	5 MB

Situations in which you could have insufficient file-system space

The Profile Management Tool and the **manageprofiles** command check that the amount of file-system space needed to create the profile is available right before profile creation begins. However, a slight chance exists that the profile creation can fail due to a lack of file-system space. This failure can occasionally occur in the following situations:

- Another user performs an action, such as copying files, that occupies file-system space at the same time that either the Profile Management Tool or the **manageprofiles** command writes to the file system.

- Another program writes to the disk at the same time that either the Profile Management Tool or the **manageprofiles** command writes to it to create a profile.
- The Profile Management Tool writes its logs and the profile that it creates to the same file system at the same time.
- The **manageprofiles** command writes its logs and the profile that it creates to the same file system at the same time.

Use the following recommendations to avoid profile creation failure:

- Ensure that enough temporary space is allocated for profile creation. Some temporary space is needed for the profile creation logs. These logs can be on a different file system than the file system on which the profile is created.
- Ensure no other program writes to the file-system space when either the Profile Management Tool or the **manageprofiles** command creates the profile.
- Ensure no user performs actions that occupy the file-system space when either the Profile Management Tool or the **manageprofiles** command creates the profile.

Differences between the manageprofiles command and the Profile Management tool when creating cell profiles

Both the **manageprofiles** command and the Profile Management tool can create a cell profile that has both a federated application server profile and a deployment manager profile. However, the Profile Management tool and the **manageprofiles** command create cell profiles differently. The differences are important to understand in terms of the available file-system space needed to create the cell profiles. You can create a cell profile in one pass through the Profile Management tool. In this case, you need 230 MB of available file-system space to create the cell profile. However, to create a cell profile using the**manageprofiles** command that is equivalent to the cell profile that the Profile Management tool creates, you must create two individual profiles, the cell deployment manager profile and the cell node profile. The cell deployment manager profile requires 30 MB of available file-system space, while the cell node profile requires 200 MB of available file-system space.

Managing profiles using commands

Use commands to create a profile, start the server of the profile, display ports used by your server, and open the administrative console.

Before you begin

This task assumes a basic familiarity with the command, other application server commands, and system commands.

Before you can create and use a profile, you must install the product.

About this task

Perform the following steps to create a profile, start the server of the profile, display ports used by your server, and open the administrative console for your server.

This example deals with the profile environment of a standalone application server.

Procedure

1. Create the server profile from the original installation:
   - Windows *app_server_root*\bin\manageprofiles.bat
   - Linux HP-UX Solaris AIX *app_server_root*/bin/manageprofiles.sh

Assume that you create the profile by using the defaults. The following script is an example for creating an application server profile:

- Windows `app_server_root\bin\manageprofiles.bat -create -templatePath app_server_root\profileTemplates\default`
- Linux HP-UX Solaris AIX `app_server_root/bin/manageprofiles.sh -create -templatePath app_server_root/profileTemplates/default`

2. Change directories to the *profile_root*`/bin` directory of the new server profile.
3. Start the server.

   Issue the startServer command.

   Windows

```
startServer.bat server1 -profileName profile_name
```

   Linux HP-UX Solaris AIX

```
startServer.sh server1 -profileName profile_name
```

   Note: The -profileName argument is not necessary if you have already changed to the *profile_root*`/bin` directory of the target profile.
4. Display the ports.

   These are the ports assigned during profile creation.

   Windows Open the portdef.props file in the *profile_root*\properties directory.

   Linux HP-UX Solaris AIX Open the portdef.props file in the *profile_root*/properties directory.
5. Open the administrative console.

   The server1 administrative console is defined on the WC_adminhost setting for the non-secure administrative console port or the WC_adminhost_secure setting for the secure administrative console port.

   If the value of the WC_adminhost port for your server is 20003, for example, specify the following web address in your browser:

```
http://host_name_or_IP_address:20003/ibm/console/
```

   If the value of the WC_adminhost_secure port for your server is 9061, for example, specify the following web address in your browser:

```
https://host_name_or_IP_address:9061/ibm/console/
```

Results

You created an application server profile, started an application server, and accessed the administrative console using your browser.

What to do next

Deploy an application.

manageprofiles command

Use the manageprofiles command to create, delete, augment, back up, and restore profiles, which define runtime environments. Using profiles instead of multiple product installations saves disk space and simplifies updating the product because a single set of core product files is maintained.

The manageprofiles command and its graphical user interface, the Profile Management Tool, are the only ways to create runtime environments.

The command file is located in the *app_server_root*`/bin` directory. The command file is a script named `manageprofiles`.

Remember: If you use this command with the managed profile template, application servers are not created. However, ports are still used if you are federating a node.

Syntax

The manageprofiles command is used to perform the following tasks:

- create a profile (-create)
- delete a profile (-delete)
- augment a profile (-augment)
- unaugment a profile (-unaugment)
- unaugment all profiles that have been augmented with a specific augmentation template (-unaugmentAll)
- delete all profiles (-deleteAll)
- list all profiles (-listProfiles)
- list augments for a profile (-listAugments)
- get a profile name (-getName)
- get a profile path (-getPath)
- validate a profile registry (-validateRegistry)
- validate and update a profile registry (-validateAndUpdateRegistry)
- get the default profile name (-getDefaultName)
- set the default profile name (-setDefaultName)
- back up a profile (-backupProfile)
- restore a profile (-restoreProfile)
- perform manageprofiles command tasks that are contained in a response file (-response)

For detailed help including the required parameters for each of the tasks accomplished with the manageprofiles command, use the `-help` parameter. The following example uses the help parameter with the manageprofiles `-augment` command on Windows operating systems:

```
app_server_root\bin\manageprofiles.bat -augment -help
```

The output from the help command will specify which parameters are required and which are optional.

Depending on the operation that you want to perform with themanageprofiles command, you need to provide one or more of the following parameters. The command-line 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 upper and lower case as the command-line tool does not validate the case of the parameter name. Incorrect results can occur when the parameter case is not typed correctly.

- -profileName *profile_name*
- -profilePath *profile_root*
- -templatePath *template_path*
- -nodeName *node_name*
- -cellName *cell_name*
- -hostName *host_name*
- -serverName *server_name*
- -adminUserName *adminUser_ID*
- -adminPassword *adminPassword*
- -appServerNodeName *application_server_node_name*
- -backupFile *backupFile_name*
- -dmgrAdminPassword *password*

- -dmgrAdminUserName *user_name*
- -dmgrProfilePath *dmgr_profile_path*
- -dmgrHost *dmgr_host_name*
- -dmgrPort *dmgr_port_number*
- -debug
- -enableAdminSecurity `true` | `false`
- -federateLater `true` | `false`
- -importPersonalCertKS *keystore_path*
- -importPersonalCertKSType *keystore_type*
- -importPersonalCertKSPassword *keystore_password*
- -importPersonalCertKSAlias *keystore_alias*
- -importSigningCertKS *keystore_path*
- -importSigningCertKSType *keystore_type*
- -importSigningCertKSPassword *keystore_password*
- -importSigningCertKSAlias *keystore_alias*
- -isDefault
- -isDeveloperServer
- -applyPerfTuningSetting `standard` | `production` | `development`
- -keyStorePassword *keystore_password*
- -listAugments
- -nodeDefaultPorts
- -nodePortsFile *node_ports_path*
- -nodeProfilePath*node_profile_path*
- -omitAction *feature1 feature2... featureN*
- -personalCertDN *distinguished_name*
- -personalCertValidityPeriod *validity_period*
- -response *response_file*
- -securityLevel *security_level*
- -serverType `DEPLOYMENT_MANAGER` | `ADMIN_AGENT` | `JOB_MANAGER`
- -signingCertDN *distinguished_name*
- -signingCertValidityPeriod *validity_period*
- -startingPort *starting_port* | -portsFile *file_path* | -defaultPorts
- -supportedProtocols *supported_protocols*
- -unaugmentAll
- -unaugmentDependents `true` | `false`
- -validatePorts
- -webServerCheck `true` | `false`
- -webServerHostname*webserver_host_name*
- -webServerInstallPath *webserver_installpath_name*
- -webServerName *webserver_name*
- -webServerOS *webserver_operating_system*
- -webServerPluginPath *webserver_plugin_path*
- -webServerPort *webserver_port*
- -webServerType *webserver_type*
- Linux -enableService `true` | `false`

- Linux -serviceUserName *service_user_ID*
- Windows -winserviceCheck `true` | `false`
- Windows -winserviceAccountType `specifieduser` | `localsystem`
- Windows -winservicePassword *winservice_password*
- Windows -winserviceStartupType `manual` | `automatic` | `disabled`
- Windows -winserviceUserName *winservice_user_ID*

The following example uses the manageprofiles `-create` command on operating systems such as AIX or Linux:

```
app_server_root/bin/manageprofiles.sh -create
   -profileName profile_name
   -profilePath profile_root
   -templatePath template_path
```

Parameters

The following options are available for the manageprofiles command:

-adminUserName *adminUser_ID*
Specify the user ID that is used for administrative security.

-adminPassword *adminPassword*
Specify the password for the administrative security user ID specified with the `-adminUserName` parameter.

-appServerNodeName *application_server_node_name*
Specifies the node name of the application server that you are federating into the cell. Specify this parameter when you create the deployment manager portion of the cell and when you create the application server portion of the cell.

-augment
Use the augment parameter to make changes to an existing profile with an augmentation template. The augment parameter causes the manageprofiles command 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.

Important: The templates that are included with the WebSphere Application Server Network Deployment product can only be used to create profiles and not to augment existing profiles because only create templates are shipped with the product.

Also, 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 -startingPort or -portsFile arguments on the manageprofiles command 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 template_path
```

You can specify a relative path for the `-templatePath` parameter if the profile templates are relative to the *app_server_root*/`profileTemplates` directory. Otherwise, specify the fully qualified template path. For example:

```
manageprofiles -augment -profileName profile_name -templatePath template_path
```

See also the `-unaugment` parameter.

-backupProfile
Performs a file system backup of a profile folder and the profile metadata from the profile registry file. Any servers using the profile that you want to back up must first be stopped prior to invoking the

manageprofiles command with the `-backupProfile` option. The `-backupProfile` parameter must be used with the `-backupFile` and `-profileName` parameters, for example:

```
manageprofiles(.bat)(.sh) -backupProfile -profileName profile_name -backupFile backupFile_name
```

When you back up a profile using the `-backupProfile` option, you must first stop the server and the running processes for the profile that you want to back up.

-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*.

-cellName *cell_name*
Specifies the cell name of the profile. Use a unique cell name for each profile.

Use a unique name even though you plan to federate the custom profile or stand alone profile into a deployment manager cell. Federation requires unique cell names before it can make the node part of the deployment manager cell. A cell name must be unique in any circumstance in which the product is running on the same physical machine or cluster of machines, such as a sysplex. Additionally, a cell name must be unique in any circumstance in which network connectivity between entities is required either between the cells or from a client that must communicate with each of the cells. Cell names must also be unique if their namespaces are federated. Otherwise, you might encounter symptoms such as a javax.naming.NameNotFoundException error, in which case, create uniquely named cells.

The default value for this parameter is based on a combination of the short host name, the constant cell, and a trailing number:

- Application server profile: Not any
- Custom profile: Not any
- Management profile with the deployment manager server: *shortHostName*Cell*CellNumber*
- Management profile with the job manager server: *shortHostName*JobMgrCell*CellNumber*
- Management profile with the administrative agent server: *shortHostName*AACell*CellNumber*
- Cell profile, application server portion: *shortHostName*Cell*CellNumber*
- Cell profile, deployment manager portion: *shortHostName*Cell*CellNumber*
- Secure proxy profile: Not any

where *CellNumber* is a sequential number starting at 01.

The value for this parameter must not contain spaces or any invalid characters that are not valid such as the following: *, ?, ", <, >, ,, /, \, |, and so on.

-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:

- cell - Deployment manager cell (dmgr and default)
- management - Management. Use in conjunction with the `-serverType` parameter to indicate the type of management profile.
- secureproxy- Secure proxy
- default - Application server
- managed - Custom

-debug
Turns on the debug function of the Ant utility, which the manageprofiles command uses.

-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.

`-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 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.

Remember: 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, suppose that you create a profile in the `/usr/WebSphere/AppServer/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 uninstall procedure.

If you delete a profile that has augmenting templates registered to it in the profile registry, then unaugment actions are performed automatically.

gotcha: If you are deleting an old node that has been migrated, shut down the new migrated deployment manager before deleting the old node. This will ensure that the new migrated node is not accidentally removed from the new migrated cell.

`-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/AppServer/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 uninstall procedure.

If you delete a profile that has augmenting templates registered to it in the profile registry, then unaugment actions are performed automatically.

`-dmgrAdminPassword` *`password`*

If you are federating a node, specify a valid user name for a deployment manager if administrative security is enabled on the deployment manager. Use this parameter with the -dmgrAdminUserName parameter and the -federateLater parameter.

`-dmgrAdminUserName` *`user_name`*

If you are federating a node, specify a valid password for a deployment manager if administrative security is enabled on the deployment manager. Use this parameter with the -dmgrAdminPassword parameter and the -federateLater parameter.

`-dmgrHost` *`dmgr_host_name`*

Identifies the machine where the deployment manager is running. Specify this parameter and the `dmgrPort` parameter to federate a custom profile as it is created.

The host name can be the long or short DNS name or the IP address of the deployment manager machine.

Specifying this optional parameter directs the manageprofiles command to attempt to federate the custom node into the deployment manager cell as it creates the custom profile with the managed -templatePath parameter. The -dmgrHost parameter is ignored when creating a deployment manager profile or an Application Server profile.

If you federate a custom node when the deployment manager is not running or is not available because of security being enabled or for other reasons, the installation indicator in the logs is INSTCONFFAIL to indicate a complete failure. The resulting custom profile is unusable. You must move the custom profile directory out of the profile repository (the profiles 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. 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 so on. 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. The deployment manager must be running and accessible.

If you have enabled security or changed the default Java Management Extensions (JMX) connector type, you cannot federate with the manageprofiles command. 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.

`-dmgrProfilePath` *`dmgr_profile_path`*

Specifies the profile path to the deployment manager portion of the cell. Specify this parameter when you create the application server portion of the cell.

`-enableAdminSecurity true | false`

Enables administrative security. Valid values include `true` or `false`. The default value is `false`.

When `enableAdminSecurity` is set to `true`, you must also specify the parameters -`adminUserName` and -`adminPassword` along with the values for these parameters.
You cannot use the -enableAdminSecurity parameter to enable administrative security for a custom profile. For security to be enabled for a custom profile, the custom profile must be federated into a deployment manager. Administrative security enabled for the deployment manager is required to enable security for the federated custom profile.

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`.

When the manageprofiles command 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 non-root user runs the manageprofiles command, the profile is created, but the Linux service is not. The Linux service is not created because the non-root 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 *`app_server_root`*`/logs/manageprofiles_create`*`profilename`*`.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 the `dmgrHost`, `dmgrPort`, `dmgrAdminUserName` and `dmgrAdminPassword` parameters do not have values, the default value for this parameter is `true`. Valid values include `true` or `false`.

-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. 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. 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 so on.

-ignoreStack
An optional parameter that is used with the -templatePath parameter to unaugment a particular profile that has been augmented. See the -unaugment parameter.

-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.

Note: When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the manageprofiles command 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 that the server is intended for development purposes only. This parameter is useful when creating profiles to test applications on a non-production server before deploying the applications on their production application servers.

This parameter is valid only for the default profile template.

If you specify both the **-isDeveloperServer** and **-applyPerfTuningSetting** parameters, depending on the option selected for **-applyPerfTuningSetting**, **-applyPerfTuningSetting** might override **-isDeveloperServer**.

-applyPerfTuningSetting *option*
Specifies the performance-tuning setting that most closely matches the type of environment in which the application server will run.

This parameter is only valid for the default profile template.

standard
The standard settings are the standard out-of-the-box default configuration settings that are optimized for general-purpose usage.

production
The production performance settings are optimized for a production environment where application changes are rare and optimal runtime performance is important.

development
The development settings are optimized for a development environment where frequent application updates are performed and system resources are at a minimum.

Important: Do not use the development settings for production servers.

If you specify both the **-isDeveloperServer** and **-applyPerfTuningSetting** parameters, depending on the option selected for **-applyPerfTuningSetting**, **-applyPerfTuningSetting** might override **-isDeveloperServer**.

-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.

-nodeDefaultPorts

Defines a set of ports when creating a profile in conjunction with a cell template. If you specify this option, you cannot specify the -nodePortsFile or nodeStartingPort options at the same time.

-nodePortsFile *node_ports_path*

Specifies ports for the node portion of the cell that you are creating. If you specify this option, you cannot specify the -nodeDefaultPorts or -nodeStartingPort options at the same time.

-nodeProfilePath *node_profile_path*

Specifies the profile path to the node portion of the cell. Specify this parameter when you create the deployment manager portion of the cell.

-nodeName *node_name*

Specifies the node name for the node that is created with the new profile. Use a unique value within the cell or on the machine. Each profile that shares the same set of product binaries must have a unique node name.

The default value for this parameter is based on the short host name, profile type, and a trailing number:

- Application server profile: *shortHostName*Node*NodeNumber*
- Custom profile: *shortHostName*Node*NodeNumber*
- Management profile with the deployment manager server: *shortHostName*CellManager*NodeNumber*
- Management profile with the job manager server: *shortHostName*JobMgr*NodeNumber*
- Management profile with the administrative agent server: *shortHostName*AANode*NodeNumber*
- Cell profile, application server portion: *shortHostName*Node*NodeNumber*
- Cell profile, deployment manager portion: *shortHostName*CellManager*NodeNumber*
- Secure proxy profile: *shortHostName*Node*NodeNumber*

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 so on.

-omitAction *feature1 feature2... featureN*

An optional parameter that excludes profile features.

Each profile template comes predefined with certain optional features. The following optional features can be used with the `-omitAction` parameter for the following profile templates:

- default - Application server
  - deployAdminConsole
  - defaultAppDeployAndConfig
- management - Management profile for the deployment manager, administrative agent, or job manager
  - deployAdminConsole
- cell - Deployment manager cell which is composed of both a dmgr and a default profile template
  - cell_dmgr (dmgr created during cell profile creation)
    - deployAdminConsole
    - defaultAppDeployAndConfig

-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 quotes. 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.

-portsFile *file_path*

An optional parameter that specifies the path to a file that defines port settings for the new profile.

Do not use this parameter when using the `-startingPort` or `-defaultPorts` parameter.

During profile creation, the manageprofiles command 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:

```
<profile_type><profile_number>
```

where

- *<profile_type>* is a value such as `AppSrv`, `Dmgr`, `AdminAgent`, `JobMgr`, or `Custom`
- *<profile_number>* 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 any of the following: *, ?, ", <, >,,, /, \, |, and so on.

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 as the *profile_root*.

Specify the full path to avoid an Ant scripting limitation that can cause a failure when federating the profile into a cell. For example:

```
-profilePath profile_root
```

Windows If the fully qualified path contains spaces, enclose the value in quotation marks.

The default value is based on the *app_server_root* directory, the profiles subdirectory, and the name of the profile.

For example, the default is:

```
WS_WSPROFILE_DEFAULT_PROFILE_HOME/profileName
```

The *WS_WSPROFILE_DEFAULT_PROFILE_HOME* element is defined in the `wasprofile.properties` file in the *app_server_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 *reponse_file*

Accesses all API functions from the command line using the manageprofiles command.

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. Use the following example response file to run a create operation:

```
create
profileName=testResponseFileCreate
profilePath=profile_root
templatePath=app_server_root/profileTemplates/default
nodeName=myNodeName
cellName=myCellName
hostName=myHostName
omitAction=myOptionalAction1,myOptionalAction2
```

Windows 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\\AppServer\\profileTemplates\\default
```

The best practice is to use forward slashes in order to reduce the chance of errors when switching between platforms.

To determine which input arguments are required for the various types of profile templates and action, use the manageprofiles command with the -help parameter.

-restoreProfile
Restores a profile backup. Must be used with the `-backupFile` parameter, for example:

```
manageprofiles(.bat)(.sh) -restoreProfile -backupFile file_name
```

To restore a profile, perform the following steps:

1. Stop the server and the running processes for the profile that you want to restore.
2. Manually delete the directory for the profile from the file system.
3. Run the `-validateAndUpdateRegistry` option of the manageprofiles command.
4. Restore the profile by using the `-restoreProfile` option of the manageprofiles command.

-securityLevel *security_level*
Specifies the initial security level settings for the secure proxy server. Valid values are `low`, `medium`, and `high`. The default value is `high`. The security level is based on startup user permissions, routing considerations, administration options, and error handling. You can optionally change your security settings after you create the secure proxy server profile.

-serverName *server_name*
Specifies the name of the server. Specify this parameter only for the default and secureproxy templates. If you do not specify this parameter when using the default or secureproxy templates, the default server name is server1 for the default profile, and proxy1 for the secure proxy profile.

-serverType DEPLOYMENT_MANAGER | ADMIN_AGENT | JOB_MANAGER
Specifies the type of management profile. Specify `DEPLOYMENT_MANAGER` for a deployment manager server, `ADMIN_AGENT` for an administrative agent server, or `JOB_MANAGER` for a job manager server. This parameter is required when you create a management profile.

Linux **-serviceUserName** *service_user_ID*
Specify the user ID that is used during the creation of the Linux service so that the Linux service runs from 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:

```
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 quotes. 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 15 years.

-startingPort *startingPort*

Specifies the starting port number for generating and assigning all ports for the 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 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.

Attention: Do not use this parameter if you are using the managed profile template.

-supportedProtocols *supported_protocols*

Specifies the protocols that are valid for the secure proxy server to proxy requests. Valid values are `SIP`, `HTTP`, and `HTTP,SIP`.

-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 happen to have any.

You can specify a relative path for the `-templatePath` parameter if the profile templates are relative to the*app_server_root*/`profileTemplates` directory. Otherwise, specify the fully qualified template path. F

-unaugment

Augmentation is the ability to change an existing profile with an augmentation template. To unaugment a profile that has been augmented, you must specify the -unaugment parameter and the -profileName parameter. If a series of manageprofiles augmentations were performed, and you specify only these two parameters to unaugment a profile, the unaugment action undoes the last augment action first.

To unaugment a particular profile that has been augmented, additionally specify the -ignoreStack parameter with the -templatePath parameter. Normally, you would not unaugment a particular profile because you must ensure that you are not violating profile template dependencies.

When using the -templatePath parameter, specify the fully qualified file path for the parameter.

See also the augment parameter.

-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 that 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.

-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`.

-webServerHostname *webserver_host_name*

The host name of the server. The default value for this parameter is the long host name of the local machine.

-webServerInstallPath *webserver_installpath_name*

The installation path of the web server, local or remote. The default value for this parameter is dependent on the operating system of the local machine and the value of the `webServerType` parameter. For example: 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"
```

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"
```

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"
```

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"
```

-webServerName *webserver_name*

The name of the web server. The default value for this parameter is webserver1.

-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.

-webServerPluginPath *webserver_pluginpath*

The path to the plug-ins that the web server uses. The default value for this parameter is *WAS_HOME*/plugins.

-webServerPort *webserver_port*

Indicates the port from where the web server will be accessed. The default value for this parameter is 80.

-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.

Windows **-winserviceAccountType specifieduser | localsystem**

The type of the owner account of the Windows service created for the profile. 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 localsystem.

If the value is specifieduser, the winservicePassword parameter is required. The winserviceUserName parameter defaults to the environment username value if not specified.

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`.

Important: With a custom profile, you cannot create a Windows service with this parameter. Instead, use the WASService command to create the service separately.

Windows **-winservicePassword** *winservice_password*

Specify the password for the specified user or the local account that is to own the Windows service.

Windows **-winserviceStartupType manual | automatic | disabled**

Possible startup_type values are:

- manual
- automatic
- disabled

See the WASService command topic in the *Setting up the application serving environment* PDF for more information about Windows services.

The default value for this parameter is automatic.

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:

- Exist 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 so on. 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.

Usage scenario

The following examples demonstrate correct syntax. Issue the command in any of the following examples on one line. Each example shows the command on more than one line to increase clarity.

- Creating a deployment manager

  The following example uses the management template to create a deployment manager named Dmgr001. The deployment manager ports start at port number 20000.

  Linux AIX HP-UX Solaris

```
app_server_root/bin/manageprofiles.sh -create
   -profileName Dmgr001
   -profilePath profile_root
   -templatePath app_server_root/profileTemplates/management
   -serverType DEPLOYMENT_MANAGER
   -nodeName Dmgr001Node
   -cellName Dmgr001NodeCell
   -hostName localhost
   -isDefault
   -startingPort 20000
```

Windows

```
app_server_root\bin\manageprofiles.bat -create
   -profileName Dmgr001
   -profilePath profile_root
   -templatePath app_server_root\profileTemplates\management
   -serverType DEPLOYMENT_MANAGER
   -nodeName Dmgr001Node
   -cellName Dmgr001NodeCell
   -hostName localhost
   -isDefault
   -startingPort 20000
```

- Creating an administrative agent

  The following example uses the management template to create an administrative agent named AdminAgent001. The administrative agent ports start at port number 24000.

  Linux AIX HP-UX Solaris

```
app_server_root/bin/manageprofiles.sh -create
   -profileName AdminAgent001
   -profilePath profile_root
   -templatePath app_server_root/profileTemplates/management
   -serverType ADMIN_AGENT
   -nodeName AdminAgent001Node
   -hostName localhost
   -isDefault
   -startingPort 24000
```

Windows

```
app_server_root\bin\manageprofiles.bat -create
   -profileName AdminAgent001
   -profilePath profile_root
   -templatePath app_server_root\profileTemplates\management
   -serverType ADMIN_AGENT
   -nodeName AdminAgent001Node
   -hostName localhost
   -isDefault
   -startingPort 24000
```

- Creating a job manager

  The following example uses the management template to create a job manager named JobMgr001. The job manager ports start at port number 25000.

  Linux AIX HP-UX Solaris

```
app_server_root/bin/manageprofiles.sh -create
   -profileName JobMgr001
   -profilePath profile_root
   -templatePath app_server_root/profileTemplates/management
   -serverType JOB_MANAGER
   -nodeName JobMgr001Node
   -cellName JobMgr001NodeCell
   -hostName localhost
   -isDefault
   -startingPort 25000
```

Windows

```
app_server_root\bin\manageprofiles.bat -create
   -profileName JobMgr001
   -profilePath profile_root
   -templatePath app_server_root\profileTemplates\management
   -serverType JOB_MANAGER
   -nodeName JobMgr001Node
   -cellName JobMgr001NodeCell
   -hostName localhost
   -isDefault
   -startingPort 25000
```

- Creating a secure proxy

The following example uses the secureproxy template to create a secure proxy named SecureProxySrv001. The secure proxy ports start at port number 26000.

Linux AIX HP-UX Solaris

```
app_server_root/bin/manageprofiles.sh -create
   -profileName SecureProxySrv001
   -profilePath profile_root
   -templatePath app_server_root/profileTemplates/secureproxy
   -nodeName SecureProxySrv001Node
   -serverName secproxy1
   -hostName localhost
   -isDefault
   -startingPort 26000
```

Windows

```
app_server_root\bin\manageprofiles.bat -create
   -profileName SecureProxySrv001
   -profilePath profile_root
   -templatePath app_server_root\profileTemplates\secureproxy
   -nodeName SecureProxySrv001Node
   -serverName secproxy1
   -hostName localhost
   -isDefault
   -startingPort 26000
```

- Creating a custom profile

  The following example creates a custom profile and federates the profile into the deployment manager cell.

  Linux AIX HP-UX Solaris

```
app_server_root/bin/manageprofiles.sh -create
   -profileName Custom01
   -profilePath profile_root
   -templatePath app_server_root/profileTemplates/managed
   -nodeName Custom01Node
   -cellName Custom01Cell
   -hostName myhost.mycity.mycompany.com
   -isDefault
   -dmgrHost myhost.mycity.mycompany.com
   -dmgrPort 8879
   -startingPort 22000
```

  Windows

```
c:\WebSphere\AppServer\bin manageprofiles.bat -create
   -profileName Custom01
   -profilePath profile_root
   -templatePath app_server_root\profileTemplates\managed
   -nodeName CustomNode01
   -cellName CustomNodeCell01
   -hostName myhost.mycity.mycompany.com
   -isDefault
   -dmgrHost myhost.mycity.mycompany.com
   -dmgrPort 8879
   -startingPort 22000
```

- Creating an application server profile

  Create an application server profile named Default01 with the following command.

  Windows The command also creates a Windows service for the application server, personal and root signing certificates for the profile, and a keystore password for the two certificates.

```
app_server_root\bin manageprofiles.bat -create
   -profileName Default01
   -profilePath profile_root
   -templatePath app_server_root\profileTemplates\default
   -nodeName Default01Node
   -cellName Default01Cell
   -hostName myhost.mycity.mycompany.com
   -isDefault
   -winserviceCheck true
   -winserviceAccountType specifieduser
   -winserviceUserName my_user_id
   -winservicePassword my_password
   -winserviceStartupType manual
   -startingPort 21000
   -personalCertDN "cn=testa, ou=Rochester, o=IBM, c=US"
   -signingCertDN "cn=testc, ou=Rochester, o=IBM, c=US"
   -keyStorePassword ap3n9krw
```

  Linux AIX HP-UX Solaris

```
app_server_root/bin/manageprofiles.sh -create
   -profileName Default01
   -profilePath profile_root
   -templatePath app_server_root/profileTemplates/default
   -nodeName Default01Node
   -cellName Default01Cell
   -hostName myhost.mycity.mycompany.com
   -isDefault
   -startingPort 21000
   -personalCertDN "cn=testa, ou=Rochester, o=IBM, c=US"
   -signingCertDN "cn=testc, ou=Rochester, o=IBM, c=US"
   -keyStorePassword ap3n9krw
```

- Creating a cell profile

  Creating a cell profile requires the creation of both the deployment manager and the application server portion of the cell profile. The two profiles are linked and some parameters must match between the creation parameters of the deployment manager and the application server portion of the cell profile.

  Important: For both the deployment manager and the application server portion of the cell profile, you must use the same values for the `cellName`, `nodeName`, and `appServerNodeName` parameters. If you did not specify names for these parameters when you created the deployment manager portion of the cell profile, you must use the default name that was assigned in the first command-line invocation. The illustration immediately below shows the use of identical values for these parameters in the deployment manager and the application server portions of the cell profile.

```
For Dmgr:
-cellName host01Cell01
-nodeName host01CellManager01
-appServerNodeName host01Node01

For AppServer:
-cellName host01Cell01
-nodeName host01CellManager01
-appServerNodeName host01Node01
```

  The following example shows the creation of a cell profile named *Dmgr001* having a cell name of *Default01Cell* and a node name of *Default01Node*. To create a full working cell, the `-nodeProfilePath`, `-cellName`, `-appServerNodeName`, `-nodeName` parameters are required to match between the cell_dmgr profile and the cell_node profile.

  1. Create the deployment manager portion of the cell profile.

     Windows

```
app_server_root\bin\manageprofiles.bat -create
   -templatePath app_server_root\profileTemplates\cell\dmgr
   -nodeProfilePath app_server_root\profiles\AppSrv01
   -profileName Dmgr001
   -cellName Default01Cell
   -nodeName Default01Node
   -appServerNodeName Default02Node
```

     Linux HP-UX Solaris AIX

```
app_server_root/bin/manageprofiles.sh -create
   -templatePath app_server_root/profileTemplates/cell/dmgr
   -nodeProfilePath app_server_root/profiles/AppSrv01
   -profileName Dmgr001
   -cellName Default01Cell
   -nodeName Default01Node
   -appServerNodeName Default02Node
```

  2. Create the application server portion of the cell profile.

     Windows

```
app_server_root\bin\manageprofiles.bat -create
   -templatePath app_server_root\profileTemplates\cell\default
   -dmgrProfilePath app_server_root\profiles\Dmgr001
   -portsFile app_server_root\profiles\Dmgr001\properties\portdef.props
   -nodePortsFile app_server_root\profiles\Dmgr001\properties\nodeportdef.props
   -profileName AppSrv01
   -cellName Default01Cell
   -nodeName Default01Node
   -appServerNodeName Default02Node
```

     Linux HP-UX Solaris AIX

```
app_server_root/bin/manageprofiles.sh -create
   -templatePath app_server_root/profileTemplates/cell/default
   -dmgrProfilePath app_server_root/profiles/Dmgr001
   -portsFile app_server_root/profiles/Dmgr001/properties/portdef.props
   -nodePortsFile app_server_root/profiles/Dmgr001/properties/nodeportdef.props
   -profileName AppSrv01
   -cellName Default01Cell
   -nodeName Default01Node
   -appServerNodeName Default02Node
```

Logs

The manageprofiles command creates a log for every profile that it creates.

- The logs are in the *app_server_root*/logs/manageprofiles directory. The files are named in this pattern: *profile_name*_create.log.
- The command also creates a log for every profile that it deletes. The logs are in the *app_server_root*/logs/manageprofiles directory. The files are named in this pattern: *profile_name*_delete.log.

Example: Creating deployment manager profiles

You can create a deployment manager profile after installing your core product files. The deployment manager provides a single administrative interface to a logical group of application servers on one or more machines. Use the manageprofiles.sh -create command to create a deployment manager profile.

To create a deployment manager profile named shasti:

AIX HP-UX Linux Solaris

```
manageprofiles.sh -create
              -profileName shasti
              -profilePath /shasti/WebSphere
              -templatePath /opt/IBM/WebSphere/AppServer/profileTemplates/management
              -serverType DEPLOYMENT_MANAGER
              -cellName cell1
              -hostName planetaix
              -nodeName dmgr1
```

Windows

```
manageprofiles.bat -create
              -profileName shasti
              -profilePath C:\shasti\WebSphere
              -templatePath C:\IBM\WebSphere\AppServer\profileTemplates\management
              -serverType DEPLOYMENT_MANAGER
              -cellName cell1
              -hostName planetnt
              -nodeName dmgr1
```

The command creates a deployment manager profile named shasti in a cell named cell1 with a node name of dmgr1 in the following location:

- AIX HP-UX Linux Solaris /shasti/WebSphere
- Windows C:\shasti\WebSphere

If you do not specify one of the port options during profile creation, a recommended set of port values will be used. The port conflict resolution algorithm determines these ports. The recommended set of ports must be free of conflict. If you want to use the IBM default ports, use the -defaultPorts option when you create a profile.

Example: Incrementing default port numbers from a starting point

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

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

For example, ports created with -startingPort 20002 would appear similar to the following example:

Assigned ports for an application server profile

```
WC_defaulthost=20002
WC_adminhost=20003
WC_defaulthost_secure=20004
WC_adminhost_secure=20005
BOOTSTRAP_ADDRESS=20006
SOAP_CONNECTOR_ADDRESS=20007
IPC_CONNECTOR_ADDRESS=20008
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=20009
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=20010
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=20011
ORB_LISTENER_ADDRESS=20012
CELL_DISCOVERY_ADDRESS=20013
NODE_MULTICAST_DISCOVERY_ADDRESS=20014
NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS=20015
NODE_DISCOVERY_ADDRESS=20016
DCS_UNICAST_ADDRESS=20017
SIB_ENDPOINT_ADDRESS=20018
SIB_ENDPOINT_SECURE_ADDRESS=20019
SIB_MQ_ENDPOINT_ADDRESS=20020
SIB_MQ_ENDPOINT_SECURE_ADDRESS=20021
SIP_DEFAULTHOST=20022
SIP_DEFAULTHOST_SECURE=20023
```

Assigned ports for a custom profile

```
BOOTSTRAP_ADDRESS=20002
SOAP_CONNECTOR_ADDRESS=20003
IPC_CONNECTOR_ADDRESS=20004
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=20005
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=20006
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=20007
ORB_LISTENER_ADDRESS=20008
NODE_MULTICAST_DISCOVERY_ADDRESS=20009
NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS=20010
NODE_DISCOVERY_ADDRESS=20011
DCS_UNICAST_ADDRESS=20012
```

Assigned ports for a cell with a federated application server profile

```
WC_defaulthost=20002
WC_defaulthost_secure=20003
BOOTSTRAP_ADDRESS=20004
SOAP_CONNECTOR_ADDRESS=20005
IPC_CONNECTOR_ADDRESS=20006
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=20007
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=20008
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=20009
ORB_LISTENER_ADDRESS=20010
DCS_UNICAST_ADDRESS=20011
SIB_ENDPOINT_ADDRESS=20012
SIB_ENDPOINT_SECURE_ADDRESS=20013
SIB_MQ_ENDPOINT_ADDRESS=20014
SIB_MQ_ENDPOINT_SECURE_ADDRESS=20015
SIP_DEFAULTHOST=20016
SIP_DEFAULTHOST_SECURE=20017
NODE_MULTICAST_DISCOVERY_ADDRESS=20018
NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS=20019
NODE_DISCOVERY_ADDRESS=20020
NODE_DCS_UNICAST_ADDRESS=20021
NODE_BOOTSTRAP_ADDRESS=20022
NODE_SOAP_CONNECTOR_ADDRESS=20023
NODE_ORB_LISTENER_ADDRESS=20024
NODE_SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=20025
NODE_CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=20026
NODE_CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=20027
NODE_IPC_CONNECTOR_ADDRESS=20028
```

Assigned ports for a cell with a deployment manager profile

```
WC_adminhost=20002
WC_adminhost_secure=20003
BOOTSTRAP_ADDRESS=20004
SOAP_CONNECTOR_ADDRESS=20005
IPC_CONNECTOR_ADDRESS=20006
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=20007
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=20008
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=20009
ORB_LISTENER_ADDRESS=20010
CELL_DISCOVERY_ADDRESS=20011
DCS_UNICAST_ADDRESS=20012
```

Assigned ports for a management profile with a deployment manager server

```
WC_adminhost=20002
WC_adminhost_secure=20003
BOOTSTRAP_ADDRESS=20004
SOAP_CONNECTOR_ADDRESS=20005
IPC_CONNECTOR_ADDRESS=20006
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=20007
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=20008
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=20009
ORB_LISTENER_ADDRESS=20010
CELL_DISCOVERY_ADDRESS=20011
DCS_UNICAST_ADDRESS=20012
DataPowerMgr_inbound_secure=20013
```

Assigned ports for a management profile with a job manager server

```
WC_adminhost=20002
WC_adminhost_secure=20003
BOOTSTRAP_ADDRESS=20004
SOAP_CONNECTOR_ADDRESS=20005
IPC_CONNECTOR_ADDRESS=20006
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=20007
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=20008
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=20009
ORB_LISTENER_ADDRESS=20010
```

Assigned ports for a management profile with an administrative agent server

```
WC_adminhost=20002
WC_adminhost_secure=20003
BOOTSTRAP_ADDRESS=20004
SOAP_CONNECTOR_ADDRESS=20005
IPC_CONNECTOR_ADDRESS=20006
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=20007
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=20008
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=20009
ORB_LISTENER_ADDRESS=20010
```

Assigned ports for a management profile with an administrative agent server

```
SOAP_CONNECTOR_ADDRESS=20002
IPC_CONNECTOR_ADDRESS=20003
```

Assigned ports for a secure proxy profile

```
PROXY_HTTP_ADDRESS=20002
PROXY_HTTPS_ADDRESS=20003
PROXY_SIP_ADDRESS=20004
PROXY_SIPS_ADDRESS=20005
IPC_CONNECTOR_ADDRESS=20006
```

The following example uses the startingPort parameter of the manageprofiles command and creates ports from an initial value of 20002, with the content shown in the previous example: Windows

```
manageprofiles.bat -create
              -profileName shasti
              -profilePath G:\shasti\WebSphere
              -templatePath G:\shasti\WebSphere\profileTemplates\default
              -nodeName W2K03
              -cellName W2K03_Cell01
              -hostName planetnt
              -startingPort 20002
```

Linux HP-UX Solaris AIX

```
app_server_root/bin/manageprofiles.sh -create
              -profileName shasti
              -profilePath app_server_root/profiles/shasti
              -templatePath app_server_root/profileTemplates/default
              -nodeName W2K03
              -cellName W2K03_Cell01
              -hostName planetnt
              -startingPort 20002
```

Example: Creating cell profiles

To create the cell profile using the manageprofiles command, you must create both the cell management profile for a deployment manager server and the cell node profile using two different manageprofiles command-line invocations. The combination of these two profiles is the cell profile.

Two templates are used to create the cell profile: cell_dmgr and cell_node. The templates are linked and some parameters must match between the creation parameters in these two invocations. Verify that the invocations match.

From the command line, you can create the two halves of the cell in any order or at any time. It is a best practice to create the deployment manager portion of the profile first. After you create the cell, the cell contains a deployment manager and a federated node. The deployment manager portion and the node portion are in separate directories.

For each of the two profiles that you create, you can specify the fully qualified path to the resulting profile using the `-profilePath` parameter. If you do not specify the parameter, the default value for each profile path is based on the *app_server_root* directory, the profiles subdirectory, and the name of the profile.

The two templates that compose a cell profile have dependencies between one another which requires some parameter values to match between the two create invocations. To create a full working cell, the `-nodeProfilePath`, `-cellName`, `-appServerNodeName`, `-nodeName` parameters are required to have the same values for both the cell_dmgr profile and the cell_node profile. In the case of ports, and especially in the case of dynamically allocated ports, the creation of the second half of the cell must reference the ports that are used in the first half of the cell. Use the `-portsFile` and `-nodePortsFile` arguments with references to the following files of the profile that represents the first half of the cell:

Linux HP-UX Solaris AIX

- *profile_root*/properties/portdef.props
- *profile_root*/properties/nodeportdef.props

Windows

- *profile_root*\properties\portdef.props
- *profile_root*\properties\nodeportdef.props

This approach ensures that the ports in the second half of the cell are created with the correct correlation to the first half of the cell.

For detailed help in creating a cell profile, use the following commands:

Linux HP-UX Solaris AIX

```
app_server_root/bin/manageprofiles.sh -create
 -templatePath
app_server_root/profileTemplates/cell/dmgr
 -help
```

Windows

```
app_server_root\bin\manageprofiles.bat -create
 -templatePath
app_server_root\profileTemplates\cell\dmgr
 -help
```

or

Linux HP-UX Solaris AIX

```
app_server_root/bin/manageprofiles.sh -create
 -templatePath
app_server_root/profileTemplates/cell/default
 -help
```

Windows

```
app_server_root\bin\manageprofiles.bat -create
 -templatePath
app_server_root\profileTemplates\cell\default
 -help
```

The output from the `-help` parameter specifies which parameters are required and which are optional when creating the cell deployment manager profile and the cell node profile.

The following example creates a cell profile named *Dmgr001* having a cell name of *Default01Cell* and a node name of *Default01Node*.

1. Verify that the following path is available for use:

   The path must be available when you create the deployment manager and node portions of the cell as subdirectories are added for each portion.

   - Linux HP-UX Solaris AIX *app_server_root*/profiles
   - Windows *app_server_root*\profiles
2. Create the deployment manager portion of the cell profile.

   Linux HP-UX Solaris AIX

```
app_server_root/bin/manageprofiles.sh -create
 -templatePath
app_server_root/profileTemplates/cell/dmgr
 -nodeProfilePath
app_server_root/profiles/AppSrv01
 -profileName Dmgr001
 -cellName Default01Cell
 -nodeName Default01Node
 -appServerNodeName federated_node_name
```

   Windows

```
app_server_root\bin\manageprofiles.bat -create
 -templatePath
app_server_root\profileTemplates\cell\dmgr
 -nodeProfilePath
app_server_root\profiles\AppSrv01
 -profileName Dmgr001
 -cellName Default01Cell
 -nodeName Default01Node
 -appServerNodeName federated_node_name
```

3. Verify that the Dmgr001 profile exists as it must exist before you create the application server portion of the cell profile.
4. Create the application server portion of the cell profile.

   Important: You must use the same values for the cellName, nodeName, and appServerNodeName parameters that you used in the deployment manager portion of the cell profile. The illustration below demonstrates the use of the same values for the cellName, nodeName, and appServerNodeName parameters in the deployment manager and application server portions of the cell profile.

```
For Dmgr:
-cellName host01Cell01
-nodeName host01CellManager01
-appServerNodeName host01Node01

For AppServer:
-cellName host01Cell01
-nodeName host01CellManager01
-appServerNodeName host01Node01
```

   If you did not specify names for these parameters when you created the deployment manager portion of the cell profile, you must use the default name that was assigned in the first command-line invocation.

   Linux HP-UX Solaris AIX

```
app_server_root/bin/manageprofiles.sh -create
 -templatePath
app_server_root/profileTemplates/cell/default
 -dmgrProfilePath
app_server_root/profiles/Dmgr001
 -portsFile
app_server_root/profiles/Dmgr001/properties/portdef.props
 -nodePortsFile
app_server_root/profiles/Dmgr001/properties/nodeportdef.props
 -profileName AppSrv01
 -cellName Default01Cell
 -nodeName Default01Node
 -appServerNodeName federated_node_name
```

Windows

```
app_server_root\bin\manageprofiles.bat -create
 -templatePath
app_server_root\profileTemplates\cell\default
 -dmgrProfilePath
app_server_root\profiles\Dmgr001
 -portsFile
app_server_root\profiles\Dmgr001\properties\portdef.props
 -nodePortsFile
app_server_root\profiles\Dmgr001\properties\nodeportdef.props
 -profileName AppSrv01
 -cellName Default01Cell
 -nodeName Default01Node
 -appServerNodeName federated_node_name
```

After the creation of the deployment manager and node portions of the cell profile, a synchronization between the two servers must occur. By default, synchronization occurs automatically between the two servers at some specified interval. However, if synchronization is disabled, the interval is too long, or some problem occurs that keeps the synchronization from occurring in a timely manner, run the syncNode command to synchronize the deployment manager and the node.

You must either use the portsFile or the nodePortsFile parameter and the startingPort or the nodeStartingPort parameter.

If you use the manageprofiles command, you can choose the profile that you want to be the default.

If you federate an application server node as part of cell profile creation using the -appServerNodeName parameter, the node does not have an original configuration. If you use the -removeNode command on a node that was created during cell profile creation, the command will indicate that the node removal utility is unable to remove the node and restore the node to a base configuration. To successfully remove a node that was federated as part of a cell profile creation, use the manageprofiles command to delete the profile for the node. Once the profile for the node is deleted, use the -cleanupNode command on Deployment Manager to remove the node configuration from the cell repository. A new profile can be created using the Profile Management Tool or the manageprofiles command.

Example: Using predefined port numbers

The manageprofiles command recommends initial port values when you do not explicitly set port values. You can use predefined port values instead.

The manageprofiles command recommends port values when the options of `-defaultPorts`, `-startingPort`, or `-portsFile` are not specified.

Table 28. File locations of default port values.

This table lists the file locations of default port values by type of profile.

Profile	File path
Application server	*app_server_root*/profileTemplates/default/actions/portsUpdate/portdef.props
Cell - application server portion	*app_server_root*/profileTemplates/cell/dmgr/actions/portsUpdate/nodeportdef.props
Cell - deployment manager portion	*app_server_root*/profileTemplates/cell/dmgr/actions/portsUpdate/portdef.props
Custom	*app_server_root*/profileTemplates/managed/actions/portsUpdate/portdef.props
Management profile for a deployment manager server	*app_server_root*/profileTemplates/management/actions/portsUpdate/dmgr.portdef.props
Management profile for an administrative agent server	*app_server_root*/profileTemplates/management/actions/portsUpdate/adminagent.portdef.props
Management profile for a job manager server	*app_server_root*/profileTemplates/management/actions/portsUpdate/jmgr.portdef.props

Table 28. File locations of default port values (continued).

This table lists the file locations of default port values by type of profile.

Profile	File path
Secure proxy	*app_server_root*/profileTemplates/secureproxy/actions/portsUpdate/portdef.props

To customize the port values in the portdef.props file before creating your profile, perform the following steps. The following example creates the default profile. For other types of profiles, you must substitute the file path with the file path of the profile that you want to create.

1. Copy the *app_server_root*/profileTemplates/*default*/actions/portsUpdate/portdef.props file from the default profile template path and place a copy of the file in an arbitrary temporary directory such as:
   - Windows c:\temp\ports
   - ▶ AIX ▶ HP-UX ▶ Solaris /temp/ports
2. In the new file, modify the port settings to specify your port values.
3. Create your profile with the manageprofiles command. Use the modified port values. Specify the location of your modified portdef.props file on the -portsFile parameter. Specify the -validatePorts parameter to ensure that ports are not reserved or in use. Use the following example as a guide:

   Windows

```
manageprofiles.bat
   -create
   -profileName Wow_Profile
   -profilePath profile_root
   -templatePath app_server_root\profileTemplates\default
   -nodeName Wow_node
   -cellName Wow_cell
   -hostName lorriemb
   -portsFile C:\temp\ports\portdef.props
   -validatePorts
```

   AIX Linux

```
manageprofiles.sh
   -create
   -profileName Wow_Profile
   -profilePath profile_root
   -templatePath app_server_root\profileTemplates\default
   -nodeName Wow_node
   -cellName Wow_cell
   -hostName lorriemb
   -portsFile \temp\ports\portdef.props
   -validatePorts
```

Suppose that the portdef.props file has the following values:

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

After running the manageprofiles command to create your profile with the user defined port values, a success or fail result displays.

The manageprofiles command creates a copy of the current `portdefs.props` file in the *profile_root*`\properties` directory.

Use only one of the three port values parameters, `-startingPort`, `-defaultPorts`, or `-portsFile` with the manageprofiles command. The three parameters are mutually exclusive.

Managing profiles using the graphical user interface

You can create profiles, which define runtime environments, using the Profile Management Tool. Using profiles instead of multiple product installations saves disk space and simplifies updating the product because a single set of core product files is maintained.

Before you begin

Before you use the Profile Management Tool, install the product files.

The Profile Management Tool is the graphical user interface for the manageprofiles command. See the description of the manageprofiles command for more information.

You must provide enough system temporary space to create a profile. For information, read about the file system requirements for profiles.

Supported configurations: The Profile Management Tool graphical user interface (GUI) for 64-bit architectures is available on Linux for zSeries platforms, x86-based Linux and Windows platforms, Linux on Power PC platforms, and AIX Power PC platforms. However, you can use the Profile Management Tool GUI on other 64–bit architectures if you use a WebSphere Application Server 32–bit installation.

About this task

You can have the installation procedure create a default profile. After installing the core product files for the WebSphere Application Server, Network Deployment product, use the Profile Management Tool or the manageprofiles command to create additional profiles.

Procedure

- Create a cell profile.

  With a cell profile, you can create a deployment manager profile and a profile for a federated application server node in a single pass through the Profile Management tool. Use the cell profile creation option to create the deployment manager profile and the federated application server node profile, unless you have a specific reason to create them separately.
- Create a management profile with a deployment manager server.

  With a deployment manager you can create the administrative node for a multinode, multi-machine group of application server nodes that you create later. This logical group of application server processes is known as a *cell*.
- Create a management profile with an administrative agent server.

  You can create a management profile for the administrative agent to administer multiple application servers that run customer applications only. The administrative agent provides a single administrative console to administer the application servers.
- Create a management profile with a job manager server.

  You can create a management profile for the job manager to coordinate administrative actions among multiple deployment managers, administer multiple unfederated application servers, asynchronously submit jobs to start servers, and a variety of other tasks.
- Create an application server profile.

Create an application server profile so that you can make applications available to the Internet or to an intranet, typically using Java technology.

- Create a custom profile.

  A custom profile is an empty node that you can customize through the deployment manager to include application servers, clusters, or other Java processes, such as a messaging server. Create a custom profile on a distributed machine and add the node into the deployment manager cell to get started customizing the node.

- Create a secure proxy profile.

  You can create a secure proxy profile to serve as the initial point of entry into your enterprise environment. Typically, a secure proxy server exists in the DMZ, accepts requests from clients on the Internet, and forwards the requests to servers in your enterprise environment.

Results

You have created one or more profiles using the Profile Management Tool.

What to do next

See the description of the **manageprofiles** command to learn more about the command-line alternative method of creating a profile and to see examples of using the command.

Read about planning for installation for examples of configurations that you can create by creating profiles.

Creating management profiles with deployment managers

You can create a management profile for the deployment manager to administer servers within the deployment manager cell. Use the Profile Management Tool to create the profile.

Before you begin

Before you use the Profile Management Tool, install the product files.

The Profile Management Tool is the graphical user interface for the manageprofiles command. See the description of the manageprofiles command for more information.

You must provide enough system temporary space to create a profile. For information, read about the file system requirements for profiles.

Attention: When you launch the Profile Management Tool, the tool could lock up in the following situation for a non-root user: Log into a machine as root, use the SetPermissions utility to change the user from *x* to *y*. Assume that you are user *x* and log back into the machine. Launch the Profile Management Tool, click **Profile Management Tool**, and click **Create**. The next click after the click on **Create** could lock up the tool.

Attention: Solaris When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons of the Profile Management Tool. To fix the problem, add the following lines to the *app_server_root*/.Xdefaults file:

```
Eclipse*spacing:0
Eclipse*fontList:-misc-fixed-medium-r-normal-*-10-100-75-75-c-60-iso8859-1
```

After adding the lines, run the following command before launching the Profile Management Tool:

```
xrdb -load user_home/.Xdefaults
```

About this task

After installing the core product files for the Network Deployment product, you must create a profile. This procedure describes creating a management profile with a deployment manager using the graphical user interface that is provided by the Profile Management Tool. You can also use the manageprofiles command to create a management profile with a deployment manager. See the description of the manageprofiles command for more information.

The deployment manager provides a single administrative interface for a logical group of application servers on one or more machines.

You can create profiles with the Profile Management Tool using the typical profile creation process or the advanced profile creation process. The typical profile creation process uses default settings and assigns unique port values. You can optionally set values as allowed. For the advanced profile creation process you can accept the default values, or specify your own values.

Procedure

1. Start the Profile Management Tool to create a new runtime environment.

   You can use one of the following ways to start the tool.

   - At the end of installation, select the check box to launch the Profile Management Tool.
   - Issue the command to open the WebSphere Customization Toolbox directly from a command prompt; then, open the Profile Management Tool.
   - Select the **WebSphere Customization Toolbox** option from the First steps console; then, open the Profile Management Tool.
   - Windows Use the **Start** menu to access the WebSphere Customization Toolbox; then, open the Profile Management Tool.
   - Linux Use the Linux operating system menus that are used to start programs to start the WebSphere Customization Toolbox; then, open the Profile Management Tool.
2. Click **Create** on the Profiles tab to create a new profile.

   The Profiles tab contains a list of profiles that have been created on your machine. No action can be done on a selected profile unless the profile can be augmented. The Augment button is greyed out unless a profile that you select can be augmented.

   The tool displays the Environment selection panel.
3. Select **Management** and click **Next**.

   The Server type selection panel is displayed.
4. Select **Deployment manager** and click **Next**.

   The Profile creation options panel is displayed.
5. Select either **Typical profile creation** or **Advanced profile creation**, and click **Next**.

   The **Typical profile creation** option creates a profile that uses default configuration settings. With the **Advanced profile creation** option, you can specify your own configuration values for a profile.
6. If you selected **Typical profile creation**, go to the step on administrative security.

7. If you selected **Advanced profile creation**, optionally select to deploy the administrative console, then click **Next**.

   The tool displays the Profile name and location panel.

8. Specify a name for the profile and the directory path for the profile directory, or accept the default values. Then, click **Next**.

   Profile naming guidelines: Double-byte characters are supported. The profile name can be any unique name with the following restrictions. Do not use any of the following characters when naming your profile:

   - Spaces
   - Special characters that are not supported within the name of a directory on your operating system, such as `*&?`
   - Slashes (/) or (\)

   The default profile

   The first profile that you create on a machine is the default profile. The default profile is the default target for commands that are issued from the `bin` directory in the product installation root. When only one profile exists on a machine, every command works on the single server process in the configuration. You can make another profile the default profile when you create that profile by checking **Make this profile the default** on the Profile name and location panel of the **Advanced profile creation** path. You can also make another profile the default profile using the manageprofiles command after you create the profile.

   Addressing a profile in a multiprofile environment

   When multiple profiles exist on a machine, certain commands require that you specify the profile to which the command applies if the profile is not the default profile. These commands use the -profileName parameter to identify which profile to address. You might find it easier to use the commands that are in the `bin` directory of each profile.

   Use these commands to query the command shell to determine the calling profile and to address these commands to the calling profile.

   Default profile information

   The default profile name is <*profile_type*><*profile_number*>:

   - <*profile_type*> is a value of `AppSrv`, `Dmgr`, `Custom`, `AdminAgent`, `JobMgr`, or `SecureProxySrv`.
   - <*profile_number*> is a sequential number that is used to create a unique profile name

   AIX HP-UX Linux Solaris The default profile directory is *app_server_root*/profiles, where *app_server_root* is the installation root.

   Windows The default profile directory is *app_server_root*\profiles, where *app_server_root* is the installation root.

9. On the Node, host, and cell names panel, specify a unique node name, the actual host name of the machine, and a unique cell name. Click **Next**.

Table 29. Characteristics of the deployment manager node.

This table shows the characteristics of the deployment manager node.

Field Name	Default Value	Constraints	Description
Node name	*shortHostName* `CellManager` *NodeNumber* where: • *shortHostName* is the short host name. • *NodeNumber* is a sequential number starting at 01.	Use a unique name for the deployment manager.	The name is used for administration within the deployment manager cell.

Table 29. Characteristics of the deployment manager node (continued).

This table shows the characteristics of the deployment manager node.

Field Name	Default Value	Constraints	Description
Host name	The long form of the domain name server (DNS) name.	The host name must be addressable through your network. Read about Host name considerations.	Use the actual DNS name or IP address of your machine to enable communication with your machine. See additional information about the host name that follows this table.

Cell name	`shortHostName`
	`Cell`
	`CellNumber`
	where:
	• *shortHostName* is the short host name.
	• *CellNumber* is a sequential number starting at 01.
		Use a unique name for the deployment manager cell. If you plan to migrate a Version 6 or Version 7 deployment manager cell to this Version 8 deployment manager, use the same cell name as the Version 6 or Version 7 deployment manager.A cell name must be unique in any circumstance in which the product is running on the same physical machine or cluster of machines, such as a sysplex. Additionally, a cell name must be unique in any circumstance in which network connectivity between entities is required either between the cells or from a client that must communicate with each of the cells. Cell names must also be unique if their namespaces are federated. Otherwise, you might encounter symptoms such as a javax.naming.NameNotFoundException error, in which case, create uniquely named cells.	All federated nodes become members of the deployment manager cell, which you name in this panel.

Reserved names: Avoid using reserved folder names as field values. The use of reserved folder names can cause unpredictable results. The following terms are reserved folder names:

- cells
- nodes
- servers
- clusters
- applications
- deployments

Directory path considerations:

Windows The number of characters in the *profiles_directory_path\profile_name* directory must be less than or equal to 80 characters.

Host name considerations:

The host name is the network name for the physical machine on which the node is installed. The host name must resolve to a physical network node on the server. When multiple network cards exist in the server, the host name or IP address must resolve to one of the network cards. Remote nodes use the host name to connect to and communicate with this node. Selecting a host name that other machines can reach within your network is important. Do not use the generic identifier, `localhost`, for this value. Also, do not attempt to install WebSphere Application Server products on a machine with a host name that uses characters from a double-byte character set (DBCS). DBCS characters are not supported when used in the host name.

If you define coexisting nodes on the same computer with unique IP addresses, then define each IP address in a domain name server (DNS) look-up table. Configuration files for standalone application servers do not provide domain name resolution for multiple IP addresses on a machine with a single network address.

The value that you specify for the host name is used as the value of the hostName property in configuration documents for the standalone application server. Specify the host name value in one of the following formats:

- Fully qualified domain name server (DNS) host name string, such as `xmachine.manhattan.ibm.com`
- The default short DNS host name string, such as `xmachine`
- Numeric IP address, such as `127.1.255.3`

The fully qualified DNS host name has the advantages of being unambiguous and flexible. You have the flexibility of changing the actual IP address for the host system without having to change the application server configuration. This value for the host name is particularly useful if you plan to change the IP address frequently when using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. A disadvantage of this format is dependency on DNS. If DNS is not available, then connectivity is compromised.

The short host name is also dynamically resolvable. A short name format has the added function of being redefined in the local hosts file so that the system can run the application server, even when disconnected from the network. To run disconnected, define the short name as the loopback address, `127.0.0.1`, in the hosts file to run disconnected. A disadvantage of this format is a dependency on DNS for remote access. If DNS is not available, then connectivity is compromised.

A numeric IP address has the advantage of not requiring name resolution through DNS. A remote node can connect to the node that you name with a numeric IP address without DNS being available. A disadvantage of this format is that the numeric IP address is fixed. You must change the setting of the hostName property in Express configuration documents whenever you change the machine IP address. Therefore, do not use a numeric IP address if you use DHCP, or if you change IP addresses regularly. Another disadvantage of this format is that you cannot use the node if the host is disconnected from the network.

After displaying deployment manager characteristics, the tool displays the Administrative security panel.

10. Optionally enable administrative security, and click **Next**.

    You can enable administrative security now during profile creation, or later from the console. If you enable administrative security now, then enter a user name and password to log onto the administrative console.

    After specifying security characteristics, the tool displays the Security certificate panel if you previously selected **Advanced profile creation**.

11. If you selected **Typical profile creation** at the beginning of these steps, then go to the step that displays the Profile summary panel.

12. Create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

    You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

Note: When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the trust.p12 file.

If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

13. Verify that the certificate information is correct, and click **Next**.

    If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is `WebAS`. You should change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the java.security file.

    When you create either or both certificates, or import either or both certificates, the keystore files that are created are key.p12, trust.p12, root-key.p12, default-signers.p12, deleted.p12, and ltpa.jceks. These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify. The key.p12 file contains the default personal certificate. The trust.p12 file contains the signer certificate from the default root certificate. The root-key.p12 file contains the root signing certificate. The default-signer.p12 file contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower® signer certificate is in the default-signer.p12 keystore file. The deleted.p12 keystore file is used to hold certificates deleted with the deleteKeyStore task so that they can be recovered if needed. The ltpa.jceks file contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

    An imported certificate is added to the key.p12 file or the root-key.p12 file.

    If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

    After displaying the Security certificate panels, the tool displays the Ports panel if you previously selected **Advanced profile creation**.

14. Verify that the ports within the deployment manager profile are unique, or intentionally conflicting, and click **Next**.

    If you chose not to deploy the administrative console, then the administrative console ports are disabled on the Ports panel.

    Port conflict resolution

    Ports are recognized as being in use if one of the following conditions exists:

    - The ports are assigned to a profile created from an installation that is performed by the current user.
    - The port is currently in use.

    Validation of ports occurs when you access the Port value assignment panel. Conflicts can still occur between the Port value assignment panel and the Profile creation complete panel because ports are not assigned until profile creation completes.

    If you suspect a port conflict, then you can investigate the port conflict after the profile is created. Determine the ports that are used during profile creation by examining the following files.

    - Linux HP-UX Solaris AIX *profile_root*/`properties/portdef.props` file
    - Windows *profile_root*\`properties\portdef.props` file

    Included in this file are the keys and values that are used in setting the ports. If you discover ports conflicts, then you can reassign ports manually. To reassign ports, run the updatePorts.ant file by using the ws_ant script.

    Windows Linux The tool displays the Windows service definition panel if you are installing on a Windows operating system and the installation ID has the administrative group privilege. The tool displays the Linux service definition panel if you are installing on a supported Linux operating system and the ID that runs the Profile Management Tool is the root user.

15. Choose whether to run the dmgr process as a Windows service on a Windows platform or as a Linux Service on a Linux platform, and click **Next**.

    The Windows service definition panel is displayed for the Windows operating system only if the ID that installs the Windows service has the administrator group privilege. However, you can run the WASService.exe command to create the Windows service as long as the installer ID belongs to the administrator group. Read about automatically restarting server processes for more information.

    Windows The product attempts to start Windows services for dmgr processes that are started by a startManager command. For example, if you configure a deployment manager as a Windows service and issue the startManager command, then the wasservice command attempts to start the defined service.

    If you chose to install a local system service, then you do not have to specify your user ID or password. If you create a specified user type of service, then you must specify the user ID and the password for the user who runs the service. The user must have `Log on as a service` authority for the service to run correctly. If the user does not have `Log on as a service` authority, then the Profile Management tool automatically adds the authority.

    To perform this profile creation task, the user ID must not contain spaces. In addition to belonging to the administrator group, the ID must also have the advanced user right of `Log on as a service`. The Installation program grants the user ID the advanced user right if the user ID does not already have the advanced user right and if the user ID belongs to the administrator group.

    You can also create other Windows services after the installation is complete to start other server processes. Read about automatically restarting server processes for more information.

    You can remove the Windows service that is added during profile creation during profile deletion. You can also remove the Windows service with the wasservice command.

    IPv6 considerations

    Profiles created to run as a Windows service fail to start when using IPv6 if the service is configured to run as `Local System`. Create a user-specific environment variable to enable IPv6. Since this environment variable is a user variable instead of a `Local System` variable, only a Windows service that runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as `Local System`. When the Windows service for the dmgr process tries to run, the service is unable to access the user environment variable that specifies IPv6, and thus tries to start as IPv4. The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the Windows service for the dmgr process runs as the same user ID under which the environment variable that specifies IPv6 is defined, instead of as `Local System`.

    Windows The following default values for the Windows service definition panel exist:

    - The default is to run as a Windows service.
    - The service process is selected to run as a system account.
    - The user account is the current user name. User name requirements are the requirements that the Windows operating system imposes for a user ID.
    - The startup type is `automatic`. The values for the startup type are those values that the Windows operating system imposes. If you want a startup type other than `automatic`, you can either select another available option from the menu or change the startup type after you create the profile. You can also remove the created service after profile creation, and add it later with the desired startup type. You can choose not to create a service at profile creation time and optionally create the service later with the desired startup type.

    Linux The Linux service definition panel is displayed if the current operating system is a supported version of Linux operating systems, and the current user has the appropriate permissions.

    The product attempts to start Linux services for application server processes that are started by a startServer command. For example, if you configure an application server as a Linux service and issue the startServer command, then the **wasservice** command attempts to start the defined service.

By default, the product is not selected to run as a Linux service.

To create the service, the user that runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a non-root user ID, then the Linux service definition panel is not displayed, and no service is created.

When you create a Linux service, you must specify a user name from which the service runs.

To delete a Linux service, the user must be the root user or have appropriate privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service for the user.

The tool displays the Profile Creation Summary panel.

16. Click **Create** to create the deployment manager, or click **Back** to change the characteristics of the deployment manager.

    The Profile creation progress panel, which shows the configuration commands that are running, is displayed.

    When the profile creation completes, the tool displays the Profile creation complete panel.

17. Optionally, select **Launch the First steps console**. Click **Finish** to exit.

    With the First steps console, you can create additional profiles and start the application server.

Results

You created a deployment manager profile.

Refer to the description of the manageprofiles command to learn about creating a profile using a command instead of the Profile Management Tool.

What to do next

Create an application server profile or a custom profile, and add the node into the cell.

Deploy an application to get started.

Read about fast paths for the product to get started deploying applications.

Creating management profiles with administrative agents

You can create a management profile for the administrative agent to administer multiple application servers that run customer applications only. The administrative agent provides a single administrative console to administer the application servers.

Before you begin

Before you use the Profile Management Tool, install the product files.

The Profile Management Tool is the graphical user interface for the manageprofiles command. See the description of the manageprofiles command for more information.

You must provide enough system temporary space to create a profile. For information, read about the file system requirements for profiles.

Attention: When you launch the Profile Management Tool, the tool could lock up in the following situation for a non-root user: Log into a machine as root, use the SetPermissions utility to change the user from *x* to *y*. Assume that you are user *x* and log back into the machine. Launch the Profile Management Tool, click **Profile Management Tool**, and click **Create**. The next click after the click on **Create** could lock up the tool.

Attention: Solaris When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons of the Profile Management Tool. To fix the problem, add the following lines to the *app_server_root*/.Xdefaults file:

```
Eclipse*spacing:0
Eclipse*fontList:-misc-fixed-medium-r-normal-*-10-100-75-75-c-60-iso8859-1
```

After adding the lines, run the following command before launching the Profile Management Tool:

```
xrdb -load user_home/.Xdefaults
```

About this task

After installing the core product files for the product, you must create a profile. This procedure describes creating a management profile with an administrative agent server using the graphical user interface that is provided by the Profile Management Tool. You can also use the manageprofiles command to create an administrative agent. See the description of the manageprofiles command for more information.

You can create profiles with the Profile Management Tool using the typical profile creation process or the advanced profile creation process. The typical profile creation process uses default settings and assigns unique port values. You can optionally set values as allowed. For the advanced profile creation process you can accept the default values, or specify your own values.

Procedure

1. Start the Profile Management Tool to create a new runtime environment.

   You can use one of the following ways to start the tool.

   - At the end of installation, select the check box to launch the Profile Management Tool.
   - Issue the command to open the WebSphere Customization Toolbox directly from a command prompt; then, open the Profile Management Tool.
   - Select the **WebSphere Customization Toolbox** option from the First steps console; then, open the Profile Management Tool.
   - Windows Use the **Start** menu to access the WebSphere Customization Toolbox; then, open the Profile Management Tool.
   - Linux Use the Linux operating system menus that are used to start programs to start the WebSphere Customization Toolbox; then, open the Profile Management Tool.
2. Click **Create** on the Profiles tab to create a new profile.

   The Profiles tab contains a list of profiles that have been created on your machine. No action can be done on a selected profile unless the profile can be augmented. The Augment button is greyed out unless a profile that you select can be augmented.

   The tool displays the Environment selection panel.
3. Select **Management**, and click **Next**.

   The Server type selection panel is displayed.
4. Select **Administrative agent**. Click **Next**.

   The Profile creation options panel is displayed.
5. Select either **Typical profile creation** or **Advanced profile creation**, and click **Next**.

   The **Typical profile creation** option creates a profile that uses default configuration settings. With the **Advanced profile creation** option, you can specify your own configuration values for a profile.
6. If you selected **Typical profile creation**, go to the step on administrative security.
7. If you selected **Advanced profile creation**, optionally select to deploy the administrative console and then click **Next**.

   If you chose not to deploy the administrative console, then the administrative console ports are disabled on the Ports panel.

The tool displays the Profile name and location panel.

8. Specify a name for the profile and the directory path for the profile directory, or accept the default values. Then, click **Next**.

   Profile naming guidelines: Double-byte characters are supported. The profile name can be any unique name with the following restrictions. Do not use any of the following characters when naming your profile:

   - Spaces
   - Special characters that are not supported within the name of a directory on your operating system, such as `*&?`
   - Slashes (/) or (\)

   The default profile

   The first profile that you create on a machine is the default profile. The default profile is the default target for commands that are issued from the `bin` directory in the product installation root. When only one profile exists on a machine, every command works on the single server process in the configuration. You can make another profile the default profile when you create that profile by checking **Make this profile the default** on the Profile name and location panel of the **Advanced profile creation** path. You can also make another profile the default profile using the manageprofiles command after you create the profile.

   Addressing a profile in a multiprofile environment

   When multiple profiles exist on a machine, certain commands require that you specify the profile to which the command applies if the profile is not the default profile. These commands use the -profileName parameter to identify which profile to address. You might find it easier to use the commands that are in the `bin` directory of each profile.

   Use these commands to query the command shell to determine the calling profile and to address these commands to the calling profile.

   Default profile information

   The default profile name is <*profile_type*><*profile_number*>:

   - <*profile_type*> is a value of `AppSrv`, `Dmgr`, `Custom`, `AdminAgent`, `JobMgr`, or `SecureProxySrv`.
   - <*profile_number*> is a sequential number that is used to create a unique profile name

   AIX HP-UX Linux Solaris The default profile directory is *app_server_root*/profiles, where *app_server_root* is the installation root.

   Windows The default profile directory is *app_server_root*\profiles, where *app_server_root* is the installation root.

9. On the Node, host, and cell names panel, specify a unique node name, the actual host name of the machine, and a unique cell name. Click **Next**.

Table 30. Characteristics of the administrative agent node.

This table shows the characteristics of the administrative agent node.

Field name	Default value	Constraints	Description
Node name	*shortHostName* AANode *NodeNumber* where: • *shortHostName* is the short host name. • *NodeNumber* is a sequential number starting at 01.	Use a unique name for the administrative agent.	The name is used for administration within the administrative agent cell.
Host name	The long form of the domain name server (DNS) name.	The host name must be addressable through your network. Read about Host name considerations.	Use the actual DNS name or IP address of your machine to enable communication with your machine. See additional information about the host name that follows this table.

Table 30. Characteristics of the administrative agent node (continued).

This table shows the characteristics of the administrative agent node.

Field name	Default value	Constraints	Description
Cell name	*shortHostName* Cell *CellNumber* where: • *shortHostName* is the short host name. • *CellNumber* is a sequential number starting at 01.	Use a unique name for the cell. If you plan to migrate a Version 6 or Version 7 cell to Version 8, use the same cell name as the Version 6 or Version 7 cell. A cell name must be unique in any circumstance in which the product is running on the same physical machine or cluster of machines, such as a sysplex. Additionally, a cell name must be unique in any circumstance in which network connectivity between entities is required either between the cells or from a client that must communicate with each of the cells. Cell names must also be unique if their namespaces are federated. Otherwise, you might encounter symptoms such as a javax.naming.NameNotFoundException error, in which case, create uniquely named cells.	All federated nodes become members of the cell, which you name in this panel.

Reserved names: Avoid using reserved folder names as field values. The use of reserved folder names can cause unpredictable results. The following terms are reserved folder names:

- cells
- nodes
- servers
- clusters
- applications
- deployments

Directory path length:

Windows The number of characters in the *profiles_directory_path\profile_name* directory must be less than or equal to 80 characters.

Host name considerations:

The host name is the network name for the physical machine on which the node is installed. The host name must resolve to a physical network node on the server. When multiple network cards exist in the server, the host name or IP address must resolve to one of the network cards. Remote nodes use the host name to connect to and communicate with this node. Selecting a host name that other machines can reach within your network is important. Do not use the generic identifier, `localhost`, for this value. Also, do not attempt to install WebSphere Application Server products on a machine with a host name that uses characters from a double-byte character set (DBCS). DBCS characters are not supported when used in the host name.

If you define coexisting nodes on the same computer with unique IP addresses, then define each IP address in a domain name server (DNS) look-up table. Configuration files for standalone application servers do not provide domain name resolution for multiple IP addresses on a machine with a single network address.

The value that you specify for the host name is used as the value of the hostName property in configuration documents for the standalone application server. Specify the host name value in one of the following formats:

- Fully qualified domain name server (DNS) host name string, such as `xmachine.manhattan.ibm.com`
- The default short DNS host name string, such as `xmachine`
- Numeric IP address, such as `127.1.255.3`

The fully qualified DNS host name has the advantages of being unambiguous and flexible. You have the flexibility of changing the actual IP address for the host system without having to change the application server configuration. This value for the host name is particularly useful if you plan to change the IP address frequently when using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. A disadvantage of this format is dependency on DNS. If DNS is not available, then connectivity is compromised.

The short host name is also dynamically resolvable. A short name format has the added function of being redefined in the local hosts file so that the system can run the application server, even when disconnected from the network. To run disconnected, define the short name as the loopback address, `127.0.0.1`, in the hosts file to run disconnected. A disadvantage of this format is a dependency on DNS for remote access. If DNS is not available, then connectivity is compromised.

A numeric IP address has the advantage of not requiring name resolution through DNS. A remote node can connect to the node that you name with a numeric IP address without DNS being available. A disadvantage of this format is that the numeric IP address is fixed. You must change the setting of the hostName property in Express configuration documents whenever you change the machine IP address. Therefore, do not use a numeric IP address if you use DHCP, or if you change IP addresses regularly. Another disadvantage of this format is that you cannot use the node if the host is disconnected from the network.

After displaying characteristics, the tool displays the Administrative security panel.

10. Optionally enable administrative security, and click **Next**.

    You can enable administrative security now during profile creation, or later from the console. If you enable administrative security now, then enter a user name and password to log onto the administrative console.

    After specifying security characteristics, the tool displays the Security certificate panel if you previously selected **Advanced profile creation**.

11. If you selected **Typical profile creation** at the beginning of these steps, then go to the step that displays the Profile summary panel.

12. Create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

    You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

    Note: When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the trust.p12 file.

    If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

13. Verify that the certificate information is correct, and click **Next**.

If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is `WebAS`. You should change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the java.security file.

When you create either or both certificates, or import either or both certificates, the keystore files that are created are key.p12, trust.p12, root-key.p12, default-signers.p12, deleted.p12, and ltpa.jceks. These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify. The key.p12 file contains the default personal certificate. The trust.p12 file contains the signer certificate from the default root certificate. The root-key.p12 file contains the root signing certificate. The default-signer.p12 file contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate is in the default-signer.p12 keystore file. The deleted.p12 keystore file is used to hold certificates deleted with the deleteKeyStore task so that they can be recovered if needed. The ltpa.jceks file contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

An imported certificate is added to the key.p12 file or the root-key.p12 file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

After displaying the Security certificate panels, the tool displays the Ports panel if you previously selected **Advanced profile creation**.

14. Verify that the ports within the administrative agent profile are unique, or intentionally conflicting, and click **Next**.

    If you chose not to deploy the administrative console, then the administrative console ports are disabled on the Ports panel.

    Port conflict resolution

    Ports are recognized as being in use if one of the following conditions exists:

    - The ports are assigned to a profile created from an installation that is performed by the current user.
    - The port is currently in use.

    Validation of ports occurs when you access the Port value assignment panel. Conflicts can still occur between the Port value assignment panel and the Profile creation complete panel because ports are not assigned until profile creation completes.

    If you suspect a port conflict, then you can investigate the port conflict after the profile is created. Determine the ports that are used during profile creation by examining the following files.

    - Linux HP-UX Solaris AIX *profile_root*/`properties/portdef.props` file
    - Windows *profile_root*\`properties\portdef.props` file

    Included in this file are the keys and values that are used in setting the ports. If you discover ports conflicts, then you can reassign ports manually. To reassign ports, run the updatePorts.ant file by using the ws_ant script.

    Windows Linux The tool displays the Windows service definition panel if you are installing on a Windows operating system and the installation ID has the administrative group privilege. The tool displays the Linux service definition panel if you are installing on a supported Linux operating system and the ID that runs the Profile Management Tool is the root user.

15. Choose whether to run the administrative agent process as a Windows service on a Windows operating system or as a Linux service on a Linux operating system, and click **Next**.

    The Windows service definition panel is displayed for the Windows operating system only if the ID that installs the Windows service has the administrator group privilege. However, you can run the

WASService.exe command to create the Windows service as long as the installer ID belongs to the administrator group. Read about automatically restarting server processes for more information.

Windows The product attempts to start Windows services for administrative agent processes that are started by a startServer command. For example, if you configure an administrative agent as a Windows service and issue the startServer command, then the **wasservice** command attempts to start the defined service.

If you chose to install a local system service, then you do not have to specify your user ID or password. If you create a specified user type of service, then you must specify the user ID and the password for the user who runs the service. The user must have `Log on as a service` authority for the service to run correctly. If the user does not have `Log on as a service` authority, then the Profile Management tool automatically adds the authority.

To perform this profile creation task, the user ID must not contain spaces. In addition to belonging to the administrator group, the ID must also have the advanced user right of `Log on as a service`. The Installation program grants the user ID the advanced user right if the user ID does not already have the advanced user right and if the user ID belongs to the administrator group.

You can also create other Windows services after the installation is complete to start other server processes. Read about automatically restarting server processes for more information.

You can remove the Windows service that is added during profile creation during profile deletion. You can also remove the Windows service with the wasservice command.

IPv6 considerations

Profiles created to run as a Windows service fail to start when using Internet Protocol version 6 (IPv6) if the service is configured to run as local system. Create a user-specific environment variable to enable IPv6. Since this environment variable is a user variable instead of a local system variable, only a Windows service that runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as local system. When the Windows service for the administrative agent process attempts to run, the service is unable to access the user environment variable that specifies IPv6, and thus, attempts to start as IPv4. The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the Windows service for the administrative agent process runs as the same user ID from which the environment variable that specifies IPv6 is defined, instead of as local system.

Windows The following default values for the Windows service definition panel exist:

- The default is to run as a Windows service.
- The service process is selected to run as a system account.
- The user account is the current user name. User name requirements are the requirements that the Windows operating system imposes for a user ID.
- The startup type is `automatic`. The values for the startup type are those values that the Windows operating system imposes. If you want a startup type other than `automatic`, you can either select another available option from the menu or change the startup type after you create the profile. You can also remove the created service after profile creation, and add it later with the desired startup type. You can choose not to create a service at profile creation time and optionally create the service later with the desired startup type.

Linux The Linux service definition panel is displayed if the current operating system is a supported version of Linux operating systems, and the current user has the appropriate permissions.

The product attempts to start Linux services for application server processes that are started by a startServer command. For example, if you configure an application server as a Linux service and issue the startServer command, then the **wasservice** command attempts to start the defined service.

By default, the product is not selected to run as a Linux service.

To create the service, the user that runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a non-root user ID, then the Linux service definition panel is not displayed, and no service is created.

When you create a Linux service, you must specify a user name from which the service runs.

To delete a Linux service, the user must be the root user or have appropriate privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service for the user.

The tool displays the Profile creation summary panel.

16. Click **Create** to create the management profile for the administrative agent, or click **Back** to change the characteristics of the profile.

    The Profile creation progress panel, which shows the configuration commands that are running, is displayed.

    When the profile creation completes, the tool displays the Profile creation complete panel.

17. Optionally, select **Launch the First steps console**. Click **Finish** to exit.

    With the First steps console, you can create additional profiles and start the application server.

Results

You created a management profile for the administrative agent.

Refer to the description of the manageprofiles command to learn about creating a profile using a command instead of the Profile Management Tool.

What to do next

Register application servers with the administrative agent using the registerNode command. Then, access the administrative agent console to administer your application servers.

Creating management profiles for job managers

You can create a management profile for the job manager to coordinate administrative actions among multiple deployment managers, administer multiple unfederated application servers, asynchronously submit jobs to start servers, and a variety of other tasks.

Before you begin

Before you use the Profile Management Tool, install the product files.

The Profile Management Tool is the graphical user interface for the manageprofiles command. See the description of the manageprofiles command for more information.

You must provide enough system temporary space to create a profile. For information, read about the file system requirements for profiles.

Attention: When you launch the Profile Management Tool, the tool could lock up in the following situation for a non-root user: Log into a machine as root, use the SetPermissions utility to change the user from *x* to *y*. Assume that you are user *x* and log back into the machine. Launch the Profile Management Tool, click **Profile Management Tool**, and click **Create**. The next click after the click on **Create** could lock up the tool.

Attention: Solaris When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons of the Profile Management Tool. To fix the problem, add the following lines to the *app_server_root*/.Xdefaults file:

```
Eclipse*spacing:0
Eclipse*fontList:-misc-fixed-medium-r-normal-*-10-100-75-75-c-60-iso8859-1
```

After adding the lines, run the following command before launching the Profile Management Tool:

```
xrdb -load user_home/.Xdefaults
```

About this task

After installing the core product files for the product, you must create a profile. This procedure describes creating a management profile with a job manager server using the graphical user interface provided by the Profile Management Tool. You can also use the manageprofiles command to create a job manager. See the description of the manageprofiles command for more information.

You can create profiles with the Profile Management Tool using the typical profile creation process or the advanced profile creation process. The typical profile creation process uses default settings and assigns unique port values. You can optionally set values as allowed. For the advanced profile creation process you can accept the default values, or specify your own values.

Procedure

1. Start the Profile Management Tool to create a new runtime environment.

   You can use one of the following ways to start the tool.

   - At the end of installation, select the check box to launch the Profile Management Tool.
   - Issue the command to open the WebSphere Customization Toolbox directly from a command prompt; then, open the Profile Management Tool.
   - Select the **WebSphere Customization Toolbox** option from the First steps console; then, open the Profile Management Tool.
   - Windows Use the **Start** menu to access the WebSphere Customization Toolbox; then, open the Profile Management Tool.
   - Linux Use the Linux operating system menus that are used to start programs to start the WebSphere Customization Toolbox; then, open the Profile Management Tool.
2. Click **Create** on the Profiles tab to create a new profile.

   The Profiles tab contains a list of profiles that have been created on your machine. No action can be done on a selected profile unless the profile can be augmented. The Augment button is greyed out unless a profile that you select can be augmented.

   The tool displays the Environment selection panel.
3. Select **Management**, and click **Next**.

   The Server type selection panel is displayed.
4. Select **Job manager**. Click **Next**.

   The Profile creation options panel is displayed.
5. Select either **Typical profile creation** or **Advanced profile creation**, and click **Next**.

   The **Typical profile creation** option creates a profile that uses default configuration settings. With the **Advanced profile creation** option, you can specify your own configuration values for a profile.
6. If you selected **Typical profile creation**, go to the step on administrative security.
7. If you selected **Advanced profile creation**, optionally select to deploy the administrative console, and then click **Next**.

   If you chose not to deploy the administrative console, then the administrative console ports are disabled on the Ports panel.

The tool displays the Profile name and location panel.

8. Specify a name for the profile and the directory path for the profile directory, or accept the default values. Then, click **Next**.

   Profile naming guidelines: Double-byte characters are supported. The profile name can be any unique name with the following restrictions. Do not use any of the following characters when naming your profile:

   - Spaces
   - Special characters that are not supported within the name of a directory on your operating system, such as `*&?`
   - Slashes (/) or (\)

   The default profile

   The first profile that you create on a machine is the default profile. The default profile is the default target for commands that are issued from the `bin` directory in the product installation root. When only one profile exists on a machine, every command works on the single server process in the configuration. You can make another profile the default profile when you create that profile by checking **Make this profile the default** on the Profile name and location panel of the **Advanced profile creation** path. You can also make another profile the default profile using the manageprofiles command after you create the profile.

   Addressing a profile in a multiprofile environment

   When multiple profiles exist on a machine, certain commands require that you specify the profile to which the command applies if the profile is not the default profile. These commands use the -profileName parameter to identify which profile to address. You might find it easier to use the commands that are in the `bin` directory of each profile.

   Use these commands to query the command shell to determine the calling profile and to address these commands to the calling profile.

   Default profile information

   The default profile name is *<profile_type><profile_number>*:

   - *<profile_type>* is a value of `AppSrv`, `Dmgr`, `Custom`, `AdminAgent`, `JobMgr`, or `SecureProxySrv`.
   - *<profile_number>* is a sequential number that is used to create a unique profile name

   AIX HP-UX Linux Solaris The default profile directory is *app_server_root*/profiles, where *app_server_root* is the installation root.

   Windows The default profile directory is *app_server_root*\profiles, where *app_server_root* is the installation root.

9. On the Node, host, and cell names panel, specify a unique node name, the actual host name of the machine, and a unique cell name. Click **Next**.

Table 31. Characteristics of the job manager node.

This table shows the characteristics of the job manager node.

Field Name	Default Value	Constraints	Description
Node name	*shortHostName* JobMgr *NodeNumber* where: • *shortHostName* is the short host name. • *NodeNumber* is a sequential number starting at 01.	Use a unique name for the job manager.	The name is used for administration within the job manager cell.
Host name	The long form of the domain name server (DNS) name.	The host name must be addressable through your network. Read about host name considerations.	Use the actual DNS name or IP address of your machine to enable communication with your machine. See additional information about the host name that follows this table.

Table 31. Characteristics of the job manager node (continued).

This table shows the characteristics of the job manager node.

Field Name	Default Value	Constraints	Description
Cell name	`shortHostNameCellCellNumber` where: • *shortHostName* is the short host name. • *CellNumber* is a sequential number starting at 01.	Use a unique name for the cell. If you plan to migrate a Version 6 or Version 7 cell to Version 8, use the same cell name as the Version 6 or Version 7 cell. A cell name must be unique in any circumstance in which the product is running on the same physical machine or cluster of machines, such as a sysplex. Additionally, a cell name must be unique in any circumstance in which network connectivity between entities is required either between the cells or from a client that must communicate with each of the cells. Cell names must also be unique if their namespaces are federated. Otherwise, you might encounter symptoms such as a javax.naming.NameNotFoundException error, in which case, create uniquely named cells.	All federated nodes become members of the cell, which you name in this panel.

Reserved names: Avoid using reserved folder names as field values. The use of reserved folder names can cause unpredictable results. The following terms are reserved folder names:

- cells
- nodes
- servers
- clusters
- applications
- deployments

Directory path length:

Windows The number of characters in the *profiles_directory_path\profile_name* directory must be less than or equal to 80 characters.

Note:

The host name is the network name for the physical machine on which the node is installed. The host name must resolve to a physical network node on the server. When multiple network cards exist in the server, the host name or IP address must resolve to one of the network cards. Remote nodes use the host name to connect to and communicate with this node. Selecting a host name that other machines can reach within your network is important. Do not use the generic identifier, `localhost`, for this value. Also, do not attempt to install WebSphere Application Server products on a machine with a host name that uses characters from a double-byte character set (DBCS). DBCS characters are not supported when used in the host name.

If you define coexisting nodes on the same computer with unique IP addresses, then define each IP address in a domain name server (DNS) look-up table. Configuration files for standalone application servers do not provide domain name resolution for multiple IP addresses on a machine with a single network address.

The value that you specify for the host name is used as the value of the hostName property in configuration documents for the standalone application server. Specify the host name value in one of the following formats:

- Fully qualified domain name server (DNS) host name string, such as `xmachine.manhattan.ibm.com`
- The default short DNS host name string, such as `xmachine`
- Numeric IP address, such as `127.1.255.3`

The fully qualified DNS host name has the advantages of being unambiguous and flexible. You have the flexibility of changing the actual IP address for the host system without having to change the application server configuration. This value for the host name is particularly useful if you plan to change the IP address frequently when using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. A disadvantage of this format is dependency on DNS. If DNS is not available, then connectivity is compromised.

The short host name is also dynamically resolvable. A short name format has the added function of being redefined in the local hosts file so that the system can run the application server, even when disconnected from the network. To run disconnected, define the short name as the loopback address, `127.0.0.1`, in the hosts file to run disconnected. A disadvantage of this format is a dependency on DNS for remote access. If DNS is not available, then connectivity is compromised.

A numeric IP address has the advantage of not requiring name resolution through DNS. A remote node can connect to the node that you name with a numeric IP address without DNS being available. A disadvantage of this format is that the numeric IP address is fixed. You must change the setting of the hostName property in Express configuration documents whenever you change the machine IP address. Therefore, do not use a numeric IP address if you use DHCP, or if you change IP addresses regularly. Another disadvantage of this format is that you cannot use the node if the host is disconnected from the network.

After displaying characteristics, the tool displays the Administrative security panel.

10. Optionally enable administrative security, and click **Next**.

    You can enable administrative security now during profile creation, or later from the console. If you enable administrative security now, then enter a user name and password to log onto the administrative console.

    After specifying security characteristics, the tool displays the Security certificate panel if you previously selected **Advanced profile creation**.

11. If you selected **Typical profile creation** at the beginning of these steps, then go to the step that displays the Profile summary panel.

12. Create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

    You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

    Note: When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the trust.p12 file.

    If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

13. Verify that the certificate information is correct, and click **Next**.

    If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is `WebAS`. You should change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the java.security file.

    When you create either or both certificates, or import either or both certificates, the keystore files that are created are key.p12, trust.p12, root-key.p12, default-signers.p12, deleted.p12, and ltpa.jceks. These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify. The key.p12 file contains the default personal certificate. The trust.p12 file contains the signer certificate from the default root certificate. The root-key.p12 file contains the root signing certificate. The default-signer.p12 file contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate is in the default-signer.p12 keystore file. The deleted.p12 keystore file is used to hold certificates deleted with the deleteKeyStore task so that they can be recovered if needed. The ltpa.jceks file contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

An imported certificate is added to the key.p12 file or the root-key.p12 file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

After displaying the Security certificate panels, the tool displays the Ports panel if you previously selected **Advanced profile creation**.

14. Verify that the ports within the management profile for the job manager are unique, or intentionally conflicting, and click **Next**.

    If you chose not to deploy the administrative console, then the administrative console ports are disabled on the Ports panel.

    Port conflict resolution

    Ports are recognized as being in use if one of the following conditions exists:

    - The ports are assigned to a profile created from an installation that is performed by the current user.
    - The port is currently in use.

    Validation of ports occurs when you access the Port value assignment panel. Conflicts can still occur between the Port value assignment panel and the Profile creation complete panel because ports are not assigned until profile creation completes.

    If you suspect a port conflict, then you can investigate the port conflict after the profile is created. Determine the ports that are used during profile creation by examining the following files.

    - Linux HP-UX Solaris AIX *profile_root*`/properties/portdef.props` file
    - Windows *profile_root*`\properties\portdef.props` file

    Included in this file are the keys and values that are used in setting the ports. If you discover ports conflicts, then you can reassign ports manually. To reassign ports, run the updatePorts.ant file by using the ws_ant script.

    Windows Linux The tool displays the Windows service definition panel if you are installing on a Windows operating system and the installation ID has the administrative group privilege. The tool displays the Linux service definition panel if you are installing on a supported Linux operating system and the ID that runs the Profile Management Tool is the root user.

15. Choose whether to run the job manager process as a Windows service on a Windows operating system or as a Linux Service on a Linux operating system, and click **Next**.

    The Windows service definition panel is displayed for the Windows operating system only if the ID that installs the Windows service has the administrator group privilege. However, you can run the WASService.exe command to create the Windows service as long as the installer ID belongs to the administrator group. Read about automatically restarting server processes for more information.

    Windows The product attempts to start Windows services for job manager processes that are started by a startServer command. For example, if you configure a job manager as a Windows service and issue the startServer command, then the wasservice command attempts to start the defined service.

    If you chose to install a local system service, then you do not have to specify your user ID or password. If you create a specified user type of service, then you must specify the user ID and the password for the user who runs the service. The user must have `Log on as a service` authority for the service to run correctly. If the user does not have `Log on as a service` authority, then the Profile Management tool automatically adds the authority.

To perform this profile creation task, the user ID must not contain spaces. In addition to belonging to the administrator group, the ID must also have the advanced user right of `Log on as a service`. The Installation program grants the user ID the advanced user right if the user ID does not already have the advanced user right and if the user ID belongs to the administrator group.

You can also create other Windows services after the installation is complete to start other server processes. Read about automatically restarting server processes for more information.

You can remove the Windows service that is added during profile creation during profile deletion. You can also remove the Windows service with the wasservice command.

IPv6 considerations

Profiles created to run as a Windows service fail to start when using Internet Protocol Version 6.0 (IPv6) if the service is configured to run as local system. Create a user-specific environment variable to enable IPv6. Since this environment variable is a user variable instead of a local system variable, only a Windows service that runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as local system. When the Windows service for the job manager process tries to run, the service is unable to access the user environment variable that specifies IPv6, and thus tries to start as IPv4. The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the Windows service for the job manager process runs as the same user ID under which the environment variable that specifies IPv6 is defined, instead of as local system.

Windows The following default values for the Windows service definition panel exist:

- The default is to run as a Windows service.
- The service process is selected to run as a system account.
- The user account is the current user name. User name requirements are the requirements that the Windows operating system imposes for a user ID.
- The startup type is `automatic`. The values for the startup type are those values that the Windows operating system imposes. If you want a startup type other than `automatic`, you can either select another available option from the menu or change the startup type after you create the profile. You can also remove the created service after profile creation, and add it later with the desired startup type. You can choose not to create a service at profile creation time and optionally create the service later with the desired startup type.

Linux The Linux service definition panel is displayed if the current operating system is a supported version of Linux operating systems, and the current user has the appropriate permissions.

The product attempts to start Linux services for application server processes that are started by a startServer command. For example, if you configure an application server as a Linux service and issue the startServer command, then the **wasservice** command attempts to start the defined service.

By default, the product is not selected to run as a Linux service.

To create the service, the user that runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a non-root user ID, then the Linux service definition panel is not displayed, and no service is created.

When you create a Linux service, you must specify a user name from which the service runs.

To delete a Linux service, the user must be the root user or have appropriate privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service for the user.

The tool displays the Profile Creation Summary panel.

16. Click **Create** to create the management profile for the job manager, or click **Back** to change the characteristics of the profile.

    The Profile creation progress panel, which shows the configuration commands that are running, is displayed.

    When the profile creation completes, the tool displays the Profile creation complete panel.

17. Optionally, select **Launch the First steps console**. Click **Finish** to exit.

    With the First steps console, you can create additional profiles and start the application server.

Results

You created a management profile for the job manager.

Refer to the description of the manageprofiles command to learn about creating a profile using a command instead of the Profile Management Tool.

What to do next

Access the job manager console to perform a variety of administrative tasks. You can coordinate management actions among multiple deployment managers, administer multiple unfederated application servers, asynchronously submit jobs to start servers, and so on.

Creating secure proxy profiles

You can create a secure proxy profile to serve as the initial point of entry into your enterprise environment. Typically, a secure proxy server exists in the demilitarized zone (DMZ), accepts requests from clients on the Internet, and forwards the requests to servers in your enterprise environment.

Before you begin

Before you use the Profile Management Tool, install the core product files. You can create two different secure proxy profiles depending on which core product files you install. The core product files could either be for a WebSphere Application Server, Network Deployment installation or a DMZ Secure Proxy Server installation. Read about the profiles created for the different installations in About this task.

The Profile Management Tool is the graphical user interface for the manageprofiles command. See the description of the manageprofiles command for more information.

You must provide enough system temporary space to create a profile. For information, read about the file system requirements for profiles.

Attention: When you launch the Profile Management Tool, the tool could lock up in the following situation for a non-root user: Log into a machine as root, use the SetPermissions utility to change the user from *x* to *y*. Assume that you are user *x* and log back into the machine. Launch the Profile Management Tool, click **Profile Management Tool**, and click **Create**. The next click after the click on **Create** could lock up the tool.

Attention: Solaris When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons of the Profile Management Tool. To fix the problem, add the following lines to the *app_server_root*/.Xdefaults file:

```
Eclipse*spacing:0
Eclipse*fontList:-misc-fixed-medium-r-normal-*-10-100-75-75-c-60-iso8859-1
```

After adding the lines, run the following command before launching the Profile Management Tool:

```
xrdb -load user_home/.Xdefaults
```

About this task

After installing the core product files for the product, you must create a profile. This procedure describes creating a secure proxy profile using the graphical user interface that is provided by the Profile Management Tool. You can also use the manageprofiles command to create a secure proxy profile. See the description of the manageprofiles command for more information.

You can create profiles with the Profile Management Tool using the typical profile creation process or the advanced profile creation process. The typical profile creation process uses default settings and assigns unique port values. You can optionally set values as allowed. For the advanced profile creation process you can accept the default values, or specify your own values.

You can create two different profiles for the DMZ Secure Proxy Server using this task. You can create a secure proxy server profile on a WebSphere Application Server, Network Deployment installation. However, you can only configure this profile in a WebSphere Application Server, Network Deployment installation. To use the secure proxy server of the profile, you must export the profile from the WebSphere Application Server, Network Deployment environment and then import it into the DMZ Secure Proxy Server installation. Read about exporting and importing the secure proxy profile in the topic about the ConfigArchiveOperations command group for the AdminTask object. Alternatively, you can create a secure proxy server profile on a DMZ Secure Proxy Server installation. In this situation the secure proxy server does not have a web container, and so cannot host an administrative console. To administer this secure proxy server, you must employ wsadmin scripting commands.

Procedure

1. Start the Profile Management Tool to create a new runtime environment.

   You can use one of the following ways to start the tool.

   - At the end of installation, select the check box to launch the Profile Management Tool.
   - Issue the command to open the WebSphere Customization Toolbox directly from a command prompt; then, open the Profile Management Tool.
   - Select the **WebSphere Customization Toolbox** option from the First steps console; then, open the Profile Management Tool.
   - Windows Use the **Start** menu to access the WebSphere Customization Toolbox; then, open the Profile Management Tool.
   - Linux Use the Linux operating system menus that are used to start programs to start the WebSphere Customization Toolbox; then, open the Profile Management Tool.
2. Click **Create** on the Profiles tab to create a new profile.

   The Profiles tab contains a list of profiles that have been created on your machine. No action can be done on a selected profile unless the profile can be augmented. The Augment button is greyed out unless a profile that you select can be augmented.

   The tool displays the Environment selection panel.
3. Select **Secure proxy (configuration only)** for the WebSphere Application Server, Network Deployment image, or **Secure proxy** for the DMZ image, and click **Next**.

   The Profile creation options panel is displayed.
4. Select either **Typical profile creation** or **Advanced profile creation**, and click **Next**.

   The **Typical profile creation** option creates a profile that uses default configuration settings. With the **Advanced profile creation** option, you can specify your own configuration values for a profile.
5. If you selected **Typical profile creation** at the beginning of these steps, then go to the step that displays the administrative security.
6. Specify a name for the profile and the directory path for the profile directory, or accept the default values. Then, click **Next**.

   Profile naming guidelines: Double-byte characters are supported. The profile name can be any unique name with the following restrictions. Do not use any of the following characters when naming your profile:

   - Spaces
   - Special characters that are not supported within the name of a directory on your operating system, such as `*&?`
   - Slashes (/) or (\)

   The default profile

The first profile that you create on a machine is the default profile. The default profile is the default target for commands that are issued from the `bin` directory in the product installation root. When only one profile exists on a machine, every command works on the single server process in the configuration. You can make another profile the default profile when you create that profile by checking **Make this profile the default** on the Profile name and location panel of the **Advanced profile creation** path. You can also make another profile the default profile using the manageprofiles command after you create the profile.

Addressing a profile in a multiprofile environment

When multiple profiles exist on a machine, certain commands require that you specify the profile to which the command applies if the profile is not the default profile. These commands use the -profileName parameter to identify which profile to address. You might find it easier to use the commands that are in the `bin` directory of each profile.

Use these commands to query the command shell to determine the calling profile and to address these commands to the calling profile.

Default profile information

The default profile name is <*profile_type*><*profile_number*>:

- <*profile_type*> is a value of `AppSrv`, `Dmgr`, `Custom`, `AdminAgent`, `JobMgr`, or `SecureProxySrv`.
- <*profile_number*> is a sequential number that is used to create a unique profile name

AIX HP-UX Linux Solaris The default profile directory is *app_server_root*/profiles, where *app_server_root* is the installation root.

Windows The default profile directory is *app_server_root*\profiles, where *app_server_root* is the installation root.

7. On the Node and Host Names panel, specify a unique node name, a server name, and the actual host name of the machine. Click **Next**.

Table 32. Characteristics of the secure proxy server node.

This table shows the characteristics of the secure proxy server node.

Field name	Default value	Constraints	Description
Node name	*shortHostName* Node where: • *shortHostName* is the short host name. • *NodeNumber* is a sequential number starting at 01.	Use a unique name for the secure proxy server.	The name is used for administration within the deployment manager cell.
Server name	proxy1	Specifies a logical name for the server. Server names must be unique within a node. However, for multiple nodes within a cluster, you might have different servers with the same server name as long as the server and node pair are unique.	The server name is used for administration within the deployment manager cell.
Host name	The long form of the domain name server (DNS) name.	The host name must be addressable through your network. Read about host name considerations.	Use the actual DNS name or IP address of your machine to enable communication with your machine. See additional information about the host name that follows this table.

Reserved names: Avoid using reserved folder names as field values. The use of reserved folder names can cause unpredictable results. The following terms are reserved folder names:

- cells
- nodes
- servers
- clusters

- applications
- deployments

Directory path length:

Windows The number of characters in the *profiles_directory_path\profile_name* directory must be less than or equal to 80 characters.

Host name considerations:

The host name is the network name for the physical machine on which the node is installed. The host name must resolve to a physical network node on the server. When multiple network cards exist in the server, the host name or IP address must resolve to one of the network cards. Remote nodes use the host name to connect to and communicate with this node. Selecting a host name that other machines can reach within your network is important. Do not use the generic identifier, `localhost`, for this value. Also, do not attempt to install WebSphere Application Server products on a machine with a host name that uses characters from a double-byte character set (DBCS). DBCS characters are not supported when used in the host name.

If you define coexisting nodes on the same computer with unique IP addresses, then define each IP address in a domain name server (DNS) look-up table. Configuration files for standalone application servers do not provide domain name resolution for multiple IP addresses on a machine with a single network address.

The value that you specify for the host name is used as the value of the hostName property in configuration documents for the standalone application server. Specify the host name value in one of the following formats:

- Fully qualified domain name server (DNS) host name string, such as `xmachine.manhattan.ibm.com`
- The default short DNS host name string, such as `xmachine`
- Numeric IP address, such as `127.1.255.3`

The fully qualified DNS host name has the advantages of being unambiguous and flexible. You have the flexibility of changing the actual IP address for the host system without having to change the application server configuration. This value for the host name is particularly useful if you plan to change the IP address frequently when using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. A disadvantage of this format is dependency on DNS. If DNS is not available, then connectivity is compromised.

The short host name is also dynamically resolvable. A short name format has the added function of being redefined in the local hosts file so that the system can run the application server, even when disconnected from the network. To run disconnected, define the short name as the loopback address, `127.0.0.1`, in the hosts file to run disconnected. A disadvantage of this format is a dependency on DNS for remote access. If DNS is not available, then connectivity is compromised.

A numeric IP address has the advantage of not requiring name resolution through DNS. A remote node can connect to the node that you name with a numeric IP address without DNS being available. A disadvantage of this format is that the numeric IP address is fixed. You must change the setting of the hostName property in Express configuration documents whenever you change the machine IP address. Therefore, do not use a numeric IP address if you use DHCP, or if you change IP addresses regularly. Another disadvantage of this format is that you cannot use the node if the host is disconnected from the network.

After displaying the node name, server name, and host name for the secure proxy profile, the tool displays the Security Level Selection panel.

8. Accept the defaults or change the proxy security level and the protocols, and click **Next**.

   You can optionally change your security settings after you create the secure proxy server profile. Read about tuning security properties for the secured proxy server.

   After displaying the security level options, the tool displays the Administrative security panel.

9. Optionally enable administrative security, and click **Next**.

   You can enable administrative security now during profile creation, or later from the console. If you enable administrative security now, then enter a user name and password to log onto the administrative console.

   After specifying security characteristics, the tool displays the Security certificate panel if you previously selected **Advanced profile creation**.

10. If you selected **Typical profile creation** at the beginning of these steps, then go to the step that displays the Profile summary panel.

11. Create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

    You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

    Note: When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the trust.p12 file.

    If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

12. Verify that the certificate information is correct, and click **Next**.

    If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is `WebAS`. You should change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the java.security file.

    When you create either or both certificates, or import either or both certificates, the keystore files that are created are key.p12, trust.p12, root-key.p12, default-signers.p12, deleted.p12, and ltpa.jceks. These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify. The key.p12 file contains the default personal certificate. The trust.p12 file contains the signer certificate from the default root certificate. The root-key.p12 file contains the root signing certificate. The default-signer.p12 file contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate is in the default-signer.p12 keystore file. The deleted.p12 keystore file is used to hold certificates deleted with the deleteKeyStore task so that they can be recovered if needed. The ltpa.jceks file contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

An imported certificate is added to the key.p12 file or the root-key.p12 file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

After displaying the Security certificate panels, the tool displays the Ports panel if you previously selected **Advanced profile creation**.

13. Verify that the ports within the secure proxy profile are unique, or intentionally conflicting, and click **Next**.

    Port conflict resolution

    Ports are recognized as being in use if one of the following conditions exists:

    - The ports are assigned to a profile created from an installation that is performed by the current user.
    - The port is currently in use.

    Validation of ports occurs when you access the Port value assignment panel. Conflicts can still occur between the Port value assignment panel and the Profile creation complete panel because ports are not assigned until profile creation completes.

    If you suspect a port conflict, then you can investigate the port conflict after the profile is created. Determine the ports that are used during profile creation by examining the following files.

    - Linux HP-UX Solaris AIX *profile_root*/`properties/portdef.props` file
    - Windows *profile_root*\`properties\portdef.props` file

    Included in this file are the keys and values that are used in setting the ports. If you discover ports conflicts, then you can reassign ports manually. To reassign ports, run the updatePorts.ant file by using the ws_ant script.

    Windows Linux The tool displays the Windows service definition panel if you are installing on a Windows operating system and the installation ID has the administrative group privilege. The tool displays the Linux service definition panel if you are installing on a supported Linux operating system and the ID that runs the Profile Management Tool is the root user.

14. Choose whether to run the secure proxy server as a Windows service on a Windows operating system or as a Linux Service on a Linux operating system, and click **Next**.

    The Windows service definition panel is displayed for the Windows operating system only if the ID that installs the Windows service has the administrator group privilege. However, you can run the WASService.exe command to create the Windows service as long as the installer ID belongs to the administrator group. Read about automatically restarting server processes for more information.

    Windows The product attempts to start Windows services for secure proxy processes that are started by a startServer command. For example, if you configure a secure proxy server as a Windows service and issue the startServer command, then the wasservice command attempts to start the defined service.

    If you chose to install a local system service, then you do not have to specify your user ID or password. If you create a specified user type of service, then you must specify the user ID and the password for the user who runs the service. The user must have `Log on as a service` authority for the service to run correctly. If the user does not have `Log on as a service` authority, then the Profile Management tool automatically adds the authority.

    To perform this profile creation task, the user ID must not contain spaces. In addition to belonging to the administrator group, the ID must also have the advanced user right of `Log on as a service`. The Installation program grants the user ID the advanced user right if the user ID does not already have the advanced user right and if the user ID belongs to the administrator group.

    You can also create other Windows services after the installation is complete to start other server processes. Read about automatically restarting server processes for more information.

You can remove the Windows service that is added during profile creation during profile deletion. You can also remove the Windows service with the wasservice command.

IPv6 considerations

Profiles created to run as a Windows service fail to start when using Internet Protocol Version 6.0 (IPv6) if the service is configured to run as local system. Create a user-specific environment variable to enable IPv6. Since this environment variable is a user variable instead of a local system variable, only a Windows service that runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as local system. When the Windows service for the secure proxy server process attempts to run, the service is unable to access the user environment variable that specifies IPv6, and thus attempts to start as IPv4. The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the Windows service for the secure proxy server process runs as the same user ID from which the environment variable that specifies IPv6 is defined, instead of as Local System.

Windows The following default values for the Windows service definition panel exist:

- The default is to run as a Windows service.
- The service process is selected to run as a system account.
- The user account is the current user name. User name requirements are the requirements that the Windows operating system imposes for a user ID.
- The startup type is `automatic`. The values for the startup type are those values that the Windows operating system imposes. If you want a startup type other than `automatic`, you can either select another available option from the menu or change the startup type after you create the profile. You can also remove the created service after profile creation, and add it later with the desired startup type. You can choose not to create a service at profile creation time and optionally create the service later with the desired startup type.

Linux The Linux service definition panel is displayed if the current operating system is a supported version of Linux operating systems, and the current user has the appropriate permissions.

The product attempts to start Linux services for application server processes that are started by a startServer command. For example, if you configure an application server as a Linux service and issue the startServer command, then the **wasservice** command attempts to start the defined service.

By default, the product is not selected to run as a Linux service.

To create the service, the user that runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a non-root user ID, then the Linux service definition panel is not displayed, and no service is created.

When you create a Linux service, you must specify a user name from which the service runs.

To delete a Linux service, the user must be the root user or have appropriate privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service for the user.

The tool displays the Profile creation summary panel.

15. Click **Create** to create the secure proxy server profile, or click **Back** to change the characteristics of the profile.

    The Profile creation progress panel, which shows the configuration commands that are running, is displayed.

    When the profile creation completes, the tool displays the Profile creation complete panel.

16. If the secure proxy profile that you are creating is part of the DMZ Secure Proxy Server for IBM WebSphere Application Server installation, optionally select **Launch the First steps console**. Click **Finish** to exit.

    With the First steps console, you can create additional profiles, and start the application server.

    If the secure proxy profile that you are creating is part of the WebSphere Application Server, Network Deployment installation, you do not have the option of launching the First steps console.

Results

Depending on your installation, you have either created a secure proxy server profile on a WebSphere Application Server, Network Deployment image or a secure proxy profile on a DMZ Secure Proxy Server installation.

Refer to the description of the manageprofiles command to learn about creating a profile using a command instead of the Profile Management Tool.

What to do next

The secure proxy server can accept requests from clients on the Internet and forward the requests to servers in your enterprise environment.

The secure proxy profile is available both on the WebSphere Application Server, Network Deployment and the DMZ images. You cannot start the profile on the WebSphere Application Server, Network Deployment image. The profile is used only for configuration on an administrative console. After you configure the profile, you can export it and then import it into the secure proxy profile of the DMZ image. The secure proxy profile is fully operational on the DMZ image.

Creating cell profiles

You can create a cell profile in a single pass with the Profile Management Tool. This cell profile contains a federated application server node and a deployment manager.

Before you begin

Before you use the Profile Management Tool, install the product files.

The Profile Management Tool is the graphical user interface for the manageprofiles command. See the description of the manageprofiles command for more information.

You must provide enough system temporary space to create a profile. For information, read about the file system requirements for profiles.

Attention: When you launch the Profile Management Tool, the tool could lock up in the following situation for a non-root user: Log into a machine as root, use the SetPermissions utility to change the user from *x* to *y*. Assume that you are user *x* and log back into the machine. Launch the Profile Management Tool, click **Profile Management Tool**, and click **Create**. The next click after the click on **Create** could lock up the tool.

Attention: Solaris When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons of the Profile Management Tool. To fix the problem, add the following lines to the *app_server_root*/.Xdefaults file:

```
Eclipse*spacing:0
Eclipse*fontList:-misc-fixed-medium-r-normal-*-10-100-75-75-c-60-iso8859-1
```

After adding the lines, run the following command before launching the Profile Management Tool:

```
xrdb -load user_home/.Xdefaults
```

About this task

After installing the core product files for the Network Deployment product, you must create a profile. This procedure describes how to create a cell profile with the Profile Management Tool, which is a graphical user interface. You can also use the manageprofiles command to create a cell profile. See the description of the manageprofiles command for more information.

A cell profile contains a deployment manager profile and a federated application server node profile. You can federate additional Application Server node profiles into this deployment manager profile after initial creation of the cell profile.

You can create profiles with the Profile Management Tool using the typical profile creation process or the advanced profile creation process. The typical profile creation process uses default settings and assigns unique port values. You can optionally set values as allowed. For the advanced profile creation process you can accept the default values, or specify your own values.

Procedure

1. Start the Profile Management Tool to create a new runtime environment.

   You can use one of the following ways to start the tool.

   - At the end of installation, select the check box to launch the Profile Management Tool.
   - Issue the command to open the WebSphere Customization Toolbox directly from a command prompt; then, open the Profile Management Tool.
   - Select the **WebSphere Customization Toolbox** option from the First steps console; then, open the Profile Management Tool.
   - Windows Use the **Start** menu to access the WebSphere Customization Toolbox; then, open the Profile Management Tool.
   - Linux Use the Linux operating system menus that are used to start programs to start the WebSphere Customization Toolbox; then, open the Profile Management Tool.
2. Click **Create** on the Profiles tab to create a new profile.

   The Profiles tab contains a list of profiles that have been created on your machine. No action can be done on a selected profile unless the profile can be augmented. The Augment button is greyed out unless a profile that you select can be augmented.

   The tool displays the Environment selection panel.
3. Select the cell profile, then click **Next**.

   The Profile creation options panel is displayed.
4. Select either **Typical profile creation** or **Advanced profile creation**, and click **Next**.

   The **Typical profile creation** option creates a profile that uses default configuration settings. With the **Advanced profile creation** option, you can specify your own configuration values for a profile.
5. If you selected **Typical profile creation**, go to the step on administrative security.
6. If you selected **Advanced profile creation**, then select the applications that you want to deploy, and click **Next**.

   The tool displays the Profile name and location panel.
7. If you selected **Advanced profile creation**, then specify the deployment manager profile name, the application server profile name and the profile directory on the Profile name and location panel, or accept the defaults. Click **Next**.

   Profile naming guidelines: Double-byte characters are supported. The profile name can be any unique name with the following restrictions. Do not use any of the following characters when naming your profile:

   - Spaces
   - Special characters that are not supported within the name of a directory on your operating system, such as `*&?`
   - Slashes (/) or (\)

   The default profile

   The first profile that you create on a machine is the default profile. The default profile is the default target for commands that are issued from the `bin` directory in the product installation root. When only one profile exists on a machine, every command works on the single server process in the configuration. You can make another profile the default profile when you create that profile by checking **Make this profile the default** on the Profile name and location panel of the **Advanced profile creation** path. You can also make another profile the default profile using the manageprofiles command after you create the profile.

Addressing a profile in a multiprofile environment:

When multiple profiles exist on a machine, certain commands require that you specify the -profileName parameter if the profile is not the default profile. In those cases, it might be easier to use the commands that are in the `bin` directory of each profile. When you issue one of these commands within the `bin` directory of a profile, the command acts on that profile unless the -profileName parameter specifies a different profile.

Default profile information

The default profile name is *`<profile_type><profile_number>`*:

- *`<profile_type>`* is a value of `AppSrv`, `Dmgr`, `Custom`, `AdminAgent`, `JobMgr`, or `SecureProxySrv`.
- *`<profile_number>`* is a sequential number that is used to create a unique profile name

AIX HP-UX Linux Solaris The default profile directory is *app_server_root*/profiles, where *app_server_root* is the installation root.

Windows The default profile directory is *app_server_root*\profiles, where *app_server_root* is the installation root.

The tool then displays the Node, host, and cell names panel.

8. Specify a unique deployment manager node name, a unique application server node name, the actual host name of the machine, and a unique cell name for the cell, and click **Next**.

Table 33. Characteristics of the cell profile.

This table shows the characteristics of the cell profile.

Field Name	Default Value	Constraints	Description

Deployment manager node name	*`shortHostName`*
	`CellManager`
	`NodeNumber`
	where:
	• *shortHostName* is the short host name.
	• *NodeNumber* is a sequential number starting at 01.
		Use a unique name for the deployment manager.	The name is used for administration within the deployment manager cell.

Application server node name	*`shortHostName`*
	`Node`
	`NodeNumber`
	where:
	• *shortHostName* is the short host name
	• *NodeNumber* is a sequential number starting at 01
		Use a unique name for the application server.	The name is used for administration within the deployment manager cell.

Host name	The long form of the domain name server (DNS) name.	The host name must be addressable through your network.	Use the actual DNS name or IP address of your machine to enable communication with your machine. See additional information about the host name that follows this table.

Table 33. Characteristics of the cell profile (continued).

This table shows the characteristics of the cell profile.

Field Name	Default Value	Constraints	Description
Cell name	*shortHostName* Cell *CellNumber* where: • *shortHostName* is the short host name. • *CellNumber* is a sequential number starting at 01.	Use a unique name for the deployment manager cell. If you plan to migrate a Version 6 or Version 7 deployment manager cell to this Version 8 deployment manager, use the same cell name as the Version 6 or Version 7 deployment manager. A cell name must be unique in any circumstance in which the product is running on the same physical machine or cluster of machines, such as a sysplex. Additionally, a cell name must be unique in any circumstance in which network connectivity between entities is required either between the cells or from a client that must communicate with each of the cells. Cell names must also be unique if their namespaces are federated. Otherwise, you might encounter symptoms such as a javax.naming.NameNotFoundException error, in which case, create uniquely named cells.	All federated nodes become members of the deployment manager cell, which you name in this panel.

Reserved names: Avoid using reserved folder names as field values. The use of reserved folder names can cause unpredictable results. The following terms are reserved folder names:

- cells
- nodes
- servers
- clusters
- applications
- deployments

Directory path considerations:

Windows The number of characters in the *profiles_directory_path\ profile_name* directory must be less than or equal to 80 characters.

Host name considerations:

The host name is the network name for the physical machine on which the node is installed. The host name must resolve to a physical network node on the server. When multiple network cards exist in the server, the host name or IP address must resolve to one of the network cards. Remote nodes use the host name to connect to and communicate with this node. Selecting a host name that other machines can reach within your network is important. Do not use the generic identifier, `localhost`, for this value. Also, do not attempt to install WebSphere Application Server products on a machine with a host name that uses characters from a double-byte character set (DBCS). DBCS characters are not supported when used in the host name.

If you define coexisting nodes on the same computer with unique IP addresses, then define each IP address in a domain name server (DNS) look-up table. Configuration files for standalone application servers do not provide domain name resolution for multiple IP addresses on a machine with a single network address.

The value that you specify for the host name is used as the value of the hostName property in configuration documents for the standalone application server. Specify the host name value in one of the following formats:

- Fully qualified domain name server (DNS) host name string, such as `xmachine.manhattan.ibm.com`
- The default short DNS host name string, such as `xmachine`
- Numeric IP address, such as `127.1.255.3`

The fully qualified DNS host name has the advantages of being unambiguous and flexible. You have the flexibility of changing the actual IP address for the host system without having to change the application server configuration. This value for the host name is particularly useful if you plan to change the IP address frequently when using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. A disadvantage of this format is dependency on DNS. If DNS is not available, then connectivity is compromised.

The short host name is also dynamically resolvable. A short name format has the added function of being redefined in the local hosts file so that the system can run the application server, even when disconnected from the network. To run disconnected, define the short name as the loopback address, `127.0.0.1`, in the hosts file to run disconnected. A disadvantage of this format is a dependency on DNS for remote access. If DNS is not available, then connectivity is compromised.

A numeric IP address has the advantage of not requiring name resolution through DNS. A remote node can connect to the node that you name with a numeric IP address without DNS being available. A disadvantage of this format is that the numeric IP address is fixed. You must change the setting of the hostName property in Express configuration documents whenever you change the machine IP address. Therefore, do not use a numeric IP address if you use DHCP, or if you change IP addresses regularly. Another disadvantage of this format is that you cannot use the node if the host is disconnected from the network.

After displaying the cell characteristics, the tool displays the Administrative security panel.

9. Optionally enable administrative security, and click **Next**.

   You can enable administrative security now during profile creation, or later from the console. If you enable administrative security now, then enter a user name and password to log onto the administrative console.

   After specifying security characteristics, the tool displays the Security certificate panel if you previously selected **Advanced profile creation**.

10. If you selected **Typical profile creation** at the beginning of these steps, then go to the step that displays the Profile summary panel.

11. Create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

    You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

    Note: When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the trust.p12 file.

    If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

12. Verify that the certificate information is correct, and click **Next**.

If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is `WebAS`. You should change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the java.security file.

When you create either or both certificates, or import either or both certificates, the keystore files that are created are key.p12, trust.p12, root-key.p12, default-signers.p12, deleted.p12, and ltpa.jceks. These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify. The key.p12 file contains the default personal certificate. The trust.p12 file contains the signer certificate from the default root certificate. The root-key.p12 file contains the root signing certificate. The default-signer.p12 file contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate is in the default-signer.p12 keystore file. The deleted.p12 keystore file is used to hold certificates deleted with the deleteKeyStore task so that they can be recovered if needed. The ltpa.jceks file contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

An imported certificate is added to the key.p12 file or the root-key.p12 file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

After displaying the Security certificate panels, the tool displays the Ports panel if you previously selected **Advanced profile creation**.

13. Verify that the ports specified for the deployment manager are unique, and click **Next**.

    If you chose not to deploy the administrative console, then the administrative console ports are disabled on the Ports panel.

    Port conflict resolution

    Ports are recognized as being in use if one of the following conditions exists:

    - The ports are assigned to a profile created from an installation that is performed by the current user.
    - The port is currently in use.

    Validation of ports occurs when you access the Port value assignment panel. Conflicts can still occur between the Port value assignment panel and the Profile creation complete panel because ports are not assigned until profile creation completes.

    If you suspect a port conflict, then you can investigate the port conflict after the profile is created. Determine the ports that are used during profile creation by examining the following files.

    - Linux HP-UX Solaris AIX *profile_root*`/properties/portdef.props` file
    - Windows *profile_root*`\properties\portdef.props` file

    Included in this file are the keys and values that are used in setting the ports. If you discover ports conflicts, then you can reassign ports manually. To reassign ports, run the updatePorts.ant file by using the ws_ant script.

14. Verify that the ports specified for the application server are unique, and click **Next**.

    The same discussion on ports in the previous step applies to this step.

    Windows Linux The tool displays the Windows service definition panel if you are installing on a Windows operating system and the installation ID has the administrative group privilege. The tool displays the Linux service definition panel if you are installing on a supported Linux operating system and the ID that runs the Profile Management Tool is the root user.

15. Choose whether to run the application server as a Windows service on a Windows operating system or as a Linux service on a Linux operating system, then click **Next**.

- Windows

  The Windows service definition panel is displayed for the Windows operating system only if the ID that installs the Windows service has the administrator group privilege. However, you can run the WASService.exe command to create the Windows service as long as the installer ID belongs to the administrator group. Read about automatically restarting server processes for more information.

  Windows The product attempts to start Windows services for application server processes that are started by a startServer command. For example, if you configure an application server as a Windows service, and issue the startServer command, then the **wasservice** command attempts to start the defined service.

  If you chose to install a local system service, then you do not have to specify your user ID or password. If you create a specified user type of service, then you must specify the user ID and the password for the user who runs the service. The user must have `Log on as a service` authority for the service to run correctly. If the user does not have `Log on as a service` authority, then the Profile Management tool automatically adds the authority.

  To perform this profile creation task, the user ID must not contain spaces. In addition to belonging to the administrator group, the ID must also have the advanced user right of `Log on as a service`. The Installation program grants the user ID the advanced user right if the user ID does not already have the advanced user right and if the user ID belongs to the administrator group.

  You can also create other Windows services after the installation is complete to start other server processes. Read about automatically restarting server processes for more information.

  You can remove the Windows service that is added during profile creation during profile deletion. You can also remove the Windows service with the wasservice command.

  IPv6 considerations

  Profiles created to run as a Windows service fail to start when using Internet Protocol Version 6 (IPv6) if the service is configured to run as local system. Create a user-specific environment variable to enable IPv6. Since this environment variable is a user variable instead of a local system variable, only a Windows service that runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as local system. When the Windows service for the product tries to run, the service is unable to access the user environment variable that specifies IPv6, and thus, tries to start as Internet Protocol Version 4 (IPv4). The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the Windows service for the product runs with the same user ID from which the environment variable that specifies IPv6 is defined, instead of as local system.

  Default values for the Windows service

  Windows The following default values for the Windows service definition panel exist:

  – The default is to run as a Windows service.

  – The service process is selected to run as a system account.

  – The user account is the current user name. User name requirements are the requirements that the Windows operating system imposes for a user ID.

  – The startup type is `automatic`. The values for the startup type are those values that the Windows operating system imposes. If you want a startup type other than `automatic`, you can either select another available option from the menu or change the startup type after you create the profile. You can also remove the created service after profile creation, and add it later with the desired startup type. You can choose not to create a service at profile creation time and optionally create the service later with the desired startup type.

- Linux

  The Linux service definition panel is displayed if the current operating system is a supported version of Linux operating systems, and the current user has the appropriate permissions.

The product attempts to start Linux services for application server processes that are started by a startServer command. For example, if you configure an application server as a Linux service and issue the startServer command, then the **wasservice** command attempts to start the defined service.

By default, the product is not selected to run as a Linux service.

To create the service, the user that runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a non-root user ID, then the Linux service definition panel is not displayed, and no service is created.

When you create a Linux service, you must specify a user name from which the service runs.

To delete a Linux service, the user must be the root user or have appropriate privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service for the user.

If you previously selected **Advanced profile creation**, the next panel displays the web server definition panel.

16. For advanced profile creation, if you choose to include a web server definition in the profile now, specify the web server characteristics on the panels, and click **Next** until you complete the web server definition panels.

    If you use a web server to route requests to the product, then you need to include a web server definition. You can include the definition now, or define the web server to the product later. If you define the Web server definition during the creation of this profile, then you can install the web server and its plug-in after you create the profile. However, you must install both to the paths that you specify on the web server definition panels. If you define the web server to the product after you create this profile, then you must define the Web server in a separate profile.

    The tool displays the Profile Creation Summary panel.

17. Click **Create** to create the cell profile, or click **Back** to change the characteristics of the cell profile.

    The Profile creation progress panel, which shows the configuration commands that are running, is displayed.

    When the profile creation completes, the tool displays the Profile creation complete panel.

18. Optionally, select **Launch the First steps console**. Click **Finish** to exit.

    With the First steps console, you can create additional profiles and start the application server.

Results

You created a cell profile.

Refer to the description of the manageprofiles command to learn about creating a profile using a command instead of the Profile Management Tool.

What to do next

Deploy an application to get started.

Read about fast paths for the product to get started deploying applications.

Creating custom profiles

Create a custom profile so that you can include application servers, clusters, or other Java processes, such as a messaging server, in its empty node. You can use the Profile Management Tool to create a custom profile.

Before you begin

Before you use the Profile Management Tool, install the product files.

The Profile Management Tool is the graphical user interface for the manageprofiles command. See the description of the manageprofiles command for more information.

You must provide enough system temporary space to create a profile. For information, read about the file system requirements for profiles.

Attention: When you launch the Profile Management Tool, the tool could lock up in the following situation for a non-root user: Log into a machine as root, use the SetPermissions utility to change the user from *x* to *y*. Assume that you are user *x* and log back into the machine. Launch the Profile Management Tool, click **Profile Management Tool**, and click **Create**. The next click after the click on **Create** could lock up the tool.

Attention: Solaris When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons of the Profile Management Tool. To fix the problem, add the following lines to the *app_server_root*/.Xdefaults file:

```
Eclipse*spacing:0
Eclipse*fontList:-misc-fixed-medium-r-normal-*-10-100-75-75-c-60-iso8859-1
```

After adding the lines, run the following command before launching the Profile Management Tool:

```
xrdb -load user_home/.Xdefaults
```

About this task

After installing the core product files for the WebSphere Application Server, Network Deployment product, you must create a profile. This topic describes creating a custom profile using the Profile Management Tool. A custom profile is an empty node that you can customize to include application servers, clusters, or other Java processes, such as a messaging server.

You can also use the manageprofiles command to create a custom profile. See the description of the manageprofiles command for more information.

By default, the Profile Management Tool federates a custom node when you create a custom profile. Federating the node makes the node operational. You must have access to a running deployment manager to federate the node. Otherwise, a connection error displays. You can federate the node later if you do not have access to a running deployment manager, or for any other reason.

If the custom profile is on a machine that does not have a deployment manager, then the deployment manager must be accessible over the network to support the federation of the node.

You can create profiles with the Profile Management Tool using the typical profile creation process or the advanced profile creation process. The typical profile creation process uses default settings and assigns unique port values. You can optionally set values as allowed. For the advanced profile creation process you can accept the default values, or specify your own values.

Procedure

1. Install the product to create the core product files.
2. Start the Profile Management Tool to create a new runtime environment.

   You can use one of the following ways to start the tool.

   - At the end of installation, select the check box to launch the Profile Management Tool.
   - Issue the command to open the WebSphere Customization Toolbox directly from a command prompt; then, open the Profile Management Tool.
   - Select the **WebSphere Customization Toolbox** option from the First steps console; then, open the Profile Management Tool.

- Windows Use the **Start** menu to access the WebSphere Customization Toolbox; then, open the Profile Management Tool.
- Linux Use the Linux operating system menus that are used to start programs to start the WebSphere Customization Toolbox; then, open the Profile Management Tool.

3. Click **Create** on the Profiles tab to create a new profile.

   The Profiles tab contains a list of profiles that have been created on your machine. No action can be done on a selected profile unless the profile can be augmented. The Augment button is greyed out unless a profile that you select can be augmented.

   The tool displays the Environment selection panel.
4. Select the custom profile, and click **Next**.

   The Profile creation options panel is displayed.
5. Select either **Typical profile creation** or **Advanced profile creation**, and click **Next**.

   The **Typical profile creation** option creates a profile that uses default configuration settings. With the **Advanced profile creation** option, you can specify your own configuration values for a profile.
6. If you selected **Typical profile creation**, then go to the step on federating the node.
7. If you selected **Advanced profile creation**, then specify the custom profile name and the profile directory on the Profile name and location panel, or accept the defaults, and click **Next**.

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

   The default profile

   The first profile that you create on a machine is the default profile. The default profile is the default target for commands that are issued from the `bin` directory in the product installation root. When only one profile exists on a machine, every command works on the single server process in the configuration. You can make another profile the default profile when you create that profile by checking **Make this profile the default** on the Profile name and location panel of the **Advanced profile creation** path. You can also make another profile the default profile using the manageprofiles command after you create the profile.

   Addressing a profile in a multiprofile environment

   When multiple profiles exist on a machine, certain commands require that you specify the profile to which the command applies if the profile is not the default profile. These commands use the -profileName parameter to identify which profile to address. You might find it easier to use the commands that are in the `bin` directory of each profile.

   Use these commands to query the command shell to determine the calling profile and to address these commands to the calling profile.

   Default profile information

   The default profile name is <*profile_type*><*profile_number*>:
   - <*profile_type*> is a value of `AppSrv`, `Dmgr`, `Custom`, `AdminAgent`, `JobMgr`, or `SecureProxySrv`.
   - <*profile_number*> is a sequential number that is used to create a unique profile name

   AIX HP-UX Linux Solaris The default profile directory is *app_server_root*/profiles, where *app_server_root* is the installation root.

   Windows The default profile directory is *app_server_root*\profiles, where *app_server_root* is the installation root.

   The tool then displays the Node and host names panel.
8. Specify the node and host characteristics for the custom profile, and click **Next**.

If you plan to migrate an installation of WebSphere Application Server, Network Deployment Version 6 or Version 7 to Version 8, then use the same cell name for the Version 8 deployment manager that you used for the Version 6 or Version 7 cell. A cell name must be unique in any circumstance in which the product is running on the same physical machine or cluster of machines, such as a sysplex. Additionally, a cell name must be unique in any circumstance in which network connectivity between entities is required either between the cells or from a client that must communicate with each of the cells. Cell names must also be unique if their namespaces are federated. Otherwise, you might encounter symptoms such as a javax.naming.NameNotFoundException error, in which case, create uniquely named cells.

After migrating the cell, the Version 6 or Version 7 managed nodes are now managed by the Version 8 deployment manager in compatibility mode. You can migrate individual Version 6 or Version 7 managed nodes in the cell to Version 8. To do so, you must create a Version 8 profile with the same node name as the Version 6 or Version 7 managed node.

Reserved names: Avoid using reserved folder names as field values. The use of reserved folder names can cause unpredictable results. The following terms are reserved folder names:

- cells
- nodes
- servers
- clusters
- applications
- deployments

Table 34. Characteristics of the custom profile.

This table shows the characteristics of the custom profile.

Field Name	Default Value	Constraints	Description
Node name	*shortHostName* Node *NodeNumber* where: • *shortHostName* is the short host name • *NodeNumber* is a sequential number starting at 01	Avoid using the reserved terms. Use a unique name within the deployment manager cell. If you plan to migrate a Version 5 or Version 6 managed node, then use the same node name for this Version 7 custom profile.	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. After migrating a Version 6 or Version 7 deployment manager cell to a Version 8 deployment manager, you can migrate the Version 6 or Version 7 custom profiles that are running in compatibility mode in the Version 8 deployment manager.
Host name	The long form of the domain name server (DNS) name.	The host name must be addressable through your network.	Use the actual DNS name or IP address of your machine to enable communication with your machine. See additional information about the host name that follows this table.

Directory path considerations:

Windows The number of characters in the *profiles_directory_path\ profile_name* directory must be less than or equal to 80 characters.

Host name considerations:

The host name is the network name for the physical machine on which the node is installed. The host name must resolve to a physical network node on the server. When multiple network cards exist in the server, the host name or IP address must resolve to one of the network cards. Remote nodes use the host name to connect to and communicate with this node. Selecting a host name that other machines can reach within your network is important. Do not use the generic identifier, `localhost`, for this value. Also, do not attempt to install WebSphere Application Server products on a machine with a host name that uses characters from a double-byte character set (DBCS). DBCS characters are not supported when used in the host name.

If you define coexisting nodes on the same computer with unique IP addresses, then define each IP address in a domain name server (DNS) look-up table. Configuration files for standalone application servers do not provide domain name resolution for multiple IP addresses on a machine with a single network address.

The value that you specify for the host name is used as the value of the hostName property in configuration documents for the standalone application server. Specify the host name value in one of the following formats:

- Fully qualified domain name server (DNS) host name string, such as `xmachine.manhattan.ibm.com`
- The default short DNS host name string, such as `xmachine`
- Numeric IP address, such as `127.1.255.3`

The fully qualified DNS host name has the advantages of being unambiguous and flexible. You have the flexibility of changing the actual IP address for the host system without having to change the application server configuration. This value for the host name is particularly useful if you plan to change the IP address frequently when using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. A disadvantage of this format is dependency on DNS. If DNS is not available, then connectivity is compromised.

The short host name is also dynamically resolvable. A short name format has the added function of being redefined in the local hosts file so that the system can run the application server, even when disconnected from the network. To run disconnected, define the short name as the loopback address, `127.0.0.1`, in the hosts file to run disconnected. A disadvantage of this format is a dependency on DNS for remote access. If DNS is not available, then connectivity is compromised.

A numeric IP address has the advantage of not requiring name resolution through DNS. A remote node can connect to the node that you name with a numeric IP address without DNS being available. A disadvantage of this format is that the numeric IP address is fixed. You must change the setting of the hostName property in Express configuration documents whenever you change the machine IP address. Therefore, do not use a numeric IP address if you use DHCP, or if you change IP addresses regularly. Another disadvantage of this format is that you cannot use the node if the host is disconnected from the network.

After specifying custom profile characteristics, the tool displays the Federation panel.

9. If administrative security is enabled for the deployment manager, specify the host name and SOAP port of the deployment manager, and the user name and password for the deployment manager. Click **Next**.

After federation, the process in the custom profile is the node agent process. The node agent process is the agent of the deployment manager for the custom node. The node agent responds to commands from the deployment manager to perform tasks that include the following actions:

- Creating application server processes, clusters, and cluster members
- Starting and stopping application server processes
- Synchronizing configurations between the current edition on the deployment manager and the copy that exists on the node
- Deleting application server processes

Should you federate the node?

The recommendation is that you federate the custom node at this time. The deployment manager must be running and accessible when you click **Next** on the Federation panel to federate the custom node. If the custom profile is on a machine that does not have a deployment manager, then the deployment manager must be running and accessible over the network to allow the federation of the node. If the deployment manager is not running or not accessible before you click **Next**, but you can start it and make it accessible at this time, then do so. Otherwise, select the **Federate the node later** check box.

If you are unsure whether the deployment manager is running or accessible, then do not federate now. Federate the node when you can verify the availability of the deployment manager.

A possibility exists that the deployment manager is reconfigured to use the non-default remote method invocation (RMI) as the preferred Java Management Extensions (JMX) connector. Click **System Administration > Deployment manager > Administrative services** in the administrative console of the deployment manager to verify the preferred connector type.

If RMI is the preferred JMX connector, then you must use the addNode command to federate the custom profile later. Use the addNode command so that you can specify the JMX connector type and the RMI port.

If the deployment manager uses the default SOAP JMX connector type, specify the host name and SOAP port and federate the node now to create a functional node that you can customize.

Federating when the deployment manager is not available

If you federate a custom node when the deployment manager is not running or is not accessible, then an error message is displayed. If the deployment manager becomes unavailable during the profile creation process, then the installation indicator in the logs is `INSTCONFFAIL`, to indicate a complete failure. The resulting custom profile is unusable. You must delete the profile. Read about deleting a profile for more information.

If you chose to federate now, and you previously selected **Advanced profile creation**, then the Security certificate panel displays next. Go to the step on creating and importing certificates.

Otherwise, the Profile Creation Summary panel displays for the typical profile creation option. Go to the step on creating the custom profile.

10. Create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

    You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

    Note: When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the trust.p12 file.

    If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

11. Verify that the certificate information is correct, and click **Next**.

    If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default.

The default keystore password for the root signing certificate is `WebAS`. You should change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the java.security file.

When you create either or both certificates, or import either or both certificates, the keystore files that are created are key.p12, trust.p12, root-key.p12, default-signers.p12, deleted.p12, and ltpa.jceks. These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify. The key.p12 file contains the default personal certificate. The trust.p12 file contains the signer certificate from the default root certificate. The root-key.p12 file contains the root signing certificate. The default-signer.p12 file contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate is in the default-signer.p12 keystore file. The deleted.p12 keystore file is used to hold certificates deleted with the deleteKeyStore task so that they can be recovered if needed. The ltpa.jceks file contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

An imported certificate is added to the key.p12 file or the root-key.p12 file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

After displaying the Security certificate panels, the tool displays the Ports panel if you previously selected **Advanced profile creation**.

12. Verify that the ports within the custom profile are unique, or intentionally conflicting, and click **Next**.

    Port conflict resolution

    If you suspect a port conflict, then you can investigate the port conflict after the profile is created. Determine the ports that are used during profile creation by examining the following files.

    - Linux HP-UX Solaris AIX *profile_root*/`properties/portdef.props` file
    - Windows *profile_root*\\`properties\portdef.props` file

    Included in this file are the keys and values that are used in setting the ports. If you discover ports conflicts, then you can reassign ports manually. To reassign ports, run the updatePorts.ant file by using the ws_ant script.

    The Profile Creation Summary panel is displayed.

13. Click **Create** to create the custom profile, or click **Back** to change the characteristics of the custom profile.

    If you previously chose to federate the custom node on the Federation panel, the deployment manager had to be running and accessible. The deployment manager must be running and accessible when you click **Create**. If you think the deployment manager might no longer be running or might have become inaccessible, then start the deployment manager and make it accessible, or make it accessible if it is already running.

    The Profile creation progress panel, which shows the configuration commands that are running, is displayed.

    When the profile creation completes, the tool displays the Profile creation complete panel.

14. Optionally, select **Launch the First steps console**. Click **Finish** to exit.

    With the First steps console, you can create additional profiles and start the application server.

Results

You created a custom profile. The node within the profile is empty until you federate the node and use the deployment manager to customize the node.

The directory structure shows the new profile folder within the profiles directory. The profile folder has the same name as the profile that you create.

Refer to the description of the manageprofiles command to learn about creating a profile using a command instead of the Profile Management Tool.

The Profile Management Tool creates a log during profile creation. The logs are in the *install_dir*/`logs`/manageprofiles directory. The files are named in this pattern: `manageprofiles_create`*`profile_name`*`.log`.

What to do next

Federate the node into the deployment manager cell if you did not already do so when you created the node. Then, use the deployment manager to create an application server on the node.

Deploy an application to get started.

Read about fast paths for the product to get started deploying applications.

Creating application server profiles

Create an application server profile so that you can make applications available to the Internet or to an intranet, typically using Java technology. You can create an application server profile using the Profile Management Tool.

Before you begin

Before you use the Profile Management Tool, install the product files.

The Profile Management Tool is the graphical user interface for the manageprofiles command. See the description of the manageprofiles command for more information.

You must provide enough system temporary space to create a profile. For information, read about the file system requirements for profiles.

Attention: When you launch the Profile Management Tool, the tool could lock up in the following situation for a non-root user: Log into a machine as root, use the SetPermissions utility to change the user from *x* to *y*. Assume that you are user *x* and log back into the machine. Launch the Profile Management Tool, click **Profile Management Tool**, and click **Create**. The next click after the click on **Create** could lock up the tool.

Attention: Solaris When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons of the Profile Management Tool. To fix the problem, add the following lines to the *app_server_root*/.Xdefaults file:

```
Eclipse*spacing:0
Eclipse*fontList:-misc-fixed-medium-r-normal-*-10-100-75-75-c-60-iso8859-1
```

After adding the lines, run the following command before launching the Profile Management Tool:

```
xrdb -load user_home/.Xdefaults
```

About this task

After installing the core product files for the WebSphere Application Server, Network Deployment product, you must create a profile. This procedure describes creating an application server profile using the graphical user interface provided by the Profile Management Tool. You can also use the manageprofiles command to create an application server profile. See the description of the manageprofiles command for more information.

An application server profile has a default server, which is server1, and the default application that includes the Snoop servlet and the Hitcount servlet. You can federate the application server or use it as a standalone application server.

You can create profiles with the Profile Management Tool using the typical profile creation process or the advanced profile creation process. The typical profile creation process uses default settings and assigns unique port values. You can optionally set values as allowed. For the advanced profile creation process you can accept the default values, or specify your own values.

Procedure

1. Start the Profile Management Tool to create a new runtime environment.

   You can use one of the following ways to start the tool.

   - At the end of installation, select the check box to launch the Profile Management Tool.
   - Issue the command to open the WebSphere Customization Toolbox directly from a command prompt; then, open the Profile Management Tool.
   - Select the **WebSphere Customization Toolbox** option from the First steps console; then, open the Profile Management Tool.
   - Windows Use the **Start** menu to access the WebSphere Customization Toolbox; then, open the Profile Management Tool.
   - Linux Use the Linux operating system menus that are used to start programs to start the WebSphere Customization Toolbox; then, open the Profile Management Tool.
2. Click **Create** on the Profiles tab to create a new profile.

   The Profiles tab contains a list of profiles that have been created on your machine. No action can be done on a selected profile unless the profile can be augmented. The Augment button is greyed out unless a profile that you select can be augmented.

   The tool displays the Environment selection panel.
3. Select **Application server** and click **Next**.

   The Profile creation options panel is displayed.
4. Select either **Typical profile creation** or **Advanced profile creation**, and click **Next**.

   The **Typical profile creation** option creates a profile that uses default configuration settings. With the **Advanced profile creation** option, you can specify your own configuration values for a profile.
5. If you selected **Typical profile creation**, then go to the step on administrative security.
6. If you selected **Advanced profile creation**, then select the applications that you want to deploy; and click **Next**.

   The tool displays the Profile name and location panel.
7. Specify a name for the profile and the directory path for the profile directory, or accept the default values. Then, click **Next**.

   Profile naming guidelines: Double-byte characters are supported. The profile name can be any unique name with the following restrictions. Do not use any of the following characters when naming your profile:

   - Spaces
   - Special characters that are not supported within the name of a directory on your operating system, such as `*&?`
   - Slashes (/) or (\)

   You can create a application server using configuration settings that are optimized for a development environment by checking **Create the server using the development template** on the Profile name and location panel of the **Advanced profile creation** path. The development template reduces startup time and allows the server to run on less powerful hardware.

   Important: Do not use the development template for production servers.

The first profile that you create on a machine is the default profile. The default profile is the default target for commands that are issued from the `bin` directory in the product installation root. When only one profile exists on a machine, every command works on the single server process in the configuration. You can make another profile the default profile when you create that profile by checking **Make this profile the default** on the Profile name and location panel of the **Advanced profile creation** path. You can also make another profile the default profile using the manageprofiles command after you create the profile.

When multiple profiles exist on a machine, certain commands require that you specify the profile to which the command applies if the profile is not the default profile. These commands use the -profileName parameter to identify which profile to address. You might find it easier to use the commands that are in the `bin` directory of each profile.

Use these commands to query the command shell to determine the calling profile and to address these commands to the calling profile.

The default profile name is <*`profile_type`*><*`profile_number`*>:

- <*`profile_type`*> is a value of `AppSrv`, `Dmgr`, `Custom`, `AdminAgent`, `JobMgr`, or `SecureProxySrv`.
- <*`profile_number`*> is a sequential number that is used to create a unique profile name

AIX HP-UX Linux Solaris The default profile directory is *app_server_root*/profiles, where *app_server_root* is the installation root.

Windows The default profile directory is *app_server_root*\profiles, where *app_server_root* is the installation root.

Performance tuning setting: Select the performance-tuning setting that most closely matches the type of environment in which the application server will run.

Standard
The standard settings are the standard out-of-the-box default configuration settings that are optimized for general-purpose usage.

Peak The peak settings are appropriate for a production environment where application changes are rare and optimal runtime performance is important.

Development
The development settings are appropriate for a development environment where frequent application updates are performed and system resources are at a minimum.

Important: Do not use the development settings for production servers.

8. On the Node and host names panel, specify the characteristics for the application server, and click **Next**.

Use unique names for each application server that you create.

Reserved names: Avoid using reserved folder names as field values. The use of reserved folder names can cause unpredictable results. The following terms are reserved folder names:

- cells
- nodes
- servers
- clusters
- applications
- deployments

Some default values in the following table are split on multiple lines for printing purposes.

Field Name	Default Value	Constraints	Description
Node name	*shortHostName*Node*NodeNumber* where: • *shortHostName* is the short host name • *NodeNumber* is a sequential number starting at 01	Avoid using the reserved terms.	Select any name you want. To help organize your installation, use a unique name if you plan to create more than one application server on the machine.
Server name	server1	Use a unique name for the application server.	The name is a logical name for the application server.
Host name	The long form of the domain name server (DNS) name.	Addressable through your network.	Use the DNS name or IP address of your machine to enable communication with your machine. See additional information about the host name following this table.

Node name considerations: If you plan to migrate an installation of Version 6 or Version 7 Network Deployment to Version 8 and migrate one of the managed nodes in the cell, use the same node name for the Version 8 application server that you used for the Version 6 or Version 7 managed node.

Directory path considerations:

- Windows The installation directory path must be less than or equal to 60 characters.
- In the Profile Management Tool, fields for entering directory paths might not grey out when disabled and might have differing context menus from normal when you right-click them.

Host name considerations:

The host name is the network name for the physical machine on which the node is installed. The host name must resolve to a physical network node on the server. When multiple network cards exist in the server, the host name or IP address must resolve to one of the network cards. Remote nodes use the host name to connect to and communicate with this node. Selecting a host name that other machines can reach within your network is important. Do not use the generic identifier, `localhost`, for this value. Also, do not attempt to install WebSphere Application Server products on a machine with a host name that uses characters from a double-byte character set (DBCS). DBCS characters are not supported when used in the host name.

If you define coexisting nodes on the same computer with unique IP addresses, then define each IP address in a domain name server (DNS) look-up table. Configuration files for standalone application servers do not provide domain name resolution for multiple IP addresses on a machine with a single network address.

The value that you specify for the host name is used as the value of the hostName property in configuration documents for the standalone application server. Specify the host name value in one of the following formats:

- Fully qualified domain name server (DNS) host name string, such as `xmachine.manhattan.ibm.com`
- The default short DNS host name string, such as `xmachine`
- Numeric IP address, such as `127.1.255.3`

The fully qualified DNS host name has the advantages of being unambiguous and flexible. You have the flexibility of changing the actual IP address for the host system without having to change the application server configuration. This value for the host name is particularly useful if you plan to change the IP address frequently when using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. A disadvantage of this format is dependency on DNS. If DNS is not available, then connectivity is compromised.

The short host name is also dynamically resolvable. A short name format has the added function of being redefined in the local hosts file so that the system can run the application server, even when disconnected from the network. To run disconnected, define the short name as the loopback address, `127.0.0.1`, in the hosts file to run disconnected. A disadvantage of this format is a dependency on DNS for remote access. If DNS is not available, then connectivity is compromised.

A numeric IP address has the advantage of not requiring name resolution through DNS. A remote node can connect to the node that you name with a numeric IP address without DNS being available. A disadvantage of this format is that the numeric IP address is fixed. You must change the setting of the hostName property in Express configuration documents whenever you change the machine IP address. Therefore, do not use a numeric IP address if you use DHCP, or if you change IP addresses regularly. Another disadvantage of this format is that you cannot use the node if the host is disconnected from the network.

After specifying application server characteristics, the tool displays the Administrative security panel.

9. Optionally enable administrative security, and click **Next**.

   You can enable administrative security now during profile creation, or later from the console. If you enable administrative security now, then enter a user name and password to log onto the administrative console.

   After specifying security characteristics, the tool displays the Security certificate panel if you previously selected **Advanced profile creation**.

10. If you selected **Typical profile creation** at the beginning of these steps, go to the step that displays the Profile summary panel.

11. Create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

    You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

    Note: When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the trust.p12 file.

    If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

12. Verify that the certificate information is correct, and click **Next**.

    If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is `WebAS`. You should change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the java.security file.

    When you create either or both certificates, or import either or both certificates, the keystore files that are created are key.p12, trust.p12, root-key.p12, default-signers.p12, deleted.p12, and ltpa.jceks. These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify. The key.p12 file contains the default personal certificate. The trust.p12 file contains the signer certificate from the default root certificate. The root-key.p12 file contains the root signing certificate. The default-signer.p12 file contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate is in the default-signer.p12 keystore file. The deleted.p12 keystore file is used to hold certificates deleted with the deleteKeyStore task so that they can be recovered if needed. The ltpa.jceks file contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

    An imported certificate is added to the key.p12 file or the root-key.p12 file.

    If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

    After displaying the Security certificate panels, the tool displays the Ports panel if you previously selected **Advanced profile creation**.

13. Verify that the ports specified for the standalone application server are unique, and click **Next**.

If you chose not to deploy the administrative console, then the administrative console ports are disabled on the Ports panel.

Port conflict resolution

Ports are recognized as being in use if one of the following conditions exists:

- The ports are assigned to a profile created from an installation that is performed by the current user.
- The port is currently in use.

Validation of ports occurs when you access the Port value assignment panel. Conflicts can still occur between the Port value assignment panel and the Profile creation complete panel because ports are not assigned until profile creation completes.

If you suspect a port conflict, then you can investigate the port conflict after the profile is created. Determine the ports that are used during profile creation by examining the following files.

- Linux HP-UX Solaris AIX *profile_root*`/properties/portdef.props` file
- Windows *profile_root*`\properties\portdef.props` file

Included in this file are the keys and values that are used in setting the ports. If you discover ports conflicts, then you can reassign ports manually. To reassign ports, run the updatePorts.ant file by using the ws_ant script.

Windows Linux The tool displays the Windows service definition panel if you are installing on a Windows operating system and the installation ID has the administrative group privilege. The tool displays the Linux service definition panel if you are installing on a supported Linux operating system and the ID that runs the Profile Management Tool is the root user.

14. Choose whether to run the application server as a Windows service on a Windows operating system or as a Linux service on a Linux operating system, then click **Next**.

    - Windows

      The Windows service definition panel is displayed for the Windows operating system only if the ID that installs the Windows service has the administrator group privilege. However, you can run the WASService.exe command to create the Windows service as long as the installer ID belongs to the administrator group. Read about automatically restarting server processes for more information.

      Windows The product attempts to start Windows services for application server processes that are started by a startServer command. For example, if you configure an application server as a Windows service, and issue the startServer command, then the **wasservice** command attempts to start the defined service.

      If you chose to install a local system service, then you do not have to specify your user ID or password. If you create a specified user type of service, then you must specify the user ID and the password for the user who runs the service. The user must have `Log on as a service` authority for the service to run correctly. If the user does not have `Log on as a service` authority, then the Profile Management tool automatically adds the authority.

      To perform this profile creation task, the user ID must not contain spaces. In addition to belonging to the administrator group, the ID must also have the advanced user right of `Log on as a service`. The Installation program grants the user ID the advanced user right if the user ID does not already have the advanced user right and if the user ID belongs to the administrator group.

      You can also create other Windows services after the installation is complete to start other server processes. Read about automatically restarting server processes for more information.

      You can remove the Windows service that is added during profile creation during profile deletion. You can also remove the Windows service with the wasservice command.

      IPv6 considerations

      Profiles created to run as a Windows service fail to start when using Internet Protocol Version 6 (IPv6) if the service is configured to run as local system. Create a user-specific environment variable to enable IPv6. Since this environment variable is a user variable instead of a local system variable, only a Windows service that runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as local system. When the Windows service for the product tries to run, the service is unable to access the user environment variable that specifies IPv6, and thus, tries to start as Internet Protocol Version 4 (IPv4). The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the Windows service for the product runs with the same user ID from which the environment variable that specifies IPv6 is defined, instead of as local system.

Default values for the Windows service

Windows The following default values for the Windows service definition panel exist:

- The default is to run as a Windows service.
- The service process is selected to run as a system account.
- The user account is the current user name. User name requirements are the requirements that the Windows operating system imposes for a user ID.
- The startup type is `automatic`. The values for the startup type are those values that the Windows operating system imposes. If you want a startup type other than `automatic`, you can either select another available option from the menu or change the startup type after you create the profile. You can also remove the created service after profile creation, and add it later with the desired startup type. You can choose not to create a service at profile creation time and optionally create the service later with the desired startup type.

- Linux

  The Linux service definition panel is displayed if the current operating system is a supported version of Linux operating systems, and the current user has the appropriate permissions.

  The product attempts to start Linux services for application server processes that are started by a startServer command. For example, if you configure an application server as a Linux service and issue the startServer command, then the **wasservice** command attempts to start the defined service.

  By default, the product is not selected to run as a Linux service.

  To create the service, the user that runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a non-root user ID, then the Linux service definition panel is not displayed, and no service is created.

  When you create a Linux service, you must specify a user name from which the service runs.

  To delete a Linux service, the user must be the root user or have appropriate privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service for the user.

If you previously selected **Advanced profile creation**, the next panel displays the web server definition panel.

15. For advanced profile creation, if you choose to include a web server definition in the profile now, specify the web server characteristics on the panels, and click **Next** until you complete the web server definition panels.

    If you use a web server to route requests to the product, then you need to include a web server definition. You can include the definition now, or define the web server to the product later. If you define the Web server definition during the creation of this profile, then you can install the web server and its plug-in after you create the profile. However, you must install both to the paths that you specify on the web server definition panels. If you define the web server to the product after you create this profile, then you must define the Web server in a separate profile.

    The tool displays the Profile Creation Summary panel.

16. Click **Create** to create the application server, or click **Back** to change the characteristics of the application server.

    The Profile creation progress panel, which shows the configuration commands that are running, is displayed.

    When the profile creation completes, the tool displays the Profile creation complete panel.

17. Optionally, select **Launch the First steps console**. Click **Finish** to exit.

    With the First steps console, you can create additional profiles and start the application server.

Results

You created an application server profile. The node within the profile has an application server named server1.

Refer to the description of the manageprofiles command to learn about creating a profile using a command instead of the Profile Management Tool.

What to do next

Deploy an application to get started.

Read about fast paths for the product to get started deploying applications.

When you create the application server profile, a default server1 process is created. You can federate the server1 node into the deployment manager cell with the addNode command or from the administrative console of the deployment manager. The server1 process must be running to begin the federation from the deployment manager.

If you include all of the applications from the application server, then the act of federation installs the applications on the deployment manager where they can be redeployed.

Managing profiles for non-root users

The non-root user can receive permissions for files and directories so that the non-root user can create a profile.

Before you begin

This task assumes a basic familiarity with the **manageprofiles** command, the Profile Management Tool, and system commands.

This task uses the following terms:

- `Root users` refers to:
  - Linux HP-UX Solaris AIX Root users
  - Windows Administrators
- `Non-root users` refers to:
  - Linux HP-UX Solaris AIX Non-root users
  - Windows Non-administrators
- `Installer` refers to a root user or a non-root user.

Remember: An ease-of-use limitation exists for non-root users who create profiles. Mechanisms within the Profile Management Tool that suggest unique names and port values are disabled for non-root users. The non-root user must change the default field values in the Profile Management Tool for the profile name, node name, cell name, and port assignments. Consider assigning non-root users a range of values for each of the fields. You can assign responsibility to the non-root users for adhering to their assigned value ranges and for maintaining the integrity of their own definitions.

About this task

Non-root users might typically need these tasks completed so that they can start their own application servers in development environments. For instance, an application developer might test an application on a application server in a profile assigned to that application developer.

Procedure

- Create a profile as an installer and assign ownership to a non-root user.

  This topic describes how the installer creates a profile and assigns ownership of the profile directory to a non-root user so that the non-root user can start the application server for a specific profile.
- Grant write permission of files and directories to a non-root user for profile creation.

  This topic describes how an installer authorizes a group to certain files and directories so that non-root users in the group can create profiles.
- Install maintenance as an installer and change the ownership of profile-related files.

  This topic describes how to install product maintenance and change the ownership of new profile files to the non-root user that owns the profile. The installer changes ownership of the files so that the non-root user can then successfully start the application server.

Results

Depending on the tasks that the installer followed, the installer has completed the following actions:

- Created a profile for a non-root user and assigned ownership of the profile directory to the non-root user
- Granted permission to the appropriate directories so that non-root users can create profiles
- After installing maintenance, changed ownership of new profile files in a directory that is owned by a non-root user, so that the non-root user can successfully start the application server

Note: Connections to the Derby database might not work, and you might see errors like the following in the logs:

```
java.io.FileNotFoundException: C:\Program Files\IBM\WebSphere\AppServer\derby\derby.log (Access is denied.)
```

This can happen when files under *app_server_root* are read-only. You can configure Derby to write its log to another location by setting the following property in the `app_server_root/derby/derby.properties` file

```
# This property can be set to make Derby log to System.err.  This is useful if you
# do not have write permission to the default location:
WAS_HOME/derby/derby.log derby.stream.error.field=java.lang.System.err
```

What to do next

Depending on the tasks that the installer completes, a non-root user can create a profile, start WebSphere Application Server, or do both.

Assigning profile ownership to a non-root user

An installer can create a profile and assign ownership of the profile directory to a non-root user so that the non-root user can start the product for a specific profile.

Before you begin

This task assumes a basic familiarity with the **manageprofiles** command and system commands.

This task uses the following terms:

- `Root users` refers to:
  - Linux HP-UX Solaris AIX Root users
  - Windows Administrators

- `Non-root users` refers to:
  - Linux HP-UX Solaris AIX Non-root users
  - Windows Non-administrators
- `Installer` refers to a root user or a non-root user.

Before you can create a profile, you must install the product.

About this task

Have the installer perform the following steps to create a profile and assign ownership for the profile directory and the logs directory. The ownership is assigned to a non-root user ID that is different from the installer ID. The non-root user needs access to these directories to start the product.

This example creates a default profile.

The commands are split on multiple lines for printing purposes.

Procedure

1. Create the profile by issuing the following code from a command prompt:

   Linux HP-UX Solaris AIX

```
./manageprofiles.sh -create -profileName profile01 -profilePath
app_server_root/profiles/profile01 -templatePath
app_server_root/profileTemplates/default
```

   Windows

```
manageprofiles.bat -create -profileName profile01 -profilePath
app_server_root\profiles\profile01 -templatePath
app_server_root\profileTemplates\default
```

2. Change ownership of the profile01 profile directory to the user1 non-root user.

   Linux HP-UX Solaris AIX For example, issue the following command:

```
chown -R user1 app_server_root/profiles/profile01
```

   Windows Follow instructions in the Windows documentation to grant user1 access to the following directory:

```
app_server_root\profiles\profile01
```

3. Change the ownership of the logs directory for the profile01 profile to the user1 non-root user to prevent displaying log messages to the console.

   Linux HP-UX Solaris AIX Issue the following command:

```
chown -R user1 app_server_root/logs/manageprofiles/profile01
```

   Windows Follow instructions in the Windows documentation to grant user1 access to the following directory:

```
app_server_root\logs\manageprofiles\profile01
```

Results

The installer has created a default profile and changed ownership of the profile directory and log directory to a non-root user.

What to do next

As the installer, you can continue to create profiles and assign ownership to non-root users as needed.

A non-root user ID can manage multiple profiles. Have the same non-root user ID manage an entire profile, whether it is the deployment manager profile, a profile that contains the application servers and the node agent, or a custom profile. A different user ID can be used for each profile in a cell, whether global security or administrative security is enabled or disabled. The user IDs can be a mix of root and non-root user IDs. For example, the root user might manage the deployment manager profile, while a non-root user might manage a profile that contains application servers and the node agent, or vice versa. However, typically, a root user or a non-root user manages all profiles in a cell.

The non-root user can use the same tasks to manage a profile that the root user uses.

Granting write permission for profile-related tasks

The installer can grant write permission of the appropriate files and directories to a non-root user. The non-root user can then create the profile. The installer can create a group for users who are authorized to create profiles, or the installer can give individual users the authority to create profiles. The following example task shows how to create a group that is authorized to create profiles.

Before you begin

This task assumes a basic familiarity with system commands.

This task uses the following terms:

- `Root users` refers to:
  - Linux HP-UX Solaris AIX Root users
  - Windows Administrators
- `Non-root users` refers to:
  - Linux HP-UX Solaris AIX Non-root users
  - Windows Non-administrators
- `Installer` refers to a root user or a non-root user.

About this task

The steps that you follow to grant write permission of files and directories to a non-root user for profile creation depend on whether a profile was previously created.

If at least one profile was created prior to implementing the following steps, then certain directories and files were created. Because these directories and files were created, skip the steps that create these directories and files. If no profile was previously created, then you must complete the steps to create the required directories and files. In most cases, a profile has been created previously.

The installer can perform the following steps to create the profilers group and give the group appropriate permissions to create a profile.

Procedure

1. Log on as the installer to the system where the product is installed.
2. Create the `profilers` group that you can use to create profiles.

   Read the documentation for your operating system for information about how to create groups.
3. Create a user named `user1` to create profiles.

   Read the documentation for your operating system for information on how to create users.
4. Add the installer and `user1` to the `profilers` group.
5. Linux HP-UX Solaris AIX Log off and log back on again as the installer to use the new group.
6. Create the following directories as the installer, if no profile was previously created:
   - Linux HP-UX Solaris AIX Create the *app_server_root*/logs/manageprofiles directory:

```
mkdir app_server_root/logs/manageprofiles
```

   Windows Create the *app_server_root*\logs\manageprofiles directory by following instructions in the Windows documentation. For this example procedure the directory is:

```
app_server_root\logs\manageprofiles
```

- Linux HP-UX Solaris AIX Create the *app_server_root*/properties/fsdb directory:

```
mkdir app_server_root/properties/fsdb
```

Windows Create the *app_server_root*\properties\fsdb directory by following instructions in the Windows documentation. For this example procedure the directory is:

```
app_server_root\properties\fsdb
```

7. As the installer, create the profileRegistry.xml file and add the appropriate information, if no profile was previously created.

   Follow directions for your operating system to create the profileRegistry.xml file. For this example, the file paths are: Linux HP-UX Solaris AIX

```
app_server_root/properties/profileRegistry.xml
```

   Windows

   ```
   app_server_root\properties\profileRegistry.xml
   ```

   Follow instructions for your operating system to add the following information to the profileRegistry.xml file. The file must be encoded as UTF-8.

```
<?xml version="1.0" encoding="UTF-8"?>
<profiles/>
```

8. As the installer, use operating system tools to change directory and file permissions.

   Linux HP-UX Solaris AIX The following example assumes that the installation root directory is /opt/IBM/WebSphere/AppServer:

```
chgrp  profilers /opt/IBM/WebSphere/AppServer/logs/manageprofiles
chmod  g+wr  /opt/IBM/WebSphere/AppServer/logs/manageprofiles
chgrp  profilers /opt/IBM/WebSphere/AppServer/properties
chmod  g+wr  /opt/IBM/WebSphere/AppServer/properties
chgrp  profilers /opt/IBM/WebSphere/AppServer/properties/fsdb
chmod  g+wr  /opt/IBM/WebSphere/AppServer/properties/fsdb
chgrp  profilers /opt/IBM/WebSphere/AppServer/properties/profileRegistry.xml
chmod  g+wr  /opt/IBM/WebSphere/AppServer/properties/profileRegistry.xml
chgrp -R profilers /opt/IBM/WebSphere/AppServer/profileTemplates
```

   HP-UX If you create a cell profile, additionally issue the following commands:

```
chmod  -R g+wr /opt/IBM/WebSphere/AppServer/profileTemplates/cell/default/documents
chmod  -R g+wr /opt/IBM/WebSphere/AppServer/profileTemplates/cell/dmgr/documents
```

   HP-UX If you create an application server profile, a deployment manager profile, or a custom profile, then additionally issue the following command:

```
chmod  -R g+wr /opt/IBM/WebSphere/AppServer/profileTemplates/profile_template_name/documents
```

   profile_template_name is `default`, `dmgr`, or `managed`, respectively.

   HP-UX The ownership of files is preserved when the files are copied to the profile directory during profile creation. You granted write permission to the profile directory so that files copied to the profile directory can be modified as part of the profile creation process. Files that are already in the profileTemplate directory structure prior to the start of profile creation are not modified during profile creation. Linux

   ```
   chgrp profilers /opt/IBM/WebSphere/AppServer/properties/Profiles.menu
   chmod  g+wr /opt/IBM/WebSphere/AppServer/properties/Profiles.menu
   ```

   Windows The following example assumes that the installation root directory is C:\Program Files\IBM\WebSphere\AppServer. Follow instructions in the Windows documentation to give the profilers group read and write permission to the following directories and their files:

```
C:\Program Files\IBM\WebSphere\AppServer\logs\manageprofiles
C:\Program Files\IBM\WebSphere\AppServer\properties
C:\Program Files\IBM\WebSphere\AppServer\properties\fsdb
C:\Program Files\IBM\WebSphere\AppServer\properties\profileRegistry.xml
```

   You might have to change the permissions on additional files if the non-root user encounters permission errors. For example, if you authorize a non-root user to delete a profile, then the user might have to delete the following file:

   Linux HP-UX Solaris AIX *app_server_root*/properties/profileRegistry.xml_LOCK

   Windows *app_server_root*\properties\profileRegistry.xml_LOCK

- Give write access to the non-root user for the file to authorize the user to delete the file. If the non-root user still cannot delete the profile, then the installer can delete the profile.

Results

The installer created the profilers group and gave the group proper permissions to certain directories and files to create profiles.

These directories and files are the only ones in the installation root of the product to which a non-root user needs to write to create profiles.

What to do next

The non-root user that belongs to the profilers group can create profiles in a directory that the non-root user owns and to which the non-root user has write permission. However, the non-root user cannot create profiles in the installation root directory of the product.

A non-root user ID can manage multiple profiles. The same non-root user ID can manage an entire profile, whether it is the deployment manager profile, a profile that contains the application servers and the node agent, or a custom profile. A different user ID can be used for each profile in a cell, whether global security or administrative security is enabled or disabled. The user IDs can be a mix of root and non-root user IDs. For example, the root user might manage the deployment manager profile, while a non-root user might manage a profile that contains application servers and the node agent, or vice versa. However, typically, a root user or a non-root user can manage all profiles in a cell.

The non-root user can use the same tasks to manage a profile that the root user uses.

Changing ownership for profile maintenance

When an installer installs a maintenance package that contains service for a profile that a non-root user owns, the installer owns any new files that the maintenance package creates. The installer can change the ownership of the new files so that a non-root user can successfully start the product.

Before you begin

This task assumes a basic familiarity with Installation Manager and system commands.

This task uses the following terms:

- `Root users` refers to:
  - Linux HP-UX Solaris AIX Root users
  - Windows Administrators
- `Non-root users` refers to:
  - Linux HP-UX Solaris AIX Non-root users
  - Windows Non-administrators
- `Installer` refers to a root user or a non-root user.

Before you can update a profile, you must install the product, and create a profile.

About this task

This example assumes that the installer completes the following actions:

- Applies service that creates new files in a profiles directory that the wsdemo non-root user owns
- Changes ownership of new profile files from the installer to the wsdemo non-root user.

If the installer does not change ownership, then when the non-root user starts the product, the application server encounters an error and issues a message that is similar to the following example:

```
ADMR0104E:
The system is unable to read document
cells/express1Cell/nodes/express1/node-metadata.properties:
java.io.IOException: No such file or directory
```

Procedure

1. Install maintenance packages for the product.
2. Reassign ownership of the entire profile directory to the wsdemo non-root user.

   The *profile_root* variable in the following examples is the profile directory that the non-root user owns.

   Linux HP-UX Solaris AIX Issue the **chown** command.

```
chown -R wsdemo profile_root
```

   Windows Follow instructions in the Windows documentation to reassign ownership of the *profile_root* directory to the wsdemo non-root user.

Results

The installer installed a maintenance package that creates new files in a non-root user profile directory and changes ownership of the new files to the non-root owner.

What to do next

The non-root user can start the product without receiving the ADMR0104E error message.

Deleting profiles

You can delete a profile using the manageprofiles command. If the command fails, you can delete the profile using operating system commands.

Before you begin

If a node within a profile is federated to a deployment manager, before you delete the profile, stop the node and remove the node from the deployment manager. Otherwise, an orphan node is left in the deployment manager.

You cannot delete a profile using the Profile Management Tool.

About this task

The following example attempts to delete a profile using the manageprofiles command, and then using operating system commands.

Procedure

1. Issue the manageprofiles command to delete a profile.

   Substitute your profile name for the *profile_name* value in the following commands.

   Linux HP-UX Solaris AIX

```
./manageprofiles.sh -delete
                 -profileName profile_name
```

   Windows

```
manageprofiles.bat -delete
                -profileName profile_name
```

   If the command is successful, you have completed the task and can skip the remaining steps. If the command is partially successful or unsuccessful, proceed to the next step to delete the profile manually. If you receive the `INSTCONFFAILED: Cannot delete profile.` message, the command was unsuccessful. If the deletion is partially successful, you could receive message information similar to the following wording:

```
INSTCONFPARTIALSUCCESS: The profiles no longer exist, but errors occurred.
For more information, consult
app_server_root/logs/manageprofiles/deleteAll.log.
```

or

```
The current user does not have sufficient permissions to detect or
remove services. If a service does exist, then an administrative or root user has
to remove it. If a service does not exist, then no further action is
required.
```

2. Issue operating system commands to delete the profile directory.
3. Issue the following command to remove references in the registry to deleted profiles:

   Linux HP-UX Solaris AIX

   ```
   ./manageprofiles.sh -validateAndUpdateRegistry
   ```

   Windows

```
manageprofiles.bat -validateAndUpdateRegistry
```

   Editing of the registry is not recommended.

Results

You have now deleted a profile.

What to do next

You can delete other profiles using this procedure, or create other profiles using the manageprofiles command or the Profile Management Tool.

firststeps command

The firststeps command starts the First steps console. The First steps console is a post-installation ease-of-use tool for directing WebSphere Application Server Network Deployment elements from one place. Options display dynamically on the First steps console, depending on features that you install and the availability of certain elements on a particular operating system platform. Options include verifying the installation, starting and stopping deployment manager and application server processes, accessing the tools for creating and managing profiles, accessing the administrative console, and accessing the online information center.

First steps overview

A prompt to launch the First steps console displays on the last panel of the Profile Management Tool.

This version lets you start the Profile Management Tool to get started defining a cell, a management profile, and application servers for the cell. A cell consists of a deployment manager profile and a federated application server profile. You can also define standalone application servers. Each profile has its own First steps console.

You can also start the First steps console from the command line as described later in this article.

First step consoles exist for the cell profile, the management profiles, the standalone application server profile, and the custom profile. The secure proxy profile only has a first steps console when installed and configured on a DMZ Secure Proxy Server node.

Table 35. Available options for Network Deployment.

Options that display on each First steps console are shown in the following table:

Option	Product	Profiles					
		Cell *		Management (Deployment Manager, Administrative Agent, and Job Manager)	Standalone Application Server	Custom	Secure Proxy
		Cell Deployment Manager	Cell Node				
Installation verification	No	Yes	No	Yes	Yes	No	Yes
Start and stop the deployment manager	No	Yes	No	Yes (deployment manager)	No	No	No
Start and stop the server	No	No	No	No	Yes	No	Yes
Administrative console	No	Yes (if available)	No	Yes (if available)	Yes (if available)	No	Yes
WebSphere Customization Toolbox (containing the Profile Management Tool and the Configuration Migration Tool)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Information center	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IBM Education Assistant	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Exit	Yes	Yes	Yes	Yes	Yes	Yes	Yes

* When launching the First steps console from the Profile Management Tool in a cell-creation flow, the dmgr instance is used.

Option descriptions

Installation verification

This option starts the installation verification test. The test consists of starting and monitoring the deployment manager or the standalone application server during its start up.

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

The **Start the deployment manager** option or the **Start the application server** option is unavailable while the IVT runs.

The IVT provides the following useful information about the deployment manager or the application server:

- Name of the server process
- Name of the profile
- Profile path, which is the file path and the name of the profile
- Type of profile
- Cell name
- Node name
- Current encoding
- Port number for the administrative console, which is 9060 by default
- Various informational messages that include the location of the `SystemOut.log` file and how many errors are listed within the file
- Completion message

Start the server

This option toggles to **Stop the server** when the application server runs.

This option displays when the First steps console is in a standalone application server profile or a cell profile.

After selecting the **Start the server** option, an output screen displays with status messages. The success message informs you that the server is open for e-business. Then the menu item toggles to **Stop the server** and the **Administrative console** option enables

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

Start the deployment manager

This option toggles to **Stop the deployment manager** when the deployment manager runs.

This option displays when the First steps console is in a deployment manager profile or a cell profile.

After selecting the **Start the deployment manager** option, an output screen displays 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**.

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

Start the administrative agent

This option toggles to **Stop the administrative agent** when the administrative agent runs.

This option displays when the First steps console is in an administrative agent profile.

After selecting the **Start the administrative agent** option, an output screen displays with status messages. The success message informs you that the administrative agent is open for e-business. Then the menu item changes to **Stop the administrative agent**.

If you select the **Start the administrative agent** option, the **Installation verification** option is unavailable while the administrative agent runs.

Start the job manager

This option toggles to **Stop the job manager** when the job manager runs.

This option displays when the First steps console is in a job manager profile or a cell profile.

After selecting the **Start the job manager** option, an output screen displays with status messages. The success message informs you that the job manager is open for e-business. Then the menu item changes to **Stop the job manager**.

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

Administrative console

This option is unavailable until the application server or deployment manager runs.

The administrative console is a configuration editor that runs in one of the supported web browsers. The administrative console lets you work with XML configuration files for the standalone application server or the deployment manager and all of the application servers that are in the cell.

To launch the administrative console, click **Administrative console** or point your browser to `http://localhost:9060/ibm/console`. Substitute the host name for `localhost` if the address does not load. Verify the installation to verify the administrative console port number, if 9060 does not load.

Note: Vista Windows 7 If you are installing the product on these operating systems, then 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 signon is also available when administrative security is enabled.

The installation procedure in the information center cautions 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.

WebSphere Customization Toolbox

This option opens the WebSphere Customization Toolbox, which contains the Profile Management Tool and the Configuration Migration Tool.

Profile Management Tool

The Profile Management Tool can create a standalone application server profile, a cell profile, a secure proxy profile, a custom profile, or a management profile.

Each profile has its own administrative interface. A custom profile is an exception. A custom profile is an empty node that you can federate into a deployment manager cell and customize. No default server processes or applications are created for a custom profile.

Each profile also has its own First steps console except for the secure proxy profile.

Configuration Migration Tool

The Configuration Migration Tool is the graphical interface to the migration tools.

See the migration documentation for more information about the Configuration Migration Tool.

Information center for WebSphere Application Server

This option links you to the online information center.

IBM Education Assistant

This option links you to the IBM Education Assistant.

Exit This option closes the First steps console.

Location of the command file

The location of the firststeps command that starts the First steps console for a profile is:

- AIX HP-UX Linux Solaris *profile_root*`/firststeps/firststeps.sh`
- Windows *profile_root*`\firststeps\firststeps.bat`

Parameters

No parameters are associated with this command.

Syntax for the firststeps command

Use the following syntax for the command:

- AIX HP-UX Linux Solaris `./firststeps.sh`
- Windows `firststeps.bat`

Link tips

The following links exist on the First steps console for the WebSphere Application Server Network Deployment product:

Network Deployment provides different types of profiles. Not all profiles have all of the links shown in the table. See the previous description of available options for each profile.

Table 36. Links on the First steps console.

Links that display on the First steps console are shown in the following table:

Option	Link
Installation verification	Calls the ivt command. The location of the installation verification test command is: - AIX HP-UX Linux Solaris *profile_root*/bin/ivt.sh - Windows *profile_root*\bin\ivt.bat
Start the server	Calls the startServer command. The location of the startServer command is: - AIX HP-UX Linux Solaris *profile_root*/bin/startServer.sh *server_name* - Windows *profile_root*\bin\startServer.bat *server_name* When you have more than one application server on the same machine, the command starts the same application server that is associated with the First steps console.
Stop the server	Calls the stopServer command. The location of the stopServer command is: - AIX HP-UX Linux Solaris *profile_root*/bin/stopServer.sh *server_name* - Windows *profile_root*\bin\stopServer.bat *server_name*
Start the deployment manager	Calls the startManager command. The location of the startManager command is: - AIX HP-UX Linux Solaris *profile_root*/bin/startManager.sh - Windows *profile_root*\bin\startManager.bat When you have more than one deployment manager on the same machine, the command starts the same deployment manager that is associated with the First steps console.
Stop the deployment manager	Calls the stopManager command. The location of the stopManager command is: - AIX HP-UX Linux Solaris *profile_root*/bin/stopManager.sh - Windows *profile_root*\bin\stopManager.bat
Administrative console	Opens the default browser to the http://localhost:9060/ibm/console web address. When you have more than one application server on the same machine, the port varies. The First steps console starts the administrative console that is associated with the First steps console. **Note:** Vista If you are installing the product on the Windows Vista operating system, then 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 on Windows Vista.
WebSphere Customization Toolbox	The command file is located at: - AIX HP-UX Linux Solaris *profile_root*/bin/wct.sh - Windows *profile_root*\bin\wct.bat
Information center for WebSphere Application Server products	Opens the default browser to the online information center.
IBM Education Assistant	Opens the default browser to the IBM Education Assistant.

Note: This topic references one or more of the application server log files. Beginning in WebSphere Application Server Version 8.0 you can configure the server to use the High Performance Extensible Logging (HPEL) log and trace infrastructure instead of using `SystemOut.log` , `SystemErr.log`, `trace.log`, and `activity.log` files or native z/OS logging facilities. If you are using HPEL, you can access all of your log and trace information using the LogViewer command-line tool from your server profile bin directory. See the information about using HPEL to troubleshoot applications for more information on using HPEL.

Using the installation verification tool

Use the installation verification tool (IVT) to verify that the installation of the product and the application server or deployment manager profile is successful. A *profile* consists of files that define the runtime environment for a deployment manager or an application server. Verify each profile from its First steps console with the IVT.

Before you begin

After installing the Network Deployment product and creating a deployment manager or application server profile, you are ready to use the IVT.

About this task

Use the IVT to gain assurance that the product is successfully installed. The IVT tests deployment manager profiles and standalone application 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.

The Profile Management Tool creates profiles. After creating a profile, the Profile Management Tool displays a prompt for starting the First steps console. The First steps console is unique for each profile. See “firststeps command” on page 221 for more information.

Installation verification is the first option on the First steps console.

The IVT program for an application server profile starts and monitors the application server process, which is the server1 process. The installation verification for a deployment manager profile starts and monitors the deployment manager process, which is the dmgr process. The IVT works differently for the deployment manager profile than for a standalone application server. On a standalone application server, the IVT queries servlets from the ivtApp application. However, the deployment manager does not have the ivtApp application, so the IVT looks at log files only.

Procedure

Use the installation verification test to verify the proper creation of profiles.

1. Start the First steps console and select **Installation verification** after creating a deployment manager profile or an application server profile.

   No installation verification is possible for a custom profile. After federating the node and using the deployment manager to create a server, you can start the server process to verify its functionality.

   Select the check box to launch the First steps console at the end of profile creation. You can also start the First steps console from the command line as described in “firststeps command” on page 221.

   You can also start the “ivt command” on page 228 directly from the `bin` directory of the profile:

   - AIX HP-UX Linux Solaris *`profile_root`*`/bin/ivt.sh server1 profile01`
   - Windows *`profile_root`*`\bin\ivt.bat server01 profile01`

   If you create profiles in another location, the `ivt` script location is within the *profile_root*`/bin` directory.
2. Observe the results in the First steps status window.

   The log file for installation verification is the *profile_root*`/logs/ivtClient.log`.

The IVT provides the following useful information about the application server:

- Application server name
- Name of the profile
- Profile file path
- Type of profile
- Node name
- Current encoding
- 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
- Completion message

As the IVT starts the application server on a Windows platform, the IVT attempts to start the Windows service for the application server, if a Windows service exists. This is true even though the Windows service might have a manual startup type.

If you federate a standalone application server, you can still run the IVT on the server.

The IVT provides the following useful information about the deployment manager:

- Deployment manager server name: dmgr
- Name of the profile
- Profile file path
- Type of profile: dmgr
- Cell name
- Node name
- Current encoding
- 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
- Completion message

As the IVT starts the deployment manager on a Windows platform, the IVT attempts to start the Windows service for the deployment manager if a Windows service exists. This is true even though the Windows service might have a manual startup type.

3. If the log shows that errors occurred during the installation verification, correct the errors and run the IVT again. If necessary, create a new profile after correcting the error, and run the IVT on the new profile.

Results

The IVT tool starts the server process of a profile automatically if the server is not running. Once the server initializes, the IVT runs a series of verification tests. The tool displays pass or fail status in a console window. The tool also logs results to the *profile_root*/`logs/ivtClient.log` file. As the IVT verifies your system, the tool reports any detectable errors in the `SystemOut.log` file.

Note: This topic references one or more of the application server log files. Beginning in WebSphere Application Server Version 8.0 you can configure the server to use the High Performance Extensible Logging (HPEL) log and trace infrastructure instead of using `SystemOut.log` , `SystemErr.log`, `trace.log`, and `activity.log` files or native z/OS logging facilities. If you are using HPEL, you can access all of your log and trace information using the LogViewer command-line tool from your server profile bin directory. See the information about using HPEL to troubleshoot applications for more information on using HPEL.

What to do next

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

You can also install other packages on the product installation image, such as IBM HTTP server, the Web Server Plug-ins, or the Application Client.

ivt command

The ivt command starts the installation verification test (IVT) program. The IVT verifies that the installation of the application server or deployment manager profile was successful. A *profile* consists of files that define the runtime environment for a deployment manager or an application server. Each profile has its own ivt command.

Note: This topic references one or more of the application server log files. Beginning in WebSphere Application Server Version 8.0 you can configure the server to use the High Performance Extensible Logging (HPEL) log and trace infrastructure instead of using `SystemOut.log` , `SystemErr.log`, `trace.log`, and `activity.log` files or native z/OS logging facilities. If you are using HPEL, you can access all of your log and trace information using the LogViewer command-line tool from your server profile bin directory. See the information about using HPEL to troubleshoot applications for more information on using HPEL.

The IVT program starts the application server or deployment manager automatically if the server process is not already running. After the server process initializes, the IVT runs a series of verification tests and displays pass or fail status in a console window.

The IVT program scans the `SystemOut.log` file for errors and verifies core functionality of the profile.

You can start the IVT program from the command line or from the First steps console.

Location of the command file

The location of the installation verification test script for a profile is the *profile_root*/`bin` directory. The script file name is:

- AIX HP-UX Linux Solaris `ivt.sh`
- Windows `ivt.bat`

Parameters

The following parameters are associated with this command.

`server_name`
Required parameter that identifies the name of the server process, such as server1 or dmgr

`profile_name`
Required parameter that identifies the name of the profile that contains the server definition

`-p` *`server_port_number`*
Optional parameter that identifies the default_host port when the port is not 9080, which is the default

`-host` *`machine_host_name`*
Optional parameter that identifies the host machine of the profile to test

The default is localhost.

Syntax for the ivt command

Use the following syntax for the command:

- AIX HP-UX Linux Solaris *profile_root*/`bin/ivt.sh`
- Windows *profile_root*\`bin\ivt.bat`

Logging

The ivt command logs results to the *profile_root*/`logs/ivtClient.log` file.

Note: This topic references one or more of the application server log files. Beginning in WebSphere Application Server Version 8.0 you can configure the server to use the High Performance Extensible Logging (HPEL) log and trace infrastructure instead of using `SystemOut.log` , `SystemErr.log`, `trace.log`, and `activity.log` files or native z/OS logging facilities. If you are using HPEL, you can access all of your log and trace information using the LogViewer command-line tool from your server profile bin directory. See the information about using HPEL to troubleshoot applications for more information on using HPEL.

Example

The following examples test the server1 process in the profile01 profile on the myhost machine using the default_host on port 9081.

AIX HP-UX Linux Solaris

```
ivt.sh server1 profile01 -p 9081 -host myhost
```

Windows

```
ivt.bat server1 profile01 -p 9081 -host myhost
```

Chapter 8. Installing and uninstalling the DMZ Secure Proxy Server on distributed operating systems

IBM Installation Manager is a common installer for many IBM software products that you use to install, update, roll back, and uninstall the DMZ Secure Proxy Server for IBM WebSphere Application Server.

Before you begin

Note: The DMZ Secure Proxy Server for IBM WebSphere Application Server is now installed by Installation Manager rather than by the programs based on InstallShield MultiPlatform (ISMP) that are used to install and uninstall previous versions.

Restrictions:

- Solaris The Installation Manager GUI is not supported on Solaris 10 x64 systems. Perform the following actions to install or uninstall the product on these systems:
  - Use the Installation Manager GUI on a supported system to record a response file that will allow you to install or uninstall the product silently.
  - Edit the recorded response file if necessary.
  - Use the response file to install or uninstall the product silently on your system.
- Linux For any Linux system that is enabled for Security Enhanced Linux (SELinux), such as Red Hat Enterprise Linux Version 5 or SUSE Linux Enterprise Server Version 11, you must identify the Java shared libraries in the Installation Manager installation image to the system. Also, you must identify the Java shared libraries in the Installation Manager installation after it has been installed. For example:

```
chcon -R -t texrel_shlib_t ${IM_Image}/jre_diectory/jre/bin
chcon -R -t texrel_shlib_t ${IM_Install_root}/eclipse/jre_diectory/jre/bin
```

- Installation Manager console mode, which is included in Installation Manager Version 1.4.3 and later, does not work with WebSphere Application Server Version 8.0 offerings.

About this task

Perform one of these procedures to install, update, roll back, or uninstall the DMZ Secure Proxy Server

Procedure

- "Installing the DMZ Secure Proxy Server using the GUI" on page 233
- "Installing the DMZ Secure Proxy Server silently" on page 237
- "Installing and removing features in the DMZ Secure Proxy Server" on page 247
- "Updating the DMZ Secure Proxy Server" on page 251
- "Rolling back the DMZ Secure Proxy Server" on page 252
- "Uninstalling the DMZ Secure Proxy Server using the GUI" on page 253
- "Uninstalling the DMZ Secure Proxy Server silently" on page 253

Results

Notes on logging and tracing:

- An easy way to view the logs is to open Installation Manager and go to **File > View Log**. An individual log file can be opened by selecting it in the table and then clicking the **Open log file** icon.
- Logs are located in the `logs` directory of Installation Manager's application data location. For example:
  - Windows **Administrative installation:**

```
C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
```

- Windows **Non-administrative installation:**

```
C:\Documents and Settings\user_name\Application Data\IBM\Installation Manager\logs
```

- AIX HP-UX Linux Solaris **Administrative installation:**

```
/var/ibm/InstallationManager/logs
```

- AIX HP-UX Linux Solaris **Non-administrative installation:**

```
user_home/var/ibm/InstallationManager/logs
```

- The main log files are time-stamped XML files in the `logs` directory, and they can be viewed using any standard web browser.
- The `log.properties` file in the `logs` directory specifies the level of logging or tracing that Installation Manager uses. To turn on tracing for the WebSphere Application Server plug-ins, for example, create a `log.properties` file with the following content:

```
com.ibm.ws=DEBUG
com.ibm.cic.agent.core.Engine=DEBUG
global=DEBUG
```

Restart Installation Manager as necessary, and Installation Manager outputs traces for the WebSphere Application Server plug-ins.

Notes on troubleshooting:

- HP-UX By default, some HP-UX systems are configured to not use DNS to resolve host names. This could result in Installation Manager not being able to connect to an external repository.

  You can ping the repository, but nslookup does not return anything.

  Work with your system administrator to configure your machine to use DNS, or use the IP address of the repository.
- In some cases, you might need to bypass existing checking mechanisms in Installation Manager.
  - On some network file systems, disk space might not be reported correctly at times; and you might need to bypass disk-space checking and proceed with your installation.

    To disable disk-space checking, specify the following system property in the `config.ini` file in *IM_install_root*`/eclipse/configuration` and restart Installation Manager:

```
cic.override.disk.space=sizeunit
```

where *size* is a positive integer and *unit* is blank for bytes, k for kilo, m for megabytes, or g for gigabytes. For example:

```
cic.override.disk.space=120 (120 bytes)
cic.override.disk.space=130k (130 kilobytes)
cic.override.disk.space=140m (140 megabytes)
cic.override.disk.space=150g (150 gigabytes)
cic.override.disk.space=true
```

Installation Manager will report a disk-space size of Long.MAX_VALUE. Instead of displaying a very large amount of available disk space, N/A is displayed.

  - To bypass operating-system prerequisite checking, add `disableOSPrereqChecking=true` to the `config.ini` file in *IM_install_root*`/eclipse/configuration` and restart Installation Manager.

If you need to use any of these bypass methods, contact IBM Support for assistance in developing a solution that does not involve bypassing the Installation Manager checking mechanisms.

- Installation Manager might display a warning message during the uninstallation process.

  Uninstalling a DMZ Secure Proxy Server using Installation Manager requires that the data repositories remain valid and available.
- For more information on using Installation Manager, read the IBM Installation Manager Information Center.

  Read the release notes to learn more about the latest version of Installation Manager. To access the release notes, complete the following task:
  - Windows Click **Start > Programs > IBM Installation Manager > Release Notes**.
  - AIX HP-UX Linux Solaris Go to the documentation subdirectory in the directory where Installation Manager is installed, and open the `readme.html` file.

Installing the DMZ Secure Proxy Server using the GUI

You can use the Installation Manager GUI to install the DMZ Secure Proxy Server for IBM WebSphere Application Server. Installing the DMZ Secure Proxy Server allows a secure proxy server profile to be created outside of the cell.

Before you begin

Install Installation Manager:

1. Perform one of the following procedures:
   - If you want to use the Installation Manager that is included with this product, perform the following actions:
     a. Obtain the necessary files from the physical media or the web.

        There are three basic options for obtaining and installing Installation Manager and the product.
        - **Access the physical media, and use local installation**

          You can access Installation Manager and the product repositories on the product media. You can install Installation Manager on your system and use it to install the product from the product repositories on the media.
        - **Download the files from the Passport Advantage site, and use local installation**

          Licensed customers can download Installation Manager as well as the necessary product repositories from the Passport Advantage site. You can then install Installation Manager on your system and use it to install the product from the repositories.
        - **Download a file from the Installation Manager website, and use web-based installation**

          You can download and unpack a compressed file containing Installation Manager from the IBM Installation Manager website. You can then install Installation Manager on your local system and use it to install the product from the web-based repository located at

`http://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v80`

     b. Change to the location containing the Installation Manager installation files, and run one of the following commands:

        Administrative installation:

        - Windows `install.exe`
        - AIX HP-UX Linux Solaris `./install`

Non-administrative installation:

- Windows `userinst.exe`
- AIX HP-UX Linux Solaris `./userinst`

Group-mode installation:

AIX HP-UX Linux Solaris `./groupinst`

Notes on group mode:

- Group mode allows multiple users to use a single instance of IBM Installation Manager to manage software packages.
- Windows Group mode is not available on Windows operating systems.
- If you do not install Installation Manager using group mode, you will not be able to use group mode to manage any of the products that you install later using this Installation Manager.
- Make sure that you change the installation location from the default location in the current user's home directory to a location that is accessible by all users in the group.
- Set up your groups, permissions, and environment variables as described in the Group mode road maps in the IBM Installation Manager Information Center before installing in group mode.
- For more information on using group mode, read the Group mode road maps in the IBM Installation Manager Information Center.

The installer opens an **Install Packages** window.

c. Make sure that the Installation Manager package is selected, and click **Next**.

d. Accept the terms in the license agreements, and click **Next**.

The program creates the directory for your installation.

e. Click **Next**.

f. Review the summary information, and click **Install**.

- If the installation is successful, the program displays a message indicating that installation is successful.
- If the installation is not successful, click **View Log File** to troubleshoot the problem.

- If you already have a version of Installation Manager installed on your system and you want to use it to install and maintain the product, obtain the necessary product files from the physical media or the web.

  There are three basic options for installing the product.

  - **Access the physical media, and use local installation**

    You can access the product repositories on the product media. Use your existing Installation Manager to install the product from the product repositories on the media.

  - **Download the files from the Passport Advantage site, and use local installation**

    Licensed customers can download the necessary product repositories from the Passport Advantage site. You can then use your existing Installation Manager to install the product from the repositories.

  - **Access the live repositories, and use web-based installation**

    You can install Installation Manager on your local system and use it to install the product from the web-based repository located at

`http://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v80`

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

2. Add the product repository to your Installation Manager preferences.
   a. Start Installation Manager.
   b. In the top menu, click **File** > **Preferences**.
   c. Select **Repositories**.
   d. Perform the following actions:
      1) Click **Add Repository**.
      2) Enter the path to the `repository.config` file in the location containing the repository files.

         For example:
         - Windows `C:\repositories\`*`product_name`*`\local-repositories`
         - AIX HP-UX Linux Solaris `/var/repositories/`*`product_name`*`/local-repositories`

         or

`http://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v80`

      3) Click **OK**.
   e. Deselect any locations listed in the Repositories window that you will not be using.
   f. Click **Apply**.
   g. Click **OK**.
   h. Click **File** > **Exit** to close Installation Manager.

About this task

Perform this procedure to use the Installation Manager GUI to install the DMZ Secure Proxy Server.

Procedure

1. Start Installation Manager.

   Tip: AIX HP-UX Linux Solaris You can start Installation Manager in group mode with the ./IBMIM command.
   - Group mode allows multiple users to use a single instance of IBM Installation Manager to manage software packages.
   - For more information on using group mode, read the Group mode road maps in the IBM Installation Manager Information Center.

2. Click **Install**.

   Note: If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.

   Installation Manager searches its defined repositories for available packages.

3. Perform the following actions:
   a. Select **DMZ Secure Proxy Server for IBM WebSphere Application Server** and the appropriate version.

      Note: If you are installing the trial version of this product, select **DMZ Secure Proxy Server for IBM WebSphere Application Server Trial**.

      If you already have the DMZ Secure Proxy Server installed on your system, a message displays indicating that the DMZ Secure Proxy Server is already installed. To create another installation of the DMZ Secure Proxy Server in another location, click **Continue**.
   b. Click **Next**.

Note: If you try to install a newer level of the DMZ Secure Proxy Server with a previous version of Installation Manager, Installation Manager might prompt you to update to the latest level of Installation Manager when it connects to the repository. Update to the newer version before you continue if you are prompted to do so. Read Installing updates in the Installation Manager information center for information about automatic updates.

4. Accept the terms in the license agreements, and click **Next**.
5. Specify the installation root directory for the product binaries, which are also referred to as the core product files or system files.

   The panel also displays the shared resources directory and disk-space information.

   Restrictions:

   - Deleting the default target location and leaving an installation-directory field empty prevents you from continuing.
   - Do not use symbolic links as the destination directory.

     Symbolic links are not supported.
   - Do not use a semicolon in the directory name.

     The DMZ Secure Proxy Server cannot install properly if the target directory includes a semicolon.

     Windows A semicolon is the character used to construct the class path on Windows systems.
   - Windows The maximum path length on the Windows Server 2008, Windows Vista, and Windows 7 operating systems is 60 characters.
6. Click **Next**.
7. Select the languages for which translated content should be installed.

   English is always selected.
8. Click **Next**.
9. Select the features that you want to install.

   Choose from the following features:

   - Administration Thin Client

     The Administration Thin Client is a runtime client that enables applications to run administration tasks to the application server.

     Tip: You can run the Installation Manager later to modify this installation and add or remove this feature.
   - AIX Linux Solaris Windows IBM Runtime Environment for Java

     This option allows you to choose between a 32-bit and 64-bit IBM Runtime Environment for Java.

     Notes:

     – This option displays only if you are installing on a 64-bit system.

     – This does not apply to Solaris x86 64-bit systems.

     – You must select one of the two options.

     – You cannot modify this installation later and change this selection.
10. Click **Next**.
11. Review the summary information, and click **Install**.
    - If the installation is successful, the program displays a message indicating that installation is successful.

      Note: The program might also display important post-installation instructions as well.
    - If the installation is not successful, click **View Log File** to troubleshoot the problem.

12. Choose whether or not you want to launch a program when this installation is finished.
    - Select **Profile Management Tool to create a profile** if you want to open the Profile Management Tool and create a new profile when this installation is finished.
    - Select **None** if you do not want to launch a program when this installation is finished.
13. Click **Finish**.
14. Click **File > Exit** to close Installation Manager.

What to do next

You can create a secure proxy profile using the Profile Management Tool or the manageprofiles command.

Installing the DMZ Secure Proxy Server silently

You can use Installation Manager to install the DMZ Secure Proxy Server for IBM WebSphere Application Server silently. Installing the DMZ Secure Proxy Server allows a secure proxy server profile to be created outside of the cell.

Before you begin

Install Installation Manager on each of the systems onto which you want to install the product.

1. Perform one of the following procedures:
   - If you want to use the Installation Manager that is included with this product, perform the following actions:
     a. Obtain the necessary files from the physical media or the web.

        There are three basic options for obtaining and installing Installation Manager and the product.
        - **Access the physical media, and use local installation**

          You can access Installation Manager and the product repositories on the product media. You can install Installation Manager on your system and use it to install the product from the product repositories on the media.
        - **Download the files from the Passport Advantage site, and use local installation**

          Licensed customers can download Installation Manager as well as the necessary product repositories from the Passport Advantage site. You can then install Installation Manager on your system and use it to install the product from the repositories.
        - **Download a file from the Installation Manager website, and use web-based installation**

          You can download and unpack a compressed file containing Installation Manager from the IBM Installation Manager website. You can then install Installation Manager on your local system and use it to install the product from the web-based repository located at

`http://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v80`

     b. Change to the location containing the Installation Manager installation files, and run one of the following commands to install Installation Manager silently:

        Administrative installation:
        - Windows installc.exe -log *log_file_path_and_name*
        - AIX HP-UX Linux Solaris ./installc -log *log_file_path_and_name*

        Non-administrative installation:
        - Windows userinstc.exe -log *log_file_path_and_name*
        - AIX HP-UX Linux Solaris ./userinstc -log *log_file_path_and_name*

Group-mode installation:

AIX HP-UX Linux Solaris `./groupinstc -dataLocation` *`application_data_location`* `-log` *`log_file_path_and_name`*

Notes on group mode:

- Group mode allows multiple users to use a single instance of IBM Installation Manager to manage software packages.
- Windows Group mode is not available on Windows operating systems.
- If you do not install Installation Manager using group mode, you will not be able to use group mode to manage any of the products that you install later using this Installation Manager.
- Make sure that you change the installation location from the default location in the current user's home directory to a location that is accessible by all users in the group.
- Set up your groups, permissions, and environment variables as described in the Group mode road maps in the IBM Installation Manager Information Center before installing in group mode.
- For more information on using group mode, read the Group mode road maps in the IBM Installation Manager Information Center.

- If you already have a version of Installation Manager installed on your system and you want to use it to install and maintain the product, obtain the necessary product files from the physical media or the web.

  There are three basic options for installing the product.

  - **Access the physical media, and use local installation**

    You can access the product repositories on the product media. Use your existing Installation Manager to install the product from the product repositories on the media.

  - **Download the files from the Passport Advantage site, and use local installation**

    Licensed customers can download the necessary product repositories from the Passport Advantage site. You can then use your existing Installation Manager to install the product from the repositories.

  - **Access the live repositories, and use web-based installation**

    You can install Installation Manager on your local system and use it to install the product from the web-based repository located at

`http://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v80`

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

2. Add the product repository to your Installation Manager preferences.
   a. Start Installation Manager.
   b. In the top menu, click **File > Preferences**.
   c. Select **Repositories**.
   d. Perform the following actions:
      1) Click **Add Repository**.
      2) Enter the path to the `repository.config` file in the location containing the repository files.

         For example:

         - Windows `C:\repositories\`*`product_name`*`\local-repositories`

- AIX HP-UX Linux Solaris /var/repositories/*product_name*/local-repositories

or

```
http://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v80
```

3) Click **OK**.

e. Deselect any locations listed in the Repositories window that you will not be using.

f. Click **Apply**.

g. Click **OK**.

h. Click **File > Exit** to close Installation Manager.

About this task

Using Installation Manager, you can work with response files to install the DMZ Secure Proxy Server silently in a variety of ways. You can record a response file using the GUI as described in the following procedure, or you can generate a new response file by hand or by taking an example and modifying it.

Procedure

1. Optional: **Record a response file to install the DMZ Secure Proxy Server:** On one of your systems, perform the following actions to record a response file that will install the DMZ Secure Proxy Server.

   a. From a command line, change to the eclipse subdirectory in the directory where you installed Installation Manager.

   b. Start Installation Manager from the command line using the -record option.

   For example:

   - Windows **Administrator or non-administrator:**

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"
  -record C:\temp\install_response_file.xml
```

   - AIX HP-UX Linux Solaris **Administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry
  -record /var/temp/install_response_file.xml
```

   - AIX HP-UX Linux Solaris **Non-administrator:**

```
./IBMIM -skipInstall user_home/var/temp/imRegistry
  -record user_home/var/temp/install_response_file.xml
```

   Tip: When you record a new response file, you can specify the -skipInstall parameter. Using this parameter has the following benefits:

   - No files are actually installed, and this speeds up the recording.
   - If you use a temporary data location with the -skipInstall parameter, Installation Manager writes the installation registry to the specified data location while recording. When you start Installation Manager again without the -skipInstall parameter, you then can use your response file to install against the real installation registry.

     The -skipInstall operation should not be used on the actual agent data location used by Installation Manager. This is unsupported. Use a clean writable location, and re-use that location for future recording sessions.

   For more information, read the IBM Installation Manager Information Center.

   c. Add the appropriate repositories to your Installation Manager preferences.

   1) In the top menu, click **File > Preferences**.

   2) Select **Repositories**.

   3) Perform the following actions for each repository:

   a) Click **Add Repository**.

   b) Enter the path to the `repository.config` file in the remote web-based repository or the local directory into which you unpacked the repository files.

For example:

- Remote repositories:

```
https://downloads.mycorp.com:8080/WAS_80_repository
```

or

```
http://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v80
```

- Local repositories:
  - Windows `C:\repositories\proxy\local-repositories`
  - AIX HP-UX Linux Solaris `/var/repositories/proxy/local-repositories`

c) Click **OK**.

4) Click **Apply**.

5) Click **OK**.

d. Click **Install**.

Note: If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.

Installation Manager searches its defined repositories for available packages.

e. Perform the following actions.

1) Select **DMZ Secure Proxy Server for IBM WebSphere Application Server** and the appropriate version.

Note: If you are installing the trial version of this product, select **DMZ Secure Proxy Server for IBM WebSphere Application Server Trial**.

If you already have the DMZ Secure Proxy Server installed on your system, a message displays indicating that the DMZ Secure Proxy Server is already installed. To create another installation of the DMZ Secure Proxy Server in another location, click **Continue**.

2) Click **Next**.

f. Accept the terms in the license agreements, and click **Next**.

g. Specify the installation root directory for the DMZ Secure Proxy Server binaries, which are also referred to as the core product files or system files.

The panel also displays the shared resources directory and disk-space information.

Restrictions:

- Deleting the default target location and leaving an installation-directory field empty prevents you from continuing.
- Do not use symbolic links as the destination directory.

  Symbolic links are not supported.
- Do not use a semicolon in the directory name.

  The DMZ Secure Proxy Server cannot install properly if the target directory includes a semicolon.

  Windows A semicolon is the character used to construct the class path on Windows systems.
- Windows The maximum path length on the Windows Server 2008, Windows Vista, and Windows 7 operating systems is 60 characters.

h. Click **Next**.

i. Select the languages for which translated content should be installed.

English is always selected.

j. Click **Next**.

k. Select the features that you want to install.

Choose from the following features:

- Administration Thin Client

  The Administration Thin Client is a runtime client that enables applications to run administration tasks to the application server.

  Tip: You can run the Installation Manager later to modify this installation and add or remove this feature.

- AIX Linux Solaris Windows IBM Runtime Environment for Java

  This option allows you to choose between a 32-bit and 64-bit IBM Runtime Environment for Java.

  Notes:

  – This option displays only if you are installing on a 64-bit system.

  – This does not apply to Solaris x86 64-bit systems.

  – You must select one of the two options.

  – You cannot modify this installation later and change this selection.

l. Click **Next**.

m. Review the summary information, and click **Install**.

- If the installation is successful, the program displays a message indicating that installation is successful.

  Note: The program might also display important post-installation instructions as well.

- If the installation is not successful, click **View Log File** to troubleshoot the problem.

n. Click **Finish**.

o. Click **File > Exit** to close Installation Manager.

p. Optional: If you are using an authenticated remote repository, create a keyring file for silent installation.

1) From a command line, change to the eclipse subdirectory in the directory where you installed Installation Manager.

2) Start Installation Manager from the command line using the -record option.

For example:

- Windows **Administrator or non-administrator:**

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"
  -keyring C:\IM\im.keyring
  -record C:\temp\keyring_response_file.xml
```

- AIX HP-UX Linux Solaris **Administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry
  -keyring /var/IM/im.keyring
  -record /var/temp/keyring_response_file.xml
```

- AIX HP-UX Linux Solaris **Non-administrator:**

```
./IBMIM -skipInstall user_home/var/temp/imRegistry
  -keyring user_home/var/IM/im.keyring
  -record user_home/var/temp/keyring_response_file.xml
```

3) When a window opens that requests your credentials for the authenticated remote repository, enter the correct credentials and **save** them.

4) Click **File > Exit** to close Installation Manager.

For more information, read the IBM Installation Manager Information Center.

2. **Use the response files to install the DMZ Secure Proxy Server silently:**

a. Optional: **Use the response file to install the keyring silently:** Go to a command line on each of the systems on which you want to install the product, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and install the keyring silently.

For example:

- Windows **Administrator or non-administrator:**

```
imcl.exe -acceptLicense
  input C:\temp\keyring_response_file.xml
  -log C:\temp\keyring_log.xml
```

- AIX HP-UX Linux Solaris **Administrator:**

```
./imcl -acceptLicense
  input /var/temp/keyring_response_file.xml
  -log /var/temp/keyring_log.xml
```

- AIX HP-UX Linux Solaris **Non-administrator:**

```
./imcl -acceptLicense
  input user_home/var/temp/keyring_response_file.xml
  -log user_home/var/temp/keyring_log.xml
```

b. **Use the response file to install the product silently:** Go to a command line on each of the systems on which you want to install the product, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and install the product silently.

For example:

- Windows **Administrator or non-administrator:**

```
imcl.exe -acceptLicense
  input C:\temp\install_response_file.xml
  -log C:\temp\install_log.xml
  -keyring C:\IM\im.keyring
```

- AIX HP-UX Linux Solaris **Administrator:**

```
./imcl -acceptLicense
  input /var/temp/install_response_file.xml
  -log /var/temp/install_log.xml
  -keyring /var/IM/im.keyring
```

- AIX HP-UX Linux Solaris **Non-administrator:**

```
./imcl -acceptLicense
  input user_home/var/temp/install_response_file.xml
  -log user_home/var/temp/install_log.xml
  -keyring user_home/var/IM/im.keyring
```

Notes:

- The relevant terms and conditions, notices, and other information are provided in the license-agreement files in the `lafiles` or *`product_name`*`/lafiles` subdirectory of the installation image or repository for this product.
- The program might write important post-installation instructions to standard output.

Read the IBM Installation Manager Information Center for more information.

Example

Windows The following is an example of a response file for silently installing the DMZ Secure Proxy Server.

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright ######################################################
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2011.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
####################################################################### -->

<!-- ##### Frequently Asked Questions #####################################
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
#     Installation Manager Information Center can be found at:
#     http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
#   Windows = IBMIM.exe -record c:\temp\responsefiles\WASv8.install.Win32.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#   Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv8.install.RHEL64.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse\tools subdirectory in the directory where you installed
# Installation Manager:
#
#   Windows = imcl.exe -acceptLicense -showProgress
#     input <response_file_path_and_name> -log <log_file_path_and_name>
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
#   Windows = imcl.exe -acceptLicense -showProgress
#     input c:\temp\responsefile\WASv8.install.Win32.xml
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input /home/user/responsefile/WASv8.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
#     license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help:  IBMIM -help
#
# Question 3. How do I store and pass credentials to repositories that
# require authentication?
# Answer 3. Installation Manager uses a key ring file to store encrypted
# credentials for authenticating with repositories. Follow this two-step
# process for creating and using a key ring file with Installation Manager.
#
# First, create a key ring file with your credentials by starting
# Installation Manager from the command line under eclipse subdirectory
# with the keyring parameter.
# Use the optional password parameter to password protect your file.
#
#   Windows = IBMIM.exe -keyring <path and file name> -password <password>
#   Linux, UNIX, IBM i and z/OS = ./IBMIM -keyring <path and file name>
#                                 -password <password>
#
# Installation Manager will start in graphical mode. Verify that the
# repositories to which you need to authenticate are included in the
# preferences, File / Preferences / Repositories. If they are not
# listed, then click Add Repositories to add the URL or UNC path.
# Installation Manager will prompt for your credentials. If the repository
# is already in the list, then any attempt to access the repository location,
# such as clicking the Test Connections button, will also prompt for your
# credentials. Enter the correct credential and check the Save password
# checkbox. The credentials are saved to the key ring file you specified.
#
# Second, when you start a silent installation, run imcl under eclipse/tools
# subdirectory, and provide Installation Manager with the location of the key
# ring file and the password if the file is protected. For example:
#
#   Windows = imcl.exe -acceptLicense -showProgress
#     input <path and file name of response file>
#     -keyring <path and name of key ring file> -password <password>
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input <path and file name of response file>
#     -keyring <path and name of key ring file> -password <password>
#
####################################################################### -->

<!-- ##### Agent Input ##############################################
#
# Note that the "acceptLicense" attribute has been deprecated.
# Use "-acceptLicense" command line option to accept license agreements.
#
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the installation finishes.
#
# Valid values for clean:
#      true = only use the repositories and other preferences that are
#           specified in the response file.
#      false = use the repositories and other preferences that are
#           specified in the response file and Installation Manager.
#
# Valid values for temporary:
#      true = repositories and other preferences specified in the
#           response file do not persist in Installation Manager.
#      false = repositories and other preferences specified in the
#           response file persist in Installation Manager.
#
####################################################################### -->

<agent-input clean="true" temporary="true">

<!-- ##### Repositories ###################################################
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#
####################################################################### -->

<server>
    <!-- ##### IBM WebSphere Live Update Repositories ####################
     # These repositories contain DMZ Secure Proxy Server for WebSphere
     # Application Server offerings, and updates for those offerings
     #
     # To use the secure repository (https), you must have an IBM ID,
     # which can be obtained by registering at: http://www.ibm.com/account
     # or your Passport Advantage account.
     #
     # And, you must use a key ring file with your response file.
     ################################################################## -->
<repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v80" />
    <!-- <repository location="https://www.ibm.com/software/rational/repositorymanager/repositories/websphere" /> -->

    <!-- ##### Custom Repositories #######################################
     # Uncomment and update the repository location key below
     # to specify URLs or UNC paths to any intranet repositories
     # and directory paths to local repositories to use.
     ################################################################## -->
    <!-- <repository location='https:\\w3.mycompany.com\repositories\'/> -->
    <!-- <repository location='/home/user/repositories/websphere/'/> -->

    <!-- ##### Local Repositories ########################################
     # Uncomment and update the following line when using a local
     # repository located on your own machine to install a
     # DMZ Secure Proxy Server offering.
     ############################################################# -->
    <!-- <repository location='insert the full directory path inside single quotes'/> -->
</server>

<!-- ##### Install Packages ##########################################
#
# Install Command
#
# Use the install command to inform Installation Manager of the
# installation packages to install.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
#    false = indicates not to modify an existing install by adding
#            or removing features.
#    true = indicates to modify an existing install by adding or
#           removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be installed. The offering listed must be present in
# at least one of the repositories listed earlier. The example
# command below contains the offering ID for the DMZ
# edition of DMZ Secure Proxy Server.
#
# The version attribute is optional. If a version number is provided,
# then the offering will be installed at the version level specified
# as long as it is available in the repositories. If the version
# attribute is not provided, then the default behavior is to install
# the latest version available in the repositories. The version number
# can be found in the repository.xml file in the repositories.
# For example, <offering ... version='8.0.0.20110617_2222'>.
#
# The profile attribute is required and typically is unique to the
# offering. If modifying or updating an existing installation, the
# profile attribute must match the profile ID of the targeted installation
# of DMZ Secure Proxy Server.
#
# The features attribute is optional. Offerings always have at least
# one feature; a required core feature which is installed regardless
# of whether it is explicitly specified. If other feature names
# are provided, then only those features will be installed.
# Features must be comma delimited without spaces.
#
# The feature values for DMZ Secure Proxy Server include:
#  thinclient,com.ibm.jre.6_32bit,com.ibm.jre.6_64bit
#
# On 32-bit machines, the 32-bit jre feature will be install
# automatically even if it is not specified in the response file.
#
# On 64-bit machines, one and only one of the Java Runtime Environment
# (JRE) features must be specified.
#
# The installFixes attribute indicates whether fixes available in
# repositories are installed with the product. By default, all
# available fixes will be installed with the offering.
#
# Valid values for installFixes:
#      none = do not install available fixes with the offering.
#      recommended = installs all available recommended fixes with the offering.
#      all = installs all available fixes with the offering.
#
# Interim fixes for offerings also can be installed while they
# are being installed by including the offering ID for the interim
# fix and specifying the profile ID. A commented out example is
# provided in the install command below.
#
# Installation Manager supports installing multiple offerings at once.
# Additional offerings can be included in the install command,
# with each offering requiring its own offering ID, version, profile value,
# and feature values.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# The eclipseLocation data key should use the same directory path to
# DMZ Secure Proxy Server as the installationLocation attribute.
#
# Include data keys for product specific profile properties.
# For instance, additional translations can be specified by including
# the cic.selector.nl data key and the language codes as values for
# the translations to install.
#
#  Language code values: cs,de,en,es,fr,hu,it,ja,ko,pl,pt_BR,ro,ru,zh,zh_HK,zh_TW
#
###################################################################### -->
<install modify='false'>
<offering id='com.ibm.websphere.NDDMZ.v80'
 profile='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.0'
 features='core.feature,thinclient,com.ibm.jre.6_32bit' installFixes='none'/>
<!-- <offering id='PM12345_WAS80' profile='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.0'/> -->
</install>

<profile id='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.0'
 installLocation='C:\Program Files\IBM\WebSphere\AppServer'>
<data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.nl' value='en'/>
</profile>

<!-- ##### Shared Data Location ########################################
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared'/>
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
```

```
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
#     true = store downloaded artifacts in the shared data location
#     false = remove downloaded artifacts from the shared data location
#
####################################################################### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
-->


<!-- ##### Preferences Settings ###########################################
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
####################################################################### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
 -->

</agent-input>
```

Important: AIX Linux Solaris Windows If you are installing on a 64-bit system, you must include one of the options for an IBM Runtime Environment for Java.

- If you want to use the 32-bit IBM Runtime Environment for Java, include `com.ibm.jre.6_32bit` as a feature in the response file.

  For example:

```
<offering profile='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.0'
  features='core.feature,thinclient,com.ibm.jre.6_32bit' id='com.ibm.websphere.NDDMZ.v80'/>
```

- If you want to use the 64-bit IBM Runtime Environment for Java, include `com.ibm.jre.6_64bit` as a feature in the response file.

  For example:

```
<offering profile='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.0'
  features='core.feature,thinclient,com.ibm.jre.6_64bit' id='com.ibm.websphere.NDDMZ.v80'/>
```

Follow these guidelines:

- Include this feature only if you are installing on a 64-bit system; do not include it if you are installing on a 32-bit system.
- This does not apply to Solaris x86 64-bit systems.
- You must include one of the two options if you are installing on a 64-bit system.

- You cannot modify this installation later and change the selection.

Installing and removing features in the DMZ Secure Proxy Server

You can use Installation Manager to install or remove a feature in the DMZ Secure Proxy Server for IBM WebSphere Application Server.

Before you begin

Make sure that your Installation Manager preferences are pointing to the appropriate web-based or local repositories containing the DMZ Secure Proxy Server.

About this task

Perform this procedure to use Installation Manager to install or remove a feature in the DMZ Secure Proxy Server.

Note: Like other Installation Manager operations, you can invoke a modification from a silent response file. You can record this response file using the GUI and Installation Manager's record mode, or you can manually create or modify a response file to suit your needs.

Procedure

1. Stop all servers and applications on the DMZ Secure Proxy Server installation that is being modified.
2. Start Installation Manager.
3. Click **Modify**.
4. Select the package group to modify.
5. Click **Next**.

   Note: If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.
6. Expand **DMZ Secure Proxy Server for IBM WebSphere Application Server**.
7. Check the appropriate checkbox to install a feature, or clear the appropriate checkbox to remove a feature if you already have it installed.
8. Click **Next**.
9. Review the summary information, and click **Modify**.
   - If the modification is successful, the program displays a message indicating that installation is successful.
   - If the modification is not successful, click **View Log File** to troubleshoot the problem.
10. Click **Finish**.
11. Click **File > Exit** to close Installation Manager.

Example

Like other Installation Manager operations, you can invoke a modification from a silent response file. You can record this response file using the GUI and Installation Manager's record mode, or you can manually create or modify a response file to suit your needs.

Windows Here is a response file that modifies an existing DMZ Secure Proxy Server installation:

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright ######################################################
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2011.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
####################################################################### -->
```

```
<!-- ##### Frequently Asked Questions #####################################
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
#     Installation Manager Information Center can be found at:
#     http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
#   Windows = IBMIM.exe -record c:\temp\responsefiles\WASv8.install.Win32.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#   Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv8.install.RHEL64.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse\tools subdirectory in the directory where you installed
# Installation Manager:
#
#   Windows = imcl.exe -acceptLicense -showProgress
#     input <response_file_path_and_name> -log <log_file_path_and_name>
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
#   Windows = imcl.exe -acceptLicense -showProgress
#     input c:\temp\responsefile\WASv8.install.Win32.xml
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input /home/user/responsefile/WASv8.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
#     license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help:  IBMIM -help
#
# Question 3. How do I store and pass credentials to repositories that
# require authentication?
# Answer 3. Installation Manager uses a key ring file to store encrypted
# credentials for authenticating with repositories. Follow this two-step
# process for creating and using a key ring file with Installation Manager.
#
# First, create a key ring file with your credentials by starting
# Installation Manager from the command line under eclipse subdirectory
# with the keyring parameter.
# Use the optional password parameter to password protect your file.
#
#   Windows = IBMIM.exe -keyring <path and file name> -password <password>
#   Linux, UNIX, IBM i and z/OS = ./IBMIM -keyring <path and file name>
#                                 -password <password>
#
# Installation Manager will start in graphical mode. Verify that the
# repositories to which you need to authenticate are included in the
# preferences, File / Preferences / Repositories. If they are not
# listed, then click Add Repositories to add the URL or UNC path.
# Installation Manager will prompt for your credentials. If the repository
# is already in the list, then any attempt to access the repository location,
# such as clicking the Test Connections button, will also prompt for your
# credentials. Enter the correct credential and check the Save password
# checkbox. The credentials are saved to the key ring file you specified.
#
# Second, when you start a silent installation, run imcl under eclipse/tools
# subdirectory, and provide Installation Manager with the location of the key
# ring file and the password if the file is protected. For example:
#
#   Windows = imcl.exe -acceptLicense -showProgress
#     input <path and file name of response file>
#     -keyring <path and name of key ring file> -password <password>
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input <path and file name of response file>
#     -keyring <path and name of key ring file> -password <password>
#
###################################################################### -->

<!-- ##### Agent Input ##############################################
```

```
#
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the installation finishes.
#
# Valid values for clean:
#      true = only use the repositories and other preferences that are
#           specified in the response file.
#      false = use the repositories and other preferences that are
#           specified in the response file and Installation Manager.
#
# Valid values for temporary:
#      true = repositories and other preferences specified in the
#           response file do not persist in Installation Manager.
#      false = repositories and other preferences specified in the
#           response file persist in Installation Manager.
#
####################################################################### -->

<agent-input clean='true' temporary='true'>

<!-- ##### Repositories ###################################################
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#
####################################################################### -->

<server>
    <!-- ##### IBM WebSphere Live Update Repositories ####################
     # These repositories contain WebSphere Application Server offerings,
     # and updates for those offerings
     #
     # To use the secure repository (https), you must have an IBM ID,
     # which can be obtained by registering at: http://www.ibm.com/account
     # or your Passport Advantage account.
     #
     # And, you must use a key ring file with your response file.
     ################################################################## -->
    <repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v80" />
    <!-- <repository location="https://www.ibm.com/software/rational/repositorymanager/repositories/websphere" /> -->

    <!-- ##### Custom Repositories #######################################
     # Uncomment and update the repository location key below
     # to specify URLs or UNC paths to any intranet repositories
     # and directory paths to local repositories to use.
     ################################################################## -->
    <!-- <repository location='https:\\w3.mycompany.com\repositories\'/> -->
    <!-- <repository location='/home/user/repositories/websphere/'/> -->

    <!-- ##### Local Repositories ########################################
     # Uncomment and update the following line when using a local
     # repository located on your own machine to install a
     # WebSphere Application Server offering.
     ############################################################# -->
    <!-- <repository location='insert the full directory path inside single quotes'/> -->
</server>

<!-- ##### Modify Packages ###############################################
#
# Install and Uninstall Commands
#
# Use the install and uninstall commands to inform Installation Manager
# of the installation packages to install or uninstall.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
#       false = indicates not to modify an existing install by adding
#            or removing features.
#    true = indicates to modify an existing install by adding or
#           removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be installed. The offering listed must be present in
# at least one of the repositories listed earlier. The example
# command below contains the offering ID for the DMZ Secure Proxy Server.
#
# The version attribute is optional. If a version number is provided,
# then the offering will be installed or uninstalled at the version level
# specified as long as it is available in the repositories. If the version
# attribute is not provided, then the default behavior is to install or
# uninstall the latest version available in the repositories. The version
# number can be found in the repository.xml file in the repositories.
# For example, <offering ... version='8.0.0.20110617_2222'>.
#
# The profile attribute is required and typically is unique to the
# offering. If modifying or updating an existing installation, the
# profile attribute must match the profile ID of the targeted installation
# of DMZ Secure Proxy Server.
#
# The features attribute is optional. Offerings always have at least
# one feature; a required core feature which is installed regardless
# of whether it is explicitly specified. If other feature names
# are provided, then only those features will be installed.
# Features must be comma delimited without spaces.
#
# The feature values for DMZ Secure Proxy Server include:
#  thinclient,com.ibm.jre.6_32bit,com.ibm.jre.6_64bit
#
# In the example that follows, the thinclient feature is being removed
# from the specified offering.
#
# Neither the core.feature nor the Java Runtime Environment (JRE)
# feature can be removed because they are required features.
#
# The installFixes attribute indicates whether fixes available in
# repositories are installed with the product. By default, all
# available fixes will be installed with the offering.
#
# Valid values for installFixes:
#      none = do not install available fixes with the offering.
#      recommended = installs all available recommended fixes with the offering.
#      all = installs all available fixes with the offering.
#
# Installation Manager supports modifying multiple offerings at once.
# Additional offerings can be included in the install and uninstall commands,
# with each offering requiring its own offering ID, version, profile value,
# and feature values.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# The eclipseLocation data key should use the same directory path to
# DMZ Secure Proxy Server as the installationLocation attribute.
#
# Include data keys for product specific profile properties.
# For instance, additional translations can be specified by including
# the cic.selector.nl data key and the language codes as values for
# the translations to install.
#
#  Language code values: cs,de,en,es,fr,hu,it,ja,ko,pl,pt_BR,ro,ru,zh,zh_HK,zh_TW
#
################################################################### -->

<uninstall modify='true'>
<offering id='com.ibm.websphere.NDDMZ.v80'
 profile='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.0'
 features='thinclient'/>
</uninstall>

<profile id='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.0'
 installLocation='C:\Program Files\IBM\WebSphere\AppServer'>
<data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.nl' value='en'/>
</profile>

<!-- ##### Shared Data Location ##########################################
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared'/>
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
```

```
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
#     true = store downloaded artifacts in the shared data location
#     false = remove downloaded artifacts from the shared data location
#
#################################################################### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
-->

<!-- ##### Preferences Settings ##########################################
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
#################################################################### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
 -->

</agent-input>
```

Updating the DMZ Secure Proxy Server

You can use Installation Manager to update the DMZ Secure Proxy Server to a later version.

Before you begin

Make sure that your Installation Manager preferences are pointing to web-based or local repositories that contain the appropriate updates for the DMZ Secure Proxy Server.

About this task

Perform this procedure to use Installation Manager to update the DMZ Secure Proxy Server.

Procedure

1. Start Installation Manager.
2. Click **Update**.
3. Select the package group to update.
4. Click **Next**.

   Note: If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.
5. Select the version to which you want to update under **DMZ Secure Proxy Server for IBM WebSphere Application Server**.
6. Click **Next**.
7. Accept the terms in the license agreements, and click **Next**.
8. Review the summary information, and click **Update**.
   - If the installation is successful, the program displays a message indicating that installation is successful.
   - If the installation is not successful, click **View Log File** to troubleshoot the problem.
9. Click **Finish**.
10. Click **File > Exit** to close Installation Manager.

Rolling back the DMZ Secure Proxy Server

You can use Installation Manager to roll back the DMZ Secure Proxy Server to an earlier version.

Before you begin

Make sure that your Installation Manager preferences are pointing to web-based or local repositories that contain the appropriate earlier version of the DMZ Secure Proxy Server.

About this task

Perform this procedure to use Installation Manager to roll back the DMZ Secure Proxy Server to an earlier version.

Procedure

1. Start Installation Manager.
2. Click **Roll Back**.
3. Select the package group to roll back.
4. Click **Next**.

   Note: If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.
5. Select the version to which you want to roll back under **DMZ Secure Proxy Server for IBM WebSphere Application Server**.
6. Click **Next**.
7. Review the summary information, and click **Roll Back**.
   - If the roll back is successful, the program displays a message indicating that the roll back is successful.
   - If the roll back is not successful, click **View Log File** to troubleshoot the problem.
8. Click **Finish**.
9. Click **File > Exit** to close Installation Manager.

Uninstalling the DMZ Secure Proxy Server using the GUI

Use the Installation Manager GUI to uninstall the DMZ Secure Proxy Server.

Procedure

1. Uninstall the DMZ Secure Proxy Server.
   a. Stop all servers and applications on the DMZ Secure Proxy Server installation that contains the product.
   b. Start Installation Manager.
   c. Click **Uninstall**.
   d. In the **Uninstall Packages** window, perform the following actions.
      1) Select **DMZ Secure Proxy Server for IBM WebSphere Application Server** and the appropriate version.

         Note: If you are uninstalling the ILAN version of this product, select **DMZ Secure Proxy Server for IBM WebSphere Application Server (ILAN)**.
      2) Click **Next**.
   e. Review the summary information.
   f. Click **Uninstall**.
      - If the uninstallation is successful, the program displays a message that indicates success.
      - If the uninstallation is not successful, click **View log** to troubleshoot the problem.
   g. Click **Finish**.
   h. Click **File > Exit** to close Installation Manager.
2. Optional: Uninstall IBM Installation Manager.

   Important: Before you can uninstall IBM Installation Manager, you must uninstall all of the packages that were installed by Installation Manager.

   Read Uninstalling Installation Manager in the Installation Manager information center for information about performing this procedure.

Uninstalling the DMZ Secure Proxy Server silently

You can use Installation Manager to uninstall the DMZ Secure Proxy Server silently.

Before you begin

Optional: Perform or record the installation of Installation Manager and installation of the DMZ Secure Proxy Server to a temporary installation registry on one of your systems so that you can use this temporary registry to record the uninstallation without using the standard registry where Installation Manager is installed.

Read the following for more information:
- "Installing the DMZ Secure Proxy Server using the GUI" on page 233
- "Installing the DMZ Secure Proxy Server silently" on page 237

About this task

Using Installation Manager, you can work with response files to uninstall the DMZ Secure Proxy Server silently in a variety of ways. You can record a response file using the GUI as described in the following procedure, or you can generate a new response file by hand or by taking an example and modifying it.

Procedure

1. Stop all servers and applications on the DMZ Secure Proxy Server installation that contains the product.
2. Optional: **Record a response file to uninstall the DMZ Secure Proxy Server:** On one of your systems, perform the following actions to record a response file that will uninstall the DMZ Secure Proxy Server:
   a. From a command line, change to the eclipse subdirectory in the directory where you installed Installation Manager.
   b. Start Installation Manager from the command line using the -record option.

      For example:

      - Windows **Administrator or non-administrator:**

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"
  -record C:\temp\uninstall_response_file.xml
```

      - AIX HP-UX Linux Solaris **Administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry
  -record /var/temp/uninstall_response_file.xml
```

      - AIX HP-UX Linux Solaris **Non-administrator:**

```
./IBMIM -skipInstall user_home/var/temp/imRegistry
  -record user_home/var/temp/uninstall_response_file.xml
```

      Tip: If you choose to use the -skipInstall parameter with a temporary installation registry created as described in "Before you begin," Installation Manager uses the temporary installation registry while recording the response file. It is important to note that when the -skipInstall parameter is specified, no packages are installed or uninstalled. All of the actions that you perform in Installation Manager simply update the installation data that is stored in the specified temporary registry. After the response file is generated, it can be used to uninstall the DMZ Secure Proxy Server, removing the DMZ Secure Proxy Server files and updating the standard installation registry.

      The -skipInstall operation should not be used on the actual agent data location used by Installation Manager. This is unsupported. Use a clean writable location, and re-use that location for future recording sessions.

      For more information, read the IBM Installation Manager Information Center.
   c. Click **Uninstall**.
   d. In the **Uninstall Packages** window, perform the following actions.
      1) Select **DMZ Secure Proxy Server for IBM WebSphere Application Server** and the appropriate version.

         Note: If you are uninstalling the ILAN version of this product, select **DMZ Secure Proxy Server for IBM WebSphere Application Server (ILAN)**.
      2) Click **Next**.
   e. Review the summary information.
   f. Click **Uninstall**.
      - If the uninstallation is successful, the program displays a message that indicates success.
      - If the uninstallation is not successful, click **View log** to troubleshoot the problem.
   g. Click **Finish**.
   h. Click **File > Exit** to close Installation Manager.
3. **Use the response file to uninstall the DMZ Secure Proxy Server silently:** From a command line on each of the systems from which you want to uninstall the DMZ Secure Proxy Server, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager and use the response file that you created to silently uninstall the DMZ Secure Proxy Server.

   For example:

- Windows **Administrator or non-administrator:**

```
imcl.exe
  input C:\temp\uninstall_response_file.xml
  -log C:\temp\uninstall_log.xml
```

- AIX HP-UX Linux Solaris **Administrator:**

```
./imcl
  input /var/temp/uninstall_response_file.xml
  -log /var/temp/uninstall_log.xml
```

- AIX HP-UX Linux Solaris **Non-administrator:**

```
./imcl
  input user_home/var/temp/uninstall_response_file.xml
  -log user_home/var/temp/uninstall_log.xml
```

Go to the IBM Installation Manager Information Center for more information.

4. Optional: Uninstall IBM Installation Manager.

   Important: Before you can uninstall IBM Installation Manager, you must uninstall all of the packages that were installed by Installation Manager.

   Read the IBM Installation Manager Information Center for information about using the uninstall script to perform this procedure.

Windows

Example

The following is an example of a response file for silently uninstalling the DMZ Secure Proxy Server.

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright ######################################################
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2011.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#################################################################### -->

<!-- ##### Frequently Asked Questions #####################################
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
#     Installation Manager Information Center can be found at:
#     http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
#   Windows = IBMIM.exe -record c:\temp\responsefiles\WASv8.install.Win32.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#   Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv8.install.RHEL64.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse\tools subdirectory in the directory where you installed
# Installation Manager:
#
#   Windows = imcl.exe -acceptLicense -showProgress
#     input <response_file_path_and_name> -log <log_file_path_and_name>
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
#   Windows = imcl.exe -acceptLicense -showProgress
#     input c:\temp\responsefile\WASv8.install.Win32.xml
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input /home/user/responsefile/WASv8.install.RHEL64.xml
#
```

```
# The -acceptLicense command must be included to indicate acceptance of all
#     license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help:  IBMIM -help
#
####################################################################### -->

<!-- ##### Agent Input #############################################
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the uninstall finishes.
#
# Valid values for clean:
#      true = only use the repositories and other preferences that are
#           specified in the response file.
#      false = use the repositories and other preferences that are
#           specified in the response file and Installation Manager.
#
# Valid values for temporary:
#      true = repositories and other preferences specified in the
#           response file do not persist in Installation Manager.
#      false = repositories and other preferences specified in the
#           response file persist in Installation Manager.
#
####################################################################### -->

<agent-input clean='true' temporary='true'>

<!-- ##### Repositories ###################################################
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#
####################################################################### -->

<server>
    <!-- ##### IBM WebSphere Live Update Repositories ####################
     # These repositories contain WebSphere Application Server offerings,
     # and updates for those offerings
     #
     # To use the secure repository (https), you must have an IBM ID,
     # which can be obtained by registering at: http://www.ibm.com/account
     # or your Passport Advantage account.
     #
     # And, you must use a key ring file with your response file.
     ################################################################## -->
    <repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v80" />
    <!-- <repository location="https://www.ibm.com/software/rational/repositorymanager/repositories/websphere" /> -->

    <!-- ##### Custom Repositories #######################################
     # Uncomment and update the repository location key below
     # to specify URLs or UNC paths to any intranet repositories
     # and directory paths to local repositories to use.
     ################################################################## -->
    <!-- <repository location='https:\\w3.mycompany.com\repositories\'/> -->
    <!-- <repository location='/home/user/repositories/websphere/'/> -->

    <!-- ##### Local Repositories ########################################
     # Uncomment and update the following line when using a local
     # repository located on your own machine to install a
     # WebSphere Application Server offering.
     ############################################################# -->
    <!-- <repository location='insert the full directory path inside single quotes'/> -->
</server>

<!-- ##### Uninstall Packages ############################################
#
# Uninstall Command
#
# Use the uninstall command to inform Installation Manager of the
# installation packages to uninstall.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
#    false = indicates not to modify an existing install by adding
#            or removing features.
#    true = indicates to modify an existing install by adding or
#           removing features.
#
```

```
# The offering ID attribute is required because it specifies the
# offering to be uninstalled. The example command below contains the
# offering ID for DMZ Secure Proxy Server.
#
# The version attribute is optional. If a version number is provided,
# then the offering will be uninstalled at the version level specified
# If the version attribute is not provided, then the default behavior is
# to uninstall the latest version. The version number can be found in
# the repository.xml file in the repositories.
# For example, <offering ... version='8.0.0.20110617_2222'>.
#
# The profile attribute is required and must match the package group
# name for the offering to be uninstalled.
#
# The features attribute is optional. If there is no feature attribute,
# then all features are uninstalled. If features are specified, then
# only those features will be uninstalled.
# Features must be comma delimited without spaces.
#
# The feature values for DMZ Secure Proxy Server include:
#  thinclient,
#  com.ibm.jre.6_32bit,com.ibm.jre.6_64bit
#
# Installation Manager supports uninstalling multiple offerings at once.
# Additional offerings can be included in the uninstall command,
# with each offering requiring its own offering ID, version, profile value,
# and feature values.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# The eclipseLocation data key should use the same directory path to
# DMZ Secure Proxy Server as the installationLocation attribute.
#
# Include data keys for product specific profile properties.
# For instance, additional translations can be specified by including
# the cic.selector.nl data key and the language codes as values for
# the translations to install.
#
#  Language code values: cs,de,en,es,fr,hu,it,ja,ko,pl,pt_BR,ro,ru,zh,zh_HK,zh_TW
#
################################################################## -->

<uninstall modify='false'>
<offering id='com.ibm.websphere.NDDMZ.v80'
 profile='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.0'
 features='core.feature,thinclient,com.ibm.jre.6_32bit'/>
</uninstall>

<profile id='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.0'
 installLocation='C:\Program Files\IBM\WebSphere\AppServer'>
<data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.nl' value='cs,de,en,es,fr,hu,it,ja,ko,pl,pt_BR,ro,ru,zh,zh_HK,zh_TW'/>
</profile>

<!-- ##### Shared Data Location ##########################################
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared'/>
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
#     true = store downloaded artifacts in the shared data location
#     false = remove downloaded artifacts from the shared data location
#
####################################################################### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
-->

<!-- ##### Preferences Settings ###########################################
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
####################################################################### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
 -->

</agent-input>
```

Chapter 9. Installing and using the WebSphere Customization Toolbox

The WebSphere Customization Toolbox include tools for managing, configuring, and migrating various parts of your WebSphere Application Server environment.

About this task

Note: The WebSphere Customization Toolbox for WebSphere Application Server Version 8.0 includes tools for customizing various parts of your WebSphere Application Server environment.

- You can launch the Web Server Plug-ins Configuration Tool to configure your web server plug-ins for any operating system on which the WebSphere Customization Toolbox can be installed.

  You can also use the WCT command-line utility to launch the command-line version of the Plug-ins Configuration Tool, the pct tool.
- You can launch the Profile Management Tool (z/OS only) on an Intel-based Windows or Linux operating system to generate jobs and instructions for creating profiles for WebSphere Application Server on z/OS systems.
- You can launch the z/OS Migration Management Tool on an Intel-based Windows or Linux operating system to generate definitions for migrating WebSphere Application Server for z/OS profiles.

Procedure

Perform one of the following procedures:

- Install and use the WebSphere Customization Toolbox GUI to invoke the following tools.
  - Profile Management Tool (z/OS only)

    The Profile Management Tool (z/OS only) allows you to build and process definitions for creating WebSphere Application Server profiles.

    Processing the definitions results in the generation of customization jobs that you then run on the z/OS system. You can upload directly to the z/OS system as you process a definition, or you can save it locally and upload it to the z/OS system later.
  - z/OS Migration Management Tool

    The z/OS Migration Management Tool allows you to build and process definitions for migrating WebSphere Application Server profiles.

    Processing the definitions results in the generation of customization jobs that you then run on the z/OS system. You can upload directly to the z/OS system as you process a definition, or you can save it locally and upload it to the z/OS system later.
  - Web Server Plug-ins Configuration Tool

    The Web Server Plug-ins Configuration Tool allows you to configure your web server plug-ins on distributed and Windows operating systems.
- Use the WCT command-line utility to invoke a WebSphere Customization Toolbox (WCT) command-line tool.

What to do next

Restriction:

You cannot use of some combinations of the GUI customization tools for IBM WebSphere Application Server Version 8.0 concurrently.

- You cannot have the following tools or two instances of either tool open at the same time:

  - Profile Management Tool for distributed operating systems
  - Configuration Migration Tool for distributed operating systems
- You cannot have the following tools within the WebSphere Customization Toolbox or two instances of any one tool open at the same time:
  - Web Server Plug-ins Configuration Tool
  - Profile Management Tool (z/OS only), which runs on Intel-based Windows or Linux operating systems
  - z/OS Migration Management Tool, which runs on Intel-based Windows or Linux operating systems

You can use one tool from one of these two sets and one tool from the other set at the same time.

Installing, updating, rolling back, and uninstalling the WebSphere Customization Toolbox

IBM Installation Manager is a common installer for many IBM software products that you use to install, update, roll back, and uninstall the WebSphere Customization Toolbox.

About this task

The WebSphere Customization Toolbox contains the following optional tools:

- Web Server Plug-ins Configuration Tool

  The Web Server Plug-ins Configuration Tool configures the web server plug-ins for WebSphere Application Server so that your web server and application server can communicate with each other.

  Note: This tool can be installed and run on AIX, HP-UX, Linux, Solaris systems.
- Profile Management Tool (z/OS only)

  The Profile Management Tool (z/OS only) creates customized definitions on an Intel-based Windows or Linux operating system that are used to create or augment WebSphere Application Server profiles on z/OS systems. Each customization definition includes a set of customized jobs with associated instructions. The generated jobs must be uploaded to and run on the target z/OS system.

  Restriction: This tool can be installed and run on Intel-based Windows and Linux platforms only.
- z/OS Migration Management Tool

  The z/OS Migration Management Tool creates migration definitions on an Intel-based Windows or Linux operating system that are used to migrate a WebSphere Application Server for z/OS node. Each migration definition consists of a set of customized migration jobs with associated instructions. The generated migration jobs must be uploaded to and run on the target z/OS system.

  Restriction: This tool can be installed and run on Intel-based Windows and Linux platforms only.
- Remote Installation Tool for IBM i

  The iRemoteInstall command that is installed when you select this option allows you to install IBM Installation Manager or a WebSphere Application Server product offering from a Windows workstation to a remote target IBM i system. The iRemoteInstall command is installed into the following directory:

```
wct_root/Remote_Installation_Tool_for_IBM_i
```

  Restriction: This tool can be installed and run on Windows operating systems only.

Perform one of these procedures to install, update, roll back, or uninstall the WebSphere Customization Toolbox using Installation Manager.

Procedure

- “Installing the WebSphere Customization Toolbox using the GUI”
- “Installing the WebSphere Customization Toolbox silently” on page 265
- “Installing and removing tools in the WebSphere Customization Toolbox” on page 275
- “Updating the WebSphere Customization Toolbox” on page 280
- “Rolling back the WebSphere Customization Toolbox” on page 280
- “Uninstalling the WebSphere Customization Toolbox using the GUI” on page 281
- “Uninstalling the WebSphere Customization Toolbox silently” on page 282

What to do next

The versionInfo and historyInfo commands return version and history information for the WebSphere Customization Toolbox based on all of the installation, uninstallation, update, and rollback activities performed on the system.

Installing the WebSphere Customization Toolbox using the GUI

You can use the Installation Manager GUI to install the WebSphere Customization Toolbox.

Before you begin

Install Installation Manager:

1. Perform one of the following procedures:
   - If you want to use the Installation Manager that is included with this product, perform the following actions:
     a. Obtain the necessary files from the physical media or the web.

        There are three basic options for obtaining and installing Installation Manager and the product.

        – **Access the physical media, and use local installation**

          You can access Installation Manager and the product repositories on the product media. You can install Installation Manager on your system and use it to install the product from the product repositories on the media.

        – **Download the files from the Passport Advantage site, and use local installation**

          Licensed customers can download Installation Manager as well as the necessary product repositories from the Passport Advantage site. You can then install Installation Manager on your system and use it to install the product from the repositories.

        – **Download a file from the Installation Manager website, and use web-based installation**

          You can download and unpack a compressed file containing Installation Manager from the IBM Installation Manager website. You can then install Installation Manager on your local system and use it to install the product from the web-based repository located at

```
http://www.ibm.com/software/repositorymanager/com.ibm.websphere.WCT.v80
```

     b. Change to the location containing the Installation Manager installation files, and run one of the following commands:

        Administrative installation:

        – **Windows:** `install.exe`

        – **AIX, HP-UX, Linux, and Solaris:** `./install`

        Non-administrative installation:

        – **Windows:** `userinst.exe`

        – **AIX, HP-UX, Linux, and Solaris:** `./userinst`

Group-mode installation (AIX, HP-UX, Linux, and Solaris only):

```
./groupinst -dataLocation application_data_location
```

Notes on group mode:

- Group mode allows users to share packages in a common location and manage them with the same instance of Installation Manager.
- Group mode is not available on Windows operating systems.
- If you do not install Installation Manager using group mode, you will not be able to use group mode to manage any of the products that you install later using this Installation Manager.
- Make sure that you change the installation location from the default location in the current user's home directory to a location that is accessible by all users in the group.
- Set up your groups, permissions, and environment variables as described in the Group mode road maps in the IBM Installation Manager Information Center before installing in group mode.
- For more information on using group mode, read the Group mode road maps in the IBM Installation Manager Information Center.

The installer opens an **Install Packages** window.

c. Make sure that the Installation Manager package is selected, and click **Next**.

d. Accept the terms in the license agreements, and click **Next**.

The program creates the directory for your installation.

e. Click **Next**.

f. Review the summary information, and click **Install**.

- If the installation is successful, the program displays a message indicating that installation is successful.
- If the installation is not successful, click **View Log File** to troubleshoot the problem.

- If you already have a version of Installation Manager installed on your system and you want to use it to install and maintain the product, obtain the necessary product files from the physical media or the web.

  There are three basic options for installing the product.

  - **Access the physical media, and use local installation**

    You can access the product repositories on the product media. Use your existing Installation Manager to install the product from the product repositories on the media.

  - **Download the files from the Passport Advantage site, and use local installation**

    Licensed customers can download the necessary product repositories from the Passport Advantage site. You can then use your existing Installation Manager to install the product from the repositories.

  - **Access the live repositories, and use web-based installation**

    You can install Installation Manager on your local system and use it to install the product from the web-based repository located at

```
http://www.ibm.com/software/repositorymanager/com.ibm.websphere.WCT.v80
```

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

2. Add the product repository to your Installation Manager preferences.

a. Start Installation Manager.

b. In the top menu, click **File > Preferences**.

c. Select **Repositories**.

d. Perform the following actions:

   1) Click **Add Repository**.

   2) Enter the path to the `repository.config` file in the location containing the repository files.

      For example:

      - **Windows:** `C:\repositories\`*`product_name`*`\local-repositories`
      - **AIX, HP-UX, Linux, Solaris:** `/var/repositories/`*`product_name`*`/local-repositories`

      or

`http://www.ibm.com/software/repositorymanager/com.ibm.websphere.WCT.v80`

   3) Click **OK**.

e. Deselect any locations listed in the Repositories window that you will not be using.

f. Click **Apply**.

g. Click **OK**.

h. Click **File > Exit** to close Installation Manager.

About this task

Perform this procedure to use the Installation Manager GUI to install the WebSphere Customization Toolbox.

Procedure

1. Start Installation Manager.

   Tip: On AIX, HP-UX, Linux, and Solaris systems, you can start Installation Manager in group mode with the ./IBMIM command.

   - Group mode allows users to share packages in a common location and manage them with the same instance of Installation Manager.
   - For more information on using group mode, read the Group mode road maps in the IBM Installation Manager Information Center.

2. Click **Install**.

   Note: If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.

   Installation Manager searches its defined repositories for available packages.

3. Perform the following actions.

   a. Select **WebSphere Customization Toolbox** and the appropriate version.

      Note: If you are installing the unsupported ILAN version of this product, select **WebSphere Customization Toolbox (ILAN)**.

      If you already have the WebSphere Customization Toolbox installed on your system, a message displays indicating that the WebSphere Customization Toolbox is already installed. To create another installation of the WebSphere Customization Toolbox in another location, click **Continue**.

   b. Click **Next**.

   Note: If you try to install a newer level of the WebSphere Customization Toolbox with a previous version of Installation Manager, Installation Manager might prompt you to update to the latest level of Installation Manager when it connects to the repository. Update to the newer version before you continue if you are prompted to do so. Read Installing updates in the Installation Manager information center for information about automatic updates.

4. Accept the terms in the license agreements, and click **Next**.
5. Specify the installation root directory for the tool binaries, which are also referred to as the core product files or system files.

   The panel also displays the shared resources directory and disk-space information.

   Restrictions:

   - Deleting the default target location and leaving an installation-directory field empty prevents you from continuing.
   - Do not use symbolic links as the destination directory.

     Symbolic links are not supported.
   - Do not use a semicolon in the directory name.

     The WebSphere Customization Toolbox cannot install properly if the target directory includes a semicolon.
   - The maximum path length on the Windows Server 2008, Windows Vista, and Windows 7 operating systems is 60 characters.
6. Click **Next**.
7. Select the tools that you want to install.

   Choose from the following optional tools:

   - Web Server Plug-ins Configuration Tool

     The Web Server Plug-ins Configuration Tool configures the web server plug-ins for WebSphere Application Server so that your web server and application server can communicate with each other.
   - Profile Management Tool (z/OS only)

     The Profile Management Tool (z/OS only) creates customized definitions on an Intel-based Windows or Linux operating system that are used to create or augment WebSphere Application Server profiles on z/OS systems. Each customization definition includes a set of customized jobs with associated instructions. The generated jobs must be uploaded to and run on the target z/OS system.

     Restriction: This tool can be installed and run on Intel-based Windows and Linux platforms only.
   - z/OS Migration Management Tool

     The z/OS Migration Management Tool creates migration definitions on an Intel-based Windows or Linux operating system that are used to migrate a WebSphere Application Server for z/OS node. Each migration definition consists of a set of customized migration jobs with associated instructions. The generated migration jobs must be uploaded to and run on the target z/OS system.

     Restriction: This tool can be installed and run on Intel-based Windows and Linux platforms only.
   - Remote Installation Tool for IBM i

     The iRemoteInstall command that is installed when you select this option allows you to install IBM Installation Manager or a WebSphere Application Server product offering from a Windows workstation to a remote target IBM i system. The iRemoteInstall command is installed into the following directory:

```
wct_root/Remote_Installation_Tool_for_IBM_i
```

     Restriction: This tool can be installed and run on Windows operating systems only.

   Note: If you install the z/OS Migration Management Tool, you must also install the Profile Management Tool (z/OS only). This selection is done automatically.
8. Click **Next**.

9. Review the summary information, and click **Install**.
   - If the installation is successful, the program displays a message indicating that installation is successful.

     Note: The program might also display important post-installation instructions as well.
   - If the installation is not successful, click **View Log File** to troubleshoot the problem.
10. Optional: Select **None** to deselect **WebSphere Customization Toolbox** if you do not want to open the WebSphere Customization Toolbox when this installation is finished.
11. Click **Finish**.
12. Click **File > Exit** to close Installation Manager.

Installing the WebSphere Customization Toolbox silently

You can use Installation Manager to install the WebSphere Customization Toolbox silently.

Before you begin

Install Installation Manager on each of the systems onto which you want to install the product.

1. Perform one of the following procedures:
   - If you want to use the Installation Manager that is included with this product, perform the following actions:
     a. Obtain the necessary files from the physical media or the web.

        There are three basic options for obtaining and installing Installation Manager and the product.
        - **Access the physical media, and use local installation**

          You can access Installation Manager and the product repositories on the product media. You can install Installation Manager on your system and use it to install the product from the product repositories on the media.
        - **Download the files from the Passport Advantage site, and use local installation**

          Licensed customers can download Installation Manager as well as the necessary product repositories from the Passport Advantage site. You can then install Installation Manager on your system and use it to install the product from the repositories.
        - **Download a file from the Installation Manager website, and use web-based installation**

          You can download and unpack a compressed file containing Installation Manager from the IBM Installation Manager website. You can then install Installation Manager on your local system and use it to install the product from the web-based repository located at

```
http://www.ibm.com/software/repositorymanager/com.ibm.websphere.WCT.v80
```

     b. Change to the location containing the Installation Manager installation files, and run one of the following commands:

        Administrative installation:
        - **Windows:** `installc.exe -acceptLicense -log` *`log_file_path_and_name`*
        - **AIX, HP-UX, Linux, and Solaris:** `./installc -acceptLicense -log` *`log_file_path_and_name`*

        Non-administrative installation:
        - **Windows:** `userinstc.exe -acceptLicense -log` *`log_file_path_and_name`*
        - **AIX, HP-UX, Linux, and Solaris:** `./userinstc -acceptLicense -log` *`log_file_path_and_name`*

        Group-mode installation (AIX, HP-UX, Linux, and Solaris only):

```
./groupinstc -acceptLicense -dataLocation application_data_location -log
log_file_path_and_name
```

Notes on group mode:

- Group mode allows users to share packages in a common location and manage them with the same instance of Installation Manager.
- Group mode is not available on Windows operating systems.
- If you do not install Installation Manager using group mode, you will not be able to use group mode to manage any of the products that you install later using this Installation Manager.
- Make sure that you change the installation location from the default location in the current user's home directory to a location that is accessible by all users in the group.
- Set up your groups, permissions, and environment variables as described in the Group mode road maps in the IBM Installation Manager Information Center before installing in group mode.
- For more information on using group mode, read the Group mode road maps in the IBM Installation Manager Information Center.

- If you already have a version of Installation Manager installed on your system and you want to use it to install and maintain the product, obtain the necessary product files from the physical media or the web.

  There are three basic options for installing the product.

  - **Access the physical media, and use local installation**

    You can access the product repositories on the product media. Use your existing Installation Manager to install the product from the product repositories on the media.

  - **Download the files from the Passport Advantage site, and use local installation**

    Licensed customers can download the necessary product repositories from the Passport Advantage site. You can then use your existing Installation Manager to install the product from the repositories.

  - **Access the live repositories, and use web-based installation**

    You can install Installation Manager on your local system and use it to install the product from the web-based repository located at

```
http://www.ibm.com/software/repositorymanager/com.ibm.websphere.WCT.v80
```

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

2. Add the product repository to your Installation Manager preferences.
   a. Start Installation Manager.
   b. In the top menu, click **File > Preferences**.
   c. Select **Repositories**.
   d. Perform the following actions:
      1) Click **Add Repository**.
      2) Enter the path to the `repository.config` file in the location containing the repository files.

         For example:

         - **Windows:** `C:\repositories\`*`product_name`*`\local-repositories`
         - **AIX, HP-UX, Linux, Solaris:** `/var/repositories/`*`product_name`*`/local-repositories`

         or

```
http://www.ibm.com/software/repositorymanager/com.ibm.websphere.WCT.v80
```

3) Click **OK**.

e. Deselect any locations listed in the Repositories window that you will not be using.

f. Click **Apply**.

g. Click **OK**.

h. Click **File > Exit** to close Installation Manager.

About this task

Using Installation Manager, you can work with response files to install the WebSphere Customization Toolbox silently in a variety of ways. You can record a response file using the GUI as described in the following procedure, or you can generate a new response file by hand or by taking an example and modifying it.

Procedure

1. Optional: **Record a response file to install the WebSphere Customization Toolbox:** On one of your systems, perform the following actions to record a response file that will install the WebSphere Customization Toolbox.

   a. From a command line, change to the eclipse subdirectory in the directory where you installed Installation Manager.

   b. Start Installation Manager from the command line using the -record option.

   For example:

   - **Windows administrator or non-administrator:**

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"
  -record C:\temp\install_response_file.xml
```

   - **AIX, HP-UX, Linux, or Solaris administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry
  -record /var/temp/install_response_file.xml
```

   - **AIX, HP-UX, Linux, or Solaris non-administrator:**

```
./IBMIM -skipInstall user_home/var/temp/imRegistry
  -record user_home/var/temp/install_response_file.xml
```

   Tip: When you record a new response file, you can specify the -skipInstall parameter. Using this parameter has the following benefits:

   - No files are actually installed, and this speeds up the recording.
   - If you use a temporary data location with the -skipInstall parameter, Installation Manager writes the installation registry to the specified data location while recording. When you start Installation Manager again without the -skipInstall parameter, you then can use your response file to install against the real installation registry.

     The -skipInstall operation should not be used on the actual agent data location used by Installation Manager. This is unsupported. Use a clean writable location, and re-use that location for future recording sessions.

   For more information, read the IBM Installation Manager Information Center.

   c. Add the appropriate repositories to your Installation Manager preferences.

   1) In the top menu, click **File > Preferences**.

   2) Select **Repositories**.

   3) Perform the following actions for each repository:

   a) Click **Add Repository**.

   b) Enter the path to the `repository.config` file in the remote web-based repository or the local directory into which you unpacked the repository files.

   For example:

   - Remote repositories:

```
https://downloads.mycorp.com:8080/WAS_80_repository
```

or

```
http://www.ibm.com/software/repositorymanager/com.ibm.websphere.WCT.v80
```

- Local repositories:
  - **Windows:** `C:\repositories\wct\local-repositories`
  - **AIX, HP-UX, Linux, Solaris:** `/var/repositories/wct/local-repositories`

c) Click **OK**.

4) Click **Apply**.

5) Click **OK**.

d. Click **Install**.

Note: If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.

Installation Manager searches its defined repositories for available packages.

e. Perform the following actions.

1) Select **WebSphere Customization Toolbox** and the appropriate version.

Note: If you are installing the unsupported ILAN version of this product, select **WebSphere Customization Toolbox (ILAN)**.

If you already have the WebSphere Customization Toolbox installed on your system, a message displays indicating that the WebSphere Customization Toolbox is already installed. To create another installation of the WebSphere Customization Toolbox in another location, click **Continue**.

2) Click **Next**.

f. Accept the terms in the license agreements, and click **Next**.

g. Specify the installation root directory for the WebSphere Customization Toolbox binaries, which are also referred to as the core product files or system files.

The panel also displays the shared resources directory and disk-space information.

Restrictions:

- Deleting the default target location and leaving an installation-directory field empty prevents you from continuing.
- Do not use symbolic links as the destination directory.

  Symbolic links are not supported.
- Do not use a semicolon in the directory name.

  The WebSphere Customization Toolbox cannot install properly if the target directory includes a semicolon.
- The maximum path length on the Windows Server 2008, Windows Vista, and Windows 7 operating systems is 60 characters.

h. Click **Next**.

i. Select the features (tools) that you want to install.

Choose from the following optional tools:

- Web Server Plug-ins Configuration Tool

  The Web Server Plug-ins Configuration Tool configures the web server plug-ins for WebSphere Application Server so that your web server and application server can communicate with each other.
- Profile Management Tool (z/OS only)

The Profile Management Tool (z/OS only) creates customized definitions on an Intel-based Windows or Linux operating system that are used to create or augment WebSphere Application Server profiles on z/OS systems. Each customization definition includes a set of customized jobs with associated instructions. The generated jobs must be uploaded to and run on the target z/OS system.

Restriction: This tool can be installed and run on Intel-based Windows and Linux platforms only.

- z/OS Migration Management Tool

  The z/OS Migration Management Tool creates migration definitions on an Intel-based Windows or Linux operating system that are used to migrate a WebSphere Application Server for z/OS node. Each migration definition consists of a set of customized migration jobs with associated instructions. The generated migration jobs must be uploaded to and run on the target z/OS system.

  Restriction: This tool can be installed and run on Intel-based Windows and Linux platforms only.

- Remote Installation Tool for IBM i

  The iRemoteInstall command that is installed when you select this option allows you to install IBM Installation Manager or a WebSphere Application Server product offering from a Windows workstation to a remote target IBM i system. The iRemoteInstall command is installed into the following directory:

```
wct_root/Remote_Installation_Tool_for_IBM_i
```

  Restriction: This tool can be installed and run on Windows operating systems only.

Note: If you install the z/OS Migration Management Tool, you must also install the Profile Management Tool (z/OS only). This selection is done automatically.

j. Click **Next**.

k. Review the summary information, and click **Install**.

- If the installation is successful, the program displays a message indicating that installation is successful.

  Note: The program might also display important post-installation instructions as well.

- If the installation is not successful, click **View Log File** to troubleshoot the problem.

l. Optional: Select **None** to deselect **WebSphere Customization Toolbox** if you do not want to open the WebSphere Customization Toolbox when this installation is finished.

This option is unavailable if you used the -skipInstall parameter.

m. Click **Finish**.

n. Click **File > Exit** to close Installation Manager.

o. Optional: If you are using an authenticated remote repository, create a keyring file for silent installation.

1) From a command line, change to the eclipse subdirectory in the directory where you installed Installation Manager.

2) Start Installation Manager from the command line using the -record option.

For example:

- **Windows administrator or non-administrator:**

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"
  -keyring C:\IM\im.keyring
  -record C:\temp\keyring_response_file.xml
```

- **AIX, HP-UX, Linux, or Solaris administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry
  -keyring /var/IM/im.keyring
  -record /var/temp/keyring_response_file.xml
```

- **AIX, HP-UX, Linux, or Solaris non-administrator:**

```
./IBMIM -skipInstall user_home/var/temp/imRegistry
  -keyring user_home/var/IM/im.keyring
  -record user_home/var/temp/keyring_response_file.xml
```

3) When a window opens that requests your credentials for the authenticated remote repository, enter the correct credentials and **save** them.

4) Click **File > Exit** to close Installation Manager.

For more information, read the IBM Installation Manager Information Center.

2. **Use the response files to install the WebSphere Customization Toolbox silently:**

   a. Optional: **Use the response file to install the keyring silently:** Go to a command line on each of the systems on which you want to install the WebSphere Customization Toolbox, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and install the keyring silently.

   For example:

   - **Windows administrator or non-administrator:**

```
imcl.exe -acceptLicense
  input C:\temp\keyring_response_file.xml
  -log C:\temp\keyring_log.xml
```

   - **AIX, HP-UX, Linux, or Solaris administrator:**

```
./imcl -acceptLicense
  input /var/temp/keyring_response_file.xml
  -log /var/temp/keyring_log.xml
```

   - **AIX, HP-UX, Linux, or Solaris non-administrator:**

```
./imcl -acceptLicense
  input user_home/var/temp/keyring_response_file.xml
  -log user_home/var/temp/keyring_log.xml
```

   b. **Use the response file to install the WebSphere Customization Toolbox silently:** Go to a command line on each of the systems on which you want to install the WebSphere Customization Toolbox, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and install the WebSphere Customization Toolbox silently.

   For example:

   - **Windows administrator or non-administrator:**

```
imcl.exe -acceptLicense
  input C:\temp\install_response_file.xml
  -log C:\temp\install_log.xml
  -keyring C:\IM\im.keyring
```

   - **AIX, HP-UX, Linux, or Solaris administrator:**

```
./imcl -acceptLicense
  input /var/temp/install_response_file.xml
  -log /var/temp/install_log.xml
  -keyring /var/IM/im.keyring
```

   - **AIX, HP-UX, Linux, or Solaris non-administrator:**

```
./imcl -acceptLicense
  input user_home/var/temp/install_response_file.xml
  -log user_home/var/temp/install_log.xml
  -keyring user_home/var/IM/im.keyring
```

Notes:

- The relevant terms and conditions, notices, and other information are provided in the license-agreement files in the `lafiles` or *product_name*/`lafiles` subdirectory of the installation image or repository for this product.
- The program might write important post-installation instructions to standard output.

Read the IBM Installation Manager Information Center for more information.

Example

The following is an example of a response file for silently installing all of the WebSphere Customization Toolbox.

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright ######################################################
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2011.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
####################################################################### -->

<!-- ##### Frequently Asked Questions #####################################
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
#     Installation Manager Information Center can be found at:
#     http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
#   Windows = IBMIM.exe -record c:\temp\responsefiles\WASv8.install.Win32.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#   Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv8.install.RHEL64.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse\tools subdirectory in the directory where you installed
# Installation Manager:
#
#   Windows = imcl.exe -acceptLicense -showProgress
#        input <response_file_path_and_name> -log <log_file_path_and_name>
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#        input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
#   Windows = imcl.exe -acceptLicense -showProgress
#        input c:\temp\responsefile\WASv8.install.Win32.xml
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input /home/user/responsefile/WASv8.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
#     license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help:  IBMIM -help
#
# Question 3. How do I store and pass credentials to repositories that
# require authentication?
# Answer 3. Installation Manager uses a key ring file to store encrypted
# credentials for authenticating with repositories. Follow this two-step
# process for creating and using a key ring file with Installation Manager.
#
# First, create a key ring file with your credentials by starting
# Installation Manager from the command line under eclipse subdirectory
# with the keyring parameter.
# Use the optional password parameter to password protect your file.
#
#   Windows = IBMIM.exe -keyring <path and file name> -password <password>
#   Linux, UNIX, IBM i and z/OS = ./IBMIM -keyring <path and file name>
#                                 -password <password>
#
# Installation Manager will start in graphical mode. Verify that the
# repositories to which you need to authenticate are included in the
# preferences, File / Preferences / Repositories. If they are not
# listed, then click Add Repositories to add the URL or UNC path.
# Installation Manager will prompt for your credentials. If the repository
# is already in the list, then any attempt to access the repository location,
# such as clicking the Test Connections button, will also prompt for your
# credentials. Enter the correct credential and check the Save password
# checkbox. The credentials are saved to the key ring file you specified.
#
# Second, when you start a silent installation, run imcl under eclipse/tools
# subdirectory, and provide Installation Manager with the location of the key
# ring file and the password if the file is protected. For example:
#
#   Windows = imcl.exe -acceptLicense -showProgress
#     input <path and file name of response file>
#     -keyring <path and name of key ring file> -password <password>
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input <path and file name of response file>
#     -keyring <path and name of key ring file> -password <password>
#
####################################################################### -->

<!-- ##### Agent Input ##############################################
#
# Note that the "acceptLicense" attribute has been deprecated.
# Use "-acceptLicense" command line option to accept license agreements.
#
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the installation finishes.
#
# Valid values for clean:
#      true = only use the repositories and other preferences that are
#           specified in the response file.
#      false = use the repositories and other preferences that are
#           specified in the response file and Installation Manager.
#
# Valid values for temporary:
#      true = repositories and other preferences specified in the
#           response file do not persist in Installation Manager.
#      false = repositories and other preferences specified in the
#           response file persist in Installation Manager.
#
####################################################################### -->

<agent-input clean="true" temporary="true">

<!-- ##### Repositories ###################################################
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#
####################################################################### -->

<server>
    <!-- ##### IBM WebSphere Live Update Repositories ####################
     # These repositories contain WebSphere Customization Toolbox offerings,
     # and updates for those offerings
     #
     # To use the secure repository (https), you must have an IBM ID,
     # which can be obtained by registering at: http://www.ibm.com/account
     # or your Passport Advantage account.
     #
     # And, you must use a key ring file with your response file.
     ################################################################## -->
<repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.WCT.v80" />
    <!-- <repository location="https://www.ibm.com/software/rational/repositorymanager/repositories/websphere" /> -->

    <!-- ##### Custom Repositories #######################################
     # Uncomment and update the repository location key below
     # to specify URLs or UNC paths to any intranet repositories
     # and directory paths to local repositories to use.
     ################################################################## -->
    <!-- <repository location='https:\\w3.mycompany.com\repositories\'/> -->
    <!-- <repository location='/home/user/repositories/websphere/'/> -->

    <!-- ##### Local Repositories ########################################
     # Uncomment and update the following line when using a local
     # repository located on your own machine to install a
     # WebSphere Customization Toolbox offering.
     ############################################################# -->
    <!-- <repository location='insert the full directory path inside single quotes'/> -->
</server>

<!-- ##### Install Packages ##########################################
#
# Install Command
#
# Use the install command to inform Installation Manager of the
# installation packages to install.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
#    false = indicates not to modify an existing install by adding
#            or removing features.
#    true = indicates to modify an existing install by adding or
#           removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be installed. The offering listed must be present in
# at least one of the repositories listed earlier. The example
# command below contains the offering ID for the WebSphere Customization
# Toolbox.
#
# The version attribute is optional. If a version number is provided,
# then the offering will be installed at the version level specified
# as long as it is available in the repositories. If the version
# attribute is not provided, then the default behavior is to install
# the latest version available in the repositories. The version number
# can be found in the repository.xml file in the repositories.
# For example, <offering ... version='8.0.0.20110617_2222'>.
#
# The profile attribute is required and typically is unique to the
# offering. If modifying or updating an existing installation, the
# profile attribute must match the profile ID of the targeted installation
# of WebSphere Customization Toolbox.
#
# The features attribute is optional. Offerings always have at least
# one feature; a required core feature which is installed regardless
# of whether it is explicitly specified. If other feature names
# are provided, then only those features will be installed.
# Features must be comma delimited without spaces.
#
# The feature values for WebSphere Customization Toolbox include:
#  pct,zpmt,zmmt
#
# The installFixes attribute indicates whether fixes available in
# repositories are installed with the product. By default, all
# available fixes will be installed with the offering.
#
# Valid values for installFixes:
#      none = do not install available fixes with the offering.
#      recommended = installs all available recommended fixes with the offering.
#      all = installs all available fixes with the offering.
#
# Interim fixes for offerings also can be installed while they
# are being installed by including the offering ID for the interim
# fix and specifying the profile ID. A commented out example is
# provided in the install command below.
#
# Installation Manager supports installing multiple offerings at once.
# Additional offerings can be included in the install command,
# with each offering requiring its own offering ID, version, profile value,
# and feature values.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# The eclipseLocation data key should use the same directory path to
# WebSphere Customization Toolbox as the installationLocation attribute.
#
# Include data keys for product specific profile properties.
#
####################################################################### -->
<install modify='false'>
<offering id='com.ibm.websphere.WCT.v80'
 profile='WebSphere Customization Toolbox V8.0'
 features='core.feature,pct,zpmt,zmmt' installFixes='none'/>
<!-- <offering id='PM12345_WAS80' profile='WebSphere Customization Toolbox V8.0'/> -->

</install>

<profile id='WebSphere Customization Toolbox V8.0'
 installLocation='C:\Program Files\IBM\WebSphere\Toolbox'>
<data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\Toolbox'/>
<data key='user.import.profile' value='false'/>
<data key='user.select.64bit.image,com.ibm.websphere.WCT.v80' value='false'/>
<data key='cic.selector.nl' value='en'/>
</profile>

<!-- ##### Shared Data Location ############################################
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared'/>
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
#     true = store downloaded artifacts in the shared data location
#     false = remove downloaded artifacts from the shared data location
#
######################################################################## -->

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
-->


<!-- ##### Preferences Settings ############################################
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
######################################################################## -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
 -->

</agent-input>
```

Tip: To select the features (tools) that you want to install, add each desired feature in the offering as an entry in a comma-separated list. To install all of the optional features, for example, specify something like this:

```
<offering profile='WebSphere Customization Toolbox V8.0'
  features='core.feature,zpmt,zmmt,pct,installtools' id='com.ibm.websphere.WCT.v80'/>
```

where `zpmt` indicates the Profile Management Tool (z/OS only), `zmmt` indicates the z/OS Migration Management Tool, `pct` indicates the Web Server Plug-ins Configuration Tool, and `installtools` indicates the Remote Installation Tool for IBM i.

Installing and removing tools in the WebSphere Customization Toolbox

You can use Installation Manager to install or remove a tool in the WebSphere Customization Toolbox.

Before you begin

Make sure that your Installation Manager preferences are pointing to the appropriate Web-based or local repositories containing the WebSphere Customization Toolbox.

Important: When you uninstall the Web Server Plug-ins Configuration Tool, the process does not unconfigure existing web server plug-ins configurations. You might want to use the Web Server Plug-ins Configuration Tool to delete any plug-in configurations that you created using the Web Server Plug-ins Configuration Tool before you remove the tool.

About this task

Perform this procedure to use Installation Manager to install or remove a tool in the WebSphere Customization Toolbox.

Note: Like other Installation Manager operations, you can invoke a modification from a silent response file. You can record this response file using the GUI and Installation Manager's record mode, or you can manually create or modify a response file to suit your needs.

Procedure

1. Close the WebSphere Customization Toolbox installation that is being modified.
2. Start Installation Manager.
3. Click **Modify**.
4. Select the package group to modify.
5. Click **Next**.

   Note: If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.
6. Expand **WebSphere Customization Toolbox**.
7. Check the appropriate checkbox to install a tool, or clear the appropriate checkbox to remove a tool if you already have it installed.
   - Web Server Plug-ins Configuration Tool

     The Web Server Plug-ins Configuration Tool configures the web server plug-ins for WebSphere Application Server so that your web server and application server can communicate with each other.
   - Profile Management Tool (z/OS only)

     The Profile Management Tool (z/OS only) creates customized definitions on an Intel-based Windows or Linux operating system that are used to create or augment WebSphere Application Server profiles on z/OS systems. Each customization definition includes a set of customized jobs with associated instructions. The generated jobs must be uploaded to and run on the target z/OS system.

     Restriction: This tool can be installed and run on Intel-based Windows and Linux platforms only.
   - z/OS Migration Management Tool

     The z/OS Migration Management Tool creates migration definitions on an Intel-based Windows or Linux operating system that are used to migrate a WebSphere Application Server for z/OS node. Each migration definition consists of a set of customized migration jobs with associated instructions. The generated migration jobs must be uploaded to and run on the target z/OS system.

Restriction: This tool can be installed and run on Intel-based Windows and Linux platforms only.

- Remote Installation Tool for IBM i

  The iRemoteInstall command that is installed when you select this option allows you to install IBM Installation Manager or a WebSphere Application Server product offering from a Windows workstation to a remote target IBM i system. The iRemoteInstall command is installed into the following directory:

```
wct_root/Remote_Installation_Tool_for_IBM_i
```

  Restriction: This tool can be installed and run on Windows operating systems only.

8. Click **Next**.
9. Review the summary information, and click **Modify**.
   - If the modification is successful, the program displays a message indicating that installation is successful.
   - If the modification is not successful, click **View Log File** to troubleshoot the problem.
10. Click **Finish**.
11. Click **File > Exit** to close Installation Manager.

Example

Like other Installation Manager operations, you can invoke a modification from a silent response file. You can record this response file using the GUI and Installation Manager's record mode, or you can manually create or modify a response file to suit your needs. In the following list, the optional feature offering names are enclosed in parentheses:

- Web Server Plug-ins Configuration Tool (`pct`)
- z/OS Profile Management Tool (`zpmt`)
- z/OS Migration Management Tool (`zmmt`)
- Remote Installation Tool for IBM i (`installtools`)

Here is a response file that modifies an existing WebSphere Customization Toolbox installation:

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright ######################################################
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2011.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
####################################################################### -->

<!-- ##### Frequently Asked Questions #####################################
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
#     Installation Manager Information Center can be found at:
#     http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
#   Windows = IBMIM.exe -record c:\temp\responsefiles\WASv8.install.Win32.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#   Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv8.install.RHEL64.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse\tools subdirectory in the directory where you installed
# Installation Manager:
#
#   Windows = imcl.exe -acceptLicense -showProgress
#     input <response_file_path_and_name> -log <log_file_path_and_name>
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
#   Windows = imcl.exe -acceptLicense -showProgress
#     input c:\temp\responsefile\WASv8.install.Win32.xml
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input /home/user/responsefile/WASv8.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
#     license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help:  IBMIM -help
#
# Question 3. How do I store and pass credentials to repositories that
# require authentication?
# Answer 3. Installation Manager uses a key ring file to store encrypted
# credentials for authenticating with repositories. Follow this two-step
# process for creating and using a key ring file with Installation Manager.
#
# First, create a key ring file with your credentials by starting
# Installation Manager from the command line under eclipse subdirectory
# with the keyring parameter.
# Use the optional password parameter to password protect your file.
#
#   Windows = IBMIM.exe -keyring <path and file name> -password <password>
#   Linux, UNIX, IBM i and z/OS = ./IBMIM -keyring <path and file name>
#                                    -password <password>
#
# Installation Manager will start in graphical mode. Verify that the
# repositories to which you need to authenticate are included in the
# preferences, File / Preferences / Repositories. If they are not
# listed, then click Add Repositories to add the URL or UNC path.
# Installation Manager will prompt for your credentials. If the repository
# is already in the list, then any attempt to access the repository location,
# such as clicking the Test Connections button, will also prompt for your
# credentials. Enter the correct credential and check the Save password
# checkbox. The credentials are saved to the key ring file you specified.
#
# Second, when you start a silent installation, run imcl under eclipse/tools
# subdirectory, and provide Installation Manager with the location of the key
# ring file and the password if the file is protected. For example:
#
#   Windows = imcl.exe -acceptLicense -showProgress
#     input <path and file name of response file>
#     -keyring <path and name of key ring file> -password <password>
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input <path and file name of response file>
#     -keyring <path and name of key ring file> -password <password>
#
####################################################################### -->

<!-- ##### Agent Input ##############################################
#
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the installation finishes.
#
# Valid values for clean:
#      true = only use the repositories and other preferences that are
#           specified in the response file.
#      false = use the repositories and other preferences that are
#           specified in the response file and Installation Manager.
#
# Valid values for temporary:
#      true = repositories and other preferences specified in the
#           response file do not persist in Installation Manager.
#      false = repositories and other preferences specified in the
#           response file persist in Installation Manager.
#
####################################################################### -->

<agent-input clean='true' temporary='true'>

<!-- ##### Repositories ###################################################
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
```

```
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#
######################################################################## -->

<server>
    <!-- ##### IBM WebSphere Live Update Repositories #####################
     # These repositories contain WebSphere Customization Toolbox offerings,
     # and updates for those offerings
     #
     # To use the secure repository (https), you must have an IBM ID,
     # which can be obtained by registering at: http://www.ibm.com/account
     # or your Passport Advantage account.
     #
     # And, you must use a key ring file with your response file.
     ################################################################### -->
    <repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.WCT.v80" />
    <!-- <repository location="https://www.ibm.com/software/rational/repositorymanager/repositories/websphere" /> -->

    <!-- ##### Custom Repositories ########################################
     # Uncomment and update the repository location key below
     # to specify URLs or UNC paths to any intranet repositories
     # and directory paths to local repositories to use.
     ################################################################### -->
    <!-- <repository location='https:\\w3.mycompany.com\repositories\'/> -->
    <!-- <repository location='/home/user/repositories/websphere/'/> -->

    <!-- ##### Local Repositories #########################################
     # Uncomment and update the following line when using a local
     # repository located on your own machine to install a
     # WebSphere Customization Toolbox offering.
     ############################################################## -->
    <!-- <repository location='insert the full directory path inside single quotes'/> -->
</server>

<!-- ##### Modify Packages ################################################
#
# Install and Uninstall Commands
#
# Use the install and uninstall commands to inform Installation Manager
# of the installation packages to install or uninstall.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
#    false = indicates not to modify an existing install by adding
#            or removing features.
#    true = indicates to modify an existing install by adding or
#           removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be installed. The offering listed must be present in
# at least one of the repositories listed earlier. The example
# command below contains the offering ID for WebSphere Customization Toolbox.
#
# The version attribute is optional. If a version number is provided,
# then the offering will be installed or uninstalled at the version level
# specified as long as it is available in the repositories. If the version
# attribute is not provided, then the default behavior is to install or
# uninstall the latest version available in the repositories. The version
# number can be found in the repository.xml file in the repositories.
# For example, <offering ... version='8.0.0.20110617_2222'>.
#
# The profile attribute is required and typically is unique to the
# offering. If modifying or updating an existing installation, the
# profile attribute must match the profile ID of the targeted installation
# of WebSphere Customization Toolbox.
#
# The features attribute is optional. Offerings always have at least
# one feature; a required core feature which is installed regardless
# of whether it is explicitly specified. If other feature names
# are provided, then only those features will be installed.
# Features must be comma delimited without spaces.
#
# The feature values for WebSphere Customization Toolbox include:
#  pct,zpmt,zmmt
#
# In the example that follows, the zpmt,zmmt features are being removed
# from the specified offering.
#
# The core.feature can not be removed because they are required features.
#
# The installFixes attribute indicates whether fixes available in
# repositories are installed with the product. By default, all
# available fixes will be installed with the offering.
#
# Valid values for installFixes:
#      none = do not install available fixes with the offering.
#      recommended = installs all available recommended fixes with the offering.
#      all = installs all available fixes with the offering.
#
# Installation Manager supports modifying multiple offerings at once.
# Additional offerings can be included in the install and uninstall commands,
# with each offering requiring its own offering ID, version, profile value,
# and feature values.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# The eclipseLocation data key should use the same directory path to
# WebSphere Customization Toolbox as the installationLocation attribute.
#
# Include data keys for product specific profile properties.
#
####################################################################### -->

<uninstall modify='true'>
<offering id='com.ibm.websphere.WCT.v80'
 profile='WebSphere Customization Toolbox V8.0'
 features='zmmt,zpmt'/>
</uninstall>

<profile id='WebSphere Customization Toolbox V8.0'
 installLocation='C:\Program Files\IBM\WebSphere\Toolbox'>
<data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\Toolbox'/>
<data key='user.import.profile' value='false'/>
<data key='user.select.64bit.image,com.ibm.websphere.WCT.v80' value='false'/>
<data key='cic.selector.nl' value='en'/>
</profile>

<!-- ##### Shared Data Location ###########################################
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared'/>
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
#     true = store downloaded artifacts in the shared data location
#     false = remove downloaded artifacts from the shared data location
#
####################################################################### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
-->

<!-- ##### Preferences Settings ###########################################
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
```

```
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
################################################################## -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
 -->

</agent-input>
```

Updating the WebSphere Customization Toolbox

You can use Installation Manager to update the WebSphere Customization Toolbox to a later version.

Before you begin

Make sure that your Installation Manager preferences are pointing to Web-based or local repositories that contain the appropriate updates for the WebSphere Customization Toolbox.

About this task

Perform this procedure to use Installation Manager to update the WebSphere Customization Toolbox.

Procedure

1. Start Installation Manager.
2. Click **Update**.
3. Select the package group to update.
4. Click **Next**.

   Note: If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.
5. Select the version to which you want to update under **WebSphere Customization Toolbox**.
6. Click **Next**.
7. Accept the terms in the license agreements, and click **Next**.
8. Review the summary information, and click **Update**.
   - If the installation is successful, the program displays a message indicating that installation is successful.
   - If the installation is not successful, click **View Log File** to troubleshoot the problem.
9. Click **Finish**.
10. Click **File > Exit** to close Installation Manager.

Rolling back the WebSphere Customization Toolbox

You can use Installation Manager to roll back the WebSphere Customization Toolbox to an earlier version.

Before you begin

Make sure that your Installation Manager preferences are pointing to Web-based or local repositories that contain the appropriate earlier version of the WebSphere Customization Toolbox.

About this task

Perform this procedure to use Installation Manager to roll back the WebSphere Customization Toolbox to an earlier version.

Procedure

1. Start Installation Manager.
2. Click **Roll Back**.
3. Select the package group to roll back.
4. Click **Next**.

   Note: If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.
5. Select the version to which you want to roll back under **WebSphere Customization Toolbox**.
6. Click **Next**.
7. Review the summary information, and click **Roll Back**.
   - If the roll back is successful, the program displays a message indicating that the roll back is successful.
   - If the roll back is not successful, click **View Log File** to troubleshoot the problem.
8. Click **Finish**.
9. Click **File > Exit** to close Installation Manager.

Uninstalling the WebSphere Customization Toolbox using the GUI

Use the Installation Manager GUI to uninstall the WebSphere Customization Toolbox.

Before you begin

Important: When you uninstall the Web Server Plug-ins Configuration Tool, the process does not unconfigure existing web server plug-ins configurations. You might want to use the Web Server Plug-ins Configuration Tool to delete any plug-in configurations that you created using the Web Server Plug-ins Configuration Tool before you remove the WebSphere Customization Toolbox.

If you do not unconfigure existing web server plug-ins that were configured using the Web Server Plug-ins Configuration Tool before uninstalling the WebSphere Customization Toolbox, the configuration information remains. If the WebSphere Customization Toolbox is reinstalled, the configuration information that displays in the Web Server Plug-ins Configuration Tool might be obsolete and greyed out, preventing you from interacting properly with the Web Server Plug-ins Configuration Tool. To resolve this problem, manually remove the workspace used by the previous WebSphere Customization Toolbox installation. The workspace is in the following location:

- `user_home/AppData/Local/IBM/WebSphere/workspaces/WCT8`
- `user_home/.ibm/WebSphere/workspaces/WCT8`

Procedure

1. Start Installation Manager.
2. Click **Uninstall**.

3. In the **Uninstall Packages** window, perform the following actions.
   a. Select **WebSphere Customization Toolbox** and the appropriate version.

      Note: If you are uninstalling the ILAN version of this product, select **WebSphere Customization Toolbox (ILAN)**.
   b. Click **Next**.
4. Review the summary information.
5. Click **Uninstall**.
   - If the uninstallation is successful, the program displays a message that indicates success.
   - If the uninstallation is not successful, click **View log** to troubleshoot the problem.
6. Click **Finish**.
7. Click **File > Exit** to close Installation Manager.

Uninstalling the WebSphere Customization Toolbox silently

You can use Installation Manager to uninstall the WebSphere Customization Toolbox silently.

Before you begin

Important: When you uninstall the Web Server Plug-ins Configuration Tool, the process does not unconfigure existing web server plug-ins configurations. You might want to use the Web Server Plug-ins Configuration Tool to delete any plug-in configurations that you created using the Web Server Plug-ins Configuration Tool before you remove the WebSphere Customization Toolbox.

If you do not unconfigure existing web server plug-ins that were configured using the Web Server Plug-ins Configuration Tool before uninstalling the WebSphere Customization Toolbox, the configuration information remains. If the WebSphere Customization Toolbox is reinstalled, the configuration information that displays in the Web Server Plug-ins Configuration Tool might be obsolete and greyed out, preventing you from interacting properly with the Web Server Plug-ins Configuration Tool. To resolve this problem, manually remove the workspace used by the previous WebSphere Customization Toolbox installation. The workspace is in the following location:

- `user_home/AppData/Local/IBM/WebSphere/workspaces/WCT8`
- `user_home/.ibm/WebSphere/workspaces/WCT8`

Optional: Perform or record the installation of Installation Manager and installation of the WebSphere Customization Toolbox to a temporary installation registry on one of your systems so that you can use this temporary registry to record the uninstallation without using the standard registry where Installation Manager is installed.

Read the following for more information:

- "Installing the WebSphere Customization Toolbox using the GUI" on page 261
- "Installing the WebSphere Customization Toolbox silently" on page 265

About this task

Using Installation Manager, you can work with response files to uninstall the WebSphere Customization Toolbox silently in a variety of ways. You can record a response file using the GUI as described in the following procedure, or you can generate a new response file by hand or by taking an example and modifying it.

Procedure

1. Optional: **Record a response file to uninstall the WebSphere Customization Toolbox:** On one of your systems, perform the following actions to record a response file that will uninstall the WebSphere Customization Toolbox:
   a. From a command line, change to the eclipse subdirectory in the directory where you installed Installation Manager.
   b. Start Installation Manager from the command line using the -record option.

      For example:

      - **Windows administrator or non-administrator:**

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"
  -record C:\temp\uninstall_response_file.xml
```

      - **AIX, HP-UX, Linux, or Solaris administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry
  -record /var/temp/uninstall_response_file.xml
```

      - **AIX, HP-UX, Linux, or Solaris non-administrator:**

```
./IBMIM -skipInstall user_home/var/temp/imRegistry
  -record user_home/var/temp/uninstall_response_file.xml
```

      Tip: If you choose to use the -skipInstall parameter with a temporary installation registry created as described in "Before you begin," Installation Manager uses the temporary installation registry while recording the response file. It is important to note that when the -skipInstall parameter is specified, no packages are installed or uninstalled. All of the actions that you perform in Installation Manager simply update the installation data that is stored in the specified temporary registry. After the response file is generated, it can be used to uninstall the WebSphere Customization Toolbox, removing the WebSphere Customization Toolbox files and updating the standard installation registry.

      The -skipInstall operation should not be used on the actual agent data location used by Installation Manager This is unsupported. Use a clean writable location, and re-use that location for future recording sessions.

      For more information, read the IBM Installation Manager Information Center.
   c. Click **Uninstall**.
   d. In the **Uninstall Packages** window, perform the following actions.
      1) Select **WebSphere Customization Toolbox** and the appropriate version.

         Note: If you are uninstalling the ILAN version of this product, select **WebSphere Customization Toolbox (ILAN)**.
      2) Click **Next**.
   e. Review the summary information.
   f. Click **Uninstall**.
      - If the uninstallation is successful, the program displays a message that indicates success.
      - If the uninstallation is not successful, click **View log** to troubleshoot the problem.
   g. Click **Finish**.
   h. Click **File > Exit** to close Installation Manager.
2. **Use the response file to uninstall the WebSphere Customization Toolbox silently:** From a command line on each of the systems from which you want to uninstall the WebSphere Customization Toolbox, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager and use the response file that you created to silently uninstall the WebSphere Customization Toolbox.

   For example:

   - **Windows administrator or non-administrator:**

```
imcl.exe
  input C:\temp\uninstall_response_file.xml
  -log C:\temp\uninstall_log.xml
```

- **AIX, HP-UX, Linux, or Solaris administrator:**

```
./imcl
  input /var/temp/uninstall_response_file.xml
  -log /var/temp/uninstall_log.xml
```

- **AIX, HP-UX, Linux, or Solaris non-administrator:**

```
./imcl
  input user_home/var/temp/uninstall_response_file.xml
  -log user_home/var/temp/uninstall_log.xml
```

Go to the IBM Installation Manager Information Center for more information.

Example

The following is an example of a response file for silently uninstalling the WebSphere Customization Toolbox.

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright #######################################################
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2011.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
######################################################################## -->

<!-- ##### Frequently Asked Questions ######################################
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
#     Installation Manager Information Center can be found at:
#     http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
#   Windows = IBMIM.exe -record c:\temp\responsefiles\WASv8.install.Win32.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#   Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv8.install.RHEL64.xml
#     -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse\tools subdirectory in the directory where you installed
# Installation Manager:
#
#   Windows = imcl.exe -acceptLicense -showProgress
#     input <response_file_path_and_name> -log <log_file_path_and_name>
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
#   Windows = imcl.exe -acceptLicense -showProgress
#     input c:\temp\responsefile\WASv8.install.Win32.xml
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#     input /home/user/responsefile/WASv8.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
#     license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help:  IBMIM -help
#
######################################################################## -->

<!-- ##### Agent Input ##############################################
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the uninstall finishes.
#
```

```
# Valid values for clean:
#      true = only use the repositories and other preferences that are
#           specified in the response file.
#      false = use the repositories and other preferences that are
#           specified in the response file and Installation Manager.
#
# Valid values for temporary:
#      true = repositories and other preferences specified in the
#           response file do not persist in Installation Manager.
#      false = repositories and other preferences specified in the
#           response file persist in Installation Manager.
#
####################################################################### -->

<agent-input clean='true' temporary='true'>

<!-- ##### Repositories ###################################################
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#
####################################################################### -->

<server>
    <!-- ##### IBM WebSphere Live Update Repositories ###################
     # These repositories contain WebSphere Customization Toolbox offerings,
     # and updates for those offerings
     #
     # To use the secure repository (https), you must have an IBM ID,
     # which can be obtained by registering at: http://www.ibm.com/account
     # or your Passport Advantage account.
     #
     # And, you must use a key ring file with your response file.
     ################################################################## -->
    <repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.WCT.v80" />
    <!-- <repository location="https://www.ibm.com/software/rational/repositorymanager/repositories/websphere" /> -->

    <!-- ##### Custom Repositories #######################################
     # Uncomment and update the repository location key below
     # to specify URLs or UNC paths to any intranet repositories
     # and directory paths to local repositories to use.
     ################################################################## -->
    <!-- <repository location='https:\\w3.mycompany.com\repositories\'/> -->
    <!-- <repository location='/home/user/repositories/websphere/'/> -->

    <!-- ##### Local Repositories ########################################
     # Uncomment and update the following line when using a local
     # repository located on your own machine to install a
     # WebSphere Customization Toolbox offering.
     ############################################################# -->
    <!-- <repository location='insert the full directory path inside single quotes'/> -->
</server>

<!-- ##### Uninstall Packages ############################################
#
# Uninstall Command
#
# Use the uninstall command to inform Installation Manager of the
# installation packages to uninstall.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
#    false = indicates not to modify an existing install by adding
#            or removing features.
#    true = indicates to modify an existing install by adding or
#           removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be uninstalled. The example command below contains the
# offering ID for WebSphere Customization Toolbox.
#
# The version attribute is optional. If a version number is provided,
# then the offering will be uninstalled at the version level specified
# If the version attribute is not provided, then the default behavior is
# to uninstall the latest version. The version number can be found in
# the repository.xml file in the repositories.
# For example, <offering ... version='8.0.0.20110617_2222'>.
#
# The profile attribute is required and must match the package group
# name for the offering to be uninstalled.
#
# The features attribute is optional. If there is no feature attribute,
# then all features are uninstalled. If features are specified, then
# only those features will be uninstalled.
# Features must be comma delimited without spaces.
#
# The feature values for WebSphere Customization Toolbox include:
#  pct,zpmt,zmmt
#
# Installation Manager supports uninstalling multiple offerings at once.
# Additional offerings can be included in the uninstall command,
# with each offering requiring its own offering ID, version, profile value,
# and feature values.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# The eclipseLocation data key should use the same directory path to
# WebSphere Customization Toolbox as the installationLocation attribute.
#
# Include data keys for product specific profile properties.
#
########################################################################## -->

<uninstall modify='false'>
<offering id='com.ibm.websphere.WCT.v80'
 profile='WebSphere Customization Toolbox V8.0'
 features='core.feature,pct,zpmt,zmmt'/>
</uninstall>

<profile id='WebSphere Customization Toolbox V8.0'
 installLocation='C:\Program Files\IBM\WebSphere\Toolbox'>
<data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\Toolbox'/>
<data key='user.import.profile' value='false'/>
<data key='user.select.64bit.image,com.ibm.websphere.WCT.v80' value='false'/>
<data key='cic.selector.nl' value='en'/>
</profile>

<!-- ##### Shared Data Location ##########################################
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared'/>
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
#     true = store downloaded artifacts in the shared data location
#     false = remove downloaded artifacts from the shared data location
#
########################################################################## -->

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
```

```
-->

<!-- ##### Preferences Settings ###########################################
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r4/index.jsp
#
####################################################################### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
 -->

</agent-input>
```

Using the wct command-line utility

The wct command-line utility invokes the command-line tool that is specified by the -tool parameter.

Procedure

Invoke the command-line tool that is specified by the -tool parameter.

Location of the utility

The product includes the following script that sets up the environment and invokes the wct command-line utility.

- Windows *WCT_install_root*\WCT\wctcmd.bat
- Linux *WCT_install_root*/WCT/wctcmd.sh

Syntax

Windows

```
wctcmd.bat
      -tool tool_ID
      -defLocPathname definition_location_pathname
      -createDefinitionLocation definition_location_name
      -importDefinitionLocation definition_location_name
      -removeDefinitionLocation definition_location_name
      -defLocName definition_location_name
      -defLocVersion definition_location_version
      -response response_file
      -listDefinitionLocations
      -deleteDefinition definition_name
      -listDefinitions
```

Linux

```
./wctcmd.sh
      -tool tool_ID
      -defLocPathname definition_location_pathname
      -createDefinitionLocation definition_location_name
      -importDefinitionLocation definition_location_name
      -removeDefinitionLocation definition_location_name
      -defLocName definition_location_name
      -defLocVersion definition_location_version
```

```
-response response_file
-listDefinitionLocations
-deleteDefinition definition_name
-listDefinitions
```

Parameters

-tool *tool_ID*
Specifies the name of the tool to launch as it is registered with the WCT command-line utility

This parameter is required.

-defLocPathname *definition_location_pathname*
Specifies the absolute path name of the definition location to use when the specified tool is launched

This parameter is required.

-createDefinitionLocation *definition_location_name*
Specifies that the WCT command-line utility should create a definition location

This parameter is optional.

-importDefinitionLocation *definition_location_name*
Specifies that the WCT command-line utility should import a definition location

This parameter is optional.

-removeDefinitionLocation *definition_location_name*
Specifies that the WCT command-line utility should remove a definition location

This parameter is optional.

-defLocName *definition_location_name*
Specifies the name of the definition location as it resides in the definition location registry

-defLocVersion *definition_location_version*
Specifies the version of definition location to create

This parameter is optional.

-response *response_file*
Specifies the response file containing tool arguments

This parameter is optional.

-listDefinitionLocations
Lists the available definition locations.

-deleteDefinition *definition_name*
Specifies that the WCT command-line utility should delete a definition

This parameter is optional.

The *definition_name* is required. Either one of the following parameters is also required:

- `-defLocName` *`definition_location_name`*
- `-defLocpathname` *`definition_location_pathname`*

If both parameter values are supplied, the first one is used. If the first value supplied does not pass the validation check, the command fails with an error message.

-listDefinitions
Lists the available definitions at a specified definition location or definition location path name

Either one of the following parameters is required:

- `-defLocName` *`definition_location_name`*

- `-defLocpathname` *`definition_location_pathname`*

If both parameter values are supplied, the first one is used. If the first value supplied does not pass the validation check, the command fails with an error message.

Notes:

- Command-line arguments are case sensitive.
- If an argument accepts a value containing spaces, the value must be enclosed in double quotes (" ").

Examples

Importing a definition location for the pct tool:

Windows

```
wctcmd.bat -tool pct -importDefinitionLocation -defLocName someDefLocName -defLocPathname \data\IBM\WebSphere\Plugins
  -response C:\IBM\WebSphere\Toolbox\WCT\responsefile.txt
```

Linux

```
./wctcmd.sh -tool pct -importDefinitionLocation -defLocName someDefLocName -defLocPathname /data/IBM/WebSphere/Plugins
  -response /var/IBM/WebSphere/Toolbox/WCT/responsefile.txt
```

Removing a definition location for the pct tool:

Windows

```
wctcmd.bat -tool pct -removeDefinitionLocation -defLocName someDefLocName -defLocPathname \data\IBM\WebSphere\Plugins
```

Linux

```
./wctcmd.sh -tool pct -removeDefinitionLocation -defLocName someDefLocName -defLocPathname /data/IBM/WebSphere/Plugins
```

Listing the available definition locations for the pct tool:

Windows

```
wctcmd.bat -tool pct -defLocPathname \data\IBM\WebSphere\Plugins -listDefinitionLocations
```

Linux

```
./wctcmd.sh -tool pct -defLocPathname /data/IBM/WebSphere/Plugins -listDefinitionLocations
```

Notes:

- Command-line arguments are case sensitive.
- If an argument accepts a parameter containing spaces, the parameter must be enclosed in "double quotes".

Chapter 10. Centralized installation manager (CIM)

Use the centralized installation manager (CIM) to shorten the number of steps that are required to create and manage environments that contain WebSphere Application Server Version 6.1.x, 7.x and 8.0.

Before you begin

The process for managing Version 7.0 and previous versions is different from the process for managing Version 8.0. The following topic explains the different CIM usage scenarios.

About this task

Note: The Version 8.0 Centralized Installation Manager (CIM) can be used to manage Version 8.0 and previous versions of WebSphere Application Server. You can use CIM to install or uninstall Version 8.0 and previous versions of WebSphere Application Server on remote machines and apply maintenance from the administrative console. In Version 8.0, targets can now be added outside of the cell. The process for managing Version 7.0 and previous versions is different from the process for managing Version 8.0, and each process is documented separately in the information center.

Note: The process for managing the centralized installation manager (CIM) for WebSphere Application Server Version 6.1.x and 7.x is different from the process for managing Version 8.0, and each process is documented separately in the information center. For Version 8.0, CIM uses the Installation Manager to install the product on remote machines. For Version 6.1.x and 7.x, CIM uses the ISMP and Update Installer.

- To get started using CIM for Version 8.0, see “Submitting Installation Manager jobs” on page 292
- To get started using CIM for Version 6.1.x and 7.0*, see Getting started with the centralized installation manager (CIM) for previous versions.

  *(Not supported on z/OS targets.)

Table 37. Differences between CIM for Version 8.0 and CIM for Version 6.1.x and 7.x

Function	CIM Version 6.1.x and 7.x	CIM Version 8.0
Scope	Install, update, uninstall Version 7.x. Update Version 6.1.x* *(Not supported on z/OS targets.)	Install, update, uninstall Version 8.0 and all Installation Manager installable products: WebSphere Application Server, IHS Plugin, and DMZ. Targets can now be added outside of the cell.
Installation software used	ISMP and Update Installer	Installation Manager
Repository	Maintains a private repository on the Deployment Manager	Maintains an installation kit directory. Uses Installation Manager repository
Administrative console	Accessible from the Deployment Manager	Accessible from the Job Manager. Job Manager is also available on the Deployment Manager
Command line	CIM AdminTask commands	Use the Job Manager's submitJob command

Procedure

1. For Version 8.0, CIM functions are accessed through the job manager or deployment manager. Using the job manager or deployment manager, you can perform the following functions:
   - Install, update, and uninstall IBM® Installation Manager on remote machines*
   - Install, update, and uninstall WebSphere Application Server Version 8.0 offerings on remote machines
   - Collect, distribute, and delete files on remote hosts
   - Run scripts on remote hosts
   - Manage profiles on remote hosts for WebSphere Application Server*

   *(Not supported on z/OS targets.)

Version 8.0 CIM offers the following improvements over previous versions:

- Support for z/OS operating system targets
- Removal of cell boundary limitations. Targets can now be added outside of the cell.
- Job scheduling

2. For Version 6.1.x and 7.0, CIM functions are accessed using the deployment manager. CIM functions with Version 6.1.x and 7.0 are not supported for z/OS operating system targets. Using the deployment manager, you can perform the following functions:
   - Install, update, and uninstall WebSphere Application Server Network Deployment Version 7.x on remote machines
   - Install and uninstall WebSphere Application Server Version 6.1.x and 7.x refresh packs, fix packs, and interim fixes on remote machines

Submitting Installation Manager jobs

In a flexible management environment, you can submit jobs to install Installation Manager instances, update Installation Manager with a repository (not supported on z/OS targets), manage Installation Manager offerings, and install WebSphere Application Server Version 8.0 products.

Before you begin

Note: This topic applies to WebSphere Application Server Version 8.0 only.

Start the job manager and make a remote host a target of the job manager. In the job manager console or deployment manager console, click **Jobs** > **Targets** > **New Host** and complete the fields on the New targets page.

A remote host typically is a different computer than the one on which the job manager is installed.

To submit jobs, your ID at the job manager must be authorized for the administrator role or the operator role. When you submit a job, you can specify a user name and password for authentication and authorization at the target or targets. When you submit a job to multiple targets, the user name and password or the credentials for the submitter must be applicable to all of the job targets.

Note: For Version 8.0, centralized installation manager (CIM) functions are accessed through the job manager. Using the job manager, you can perform the following functions:

- Install, update, and uninstall WebSphere Application Server offerings on remote machines
- Install, update, and uninstall IBM Installation Manager on remote machines. Not supported on z/OS targets. For z/OS targets, you must install Installation Manager prior to working with CIM.
- Collect, distribute, and delete files on remote hosts
- Run scripts on remote hosts

The Centralized Installation Manager (CIM) can be used to manage Version 6.x and 7.x of WebSphere Application Server. You can use CIM to install or uninstall previous versions of WebSphere Application Server on remote machines and apply maintenance from the administrative console. The process for managing Version 6.x and 7.x is different from the process for managing Version 8.0, which is managed through the job manager.

Table 38. Differences between CIM for Version 8.0 and CIM for Versions 6.x and 7.x. Shows how CIM functions differ among product versions.

Function	CIM Version 6.x and 7.x	CIM Version 8.0
Scope	Install, update, uninstall Version 7.x. Update Version 6.x.	Install, update, uninstall Version 8.0 and all Installation Manager installable products

Table 38. Differences between CIM for Version 8.0 and CIM for Versions 6.x and 7.x (continued). Shows how CIM functions differ among product versions.

Function	CIM Version 6.x and 7.x	CIM Version 8.0
Installation software used	ISMP and Update Installer	Installation Manager
Repository	Maintains a private repository on the deployment manager	Maintains an installation kit directory. Uses an Installation Manager repository.
Administrative console	Accessible from the deployment manager	Accessible from the job manager. The job manager is also available on the deployment manager.
Command line	CIM AdminTask commands	Use the job manager submitJob command.

Note: IBM Installation Manager 1.4.3 or above is required.

About this task

You can use the Installation Manager to install and manage installations on remote hosts. Using the job manager, you can run jobs that create and update Installation Manager instances and install the product on remote hosts.

The topics in this section describe how to use the Installation Manager by running jobs in the job manager console or the deployment manager console. Instead of using a console, you can run wsadmin commands in the AdministrativeJobs command group. See the Administrative job types topic.

Procedure

- Run the install Installation Manager job.
- Run the update Installation Manager job.
- Run the uninstall Installation Manager job.
- Run the install SSH public key job.
- Manage your Installation Manager install kits.

What to do next

On the Job status page, click the ID of the job and view the job status. If the job is not successful, view any error messages that result from running the job, correct the error condition, and submit the job again.

To review the Installation Manager license, perform the following steps:

- If you are using the graphical user interface (GUI), run the following command and follow the instructions:
  - AIX HP-UX Solaris install
  - Windows install.exe
- If you are using the command line, run the following command and follow the instructions:
  - AIX HP-UX Solaris installc -c
  - Windows installc.exe -c

Submitting jobs to install Installation Manager on remote hosts

In a flexible management environment, you can submit the **Install IBM Installation Manager** job to install the Installation Manager on registered hosts of the job manager.

Before you begin

Start the job manager and the targets. Ensure that the targets for which you want to install Installation Manager are registered with the job manager.

To submit jobs, your ID at the job manager must be authorized for the administrator role or the operator role. When you submit a job, you can specify a user name and password for authentication and authorization at the target or targets. When you submit a job to multiple targets, the user name and password or the credentials for the submitter must apply to all of the job targets.

To run the job against a large number of targets, optionally create a group of targets and submit the job against the group.

For instructions on updating an existing instance of Installation Manager, see Submitting jobs to update Installation Manager on remote hosts.

About this task

You can use the administrative console of the job manager or the deployment manager to submit the job. From the console, choose the **Install IBM Installation Manager** job, specify the targets, schedule the job, review the summary, and submit the job.

Instead of using a console, you can run the installIM job script in the AdministrativeJobs command group. See the Administrative job types topic.

For Windows targets, CIM sends unzip.exe to the target to unzip the Installation Manager zip file. If you do not want to use unzip.exe from CIM, you can set the JVM parameter:

```
com.ibm.ws.admin.cimjm.unzipOnTheFly=true/TRUE"
```

If this parameter is set to "true", CIM unzips the zip file from the job manager and sends individual files to the target. You must restart the server after changing this parameter.

For Linux/UNIX targets, if CIM detects an instance of unzip, CIM sends the zip file to the target and then unzips the zip file. If CIM does not detect an instance of unzip, CIM unzips the zip file from the job manager and sends individual files to the target. Sending the files individually usually requires more time than unzipping on the target. For IBM i targets, CIM uses the jar command found on the IBM i target to unzip the zip file.

After the centralized installation manager successfully completes the installation process on a remote node, it then deletes the installation image files that are located in the temporary location that you specify during the installation process. If the installation is unsuccessful, the files remain in the temporary location for you to use to determine what caused the installation error. However, you can safely delete the files.

Note: IBM Installation Manager 1.4.3 or above is required.

Procedure

1. Click **Jobs** > **Submit** from the navigation tree of the administrative console.
2. Choose the **Install IBM Installation Manager** job and click **Next**.
3. Choose job targets.
   a. Select a group of targets from the list, or select **Target names**.
   b. If you selected **Target names**, then specify a target name and click **Add**, or click **Find** and specify the chosen targets on the Find targets page.
   c. If user authentication is required, specify a user name, password, or any other authentication values as needed.

   d. Click **Next**.

4. On the Specify the job parameters page, specify the location of the Installation Manager instance that you want to install.

   Note: If you do not specify the IBM Installation Manager installation kit path, the installIM job searches for the most recent IBM Installation Manager installation kit that is suitable for the target platform from the installation kit repository on the Job Manager. By default, the installation kit repository is `<profile_home>/IMKits`. You can change the location from the Job Manager. Click **Jobs** > **Installation Manager installation kits**, then modify 'Installation Manager installation kits location' to a different location. If you are using the command line, you can check for the repository location at: `<profile_home>/properties/cimjm/CIMJMMetadata.xml`.

   Optional parameters:

   - Installation Manager agent data location: specifies the location of the Installation Manager agent data.

     Note: The data location cannot be a subdirectory of the installation location.
   - Installation Manager installation directory: specifies the location of the Installation Manager installation directory.

   If you select the **Skip prerequisite checking** check box, you specify that no prerequisite checking is performed when installing Installation Manager and that Installation Manager disk space checking is disabled.For the job to run successfully, you must select **I accept the terms in the license agreements**. Click **Next**

   To review the Installation Manager license, perform the following steps:

   Note: Run the install command from the Installation Manager install kit.

   - If you are using the graphical user interface (GUI), run the following command and follow the instructions:
     - AIX HP-UX Solaris install
     - Windows install.exe
   - If you are using the command line, run the following command and follow the instructions:
     - AIX HP-UX Solaris installc -c
     - Windows installc.exe -c

   Note: You can install Installation Manager so that it can be used by a group of users. Specify the following optional parameter: **installType**

   Values:

   - AIX Solaris Linux HP-UX group: specify a group installation of Installation Manager. If the target is not one of the supported operating system types, the job will fail.
   - single: perform a single user installation in non administrative mode. This option is available for all CIM supported platforms.
   - Auto: the command initiates a single user installation in non administrative mode if your are a non administrative user. If you are an administrator, this action performs an administrative installation.

5. Schedule the job, and click **Next**.
6. Review the summary, and click **Finish** to submit the job.

Results

The job runs and installs Installation Manager on the selected targets.

What to do next

On the Job status page, click the job ID and view the job status. Click the status refresh icon ⟳ to refresh the displayed job status.

If the job is not successful, view any error messages that result from running the job, correct the error condition, and submit the job again.

Submitting jobs to update Installation Manager on remote hosts for Version 8.0

In a flexible management environment, you can submit the **Update IBM Installation Manager** job to update the Installation Manager on registered hosts of the job manager.

Before you begin

Start the job manager and the targets. Ensure that the targets for which you want to update Installation Manager are registered with the job manager.

To submit jobs, your ID at the job manager must be authorized for the administrator role or the operator role. When you submit a job, you can specify a user name and password for authentication and authorization at the target or targets. When you submit a job to multiple targets, the user name and password or the credentials for the submitter must apply all of the job targets.

To run the job against a large number of targets, optionally create a group of targets and submit the job against the group.

To review the Installation Manager license, perform the following steps:

- If you are using the graphical user interface (GUI), run the following command and follow the instructions:
  - ▶ AIX ▶ HP-UX ▶ Solaris install
  - Windows install.exe
- If you are using the command line, run the following command and follow the instructions:
  - ▶ AIX ▶ HP-UX ▶ Solaris installc -c
  - Windows installc.exe -c

About this task

You can use the administrative console of the job manager or the deployment manager to submit the job. From the console, choose the **Update IBM Installation Manager** job, specify the targets, schedule the job, review the summary, and submit the job.

Instead of using a console, you can run the updateIM job script in the AdministrativeJobs command group. See the Administrative job types topic.

Note: IBM Installation Manager 1.4.3 or above is required.

Procedure

1. Click **Jobs** > **Submit** from the navigation tree of the administrative console.
2. Choose the **Update IBM Installation Manager** job and click **Next**.
3. Choose job targets.
   a. Select a group of targets from the list, or select **Target names**.

   b. If you selected **Target names**, then specify a target name and click **Add**, or click **Find** and specify the chosen targets on the Find targets page.
   c. If user authentication is required, specify a user name, password, or any other authentication values as needed.
   d. Click **Next**.
4. On the Specify the job parameters page, specify the location of the Installation Manager instance that you want to update and the location of the repository that contains the update. For the job to run successfully, you must select **I accept the terms in the license agreements**. Click **Next**. You can also update Installation Manager using an installation kit. Specify the existing installation location. Select the **Update existing installation** check box. If updating with an Installation Manager installation kit, specify the fully qualified local path and file name of the installation kit. If the field is left blank, the update IBM Installation Manager job will locate and use the most recent IBM Installation Manager installation kit available in the default location for installation kits: `$JOB_MANAGER_HOME/IMKit`.
5. Schedule the job and click **Next**.
6. Review the summary, and click **Finish** to submit the job.

Results

The job runs and updates Installation Manager on the selected targets.

What to do next

On the Job status page, click the job ID and view the job status. Click the status refresh icon ⟳ to refresh the displayed job status.

If the job is not successful, view any error messages that result from running the job, correct the error condition, and submit the job again.

Submitting jobs to uninstall Installation Manager on remote hosts

In a flexible management environment, you can submit the **Uninstall IBM Installation Manager** job to remove the installation manager from registered hosts of the job manager.

Before you begin

Start the job manager and the targets. Ensure that the targets for which you want to remove Installation Manager are registered with the job manager.

To submit jobs, your ID at the job manager must be authorized for the administrator role or the operator role . When you submit a job, you can specify a user name and password for authentication and authorization at the target or targets. When you submit a job to multiple targets, the user name and password or the credentials for the submitter must apply all of the job targets.

To run the job against a large number of targets, optionally create a group of targets and submit the job against the group.

About this task

You can use the administrative console of the job manager or the deployment manager to submit the job. From the console, choose the **Uninstall IBM Installation Manager** job, specify the targets, schedule the job, review the summary, and submit the job.

Instead of using a console, you can run the manageOfferings job script in the AdministrativeJobs command group. See the Administrative job types topic.

Procedure

1. Click **Jobs** > **Submit** from the navigation tree of the administrative console.
2. Choose the **Uninstall IBM Installation Manager** job and click **Next**.
3. Choose job targets.
   a. Select a group of targets from the list, or select **Target names**.
   b. If you selected **Target names**, then specify a target name and click **Add**, or click **Find** and specify the chosen targets on the Find targets page.
   c. If user authentication is required, specify a user name, password, or any other authentication values as needed.
   d. Click **Next**.
4. On the Specify the job parameters page, specify the location of the Installation Manager instance that you want to uninstall. Click **Next**.
5. Schedule the job and click **Next**.
6. Review the summary, and click **Finish** to submit the job.

Results

The job runs and uninstalls Installation Manager on the selected targets.

What to do next

On the Job status page, click the job ID and view the job status. Click the status refresh icon ⟳ to refresh the displayed job status.

If the job is not successful, view any error messages that result from running the job, correct the error condition, and submit the job again.

Submitting jobs to install SSH public keys on remote hosts

In a flexible management environment, you can submit the **Install SSH Public Key** job to install SSH public keys on registered hosts of the job manager.

Before you begin

Start the job manager and the targets. Ensure that the targets for which you want to install an SSH public key are registered with the job manager.

To submit jobs, your ID at the job manager must be authorized for the administrator role or the operator role. When you submit a job, you can specify a user name and password for authentication and authorization at the target or targets. When you submit a job to multiple targets, the user name and password or the credentials for the submitter must apply all of the job targets.

To run the job against a large number of targets, optionally create a group of targets and submit the job against the group.

Note: IBM Installation Manager 1.4.3 or above is required.

About this task

You can use the administrative console of the job manager or the deployment manager to submit the job. From the job manager console, choose the **Install SSH Public Key** job, specify the targets, schedule the job, review the summary, and submit the job.

Instead of using a console, you can run the Install SSH Public Key job script in the AdministrativeJobs command group. See the Administrative job types topic.

Procedure

1. Click **Jobs** > **Submit** from the navigation tree of the administrative console.
2. Choose the **Install SSH Public Key** job and click **Next**.
3. Choose job targets.
   a. Select a group of targets from the list, or select **Target names**.
   b. If you selected **Target names**, then specify a target name and click **Add**, or click **Find** and specify the chosen targets on the Find targets page.
   c. If user authentication is required, specify a user name, password, or any other authentication values as needed.
   d. Click **Next**.
4. On the Specify the job parameters page, specify the location of the public key file that you want to install on the selected target. Click **Next**.
5. Schedule the job and click **Next**.
6. Review the summary, and click **Finish** to submit the job.

Results

The job runs and installs a public key file on the selected targets.

What to do next

On the Job status page, click the job ID and view the job status. Click the status refresh icon ↻ to refresh the displayed job status.

If the job is not successful, view any error messages that result from running the job, correct the error condition, and submit the job again.

Installing the Version 8.0 product using the job manager and administrative console

In a flexible management environment, you can use the job manager to install, update, and uninstall IBM WebSphere Application Server using the graphical user interface.

Before you begin

Note: This topic applies to WebSphere Application Server Version 8.0 only. For information about using centralized installation manager (CIM) for Version 6.1.x and 7.x, see Getting started with the centralized installation manager (CIM) for previous versions.

Ensure that you have the administrative console installed on your primary machine.

About this task

To install WebSphere Application Server, use the administrative console to register your target machine, install IBM Installation manager, and install WebSphere Application Server or other product offerings that are compatible with Installation Manager. Using the administrative console, you can set parameters for the directory in which to install the product on the target machine, specify where to store product data on the target machine, and specify the URL of the repository to download the product from. Depending on your security setup, you can also specify keyring credentials to log in to the product repository.

After the centralized installation manager successfully completes the installation process on a remote node, it then deletes the installation image files that are located in the temporary location that you specify during the installation process. If the installation is unsuccessful, the files remain in the temporary location for you to use to determine what caused the installation error. However, you can safely delete the files.

Note: IBM Installation Manager 1.4.3 or above is required.

Procedure

1. Start the job manager. See Starting the job manager.
2. Register a host with the job manager. Before you can install the product on a target machine, you must register it with the job manager. For more information, see Register or unregister with job manager settings.
3. Launch the administrative console. For more information, read about the Administrative console.
4. Test the connection to the targets on which you want to install the product. This step is optional. Before you install the product on a target machine, you can test the connection.
   a. In the administrative console, select **Job** > **Submit**.
   b. In the Job type menu list, select **Test connection**. Click **Next**.
   c. Specify the target names and target authentication.
      - If you test the connection without specifying credentials, the test will use default to existing credentials.
      - You can submit the **Test connection** job with a user name and password.
      - You can submit the **Test connection** job with a user name and private key file.
5. Optionally run an inventory job. To see what is installed on your target machine, you can run an inventory job.
   a. In the administrative console, select **Job** > **Submit**.
   b. In the job type menu list, select **Inventory**. Click **Next**.
   c. Specify the target names and target authentication.
      - You can submit an inventory job with a user name and password.
      - You can submit an inventory job without a user name and password.
6. Install or update Installation Manager on your target machine. This step is optional. If you already have the correct version of Installation Manager on your target machine, you can proceed to the next step. For more information, see Managing Installation Manager using the job manager. This step does not apply to zOS targets.
7. If you use secure shell (SSH) security, install your public key file. You can install the public key file using the same credentials as the job manager. This step does not apply to IBM i targets.
   a. In the administrative console, select **Job** > **Submit**.
   b. In the job type drop down menu, select **Install SSH Public Key**. Click **Next**.
   c. Specify the job parameters.
8. Install the product. Use the manageOfferings job to install the product.
   a. In the administrative console, select **Job** > **Submit**.
   b. In the job type drop down menu, select **Manage offerings**. Click **Next**.
   c. Specify the following optional or required job parameters.

      Required parameter:
      - Response file path name: The full path name to the response file on the job manager machine.

      Optional parameters:
      - IBM Installation Manager Path: Specify the path to install Installation Manager on the remote machine. If this parameter is blank, then Installation Manager is installed to the default location.

- IBM Installation Manager key ring file: If the package repository requires a key ring file for authentication, specify the full path name of the key ring file on the job manager machine.
- Key ring file password: If the key ring file is password protected, specify the key ring password.
- IBM Installation Manager agent data location: Specify an IBM Installation Manager data location that is not the default location for the manageOfferings job.

  Note: Do not use a non-default data location unless you are familiar with IBM Installation Manager.

d. Select **I accept the terms in the license agreements**.

9. Optionally transfer files to or from the target machine. For example, if the installation fails, you might want to transfer the log files from the target machine to understand why the job failed.
   - To collect a file from remote hosts:
     a. In the administrative console, select **Job** > **Submit**.
     b. In the job type menu list, select **Collect file**. Click **Next**.
     c. Specify the job parameters.
        – The destination location is `<profile home>/config/temp/JobManager/<task id>/<host name>`.
   - To distribute a file to remote hosts:
     a. In the administrative console, select **Job** > **Submit**.
     b. In the job type menu list, select **Distribute file**. Click **Next**.
     c. Specify the job parameters.
        – The source location must be `<profile home>/config/temp/JobManager`.
   - To delete a file on remote hosts:
     a. In the administrative console, select **Job** > **Submit**.
     b. In the job type menu list, select **Remove file**. Click **Next**.
     c. Specify the job parameters.
10. Create a profile for the newly installed product on the target machine.
    a. In the administrative console, select **Job** > **Submit**.
    b. In the job type menu list, optionally select **Manage Profiles**. Click **Next**.
    c. Choose the job targets.
    d. Specify the job parameters.
       - wasHome: The directory where you installed the product on the target machine
       - responseFile: The response file used to create an IBM WebSphere Application Server profile

Results

You have installed WebSphere Application Server on a target machine and created a profile using the job manager.

What to do next

Using the job manager, you can run any command or script on your target machine.

1. In the administrative console, select **Job** > **Submit**.
2. In the job type drop down menu, select **runCommand**. Click **Next**.
3. Specify the job parameters.

You can uninstall Installation Manager using the administrative console. For more information, see Managing Installation Manager using the job manager.

Installing the Version 8.0 product using the job manager and command line

In a flexible management environment, you can use the job manager to install, update, and uninstall IBM WebSphere Application Server using the command line with a response file.

Before you begin

Note: This topic applies to WebSphere Application Server Version 8.0 only. For information about using centralized installation manager (CIM) for Version 6.1.x and 7.x, see Getting started with the centralized installation manager (CIM) for previous versions.

Before you install WebSphere Application Server using the job manager, ensure that you have WebSphere Application Server Version 8.0 installed on your primary machine.

About this task

To install WebSphere Application Server, use wsadmin to run the manageOfferings command. The manageOfferings command uses a response file and a security keyring. In the response file, you can set parameters for the directory in which to install the product on the target machine, specify where to store product data on the target machine, and specify the URL of the repository to download the product from. Depending on your security setup, you can also specify keyring credentials to log in to the product repository.

After the centralized installation manager successfully completes the installation process on a remote node, it then deletes the installation image files that are located in the temporary location that you specify during the installation process. If the installation is unsuccessful, the files remain in the temporary location for you to use to determine what caused the installation error. However, you can safely delete the files.

Note: IBM Installation Manager 1.4.3 or above is required.

Procedure

1. Start the job manager. For detailed instructions, see starting the job manager.
2. Register a host with the job manager. Before you can install the product on a target machine, you must register it with the job manager. Use the wsadmin tool to run the registerHost command.
   - You can register the host with a private key; for example:
     - Using Jacl:

       ```
       $AdminTask registerHost  {-host hostname -hostProps
       {{privateKeyFile filename} {username root }{saveSecurity true}}}
       ```

     - Using Jython:

       ```
       AdminTask.registerHost('[-host hostname -hostProps
       [[username user][privateKeyFile filename][saveSecurity true]]]')
       ```

   - You can register the host with a user name and password; for example:
     - Using Jacl:

       ```
       $AdminTask registerHost {-host hostname -hostProps { {password xxxxx}
       { username root } {saveSecurity true}}}
       ```

     - Using Jython:

       ```
       AdminTask.registerHost('[-host hostname -hostProps [[password xxxxx][username user]
       [saveSecurity true]]]')
       ```

3. Optional: Test the connection to the targets on which you want to install the product. Before you install the product on a target machine, you can test the connection.
   - If you test the connection without specifying credentials, the test will use default to existing credentials; for example:

  - Using Jacl:

    ```
    $AdminTask submitJob {-jobType testConnection -targetList {hostname}}
    ```

  - Using Jython:

    ```
    AdminTask.submitJob('-jobType testConnection -targetList [hostname]')
    ```

- You can submit the Test connection job with a username and password; for example:
  - Using Jacl:

    ```
    $AdminTask submitJob {-jobType testConnection -targetList
    {hostname} -username username -password password}
    ```

  - Using Jython:

    ```
    AdminTask.submitJob('-jobType testConnection -targetList
    [hostname]  -username username -password password')
    ```

- You can submit the Test connection job with a user name and private key file; for example:
  - Using Jacl:

    ```
    $AdminTask submitJob {-jobType testConnection -targetList
    {hostname} -username username -privateKeyFile private_key_filename}
    ```

  - Using Jython:

    ```
    AdminTask.submitJob('-jobType testConnection -targetList
    [hostname] -username username -privateKeyFile C:\temp\private_key_filename')
    ```

4. Optionally run an Inventory job to see what is installed on your target machine.
   1. Submit an Inventory job with a user name and password.
      - Using Jacl:

        ```
        $AdminTask submitJob {-jobType inventory -targetList {hostname}
        -username username -password password}
        ```

      - Using Jython:

        ```
        AdminTask.submitJob('-jobType inventory -targetList [hostname]
        -username username -password password')
        ```

   2. Submit an Inventory job without a user name and password.
      - Using Jacl:

        ```
        $AdminTask submitJob {-jobType inventory -targetList {hostname}}
        ```

      - Using Jython:

        ```
        AdminTask.submitJob('-jobType inventory -targetList [hostname]')
        ```

5. Optional: Install or update Installation Manager on your target machine.

   If you already have the correct version of Installation Manager on your target machine, you can proceed to the next step. For more information, see managing Installation Manager using the job manager.
6. If you use SSH security, install your public key file.

   You can install the public key file using the same credentials as the job manager. This step does not apply to IBM i targets.
   1. Run the installSSHPublicKey admin task; for example:
      - Using Jacl:

        ```
        $AdminTask submitJob {-jobType installSSHPublicKey -targetList {target}
        -jobParams { {publicKeyFile keyfilepath} } -description "test installSSHPublicKey"}
        ```

      - Using Jython:

        ```
        AdminTask.submitJob ('-jobType installSSHPublicKey -targetList [target]
        -jobParams [[publicKeyFile keyfilepath]] -description "test installSSHPublicKey"')
        ```

7. Set up a response file for the manageOfferings command.
   1. Create a response file. You can create a response file using the Installation Manager. For more information, see creating a response file with Installation Manager.
   2. You can edit the response file to include information about your target machine.
   3. You can use the response file to install any offering that is compatible with Installation Manager. For more information, see the Installation Manager information center.

Windows Create a response file that specifies the offering profile parameter as WebSphere Application Server, Network Deployment on Windows; for example:

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input acceptLicense='true' clean='true' temporary='true'>
<server>
<repository location='<MY REPOSITORY LOCATION>'/>
</server>
<profile installLocation='<LOCATION TO INSTALL PRODUCT ON TARGET MACHINE>' id='IBM WebSphere Application Server - ND'>
<data key='cic.selector.nl' value='en'/>
<data key='eclipseLocation' value='<LOCATION TO INSTALL PRODUCT DATA ON TARGET MACHINE>'/>
<data key='user.select.64bit.image,com.ibm.websphere.ND.v80' value='false'/>
</profile>
<install modify='false'>
<offering profile='IBM WebSphere Application Server - ND' features='core.feature' id='com.ibm.websphere.ND.v80' />
</install>
<preference value='false' name='PassportAdvantageIsEnabled'/>
<preference value='30' name='com.ibm.cic.common.core.preferences.connectTimeout'/>
<preference value='0' name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount'/>
<preference value='C:\Program Files\IBM\WebSphere\AppServer-Shared' name='com.ibm.cic.common.core.preferences.eclipseCache'/>
<preference value='false' name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication'/>
<preference value='false' name='com.ibm.cic.common.core.preferences.keepFetchedFiles'/>
<preference value='true' name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts'/>
<preference value='30' name='com.ibm.cic.common.core.preferences.readTimeout'/>
<preference value='false' name='com.ibm.cic.common.core.preferences.searchForUpdates'/>
<preference value='false' name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode'/>
<preference value='true' name='http.ntlm.auth.enableIntegrated.win32'/>
<preference value='NTLM' name='http.ntlm.auth.kind'/>
<preference value='true' name='offering.service.repositories.areUsed'/>
</agent-input>
```

a. Save the response file as `filename.txt`.

8. Run the manageOfferings command. For the job to run successfully, you must specify `acceptLicense TRUE`.

   a. Open wsadmin from the job manager profile bin directory.

   b. Enter the manageOfferings command in wsadmin. For example:

      - Using Jacl:

        ```
        $AdminTask submitJob {-jobType manageOfferings -targetList hostname -username user -password *******
        -jobParams
        {{responseFile <RESPONSE FILE LOCATION>} {acceptLicense TRUE} {IMPath <IM install location>}
        {keyringFile <key ring file location>} {keyringPassword pwd} }}
        ```

      - Using Jython:

        ```
        AdminTask.submitJob ('-jobType manageOfferings -targetList hostname -username user -password *******
        -jobParams
        [[responseFile <RESPONSE FILE LOCATION>] [acceptLicense TRUE][IMPath <IM install location>]
        [keyringFile <key ring file location>] [keyringPassword pwd]]')
        ```

      The manageOfferings command pulls the response file that you created in this task and begins the product installation.

   The following parameter for this job is required:

   - responseFile: (Response file path name) This parameter contains the full path name to the offering response file on the job manager machine.

   The following parameters for this job are optional:

   a. IMPath: (IBM Installation Manager Path) This parameter contains the full path of the IBM installation manager on the remote machine. Use this parameter if you have more than one instance of Installation Manager on your remote machine. If you have only one instance of Installation Manager installed, you can leave this parameter empty because the job can find it. Specify whether the target machine has more than one instance of Installation Manager installed.

   b. keyringFile: (IBM Installation Manager key ring file): If the package repository requires a key ring file for authentication, specify the full path name of the key ring file on the job manager machine.

   c. keyringPassword: (Key ring file password If the key ring file is password protected, specify the key ring password.

9. Optional: Run the collectFile and distributeFile administrative tasks.

Optionally transfer files to or from the target machine and delete files on the target machine. For example, if the installation fails, you might want to transfer the log files from the target machine to understand why the job failed. When using these administrative tasks, you can specify wildcards in the filename.

Note: The destination must be a directory, it cannot be a file.

- To collect a file from remote hosts:
  - Using Jacl:

    ```
    $AdminTask submitJob {-jobType collectFile -targetList hostname -jobParams
    {{source D:\\WAS80\\logs\\manageprofiles\\response.log} {destination log}}}
    ```
  - Using Jython:

    ```
    AdminTask.submitJob('-jobType collectFile -targetList hostname -jobParams
    [[source D:\\WAS80\\logs\\manageprofiles\\response.log] [destination log]')
    ```
- To distribute a file to remote hosts:
  - Using Jacl:

    ```
    $AdminTask submitJob{-jobType distributeFile -targetList hostname
    -jobParams {{source test.txt}{destination D:\\temp\\test.txt} }}
    ```
  - Using Jython:

    ```
    AdminTask.submitJob('-jobType distributeFile -targetList hostname
    -jobParams [[source test.txt][destination D:\\temp\\test.txt] ]')
    ```
- To delete a file on remote hosts:
  - Using Jacl:

    ```
    $AdminTask submitJob{-jobType removeFile -targetList hostname
    -jobParams {{location D:\\temp\\test.txt}}}
    ```
  - Using Jython:

    ```
    AdminTask.submitJob('-jobType removeFile -targetList hostname
    -jobParams [[location D:\\temp\\test.txt] ]')
    ```

10. Create a profile for the newly installed product on the target machine.

    Specify the following parameters:

    - targetList: The machine where you want to create a new profile
    - wasHome: The directory where you installed the product on the machine that is running job manager
    - responsefile: Enter the directory where you saved your response file. This text file provides the parameters and information of the profile to create.

    For example:

    - Using Jacl:

      ```
      $AdminTask submitJob {-jobType manageprofiles -targetList hostname
      -jobParams {{wasHome D:\\WAS70GA} {responseFile D:\\temp\\mp1.txt}}}
      ```
    - Using Jython:

      ```
      $AdminTask submitJob {-jobType manageprofiles -targetList hostname
      -jobParams {{wasHome D:\\WAS70GA} {responseFile D:\\temp\\mp1.txt}}}
      ```

Results

You have installed the product on a target machine and created a profile using the job manager.

What to do next

Using the job manager, you can run any command or script on your target computer.

- Using Jacl:

  ```
  $AdminTask runCommand {-host hostname -jobParams
  {{command command_to_run}{workingDir working_directory_on_remote_host}}}
  ```
- Using Jython:

```
$AdminTask.runCommand ('-host hostname -jobParams
[[command command_to_run][workingDir working_directory_on_remote_host]]')
```

Managing Installation Manager using the job manager

You can store and manage all of your installation manager installation kits from a central location.

Before you begin

Before you can work with IBM Installation Manager, you must register at least one host with the job manager. You must also have acquired one or more Installation Manager installation kits.

Note: IBM Installation Manager 1.4.3 or above is required.

About this task

If you have multiple Installation Manager offerings or need to manage Installation Manager on multiple remote machines, the job manager can automate this process. Job manager can also store your Installation Manager installation kits in a single repository. This allows you to manage your installation kits from a single location and send your installation kits to multiple machines.

Procedure

- You can submit an inventory job to see what is installed on a host.
  - You can submit and inventory job with a username and password; for example:
    - Using Jacl:

```
$AdminTask submitJob {-jobType inventory -targetList {hostname} -username username -password password}
```

    - Using Jython:

```
AdminTask.submitJob('-jobType inventory -targetList [hostname] -username user -password xxxxxx')
```

  - If you saved user credentials while registering host, you can submit an inventory job without credentials; for example:
    - Using Jacl:

```
$AdminTask submitJob {-jobType inventory -targetList {hostname} }
```

    - Using Jython:

```
AdminTask.submitJob('-jobType inventory -targetList [hostname] ')
```

- You can browse the Installation Manager installation kit directory and change the directory location. Perform this task using the administrative console graphical user interface. Open the administrative console and select **Submit Jobs** > **Installation Manager installation kits**. For more information, see Installation Manager installation kits.
- You can submit a job to install Installation Manager on a host using the administrative console.
  1. In the administrative console, select **Job** > **Submit**.
  2. In the job type menu list, select **Install IBM Installation Manager**. Click **Next**.
  3. Specify the job parameters. The **Install Action** menu has the following options:
     - Install based on login credentials
     - Install for single user only
     - Install for a group of users
- You can submit a job to install Installation Manager on a host by sending the installation kit from the command line.

  The installIM job has the following required parameters:
  - kitPath: Specify the full path name to the IBM Installation Manager kit on the job manager machine.
  - acceptLicense: Must be set to true, if you do not specify this parameter, the job will fail.

  The installIM job has the following optional parameters:

- **installPath**: Specify the path to install Installation Manager on the remote machine. If this parameter is not specified, then Installation Manager is installed to the default location.
- **dataPath**: Specify the Installation Manager data path on the remote machine. If this parameter is not specified, the default Installation Manager data path is used.
- AIX Linux Solaris HP-UX **installAction**: Specify a group or single user installation of Installation Manager. If the parameter is not specified, then the parameter is automatically selected depending on the user account type. For example, if your user account belongs to an administrative group, then the job will install Installation Manager for all users of the administrative group.
- Submit the install Installation Manager job without credentials; for example:
  - Using Jacl:

```
$AdminTask submitJob {-jobType installIM -targetList {hostname} -jobParams { {installPath <path>}
{dataPath <path>} {kitPath <path>} {acceptLicense true} } -description "IM install without username"}
```

  - Using Jython:

```
AdminTask.submitJob ('-jobType installIM -targetList [hostname] -jobParams [[installPath <path>]
[dataPath <path>] [kitPath <path>] [acceptLicense true]] -description "IM install without username"')
```

- Submit the install Installation Manager job using a private key; for example:
  - Using Jacl:

```
$AdminTask submitJob {-jobType installIM -targetList {hostname} -jobParams {
{installPath <path>} {dataPath <path>} {kitPath <path>} {acceptLicense true} }
-privateKeyFile "<key file path>" -description "IM install with private key"}
```

  - Using Jython:

```
AdminTask.submitJob ('-jobType installIM -targetList [hostname] -jobParams [
[installPath <path>] [dataPath <path>] [kitPath <path>] [acceptLicense true] ]
-privateKeyFile '<key file path>' -description "IM install with private key"')
```

- Submit the install Installation Manager job using a user name and password; for example:
  - Using Jacl:

```
$AdminTask submitJob {-jobType installIM -targetList {hostname} -jobParams { {installPath <path>}
{dataPath <path>} {kitPath <path>} {acceptLicense true} } -username root -password abcd
-description "IM install with username and pwd"}
```

  - Using Jython:

```
AdminTask.submitJob ('-jobType installIM -targetList [hostname] -jobParams [[installPath <path>]
[dataPath <path>] [kitPath <path>] [acceptLicense true] ] -username root -password abcd
-description "IM install with username and pwd"')
```

- You can review the Installation Manager license.
  - If you are using the graphical user interface (GUI), run the following command and follow the instructions:
    - AIX HP-UX Solaris run install
    - Windows install.exe
  - If you are using the command line, run the following command and follow the instructions:
    - AIX HP-UX Solaris run installc -c
    - Windows installc.exe -c
- You can submit a job to update Installation Manager on a host by providing an Installation Manager repository URL from the command line. This job has the following required parameter:
  - acceptLicense: Must be set to true, if you do not specify this parameter, the job will fail.

  For example:
  - Using Jacl:

```
$AdminTask submitJob {-jobType updateIM -targetList {hostname} -jobParams { {installPath <path>}
{repository <repository URL>} {keyringFile <file path>} {keyringPassword <keyringpwd>} {acceptLicense true} }
-username root -password <password> -description "update IM with username and pwd"}
```

  - Using Jython:

```
AdminTask.submitJob('-jobType updateIM -targetList [hostname] -jobParams [ [installPath <path>]
[repository <repository URL>] [keyringFile <file path>] [keyringPassword]  [acceptLicense true] ]
-username <username> -password <password>')
```

- You can submit a job to update Installation Manager on a host using the administrative console.

1. In the administrative console, select**Job** > **Submit**.
2. In the job type menu list, select **Update IBM Installation Manager**. Click **Next**.
3. Specify target names and target authentication.
4. Specify the job parameters and accept the license agreement:
   - installPath: IBM Installation Manager installation location.
   - repository: IBM Installation Manager repository.
   - keyringFile: IBM Installation Manager key ring file, the credentials for the protected repository are retrieved from the key ring file.
   - keyringPassword: Password for accessing key ring file.

- You can delete Installation Manager installation kits from the repository. Perform this task using the administrative console graphical user interface. Open the administrative console and select **Jobs** > **Installation Manager installation kits**. For more information, see Installation Manager installation kits.
- You can submit a job to uninstall IBM Installation Manager. For example:
  - Using Jacl:

```
$AdminTask submitJob {-jobType uninstallIM -targetList {hostname} -jobParams { {installPath <IM install path>}}}
```

  - Using Jython:

```
AdminTask.submitJob('-jobType uninstallIM -targetList [hostname] -jobParams [ [installPath <IM install path>] ]]')
```

- You can submit a job to uninstall Installation Manager using the administrative console.
  1. In the administrative console, select **Jobs** > **Submit**.
  2. In the job type menu list, select **Uninstall IBM Installation Manager**. Click **Next**.
  3. Specify target names and target authentication.
  4. Specify the job parameters.
     - The following parameter is required: installPath, IBM Installation Manager installation location.
- You can submit a job to find Installation Manager data locations. You can add specific data locations, or search the system for Installation Manager data locations.
  1. In the administrative console, select **Jobs** > **Submit**.
  2. In the job type menu list, select **Add or search for Installation Manager data locations**. Click **Next**.
  3. Specify target names and target authentication.
  4. Specify the job parameters.
     - You can specify Installation Manager data locations.
     - You can search the system for Installation Manager data locations.

Results

You have installed, updated, or deleted Installation Manager and Installation Manager installation kits on a target machine.

What to do next

You can continue to view node resources and do other job management tasks such as submit jobs, create node groups for job submission, and view nodes.

Using the centralized installation manager (CIM) to manage Version 6.1.x and 7.x

Use the centralized installation manager (CIM) to shorten the number of steps that are required to create and manage environments that contain previous versions of WebSphere Application Server. As an administrator, you can remotely install or uninstall product components and apply maintenance from the administrative console.

Before you begin

Note: This topic applies to WebSphere Application Server Version 6.1.x and 7.x only. For information about using centralized installation manager (CIM) for Version 8.0, see “Submitting Installation Manager jobs” on page 292.

You must first install the CIM repository on the deployment manager, and add one or more product components to the repository using the IBM WebSphere Installation Factory. For more information on installing the CIM and creating the repository, read “Installing packages using the centralized installation manager (CIM) for previous versions” on page 317.

Restriction: This feature is not available in WebSphere Application Server Network Deployment for z/OS.

About this task

Table 39. Differences between CIM versions. This table lists the differences between CIM for Version 8.0 and CIM for Version 6.x and 7.x

Function	CIM Version 6.x and 7.x	CIM Version 8.0
Scope	Install, update, uninstall Version 7.x. Update Version 6.x	Install, update, uninstall Version 8.0 and all Installation Manager installable products: WebSphere Application Server, IHS Plugin, and DMZ.
Installation software used	ISMP and Update Installer	Installation Manager
Repository	Maintains a private repository on the Deployment Manager	Maintains an installation kit directory. Uses Installation Manager repository
Administrative console	Accessible from the Deployment Manager	Accessible from the Job Manager. Job Manager is also available on the Deployment Manager
Command line	CIM AdminTask commands	Use Job Manager's submitJob command

The CIM does not replace the standard installer and the Update Installer for WebSphere Software used to install and update the WebSphere Application Server product. Rather, the CIM pushes the product binary files or maintenance to the remote targets and invokes the standard installer or update installer tool to perform the installation or update on the targets.

- Use the CIM to simplify the installation and maintenance of application servers within a Network Deployment cell.

  The CIM is a flexible administration solution that you can use to perform the following actions:

  – Download previous version interim fixes and fix packs from the IBM support site directly to the CIM repository.

  – Install interim fixes and fix packs for WebSphere Application Server Network Deployment, Version 7.0 on target nodes that are within the Network Deployment cell. This is a mixed-version cell where the deployment manager node is a Version 8.0 node.

  – Monitor download and installation status of packages through the administrative console.

Procedure

1. Prepare the CIM for use in your application server environment.

Read “Getting started with the centralized installation manager (CIM) for previous versions.”

2. Use the CIM to install one or more packages to the specified target workstations.

   Read “Installing packages using the centralized installation manager (CIM) for previous versions” on page 317.
3. Download installation packages and maintenance files to the CIM repository to install later on the remote workstations.

   Read “Downloading package descriptors and binary files for previous versions to the centralized installation manager (CIM) repository” on page 330.
4. Add or remove installation targets, edit the configuration of an existing installation target, and store the administrative ID and password of each target for later use when installing or uninstalling packages.

   Read “Managing Version 6.1.x and 7.x centralized installation manager (CIM) installation targets” on page 336.
5. Review end-to-end use cases of how the CIM can be used to assist WebSphere Application Server administrators.

   Read “Centralized installation manager (CIM) Version 6.1.x and 7.x usage scenarios” on page 341.
6. Use wsadmin commands and parameters to install, uninstall, and manage various software packages and maintenance files through the CIM.

   Read “Centralized installation manager (CIM) AdminTask commands for Version 6.1.x and 7.x” on page 343.

Getting started with the centralized installation manager (CIM) for previous versions

Prepare the centralized installation manager (CIM) for use in your application server environment.

Before you begin

Create the CIM repository on the deployment manager using IBM WebSphere Installation Factory Version 7.0.0.15 or later. TheIBM WebSphere Installation Factory is included with WebSphere Application Server Network Deployment Version 7.0, or you can download the latest version from the IBM website. For more information, read the "Installing Network Deployment" topic.

Restriction: Only Network Deployment packages and Network Deployment customized installation packages are supported in a CIM repository.

About this task

Familiarize yourself with the CIM and prepare for its use by reading the following topics in this section:

- “Considerations when using the centralized installation manager (CIM) for previous versions” on page 311
- “Adding installation packages of previous versions to the centralized installation manager (CIM) repository using the Installation Factory” on page 312
- “Special procedures for IBM i operating systems when running the centralized installation manager (CIM) for previous versions” on page 313
- “Installing Version 6.1.x and 7.x customized installation packages (CIPs) using the centralized installation manager (CIM)” on page 320
- “Requirements for using Remote Execution and Access (RXA)” on page 315
- “Additional requirements for installing or uninstalling maintenance to previous versions on AIX as a non-root user” on page 317

What to do next

Use the CIM to download and install packages to targets in a cell or review the CIM usage scenarios.

Considerations when using the centralized installation manager (CIM) for previous versions

Consider the following information before installing and using the centralized installation manager (CIM) in your application server environment.

Note: Vista 2008 Windows 7 You must elevate your Windows user account privileges to perform CIM operations. For more information on the elevated user account privileges, see the Microsoft documentation on the User Account Control or see the Managing centralized installation manager (CIM) installation targets documentation. In addition to the elevated Windows user account privileges, you must enable the Remote Registry service to perform CIM operations on remote Microsoft Windows systems.

Note: Centralized installation manager does not support adding targets outside of the cell.

Installable packages and products

The centralized installation manager does not replace the Installation wizard or the IBM Update Installer for WebSphere Software. Instead, the centralized installation manager starts the Installation wizard for the product component or the Update Installer to install or uninstall the components or maintenance.

The various product components and maintenance files that you can install or uninstall by using the centralized installation manager are included in the following list:

- WebSphere Application Server Network Deployment Version 7.x
- WebSphere Application Server Version 6.x and 7.x refresh packs, fix packs, and interim fixes

gotcha: The WebSphere Application Server centralized installation manager (CIM) does not support the installation of integrated installation packages (IIPs).

Consult the documentation for WebSphere Application Server to learn more about installing or uninstalling product components or maintenance from the application server and uninstalling product components when no augmented profiles exist.

Cell-based function

Centralized installation manager for previous versions is a cell-based function. If WebSphere Application Server is installed on a target, it will be federated back to the deployment manager as a new node. Fix packs and interim fixes can be applied to nodes within the cell only.

Temporary installation locations

After the centralized installation manager successfully completes the installation process on a remote node, it then deletes the installation image files that are located in the temporary location that you specify during the installation process. If the installation is unsuccessful, the files remain in the temporary location for you to use to determine what caused the installation error. However, you can safely delete the files.

Starting the node agent

The centralized installation manager relies on current information regarding the versions of WebSphere Application Server that are installed on each node. This information is kept current on the deployment manager configuration by the node agent that is running on each node. The deployment manager contains the correct versions of WebSphere Application Server that are installed on each node if the node agent of each node is started at least once after each update is applied. To ensure that the deployment manager receives this information, the centralized installation manager automatically starts the node agent after each installation or uninstallation of maintenance.

Note: To locally apply updates on the nodes without using the centralized installation manager, issue the startNode command after you complete the operation to manually start the node agent.

Secondly, the centralized installation manager relies on the node agent to effectively stop the server processes on the target node and if the node agent is not running, the administrator will have to ensure that all the server processes are stopped on the target node before initiating any maintenance update operations on the node.

Update Installer for WebSphere Software

The centralized installation manager installs an appropriate level of the Update Installer on the target systems that it uses to install fix packs and other maintenance. If you had previously installed the Update Installer tool on any of the target hosts in a directory location other than *app_server_root*/`UpdateInstaller`, then you may want to consider uninstalling the Update Installer by using its uninstallation process because that copy would not be used by the centralized installation manager. But it is not mandatory to uninstall that copy for CIM to work properly.

The centralized installation manager will automatically install the Update Installer tool (if it is not already installed in *app_server_root*/`UpdateInstaller`) when you install fix packs or other maintenance on the target systems. If the version of the Update Installer tool found in *app_server_root*/`UpdateInstaller` does not meet the minimum version required by the interim fix or fix pack, the centralized installation manager automatically installs a newer version on the targets, if you have downloaded the newer version of the Update Installer tool to your repository.

Lastly, you cannot use centralized installation manager to install the Update Installer on nodes that are not federated to the deployment manager cell.

Adding installation packages of previous versions to the centralized installation manager (CIM) repository using the Installation Factory

Use IBM WebSphere Installation Factory Version 7.0.0.15 or later to add WebSphere Application Server Network Deployment Version 7.0 installation packages to the repository. From the administrative console, you can then use the centralized installation manager to install your added components from the repository to the nodes. Each WebSphere Application Server installation has only one associated repository. The repository is shared among all the deployment managers of the installation.

Before you begin

To populate the repository, ensure you have write permission to the specified repository directory. To configure the WebSphere Application Server installation to associate with the repository, ensure you have write permission to the *`app_server_root`*`/properties` directory.

Procedure

1. Launch the Installation Factory from the following location, where *if_root* is the Installation Factory root directory.
   - AIX HP-UX Linux Solaris *if_root*/`bin/ifgui.sh`
   - Windows *if_root*`\bin\ifgui.bat`
2. Click **Manage Repository for Centralized Installation Manager**.
3. On the WebSphere Application Server installation directory page, you can optionally enter the directory path to a WebSphere Application Server installation to associate the repository with the installation. Click **Next**.

4. On the Repository and Installation Package page, enter the directory path to the repository, and enter the directory path to an installation package. Click **Next**.

   The specified installation package is populated to the repository when the procedure is complete. If you only want to configure the WebSphere Application Server installation to associate the repository, then enter the directory path to the WebSphere Application Server installation on the previous page and leave the directory path to installation package to empty.

   To change your selections, click **Back**.
5. Review the preview page, and click **Finish** to begin the procedure on the repository.
6. Optional: You can also add a CIP to the repository from the Installation Factory command line interface. Run the ifcli command using the options in table.
   - AIX HP-UX Linux Solaris *if_root*`/bin/ifcli.sh`
   - Windows *if_root*`\bin\ifcli.bat`

Table 40. ifcli command-line options for centralized installation manager.

This table describes command-line options for centralized installation manager.

Option	Description
`-wasPath wasInstallationPath`	Specifies the directory path of the WebSphere Application Server installation.
`-repositoryPath repositoryPath`	Specifies the directory path of the repository.
`-installationPackagePath installationPackagePath`	Specifies the directory path of the installation package.
`-overwrite`	Overwrites the existing installation package in the repository.

Results

The centralized installation manager repository you specified now contains one or more WebSphere Application Server installation packages. Alternatively, you can add the installation package to the repository as you install the installation package on the deployment manager workstation. Read the "Adding the current installation package during installation" topic for more information.

Example

- Example 1: Use the following command to create the repository on `D:\CIM\repository`. If the repository does not already exist, populate the repository with the installation package on `E:\WAS70ND`, and configure the WebSphere Application Server installation on `C:\IBM\WebSphere\AppServer` with the repository.

```
ifcli.bat -wasPath C:\IBM\WebSphere\AppServer -repositoryPath D:\CIM\repository -installationPackagePath E:\WAS70ND
```

- Example 2: Use the following command to add the installation package in `E:\WAS70ND` to the repository, which is associated with the WebSphere Application Server installation in `C:\IBM\WebSphere\AppServer`.

```
ifcli.bat -wasPath C:\IBM\WebSphere\AppServer -installationPackagePath E:\WAS70ND
```

- Example 3: Use the following command to add the installation package in `E:\WAS70ND` to the repository in `D:\CIM\repository`. Overwrite the installation package in the repository if it exists already.

```
ifcli.bat -repositoryPath D:\CIM\repository -installationPackagePath E:\WAS70ND -overwrite
```

- Example 4: Use the following command to configure the WebSphere Application Server installation in `C:\IBM\WebSphere\AppServer` with the repository at `D:\CIM\repository`. The repository is created if it does not exist.

```
ifcli.bat -wasPath C:\IBM\WebSphere\AppServer -repositoryPath D:\CIM\repository
```

Special procedures for IBM i operating systems when running the centralized installation manager (CIM) for previous versions

Special procedures are required if you choose to run centralized installation manager (CIM) on IBM i operating systems. Since IBM WebSphere Installation Factory is not supported on IBM i operating system, you must create the repository on a Windows operating system and then transfer the repository to the IBM i operating system.

About this task

Note: This topic applies to WebSphere Application Server Version 6.1.x and 7.x only. For information about using centralized installation manager (CIM) for Version 8.0, see “Submitting Installation Manager jobs” on page 292.

Use the Installation Factory Version 7.0.0.15 or later to create a repository on a Windows system, and then transfer the packages to the repository that resides on the IBM i system.

Use the following procedure to add the installation packages into the CIM repository on the IBM i system using the Windows operating system.

Procedure

1. Install WebSphere Application Server Network Deployment Version 8.0 onto the IBM i operating system.
2. Install the Installation Factory onto the Windows operating system.
3. Insert the WebSphere Application Server Network Deployment Version 7.0 installation disk into the drive of the Windows system, or create a customized installation package (CIP) with the Installation Factory on the Windows system.
4. Create a repository locally on the Windows operating system with the Installation Factory.
5. Change the directory to the repository path.

   Run the command zip -r cimrepos.zip * to create a compressed file including all the directories in the repository.

   You can also selectively include only the directories you want. If you are including any CIP images, you need to also include the corresponding CIP descriptors that are in the descriptors directory. The CIP descriptor is an XML file whose name contains the CIP directory name. For example, if the CIP directory name is `com.ibm.torolab.ND70_AIX_PPC32_1.0.0.0`, then the descriptor name is something like `InstallPackageND70X_com.ibm.torolab.ND70_AIX_PPC32_1.0.0.0.xml`.
6. Log onto the IBM i system. The centralized installation manager repository location is stored in `<WAS_HOME>/properties/cimgr.props`. The default value is *"${WAS_INSTALL_ROOT}/cimrepos"*. The default location is "`/QIBM/ProdData/WebSphere/AppServer/cimrepos`". The user that runs WebSphere Application Server must have write permission to create the *cimrepos* directory and its contents. Otherwise, errors can occur when CIM downloads new descriptors or runs the Update Installer. You might see an error in the SystemOut.log that is similar to the following error:

```
XCIM0903E: Cannot download file 7.0.0.13-WS-UPDI-i5OsPPC.zip.part to /QIBM/ProdData/WebSphere/AppServer/cimrepos/UPDI70.
Reason:  /QIBM/ProdData/WebSphere/AppServer/cimrepos/UPDI70/7.0.0.13-WS-UPDI-i5OsPPC.zip.part (A file or  directory in the path name does not exist.)
```

   If the user that runs WebSphere Application Server does not have write permission to the *<WAS_HOME>* directory, you can relocate the repository location to a directory other than *<WAS_HOME>* by modifying the value in `cimgr.props`.
7. Create the repository directory if it is not already created.
8. Transfer cimrepos.zip from the Windows system to the repository directory on the IBM i system. Extract the contents of the cimrepos.zip file onto the repository directory and optionally delete the original zip file.

Results

You have added the installation packages into the CIM repository on the IBM i system.

Instead of creating the repository on the disk drive of the Windows system and transferring the file, alternatively, you can map the IBM i file system of the repository onto the Windows system and use it for populating the installation packages. Using this alternative method eliminates transferring the files to the IBM i system.

What to do next

Use the centralized installation manager to install the components to the nodes and begin managing your environments. In the administrative console, click **System administration** > **Centralized Installation Manager**.

Requirements for using Remote Execution and Access (RXA)

You can use Remote Execution and Access in WebSphere Application Server Version 8.0 and 7.0. WebSphere Application Server Network Deployment provides management features, such as initiating installations of product packages and maintenance from the administrative console. The product uses the Tivoli Remote Execution and Access (RXA) toolkit to access your remote workstations.

Windows target requirements

Many RXA operations require access to resources that are not generally accessible by standard user accounts. Therefore, the account names that you use to log onto remote Windows targets must have administrative privileges.

Simple file sharing

Windows XP system targets must have simple file sharing disabled for RXA to work. Simple networking requires that you log in as `guest`. A guest login does not have the authorization necessary for RXA to function correctly.

To disable Simple File Sharing, open Windows Explorer and click **Tools** > **Folder Options** > **View** > **Use Simple File Sharing**. Clear the **Use Simple File Sharing** check box. Click **Apply** and **OK**.

Vista Windows 7 2008 You must enable file sharing for the Guest or Everyone accounts, and disable password protected sharing. To disable password protected sharing, perform the following steps:

1. Click **Control Panel** > **Network and Sharing Center** > **Sharing and Discovery**.
2. Expand **Password protected sharing** by clicking the down arrow on the far right.
3. Select **Turn off password protected sharing**.
4. Click **Apply**, and exit the control panel.

Firewalls

Windows XP systems include a built-in firewall called the Internet Connection Firewall (ICF), which is disabled by default. For Windows XP Service Pack 2 systems, the Windows firewall is enabled by default. If either firewall is enabled on a Windows target workstation, RXA cannot access the target workstation. On Windows XP Service Pack 2, you can select the **File and Printer Sharing** check box in the Exceptions tab of the Windows Firewall configuration to allow access. Do not block port 445.

Administrative sharing

You must enable the remote registry administration, which is the default configuration, on the target workstation for RXA to run commands and scripts. To verify that the remote registry is enabled and started, click **Start** > **Programs** > **Administrative Tools** > **Services**. From **Remote Registry**, ensure the status of the service is started.

You must enable administrative sharing to successfully use RXA to connect to your Windows systems targets. Examples of the default administrative disk share are C$ and D$. If you disable sharing, RXA considers directories that are located within the drives as hidden. In this case, the following message is displayed:

```
XCIM0009E: Error connecting to remote target <host_name>. Exception: java.io.FileNotFoundException:
CTGRI0003E The remote path name specified cannot be found: file_or_directory_path>.
Cause: com.starla.smb.SMBException: The network name is incorrect.
```

Follow these steps to enable administrative sharing:

1. Click **My Computer**.
2. Right click the disk drive that you are enabling for administrative sharing.
3. Click **Sharing and Security**.
4. Select **Share this folder**.
5. Specify the share name, such as C$ or D$, and click **OK**.

Vista Windows 7 2008

Connecting to Windows Vista, Windows 7, or Windows 2008 Server R2 targets

To connect to Windows Vista, Windows 7, and Windows 2008 Server R2 targets, use one of the following options. Before you begin, ensure that the Remote Registry in Windows Services is started, and port 445 is unblocked in the firewall.

1. Configure both the deployment manager machine and the Windows Vista, Windows 7, or Windows 2008 Server R2 target as members of a Windows domain. Use a user account in that domain, or in a trusted domain, when you connect to the target.
2. Enable and use the built-in administrator account to connect to the target workstation. To enable the built-in administrator account perform the following steps:
   a. Select **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Security Settings** > **Local Policies** > **Security Options**.
   b. Next, double-click **Accounts: Administrator account status**.
   c. Select **Enable**, and click **OK**.
3. Disable the User Account Control that is enabled by default if you are using a different user account to connect to the target workstation. To disable User Account Control perform the following steps:
   a. Select **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Security Settings** > **Local Policies** > **Security Options**.
   b. Next, double-click **User Account Control: Run all administrators in Admin Approval Mode**.
   c. Select **Disable**, and click **OK**.

Note: For the configuration changes to take effect, you must restart the workstation.

Linux and UNIX target requirements

The centralized installation manager, through RXA, uses SSH Version 2 to access UNIX and Linux target workstations. This usage requires the use of either OpenSSH 3.6.1 (or, if accessing AIX targets, OpenSSH 4.7), or Sun SSH 1.1 on the target hosts.

Note that OpenSSH 3.7.1, or higher, contains security enhancements not available in earlier releases, and is recommended.

Note: OpenSSH Version 4.7.0.5302 for IBM AIX Version 5.3 is not compatible with Remote Execution and Access Version 2.3. If your target systems are running AIX Version 5.3 with OpenSSH Version 4.7.0.5302 installed, the file transfer might stop in the middle of the transfer. To avoid this problem, revert the OpenSSH version from Version 4.7.0.5302 to Version 4.7.0.5301.

Using Secure Shell (SSH) protocol

Remote Execution and Access does not supply SSH code for UNIX operating systems. You must ensure SSH is installed and enabled on any target you want to access using CIM.

In all UNIX environments except Solaris, the Bourne shell (sh) is used as the target shell. On Solaris targets, the Korn shell (ksh) is used instead due to problems encountered with sh.

To communicate with Linux and other SSH targets using password authentication, you must edit the /etc/ssh/sshd_config file on the targets and set the following property:

```
PasswordAuthentication yes
```

The default value for the `PasswordAuthentication` property is no.

After changing this setting, stop and restart the SSH daemon using the following commands:

```
/etc/init.d/sshd stop
/etc/init.d/sshd start
```

IBM i targets

Use of SSH public/private key authentication to IBM i targets is not supported.

Additional requirements for installing or uninstalling maintenance to previous versions on AIX as a non-root user

Before using the centralized installation manager (CIM) to install or uninstall maintenance on IBM AIX operating systems as a non-root user, you must install and configure *sudo*, an open-source tool, on the target AIX operating systems.

About this task

Complete the installation and configuration operations locally as the root user of the AIX operating systems without using centralized installation manager. You are required to complete the operations only once.

Procedure

1. Download sudo from the IBM AIX Toolbox Download website.
2. Issue the following command to install sudo:

```
rpm -i sudo-*.rpm
```

Note: Some newer versions of sudo might require other packages. In that case, download the package from the same website and install it using a similar command. For example:

```
rpm -i openldap-*.rpm
```

You can download an AIX installp image for the rpm package manager for POWER from the previous download website if your AIX machine does not already have rpm installed.

3. Authorize a non-root user ID, which you specify, to run the slibclean command as a root user without providing a password. Issue the visudo command to add the following entry to the `/etc/sudoers` configuration file:

```
userid ALL = NOPASSWD: /usr/sbin/slibclean
```

4. Log in with the specified user ID, and issue the **sudo -l** command. If successful, a message that is similar to the following example is displayed:

```
User userid may run the following commands on this host: (root) NOPASSWD: /usr/sbin/slibclean
```

If you do not have sudo installed, or sudo is installed but not configured correctly for the specified user ID, error messages are displayed.

Installing packages using the centralized installation manager (CIM) for previous versions

Use the centralized installation manager (CIM) to install one or more packages of previous versions to the specified target workstations.

Before you begin

To successfully install a package, you must first define an *installation target*, which is the remote workstation on which selected software packages might be installed. By default, all of the workstations that contain nodes that are defined in the cell are displayed as installation targets.

Note: The CIM does not install maintenance on the deployment manager. Instead, use the Installation Manager to apply maintenance to the deployment manager.

During the installation process, the wizard prompts you to select an authentication method which is either user name and password or Secure Shell (SSH) public/private key. If you choose to use the SSH public/private key method, you must first create a pair of public/private keys and install the public key on all the installation targets. Read the “Managing installation targets" topic for details.

You must first create the repository to use the features of the CIM. If you did not create the repository during the product installation, you can still set up the CIM repository and add the binary installation images to the repository using the Installation Factory. Ensure that the CIM repository is populated with the installation image for the components that you want to install on the remote workstations. For more information on the steps to populate the CIM repository, refer to the "Getting started with the centralized installation manager" topic for more information.

About this task

The number of steps to complete this task can vary depending on the type of installation package that you choose to install.

Procedure

1. Access the wizard from the administrative console.
   a. Click **System administration** > **Centralized Installation Manager** > **Available installations**.
   b. Select a package type, which is the type of installation you want to perform. For example, you can choose to complete a product installation, or an installation that applies various types of maintenance files.
   c. Next, select an installation package. If you choose a package that includes available features, select each feature from the feature list. This list is not displayed if you choose an installation package that does not include available features.

      Note: To deselect any selected feature from the feature list, press `Ctrl` while you click the selected feature.
   d. Click **Show installation targets** to populate the table with a list of applicable target workstations on which to install the selected software package.
   e. Select one or more installation targets from the list, and click **Install** or **Install Using Response File** to start the Installation wizard.

   Not all installation packages support response files. The **Install Using Response File** button is disabled if that installation package does not support response files.
2. Accept the license agreement. Click **View License Agreement** to read the agreement and accept the terms. Click **Next** to continue.
3. Select an authentication method to access the installation target, and click **Next**. You can choose to use either the Secure Shell (SSH) public/private key method, or the user name and password method to authenticate.
4. Provide the authentication settings, and click **Next**.

   Depending on the authentication method that you choose in step 3, provide the appropriate user name and password for one or more installation targets, or provide the location of the SSH private key file and password on the deployment manager.

If you choose to authenticate using the user name and password method, you can provide a common user name and password to access all of the installation targets, or you can configure unique user names and passwords for each target.

Note: Do not use the browser to save the user name and password. The browser might offer the same user name and password on different target names.

5. Optional: If you choose to install using a response file, you can click **Browse** to locate the response file in the deployment manager. For security reasons the browse function is restricted to browse response files in the *app_server_root*/`cim/responsefiles` directory and any subdirectories below it.

   The passwords specified in the response file may optionally be encoded using the ResponseFilePasswordEncoder utility. The following script files for running the utility are located in the *app_server_root* /`bin` directory:

   - AIX HP-UX Linux Solaris `ResponseFilePasswordEncoder.sh file_name password_keys_list [-Backup | -noBackup]`
   - Windows `ResponseFilePasswordEncoder.bat file_name password_keys_list [-Backup | -noBackup]`

   The *password_keys_list* element is a list of password keys (delimited by comma) for which the password values are to be encoded.

   The `-Backup` option is an optional argument for making a backup copy of the response file to be encoded. The default option is `-noBackup`.

   For example:

   - AIX HP-UX Linux Solaris To encode the password values in the response file, responsefile.nd.txt, identified by the keys `PROF_importSigningCertKSPassword` and `PROF_importPersonalCertKSPassword`, enter:

```
./ResponseFilePasswordEncoder.sh responsefile.nd.txt PROF_importSigningCertKSPassword,PROF_importPersonalCertKSPassword
```

   - Windows To encode the password values in the response file, responsefile.nd.txt, identified by the keys `PROF_importSigningCertKSPassword` and `PROF_importPersonalCertKSPassword` and to keep a back-up copy of the original response file, enter:

```
ResponseFilePasswordEncoder.bat responsefile.nd.txt PROF_importSigningCertKSPassword,PROF_importPersonalCertKSPassword -Backup
```

   Invalid arguments in the command line cause the utility to display the command usage information.

6. Specify the installation location and the working location of each installation target, and click **Next**.

   The installation location is the remote location of the installation target where the package will be installed.

   The working location specifies the directory on the remote target where the CIM will transfer the binary installation files from its repository to the target for subsequent installation on the target.

   Make sure you have enough disk space on both the installation location and the working location. The space required in the installation and working location varies by installation packages. CIM transfers the binary files for the selected installation package from the repository and extracts the content of the binary files into the working location.

7. Specify other command parameters.

   The Installation wizard is a generic wizard for all installation packages that the CIM supports. In addition to the standard installation location parameter, a particular installation package might have zero or more command parameters that require user input. Specify values for these parameters as needed or take the default values.

8. Read the installation summary, and click **Finish** to submit the installation request to the CIM for processing.

Results

You completed the steps to install one or more packages to the specified target workstations. The CIM receives your installation request, processes the information that you provided, and then installs the package to the workstations.

Note:

- The CIM only works on nodes that are part of a deployment manager cell. If you use a response file to install WebSphere Application Server Version 7.x, whether a profile is created and federated to the cell is entirely controlled by the response file. After you have installed a target node, you must federate the target node to the deployment manager in order for the CIM to perform operations against it.
- If you use the CIM to install WebSphere Application Server Version 7.x on a machine that is not yet part of the cell and do not use a response file, the CIM automatically creates a custom profile after completing the installation. The CIM then federates the newly defined node to the cell.
- You might encounter a time out error when installing WebSphere Application Server Version 7.0 to a node using CIM that is similar to the following example:

```
XCIM0203E: The installation command [install -silent -OPT silentInstallLicenseAcceptance="true"  -OPT installType="installNew"
-OPT installLocation="/QIBM/ProdData/WebSphere/AppServer" -OPT  disableOSPrereqChecking="false" -OPT profileType="none"
-OPT feature="languagepack.console.all"  -OPT feature="languagepack.server.all" -OPT defaultProfileLocation="/QIBM/UserData/WebSphere/AppServer"]  timed out.
```

  You can modify the default time out value in the descriptor file `InstallPackageND70X.xml`, located at `<WAS_HOME>/properties/cim`. Open `InstallPackageND70X.xml` in a text editor and locate the *<InstallCmd TimeoutInSecs="1800">* tag. The default time out value is 1,800 seconds (30 mins). To install WebSphere Application Server version 7.0 on IBM i nodes, change the time out value to 5,400 seconds (90 mins). Save the changes and restart the deployment manager.

What to do next

In the administrative console, check the status of your pending requests on the Installations in Progress page, and review the log files of your submitted installation requests from the Installation History page. Read the details about the options that you can use to further monitor the progress of each request.

From the Installation History panel you can click **View Details** to display a panel with additional details on the results. Links to log files on the remote targets are included. However, those logs might be moved, replaced, or deleted if they are not viewed immediately after an installation operation.

Installing Version 6.1.x and 7.x customized installation packages (CIPs) using the centralized installation manager (CIM)

Consider the following information when using the centralized installation manager (CIM) with customized installation packages (CIPs).

Note: This topic applies to WebSphere Application Server Version 6.1.x and 7.x only. For information about using centralized installation manager (CIM) for Version 8.0, see “Submitting Installation Manager jobs” on page 292.

WebSphere Application Server Version 7.0 customized installation packages

You can install WebSphere Application Server Version 7.0 CIPs using centralized installation manager. For a new installation, you can either click the **Install** button or the **Install with response file** button on the Available Installation page.

A *slip installation* of a CIP means that you are installing a CIP on top of an existing product or component. For a slip installation of a CIP, you must use a response file. Click the **Install with response file** button on the Available Installations page. After you complete a slip installation, you cannot use centralized installation manager to roll back the slip installation.

To uninstall WebSphere Application Server Version 7.0 that was installed using a CIP, you can select either the WebSphere Application Server Network Deployment Version 7.0 package or the WebSphere Application Server CIP as the installation package. Clear all features under **Select optional features**. Click the **Show Uninstallation Targets** button. Select one or more targets from the table, and click

Uninstall to launch the wizard. Any CIP can be used to uninstall all platforms of WebSphere Application Server Version 7.0 from workstations that are part of the Network Deployment cell.

Note: This topic references one or more of the application server log files. Beginning in WebSphere Application Server Version 8.0 you can configure the server to use the High Performance Extensible Logging (HPEL) log and trace infrastructure instead of using `SystemOut.log` , `SystemErr.log`, `trace.log`, and `activity.log` files or native z/OS logging facilities. If you are using HPEL, you can access all of your log and trace information using the LogViewer command-line tool from your server profile bin directory. See the information about using HPEL to troubleshoot applications for more information on using HPEL.

WebSphere Application Server Version 6.1 customized installation packages

Centralized installation manager does not support the installation of WebSphere Application Server Version 6.1 CIPs. Instead, use the fix packs to upgrade your WebSphere Application Server.

Troubleshooting

You might experience a timeout situation when attempting to install a CIP with customized scripts from the CIM. For example, consider a CIP that consists of WebSphere Application Server Version 7.0 and a large custom tar file with associated custom scripts. You must first add the CIP to the CIM repository. At this point you can install the CIP to a remote server. However, the installation might fail with the following error:

```
XCIM0203E: The installation command [install -silent -OPT ..............] timed out.
```

It appears that the custom script that runs at the end of the installation takes a long time to complete its tasks which causes the timeout. There is a way to change the timeout value used by CIM for the CIP.

The installation timeout value used by CIM for the CIP is specified in the CIM descriptor for the CIP. When you add the CIP to the CIM repository using the IBM WebSphere Installation Factory, a copy of the descriptor file is placed in the *<CIM_repository_root>*`/descriptors` directory. The descriptor file controls how CIM is to handle the remote installation of the CIP including the timeout value to use for different commands. Each CIP has its own descriptor file with a name that identifies the CIP. For example, if the CIP directory name is `com.ibm.torolab.ND70_AIX_PPC32_1.0.0.0`, then the descriptor file for the CIP is named `InstallPackageND70X_com.ibm.torolab.ND70_AIX_PPC32_1.0.0.0.xml`. The timeout value that CIM uses for the installation command is specified by the `TimeoutInSecs` attribute of the `InstallCmd` element. For example:

```
<InstallCmd  TimeoutInSecs="1800">
```

This specifies a timeout value of 1800 seconds.

To force CIM to use a larger timeout value, update the value within the quotes, save the file, and retry the installation. It is strongly recommended that you make a copy of the descriptor file in a separate place and do not attempt any other changes. There is no need to restart the deployment manager to make the change effective. If you are using a response file to install the CIP using CIM, you may want to verify that the preset timeout value for installation with a response file is sufficient for this CIP. The timeout value that CIM will use for the installation of the CIP using a response file is specified by the `TimeoutInSecs` attribute of the `InstallWithRespFileCmd` element. For example:

```
<InstallWithRespFileCmd  TimeoutInSecs="7200" .......>
```

This specifies a timeout value of 7200 seconds.

The preset timeout value for installation with response file is longer because installation with response file could potentially include creation of profiles and federation of the node to a cell in a single invocation of the install command to the remote server. This larger timeout value may be sufficient for the CIP without modification. If you no longer see the CIP in the CIM's Available Installations panel after making the above change, it means you have likely made a mistake in your editing and the descriptor file has become invalid. Compare the changed file with the original copy you saved to make sure that is the only change you made or check the deployment manager's SystemOut.log for any error messages. Correct the error and retry. Note that if you populate the CIP to another CIM repository using the IBM WebSphere Installation Factory, then the same change has to be made to the CIM descriptor for the CIP in the descriptors directory of that other repository.

Installing Version 6.1.x and 7.x interim fixes using the centralized installation manager (CIM)

Install selected interim fixes to specific installation targets using the centralized installation manager (CIM) to update your product environment.

Before you begin

Note: This topic applies to WebSphere Application Server Version 6.1.x and 7.x only. For information about using centralized installation manager (CIM) for Version 8.0, see “Submitting Installation Manager jobs” on page 292.

You must download the following items to the CIM repository before you can complete this task:

- The binary files for one or more interim fixes

You do not need to install the Update Installer after you have downloaded it. The CIM automatically installs the Update Installer before installing any refresh packs, fix packs or interim fixes if the target does not have the Update Installer already installed.

The descriptors for an interim fix package type are installed when you install WebSphere Application Server Network Deployment Version 8.0. These specific descriptors are included to apply the following types of updates:

- Maintenance for WebSphere Application Server Network Deployment Version 6.x
- Maintenance for WebSphere Application Server Network Deployment Version 7.x

For details on how to locate the descriptor and associated files, read the "Downloading package descriptors and the associated binary files" topic.

By default, all of the workstations containing nodes that are defined in the cell are displayed as installation targets. You can only install interim fixes on targets that are part of the cell. During the installation process, the wizard prompts you to select an authentication method, either user name and password or Secure Shell (SSH) public/private key. If you choose to use the SSH public/private key authentication method, you must first create a pair of keys and install the public key on all the installation targets to successfully complete this task.

Before installing an interim fix to any targets, you must install the same interim fix to the deployment manager first, if the interim fix is applicable to the deployment manager node.

For WebSphere Application Server Version 7.x nodes, CIM can detect what interim fixes have been installed. If you select an interim fix that has been previously installed to a node, that node is not available for selection.

For WebSphere Application Server Version 6.x nodes, you can still select nodes that have the interim fix installed, but you are notified that the interim fix has been previously applied on the Installation history page.

About this task

The CIM relies heavily on remote node information maintained locally on the deployment manager node. This remote node information (namely the node-metadata.properties file) for each node is refreshed every time the node agent on the remote node starts and provides the centralized installation manager with up-to-date information regarding the WebSphere products and versions that are installed on the target nodes.

One example of how the node-metadata.properties information is being used by the CIM is in the filtering of nodes that might be selected for the installation of an interim fix.

Assume you have downloaded an interim fix for the Feature Pack for Web Services to the CIM repository to be installed on remote node. CIM looks at the information contained within the interim fix and determines that the fix is only applicable for nodes that have the Feature Pack for Web Services Version 6.1.0.9 or higher installed. CIM then checks the node-metadata.properties of all the nodes within the cell to determine which of the remote nodes meet the requirement for this interim fix. This process allows the cell administrator to see which nodes are potential candidates for this update and then initiate the installation of the interim fix on one or all the candidate nodes. Because of the availability of the node-metadata.properties on the deployment manager node, you could use CIM to perform this filtering without accessing the target nodes. The node agent process that runs on each node ensures that the node-metadata.properties files of the nodes on the deployment manager are kept up-to-date.

For this reason, if you apply maintenance to the node or install new WebSphere products (such as the Feature Pack for Web Services) outside of CIM on the remote node, you must restart the node agent process after the installation to get the deployment manager copy of the node-metadata.properties of the node up to date.

In addition, for the case of installing a new WebSphere product on the remote 6.1 nodes you **must** take one of the following two steps:

- If the product you are installing supports profile augmentation, augment an existing profile for an already federated node.
- If the product you are installing does not support augmenting an existing profile or you prefer not to augment an existing profile, then create a new profile using a profile template for the new product (for example, a Feature Pack for Web Services profile) thereby creating a new node. Federate this new node to the current deployment manager cell.

After the profile is augmented or a new one is created and federated to the cell, the node agent must be started to make the updated or new node-metadata.properties file that contains the new product information available to the deployment manager node. Unless this is done, CIM, running on the deployment manager node, has no knowledge of the new product that has been installed on the remote host and cannot perform the filtering correctly.

Complete the following steps to install recommended interim fixes for WebSphere Application Server Network Deployment Version 6.x or 7.x.

Procedure

1. Access the wizard from the administrative console.
   a. Click **System administration** > **Centralized Installation Manager** > **Available installations**.
   b. Select **Interim fix** as the package type. Next, select one of the following maintenance installation packages.
      - Maintenance for WebSphere Application Server Network Deployment 7.x
      - Maintenance for WebSphere Application Server Network Deployment 6.x

If you previously downloaded any interim fixes by using the **Installation Packages** function, the interim fixes are displayed in a list below the **Select one or more maintenance packs** prompt. Select one or more interim fixes from this list.

c. Click **Show installation targets** to populate the table with a list of applicable target workstations on which to install the selected interim fixes. After you select one or more installation targets, click **Install** to start the Installation wizard.

2. Read and accept the license agreement.

   Click **View License Agreement** to read the agreement and accept the terms. Click **Next** to continue.
3. Select an authentication method to access the installation target, and click **Next**. You can select to either use the Secure Shell (SSH) public/private key method or the user name and password method to authenticate.
4. Provide your authentication information, and click **Next**.

   Depending on the authentication method that you choose in the previous step, provide the appropriate user name and password for one or more installation targets, or provide the location of the SSH private key file and password on the deployment manager.

   If you choose to authenticate by using the user name and password method, you can provide a common user name and password to access all of the installation targets, or you can configure unique user names and passwords for each target.
5. Verify the installation and the working locations of each installation target, and click **Next**.

   The installation location is the remote location of each installation target in which the interim fixes are to be installed. The working location specifies the directory on the remote target where the files are sent before the package is installed in the specified location.

   Make sure you have enough disk space in both the installation location and the working location. The space required in the installation and working location varies by installation packages. The CIM transfers the selected interim fix files and the Update Installer binary file if necessary from the repository to the working location.
6. Read the installation summary, and click **Finish** to submit the installation request to the CIM for processing.

Results

Your installation request is sent to the CIM for processing. The Update Installer is automatically installed to the selected targets if the Update Installer is not found on the targets.

To check the status of your request, click **Installations in progress** in the administrative console.

Troubleshooting

- The following message is displayed if you attempt to install an interim fix without having a copy of the IBM Update Installer for WebSphere Software in your CIM repository:

```
The installation binary files required for the install_package_name or its dependent package
Update Installer for WebSphere Application Server for workstation_platform do not exist.
```

- If you are trying to use CIM to install an interim fix for the Feature Pack for Web Services on a WebSphere Application Server Version 6.1 or 7.x host in your Version 8.0 Network Deployment cell, the **Show Installation Targets** function on the CIM Available installations panel might not list the host as an available installation target. WebSphere Application Server Version 6.1 or 7.x Feature Pack installations without a profile created for the environment are not visible to CIM as installed products on the target host. To make the deployment manager and CIM aware that the Version 6.1 or 7.x feature pack is installed, you must create a Feature Pack for Web Services profile and federate the defined node to the deployment manager.

What to do next

Click **Installation history** in the administrative console to review the log files for each of the installation requests that you submit.

From the Installation History panel the administrator can click **View Details** to display a panel with additional details on the results. Links to logs on the remote targets are included. However, those logs can be moved, replaced, or deleted by other users or administrator, if they are not viewed immediately after an installation operation.

Installing refresh packs or fix packs for previous versions using the centralized installation manager (CIM)

Install recommended fix packs or refresh packs to specific installation targets using the centralized installation manager (CIM) to update your product environment.

Before you begin

You must download the following items to the centralized installation manager repository before you can complete this task:

- Installation package descriptor and binary files for a refresh pack or fix pack

For details on how to locate the descriptor and associated files, read the "Downloading package descriptors and the associated binary files" topic.

You do not need to install the Update Installer after you have downloaded it. The centralized installation manager automatically installs the Update Installer before installing any refresh packs, fix packs or interim fixes if the target does not have the Update Installer installed.

By default, all of the workstations containing nodes that are defined in the cell are displayed as installation targets. During the installation process, the wizard prompts you to select an authentication method, either user name and password or Secure Shell (SSH) public/private key. If you choose to use the SSH public/private key method, you must first create a pair of keys and install the public key on all the installation targets to successfully complete this task.

Before installing a refresh pack or fix pack to any targets, you must install the refresh pack or fix pack to the deployment manager first, if it is applicable. The deployment manager must have the highest level of refresh pack or fix pack in the cell.

Attention: Fix packs that include updates to the Software Development Kit (SDK) might overwrite unrestricted policy files. Back up unrestricted policy files before you apply a fix pack and reapply these files after the fix pack is applied.

About this task

The centralized installation manager supports the installation of Network Deployment Version 6.x and 7.x fix packs on remote nodes that are within the Network Deployment cell. This configuration is known as a mixed-version cell where the deployment manager node is at Version 8.0 or higher and the other nodes within the cell are either at the same level as the deployment manager node or at the Version 6.x or 7.x level.

CIM does not support maintenance levels below Version 6.1.

The content of these CIM-defined Network Deployment Version 6.1 Fix Packs include the following individual fix packs for the distributed platforms and Windows:

- WebSphere Application Server fix pack

- Java Software Developer Kit (SDK) fix pack
- WebSphere Application Server Feature Pack for Web Services fix pack
- WebSphere Application Server Feature Pack for EJB 3.0 fix pack

For IBM i targets, the CIM-defined Network Deployment Version 6.1 Fix Packs are the same but without the Java SDK fix pack.

With the CIM-defined Network Deployment Version 6.1 Fix Packs preloaded in the CIM repository, the cell administrator can specify the remote nodes that the CIM-defined Network Deployment Version 6.1 Fix Pack is to be installed in. CIM determines whether any of the two Feature Pack fix packs are required and only sends the necessary ones to the target nodes for installation. Since both Network Deployment Version 6.1 Fix Pack 15 and 17 specify that a mandatory Interim Fix, PK53084, must be installed on the target if the Feature Pack for Web Services is installed, CIM also performs a check before allowing the installation of Fix Pack 15 and 17 to proceed.

CIM supports the uninstallation of the CIM-defined Network Deployment Version 6.1 Fix Pack from the target nodes, if the Fix Pack was installed through CIM and the CIM-defined Fix Packs are still in the CIM repository. Note that for uninstallation operations, CIM expects that the Update Installer tool is already installed on the target nodes. If the Fix Pack was originally installed using CIM, both of these conditions are automatically satisfied.

Lastly, CIM uses the Update Installer for WebSphere Application Server Version 7.0 to install and uninstall the CIM-defined Network Deployment Version 6.1 Fix Packs.

Complete the following steps to install recommended fix packs or refresh packs for WebSphere Application Server Network Deployment Version 6.1 or 7.0.

Procedure

1. Access the wizard from the administrative console.
   a. Click **System administration** > **Centralized Installation Manager** > **Available installations**.
   b. Select **Refresh pack, fix pack, or maintenance tool** as the package type. Next, select the specific installation package that contains the refresh pack or fix pack that you want to install on the remote workstations.
   c. Click **Show installation targets** to populate the table with a list of applicable target workstations on which to install the selected package. After you select one or more installation targets, click **Install** to start the Installation wizard.
2. Read and accept the license agreement.

   Click **View License Agreement** to read the agreement and accept the terms. Click **Next** to continue.
3. Select an authentication method to access the installation target, and click **Next**. You can select to either use the Secure Shell (SSH) public/private key method or the user name and password method to authenticate.
4. Provide your authentication information, and click **Next**.

   Depending on the authentication method that you choose in the previous step, provide the appropriate user name and password for one or more installation targets, or provide the location of the SSH private key file and password on the deployment manager.

   If you choose to authenticate by using the user name and password method, you can provide a common user name and password to access all of the installation targets, or you can configure unique user names and passwords for each target.
5. Verify the installation and the working locations of each installation target, and click **Next**.

   The installation location is the remote location of each installation target in which the package is to be installed. The working location specifies the directory on the remote target where the files are sent before the package is installed in the specified location.

Make sure you have enough disk space in both the installation location and the working location. The space required in the installation and working location varies by installation packages. The centralized installation manager transfers the selected refresh pack or fix pack files and the Update Installer if necessary from the repository to the working location.

6. The Update Installer on the targets is updated to the latest version from the repository automatically, if required. Clear the check box if you do not want the Update Installer on the targets to be updated.
7. Read the installation summary, and click **Finish** to submit the installation request to the CIM for processing.

   Note: Any interim fixes that you previously installed on the remote targets are uninstalled by the Update Installer prior to installing the refresh pack or fix pack. If the refresh pack or fix pack does not include the official fixes that were included in the removed interim fixes, you must reinstall the interim fixes after you install the refresh pack or fix pack.

Results

Your installation request is sent to the CIM for processing. To check the status of your request, click **Installations in progress** in the administrative console.

Troubleshooting

- The following message is displayed if you attempt to install an interim fix without having a copy of the IBM Update Installer for WebSphere Software in your CIM repository:

```
The installation binary files required for the install_package_name or its dependent package
Update Installer for WebSphere Application Server for workstation_platform do not exist.
```

- If you are trying to use CIM to install an interim fix for the Feature Pack for Web Services on a WebSphere Application Server Version 6.x or 7.x host in your Version 8.0 Network Deployment cell, the **Show Installation Targets** function on the CIM Available installations panel might not list the host as an available installation target. WebSphere Application Server Version 6.1 Feature Pack installations without a profile created for the environment are not visible to CIM as installed products on the target host. To make the deployment manager and CIM aware that the Version 6.x or 7.x feature pack is installed, you must create a Feature Pack for Web Services profile and federate the defined node to the deployment manager. For feature packs installed on Version 8.0 application server hosts this is not necessary because CIM has added support to handle this situation.

What to do next

Click **Installation history** in the administrative console to review the log files for each of the installation requests that you submit.

From the Installation History panel the administrator can click **View Details** to display a panel with additional details on the results. Links to logs on the remote targets are included. However, those logs can be moved, replaced, or deleted by other users or administrator, if they are not viewed immediately after an installation operation.

Monitoring requests to the centralized installation manager (CIM) for previous versions

After you submit one or more requests to the centralized installation manager (CIM), you can monitor the progress of and view specific details about each installation and uninstallation request.

About this task

In the administrative console, the **Installations in Progress** and **Installation History** panels provide you with information on the status of the installation and uninstallation requests that you submit to the centralized installation manager for processing. However, each panel provides you with different options for using that information to monitor and manage your requests. The **Installations in Progress** panel provides you with options to view and monitor the progress of each request. You can also cancel any pending requests from this panel. From the **Installation History** panel, you can monitor the completion status, delete the history records, and access the error messages and log files of each completed request.

- Monitoring the progress of requests

  Complete the following steps to monitor the progress of requests:

  1. Click **System administration** > **Centralized Installation Manager** > **Installations in Progress** in the administrative console.
  2. Review the table for specific details about each request, which are described in the following list:
     - `Host name` specifies the name of the workstation on which the request is performed.
     - `Operation` specifies the type of request, such as install, uninstall, or install SSH public key.
     - `Package and Features` specifies the name of the software package and any accompanying features that make up the installation request.
     - `Creation time` specifies the date and time you submit the request.
     - `Status` specifies the progress of the request.
  3. You may optionally cancel a request if it has not started. Select one or more rows from the table, and click **Cancel Pending Request** to cancel only the requests that are not yet started.

     Review the confirmation panel, and click **OK** to return to the **Installations in Progress** page.

- Viewing completion status and request details

  Complete the following steps to view the completion status and details of requests:

  1. Click **System administration** > **Centralized Installation Manager** > **Installation History** in the administrative console.
  2. Review the table for specific details about each request. The table that is displayed on this page lists the same descriptive information as the table on the Installations in Progress page, except the status is displayed as one of the following completion types:
     - Succeeded
     - Failed
     - Installation completed, but errors detected
     - Uninstallation completed, but errors detected
  3. Click **Remove** to delete the history records from the deployment manager. Review the confirmation panel, and click **Remove** again.
  4. Click **View details** to view the log files and any error messages. A new page now displays any errors that might have occurred, and the links to the actual log content.
     a. Click the specific link to read the content of a log file. If you previously deleted the log files from the remote workstation, an error message is displayed. If you replace existing log files with new ones, the updated content is displayed.
     b. Click **OK** to return to the Installation History page.

What to do next

Return to the Available Installations page to resubmit a canceled or failed request, or submit a new request to the CIM.

In the case of certain failed requests, you might need to correct the error on the remote workstations before resubmitting the requests. For installations that are partially successful, examine the logs to correct the problem. You can manually complete the remaining installation steps. With this option, you do not need to resubmit the requests. Alternatively, if the failure state of the request is closer to the starting state, you can return the workstation to the starting state before you resubmit the requests.

Uninstalling packages for Version 6.1.x and 7.x using the centralized installation manager (CIM)

Use the centralized installation manager (CIM) to uninstall a previously installed package from the target workstation.

Before you begin

The wizard prompts you to select an authentication method, either user name and password or Secure Shell (SSH) public/private key. If you choose to use the SSH public/private key method, you must first create a pair of keys and install the public key on all the installation targets.

About this task

The number of steps for this task can vary depending on the type of installation package you choose to uninstall.

Procedure

1. Access the wizard from the administrative console.
   a. Click **System administration** > **Centralized Installation Manager** > **Available installations**.
   b. Select a package type and an installation package. Depending on the package that you choose, you can choose to uninstall maintenance packs.
   c. Click **Show uninstallation targets** to populate the table with a list of applicable target workstations from which to remove the selected software package. After you select one or more uninstallation targets, click **Uninstall** to start the wizard.
2. Select an authentication method to access the installation target, and click **Next**. You can choose to use the Secure Shell (SSH) public/private key method or the user name and password method to authenticate.
3. Provide the authentication settings, and click **Next**. Depending on the authentication method that you choose in the previous step, provide the appropriate user name and password for one or more installation targets, or provide the location of the SSH private key file and password on the deployment manager.

   If you choose to authenticate by using the user name and password method, you can provide a common user name and password to access all of the installation targets, or you can configure unique user names and passwords for each target. Do not use the browser to save the user name and password. The browser might offer the same user name and password on different target names.
4. Specify the installation location of each installation target, and click **Next**. The installation location is the remote location of the installation target in which the packages are installed.
5. Read the summary, and click **Finish** to submit the request to the centralized installation manager for processing.

Results

Your uninstallation request is sent to the CIM for processing. To check the status of your request, click **Installations in progress** in the administrative console.

Troubleshooting

- If you installed WebSphere Application Server Version 7.0 using a response file on a remote host through the CIM but did not federate the node to the deployment manager, then the **Show Uninstallation Targets** function in the CIM Available installations panel will not list your target host as an available uninstallation target.

  The CIM only works on nodes that are part of the deployment manager cell. Since your node is not federated to the cell, you must run the uninstaller locally to uninstall the server.

What to do next

Click **Installation history** in the administrative console to review the log files for each of the uninstallation requests that you submit.

From the Installation History panel, the administrator can click **View Details** to display a panel with additional details on the results. Links to logs on the remote targets are included. However, those logs can be moved, replaced or deleted by other users or the administrator, if they are not viewed immediately after an uninstallation operation.

Downloading package descriptors and binary files for previous versions to the centralized installation manager (CIM) repository

To enhance your product environment, download additional installation packages and maintenance files to the centralized installation manager (CIM) repository to install later on the remote workstations. Use this topic to manage the installation packages and maintenance files that are located in your CIM repository.

Before you begin

You must first create the CIM repository and add one or more product packages to the repository on the host workstation. For more information, see Adding installation packages of previous versions to the centralized installation manager (CIM) repository using the Installation Factory.

If you do not have direct access to the Internet, then you can set up an FTP gateway and perform the download indirectly through the gateway. Read the "Using CIM download function when the deployment manager does not have direct Internet access" topic for more information.

Alternatively, if you have no access to the Internet whatsoever, you can manually add the packages to the repository. Read the "Manually adding package files to the repository" topic for more information.

About this task

From the **Installation Packages** panel in the administrative console, download the descriptor files and any associated binary files of new or additional installation packages to the CIM repository. You can selectively download only the binary files of the platforms that you might need from the IBM support website. The following list describes the four types of installation packages:

- **Product installation**

  This package type includes WebSphere Application Server Network Deployment Version 7.0. The descriptor and binary files for this installation type are not available to download because the files are included during the installation of the WebSphere Application Server product on the deployment manager host.
- **Refresh packs or fix packs**

  You can download the binary files for this package type based on specific platforms. When a fix pack for the application server is released, it usually comes with a fix pack for the application server and a fix pack for the Java SDK. CIM requires having both fix packs in the repository, and CIM will install both fix packs to all selected targets.
- **Interim fix**

  You can search for an interim fix using its identifying Authorized Program Analysis Report (APAR) number. Specify the APAR number of the interim fix and click **Search** to display a list of files associated with the interim fix and optionally download the binary files.

Complete the following steps to download fix pack descriptors and binary files for fix packs or interim fixes to your CIM repository.

Procedure

1. In the administrative console, click **System administration** > **Centralized Installation Manager** > **Installation Packages**.
2. Click **Add Packages** to download a new installation package descriptor to the centralized installation manager repository if the descriptor is not included in the table displayed from the previous step. The **Download Descriptors** page is then displayed.

   Note: Ensure that the descriptor file for the type of package that you choose is not included as part of the product installation. The installation package descriptors that are included during the product installation are provided in the following list:

   - Maintenance for WebSphere Application Server Network Deployment 7.0
   - WebSphere Application Server Network Deployment 7.0
3. Select one or more descriptor files from the list, and click **Download**.

   After you have confirmed to download the selected descriptor files, they are displayed in the table on the **Installation Packages** panel with the following text:

```
Downloading filename
```

   Click the refresh icon to refresh the contents of the table. After the descriptor file is downloaded, the package name is displayed as a hyperlink.

   To download the binary files for the installation packages in the preceding list, click the name of the descriptor, and proceed to the next step. To download additional package descriptors from the IBM support website, click **Add packages**.
4. Download the binary files from the **Installation Packages** panel.

   You can download the associated binary files of the specific descriptor file that you just downloaded, or you can also download the binary files for the Interim fix package type.

   Determine the type of installation package to download by the viewing the descriptions of each type in the table. The steps to download the binary files differ, depending on the package type.

   - To download the binary files for a refresh pack, fix pack, or maintenance tool package type, complete the following steps:
     a. Click the name of the package in the table. A new page is then displayed.
     b. Select one or more platforms in the table, and click **Download**.
     c. Click **Download** on the confirmation page to start downloading the binaries. After the download process begins, the previous page is then displayed, from which you can check the download status of the files in the third column of the table. Click the refresh icon to refresh the contents of the table, if necessary.
     d. When all the required files have been downloaded, the download status column displays a Completed status.

     If one or more files are missing, the download status column displays an Incomplete status. In this case, you can try to download again. If your status is Incomplete, check for error messages in the *profile_root*/`logs/dmgr/SystemOut.log` file where *profile_root* is the profile location of the deployment manager.

     Note: This topic references one or more of the application server log files. Beginning in WebSphere Application Server Version 8.0 you can configure the server to use the High Performance Extensible Logging (HPEL) log and trace infrastructure instead of using `SystemOut.log` , `SystemErr.log`, `trace.log`, and `activity.log` files or native z/OS logging facilities. If you are using HPEL, you can access all of your log and trace information using the LogViewer command-line tool from your server profile bin directory. See the information about using HPEL to troubleshoot applications for more information on using HPEL.
   - To download the binary files for an interim fix package type, complete the following steps:
     a. Click the name of the package in the table. A new page is then displayed.
     b. Click **Add Files** to go to the **Download Files** page.

c. You can type the specific APAR name (For example, PK55555), and click **Search** to navigate directly to the corresponding FTP location. You can also specify the FTP URL directly, and click **Go** from the **Download Options** section.

d. Click the APAR number, select the individual maintenance files that are contained in the directory, and click **Download**. The binary files are then downloaded to the CIM repository.

e. Click **Download** on the confirmation page to start downloading the binaries.

   After the download process begins, the previous page is then displayed, where you can check the download status of the files in third column of the table. Click the refresh icon to refresh the contents of the table, if necessary.

   If your status is Incomplete, check for error messages in the *profile_root*`/logs/dmgr/SystemOut.log` file where *profile_root* is the profile location of the deployment manager.

Results

The CIM repository now contains maintenance files to install later on the remote workstations.

Using the Version 6.1.x and 7.x centralized installation manager (CIM) download function when the deployment manager does not have direct Internet access

The centralized installation manager (CIM) provides a download function in the administrative console to allow the cell administrator to navigate to IBM support and download the latest version of the IBM Update Installer for WebSphere Software, fix packs and interim fixes. To use this feature, the WebSphere Application Server deployment manager node must have Internet access to the external IBM FTP server.

Before you begin

Note: This topic applies to WebSphere Application Server Version 6.1.x and 7.x only. For information about using centralized installation manager (CIM) for Version 8.0, see “Submitting Installation Manager jobs” on page 292.

You must first create the CIM repository and add one or more product packages to the repository on the host workstation. For more information, read the "Adding the current installation package during installation" topic.

Alternatively, you can use the IBM WebSphere Installation Factory to add one or more product packages to the repository. The Installation Factory is included in one of the WebSphere Application Server Network Deployment discs, which you must install separately. For more details about the Installation Factory, read the "Adding installation packages with the Installation Factory" topic.

About this task

If you do not allow Internet access from your deployment manager workstation, then you can set up an FTP gateway on a workstation that has internet access, point the CIM download URL to that gateway, and do the download indirectly through the gateway. The following section describes how you can set up a simple FTP gateway using a program called DeleGate. You can use other FTP gateway products with similar capability instead.

DeleGate is a multipurpose application level gateway, or a proxy server which runs on multiple platforms (UNIX, Windows and OS/2®). See the DeleGate Home Page for more information.

Alternatively, you can manually add the packages to the repository. Read the "Manually adding package files to the repository" topic for more information.

Perform the following steps to set up DeleGate as an FTP gateway for CIM running on a deployment manager node that does not have direct access to the Internet.

Procedure

1. Download a copy of DeleGate. At the time of writing the latest version is Version 9.7.7.
2. To install the software on Windows operating systems, open and extract the downloaded compressed file, dg9_7_7-fix1.zip, to a directory.
3. Start DeleGate by running dg9_7_7-fix1.exe from the bin directory
4. To start DeleGate as an FTP Gateway for the CIM download function, use the following command on one line:

```
dg -P21 SERVER=ftp   MOUNT="/* ftp://ftp.software.ibm.com/software/websphere/*"
ADMIN=administrator@ftpgate01.mydomain.com PERMIT="*:*:*. mydomain.com"
```

Results

- In the above example, DeleGate is running on host ftpgate01.mydomain.com and it has direct connection to the Internet.
- For convenience, the dg9_7_7-fix1.exe file is renamed to dg.exe so that dg can be used to start DeleGate.
- The `PERMIT` parameter allows access from any host with the domain name, mydomain.com, to access the gateway.
- You can add the " -v " option to make DeleGate run in the foreground with logging to the console to observe activities.
- You can also run DeleGate using arguments loaded from a configuration file with the `+=`*`filename`* option with the specified file holding all the arguments (1 argument per line), for example:

```
dg +=dg.conf
```

With the previous setup, you can then replace ftp://ftp.software.ibm.com/software/websphere with ftp://ftpgate01.mydomain.com anywhere you see **Download Options** in any of the CIM download panels and you will be able to access the IBM Support FTP Server via the FTP gateway.

Note: Expand the Download Options tag to reveal the FTP URL field that you need to replace. Only replace the front portion of the URL as described and keep the remaining portion of the URL string as is.

For example, if the FTP URL field shows the following:

```
ftp://ftp.software.ibm.com/software/websphere/appserv/support/fixpacks/was80/cumulative/
```

Replace it with the following:

```
ftp://ftpgate01.mydomain.com/appserv/support/fixpacks/was80/cumulative/
```

Manually adding package files for previous versions to the centralized installation manager (CIM) repository

This topic explains the directory structure of the centralized installation manager (CIM) repository and outlines the steps to download CIM descriptor files for Version 7.0 fix packs.

Before you begin

To use the centralized installation manager (CIM) download function the deployment manager must have access to the IBM websites. When the deployment manager workstation does not have Internet access, you must first download the descriptors and files to a separate workstation that has Internet access. Then, you must manually transfer those files to the CIM repository before you can use CIM to install the respective maintenance on remote nodes.

Before you complete this task, consider the following issues:

- If you have indirect access to the Internet through another machine, then you can set up an FTP gateway and perform the download indirectly through the gateway instead of manually adding files to the repository. Read the "Using CIM download function when the deployment manager does not have direct Internet access" topic for more information.
- If your deployment manager has direct Internet access, see the information on using the centralized installation manager repository instead of completing the steps in this topic.
- Steps 1 - 4 in this document apply when you have a mixed cell environment, which can consist of Version 6.1, 7.0 and 8.0 nodes in the same cell. The steps in this task enable you to obtain the centralized installation manager descriptors for Version 7.0 fix packs within this mixed cell environment. If you do not have a mixed cell environment or you do not intend to install fix packs for your Version 7.0 nodes in a mixed cell environment, you do not need to download these descriptors.

  Important: In a mixed cell environment, the deployment manager must be at the highest version level in the environment. For example, a Version 7.0 deployment manager cannot manage both Version 7.0 and 8.0 nodes. However, a Version 8.0 deployment manager can manage both Version 7.0 and 8.0 nodes.
- When you use the Update Installer to install a fix pack on the deployment manager, the process does not add the binary *.pak files to the CIM repository. You still need to copy those binary files to the appropriate directory as indicated in the following section.

When you installed Version 8.0, the product installed most of the descriptors for the centralized installation manager that are needed in a mixed cell environment. These previously installed descriptors enable you to install the interim fixes for both Version 6.1 and 7.0. However, the Version 8.0 product does not install the Version 6.1 and 7.0 fix pack descriptors for the centralized installation manager. These steps enable you to obtain those Version 6.1 and 7.0 descriptors when direct Internet access is not available.

You must first create the CIM repository on the host workstation. For more information, read the "Adding the current installation package during installation" topic.

Alternatively, you can use the IBM WebSphere Installation Factory to create the CIM repository and add one or more product packages to the repository. The Installation Factory is included in one of the WebSphere Application Server Network Deployment discs, which you must install separately. For more details about the Installation Factory, read the "Adding installation packages with the Installation Factory" topic.

If the CIM repository was previously created, find out the directory root path to the repository from the administrator who created it. You need that path information to manually copy files to subdirectories under that directory root path. Alternatively, you can obtain the repository directory root path by looking at the value of the CENTRALIZED_INSTALL_REPOSITORY_ROOT property in the `*install_root*/properties/cimgr.props` file for the deployment manager profile.

About this task

The Update Installer and the maintenance files that are required by the CIM to remotely install maintenance are the same tool and files that are used to apply maintenance to the deployment manager workstation. Complete the steps to download the Update Installer and maintenance files without using the CIM.

The repository consists of directories where the installation image for the Update Installer and maintenance files are located. The following information lists the directories and their content. Use a browser on a machine that has internet access to download the binaries for the various WebSphere maintenance files from the following URL: http://www.ibm.com/software/webservers/appserv/was/support/download.html

After you download the respective maintenance files to the file system of the machine, the information in this section enables you to determine the directory in the CIM repository to which you must transfer the files.

WAS70Updates

This directory contains all the interim fixes for WebSphere Application Server Network Deployment Version 7.0. Copy the `.pak` files for all your WebSphere Application Server Network Deployment Version 7.0.0 interim fixes to this directory. You can also remove any `.pak` files that you no longer need from this directory.

WAS70FPn

This directory contains various `.pak` files that make up a specific fix pack for WebSphere Application Server Version 7.0. Refer to the WebSphere Application Server Version 7.0.0 support website for the list of files that are required for each fix pack.

For example, for WebSphere Application Server Network Deployment Version 7.0.0 Fix Pack 1, copy the following `.pak` files to the `WAS70FP1` directory.

- 7.0.0.0-WS-WAS-*platform_architecture*-FP0000001.pak
- 7.0.0.0-WS-WASSDK-*platform_architecture*-FP0000001.pak

ND61Updates

This directory contains all the interim fixes for WebSphere Application Server Network Deployment Version 6.1. Copy the `.pak` files for all your WebSphere Application Server Network Deployment Version 6.1 interim fixes to this directory. You can also remove any `.pak` files that you no longer need from this directory.

ND61FPn

This directory contains the `.pak` files that make up a specific fix pack for WebSphere Application Server Version 6.1. Refer to the WebSphere Application Server Version 6.1 support website for the list of files required for each fix pack.

For example, for WebSphere Application Server Network Deployment Version 6.1 Fix Pack 25, copy the following .pak files into the `ND70FP25` directory:

- 6.1.0-WS-WAS-*platform_architecture*-FP0000025.pak
- 6.1.0-WS-WASSDK-*platform_architecture*-FP0000025.pak
- 6.1.0-WS-WASWebSvc-*platform_architecture*-FP0000025.pak
- 6.1.0-WS-WASEJB3-*platform_architecture*-FP0000025.pak

Note: If you do not plan to install interim fixes or fix packs for a particular release, you do not need to populate the directory.

You can either download the descriptors from an IBM ftp site or import descriptors from a fix pack. Choose one of the following options to manually add the CIM descriptors for Version 6.1 and 7.0 fix packs to the CIM repository:

Procedure

- Download the descriptor from an IBM ftp site.
  1. In the administrative console, click **System administration** > **Centralized Installation Manager** > **Installation Packages**. Click **Add Packages**. The Download Descriptors panel is displayed.
  2. Determine the location of the FTP site from which you download the descriptors. Expand **Download Options** to view the FTP URL that is used by the CIM. The URL format is ftp://ftp.software.ibm.com/software/websphere/appserv/support/cim/cim70_*yyyymmdd*. If the deployment manager workstation does not have Internet access, an error message is displayed indicating that the host name, ftp.software.ibm.com, is not known. You can either download the descriptors from another workstation that has internet access or use descriptors from a previously downloaded fix pack (see Import descriptors from a previously downloaded fix pack).

3. Use the URL from the previous step to download the available descriptors from a separate workstation that has internet access.
4. Transfer the downloaded descriptors to the `CIM_REPOSITORY_ROOT/descriptors` directory on the deployment manager workstation, where *CIM_REPOSITORY_ROOT* is the root directory of the CIM repository, such as `/opt/IBM/WebSphere/cimrepos`.

- Import descriptors from a previously downloaded fix pack.
  1. Extract the InstallPackageND70FPXX.xml file from the .pak file.
  2. Place the InstallPackageND70FPXX.xml file in the cimrepos/descriptors folder.

Results

The CIM repository now contains maintenance files to install later on the target workstations in the cell.

Managing Version 6.1.x and 7.x centralized installation manager (CIM) installation targets

You can add or remove an installation target, which is the workstation on which selected software packages might be installed from the centralized installation manager (CIM). You can also edit the configuration of an existing installation target, and store the administrative ID and password of each target for later use when installing or uninstalling packages.

Before you begin

Note: This topic applies to WebSphere Application Server Version 6.1.x and 7.x only. For information about using centralized installation manager (CIM) for Version 8.0, see “Submitting Installation Manager jobs” on page 292.

You must first create an installation target to install one or more software packages on your workstations. By default, all of the workstations containing nodes that are defined in the cell are displayed as installation targets.

About this task

From the **Installation Targets** page in the administrative console, you can add additional installation targets that are located outside of the cell. For example, you can install the middleware agent on a node that is running other middleware servers that were created outside of the product cell by adding the remote workstation as a new installation target. Other tasks that you can complete to further manage your installation targets include removing installation targets, editing the configuration of installation targets, and installing a Secure Shell (SSH) public key on installation targets. To access this page, click **System administration** > **Centralized Installation Manager** > **Installation targets**.

- **Adding targets:** To add additional installation targets that are located outside of the cell, click **Add Installation Target**. The configuration page is displayed next.
  1. Provide the fully qualified host name and platform of the installation target.

     It is important that you specify the domain-qualified host name rather than a short host name. This is especially important if you will be installing WebSphere Application Server on the remote target because the value specified will be used in the configuration of the node.
  2. Specify the administrative ID and password, which the centralized installation manager later uses to install one or more packages on the installation target.

     Do not use the browser to save the user name and password. The browser might offer the same user name and password on different target names.
  3. Click **Test Connection** to test the connection using the administrative ID and password that you provide.

4. Click **OK** after you specify the configuration settings to return to the **Installation targets** page. The new installation target is now displayed in the table.

- **Removing targets:** To remove existing installation targets, select one or more targets from the table, and click **Remove Installation Target**. The confirmation page then lists each selected installation target. Click **Remove** to complete the action, and to return to the **Installation targets** page.
- **Edit target configuration settings:** To edit the configuration settings of an existing installation target, click the host name. The configuration page is displayed next.
  1. Edit any of the configuration settings that are displayed on the page, which are the same fields that you complete to configure a newly created installation target.
  2. Click **OK** after you complete your changes to return to the **Installation targets** page. Any changes that you make now display in the table.
- **Securing targets:** To install a Secure Shell (SSH) public key on specific installation targets, select one or more targets from the table, and click **Install SSH Public Key**.

  As a result, the wizard is then launched to complete the SSH public key installation process. The actual wizard steps are further explained in the "Installing a Secure Shell public key" topics. Refer to those topics for the detailed wizard instructions, and for more information on accessing your remote workstations by using the SSH public/private key pair authentication method.

Results

Troubleshooting

- Windows You might receive the following error trying to connect to your Windows workstation using a non-administrator user ID and password:

```
XCIM0010E: An error occurred while connecting to the remote target ip_address.
Cause: CTGRI0011E An error occurred when accessing the remote registry or service control manager.
```

  Many operations that CIM performs require access to resources that are not generally accessible by ordinary user accounts. Therefore, the account names that you use to log onto remote Windows machines must have administrative privileges. The simplest way is to add the user account to the Administrators group using the following steps:

  1. Right click **My Computer** from your Windows desktop and select **Manage**.
  2. Expand **Local Users and Groups** on the resulting Computer Management windows and select the **Users** folder.
  3. On the right panel, double-click the user account to open the Properties window for that account.
  4. Select the **Member Of** tab, and add the **Administrators** group to the list of groups that this account belongs to.

What to do next

You can now begin installing packages to specific installation targets. For more information on the different types of available installation packages, read a description about each in the "Installing packages using the centralized installation manager" topics.

Installing a Secure Shell (SSH) public key to access remote workstations for Version 6.1.x and 7.x

To use Secure Shell (SSH) public/private key as an authentication method for accessing your remote workstations, you must first install the public key of a public/private key pair on the installation targets. You can then securely connect to the remote workstation by using the corresponding private key. Use this topic to install the SSH public key on one or more installation targets.

Before you begin

Note: This topic applies to WebSphere Application Server Version 6.1.x and 7.x only. For information about using centralized installation manager (CIM) for Version 8.0, see “Submitting Installation Manager jobs” on page 292.

To successfully complete this task, you must have SSH installed and enabled on the installation target. First create a pair of keys, and install the public key on all the installation targets. Issue the following command to ensure that SSH is started on the workstation:

```
ps -e | grep sshd
```

You can generate an RSA private key and its corresponding public key using the ssh-keygen command in the following example:

```
ssh-keygen -t rsa
```

Take the default location for storing the private key and make note of it. If you specify a non-empty string for the passphrase prompt, make sure you remember the string because you will need it when you want to use the generated private key.

Additionally, you must know the location of the SSH public key file on the deployment manager, and the administrative ID and password for the installation target. This is the same administrative ID and password that you use to later install or uninstall software packages on the same installation target.

About this task

UNIX and Linux platforms generally support the use of SSH protocol. For Windows operating systems, however, you might have to install third-party software to use SSH protocol. Read the "Using the Secure Shell authentication method on target Windows operating systems" topic for more information.

With the centralized installation manager (CIM) , you can install product packages and maintenance for distributed platforms directly from the administrative console. Complete the steps that are outlined in the wizard to install the SSH public key, which uses the SSH protocol to communicate with the installation targets.

Procedure

1. To access the wizard from the administrative console, click **System administration** > **Centralized Installation Manager** > **Installation targets**.
2. Select one or more existing installation targets from the table, and click **Install SSH Public Key**.
3. Select the appropriate password settings, and click **Next**. You can either select to specify the same user name and password to access all of the installation targets, or you can configure individual user names and passwords for each installation target.
4. Specify the location of the SSH public key file on the deployment manager, and click **Next**.
5. Review the summary of your selections, and click **Finish** to complete the installation process. Click **Previous** to change any of your selections.

Results

You successfully installed the SSH public key on specific installation targets.

Alternate key installation

- If you had previously installed the SSH public key on the remote workstations through some other method outside of the CIM, skip the steps outlined in this section. You can update the SSH public key installation records kept by the CIM using an AdminTask command. The Administrator must first save the user name to be used with the SSH key to access the target host, and then invoke the relevant AdminTask commands:

1. Log in to the administrative console.
2. Navigate to the CIM "Installation Targets" panel.
   a. Click on the target host name.
   b. On the resulting page, fill in the **user name** field and click **Save**.
   c. Repeat this for all target hosts that have the SSH public key installed outside of CIM.
3. Update the SSH public key installation records using the `updateKeyInstallationRecords` AdminTask command:
   – Using Jacl:

```
$AdminTask updateKeyInstallationRecords {-add "abc.com,river.com"}
$AdminTask listKeyInstallationRecords
```

   – Using Jython:

```
AdminTask.updateKeyInstallationRecords ('[-add "abc.com,river.com"]')
print AdminTask.listKeyInstallationRecords()
```

Troubleshooting

- If your deployment manager is on a Windows system and you have generated a public-private key pair to use SSH authentication with remote target hosts running on UNIX-based platforms such as AIX or Linux, CIM might not be able to access the private key store on the deployment manager system. If you had generated a public-private key pair on your Windows workstation using the OpenSSH package that is part of the CYGWIN software, the private key store is protected and is accessible only to the user account that creates the key pair. However, the default setup for WebSphere Application Server on Windows operating system is to have the server running under the local `SYSTEM` account.

  To allow CIM to access the private key store you must also grant the local `SYSTEM` account read permission to the private key store:

  1. From the Windows Explorer navigate to the private key store, right click the key store file name, id_rsa, for example, and select **Properties**.
  2. Select the **Security** tab and add the `SYSTEM` account giving **Read** and **Read & Execute** permissions to the account.
  3. Click **OK**.

What to do next

You can install the same SSH public key on other installation targets to securely access all of your workstations.

Using the Secure Shell (SSH) authentication method on target Windows operating systems

For hosts running on Windows operating systems, support for SSH protocol requires the addition of a third-party product such as SSH on CYGWIN on the target Windows host and the software package you are installing will be installed under CYGWIN. Since WebSphere Application Server does not officially support installing under CYGWIN, this tool has only been tested to verify that centralized installation manager (CIM) can be used to install a software package on Windows targets using the SSH public/private key authentication. Other SSH support for Windows operating systems has not been tested and is not supported by CIM.

Before you begin

Use the information provided in this topic only if you want to use the SSH public/private key authentication method to access remote target workstations that are running any of the Windows operating systems. You can skip this topic if you plan to use the user name and password authentication method to access the installation targets.

Ensure CYGWIN SSH server is installed on the Windows target workstation.

In a typical setup of the CYGWIN sshd server running as a Windows service, the server runs under the Local SYSTEM account (or for a Windows 2003 Server, runs under a local account, `sshd_server`) specifically created with special privileges to run the service. With an SSH server configured and started on the Windows target, the server authenticates user logins using a public/private key-pair. With this setup, however, installation programs that are located on the Windows target and invoked by the centralized installation manager—which is using SSH public/private key authentication to gain access to the target workstation—are run using the identity of the account under which the SSH server is running. This causes problems with certain centralized installation manager operations when the files or directories on the target system, which the operation is to operate on, were created using different identities. To work around this, change the service that the CYGWIN sshd server runs under to log on with the same account, `root`, which is used to install software on that specific target Windows workstation.

Restriction: When installing WebSphere Application Server Version 8.0 on Windows targets using SSH public/private key authentication, do not specify installation directory path with one or more spaces within the path. Having spaces within the installation path will cause failure in some Windows `bat` files when the input argument also contains spaces.

Assuming that a local ID `root` that has Administrator authority to install software on the Windows workstation has been created, complete the following steps to change the CYGWIN sshd server to run under the ID `root`:

About this task

Procedure

1. Change the login ID of the CYGWIN sshd service.
   a. From the Windows Start menu, click **Settings** > **Control Panel** > **Administrative Tools** > **Services**.
   b. From the Services window, right-click **CYGWIN sshd**, and select **Properties**.
   c. From the Properties window, select the General tab, and click **Stop** to stop the sshd service.
   d. Next, select the Log on tab. Under the Log on as section or prompt, clear the **Local System account** radio button, and select **This account**.
   e. Type `.\root` as the ID and type the password for the account. Click **Apply**.
2. Grant additional rights to the `root` account. Ensure that the account has the required privileges in addition to membership to the Administrators group.
   a. From the Windows Start menu, click **Settings** > **Control Panel** > **Administrative Tools** > **Local Security Policy**.
   b. From the Local Security Settings window, expand **Local Policies**, and select **User Rights Assignment**.
   c. From the resulting page that is displayed on the right, verify that the `root` account has the following four rights:
      - Adjust memory quotas for a process
      - Create a token object
      - Log on as a service
      - Replace a process level token

      If not, add `root` as a user with the four rights.
3. Close the Local Security Settings window.
4. From a CYGWIN console panel, change ownership of the following directories and files to `root`:
   - `chown root /var/log/sshd.log`
   - `chown -R root /var/empty`

- `chown root /etc/ssh*`

5. Restart the CYGWIN sshd service.

   From the Properties page of the CYGWIN sshd service, select the General tab, and click **Start**. Verify that the service is now running under the `root` user account.

Results

You can now install product packages and maintenance to your Windows target workstations.

Troubleshooting: Windows You might receive the following error trying to connect to your Windows workstation using a non-administrator user ID and password:

```
XCIM0010E: An error occurred while connecting to the remote target ip_address.
Cause: CTGRI0011E An error occurred when accessing the remote registry or service control manager.
```

Many operations that CIM performs require access to resources that are not generally accessible by ordinary user accounts. Therefore, the account names that you use to log onto remote Windows machines must have administrative privileges. The simplest way is to add the user account to the Administrators group using the following steps:

1. Right click **My Computer** from your Windows desktop and select **Manage**.
2. Expand **Local Users and Groups** on the resulting Computer Management windows and select the **Users** folder.
3. On the right panel, double-click the user account to open the Properties window for that account.
4. Select the **Member Of** tab, and add the Administrators group to the list of groups that this account belongs to.

What to do next

From the administrative console, click **System administration** > **Centralized Installation Manager** > **Installation targets**.

Centralized installation manager (CIM) Version 6.1.x and 7.x usage scenarios

This section shows end-to-end use cases of how the centralized installation manager (CIM) can be used to assist WebSphere administrators.

Before you begin

Note: This topic applies to WebSphere Application Server Version 6.1.x and 7.x only. For information about using centralized installation manager (CIM) for Version 8.0, see “Submitting Installation Manager jobs” on page 292.

You must have CIM installed as part of your Network Deployment environment before you can perform the following scenarios.

About this task

- Creating and managing a Network Deployment cell using CIM

  Use the centralized installation manager to create and manage a WebSphere Network Deployment cell.
- Updating a cell to a new maintenance level

  Update your cell to a new maintenance level.

Creating and managing Version 6.1.x and 7.x Network Deployment cells using the centralized installation manager (CIM)

Use the centralized installation manager (CIM) to create and manage a WebSphere Network Deployment cell.

Before you begin

Note: This topic applies to WebSphere Application Server Version 6.1.x and 7.x only. For information about using centralized installation manager (CIM) for Version 8.0, see “Submitting Installation Manager jobs” on page 292.

To create a multiplatform cell using the CIM, you need the following items:

1. The CDs of all the WebSphere Application Server node platforms within the cell. For example, if your cell is running on Windows, Linux and AIX operating systems, then you need the CDs for those platforms in the WebSphere Application Server Network Deployment edition.
2. For the CIM repository, you require approximately 3 GB for each platform that you have in the cell. If you plan to create custom installation packages (CIP) for use with CIM, then you must factor in additional disk space required for CIPs. You can delete images that are no longer needed from the repository to make more space available.

About this task

The CIM is capable of creating nodes on remote hosts by installing WebSphere Application Server Network Deployment and federating them to the existing deployment manager.

Prior to CIM, you had to log in to every machine in the potential cell, install the servers manually, create a profile for each node, and federate the nodes to the deployment manager. Now, these steps are all done for you by the CIM. You only select the machine host name, and provide the login credentials.

Procedure

1. On the deployment manager machine, install WebSphere Application Server Network Deployment with management profile and deployment manager server type.
   a. Install WebSphere Application Server Version 8.0.
   b. Use the profile management tool to create a deployment manager profile.
   c. Use the Installation Factory to create a CIM repository.
2. Start the deployment manager. This can be done from the command line. From *app_server_root*/`profiles/Dmgr01/bin`, enter the following command:
   - AIX HP-UX Linux Solaris `./startManager.sh`
   - Windows `startManager.bat`
3. Log in to the administrative console.
4. Add other platform images for WebSphere Application Server Network Deployment to the CIM repository. For more information, see Adding installation packages of previous versions to the centralized installation manager (CIM) repository using the Installation Factory.
5. Launch installations of WebSphere Application Server Network Deployment on the remote machines. Refer to "Installing packages" for more details.
6. You can monitor the status of the installations using CIM. Refer to "Monitoring requests" for more details.

Results

The installation requests are sent via the centralized installation manager to install WebSphere application servers on the remote machines to create the cell.

What to do next

The cell is now ready for management. You can add servers, install applications, and so on.

Updating Version 6.1.x and 7.x cells to a new maintenance level using the centralized installation manager (CIM)

This section shows end-to-end use cases of how the centralized installation manager (CIM) can be used to assist WebSphere administrators.

About this task

Note: This topic applies to WebSphere Application Server Version 6.1.x and 7.x only. For information about using centralized installation manager (CIM) for Version 8.0, see “Submitting Installation Manager jobs” on page 292.

Complete the following steps to update all the nodes within the cell to the new maintenance level. You do not need to access the managed nodes directly while using CIM. With the node agent running on the targets, CIM will be able to stop all the running servers on the target node, update the remote node, and then restart the node agent.

Procedure

1. Log in to the administrative console.
2. Download the fix pack binary files and Update Installer tool for the platforms that you need into the centralized installation manager repository. You need the fix packs and Update Installers for all the platforms in the cell. Refer to the "Downloading the IBM Update Installer for WebSphere Software" and "Downloading package descriptors and the associated binary files to the repository" topics for more information.
3. Using the administrative console, install the new fix pack on all the nodes. You do not need to install the Update Installer tool directly on each node. CIM installs UPDI automatically if needed. Refer to the "Installing refresh packs or fix packs" topic for more details on this step.
4. Monitor the installation requests of the maintenance packages. Refer to the "Monitoring requests" topic for more details on this step.

Results

The installation requests are sent via the centralized installation manager to install WebSphere application servers on the remote machines to create the cell.

Centralized installation manager (CIM) AdminTask commands for Version 6.1.x and 7.x

You can use the Jacl or Jython scripting languages to use the features of the centralized installation manager (CIM) with the wsadmin tool. Use the commands and parameters to install, uninstall, and manage various software packages and maintenance files.

Note: This topic applies to WebSphere Application Server Version 6.1.x and 7.x only. For information about using centralized installation manager (CIM) for Version 8.0, see “Submitting Installation Manager jobs” on page 292.

The administrative tasks for the centralized installation manager include the following commands:

- “installWASExtension” on page 344
- “installSoftware” on page 345
- “installWithResponseFile” on page 347
- “installMaintenance” on page 349

- “listPackagesForInstall” on page 350
- “listFeaturesForInstall” on page 350
- “showPackageInfo” on page 351
- “showLicenseAgreement” on page 351
- “getManagedNodesOnHostByInstallLoc” on page 352
- “listManagedNodesOnHost” on page 353
- “testConnectionToHost” on page 353
- “testConnectionToHostUsingSSHKey” on page 354
- “installSSHPublicKeyOnHost” on page 355
- “listKeyInstallationRecords” on page 355
- “updateKeyInstallationRecords” on page 356
- “listPendingRequests” on page 356
- “listInProgressRequests” on page 357
- “listRequestsForTarget” on page 357
- “showLatestInstallStatus” on page 358
- “showLatestUninstallStatus” on page 359
- “uninstallSoftware” on page 359
- “uninstallMaintenance” on page 360

Note: Several of the commands include an `adminName` parameter. This refers to the name of an administrator account on the remote target machine. For targets on distributed operating systems, this administrator account can be either the root account or a non-root account if the software package supports a non-root install. However, for targets on Windows operating systems the added requirement is that the user account must have administrative privileges in order to use CIM for remote installations.

installWASExtension

The installWASExtension command installs the specified WebSphere® Application Server extension package on a specified host that contains one or more WebSphere Application Server, Network Deployment nodes. The nodes must be defined and part of the WebSphere Application Server, Network Deployment cell.

Note: This command is applicable if you have installed WebSphere Virtual Enterprise on your deployment manager node.

Target object:

None.

Required parameters:

`-packageName`
Specifies the name of the software package. (String, required)

`-hostName`
Specifies the domain-qualified host name of the remote host. (String, required)

`-augment`
Specifies a list of nodes to augment. Valid nodes are those defined on the host under the same installation location for WebSphere Application Server. Specify ALL_NODES as the keyword value to augment all of the nodes defined for the same installation location. (String, required)

-adminName
Specifies the administrative ID for the remote host. (String, required)

-acceptLicense
Specifies if the license agreement is accepted. Specify true to indicate that you reviewed and agreed to the terms of the IBM® International Program License Agreement accompanying this program. Otherwise, you cannot proceed with the installation of the program or component. (String, required)

Optional parameters:

-installLocation
Specifies the path of the installation directory on the remote host. Specify this parameter only if there are multiple installation locations that exist within the current cell on the same host. (String, optional)

-featureList
Specifies a list of features to install on the remote target. (String, optional)

-adminPassword
Specifies the administrative password for the remote host. Specify either the adminPassword command or the privateKeyStore command to authenticate. (String, optional)

-privateKeyStore
Specifies the path to the private key file, which is located on the deployment manager. Specify either the adminPassword command or the privateKeyStore command to authenticate. (String, optional)

-keyStorePassword
Specifies an optional password, also known as the passphrase, which is used to protect the private key file. (String, the parameter is required if a non-blank password is used to protect private key store.)

-specialParms
Specifies optional name-value pairs for other parameters that might be required. Obtain information about any name-value pairs from the provider of the software package. You can also use the showPackageInfo command to gather this information. (String, optional)

-tempDir
Specifies the location of the temporary directory on the target host. If this parameter is omitted, the centralized installation manager uses the default temporary directory of the target host. (String, optional)

Batch mode example usage:

- Using Jacl:

```
$AdminTask installWASExtension {-packageName XDOps -hostName river.com
  -augment ALL_NODES -adminName admin1
  -adminPassword  passw0rd1 -acceptLicense true}
```

- Using Jython:

```
AdminTask.installWASExtension ('[-packageName XDOps -hostName river.com
   -augment ALL_NODES -adminName admin1
  -adminPassword passw0rd1 -acceptLicense true]')
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask installWASExtension {-interactive}
```

- Using Jython:

```
AdminTask.installWASExtension ('[-interactive]')
```

installSoftware

The installSoftware command installs the specified software package on the target host.

Use this command to install WebSphere Application Server, Network Deployment Version 8.0, `packageName` **ND80**, on remote workstations.

Target object:

None.

Required parameters:

`-packageName`
Specifies the name of the software package. (String, required)

`-hostName`
Specifies the domain-qualified host name of the remote host. (String, required)

`-installLocation`
Specifies the path to the installation directory on the remote host. Specify this parameter only if there are multiple installation locations that exist within the current cell on the same host. (String, required)

`-adminName`
Specifies the administrative ID for the remote host. (String, required)

`-acceptLicense`
Specifies if the license agreement is accepted. Specify true to indicate that you reviewed and agreed to the terms of the IBM® International Program License Agreement accompanying this program. Otherwise, you cannot proceed with the installation of the program or component. (String, required)

Optional parameters:

`-featureList`
Specifies a list of features to install on the remote target. (String, optional) For the package ND80, available features are:

- **noFeature**, for no feature
- **samplesSelected**, for Application Server samples
- **languagepack.console.all**, for language pack for administrative console
- **languagepack.server.all**, for language pack for server runtime

The default features for this package are: **languagepack.console.all** and **languagepack.server.all**

`-adminPassword`
Specifies the administrative password for the remote host. Specify either the adminPassword command or the privateKeyStore command to authenticate. (String, optional)

`-privateKeyStore`
Specifies the path to the private key file, which is located on the deployment manager. Specify either the adminPassword command or the privateKeyStore command to authenticate. (String, optional)

`-keyStorePassword`
Specifies an optional password, also known as the passphrase, which is used to protect the private key file. (String, the parameter is required if a non-blank password is used to protect private key store.)

`-specialParms`
Specifies optional name-value pairs for other parameters that might be required. Obtain information about any name-value pairs from the provider of the software package. You can also use the showPackageInfo command to gather this information. (String, optional)

If global security is enabled for the WebSphere Application Server, Network Deployment cell, you must include the following parameters as specialParms:

- DMGR_ADMIN_ID: Specify the administrator ID used to log in to the administrative console.

- DMGR_ADMIN_PWD: Specify the password for the administrator ID used to log in to the administrative console.

Optionally, you can specify the following parameters with the specialParms parameter when you install WebSphere Application Server, Network Deployment Version 8.0:

- DISABLE_OS_PREREQ_CHECKING : Specify true or false with this parameter to disable or enable prerequisite checking on the operating system.
- USE_32BIT_IMAGE_ON_64BIT_OS : Specify true if you want to override the default behavior of using 64-bit installation image on 64-bit operating systems. This parameter has effect only if the software package includes a 32-bit image for the platform and machine architecture.

-tempDir
Specifies the location of the temporary directory on the target host. If this parameter is omitted, the centralized installation manager uses the default temporary directory of the target host. (String, optional)

Batch mode example usage:

- Using Jacl:

```
$AdminTask installSoftware {-packageName ND80 -hostName abc.com
-platformType windows -installLocation C:/WAS80 -adminName admin1
-adminPassword passw0rd1
-specialParms "{DMGR_ADMIN_ID admin2}{DMGR_ADMIN_PWD passw0rd2}"
-acceptLicense true}
```

```
$AdminTask installSoftware {-packageName ND80 -hostName abc.com
-platformType linux -installLocation "/opt/IBM/WAS80"
-adminName root -adminPassword passw0rd1 -acceptLicense true
-specialParms
"{DISABLE_OS_PREREQ_CHECKING true}{USE_32BIT_IMAGE_ON_64BIT_OS true}"}
```

- Using Jython:

```
AdminTask.installSoftware ('[-packageName ND80 -hostName abc.com
-platformType windows -installLocation C:/WAS80 -adminName admin1
-adminPassword passw0rd1
-specialParms "[DMGR_ADMIN_ID admin2][DMGR_ADMIN_PWD passw0rd2]"
-acceptLicense true]')
```

```
AdminTask.installSoftware ('[-packageName ND80
-featureList noFeature -hostName abc.com
-platformType linux -installLocation "/opt/IBM/WAS80" -adminName admin1
-adminPassword passw0rd1 -acceptLicense true -specialParms
"[DISABLE_OS_PREREQ_CHECKING true]" ]')
```

Interactive mode example usage:

- Using Jacl:

```
$$AdminTask installSoftware {-interactive}
```

- Using Jython:

```
AdminTask.installSoftware ('[-interactive]')
```

installWithResponseFile

The installWithResponseFile command installs the specified software package on the target host using parameters specified in a response file.

Target object:

None.

Required parameters:

-packageName
Specifies the name of the software package. (String, required)

-hostName
Specifies the domain-qualified host name of the remote host. (String, required)

-platformType
Specifies the operating system of the remote workstation. The valid types are: Windows, AIX, HP-UX, Linux, UNIX, OS400 or Solaris. This parameter is not case-sensitive. (String, required)

-responseFile
Specifies the relative path name of the response file on the deployment manager host that contains the parameters to be used for the installation operation. The response files for centralized installation are kept in the cim/responsefiles directory under the deployment manager profile root. The relative pathname is the pathname relative to this directory. (String, required)

-adminName
Specifies the administrative ID for the remote host. (String, required)

-acceptLicense
Specifies whether the terms of the license agreement are accepted. Specify true to indicate that you reviewed and agreed to the terms of the IBM® International Program License Agreement accompanying this program. Otherwise, you cannot proceed with the installation of the program or component. (String, required)

Optional parameters:

-adminPassword
Specifies the administrative password for the remote host. Specify either the adminPassword command or the privateKeyStore command to authenticate. (String, optional)

-privateKeyStore
Specifies the path to the private key file, which is located on the deployment manager. Specify either the adminPassword command or the privateKeyStore command to authenticate. (String, optional)

-keyStorePassword
Specifies an optional password, also known as the passphrase, which is used to protect the private key file. (String, the parameter is required if a non-blank password is used to protect private key store.)

-specialParms
Specifies optional name-value pairs for other parameters that might be required. Obtain information about any name-value pairs from the provider of the software package. You can also use the showPackageInfo command to gather this information. (String, optional)

-tempDir
Specifies the location of the temporary directory on the target host. If this parameter is omitted, the centralized installation manager uses the default temporary directory of the target host. (String, optional)

Batch mode example usage:

- Using Jacl:

```
$AdminTask installWithResponseFile {-packageName ND80 -hostName abc.com
-platformType windows –responseFile myOptionsfileForWindows.txt
-adminName admin1 -adminPassword passw0rd1 -acceptLicense true}
```

```
$AdminTask installWithResponseFile {-packageName ND80 -hostName abc.com
-platformType aix –responseFile myOptionsfileForAIX.txt
-adminName root -adminPassword passw0rd1 -acceptLicense true
-specialParms "{USE_32BIT_IMAGE_ON_64BIT_OS true}"}
```

- Using Jython:

```
AdminTask.installWithResponseFile ('[-packageName ND80 -hostName
 abc.com -platformType linux –responseFile myOptionsfileForLinux.txt
-adminName root -adminPassword passw0rd1 -acceptLicense true]')
```

```
AdminTask.installWithResponseFile ('[-packageName ND80 -hostName
abc.com -platformType aix –responseFile myOptionsfileForAIX.txt
-adminName root -adminPassword passw0rd1 -acceptLicense true
-specialParms "[USE_32BIT_IMAGE_ON_64BIT_OS true]"]')
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask installWithResponseFile {-interactive}
```

- Using Jython:

```
AdminTask.installWithResponseFile ('[-interactive]')
```

installMaintenance

The installMaintenance command installs maintenance on the target host.

Target object:

None.

Required parameters:

-packageName
Specifies the name of the software package. (String, required)

-hostName
Specifies the domain-qualified host name of the remote host. (String, required)

-adminName
Specifies the administrative ID for the remote host. (String, required)

-acceptLicense
Specifies whether the terms of the license agreement are accepted. Specify true to indicate that you reviewed and agreed to the terms of the IBM® International Program License Agreement accompanying this program. Otherwise, you cannot proceed with the installation of the program or component. (String, required)

Optional parameters:

-fileList
Specifies a list of .pak maintenance files to install on the remote target. This parameter is ignored if you install a predefined maintenance package. (String, optional)

-installLocation
Specifies the path of the installation directory in which to install the package on the remote host. Specify this parameter only if there are multiple installation locations that exist within the current cell on the same host. (String, optional)

-adminPassword
Specifies the administrative password for the remote host. Specify either the adminPassword command or the privateKeyStore command to authenticate. (String, optional)

-privateKeyStore
Specifies the path to the private key file, which is located on the deployment manager. Specify either the adminPassword command or the privateKeyStore command to authenticate. (String, optional)

-keyStorePassword
Specifies an optional password, also known as the passphrase, which is used to protect the private key file. (String, the parameter is required if a non-blank password is used to protect private key store.)

-tempDir
Specifies the location of the temporary directory on the target host. If this parameter is omitted, the centralized installation manager uses the default temporary directory of the target host. (String, optional)

Batch mode example usage:

- Using Jacl:

```
$AdminTask installMaintenance {-packageName ND80Maintenance -fileList
"8.0.0.5-WS-WAS-IFPKxxxxx.pak,8.0.0.5-WS-WAS-IFPKyyyyy.pak" -hostName
river.com -installLocation D:/WAS80 -adminName admin1 -adminPassword
passw0rd1 -acceptLicense true}
```

- Using Jython:

```
AdminTask.installMaintenance ('[-packageName ND80Maintenance -fileList
"8.0.0.5-WS-WAS-IFPKxxxxx.pak,8.0.0.5-WS-WAS-IFPKyyyyy.pak" -hostName
river.com -installLocation D:/WAS80 -adminName admin1 -adminPassword
passw0rd1 -acceptLicense true]')
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask installMaintenance {-interactive}
```

- Using Jython:

```
AdminTask.installMaintenance ('[-interactive]')
```

listPackagesForInstall

The listPackagesForInstall command lists all of the software packages that you can use the centralized installation manager to install.

Target object:

None.

Required parameters:

None.

Optional parameters:

None.

Batch mode example usage:

- Using Jacl:

```
$AdminTask listPackagesForInstall
```

- Using Jython:

```
AdminTask.listPackagesForInstall ()
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask listPackagesForInstall {-interactive}
```

- Using Jython:

```
AdminTask.listPackagesForInstall ('[-interactive]')
```

listFeaturesForInstall

The **listFeaturesForInstall** command lists the available features of a software package that you can use the centralized installation manager to install.

None of the WebSphere Virtual Enterprise components provide separately installable features. This command returns an empty list when used against one of the WebSphere Virtual Enterprise components.

Target object:

None.

Required parameters:

-packageName
Specifies the name of the software package. (String, required)

Optional parameters

None.

Batch mode example usage:

- Using Jacl:

```
$AdminTask listFeaturesForInstall {-packageName sample_package}
```

- Using Jython:

```
AdminTask.listFeaturesForInstall ('[-packageName sample_package]')
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask listFeaturesForInstall {-interactive}
```

- Using Jython:

```
AdminTask.listFeaturesForInstall ('[-interactive]')
```

showPackageInfo

The showPackageInfo command displays general information about a specific software package.

Target object:

None.

Required parameters:

-packageName
Specifies the name of the software package. (String, required)

Optional parameters:

None.

Batch mode example usage:

- Using Jacl:

```
$AdminTask showPackageInfo {-packageName sample_package}
```

- Using Jython:

```
AdminTask.showPackageInfo ('[-packageName sample_package]')
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask showPackageInfo {-interactive}
```

- Using Jython:

```
AdminTask.showPackageInfo ('[-interactive]')
```

showLicenseAgreement

The showLicenseAgreement command displays the license agreement associated with the specified installation package.

Target object:

None.

Required parameters:

-packageName
Specifies the name of the software package. (String, required)

Optional parameters:

-showLicenseInfoOnly
Specifies that only the content of the license file is shown. The default is false. (String, required)

Batch mode example usage:

- Using Jacl:

```
$AdminTask showLicenseAgreement {-packageName sample_package}
```

- Using Jython:

```
AdminTask.showLicenseAgreement ('[-packageName sample_package]')
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask showLicenseAgreement {-interactive}
```

- Using Jython:

```
AdminTask.showLicenseAgreement ('[-interactive]')
```

getManagedNodesOnHostByInstallLoc

The getManagedNodesOnHostByInstallLoc command returns the names of the managed nodes that are defined in the current deployment manager cell. Issue this command when a host contains multiple installations of WebSphere Application Server, Network Deployment with nodes that are federated into the same cell.

Target object:

The required target object is the host name of the workstation containing the managed nodes that are federated into the current deployment manager cell.

Required parameters:

None.

Optional parameters:

None.

Batch mode example usage:

- Using Jacl:

```
$AdminTask getManagedNodesOnHostByInstallLoc host_name
```

- Using Jython:

```
AdminTask.getManagedNodesOnHostByInstallLoc ('host_name')
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask getManagedNodesOnHostByInstallLoc {-interactive}
```

- Using Jython:

```
AdminTask.getManagedNodesOnHostByInstallLoc ('[-interactive]')
```

listManagedNodesOnHost

The listManagedNodesOnHost command lists the managed nodes that are located on the federated host in the current deployment manager cell.

Target object:

The required target object is the host name of the workstation containing the managed nodes that are federated into the current deployment manager cell.

Required parameters:

None.

Optional parameters:

None.

Batch mode example usage:

- Using Jacl:

```
$AdminTask listManagedNodesOnHost host_name
```

- Using Jython:

```
AdminTask.listManagedNodesOnHost ('host_name')
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask listManagedNodesOnHost {-interactive}
```

- Using Jython:

```
AdminTask.listManagedNodesOnHost ('[-interactive]')
```

testConnectionToHost

The testConnectionToHost command verifies that a connection can be established from the deployment manager to the remote host by using an administrator ID and password for the remote host.

Target object:

None.

Required parameters:

-hostName
Specifies the name of the remote host. (String, required)

-platformType
Specifies the platform type of the remote host. The valid types are Windows, AIX, HP-UX, Linux, UNIX, OS400 or Solaris. This parameter is not case-sensitive. (String, required)

-adminName
Specifies the administrative ID for the remote host. (String, required)

-adminPassword
Specifies the administrative password for the remote host. (String, required)

Optional parameters:

None.

Batch mode example usage:

- Using Jacl:

```
$AdminTask testConnectionToHost {-hostName big.mountain.com
-platformType linux -adminName root -adminPassword passw0rd3}
```

- Using Jython:

```
AdminTask.testConnectionToHost ('[-hostName big.mountain.com
-platformType linux -adminName root -adminPassword passw0rd3]')
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask testConnectionToHost {-interactive}
```

- Using Jython:

```
AdminTask.testConnectionToHost ('[-interactive]')
```

testConnectionToHostUsingSSHKey

The testConnectionToHostUsingSSHKey command verifies that a connection can be established from the deployment manager to the remote host by using the Secure Shell (SSH) private key for the remote host.

Target object:

None.

Required parameters:

-hostName
Specifies the name of the remote host. (String, required)

-adminName
Specifies the administrative ID for the remote host. (String, required)

-privateKeyStore
Specifies the path to the private key file, which is located on the deployment manager. (String, required)

Optional parameters:

-keyStorePassword
Specifies the optional password, also known as the passphrase, which is used to protect the private key file. (String, the parameter is required if a non-blank password is used to protect private key store.)

Batch mode example usage:

- Using Jacl:

```
$AdminTask testConnectionToHostUsingSSHKey {-hostName abc.com
-adminName root -privateKeyStore /root/.ssh/id_rsa}
```

- Using Jython:

```
AdminTask.testConnectionToHostUsingSSHKey ('[-hostName abc.com
-adminName root -privateKeyStore /root/.ssh/id_rsa]')
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask testConnectionToHostUsingSSHKey {-interactive}
```

- Using Jython:

```
AdminTask.testConnectionToHostUsingSSHKey ('[-interactive]')
```

installSSHPublicKeyOnHost

The installSSHPublicKeyOnHost command installs the administrative Secure Shell (SSH) public key on the remote host.

Target object:

None.

Required parameters:

-hostName
Specifies the name of the remote host. (String, required)

-adminName
Specifies the administrative ID for the remote host. (String, required)

-adminPassword
Specifies the administrative password for the remote host. (String, required)

-privateKeyStore
Specifies the path to the private key file, which is located on the deployment manager. (String, required)

Optional parameters:

None.

Batch mode example usage:

- Using Jacl:

```
$AdminTask installSSHPublicKeyOnHost {-hostName abc.com -adminName
root -adminPassword passw0rd3 -publicKeyStore /root/.ssh/id_rsa.pub}
```

- Using Jython:

```
AdminTask.installSSHPublicKeyOnHost ('[-hostName abc.com -adminName
root -adminPassword passw0rd3 -publicKeyStore /root/.ssh/id_rsa.pub]')
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask installSSHPublicKeyOnHost {-interactive}
```

- Using Jython:

```
AdminTask.installSSHPublicKeyOnHost ('[-interactive]')
```

listKeyInstallationRecords

The listKeyInstallationRecords command lists the SSH public key installation records that the centralized installation manager maintains.

Target object:

None.

Required parameters:

None.

Optional parameters:

None.

Batch mode example usage:

- Using Jacl:

```
$AdminTask listKeyInstallationRecords
```

- Using Jython:

```
AdminTask.listKeyInstallationRecords ()
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask listKeyInstallationRecords {-interactive}
```

- Using Jython:

```
AdminTask.listKeyInstallationRecords ('[-interactive]')
```

updateKeyInstallationRecords

The updateKeyInstallationRecords command updates the SSH public key installation records that the centralized installation manager maintains.

Target object:

None.

Required parameters:

None.

Optional parameters:

-add
Adds a list of host names to the installation records. (String, optional)

-remove
Removes a list of host names from the installation records. (String, optional)

Batch mode example usage:

- Using Jacl:

```
$AdminTask updateKeyInstallationRecords {-add "abc.com,river.com"}
```

- Using Jython:

```
AdminTask.updateKeyInstallationRecords ('[-add "abc.com,river.com"]')
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask updateKeyInstallationRecords {-interactive}
```

- Using Jython:

```
AdminTask.updateKeyInstallationRecords ('[-interactive]')
```

listPendingRequests

The listPendingRequests command lists the submitted installation or uninstallation requests that are not started

Target object:

None.

Required parameters:

None.

Optional parameters:

None.

Batch mode example usage:

- Using Jacl:

```
$AdminTask listPendingRequests
```

- Using Jython:

```
AdminTask.listPendingRequests ()
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask listPendingRequests {-interactive}
```

- Using Jython:

```
AdminTask.listPendingRequests ('[-interactive]')
```

listInProgressRequests

The listInProgressRequests command lists the installation or uninstallation requests that are in progress for completion.

Target object:

None.

Required parameters:

None.

Optional parameters:

None.

Batch mode example usage:

- Using Jacl:

```
$AdminTask listInProgressRequests
```

- Using Jython:

```
AdminTask.listInProgressRequests ()
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask listInProgressRequests {-interactive}
```

- Using Jython:

```
AdminTask.listInProgressRequests ('[-interactive]')
```

listRequestsForTarget

The listRequestsForTarget command lists all of the submitted installation and uninstallation requests for a specific host.

Target object:

The required target object is the host name of the target workstation. You must specify the same host name that you use for the installSoftware and uninstallSoftware commands.

Required parameters:

None.

Optional parameters:

None.

Batch mode example usage:

- Using Jacl:

```
$AdminTask listRequestsForTarget host_name
```

- Using Jython:

```
AdminTask.listRequestsForTarget ('host_name')
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask listRequestsForTarget {-interactive}
```

- Using Jython:

```
AdminTask.listRequestsForTarget ('[-interactive]')
```

showLatestInstallStatus

The showLatestInstallStatus command lists all of the submitted installation requests for a specific host.

Target object:

The required target object is the host name of the target workstation. You must specify the same host name that you use for the installSoftware command.

Required parameters:

None.

Optional parameters:

None.

Batch mode example usage:

- Using Jacl:

```
$AdminTask showLatestInstallStatus host_name
```

- Using Jython:

```
AdminTask.showLatestInstallStatus ('host_name')
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask showLatestInstallStatus {-interactive}
```

- Using Jython:

```
AdminTask.showLatestInstallStatus ('[-interactive]')
```

showLatestUninstallStatus

The showLatestUninstallStatus command displays the status of the most recently submitted uninstallation request.

Target object:

The required target object is the host name of the target workstation. You must specify the same host name that you use for the uninstallSoftware command.

Required parameters:

None.

Optional parameters:

None.

Batch mode example usage:

- Using Jacl:

```
$AdminTask showLatestUninstallStatus host_name
```

- Using Jython:

```
AdminTask.showLatestUninstallStatus ('host_name')
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask showLatestUninstallStatus {-interactive}
```

- Using Jython:

```
AdminTask.showLatestUninstallStatus ('[-interactive]')
```

uninstallSoftware

The uninstallSoftware command uninstalls the software package from the remote host.

Target object:

None.

Required parameters:

-packageName
Specifies the name of the software package. (String, required)

-hostName
Specifies the domain-qualified host name of the remote host. (String, required)

-platformType
Specifies the operating system of the remote workstation. The valid types are Windows, AIX, HP-UX, Linux, UNIX, OS400 or Solaris. This parameter is not case-sensitive. (String, required)

-installLocation
Specifies the path to the installation directory on the remote host. Specify this parameter only if there are multiple installation locations that exist within the current cell on the same host. (String, required)

-adminName
Specifies the administrative ID for the remote host. (String, required)

Optional parameters:

-adminPassword
Specifies the administrative password for the remote host. Specify either the adminPassword command or the privateKeyStore command to authenticate. (String, optional)

-privateKeyStore
Specifies the path to the private key file, which is located on the deployment manager. Specify either the adminPassword command or the privateKeyStore command to authenticate. (String, optional)

-keyStorePassword
Specifies an optional password, also known as the passphrase, which is used to protect the private key file. (String, the parameter is required if a non-blank password is used to protect private key store.)

Batch mode example usage:

- Using Jacl:

```
$AdminTask uninstallSoftware {-packageName ND80 -hostName abc.com
-platformType windows -installLocation C:/WAS80 -adminName admin1
-adminPassword passw0rd1}
```

- Using Jython:

```
AdminTask.uninstallSoftware ('[-packageName ND80 -hostName abc.com
-platformType windows -installLocation C:/WAS80 -adminName admin1
-adminPassword passw0rd1]')
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask uninstallSoftware {-interactive}
```

- Using Jython:

```
AdminTask.uninstallSoftware ('[-interactive]')
```

uninstallMaintenance

The uninstallMaintenance command uninstalls maintenance, such as fix packs and interim fixes, from the remote host.

Target object:

None.

Required parameters:

-packageName
Specifies the name of the software package. (String, required)

-hostName
Specifies the domain-qualified host name of the remote host. (String, required)

-adminName
Specifies the administrative ID for the remote host. (String, required)

Optional parameters:

-fileList
Specifies a list of maintenance files to uninstall on the remote target. (String, optional)

-installLocation
Specifies the path to the installation directory on the remote host. Specify this parameter only if there are multiple installation locations that exist within the current cell on the same host. (String, optional)

-adminPassword
Specifies the administrative password for the remote host. Specify either the adminPassword command or the privateKeyStore command to authenticate. (String, optional)

-privateKeyStore

Specifies the path to the private key file, which is located on the deployment manager. Specify either the adminPassword command or the privateKeyStore command to authenticate. (String, optional)

-keyStorePassword

Specifies an optional password, also known as the passphrase, which is used to protect the private key file. (String, the parameter is required if a non-blank password is used to protect private key store.)

Batch mode example usage:

- Using Jacl:

```
$AdminTask uninstallMaintenance {-packageName ND80Maintenance -hostName
river.com -adminName admin1 -adminPassword passw0rd1 -fileList
"8.0.0.5-WS-WAS-IFPKxxxxx.pak,8.0.0.5-WS-WAS-IFPKyyyyy.pak"}
```

- Using Jython:

```
AdminTask.uninstallMaintenance ('[-packageName ND80Maintenance -hostName
river.com -adminName admin1 -adminPassword passw0rd1 -fileList
"8.0.0.5-WS-WAS-IFPKxxxxx.pak,8.0.0.5-WS-WAS-IFPKyyyyy.pak"]')
```

Interactive mode example usage:

- Using Jacl:

```
$AdminTask uninstallMaintenance {-interactive}
```

- Using Jython:

```
AdminTask.uninstallMaintenance ('[-interactive]')
```

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, is the user's responsibility.

APACHE INFORMATION. This information may include all or portions of information which IBM obtained under the terms and conditions of the Apache License Version 2.0, January 2004. The information may also consist of voluntary contributions made by many individuals to the Apache Software Foundation. For more information on the Apache Software Foundation, please see http://www.apache.org. You may obtain a copy of the Apache License at http://www.apache.org/licenses/LICENSE-2.0.

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

> IBM Director of Intellectual Property & Licensing
> IBM Corporation
> North Castle Drive
> Armonk, NY 10504-1785
> USA

Trademarks and service marks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. For a current list of IBM trademarks, visit the IBM Copyright and trademark information Web site (www.ibm.com/legal/copytrade.shtml).

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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

Index