

IBM WebSphere Application Server Network Deployment
for IBM i, Version 8.5

*Installing your application serving
environment*

IBM

Note

Before using this information, be sure to read the general information under “Notices” on page 175.

Compilation date: June 2, 2012

© Copyright IBM Corporation 2012.

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

Contents

How to send your comments	v
Using this PDF	vii
Chapter 1. What is new for installers	1
Chapter 2. How do I install an application serving environment?	3
Chapter 3. Checklist: Installing WebSphere Application Server on the IBM i platform	5
Chapter 4. Task overview: Installing on IBM i	7
WebSphere Application Server Version 8.5 product offerings for supported operating systems	7
Directory conventions	17
Hardware and software requirements	18
Required disk space	18
Translated Languages	18
Updating ports in existing profiles on IBM i	19
Installing the WebSphere Application Server group PTF on IBM i	22
Installation: Resources for learning	24
Chapter 5. Preparing the operating system for installation on IBM i	27
IBM i prerequisites	28
Workstation prerequisites	31
Determining the proper cumulative PTF level on IBM i	32
Cumulative PTFs for IBM i	33
Chapter 6. Installing and uninstalling the product on IBM i operating systems	35
Installing the product on IBM i operating systems using response files	37
Installing the product on IBM i operating systems using the command line	43
Installing the product remotely on IBM i operating systems using the <code>iRemoteInstall</code> command	48
Installing and removing features on IBM i operating systems using response files	52
Installing interim fixes on IBM i operating systems using the command line	55
Installing fix packs on IBM i operating systems using response files	58
Installing fix packs on IBM i operating systems using the command line	60
Uninstalling interim fixes from IBM i operating systems using the command line	63
Uninstalling fix packs from IBM i operating systems using response files	64
Uninstalling fix packs from IBM i operating systems using the command line	65
Uninstalling the product from IBM i operating systems using response files	66
Uninstalling the product from IBM i operating systems using the command line	67
Chapter 7. Verifying the installation	69
Chapter 8. Configuring the product after installation on IBM i	71
Configuring software license information	71
Configuring SQL jobs on IBM i	72
Configuring TCP/IP on IBM i	73
Configuring an HTTP server instance on IBM i	74
Configuring IBM HTTP Server for IBM i	75
Configuring Lotus Domino HTTP Server on IBM i	78
Chapter 9. Starting WebSphere Application Server on IBM i	81
Starting default standalone application server profiles on IBM i	81
Verifying that the application server is running on IBM i	82

Starting the administrative console on IBM i	83
Starting and configuring default deployment manager profiles on IBM i	84
Verifying that the deployment manager is running on IBM i	85
Adding nodes to deployment manager profiles on IBM i	86
Verifying that the node agent is running on IBM i	86
Starting the administrative console for deployment managers on IBM i	87
Verifying that nodes exist on IBM i	88
Configuring virtual hosts on IBM i	88
Starting HTTP server instances on IBM i	89
Starting default application server nodes on IBM i	90
Chapter 10. Installing and uninstalling the DMZ Secure Proxy Server on IBM i systems	93
Installing the DMZ Secure Proxy Server on IBM i operating systems using response files	94
Installing the DMZ Secure Proxy Server on IBM i operating systems using the command line	97
Installing and removing DMZ Secure Proxy Server features on IBM i operating systems using response files	101
Installing fix packs on the DMZ Secure Proxy Server on IBM i operating systems using response files	102
Uninstalling fix packs from the DMZ Secure Proxy Server on IBM i operating systems using response files	104
Uninstalling the DMZ Secure Proxy Server from IBM i operating systems using response files.	105
Uninstalling the DMZ Secure Proxy Server from IBM i operating systems using the command line	106
Chapter 11. Centralized installation manager (CIM)	107
Submitting Installation Manager jobs	108
Submitting jobs to install Installation Manager on remote hosts	109
Submitting jobs to update Installation Manager on remote hosts for Version 8.5	111
Submitting jobs to uninstall Installation Manager on remote hosts	112
Installing the Version 8.5 product using the job manager and administrative console	114
Installing the Version 8.5 product using the job manager and command line	116
Managing Installation Manager using the job manager	120
Using the centralized installation manager (CIM) to manage Version 6.1.x and 7.x	122
Getting started with the centralized installation manager (CIM) for previous versions	124
Installing packages using the centralized installation manager (CIM) for previous versions	131
Downloading package descriptors and binary files for previous versions to the centralized installation manager (CIM) repository	143
Managing Version 6.1.x and 7.x centralized installation manager (CIM) installation targets	149
Centralized installation manager (CIM) Version 6.1.x and 7.x usage scenarios	154
Centralized installation manager (CIM) AdminTask commands for Version 6.1.x and 7.x	156
Notices	175
Trademarks and service marks	177
Index	179

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 email form appears.
 3. Fill out the email form as instructed, and submit your feedback.
- To send comments on PDF books, you can email your comments to: **wasdoc@us.ibm.com**.

Your comment should pertain to specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. 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.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer. When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about your comments.

Using this PDF

Links

Because the content within this PDF is designed for an online information center deliverable, you might experience broken links. You can expect the following link behavior within this PDF:

- 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.

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.

Chapter 1. What is new for installers





Installation is an easier, more consistent, and 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
-  Install the product
-  Configure the product after installation
-  Start the application server

Chapter 3. Checklist: Installing WebSphere Application Server on the IBM i platform

Print this article and use it as a checklist of steps for installing WebSphere Application Server products on the IBM® i platform.

Procedure

1. Step 1: Preparing for the installation

- a. ____ Determine if WebSphere Application Server for IBM i is already installed on your server.
Note that you are looking for Version 8.5 only, not previous versions of the product.
See Chapter 5, “Preparing the operating system for installation on IBM i,” on page 27 for more information.
- b. ____ Read the product Release Notes for the WebSphere Application Server product.
- c. ____ Schedule enough time for each step of the process.
See Chapter 5, “Preparing the operating system for installation on IBM i,” on page 27 for more information.
- d. ____ Verify that your system meets all hardware and software prerequisites, and install prerequisite software if necessary.
 - ____ IBM i server hardware requirements
 - ____ IBM i server software requirementsSee “IBM i prerequisites” on page 28 for more information.
- e. ____ Verify that your workstation meets all hardware and software prerequisites, and install prerequisite software if necessary.
See “Workstation prerequisites” on page 31 for more information.
- f. ____ Obtain and install the correct IBM i cumulative PTF package.
See “Cumulative PTFs for IBM i” on page 33 for more information.
- g. ____ Obtain the WebSphere Application Server product and current fixes.
See Chapter 5, “Preparing the operating system for installation on IBM i,” on page 27 for more information.

2. Step 2: Installing WebSphere Application Server

- a. ____ Install WebSphere Application Server on your IBM i server.
See Chapter 6, “Installing and uninstalling the product on IBM i operating systems,” on page 35 for more information.
- b. ____ Install the WebSphere Application Server group PTF.
See “Installing the WebSphere Application Server group PTF on IBM i” on page 22 for more information.

3. Step 3: Configuring WebSphere Application Server

- a. ____ Configure software license information.
See “Configuring software license information” on page 71 for more information.
- b. ____ Set SQL server jobs.
See “Configuring SQL jobs on IBM i” on page 72 for more information.
- c. ____ Configure TCP/IP.
See “Configuring TCP/IP on IBM i” on page 73 for more information.
- d. ____ Configure an HTTP server instance.
See “Configuring an HTTP server instance on IBM i” on page 74 for more information.

4. Step 4: Starting WebSphere Application Server

- a. ____ Start WebSphere Application Server.
See Chapter 9, “Starting WebSphere Application Server on IBM i,” on page 81 for more information.
- b. ____ Verify that WebSphere Application Server is running.
See “Verifying that the application server is running on IBM i” on page 82 for more information.
- c. ____ Start the administrative console.
See “Starting the administrative console on IBM i” on page 83 for more information.
- d. ____ Configure the virtual host.
See “Configuring virtual hosts on IBM i” on page 88 for more information.
- e. ____ Start the HTTP server.
See “Starting HTTP server instances on IBM i” on page 89 for more information.

5. **Step 5: Verifying the installation**

- a. ____ Verify the installation.
See Chapter 7, “Verifying the installation,” on page 69 for more information.

Chapter 4. Task overview: Installing on IBM i

Use this high-level procedure to install and customize IBM WebSphere Application Server on IBM i systems.

Before you begin

Read through the major articles in the Welcome, Learn about, and Product overview sections of the information center before beginning the installation.

About this task

Use this procedure to install WebSphere Application Server for IBM i.

Procedure

1. Prepare your operating system for installation.
See Chapter 5, “Preparing the operating system for installation on IBM i,” on page 27 for more information.
2. Install the product on your IBM i system.
See Chapter 6, “Installing and uninstalling the product on IBM i operating systems,” on page 35.
3. Install the WebSphere Application Server group PTF.
Apply the most recent WebSphere Application Server for IBM i group PTF before you start WebSphere Application Server for the first time.
The group PTF includes the most recent WebSphere Application Server PTFs and recent PTFs for other products that are required for WebSphere Application Server.
See “Installing the WebSphere Application Server group PTF on IBM i” on page 22.
4. Configure the product after installation.
For example, you can create a standalone application server profile, management profile, managed (custom) profile, cell profile, or secure proxy profile using the **manageprofiles** command.
See the *What to do next* section at the end of “Installing the product on IBM i operating systems using response files” on page 37 for examples of creating a default standalone application server profile and a default cell profile using the **manageprofiles** command.

What to do next

Go to Chapter 6, “Installing and uninstalling the product on IBM i operating systems,” on page 35 to continue the installation.

WebSphere Application Server Version 8.5 product offerings for supported operating systems

WebSphere Application Server Version 8.5 includes several related offerings.

Table 1. WebSphere Application Server Version 8.5 product offerings for supported operating systems. The following table shows the WebSphere Application Server Version 8.5 product offerings for supported operating systems.

Offering, offering ID, and operating systems	Description	Location					
		Product media	Passport Advantage [®] offerings ² (non-z/OS systems only)	Shop zSeries (z/OS [®] systems only)	Entitled Software Support (ESS)	developer Works	Web-based repository
Application Client for IBM WebSphere Application Server com.ibm.websphere.APPLCLIENT.v85 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.	↘ ³	↘				↘
Application Client for IBM WebSphere Application Server (ILAN) com.ibm.websphere.APPLCLIENTILAN.v85 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.v85 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.	↘ ⁴	↘				↘
DMZ Secure Proxy Server for IBM WebSphere Application Server Trial com.ibm.websphere.NDDMZTRIAL.v85 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. This offering is a no-cost trial version of the product.					↘	
DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS com.ibm.websphere.NDDMZ.zOS.v85 z/OS	DMZ Secure Proxy Server for IBM WebSphere Application Server 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.	↘		↘ ⁵			
IBM HTTP Server for WebSphere Application Server com.ibm.websphere.IHS.v85 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.	↘ ³	↘				↘

Table 1. WebSphere Application Server Version 8.5 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8.5 product offerings for supported operating systems.

Offering, offering ID, and operating systems	Description	Location					
		Product media	Presort Advantage® images ² (non-z/OS systems only)	Shop ZSeries (z/OS® systems only)	Entitled Software Support (ESS)	developer Works	Web-based repository
IBM HTTP Server for WebSphere Application Server (ILAN) com.ibm.websphere. IHS.LAN.v85 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.v85 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. com.ibm.websphere. IHS.zOS.v85 z/OS	↘		↘ ⁵			
IBM Web Enablement for IBM I com.ibm.websphere. WEBEMB.v85 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 Application Server Trial com.ibm.websphere. BASE.v85 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. WebSphere Application Server also includes the Liberty profile. ⁶	↘ ⁴	↘				↘
IBM WebSphere Application Server Trial com.ibm.websphere. BASE.ITML.v85 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. WebSphere Application Server also includes the Liberty profile. ⁶	↘ ⁴	↘				↘
IBM WebSphere Application Server - Express com.ibm.websphere. EXPRESS.v85 AIX, HP-UX, IBM I, Linux, Solaris, Windows	This offering is a no-cost trial version of the product. 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. WebSphere Application Server also includes the Liberty profile. ⁶	↘ ⁴	↘				↘

Table 1. WebSphere Application Server Version 8.5 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8.5 product offerings for supported operating systems.

Offering, offering ID, and operating systems	Description	Location					
		Product media	Passport Advantage [®] offerings ² (non-z/OS systems only)	Shop ZSeries (z/OS [®] systems only)	Entitled Software Support (ESS)	developer Works	Web-based repository
IBM WebSphere Application Server - Express Trial com.ibm.websphere.EXPRESSTRIAL.v85 AIX, HP-UX, IBM i, Linux, Solaris ⁷ , 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 or dynamic web applications which can be effortlessly migrated to more advanced versions of the WebSphere Application Server family as business needs change. WebSphere Application Server also includes the Liberty profile. ⁶ This offering is a no-cost trial version of the product.	↗ ⁴	↗			↗	↗
IBM WebSphere Application Server for Developers com.ibm.websphere.DEVELOPERS.v85 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. WebSphere Application Server also includes the Liberty profile. ⁶	↗ ⁴	↗				↗
IBM WebSphere Application Server for Developers (LAN) com.ibm.websphere.DEVELOPERS.LAN.v85 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. WebSphere Application Server also includes the Liberty profile. ⁶					↗	↗
IBM WebSphere Application Server for z/OS com.ibm.websphere.zOS.v85 z/OS	This offering is a no-cost non-supported and non-warranted version of the product. 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.	↗		↗ ⁵			
IBM WebSphere Application Server Network Deployment com.ibm.websphere.ND.v85 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. WebSphere Application Server also includes the Liberty profile. ⁶	↗ ⁴	↗				↗
IBM WebSphere Application Server Network Deployment Trial com.ibm.websphere.NDTRIAL.v85 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. WebSphere Application Server also includes the Liberty profile. ⁶ This offering is a no-cost trial version of the product.						↗

Table 1. WebSphere Application Server Version 8.5 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8.5 product offerings for supported operating systems.

Offering, offering ID, and operating systems	Description	Location					
		Product media	Passport Advantage® images ² (non-z/OS systems only)	Shop ZSeries (z/OS® systems only)	Entitled Software Support (ESS)	developer Works	Web-based repository
IBM WebSphere Application Server Web 2.0 and Mobile Toolkit com.ibm.websphere.w20tk.v11	Web 2.0 and Mobile Toolkit offers targeted, incremental new features that can make your web applications running on WebSphere Application Server easier to use. With this offering, WebSphere Application Server applications that were originally developed for desktop browsers can be adapted and deployed to mobile devices such as smartphones and tablets. This offering extends Service Oriented Architecture (SOA) by connecting external web services, internal SOA services, and Java Platform, Enterprise Edition (Java EE) objects into highly-interactive web application interfaces. Web 2.0 and Mobile Toolkit provides a supported, best-in-class Ajax development toolkit for WebSphere Application Server.	↘ 4	↘	↘ 5			↘
AIX, HP-UX, IBM i, Linux, Solaris, Windows, z/OS							
IBM WebSphere Application Server Web 2.0 and Mobile Toolkit (LAN) com.ibm.websphere.w20tklan.v11	Web 2.0 and Mobile Toolkit offers targeted, incremental new features that can make your web applications running on WebSphere Application Server easier to use. With this offering, WebSphere Application Server applications that were originally developed for desktop browsers can be adapted and deployed to mobile devices such as smartphones and tablets. This offering extends Service Oriented Architecture (SOA) by connecting external web services, internal SOA services, and Java Platform, Enterprise Edition (Java EE) objects into highly-interactive web application interfaces. Web 2.0 and Mobile Toolkit provides a supported, best-in-class Ajax development toolkit for WebSphere Application Server. This offering is a no-cost non-supported and non-warranted version of the product.	↘				↘	↘
AIX, HP-UX, IBM i, Linux, Solaris, Windows, z/OS							
IBM WebSphere Edge Components: Caching Proxy com.ibm.websphere.EDGECP.v85	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.	↘	↘				↘
AIX, HP-UX, Linux, Solaris, Windows							
IBM WebSphere Edge Components: Load Balancer for IPv4 com.ibm.websphere.EDGEIPV4.v85	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.	↘	↘				↘
AIX, HP-UX, Linux, Solaris, Windows							
IBM WebSphere Edge Components: Load Balancer for IPv4 and IPv6 com.ibm.websphere.EDGEIPV4IPV6.v85	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. This offering is a no-cost trial version of the product.	↘	↘				↘
AIX, HP-UX, Linux, Solaris, Windows							
IBM WebSphere Edge Components: Load Balancer for IPv4 and IPv6 Trial com.ibm.websphere.EDGEIPV4IPV6TRIAL.v85	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. This offering is a no-cost trial version of the product.						↘
AIX, HP-UX, Linux, Solaris, Windows							

Table 1. WebSphere Application Server Version 8.5 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8.5 product offerings for supported operating systems.

Offering, offering ID, and operating systems	Description	Location					
		Product media	Passport Advantage [®] offerings ² (non-z/OS systems only)	Shop ZSeries (z/OS [®] systems only)	Entitled Software Support (ESS)	Developer Works	Web-based repository
IBM WebSphere SDK Java Technology Edition Version 7.0[®] com.ibm.websphere. IBUNAV1.v70	This IBM Software Development Kit (SDK) provides a full-function SDK for Java that is compliant with Java Platform, Standard Edition (Java SE) 7 application programming interfaces (APIs). With IBM WebSphere SDK Java Technology Edition Version 7.0, you can develop and deploy Java applications at the Java 7 API level and continue the "write once, run anywhere" Java paradigm at the Java API level. The SDK contains the Runtime Environment. The Runtime Environment allows users to run Java applications. The SDK also contains other tools that enable developers to create Java applications.	↗ ⁴	↗	↗ ⁵			↗
AIX, HP-UX, Linux, Solaris, Windows, z/OS							
Pluggable Application Client for IBM WebSphere	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 platform.	↗ ³	↗				↗
WebSphere Application Server com.ibm.websphere. PUGCLIENT.v85	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.						
Windows							
Pluggable Application Client for IBM WebSphere	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 platform.						↗
WebSphere Application Server (ILAN) com.ibm.websphere. PUGCLIENTILAN.v85	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.						
Windows	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.v85	Web Server Plug-ins for IBM WebSphere Application Server provides an optimized connection to route requests from a web server and WebSphere Application Server.	↗ ³	↗				↗
AIX, HP-UX, IBM i, Linux, Solaris, Windows							
Web Server Plug-ins for IBM WebSphere Application Server (ILAN) com.ibm.websphere. PLGLAN.v85	Web Server Plug-ins for IBM WebSphere Application Server provides an optimized connection to route requests from a web server and WebSphere Application Server.						↗
AIX, HP-UX, IBM i, Linux, Solaris, Windows	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.v85	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.	↗		↗ ⁵			
z/OS							

Table 1. WebSphere Application Server Version 8.5 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8.5 product offerings for supported operating systems.

Offering, offering ID, and operating systems	Description	Location					
		Product media ³	Passport Advantage [®] eImage ² (non-z/OS systems only)	Shop ZSeries (z/OS [®] systems only)	Entitled Software Support (ESS)	developer Works	Web-based repository
WebSphere Customization Toolbox com.ibm.websphere.wct1.v85 AIX, HP-UX, Linux, Solaris, Windows ⁸	<p>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.</p> <p>Launch the Profile Management Tool (z/OS only) 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.</p> <p>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.</p> <p>Restriction: These tools are intended for use with the full WebSphere Application Server profile; they are not required or supported for use with the Liberty profile.</p>	↘	↘	↘		↘	
WebSphere Customization Toolbox (LAN) com.ibm.websphere.wctLAN.v85 AIX, HP-UX, Linux, Solaris, Windows ⁸	<p>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.</p> <p>Launch the Profile Management Tool (z/OS only) 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.</p> <p>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.</p> <p>Restriction: These tools are intended for use with the full WebSphere Application Server profile; they are not required or supported for use with the Liberty profile.</p> <p>This offering is a no-cost non-supported and non-warranted version of the product.</p>					↘	

Table 1. WebSphere Application Server Version 8.5 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8.5 product offerings for supported operating systems.

Offering, offering ID, and operating systems	Description	Location				
		Product media	Passport Advantage® images ² (non-z/OS systems only)	Shop ZSeries (z/OS® systems only)	Entitled Software Support (ESS)	Web-based repository
	<p>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 <i>Supported hardware and software</i> pages, the information at the website takes precedence. Prerequisites information in the information center is provided as a convenience only.</p> <p>2 See How to download WebSphere Application Server V8.5 from Passport Advantage Online for a list of the IBM WebSphere Application Server Version 8.5 installation images downloadable from the IBM Passport Advantage Online website and other information.</p> <p>3 Located on the Supplements disk in the physical media for non-z/OS systems</p> <p>4 Located on its own disk in the physical media for non-z/OS systems</p> <p>5 Installation Manager repositories in SMP/E format, available through CBPDO or ServerPac</p> <p>6 The Liberty profile delivers a simplified and lightweight runtime environment for OSGi and web applications. Fast restart times, coupled with its small size and ease of use, make this a good option for developers building applications that do not require the full Java EE environment of traditional enterprise application-server profiles. In addition to being installable when you install the full product using Installation Manager, the Liberty profile can be downloaded and installed separately. When installed separately using downloaded files, the Liberty profile is supported on the Mac OS as well as on the platforms supported by the full WebSphere Application Server profile.</p> <p>7 IBM WebSphere Application Server - Express is not supported on Solaris x86.</p> <p>8 The Java 7 extension offering works with the following primary offerings:</p> <ul style="list-style-type: none"> • Application Client for IBM WebSphere Application Server • DMZ Secure Proxy Server for IBM WebSphere Application Server • DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS • IBM WebSphere Application Server • IBM WebSphere Application Server - Express • IBM WebSphere Application Server for Developers • IBM WebSphere Application Server for z/OS • IBM WebSphere Application Server Network Deployment <p>9 Platform-related notes:</p> <ul style="list-style-type: none"> • 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 Plugins 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 J (the <code>RemoteInst11</code> command) can be run on Windows operating systems only. <p>A version of this utility that is current when the product is released is available also on the media or installation image.</p>					

Web-based service repositories for WebSphere Application Server Version 8.5 product offerings:

- For the live service repositories, use the same URLs as those used for the generally available product-offering repositories during installation. These URLs are based on the following pattern:

`http://www.ibm.com/software/repositorymanager/offering_ID`

where *offering_ID* is the offering ID that you can find in the table above.

- These locations do not contain web pages that you can access using a web browser. They are remote web-based repository locations that you specify for Installation Manager so that it can maintain the product.

Table 2. WebSphere Application Server Version 8.5 associated products. The following table shows the products associated with WebSphere Application Server Version 8.5.

Offering	Operating systems	Description	Location		
			Product media	Passport Advantage images (Non-z/OS systems only)	Shop ZSeries (z/OS systems only)
IBM Assembly and Deploy Tools for WebSphere Administration Version 8.5	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 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 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 Installation Manager Version 1.5.2	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
IBM Packaging Utility Version 1.5.2	AIX, HP-UX, Linux, Solaris, Windows 3	IBM Packaging Utility is a program that is used to create and manage packages for repositories to be used by Installation Manager. You can generate a new repository for packages, copy multiple packages to one repository, copy multiple versions of a product to one repository, delete packages that are no longer needed, create a repository to install packages over HTTP, or copy packages from installation images or IBM repositories to a repository that resides on an internal server or a local machine for example.	✓	✓	2
IBM Rational Agent Controller Version 8.3.5	AIX, Solaris, 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 Trial Version 8.5	AIX, HP-UX, IBM i, Linux, Solaris, Windows	IBM Rational Application Developer, 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 Support Assistant Version 4.1.2 or Version 5	AIX, HP-UX, IBM i, Linux, Solaris, Windows, z/OS	IBM Support Assistant is a free 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	AIX, HP-UX, Linux, Solaris, Windows, z/OS	IBM Tivoli Composite Application Manager for WebSphere Application Server is an optional tool that can be installed after the installation of WebSphere Application Server. It monitors the performance of WebSphere Application Server applications and provides transaction response metrics and realtime status on the health of applications. You can view this data in the Tivoli Performance Viewer, which you can access from the WebSphere Application Server administrative console. This tool also provides integration with the Tivoli Application Performance Monitoring solutions.	✓	✓	✓
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 7.5.0.1 4	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 3.5.13 (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 See How to download WebSphere Application Server V8.5 from Passport Advantage Online for a list of the IBM WebSphere Application Server 8.5 installation images downloadable from the IBM Passport Advantage Online website and other information.

2 Installation Manager repositories in SMP/E format, available through CBRPO or ServerPac

3 IBM i customers can build repositories using the IBM Packaging Utility on a Windows system.

4 WebSphere Adapters Version 7.5.0.1 for WebSphere Application Server for z/OS Version 8.5 cannot be installed using the Installing IBM WebSphere Adapters Version 7.5.0.1 on IBM WebSphere Application Server Version 8.5 Adobe Acrobat PDF and follow the z/OS installation instructions in the section on performing silent installation and uninstallation.

Directory conventions

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

IBM i

Default product locations - IBM i

These file paths are default locations. You can install the product and other components in any directory where you have write access. You can create profiles in any valid directory where you have write access. Multiple installations of WebSphere Application Server products or components require multiple locations.

app_client_root

The default installation root directory for the Application Client for IBM WebSphere Application Server is the /QIBM/ProdData/WebSphere/AppClient/V85/client directory.

app_client_user_data_root

The default Application Client for IBM WebSphere Application Server user data root is the /QIBM/UserData/WebSphere/AppClient/V85/client directory.

app_client_profile_root

The default Application Client for IBM WebSphere Application Server profile root is the /QIBM/UserData/WebSphere/AppClient/V85/client/profiles/*profile_name* directory.

app_server_root

The default installation root directory for WebSphere Application Server Network Deployment is the /QIBM/ProdData/WebSphere/AppServer/V85/ND directory.

java_home

Table 3. Root directories for supported Java Virtual Machines.

This table shows the root directories for all supported Java Virtual Machines (JVMs).

JVM	Directory
32-bit IBM Technology for Java	/QOpenSys/QIBM/ProdData/JavaVM/jdk60/32bit
64-bit IBM Technology for Java	/QOpenSys/QIBM/ProdData/JavaVM/jdk60/64bit

plugins_profile_root

The default Web Server Plug-ins profile root is the /QIBM/UserData/WebSphere/Plugins/V85/webserver/profiles/*profile_name* directory.

plugins_root

The default installation root directory for Web Server Plug-ins is the /QIBM/ProdData/WebSphere/Plugins/V85/webserver directory.

plugins_user_data_root

The default Web Server Plug-ins user data root is the /QIBM/UserData/WebSphere/Plugins/V85/webserver directory.

product_library

product_lib

This is the product library for the installed product. The product library for each Version 8.5 installation on the system contains the program and service program objects (similar to .exe, .dll, .so objects) for the installed product. The product library name is QWAS85x (where x is A, B, C, and so on). The product library for the first WebSphere Application Server Version 8.5 product installed on the system is QWAS85A. The *app_server_root*/properties/product.properties file contains the value for the product library of the installation, was.install.library, and is located under the *app_server_root* directory.

profile_root

The default directory for a profile named *profile_name* for WebSphere Application Server Network Deployment is the `/QIBM/UserData/WebSphere/AppServer/V85/ND/profiles/profile_name` directory.

shared_product_library

The shared product library, which contains all of the objects shared by all installations on the system, is QWAS85. This library contains objects such as the product definition, the subsystem description, the job description, and the job queue.

user_data_root

The default user data directory for WebSphere Application Server Network Deployment is the `/QIBM/UserData/WebSphere/AppServer/V85/ND` directory.

The profiles and profileRegistry subdirectories are created under this directory when you install the product.

The *user_data_root* directory contains the default locations for WLP_USR_DIR and WLP_OUTPUT_DIR when the Liberty profile is installed. These directories are `user_data_root/wlp/usr` and `user_data_root/wlp/output/servers`, respectively.

web_server_root

The default web server path is `/www/web_server_name`.

Hardware and software requirements

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

See Supported hardware and software website 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

IBM i

Disk-space requirements vary according to the hardware platform. See Chapter 5, “Preparing the operating system for installation on IBM i,” on page 27 for information about required disk space and how to prepare your operating system for installation:

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

Translated Languages

IBM i

The WebSphere Application Server Version 8.5 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

Updating ports in existing profiles on IBM i

Use the `updatePorts.ant` script to change ports in an installed profile.

Before you begin

Each profile template has its own `updatePorts.ant` script.

The `updatePorts.ant` script for application server profiles is in the `app_server_root/profileTemplates/template_name/actions` directory. To use the script, you have to identify which profile to update.

Note: You should only run this script if the profile is unfederated and if the configuration is the same structure as it was when the profile was created. For example, this script is ideal for changing ports for an unfederated application server profile after you created the profile but before you altered its configuration. For all other situations, use the techniques described in the *Setting port numbers to the `serverindex.xml` file using scripting* article.

About this task

Use the following procedure to become familiar with using the `updatePorts.ant` script. Each step is an exercise that results in reassigning ports using a particular method that the `updatePorts.ant` script supports.

Procedure

- Assign nonconflicting ports to profile *myprofile*.

The ANT script assigns nonconflicting ports by default. No special arguments are needed. Identify the fully qualified directory paths, profile name, unique node name, and unique cell name. Then issue the command.

1. Create the Java properties file encoded in CCSID 819 (ASCII), to assign nonconflicting port values to the application server profile.

For this example, assume that you create the following `/TMP/was_props/appserver.props` properties file.

```
WAS_HOME=/QIBM/ProdData/WebSphere/AppServer/V85/<edition>
was_install.root=/QIBM/ProdData/WebSphere/AppServer/V85/<edition>
profileName=myprofile
profilePath=/QIBM/UserData/WebSphere/AppServer/V85/<edition>/profiles/myprofile
templatePath=/QIBM/ProdData/WebSphere/AppServer/V85/<edition>/profileTemplates/default
nodeName=MYISERIES_myprofile
cellName=MYISERIES_myprofile
hostName=MYISERIES.mycompany.com
```

2. Start a Qshell session

```
STRQSH
```

3. Change directories to the `app_server_root/bin` directory.

```
cd /QIBM/ProdData/WebSphere/AppServer/V85/<edition>/bin
```

4. Issue the command.

```
ws ant -propertyfile /TMP/was_props/appserver.props -file
/QIBM/ProdData/WebSphere/AppServer/V85/<edition>/profileTemplates/default/actions/updatePorts.ant
```

5. Open the administrative console and view the changed port assignments.

To view the port assignments, click **Servers > Server Types > WebSphere application servers > server1 > [Communications] > Ports**.

6. Run the script again and view the ports. Are they the same as before?

The resulting dynamically assigned port values apply to all of the ports currently assigned to the AppSrv01 profile, for every server listed in the `serverindex.xml` file for the profile node name. Each port receives a new nonconflicting value. None of the old port value assignments are used because the port values are in use at the time of the new assignment.

- Assign default ports to the AppSrv02 profile.

The ANT script assigns nonconflicting ports by default. The `defaultPorts=true` special argument is needed. Identify the fully qualified directory paths, profile name, unique node name, and unique cell name. Then issue the command.

1. Create the Java properties file encoded in CCSID 819 (ASCII), to assign default port values to the application server profile.

For this example, assume that you create the following `/TMP/was_props/appserver.props` properties file.

```
WAS_HOME=/QIBM/ProdData/WebSphere/AppServer/V85/<edition>
was.install.root=/QIBM/ProdData/WebSphere/AppServer/V85/<edition>
profileName=AppSrv02
profilePath=/QIBM/UserData/WebSphere/AppServer/V85/<edition>/profiles/AppSrv02
templatePath=/QIBM/ProdData/WebSphere/AppServer/V85/<edition>/profileTemplates/default
nodeName=MYISERIES_AppSvr02
cellName=MYISERIES_AppSvr02
hostName=MYISERIES.mycompany.com
defaultPorts=true
```

2. Start a Qshell session

```
STRQSH
```

3. Change directories to the `app_server_root/bin` directory.

```
cd /QIBM/ProdData/WebSphere/AppServer/V85/<edition>/bin
```

4. Issue the command.

```
ws_ant -propertyfile /TMP/was_props/appserver.props -file
/QIBM/ProdData/WebSphere/AppServer/V85/<edition>/profileTemplates/default/actions/updatePorts.ant
```

5. Open the administrative console and view the changed port assignments.

To view the port assignments, click **Servers > Server Types > WebSphere application servers > server1 > [Communications] > Ports**.

6. Run the script again and view the ports. Are they the same as before?

The resulting assigned port values are the same each time because the values are the default values. This method does not resolve conflicting port assignments. To view all port assignments for a profile, see the `\serverindex.xml` file for your profile. Issue the `netstat *cnn` command from the IBM i command line to see all ports in use on the machine.

- Assign ports starting at 20050 to the AppSrv03 profile.

On IBM i, the ANT script assigns ports starting at 20050 and does not attempt to determine port conflicts. The `startingPort=20050` argument is needed. Identify the fully qualified directory paths, profile name, unique node name, and unique cell name. Then issue the command.

1. Create the Java properties file encoded in CCSID 819 (ASCII), to assign default port values to the application server profile.

For this example, assume that you create the following `/TMP/was_props/appserver.props` properties file.

```
WAS_HOME=/QIBM/ProdData/WebSphere/AppServer/V85/<edition>
was.install.root=/QIBM/ProdData/WebSphere/AppServer/V85/<edition>
profileName=AppSrv03
profilePath=/QIBM/UserData/WebSphere/AppServer/V85/<edition>/profiles/AppSrv03
templatePath=/QIBM/ProdData/WebSphere/AppServer/V85/<edition>/profileTemplates/default
nodeName=MYISERIES_AppSvr03
cellName=MYISERIES_AppSvr03
hostName=MYISERIES.mycompany.com
startingPort=20050
```

2. Start a Qshell session

```
STRQSH
```

3. Change directories to the `app_server_root/bin` directory.

```
cd /QIBM/ProdData/WebSphere/AppServer/V85/<edition>/bin
```

4. Issue the command.

```
ws_ant -propertyfile /TMP/was_props/appserver.props -file
/QIBM/ProdData/WebSphere/AppServer/V85/<edition>/profileTemplates/default/actions/updatePorts.ant
```

5. Open the administrative console and view the changed port assignments.

To view the port assignments, click **Servers > Server Types > WebSphere application servers > server1 > [Communications] > Ports**.

6. Run the script again and view the ports. Are they the same as before?

After using the `-startingPort` option, the resulting port values are the same each time because the ANT script assigns port values starting from the `startingPort` number (port 20050 in this case).

- Use a port definition property file to assign ports to the AppSrv04 profile.

The `portsFile=/opt/was/portdefs.our_appsrv_ex.props` special argument allows you to assign specific ports for your profile. Port conflict resolution is not done for the specified ports. Identify the fully qualified directory paths, profile name, unique node name, and unique cell name. Then issue the command.

1. Create the Java properties file encoded in CCSID 819 (ASCII), to assign nonconflicting port values to the application server profile.

Assume that you create the following `/TMP/was_props/portdefs.our_appsrv_ex.props` properties file:

```
WC_defaulthost=19080
WC_adminhost=19060
WC_defaulthost_secure=19443
WC_adminhost_secure=19043
BOOTSTRAP_ADDRESS=22809
SOAP_CONNECTOR_ADDRESS=28880
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=29401
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=29403
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=29402
ORB_LISTENER_ADDRESS=39100
DCS_UNICAST_ADDRESS=39353
SIB_ENDPOINT_ADDRESS=37276
SIB_ENDPOINT_SECURE_ADDRESS=37286
SIB_MQ_ENDPOINT_ADDRESS=45558
SIB_MQ_ENDPOINT_SECURE_ADDRESS=45578
SIP_DEFAULTHOST=45060
SIP_DEFAULTHOST_SECURE=45061
```

Note: The ports used in the port definition property file should reflect the template type. The ports in this example are for the default template type, and they might vary for other template types.

They can be modelled after the `portdef.props` file found in the template directory.

Assume that you create the following `/TMP/was_props/appserver.props` properties file:

```
WAS_HOME=/QIBM/ProdData/WebSphere/AppServer/V85/<edition>
was.install.root=/QIBM/ProdData/WebSphere/AppServer/V85/<edition>
profileName=AppSrv04
profilePath=/QIBM/UserData/WebSphere/AppServer/V85/<edition>/profiles/AppSrv04
templatePath=/QIBM/ProdData/WebSphere/AppServer/V85/<edition>/profileTemplates/default
nodeName=MYISERIES_AppSrv04
cellName=MYISERIES_AppSrv04
hostName=MYISERIES.mycompany.com
portsFile=/TMP/was_props/portdefs.our_appsrv_ex.props
```

2. Start a Qshell session

```
STRQSH
```

3. Change directories to the `app_server_root/bin` directory.

```
cd /QIBM/ProdData/WebSphere/AppServer/V85/<edition>/bin
```

(Or, if the product is installed to a non-default directory, change directories to the `<install_root_directory>/bin` directory.)

4. Issue the command.

```
ws_ant -propertyfile /TMP/was_props/appserver.props -file
/QIBM/ProdData/WebSphere/AppServer/V85/<edition>/profileTemplates/default/actions/updatePorts.ant
```

5. Open the administrative console and view the changed port assignments.

To view the port assignments, click **Servers > Server Types > WebSphere application servers > server1 > [Communications] > Ports**.

6. Run the script again and view the ports. Are they the same as before?

The resulting assigned port values are from a props file. Therefore, the values do not change. This method does not resolve conflicting port assignments.

Results

This procedure results in four different methods of port assignments with the `updatePorts.ant` script.

What to do next

Start or restart your server to use the new ports.

Installing the WebSphere Application Server group PTF on IBM i

Install the WebSphere Application Server group PTF to obtain the latest fix pack for the product and to install required PTFs for other products on which WebSphere Application Server relies. After installing the group PTF, an additional step is required to install the fix pack and bring the product to the current fix level.

Before you begin

Install the WebSphere Application Server product before using this procedure. See Chapter 4, “Task overview: Installing on IBM i,” on page 7 for more information.

About this task

Fixes for the WebSphere Application Server product are shipped in a fix pack. The WebSphere Application Server for IBM i group PTF delivers the most current level of the fix pack for the product.

Use this procedure to load and apply the latest WebSphere Application Server for IBM i group PTF before installing the current level of fix pack and then starting WebSphere Application Server for the first time.

Along with the current fix pack, the group PTF includes WebSphere Application Server PTFs that bring the product up to the latest service level for WebSphere Application Server Version for IBM i as well as the latest IBM DB2 Universal Database™, IBM Developer Kit for Java, and IBM HTTP Server group PTFs.

This group PTF also contains miscellaneous PTFs for IBM Developer Kit for Java, DB2 Universal Database for IBM i, and IBM HTTP Server that are not included in other group PTFs or cumulative PTF packages but must be installed.

See the PTFs page on the WebSphere Application Server website to determine the group PTF that you must order and install for your WebSphere Application Server edition and for your IBM i release level.

Install all product prerequisites before you install the group PTF package. Otherwise, WebSphere Application Server might fail as it starts.

These instructions assume that you are ready to load and apply all PTFs included in the group PTF. Because some of these PTFs might require a restart of your IBM i server, the instructions include steps for placing the server in a restricted state and doing the IPL of the server.

If it is not convenient to restart your server, specify that the PTFs that require an IPL be applied at the next normal IPL of the server. However, do not attempt to start or use WebSphere Application Server until all of the PTFs have been successfully loaded and applied and the system has performed an IPL.

Procedure

1. Verify that all of the prerequisite software is installed.
2. Place the WebSphere for IBM i group PTF disk into the disk drive on your IBM i server.
3. Sign on to your server and verify that your user profile has the *ALLOBJ and *SECADM special authorities.
4. Enter this command to bring your system into a restricted state:

```
ENDSBS SBS(*ALL)
```

5. Enter the following command from the CL command line when the system is in a restricted state:

```
GO PTF
```

6. Select option 8 (Install program temporary fix package) from the menu.

7. Specify the following parameter values and press **Enter**:

- **Device:** Specify the device name of your disk drive, for example, OPT01.
- **Automatic IPL:** Y
- **PTF type:** 1 (All PTFs)

If it is not convenient to restart your server, specify **No** for **Automatic IPL**. Any PTFs that require an IPL are applied at the next normal IPL of the server. However, do not attempt to start or use WebSphere Application Server until all of the PTFs have been successfully loaded and applied.

After all of the PTFs are installed, your IBM i server restarts unless you specify **No** for **Automatic IPL**.

```
Install Options for Program Temporary Fixes
System: your.server
Type choices, press Enter.
Device . . . . . OPT01 Name, *SERVICE
Automatic IPL . . . . . Y Y=Yes
N=No
Restart type . . . . . *SYS *SYS, *FULL
PTF type . . . . . 1 1=All PTFs
2=HIPER PTFs and HIPER
LIC fixes only
3=HIPER LIC fixes only
4=Refreshed Licensed Internal Code
Other options . . . . . N Y=Yes
N=No
F3=Exit F12=Cancel
```

8. After you have installed the group PTF, install the fix pack for the product.
If you obtained the fix pack by installing the WebSphere Application Server group PTF, the instructions for installing the fix pack can be found in file /QIBM/WAS/WASFixpacks/ReadmeV8.html or /QIBM/WAS/WASFixpacks/ReadmeV8.txt. Otherwise, see “Installing fix packs on IBM i operating systems using response files” on page 58 or “Installing fix packs on IBM i operating systems using the command line” on page 60 for details on installing the fix pack.
9. See the product release notes for information about the release, including a description of known problems and workarounds.

Results

Installing the WebSphere Application Server group PTF and the fix pack results in a fully updated installation. At that point, you can set up the initial product configuration.

What to do next

Go to Chapter 8, “Configuring the product after installation on IBM i,” on page 71 to continue the installation.

Installation: Resources for learning

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

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

One important link is:

How to buy WebSphere Application Server software

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

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

Planning, business scenarios, and IT architecture

- Supported hardware and software

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

- IBM developerWorks WebSphere

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

- IBM WebSphere Application Server library and information centers website

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

- IBM WebSphere Application Server home page

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

- IBM WebSphere software platform home page

The IBM WebSphere software platform home page introduces WebSphere products and describes how companies can easily transform to an e-business, with software that can grow as fast as the business it supports.

- WebSphere Application Server Edge components library and information centers website

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

Programming instructions and examples

- IBM developerWorks

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

- IBM Redbooks

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

Programming specifications

- Java EE information

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

Administration

- WebSphere technical library on developerWorks

The WebSphere library includes a wide range of content, including technical articles, downloads, product documentation, and tutorials

- The IBM Terminology website

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

Support

- Steps to getting support for WebSphere Application Server

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

-  Support page for WebSphere Application Server

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

-  IBM Software Support portal

Take advantage of the Web-based Support and Service resources from IBM to quickly find answers to your technical questions. You can easily access this extensive Web-based support through the IBM Software Support portal and search by product category, or by product name. If you are experiencing problems specific to WebSphere Application Server, for example, click **WebSphere Application Server** or **WebSphere Application Server for z/OS** in the product list. The WebSphere Application Server Support page displays.

-  IBM e-server Support: Fix Central

A web facility for downloading fixes for hardware and operating systems, including z/OS and IBM i.

- Adobe Acrobat website

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

Chapter 5. Preparing the operating system for installation on IBM i

Select the product components that you intend to install and verify that the product prerequisites are met. Also, plan for the amount of time required to perform each step of the installation.

About this task

Use this procedure to verify that you are ready to install. Complete the following procedure before you begin to install the product on your IBM i system.

Procedure

1. Determine if WebSphere Application Server is already installed on your server.
 - a. Enter the Display Software Resources (**DSPSFWRSC**) command on a CL command line.
 - b. Look for an entry with the product Resource ID 5733W80.
 - If you do not find the product Resources ID, then this product has not been installed on your iSeries® server.
 - If a previous version of WebSphere Application Server is installed on your server, read the coexistence instructions before you install the new version.
2. Print the Chapter 3, “Checklist: Installing WebSphere Application Server on the IBM i platform,” on page 5 to use as a checklist during the installation process.
3. Determine the time requirements for installation.

Plan to set aside enough time for each step of the process. Depending on your server specifications, the process may take more or less time than the estimates provided in this documentation.

Attention: The installation process might require at least one initial program load (IPL or restart) of the server if you need to install an IBM i cumulative PTF package.

Table 4. Tasks for preparing your operating system.

The following table shows the tasks for preparing your operating system.

Task	Estimated time
Preparing for the installation	
Reading release notes and migration instructions, and verifying hardware and software prerequisites	1-2 hours ¹
Obtaining the product and current fixes	Up to 2 weeks
Installing any additional products and IBM i cumulative PTF package	1-2 hours
Installing WebSphere Application Server	
Installing WebSphere Application Server on your IBM i server ²	45-120 minutes
Installing WebSphere Application Server Group PTF (depends on your system)	Up to 2 hours
Creating an initial configuration	30 minutes
Starting WebSphere Application Server for the first time	1-20 minutes
Verifying the installation	10 minutes

¹ This estimate applies if all product prerequisites are met. It does not take into account the time required to install additional prerequisite software.

² Actual time requirement depends on the method used.

4. Read the product release notes for important information about the product.

See the WebSphere Application Server documentation page for IBM i .
5. Verify that your system meets all hardware and software prerequisites, and install prerequisite software if necessary.

Verify that the IBM i prerequisites are satisfied. Install prerequisite software if necessary.

If you are running an IBM i server that does not meet the minimum recommended hardware requirements for WebSphere Application Server, you can still install and run the product. However, the WebSphere Application Server environment might run slowly, and your applications might not run successfully.

See “IBM i prerequisites” for more information.

6. Verify that your workstation meets all hardware and software prerequisites, and install prerequisite software if necessary.

See “Workstation prerequisites” on page 31 for more information.

7. Obtain and install the correct IBM i cumulative PTF package.

See “Cumulative PTFs for IBM i” on page 33 for more information.

8. Obtain the WebSphere Application Server product and current fixes.

Before you install WebSphere Application Server for IBM i, you need to obtain the application server product and current fixes.

- **WebSphere Application Server Version 8.5 for IBM i**

For information about how to order the product, see the **Ordering information** section of the WebSphere Application Server packaging information page.

- **Cumulative PTFs**

WebSphere Application Server Version 8.5 for IBM i was tested on a specific IBM i cumulative PTF package level.

To view the cumulative PTF package tested, see WebSphere Application Server PTFs.

From the PTFs page, select the link for your operating system release level. On the resulting page, click the **Cumulative Package** link.

You can install and run WebSphere Application Server Version 8.5 for IBM i successfully on earlier or later cumulative PTF packages.

See “Determining the proper cumulative PTF level on IBM i” on page 32 for more information about determining the cumulative PTF package level for your server.

- **PTFs**

To install the WebSphere Application Server product, ensure that you have a recent level of the Java group PTF installed. For V5R4M0, level 13 or higher is recommended.

The WebSphere Application Server Version 8.5 for IBM i group PTF includes fixes for WebSphere Application Server and other IBM i products such as IBM DB2 Universal Database, IBM Developer Kit for Java, and the IBM HTTP Server.

Installing the group PTF requires an IPL of your server, so plan accordingly.

To determine which IBM i group PTF you must order and install, see the WebSphere Application Server for IBM i PTFs web page. Group PTF numbers differ by WebSphere Application Server product and IBM i release level.

What to do next

See Chapter 4, “Task overview: Installing on IBM i,” on page 7 to continue the installation.

IBM i prerequisites

Before you install WebSphere Application Server, verify that your hardware and software meet the minimum requirements.

Hardware requirements

Overall system requirements will vary based on actual workload requirements. Use IBM Systems Workload Estimator for sizing assistance.

Systems that do not meet the recommended minimums may be used in environments that support a limited number of users and where longer server initialization times are acceptable. The recommended hardware minimum requirements follow:

- Server requirements for servlets and JavaServer Pages (JSP) files
- Disk requirements

Minimum server requirements

- Recommended minimum server models:
 - WebSphere requires a partition with a minimum of 600 CPW
 - WebSphere applications can benefit from the addition of an Accelerator Feature on models where this is available
 - Each active WebSphere profile requires a minimum of 1 GB of memory
- Any partition running WebSphere Application Server should have a minimum of 2 GB of memory. This memory requirement is in addition to memory required for any other applications running on your IBM i server.

These requirements are based on a single WebSphere Application Server profile. Additional profiles running concurrently require additional resources.

These requirements represent the recommended minimum requirements. Deployments that must support many users or require shorter response times might require additional resources.

Disk requirements

Table 5. Disk requirements.

This table describes WebSphere Application Server for IBM i disk requirements.

Installation option	Description	Disk space after installation
WebSphere Application Server	WebSphere Application Server run time	910 MB
Application Server Samples	Sample applications	90 MB
Application Client	Client development and run time	230 MB
Web Server Plug-ins	Web Server Plug-ins	100 MB

IBM i software requirements

The software required is as follows:

IBM i Version X Release Y (VXRY)

WebSphere Application Server is supported on IBM i Version 6 Release 1 (V6R1) and Version 7 Release 1 (V7R1). The IBM i server must be in an unrestricted state, and your user profile must have *ALLOBJ and *SECADM special authorities.

Java requirements

The following Java product is required to use or install WebSphere Application Server Version 8.5:

V6R1 and V7R1

- IBM J2SE 6.0 32-bit JVM (5761-JV1 option 11)

The following PTFs are required for 5761-JV1 option 11:

- SI42021
- SI42022
- SI42026

IBM i Qshell (5761-SS1, or 5770-SS1 option 30)

Required to run installation scripts and to use other scripts in WebSphere Application Server.

IBM i Extended Base Directory Support (5761-SS1, or 5770-SS1 option 3)

Required for installation.

IBM i Portable Application Solutions Environment (5761-SS1, or 5770-SS1 option 33)

Required to use Tivoli Performance Viewer. Required for Java SE 6 32 bit and Java SE 6 64 bit.

IBM i Host Servers (5761-SS1, or 5770-SS1 option 12)

Required for installation.

IBM i Digital Certificate Manager (5761-SS1, or 5770-SS1 option 34)

Required for installation to use Secure Sockets Layer (SSL) protocol.

All necessary fixes

The following PTF is required for 5761-SS1:

- SI41986

The following PTF is required for 5770-SS1:

- SI41988

For a list of current fixes, see <http://www.ibm.com/systems/i/software/websphere/index.html> and click **PTFs**.

IBM i optional software

The optional software is as follows:

Java products

You can choose the following optional Java product to use with WebSphere Application Server Version 8.5:

- **V6R1** and **V7R1**

- IBM SE 6.0 64 bit (5761-JV1 option 12)

The following PTFs are required for 5761-JV1 option 12:

- SI41985
- SI41998
- SI42024

- **V7R1** only

- IBM SE 7

- IBM SE 7 32 bit (5761-JV1 option 14)
Level 7 or higher of group PTF SF99572
- IBM SE 7 64 bit (5761-JV1 option 15)
Level 7 or higher of group PTF SF99572

- IBM WebSphere SDK Java Technology Edition Version 7.0

- IBM WebSphere SDK Java Technology Edition Version 7.0 32 bit (5761-JV1 option 14)
PTF SI46212
- IBM WebSphere SDK Java Technology Edition Version 7.0 64 bit (5761-JV1 option 15)
PTF SI46211

You can obtain 5761-JV1 option 14 and option 15 from the IBM Entitled software support site.

HTTP server

An HTTP server is not required for installation, but recommended for production environments that use servlets and JSP files. If you plan to deploy only enterprise beans, you do not need an HTTP server instance. WebSphere Application Server supports these HTTP server products:

- IBM HTTP Server (powered by Apache) (5761-DG1 or 5770-DG1)
- Lotus® Domino® 8 for System i® 8.0 (5733-LD8), versions 8.0.1 and 8.0.2
- IBM Domino 8.5 for i (5733-L85)

DB2 Query Manager and SQL Development Kit for iSeries (5761-ST1 or 5770-ST1)

The DB2 Query Manager and SQL Development Kit for iSeries help you develop client applications.

Next, see “Workstation prerequisites.”

Workstation prerequisites

Before you install WebSphere Application Server workstation components, verify that your hardware and software meet the minimum requirements.

Workstation hardware requirements

If you only plan to use your workstation to administer WebSphere Application Server, you can use any workstation running a supported web browser.

The workstation hardware requirements for application development and assembly components follow:

Capable workstations

See Detailed system requirements for more information.

Communications adapter or network interface

Your workstation must support a communications adapter or an appropriate network interface.

Free disk space

Your workstation must have a minimum of 120 MB of free disk space.

Memory

Your workstation must have a minimum of 256 MB of memory.

Disk drive

Your workstation must have a disk drive.

Workstation software requirements

If you only plan to use your workstation to administer WebSphere Application Server, you can use any operating system with a supported web browser.

The following workstation software requirements apply to the application development and assembly component. See Detailed system requirements for more information.

Any of these IBM development kits for Java

- Windows IBM Enhanced Java SE Development Kit 6
- HP-UX IBM Software Development Kit for the Java Platform, Version 1.6
- IBM Developer Kit for Linux, Java 2 Technology Edition, Version 1.6
- Solaris IBM Java SE Development Kit 6
- IBM Developer Kit for AIX, Java 2 Technology Edition, Version 1.6

These IBM development kits for Java are included on the WebSphere Application Server workstation disk. The appropriate development kit is automatically installed when you install any of the workstation components of WebSphere Application Server.

TCP/IP

TCP/IP must be installed and running.

Any of the following web browsers

- Microsoft Internet Explorer Version 6.0 SP2 or later
- AIX: Mozilla Firefox Version 1.5 or later

- HP-UX, Linux, Solaris: Mozilla Firefox Version 2.0 or later

Next, see “Determining the proper cumulative PTF level on IBM i.”

Determining the proper cumulative PTF level on IBM i

WebSphere Application Server for IBM i was tested with a specific cumulative PTF package. Ensure that you have the same cumulative PTF package or newer applied to your system before using WebSphere Application Server for IBM i.

Before you begin

Check the cumulative PTF package level applied to your system. If it is not at the minimum required level, order and apply the currently available cumulative PTF package.

About this task

Perform this task to gather the needed information about the cumulative PTF level applied to your system.

Procedure

1. Determine the prerequisite cumulative PTF package level for the version of WebSphere Application Server that you plan to install.
 - a. Go to the PTF page.
 - b. Under WebSphere PTF information, click the release level for your operating system.
 - c. Click the Cumulative Package link to see the minimum cumulative PTF package that is required.
2. Determine if the correct operating system cumulative PTF package is installed on your server.
 - a. Sign onto your server.
 - b. Enter the **Display PTF Status (DSPPTF)** command on a CL command line. The Display PTF Status screen is displayed. This screen lists the PTFs that are applied to the server.

The following example shows the Display PTF status screen on V6R1:

```

                                Display PTF Status
                                System: your.server
Product ID . . . . . : 5761999
IPL source . . . . . : ##MACH#B
Release of base option . . . . . : V6R1M0 L00

Type options, press Enter.
  5=Display PTF details  6=Print cover letter  8=Display cover letter

   PTF                               IPL
Opt ID      Status                    Action
-----
TL10215    Temporarily applied        None
TL10047    Permanently applied         None
TL09279    Permanently applied         None
TL09111    Permanently applied         None
TL08365    Permanently applied         None
TL08288    Superseded                    None
TL08190    Superseded                    None
TL08127    Superseded                    None
More...

F3=Exit  F11=Display alternate view  F17=Position to  F12=Cancel

```

What to do next

Next: Continue with one of the following steps:

- Install the correct cumulative PTF if it is not already installed on your server. See “Cumulative PTFs for IBM i” on page 33 for more information.

- Obtain WebSphere Application Server for IBM i if the correct cumulative PTF is installed. See Chapter 5, “Preparing the operating system for installation on IBM i,” on page 27.

Cumulative PTFs for IBM i

WebSphere Application Server requires a minimum cumulative PTF package level for the operating system on your IBM i server. If the correct cumulative PTF package is not installed on your IBM i server, you must install the cumulative PTF before you install WebSphere Application Server.

To install the cumulative PTF, follow your normal PTF installation procedures.

For more information about installing cumulative PTFs, see [Installing cumulative PTF packages in the IBM i information center](#).

Installing the cumulative PTF package requires you to restart your IBM i server. If it is not convenient to restart your server at the time that you apply the new PTF package, you can load and apply the PTFs and then specify that any PTFs that require an IPL be applied at the next normal IPL of the server. However, do not install the WebSphere Application Server product until all of the PTFs have been successfully applied.

For information about verifying your cumulative PTF level, see [“Determining the proper cumulative PTF level on IBM i”](#) on page 32.

If the correct cumulative PTF is already installed, skip this step and continue to Chapter 4, “Task overview: Installing on IBM i,” on page 7.

Next, go to Chapter 4, “Task overview: Installing on IBM i,” on page 7.

Chapter 6. Installing and uninstalling the product on IBM i operating systems

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

Before you begin

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 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 uninstall the packages that it installed.

Restriction: The Installation Manager GUI is not available on IBM i; all interaction with Installation Manager on IBM i is done through the command line or response files.

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 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 Version 1.5 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.

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.

Creating an Installation Manager: When the installation kit is available on your system, you can create an Installation Manager. An 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 creating an 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 installation command from the appropriate user ID to create the Installation Manager.

Accessing product repositories: All software materials that will be installed with IBM Installation Manager are stored in 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 interim fixes. 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 created an 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 8.5 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.

Notes:

- You must have Java SE 6 32 bit (option 11 of the IBM Developer Kit for Java) installed on your IBM i system before installing WebSphere Application Server Version 8.5. For more information, read “IBM i prerequisites” on page 28.
- Installation Manager console mode, which is included in Installation Manager Version 1.4.3 and later, does not work with WebSphere Application Server Version 8.5 offerings on systems other than z/OS.
- Do not transfer the content of a repository in non-binary mode and do not convert any content on extraction.
- When you try to install IBM Installation Manager locally from the WebSphere Application Server product media on an IBM i operating system, the following error message might be displayed:
The Installc executable launcher was unable to locate its companion shared library.

This error occurs because all directory and files names contained by the product media are displayed in upper case. To resolve this issue, enable the handling of mixed case on your IBM i operating system using the following command:

```
CHGOPTA EXTMEDFMT(*YES)
```

About this task

For more information on using Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

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

Note: Before using Installation Manager to install a product, you might want to back up your Installation Manager configuration using the instructions in the IBM Installation Manager Version 1.5 Information Center if the possibility of corruption is a concern.

Procedure

- “Installing the product on IBM i operating systems using response files” on page 37
- “Installing the product on IBM i operating systems using the command line” on page 43
- “Installing the product remotely on IBM i operating systems using the `iRemoteInstall` command” on page 48
- “Installing and removing features on IBM i operating systems using response files” on page 52
- “Installing interim fixes on IBM i operating systems using the command line” on page 55
- “Uninstalling interim fixes from IBM i operating systems using the command line” on page 63
- “Installing fix packs on IBM i operating systems using response files” on page 58
- “Installing fix packs on IBM i operating systems using the command line” on page 60
- “Uninstalling fix packs from IBM i operating systems using response files” on page 64
- “Uninstalling fix packs from IBM i operating systems using the command line” on page 65
- “Uninstalling the product from IBM i operating systems using response files” on page 66
- “Uninstalling the product from IBM i operating systems using the command line” on page 67

Results

- The following locations are the defaults for Installation Manager files on IBM i systems:
 - **Installation location:** /QIBM/ProdData/InstallationManager
 - **Agent data location:** /QIBM/UserData/InstallationManager
 - **Registry:** /QIBM/InstallationManager/.ibm/registry/InstallationManager.dat
- Logs are located in the logs directory of Installation Manager's agent data location. For example:

/QIBM/UserData/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.

Note: 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.

Installing the product on IBM i operating systems using response files

You can install WebSphere Application Server Version 8.5 on IBM i operating systems using Installation Manager response files.

Before you begin

Prepare for the installation before using this procedure. See Chapter 5, “Preparing the operating system for installation on IBM i,” on page 27 for more information.

Before you install WebSphere Application Server, ensure that your user profile has *ALLOBJ and *SECADM special authorities.

Install Installation Manager on the system onto which you want to install the product.

- If you want to use the Installation Manager that comes with this product, perform the following actions:

1. Obtain the necessary files.

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 the product repositories on the product media.

- a. Install Installation Manager on your system.

You can install Installation Manager using the product media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

- b. Use 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 with a Passport Advantage ID and password can download the necessary product repositories from the Passport Advantage site.

- a. Download the files from the Passport Advantage site.

- b. Install Installation Manager on your system.

You can install Installation Manager using the product media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

- c. Use Installation Manager to install the product from the downloaded repositories.

- **Access the live repositories, and use web-based installation**

If you have a Passport Advantage ID and password, you can install the product from the web-based repositories.

- a. Install Installation Manager on your system.

You can install Installation Manager using the product media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

- b. Use Installation Manager to install the product from the web-based repository located at

<http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v85>

Note: This location does not contain a web page that you can access using a web browser. This is a remote web-based repository location that you must specify in the response file so that the installation can access the files in this repository.

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

Note: If you do not have a Passport Advantage ID and password, you must install the product from the product repositories on the media or local repositories.

2. Install Installation Manager.

- a. Sign on to the IBM i system with a user profile that has *ALLOBJ and *SECADM special authorities.
- b. On a CL command line, run the **STRQSH** command to start the Qshell command shell.
- c. Make sure that the umask is set to 022.

To verify the umask setting, issue the following command:

```
umask
```

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

```
umask 022
```

- d. Change to the temporary directory where you unpacked the Installation Manager files.
- e. Run the following command in the temporary folder:

```
installc -acceptLicense -log log_file_path_and_name
```

Notes:

- For more information on installing Installation Manager, see the IBM Installation Manager Version 1.5 Information Center.
- Use only the **installc** command to install Installation Manager.
- 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.

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 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 with a Passport Advantage ID and password can download the necessary product repositories from the Passport Advantage site.

1. Download the product repositories from the Passport Advantage site.
2. Use Installation Manager to install the product from the downloaded repositories.

– Access the live repositories, and use web-based installation

If you have a Passport Advantage ID and password, you can use Installation Manager to install the product from the web-based repositories. Use Installation Manager to install the product from the web-based repository located at

<http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v85>

Note: This location does not contain a web page that you can access using a web browser. This is a remote web-based repository location that you must specify in the response file so that the installation can access the files in this repository.

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

Note: If you do not have a Passport Advantage ID and password, you must install the product from the product repositories on the media or local repositories.

Procedure

1. Optional: If the repository requires a username and password, create a keyring file to access this repository.

For more information on creating a keyring file for Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Tip: When creating a keyring file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

2. Sign on to the IBM i system with a user profile that has `*ALLOBJ` and `*SECADM` special authorities.
3. On a CL command line, run the `STRQSH` command to start the Qshell command shell.
4. Make sure that the `umask` is set to `022`.

To verify the `umask` setting, issue the following command:

```
umask
```

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

```
umask 022
```

5. Use a response file to install the product.

Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and install the product. For example:

```
./imcl -acceptLicense  
input $HOME/WASFiles/temp/install_response_file.xml  
-log $HOME/WASFiles/temp/install_log.xml  
-keyring $HOME/WASFiles/temp/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.
- `/QIBM/ProdData/InstallationManager` is the default installation location for Installation Manager files on IBM i systems.
- The program might write important post-installation instructions to standard output.

Read the IBM Installation Manager Version 1.5 Information Center for more information.

Example

The following is an example of a response file for installing the product with no optional features into the `/QIBM/ProdData/WebSphere/AppServer/V85/ND` directory using a web-based repository located at `http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v85`.

```
<?xml version="1.0" encoding="UTF-8"?>  
<agent-input>  
<server>  
  <repository location='http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v85' />  
</server>  
</agent-input>  
<profile id='IBM WebSphere Application Server V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/ND'>  
  <data key='eclipseLocation' value='/QIBM/ProdData/WebSphere/AppServer/V85/ND' />  
  <data key='was.install.os400.profile.location' value='/QIBM/UserData/WebSphere/AppServer/V85/ND' />  
  <data key='user.import.profile' value='false' />  
  <data key='cic.selector.nl' value='en, fr, it, zh, ro, ru, zh_TW, de, ja, pl, es, cs, hu, ko, pt_BR' />  
</profile>
```

```

<install modify='false'>
  <offering profile='IBM WebSphere Application Server V8.5'
    features='core.feature' id='com.ibm.websphere.ND.v85' />
</install>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache'
  value='/QIBM/UserData/InstallationManager/IMShared' />
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='30' />
<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.preserveDownloadedArtifacts' 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' />
</agent-input>

```

Tips:

- Make sure that the repository location points to the web-based or local product repository. For example:

```
<repository location='https://downloads.mycorp.com:8080/WAS_85_repository' />
```

- The following line from the example specifies the default value of the profile location for IBM i:

```
<data key='was.install.os400.profile.location' value='/QIBM/UserData/WebSphere/AppServer/V85/ND' />
```

To override this default location, specify a different location

- The following line from the example specifies the default value of the shared resources directory for IBM i:

```
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/QIBM/UserData/InstallationManager/IMShared' />
```

To override this default location, specify a different location

Note: There is only one shared resources directory for Installation Manager. If there has been an installation on the system in the past, it will use that shared resources directory and not the one specified in the response file.

- 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 Version 1.5 Information Center.

- To install more than one instance of an offering, you must make the profile ID of each additional instance unique. For example:

```

<offering profile='IBM WebSphere Application Server V8.5 - Another User's WAS ND'
  features='core.feature' id='com.ibm.websphere.ND.v85' />

```

This must be changed in both places that specify the profile ID in the response file.

Here are some examples of changes that you could make to manipulate this response file to perform alternative actions.

- To alter the location of the installation, simply change the installation location. For example:

Replace

```
<profile id='IBM WebSphere Application Server V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/ND'>
```


with

```
<profile id='IBM WebSphere Application Server V8.5' installLocation='/home/user/IBM/WebSphere/AppServer/V85/Server'>
```

- To install from a local repository instead of the live remote repository, replace the repository location. For example:

Replace

```
<repository location='http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v85' />
```

with

```
<repository location='/home/user/repositories/WAS85/local-repositories' />
```

- To add the optional features, add each desired feature in the offering as an entry in a comma-separated list.

In the following list, the offering IDs to be used in the response files are enclosed in parentheses:

- WebSphere Application Server full profile (core.feature)

Installing this application-server feature gives you the traditional standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation, offering broad programming model choice and low total cost of ownership through high performance and high manageability.

- EJBDeploy tool for pre-EJB 3.0 modules (ejbdeploy)

This option installs the EJBDeploy tool for pre-EJB 3.0 modules.

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.

Note: Unexpected errors might occur if applications that are provided with IBM WebSphere Application Server, such as the samples, require the optional EJBDeploy tool for pre-EJB 3.0 modules but the feature is not installed. If you deploy and use applications that might require pre-EJB 3.0 modules, include the optional EJBDeploy feature in all WebSphere Application Server installations that will be used by servers running the pre-EJB 3.0 applications.

- Standalone thin clients, resource adapters, and embeddable containers

- Standalone thin clients and resource adapters (thinclient)

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 (embeddablecontainer)

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 (samples)

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.

- WebSphere Application Server Liberty profile (`liberty`)

Installing this application-server feature gives you a lightweight profile of the application server along with a simplified configuration approach for the development environment. Its fast restart times, small size, and ease of use make it a good option for building web applications that do not require the full JEE environment of traditional enterprise application server profiles. The Liberty profile also can be used in production; and because it is a dynamic configuration, the application server provisions only the features required by the running applications.

Notes:

- The features `samples`, `thinclient`, `embeddablecontainer`, and `ejbdeploy` are subfeatures of `core.feature`.
- If no features are specified, the default features (`core.feature`, `ejbdeploy`, `thinclient`, and `embeddablecontainer`) are installed. To install only the features that you want, specify the list of features explicitly.
- You must install `core.feature` (full WebSphere Application Server profile), `liberty` (Liberty profile), or both.
- You cannot use the Installation Manager modify, update, or rollback functions to modify this installation later and add or remove `core.feature` (full WebSphere Application Server profile) or `liberty` (Liberty profile). You can use these functions to add or remove the `ejbdeploy`, `thinclient`, `embeddablecontainer`, or `samples` subfeature of `core.feature` later.

For example, to install the samples:

Replace

```
<offering profile='IBM WebSphere Application Server V8.5'  
  features='core.feature' id='com.ibm.websphere.ND.v85' />
```

with

```
<offering profile='IBM WebSphere Application Server V8.5'  
  features='core.feature,samples' id='com.ibm.websphere.ND.v85' />
```

Tip: If no features are specified, the default features (`core.feature`, `ejbdeploy`, `thinclient`, and `embeddablecontainer`) are installed. To install only the features that you want, specify the list of features explicitly.

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 **manageprofiles** command.

The following are examples of using the **manageprofiles** command to create a default standalone application server profile and a default cell profile. These examples are based on the following assumptions:

- The `samples` feature is installed.
- Security is to be enabled.
- The system host name is `myhost.abc.com`.
- The `appserver_install_root` is `/QIBM/ProdData/WebSphere/AppServer/V85/ND`.
- The `user_data_root` is `/QIBM/UserData/WebSphere/AppServer/V85/ND`.
- The administrative user name is `wasadmin`.
- The password is `password`.

Default standalone application server:

```
manageprofiles -create  
-portsFile /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/default/actions/portsUpdate/portdef.props  
-serverName server1  
-nodeName myhost  
-hostName myhost.abc.com
```

```
-cellName myhost
-adminUserName wasadmin
-adminPassword password
-templatePath /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/default
-enableAdminSecurity true
-profileName default
```

Default cell profile:

1. Create the deployment manager portion of the default cell profile:

```
manageprofiles -create
-appServerNodeName myhost
-portsFile /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/cell/dmgr/actions/portsUpdate/portdef.props
-nodeName myhostManager
-nodeProfilePath /QIBM/UserData/WebSphere/AppServer/V85/ND/profiles/default
-nodePortsFile /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/cell/dmgr/actions/portsUpdate/nodeportdef.props
-hostName myhost.abc.com
-cellName myhostNetwork
-adminUserName wasadmin
-adminPassword password
-templatePath /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/cell/dmgr
-enableAdminSecurity true
-profileName dmgr
```

2. Create the application server portion of the cell profile:

```
manageprofiles -create
-appServerNodeName myhost
-portsFile /QIBM/UserData/WebSphere/AppServer/V85/ND/profiles/dmgr/properties/portdef.props
-dmgrProfilePath /QIBM/UserData/WebSphere/AppServer/V85/ND/profiles/dmgr
-serverName server1
-nodeName myhostManager
-nodePortsFile /QIBM/UserData/WebSphere/AppServer/V85/ND/profiles/dmgr/properties/nodeportdef.props
-hostName myhost.abc.com
-cellName myhostNetwork
-adminUserName wasadmin
-adminPassword password
-isDefault
-templatePath /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/cell/default
-enableAdminSecurity true
-profileName default
```

Installing the product on IBM i operating systems using the command line

You can install WebSphere Application Server Version 8.5 using the Installation Manager command line.

Before you begin

Prepare for the installation before using this procedure. See Chapter 5, “Preparing the operating system for installation on IBM i,” on page 27 for more information.

Important: Before installing WebSphere Application Server Version 8, you must read the license agreement that you can find with the product files. Signify your acceptance of the license agreement by specifying `-acceptLicense` in the command as described below.

Install Installation Manager on the system onto which you want to install the product.

- If you want to use the Installation Manager that comes with this product, perform the following actions:

1. Obtain the necessary files.

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 the product repositories on the product media.

- a. Install Installation Manager on your system.

You can install Installation Manager using the product media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

- b. Use 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 with a Passport Advantage ID and password can download the necessary product repositories from the Passport Advantage site.

- a. Download the files from the Passport Advantage site.
- b. Install Installation Manager on your system.

You can install Installation Manager using the product media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

- c. Use Installation Manager to install the product from the downloaded repositories.

– **Access the live repositories, and use web-based installation**

If you have a Passport Advantage ID and password, you can install the product from the web-based repositories.

- a. Install Installation Manager on your system.

You can install Installation Manager using the product media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

- b. Use Installation Manager to install the product from the web-based repository located at

<http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v85>

Note: This location does not contain a web page that you can access using a web browser. This is a remote web-based repository location that you must specify for the value of the `-repositories` parameter so that the `imcl` command can access the files in this repository to install the product.

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

Note: If you do not have a Passport Advantage ID and password, you must install the product from the product repositories on the media or local repositories.

2. Choose three separate locations for Installation Manager's binaries, runtime data (agent data), and shared data locations.
3. Install Installation Manager using the Installation Manager command line.
 - a. Sign on to the IBM i system with a user profile that has *ALLOBJ and *SECADM special authorities.
 - b. On a CL command line, run the `STRQSH` command to start the Qshell command shell.
 - c. Make sure that the umask is set to 022.

To verify the umask setting, issue the following command:

```
umask
```

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

```
umask 022
```

- d. Change to the location containing the Installation Manager installation files, and run the following command:

```
installc -acceptLicense -log log_file_path_and_name
```

Notes:

- For more information on installing Installation Manager, see the IBM Installation Manager Version 1.5 Information Center.
- Use only the `installc` command to install Installation Manager.
- 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.

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 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 with a Passport Advantage ID and password can download the necessary product repositories from the Passport Advantage site.

1. Download the product repositories from the Passport Advantage site.
2. Use Installation Manager to install the product from the downloaded repositories.

– **Access the live repositories, and use web-based installation**

If you have a Passport Advantage ID and password, you can use Installation Manager to install the product from the web-based repositories. Use Installation Manager to install the product from the web-based repository located at

<http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v85>

Note: This location does not contain a web page that you can access using a web browser. This is a remote web-based repository location that you must specify for the value of the `-repositories` parameter so that the `imcl` command can access the files in this repository to install the product.

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

Note: If you do not have a Passport Advantage ID and password, you must install the product from the product repositories on the media or local repositories.

Procedure

1. Optional: If the repository requires a username and password, create a keyring file to access this repository.

For more information on creating a keyring file for Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Tip: When creating a keyring file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

2. Choose three separate locations for the product's binaries, runtime data (agent data), and shared data locations.
3. Sign on to the IBM i system with a user profile that has `*ALLOBJ` and `*SECADM` special authorities.
4. On a CL command line, run the `STRQSH` command to start the Qshell command shell.
5. Make sure that the `umask` is set to `022`.

To verify the `umask` setting, issue the following command:

```
umask
```

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

```
umask 022
```

6. Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.
7. Use the `imcl` command to install the product.

```
./imcl install com.ibm.websphere.ND.v85_offering_version,optional_feature_ID  
-repositories source_repository  
-installationDirectory installation_directory  
-sharedResourcesDirectory shared_directory  
-accessRights access_mode  
-preferences preference_key=value  
-properties property_key=value  
-keyring keyring_file -password password  
-acceptLicense
```

Tips:

- The relevant terms and conditions, notices, and other information are provided in the license-agreement files in the `1afiles` or `product_name/1afiles` subdirectory of the installation image or repository for this product.
- You can install a list of features that are separated by commas.

In the following list, the optional offering IDs are enclosed in parentheses:

- WebSphere Application Server full profile (`core.feature`)

Installing this application-server feature gives you the traditional standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation, offering broad programming model choice and low total cost of ownership through high performance and high manageability.

- EJBDeploy tool for pre-EJB 3.0 modules (`ejbdeploy`)

This option installs the EJBDeploy tool for pre-EJB 3.0 modules.

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.

Note: Unexpected errors might occur if applications that are provided with IBM WebSphere Application Server, such as the samples, require the optional EJBDeploy tool for pre-EJB 3.0 modules but the feature is not installed. If you deploy and use applications that might require pre-EJB 3.0 modules, include the optional EJBDeploy feature in all WebSphere Application Server installations that will be used by servers running the pre-EJB 3.0 applications.

- Standalone thin clients, resource adapters, and embeddable containers

- Standalone thin clients and resource adapters (`thinclient`)

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 (`embeddablecontainer`)

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 (`samples`)

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.

- WebSphere Application Server Liberty profile (`liberty`)

Installing this application-server feature gives you a lightweight profile of the application server along with a simplified configuration approach for the development environment. Its fast restart times, small size, and ease of use make it a good option for building web applications that do not require the full JEE environment of traditional enterprise

application server profiles. The Liberty profile also can be used in production; and because it is a dynamic configuration, the application server provisions only the features required by the running applications.

Notes:

- The features `samples`, `thinclient`, `embeddablecontainer`, and `ejbdeploy` are subfeatures of `core.feature`.
 - If no features are specified, the default features (`core.feature`, `ejbdeploy`, `thinclient`, and `embeddablecontainer`) are installed. To install only the features that you want, specify the list of features explicitly.
 - You must install `core.feature` (full WebSphere Application Server profile), `liberty` (Liberty profile), or both.
 - You cannot use the Installation Manager `modify`, `update`, or `rollback` functions to modify this installation later and add or remove `core.feature` (full WebSphere Application Server profile) or `liberty` (Liberty profile). You can use these functions to add or remove the `ejbdeploy`, `thinclient`, `embeddablecontainer`, or `samples` subfeature of `core.feature` later.
- The *offering_version*, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to install (8.5.0.20110503_0200 for example).
 - If *offering_version* is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
 - If *offering_version* is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
./imcl listAvailablePackages -repositories source_repository
```

- You can also specify `none`, `recommended` or `all` with the `-installFixes` argument to indicate which interim fixes you want installed with the offering.
 - If the offering version is **not** specified, the `-installFixes` option defaults to `all`.
 - If the offering version is specified, the `-installFixes` option defaults to `none`.
- For initial installations, it is a good practice to specify the *user_data_root*; otherwise, the default value for the *user_data_root*, `/QIBM/UserData/WebSphere/AppServer/V85/ND`, is used. Use the `was.install.os400.profile.location` property to specify the *user_data_root*. If the *user_data_root* is to be `/QIBM/UserData/WebSphere/AppServer/V85/ND`, for example, specify `-properties was.install.os400.profile.location=/QIBM/UserData/WebSphere/AppServer/V85/ND` on the `imcl` installation command.
- The program might write important post-installation instructions to standard output.

For more information on using the `imcl` command to install the product, see the IBM Installation Manager Version 1.5 Information Center.

Example

Here is an example of using the `imcl` command to install Websphere Application Server:

```
./imcl install com.ibm.websphere.ND.v85
-repositories https://downloads.mycorp.com:8080/WAS_85_repository
-installationDirectory /QIBM/ProdData/WebSphere/AppServer/V85/ND
-properties was.install.os400.profile.location=/QIBM/UserData/WebSphere/AppServer/V85/ND
-sharedResourcesDirectory /QIBM/UserData/InstallationManager/IMShared
-keyring $HOME/WASFiles/temp/im.keyring
-acceptLicense
```

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 `manageprofiles` command.

The following are examples of using the **manageprofiles** command to create a default standalone application server profile and a default cell profile. These examples are based on the following assumptions:

- The samples feature is installed.
- Security is to be enabled.
- The system host name is myhost.abc.com.
- The *appserver_install_root* is /QIBM/ProdData/WebSphere/AppServer/V85/ND.
- The *user_data_root* is /QIBM/UserData/WebSphere/AppServer/V85/ND.
- The administrative user name is wasadmin.
- The password is password.

Default standalone application server:

```
manageprofiles -create
-portsFile /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/default/actions/portsUpdate/portdef.props
-serverName server1
-nodeName myhost
-hostName myhost.abc.com
-cellName myhost
-adminUserName wasadmin
-adminPassword password
-templatePath /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/default
-enableAdminSecurity true
-profileName default
```

Default cell profile:

1. Create the deployment manager portion of the default cell profile:

```
manageprofiles -create
-appServerNodeName myhost
-portsFile /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/cell/dmgr/actions/portsUpdate/portdef.props
-nodeName myhostManager
-nodeProfilePath /QIBM/UserData/WebSphere/AppServer/V85/ND/profiles/default
-nodePortsFile /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/cell/dmgr/actions/portsUpdate/nodeportdef.props
-hostName myhost.abc.com
-cellName myhostNetwork
-adminUserName wasadmin
-adminPassword password
-templatePath /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/cell/dmgr
-enableAdminSecurity true
-profileName dmgr
```

2. Create the application server portion of the cell profile:

```
manageprofiles -create
-appServerNodeName myhost
-portsFile /QIBM/UserData/WebSphere/AppServer/V85/ND/profiles/dmgr/properties/portdef.props
-dmgrProfilePath /QIBM/UserData/WebSphere/AppServer/V85/ND/profiles/dmgr
-serverName server1
-nodeName myhostManager
-nodePortsFile /QIBM/UserData/WebSphere/AppServer/V85/ND/profiles/dmgr/properties/nodeportdef.props
-hostName myhost.abc.com
-cellName myhostNetwork
-adminUserName wasadmin
-adminPassword password
-isDefault
-templatePath /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/cell/default
-enableAdminSecurity true
-profileName default
```

Installing the product remotely on IBM i operating systems using the **iRemoteInstall** command

You can use the **iRemoteInstall** command to install IBM Installation Manager or a WebSphere Application Server product offering from a Windows workstation to a remote target IBM i system.

Before you begin

Prepare for the installation before using this procedure. See Chapter 5, “Preparing the operating system for installation on IBM i,” on page 27 for more information.

The product offering repository files or the IBM Installation Manager for IBM i installation kit compressed file must be available on the Windows system.

Important: You must set your JAVA_HOME environment variable to your IBM Installation Manager JRE home before running the command directly from the product media. You do not need to set your JAVA_HOME environment variable to your IBM Installation Manager JRE home before running the command from a WebSphere Customization Toolbox installation.

Restrictions:

- The `iRemoteInstall` command does not support keyring files used to pass confidential information. You must use the physical media or download the installation files to your local system.
- The `iRemoteInstall` command does not support the use of response files.

About this task

Note: By running this script, you accept the terms of the product license. The relevant terms and conditions, notices, and other information are provided in the license-agreement files in the `1afiles` or `product_name/1afiles` subdirectory of the installation image or repository for this product.

Location of the iRemoteInstall command:

The `iRemoteInstall` command is located in the following directory when it has been installed as part of the WebSphere Customization Toolbox:

```
wct_root/Remote_Installation_Tool_for_IBM_i
```

Tip: A version of this utility that is current when the product is released is also available on the media or installation image. You can run the command directly from the media connected to a Windows system to install the offering on a remote target IBM i system. This version of the utility is located at the following location:

```
media_root\Remote_Installation_Tool_for_IBM_i\iRemoteInstall.bat
```

where `media_root` is the root directory of the media or installation image containing the product or supplements.

Syntax of the iRemoteInstall command:

```
iRemoteInstall.bat
-hostname i5_hostname
-username user_login_name
-password user_login_password
-iminstit im_install_kit_file_path_and_name | -wasoid was_offering_id
-wasrepoloc was_install_file_location
-appdataloc im_agent_data_location
-wasinstloc was_install_location
-wassharedloc was_shared_location
-features feature_ID_1,feature_ID_2, . . .
-waslangs lang_ID_1,lang_ID_2, . . .
-properties key=value,key=value, . . .
-log log_file_path_and_name
-trace
-version
-help
```

Parameters of the iRemoteInstall command:

-hostname *i5_hostname*

Specifies the host name of the target IBM i machine to which Installation Manager or the WebSphere Application Server product offering is going to be installed

This parameter is required.

-username *user_login_name*

Specifies the login name of the user who is performing the Installation Manager or WebSphere Application Server remote installation

This user must be a valid user for the target IBM i system with *ALLOBJ and *SECADM special authorization.

-password *user_login_password*

Specifies the login password of the user specified in -username

-iminstkit *im_install_kit_file_name*

Specifies the location of the Installation Manager for IBM i installation kit

You must include the path if it is not in the same directory as the command.

This parameter is required.

-wasoid *was_offering_id*

Specifies the ID of the WebSphere Application Server product offering being installed

Example values are base, nd, express, etc. This parameter is not case sensitive.

The value to use can be found in the product offering ID. If the offering ID is com.ibm.websphere.XXX.v85, for example, the -wasoid value should be XXX. The IDs for various WebSphere Application Server product offerings can be found in “WebSphere Application Server Version 8.5 product offerings for supported operating systems” on page 7

-wasrepoloc *was_install_file_location*

Specifies the location of the WebSphere Application Server installation repository

This option must be specified if the -wasoid parameter is specified.

-appdataloc *im_agent_data_location*

Specifies the location of the Installation Manager agent data

If no value is specified for this parameter, it is set to the default value of /QIBM/UserData/InstallationManager.

-wasinstloc *was_install_location*

Specifies the location of the WebSphere Application Server installation

If no value is specified for this parameter, it is set to the default value of /QIBM/WAS85/AppServer.

-wassharedloc *was_shared_location*

Specifies the location of the WebSphere Application Server shared location

If no value is specified for this parameter, it is set to the default value of /QIBM/WAS85/AppServer_Shared.

-features *feature_ID_1,feature_ID_2, . . .*

Specifies the features to be installed

The feature IDs must be separated by commas (.). For example:

core.feature,ejbdeploy,thinclient,embeddablecontainer,samples,liberty

Tip: If no features are specified, the default features (core.feature, ejbdeploy, thinclient, and embeddablecontainer) are installed. To install only the features that you want, specify the list of features explicitly.

-waslangs *lang_ID_1,lang_ID_2, . . .*

Specifies the languages for which translated content should be installed

The language IDs must be separated by commas (.). For example:

en,fr,it,zh,ro,ru,zh_TW,de,ja,pl,es,cs,hu,ko,pt_BR

English is installed even if it is not specified in the language list.

If this parameter is not specified, only the English translation content is installed by default.

If languages are specified using both this parameter and the `-properties` parameter, the values specified in this parameter are used.

-properties *key=value,key=value, . . .*
Specifies package-group (profile) properties

-log *log_file_path_and_name*
Turns on the log, and sends all messages to the specified file and location

The path can be absolute (c:\temp\mylog.log for example) or relative (..\mylog.log for example).

Because you can append multiple installation actions into the same log, the actual name of a log file that is generated is *log_file_path_and_name.x.log*, where *x* is the number of the log file from 0 to 29. The maximum log file size is approximately 10 MB; and the maximum number of log files generated is 30.

-trace
Provides trace output of what the command checks and what the command discovers

-version
Displays the version information for the command

-help
Displays usage information for the command

Procedure

1. Log in to the IBM i machine using the IBM Personal Communications tool, or telnet with TN5250 to the IBM i machine.
2. If TCP/IP is not started or if you do not know if TCP/IP is started, enter the following command on the Control Language (CL) command line:

```
STRTCP
```

3. Verify that the host server jobs are started on your IBM i server.
The host server jobs allow the installation code to run on IBM i.
Enter the following command on the CL command line:

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

4. Verify that your user profile has *ALLOBJ and *SECADM special authorities.
5. Run the **iRemoteInstall** command in the temporary directory to install Installation Manager or the Websphere Application Server product offering.

In order to install a Websphere Application Server product offering, Installation manager must already be installed on the target system.

Example

Here is an example of installing IBM Installation Manager with the **iRemoteInstall** command:

```
./iRemoteInstall  
-hostname iserver1.somedomain.com  
-username wasadmin -password mypwd  
-iminstkit E:\agent.installer.os400.motif.ppc_1.4.3000.20101206_0100.zip
```

Here is an example of installing WebSphere Application Server with the **iRemoteInstall** command:

```
./iRemoteInstall  
-hostname iserver1.somedomain.com  
-username wasadmin -password mypwd  
-wasoid ND  
-wasrepoloc E:\repository
```

What to do next

After you install WebSphere Application Server, you can create a standalone application server profile, management profile, managed (custom) profile, cell profile, or secure proxy profile by running the **manageprofiles** command on the IBM i system containing the WebSphere Application Server installation.

The following are examples of using the **manageprofiles** command to create a default standalone application server profile and a default cell profile. These examples are based on the following assumptions:

- The samples feature is installed.
- Security is to be enabled.
- The system host name is `myhost.abc.com`.
- The `appserver_install_root` is `/QIBM/ProdData/WebSphere/AppServer/V85/ND`.
- The `user_data_root` is `/QIBM/UserData/WebSphere/AppServer/V85/ND`.
- The administrative user name is `wasadmin`.
- The password is `password`.

Default standalone application server:

```
manageprofiles -create
-portsFile /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/default/actions/portsUpdate/portdef.props
-serverName server1
-nodeName myhost
-hostName myhost.abc.com
-cellName myhost
-adminUserName wasadmin
-adminPassword password
-templatePath /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/default
-enableAdminSecurity true
-profileName default
```

Default cell profile:

1. Create the deployment manager portion of the default cell profile:

```
manageprofiles -create
-appServerNodeName myhost
-portsFile /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/cell/dmgr/actions/portsUpdate/portdef.props
-nodeName myhostManager
-nodeProfilePath /QIBM/UserData/WebSphere/AppServer/V85/ND/profiles/default
-nodePortsFile /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/cell/dmgr/actions/portsUpdate/nodeportdef.props
-hostName myhost.abc.com
-cellName myhostNetwork
-adminUserName wasadmin
-adminPassword password
-templatePath /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/cell/dmgr
-enableAdminSecurity true
-profileName dmgr
```

2. Create the application server portion of the cell profile:

```
manageprofiles -create
-appServerNodeName myhost
-portsFile /QIBM/UserData/WebSphere/AppServer/V85/ND/profiles/dmgr/properties/portdef.props
-dmgrProfilePath /QIBM/UserData/WebSphere/AppServer/V85/ND/profiles/dmgr
-serverName server1
-nodeName myhostManager
-nodePortsFile /QIBM/UserData/WebSphere/AppServer/V85/ND/profiles/dmgr/properties/nodeportdef.props
-hostName myhost.abc.com
-cellName myhostNetwork
-adminUserName wasadmin
-adminPassword password
-isDefault
-templatePath /QIBM/ProdData/WebSphere/AppServer/V85/ND/profileTemplates/cell/default
-enableAdminSecurity true
-profileName default
```

Installing and removing features on IBM i operating systems using response files

You can install and remove a product feature using Installation Manager response files.

About this task

Perform this procedure to use Installation Manager to install or remove a feature silently using a response file.

Like other Installation Manager operations, you can invoke a modification using the `imcl` command-line tool. Go to the IBM Installation Manager Version 1.5 Information Center for more information.

Optional features: In the following list of optional features, the offering names to be used in the response files are enclosed in parentheses:

- EJBDeploy tool for pre-EJB 3.0 modules (`ejbdeploy`)

This option installs the EJBDeploy tool for pre-EJB 3.0 modules.

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: Unexpected errors might occur if applications that are provided with IBM WebSphere Application Server, such as the samples, require the optional EJBDeploy tool for pre-EJB 3.0 modules but the feature is not installed. If you deploy and use applications that might require pre-EJB 3.0 modules, include the optional EJBDeploy feature in all WebSphere Application Server installations that will be used by servers running the pre-EJB 3.0 applications.

- Standalone thin clients, resource adapters, and embeddable containers

- Standalone thin clients and resource adapters (`thinclient`)

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 (`embeddablecontainer`)

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 (`samples`)

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.

Restriction: You cannot use the Installation Manager to modify an installation and add or remove the full WebSphere Application Server profile feature or the Liberty profile feature.

Procedure

1. Optional: If the repository requires a username and password, create a keyring file to access this repository.

For more information on creating a keyring file for Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Tip: When creating a keyring file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

2. Sign on to the IBM i system with a user profile that has `*ALLOBJ` and `*SECADM` special authorities.
3. On a CL command line, run the `STRQSH` command to start the Qshell command shell.
4. Use a response file to install or remove a feature.

Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and modify the product. For example:

```
./imcl
input $HOME/WASFiles/temp/modify_response_file.xml
-log $HOME/WASFiles/temp/modify_log.xml
-keyring $HOME/WASFiles/temp/im.keyring
```

Note: The program might write important post-installation instructions to standard output.

For more information on using Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Example

- Here are examples of response files for modifying the features in an installation:
 - Here is a response file that adds the sample applications feature to an existing product that is installed in the `/QIBM/ProdData/WebSphere/AppServer/V85/ND` directory:

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<server>
  <repository location='https://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v85'/>
</server>
<profile id='IBM WebSphere Application Server V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/ND'>
  <data key='eclipseLocation' value='/QIBM/ProdData/WebSphere/AppServer/V85/ND'/>
  <data key='was.install.os400.profile.location' value='/QIBM/UserData/WebSphere/AppServer/V85/ND'/>
  <data key='user.import.profile' value='false'/>
  <data key='cic.selector.nl' value='en, fr, it, zh, ro, ru, zh_TW, de, ja, pl, es, cs, hu, ko, pt_BR'/>
</profile>
<install modify='true'>
  <offering profile='IBM WebSphere Application Server V8.5' features='samples' id='com.ibm.websphere.ND.v85'/>
</install>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/QIBM/UserData/InstallationManager/IMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='30'/>
<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.preserveDownloadedArtifacts' 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'/>
</agent-input>
```

- To alter this response file to remove a feature, simply change the `install` tags to `uninstall`. Here is the same response file modified to remove the standalone thin clients and resource adapters feature:

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<server>
  <repository location='https://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v85'/>
</server>
<profile id='IBM WebSphere Application Server V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/ND'>
  <data key='eclipseLocation' value='/QIBM/ProdData/WebSphere/AppServer/V85/ND'/>
  <data key='was.install.os400.profile.location' value='/QIBM/UserData/WebSphere/AppServer/V85/ND'/>
  <data key='user.import.profile' value='false'/>
  <data key='cic.selector.nl' value='en, fr, it, zh, ro, ru, zh_TW, de, ja, pl, es, cs, hu, ko, pt_BR'/>
</profile>
<uninstall modify='true'>
  <offering profile='IBM WebSphere Application Server V8.5' features='thinclient' id='com.ibm.websphere.ND.v85'/>
</uninstall>
```

```

<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/QIBM/UserData/InstallationManager/IMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='30'/>
<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.preserveDownloadedArtifacts' 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'/>
</agent-input>

```

- To combine adding and removing features using a single response file, add both an install action and an uninstall action. Here is the same response file combining the previous two examples, installing the sample applications while removing the standalone thin clients and resource adapters feature:

```

<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<server>
  <repository location='https://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v85'/>
</server>
<profile id='IBM WebSphere Application Server V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/ND'>
  <data key='eclipseLocation' value='/QIBM/ProdData/WebSphere/AppServer/V85/ND'/>
  <data key='was.install.os400.profile.location' value='/QIBM/UserData/WebSphere/AppServer/V85/ND'/>
  <data key='user.import.profile' value='false'/>
  <data key='cic.selector.nl' value='en, fr, it, zh, ro, ru, zh_TW, de, ja, pl, es, cs, hu, ko, pt_BR'/>
</profile>
<install modify='true'>
  <offering profile='IBM WebSphere Application Server V8.5' features='samples' id='com.ibm.websphere.ND.v85'/>
</install>
<uninstall modify='true'>
  <offering profile='IBM WebSphere Application Server V8.5' features='thinclient' id='com.ibm.websphere.ND.v85'/>
</uninstall>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/QIBM/UserData/InstallationManager/IMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='30'/>
<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.preserveDownloadedArtifacts' 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'/>
</agent-input>

```

- Here is an example of the `imcl` command for modifying the features in an installation:

```

./imcl.exe modify com.ibm.websphere.ND.v85
-addFeatures samples
-removeFeatures thinclient,ejbdeploy,embeddablecontainer
-repositories http://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v85
-installationDirectory /QIBM/ProdData/WebSphere/AppServer/V85/ND
-keyring /var/keyring.file.keyring -password password

```

Installing interim fixes on IBM i operating systems using the command line

Product fix packs contain bundled service to bring WebSphere Application Server up to a new product level. Interim fixes provide corrective service for specific known problems. You can use the IBM Installation Manager command-line function to update the product with the fixes that are available for your service level of WebSphere Application Server Version 8.5.

Before you begin

Contact the IBM Software Support Center for information about upgrades for WebSphere Application Server for IBM i. The most current information is available from the IBM Software Support Center and Fix Central.

IBM Installation Manager is used to apply product maintenance to WebSphere Application Server for IBM i.

About this task

Use this procedure whenever you want to apply a new interim fix to your system.

Tip: You can also install interim fixes using silent response files with Installation Manager. For information on creating and using response files, read the IBM Installation Manager Version 1.5 Information Center.

Restriction: You cannot use the `iRemoteInstall` command to install an interim fix.

Procedure

1. For a list of interim fixes that are available for WebSphere Application Server Version 8.x and specific information about each interim fix, perform the following actions.
 - a. Go to Fix Central.
 - b. Select **WebSphere** as the product group.
 - c. Select **WebSphere Application Server** as the product.
 - d. Select the version of the product to be updated (8.x.x.x).
 - e. Select your operating system as the platform, and click **Continue**.
 - f. Select **Browse for fixes**, and click **Continue**.
 - g. Click **More Information** under each fix to view information about the fix.
 - h. **Recommendation:** Make a list of the names of the interim fixes that you would like to install.
2. Update WebSphere Application Server Version 8.x with the interim fixes using one of the following procedures.

- Access the live service repository that contains the fixes, and use web-based updating.

Use Installation Manager on your local system to update WebSphere Application Server Version 8.x with the interim fixes from the live web-based service repositories.

- For the live service repositories, use the same URLs as those used for the generally available product-offering repositories during installation. These URLs are based on the following pattern:

`http://www.ibm.com/software/repositorymanager/offering_ID`

where *offering_ID* is the offering ID that you can find in “WebSphere Application Server Version 8.5 product offerings for supported operating systems” on page 7.

- These locations do not contain web pages that you can access using a web browser. They are remote web-based repository locations that you specify for Installation Manager so that it can maintain the product.

To install an interim fix from a service repository, perform the following actions:

- a. If you do not already have an Installation Manager credentials file containing your IBM software user ID and password, create one that will allow you to access the repository.

Note: These are the credentials that you use to access protected IBM software websites. For information on creating a keyring file for Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Tip: When creating a keyring file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

- b. Sign on to the IBM i system with a user profile that has `*ALLOBJ` and `*SECADM` special authorities.
- c. Stop all servers and applications on the WebSphere Application Server installation that is being updated.
- d. On a CL command line, run the `STRQSH` command to start the Qshell command shell.
- e. Make sure that the `umask` is set to `022`.

To verify the umask setting, issue the following command:

```
umask
```

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

```
umask 022
```

- f. Change to the *Installation_Manager_binaries/eclipse/tools* directory, where *Installation_Manager_binaries* is the installation root directory for the Installation Manager.

On IBM i systems, the root directory for the Installation Manager is */QIBM/ProdData/InstallationManager*.

- g. Install the interim fix.

```
./imcl install interim_fix_name  
-installationDirectory product_installation_location  
-repositories repository_URL  
-keyring keyring_file
```

Tip: If a keyring file is specified and the keyring is password protected, you also need to specify *-password password*.

- h. **Optional:** List all installed packages to verify the installation:

```
./imcl listInstalledPackages -long
```

- Download the files that contain the fixes from Fix Central, and use local updating.

You can download compressed files that contain the fixes from Fix Central. Each compressed fix file contains an Installation Manager repository for the fix and usually has a .zip extension. After downloading the fix files, you can use Installation Manager to update WebSphere Application Server Version 8.x with the interim fixes.

- a. To download the interim fixes, perform the following actions:

- 1) Go to Fix Central.
- 2) Select **WebSphere** as the product group.
- 3) Select **WebSphere Application Server** as the product.
- 4) Select the version of the product to be updated (8.x.x.x).
- 5) Select your operating system as the platform, and click **Continue**.
- 6) Select **Browse for fixes**, and click **Continue**.
- 7) Select the interim fixes that you want to download, and click **Continue**.
- 8) Select your download options, and click **Continue**.
- 9) Click **I agree** to agree to the terms and conditions.
- 10) Click **Download now** to download the interim fixes.
- 11) Transfer the compressed fix files in binary format to the IBM i system on which they will be installed.

- b. To install an interim fix from a downloaded file, perform the following actions:

- 1) Sign on to the IBM i system with a user profile that has *ALLOBJ and *SECADM special authorities.
- 2) Stop all servers and applications on the WebSphere Application Server installation that is being updated.
- 3) On a CL command line, run the STRQSH command to start the Qshell command shell.
- 4) Make sure that the umask is set to 022.

To verify the umask setting, issue the following command:

```
umask
```

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

```
umask 022
```

- 5) Change to the *Installation_Manager_binaries/eclipse/tools* directory, where *Installation_Manager_binaries* is the installation root directory for the Installation Manager. On IBM i systems, the root directory for the Installation Manager is */QIBM/ProdData/InstallationManager*.
- 6) Install the interim fix.


```
./imcl install interim_fix_name
      -installationDirectory product_installation_location
      -repositories compressed_file
```
- 7) **Optional:** List all installed packages to verify the installation:


```
./imcl listInstalledPackages -long
```

Installing fix packs on IBM i operating systems using response files

You can update this product to a later version using Installation Manager response files.

Before you begin

Tip: As an alternative to the procedure that is described in this article, Installation Manager allows you to use the **updateAll** command in a response file or on the command line to search for and update all installed packages. Use this command only if you have full control over which fixes are contained in the targeted repositories. If you create and point to a set of custom repositories that include only the specific fixes that you want to install, you should be able to use this command confidently. If you enable searching service repositories or install fixes directly from other live web-based repositories, then you might not want to select this option so that you can select only the fixes that you want to install using the **-installFixes** option with the **install** command on the command line or the **installFixes** attribute in a response file.

About this task

Restriction: You cannot use the Installation Manager to upgrade an installation and add or remove the full WebSphere Application Server profile feature or the Liberty profile feature.

Procedure

1. Optional: If the repository requires a username and password, create a keyring file to access this repository.

For more information on creating a keyring file for Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Tip: When creating a keyring file, append */repository.config* at the end of the repository URL location if the **imutilsc** command is unable to find the URL that is specified.

2. Sign on to the IBM i system with a user profile that has ***ALLOBJ** and ***SECADM** special authorities.
3. On a CL command line, run the **STRQSH** command to start the Qshell command shell.
4. Use a response file to update the product.

Change to the *eclipse/tools* subdirectory in the directory where you installed Installation Manager, and update the product. For example:

```
./imcl -acceptLicense
input $HOME/WASFiles/temp/update_response_file.xml
-log $HOME/WASFiles/temp/update_log.xml
-keyring $HOME/WASFiles/temp/im.keyring
```

Note: The program might write important post-installation instructions to standard output.

For more information on using Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Example

The following is an example of a response file for updating the product to a later version.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<server>
  <repository location='https://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v85' />
</server>
<profile id='IBM WebSphere Application Server V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/ND'>
  <data key='eclipseLocation' value='/QIBM/ProdData/WebSphere/AppServer/V85/ND' />
  <data key='was.install.os400.profile.location' value='/QIBM/UserData/WebSphere/AppServer/V85/ND' />
  <data key='user.import.profile' value='false' />
  <data key='cic.selector.nl' value='en, fr, it, zh, ro, ru, zh_TW, de, ja, pl, es, cs, hu, ko, pt_BR' />
</profile>
<install modify='false'>
  <offering profile='IBM WebSphere Application Server V8.5' id='com.ibm.websphere.ND.v85'
    version='8.5.0.20101025_2108' features='core.feature' />
</install>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/QIBM/UserData/InstallationManager/IMShared' />
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='30' />
<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.preserveDownloadedArtifacts' 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' />
</agent-input>
```

Tips:

- The profile ID (`<profile . . . id='profile_ID'>` and `<offering . . . profile='profile_ID'>`) can be found when you run the `imcl listInstallationDirectories -verbose` command from the `eclipse/tools` subdirectory in the directory where you installed Installation Manager. It is the same as the package group's name.
- The offering ID (`<offering . . . id='offering_ID'>`) can be found in the Install Manager Offering ID section of the report that is generated when you run the **historyInfo** or **genHistoryReport** command from the `app_server_root/bin` directory.
- The *version* is a specific version of the offering to install (8.5.0.20101025_2108 for example). This specification is optional.
 - If *version* is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
 - If *version* is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
./imcl listAvailablePackages -repositories source_repository
```

- You can also specify none, recommended or all with the `-installFixes` argument to indicate which interim fixes you want installed with the offering.
 - If the offering version is **not** specified, the `-installFixes` option defaults to all.
 - If the offering version is specified, the `-installFixes` option defaults to none.
- If you obtained the fix pack by installing the WebSphere Application Server group PTF, you can use the local fix-pack repositories to install the fix pack.

For information about the local fix-pack repositories, see file `/QIBM/WAS/WASFixpacks/ReadmeV8.html` or `/QIBM/WAS/WASFixpacks/ReadmeV8.txt`.

Installing fix packs on IBM i operating systems using the command line

Product fix packs contain bundled service to bring WebSphere Application Server up to a new product level. Interim fixes provide corrective service for specific known problems. You can use the IBM Installation Manager command-line function to update the product with the fixes that are available for your service level of WebSphere Application Server Version 8.5.

Before you begin

Contact the IBM Software Support Center for information about upgrades for WebSphere Application Server for IBM i. The most current information is available from the IBM Software Support Center and Fix Central.

IBM Installation Manager is used to apply product maintenance to WebSphere Application Server for IBM i.

Tip: As an alternative to the procedure that is described in this article, Installation Manager allows you to use the `updateAll` command in a response file or on the command line to search for and update all installed packages. Use this command only if you have full control over which fixes are contained in the targeted repositories. If you create and point to a set of custom repositories that include only the specific fixes that you want to install, you should be able to use this command confidently. If you enable searching service repositories or install fixes directly from other live web-based repositories, then you might not want to select this option so that you can select only the fixes that you want to install using the `-installFixes` option with the `install` command on the command line or the `installFixes` attribute in a response file.

About this task

Use this procedure whenever you want to apply a new fix pack to your system.

Tip: You can also install fix packs using response files with Installation Manager. For information on creating and using response files, read “Installing fix packs on IBM i operating systems using response files” on page 58 and the IBM Installation Manager Version 1.5 Information Center.

Restrictions:

- You cannot use the `iRemoteInstall` command to install a fix pack.
- You cannot use Installation Manager to upgrade an installation and add or remove the full WebSphere Application Server profile feature or the Liberty profile feature.

Procedure

1. For a list of fixes that are available for WebSphere Application Server Version 8.x and specific information about each fix, perform the following actions.
 - a. Go to Fix Central.
 - b. Select **WebSphere** as the product group.
 - c. Select **WebSphere Application Server** as the product.
 - d. Select **8.x** as the installed version.
 - e. Select your operating system as the platform, and click **Continue**.
 - f. Select **Browse for fixes**, and click **Continue**.
 - g. Click **More Information** under each fix to view information about the fix.
 - h. **Recommendation:** Make a list of the names of the fixes that you would like to install.
2. Update WebSphere Application Server Version 8.x with the fix pack using one of the following procedures.

- Access the live service repository that contains the fix pack, and use web-based updating. Use Installation Manager on your local system to update WebSphere Application Server Version 8.x with the interim fixes from the live web-based service repositories.

- For the live service repositories, use the same URLs as those used for the generally available product-offering repositories during installation. These URLs are based on the following pattern:
`http://www.ibm.com/software/repositorymanager/offering_ID`

where *offering_ID* is the offering ID that you can find in “WebSphere Application Server Version 8.5 product offerings for supported operating systems” on page 7.

- These locations do not contain web pages that you can access using a web browser. They are remote web-based repository locations that you specify for Installation Manager so that it can maintain the product.

To install a fix from a service repository, perform the following actions:

- a. If you do not already have an Installation Manager credentials file containing your IBM software user ID and password, create one that will allow you to access the repository.

Note: These are the credentials that you use to access protected IBM software websites. For information on creating a keyring file for Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Tip: When creating a keyring file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

- b. Sign on to the IBM i system with a user profile that has *ALLOBJ and *SECADM special authorities.
- c. Stop all servers and applications on the WebSphere Application Server installation that is being updated.
- d. On a CL command line, run the STRQSH command to start the Qshell command shell.
- e. Make sure that the umask is set to 022.

To verify the umask setting, issue the following command:

```
umask
```

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

```
umask 022
```

- f. Change to the `Installation_Manager_binaries/eclipse/tools` directory, where `Installation_Manager_binaries` is the installation root directory for the Installation Manager.

On IBM i systems, the root directory for the Installation Manager is `/QIBM/ProdData/InstallationManager`.

- g. Install the fix pack.

```
./imcl install offering_ID_offering_version,optional_feature_ID
  -repositories source_repository
  -installationDirectory product_installation_location
  -keyring keyring_file -password password
  -acceptLicense
```

Tips:

- The *offering_ID* is the offering ID that is listed in “WebSphere Application Server Version 8.5 product offerings for supported operating systems” on page 7.
- The *offering_version*, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to install (8.5.0.20110503_0200 for example).
 - If *offering_version* is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.

- If *offering_version* is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
./imcl listAvailablePackages -repositories source_repository
```

- You can also specify none, recommended or all with the `-installFixes` argument to indicate which interim fixes you want installed with the offering.
 - If the offering version is **not** specified, the `-installFixes` option defaults to all.
 - If the offering version is specified, the `-installFixes` option defaults to none.
- You can add a list of features that are separated by commas. If a list of features is not specified, the default features are installed.
- If you obtained the fix pack by installing the WebSphere Application Server group PTF, you can use the local fix-pack repositories to install the fix pack.

For information about the local fix-pack repositories, see file `/QIBM/WAS/WASFixpacks/ReadmeV85.html` or `/QIBM/WAS/WASFixpacks/ReadmeV85.txt`.

- h. **Optional:** List all installed packages to verify the installation:

```
./imcl listInstalledPackages -long
```

- Download a file that contains the fix pack from Fix Central, and use local updating.

You can download a compressed file that contains the fix pack from Fix Central. Each compressed fix file contains an Installation Manager repository for the fix pack and usually has a `.zip` extension. After downloading the fix file, you can use Installation Manager to update WebSphere Application Server Version 8.x with the fix pack.

- a. To download the fix pack, perform the following actions:

- 1) Go to Fix Central.
- 2) Select **WebSphere** as the product group.
- 3) Select **WebSphere Application Server** as the product.
- 4) Select **8.x** as the installed version.
- 5) Select your operating system as the platform, and click **Continue**.
- 6) Select **Browse for fixes**, and click **Continue**.
- 7) Select the fix pack that you want to download, and click **Continue**.
- 8) Select your download options, and click **Continue**.
- 9) Click **I agree** to agree to the terms and conditions.
- 10) Click **Download now** to download the fix pack.
- 11) Transfer the compressed fix file in binary format to the IBM i systems on which it will be installed.
- 12) Extract the compressed repository file to a directory on your system.

- b. To install a fix pack from a downloaded file, perform the following actions:

- 1) Sign on to the IBM i system with a user profile that has `*ALLOBJ` and `*SECADM` special authorities.
- 2) Stop all servers and applications on the WebSphere Application Server installation that is being updated.
- 3) On a CL command line, run the STRQSH command to start the Qshell command shell.
- 4) Make sure that the umask is set to 022.

To verify the umask setting, issue the following command:

```
umask
```

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

```
umask 022
```


- 5) Change to the *Installation_Manager_binaries/eclipse/tools* directory, where *Installation_Manager_binaries* is the installation root directory for the Installation Manager. On IBM i systems, the root directory for the Installation Manager is */QIBM/ProdData/InstallationManager*.

- 6) Install the fix pack.

```
./imcl install offering_ID_offering_version,optional_feature_ID
-repositories location_of_expanded_files
-installationDirectory product_installation_location
-acceptLicense
```

Tips:

- The *offering_ID* is the offering ID that is listed in “WebSphere Application Server Version 8.5 product offerings for supported operating systems” on page 7.
- The *offering_version*, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to install (8.5.0.20110503_0200 for example).
 - If *offering_version* is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
 - If *offering_version* is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
./imcl listAvailablePackages -repositories source_repository
```

- You can also specify none, recommended or all with the *-installFixes* argument to indicate which interim fixes you want installed with the offering.
 - If the offering version is **not** specified, the *-installFixes* option defaults to all.
 - If the offering version is specified, the *-installFixes* option defaults to none.
- You can add a list of features that are separated by commas. If a list of features is not specified, the default features are installed.
- If you obtained the fix pack by installing the WebSphere Application Server group PTF, you can use the local fix-pack repositories to install the fix pack.

For information about the local fix-pack repositories, see file */QIBM/WAS/WASFixpacks/ReadmeV85.html* or */QIBM/WAS/WASFixpacks/ReadmeV85.txt*.

- 7) **Optional:** List all installed packages to verify the installation:

```
./imcl listInstalledPackages -long
```

Uninstalling interim fixes from IBM i operating systems using the command line

You can use the IBM Installation Manager command-line function to remove interim fixes.

About this task

Use this procedure whenever you want to remove an interim fix from your system using the command line.

Tip: You can also uninstall interim fixes using silent response files with Installation Manager. For information on creating and using response files, read “Installing fix packs on IBM i operating systems using response files” on page 58 and the IBM Installation Manager Version 1.5 Information Center.

Procedure

1. Sign on to the IBM i system with a user profile that has *ALLOBJ and *SECADM special authorities.
2. Stop all servers and applications on the WebSphere Application Server installation.
3. On a CL command line, run the STRQSH command to start the Qshell command shell.
4. Make sure that the umask is set to 022.

To verify the umask setting, issue the following command:

```
umask
```

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

```
umask 022
```

5. Change to the *Installation_Manager_binaries/eclipse/tools* directory, where *Installation_Manager_binaries* is the installation root directory for the Installation Manager.

On IBM i systems, the root directory for the Installation Manager is /QIBM/ProdData/InstallationManager.

6. Uninstall the interim fix:

```
./imcl uninstall interim_fix_name  
-installationDirectory product_installation_location
```

7. Optional: List all installed packages to verify the uninstallation.

```
./imcl listInstalledPackages -long
```

Uninstalling fix packs from IBM i operating systems using response files

You can roll back this product to an earlier version using Installation Manager response files.

Before you begin

During the rollback process, Installation Manager must access files from the earlier version of the package. By default, these files are stored on your computer when you install a package. If you change the default setting or delete the saved files, Installation Manager requires access to the repository that was used to install the earlier version.

Restriction: You cannot use the Installation Manager to roll back an installation and add or remove the full WebSphere Application Server profile feature or the Liberty profile feature.

Procedure

1. Optional: If the repository requires a username and password, create a keyring file to access this repository.

For more information on creating a keyring file for Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Tip: When creating a keyring file, append */repository.config* at the end of the repository URL location if the **imutilsc** command is unable to find the URL that is specified.

2. Sign on to the IBM i system with a user profile that has *ALLOBJ and *SECADM special authorities.
3. Stop all servers and applications on the WebSphere Application Server installation that is being rolled back.
4. On a CL command line, run the **STRQSH** command to start the Qshell command shell.
5. Use a response file to roll back the product.

Change to the *eclipse/tools* subdirectory in the directory where you installed Installation Manager, and roll back the product. For example:


```
./imcl
input $HOME/WASFiles/temp/rollback_response_file.xml
-log $HOME/WASFiles/temp/rollback_log.xml
-keyring $HOME/WASFiles/temp/im.keyring
```

Note: The program might write important post-installation instructions to standard output.

For more information on using Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

6. Optional: List all installed packages to verify the roll back.

```
./imcl listInstalledPackages -long
```

Example

The following is an example of a response file for rolling back the product to an earlier version.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<server>
  <repository location='https://www.ibm.com/software/repositorymanager/com.ibm.websphere.ND.v85' />
</server>
<profile id='IBM WebSphere Application Server V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/ND'>
  <data key='eclipseLocation' value='/QIBM/ProdData/InstallationManager' />
</profile>
<rollback>
  <offering profile='IBM WebSphere Application Server V8.5' id='com.ibm.websphere.ND.v85' version='8.5.0.20101025_2108' />
</rollback>
</agent-input>
```

Tips:

- The profile ID (<profile . . . id='profile_ID'> and <offering . . . profile='profile_ID'>) can be found when you run the `imcl listInstallationDirectories -verbose` command from the `eclipse/tools` subdirectory in the directory where you installed Installation Manager. It is the same as the package group's name.
- The offering ID (<offering . . . id='offering_ID'>) can be found in the Install Manager Offering ID section of the report that is generated when you run the **historyInfo** or **genHistoryReport** command from the `app_server_root/bin` directory.
- The *version* is a specific version of the offering to which to roll back (8.5.0.20101025_2108 for example).

This specification is optional if you are using Installation Manager Version 1.5 or later.

- If *version* is **not** specified, the installation rolls back to the previously installed version of the offering and **all** interim fixes for that version are installed.
- If *version* is specified, the installation rolls back to the specified earlier version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore in the Package section of the report that is generated when you run the **historyInfo** or **genHistoryReport** command from the `app_server_root/bin` directory.

Uninstalling fix packs from IBM i operating systems using the command line

You can roll back this product to an earlier version using the Installation Manager command line.

Before you begin

Restriction: In order to use this procedure, you must have Installation Manager Version 1.5 or later installed on your system.

During the rollback process, Installation Manager must access files from the earlier version of the package. By default, these files are stored on your computer when you install a package. If you change the default setting or delete the saved files, Installation Manager requires access to the repository that was used to install the earlier version.

Restriction: You cannot use the Installation Manager to roll back an installation and add or remove the full WebSphere Application Server profile feature or the Liberty profile feature.

Procedure

1. Optional: If the repository requires a username and password, create a keyring file to access this repository.

For more information on creating a keyring file for Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Tip: When creating a keyring file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

2. Sign on to the IBM i system with a user profile that has *ALLOBJ and *SECADM special authorities.
3. Stop all servers and applications on the WebSphere Application Server installation that is being rolled back.
4. On a CL command line, run the **STRQSH** command to start the Qshell command shell.
5. Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.
6. Use the **imcl** command to roll back the product.

```
./imcl rollback offering_ID_offering_version
-repositories source_repository
-installationDirectory installation_directory
-preferences preference_key=value
-properties property_key=value
-keyring keyring_file -password password
-acceptLicense
```

Tips:

- The *offering_ID* is the offering ID that is listed in “WebSphere Application Server Version 8.5 product offerings for supported operating systems” on page 7.
- The *offering_version*, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to which to roll back (8.5.0.20110503_0200 for example).
 - If *offering_version* is **not** specified, the installation rolls back to the previously installed version of the offering and **all** interim fixes for that version are installed.
 - If *offering_version* is specified, the installation rolls back to the specified earlier version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore in the Package section of the report that is generated when you run the **historyInfo** or **genHistoryReport** command from the `app_server_root/bin` directory.

For more information on using the **imcl** command, read the IBM Installation Manager Version 1.5 Information Center.

7. Optional: List all installed packages to verify the roll back.

```
./imcl listInstalledPackages -long
```

Uninstalling the product from IBM i operating systems using response files

You can uninstall this product using Installation Manager response files.

About this task

Using Installation Manager, you can work with response files to uninstall the product.

Procedure

1. Stop all servers and applications on the WebSphere Application Server installations that contain the product.
2. Sign on to the IBM i system with a user profile that has *ALLOBJ and *SECADM special authorities.
3. On a CL command line, run the **STRQSH** command to start the Qshell command shell.
4. Use a response file to uninstall the product.

Complete one of the following actions:

- From a command line on each of the systems from which you want to uninstall the product, run the **uninstall** script (which uses the `uninstall.xml` response file in the same directory) to uninstall the product. For example:

```
app_server_root/uninstall/uninstall
```

- 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 `uninstall.xml` response file in the same directory to uninstall the product. For example:

```
./imc1  
input app_server_root/uninstall/uninstall.xml  
-log $HOME/WASFiles/temp/uninstall_log.xml
```

- 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 a response file that you created to uninstall the product. For example:

```
./imc1  
input $HOME/WASFiles/temp/uninstall_response_file.xml  
-log $HOME/WASFiles/temp/uninstall_log.xml
```

Go to the IBM Installation Manager Version 1.5 Information Center for more information.

5. 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 Version 1.5 Information Center for information about using the `uninstall` script to perform this procedure.

Example

The `app_server_root/uninstall/uninstall.xml` file is an example of a response file for uninstalling the product.

Uninstalling the product from IBM i operating systems using the command line

You can use Installation Manager to uninstall this product using the Installation Manager command line (`imc1`).

Procedure

1. Stop all servers and applications on the WebSphere Application Server installations that contain the product.
2. Sign on to the IBM i system with a user profile that has *ALLOBJ and *SECADM special authorities.
3. On a CL command line, run the **STRQSH** command to start the Qshell command shell.
4. Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.
5. Use the `imc1` command to uninstall the product.

For example:

```
./imc1 uninstall com.ibm.websphere.ND.v85,optional_feature_ID  
-installationDirectory installation_directory
```

You can remove a list of features that are separated by commas. If a list of features is not specified, the entire product is uninstalled.

For more information on using the **imc1** command to uninstall the product, see the IBM Installation Manager Version 1.5 Information Center.

6. 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.

For more information on uninstalling Installation Manager, see the IBM Installation Manager Version 1.5 Information Center.

Example

Here is an example of using the **imc1** command to uninstall Websphere Application Server:

```
./imc1 uninstall com.ibm.websphere.ND.v85  
-installationDirectory /QIBM/ProdData/WebSphere/AppServer/V85/ND
```

Chapter 7. 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.

Change the directory to the `eclipse/tools` subdirectory of the Installation Manager binaries location and run this command:

```
./imcl listInstalledPackages
```

This will display a list indicating which packages this Installation Manager has installed. For example:

```
com.ibm.websphere.ND.v85_8.5.0.20110203_0234
```

- If an installation was successful, the `installed.xml` file should contain a location element for the installed product.

For example, the following file:

```
installation_manager_root/properties/version/installed.xml
```

should contain something like this:

```
<location id="IBM WebSphere Application Server V8.5" kind="product" path="/QIBM/ProdData/WebSphere/AppServer/V85/ND"> ..... </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:

```
./imcl -acceptLicense  
input $HOME/WASFiles/temp/install_response_file.xml  
-log $HOME/WASFiles/temp/install_log.xml  
-keyring $HOME/WASFiles/temp/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>
```

Chapter 8. Configuring the product after installation on IBM i

Configure your IBM i server, WebSphere Application Server Network Deployment, and your HTTP server so that WebSphere Application Server runs correctly.

About this task

Creating the initial configuration for WebSphere Application Server involves configuring the IBM i server, the WebSphere Application Server product, and the HTTP server.

Procedure

1. Configure software license information, as described in “Configuring software license information.”
Set the usage limit from the Proof of Entitlement (POE) or invoice.
2. Configure SQL jobs, as described in “Configuring SQL jobs on IBM i” on page 72.
Set the maximum number of jobs that are allowed for the SQL server jobs.
3. Configure TCP/IP, as described in “Configuring TCP/IP on IBM i” on page 73.
Configure TCP/IP for WebSphere Application Server.
4. Configure an HTTP server instance, as described in “Configuring an HTTP server instance on IBM i” on page 74.
Create an HTTP server instance and configure it to use WebSphere Application Server to serve JavaServer Pages (JSP) files and servlets.

Results

The result of performing each of the procedures listed in this article is an initial configuration for WebSphere Application Server.

What to do next

Go to “Configuring software license information” to continue the installation.

Configuring software license information

Set the usage limit from the Proof of Entitlement (POE) or invoice before you start WebSphere Application Server for the first time.

Before you begin

This article assumes that you have installed the WebSphere Application Server for IBM i product and that you have installed the WebSphere Application Server group PTF.

See Chapter 4, “Task overview: Installing on IBM i,” on page 7 to install the product and the group PTF.

Before you set the usage limit from a POE or invoice, verify that your user profile has the *ALLOBJ special authority.

About this task

Use the Work with License Information menu to set the usage limit from a POE or invoice.

Procedure

1. Access the Work with License Information menu.

On a Control Language (CL) command line, enter the Work with License Information (**WRKLICINF**) command.

2. On the Work with License Information menu, press **F11 (Display Usage Information)**.
3. Move the cursor to the line that contains the product 5733W80 and the feature code for the product that you installed.
The feature code is 5103 for WebSphere Application Server Network Deployment Version 8.5.
4. Select option **2 (Change)**, then press **Enter**.
The Change License Information display is shown.
5. Specify the usage limit shown on the POE or invoice for the Usage limit prompt (**USGLMT**).
Do not specify a number that exceeds the purchased limit because doing so violates the IBM purchase agreement.
6. On the Change License Information display, press **F9 (All parameters)**.
7. Specify ***USGLMT** for the Threshold (**THRESHOLD**) prompt, then press **Enter**.
Do not leave the threshold set to zero.

Results

The usage limit changes to the value that you specified.

If the following message is displayed, type **G**.

```
CPA9E1B: Usage limit increase must be authorized.  
Press help before replying (C G)
```

After you respond to the CPA9E1B message, you must respond to the same message on the QSYSOPR message queue. Run the **DSPMSG QSYSOPR** command to see the message in the QSYSOPR message queue. When the message is displayed, type **G**.

What to do next

Go to “Configuring SQL jobs on IBM i” to continue the installation.

Configuring SQL jobs on IBM i

Choose either of two methods to change the maximum number of SQL server jobs allowed. Each Java Database Connector (JDBC) connection object requires one SQL server job.

Before you begin

If you are using the JDBC driver in the IBM Developer Kit for Java to access the IBM i database from your applications, you might need to change the maximum number of jobs allowed.

About this task

This procedure describes two methods for setting the number of SQL server jobs allowed to an adequate amount to handle the workload.

Procedure

- Set the maximum number of jobs to ***NOMAX**.
Generally, it is easier to account for the number of jobs you need by setting the maximum number of jobs to ***NOMAX**. Use the Change Prestart Job Entry (**CHGPJE**) command to change the prestart job entry for the SQL server jobs.
CHGPJE SBSDB(QSYSWRK) PGM(QSQSRVR) MAXJOBS(*NOMAX)
- Set **MAXJOBS** to a large enough integer value for your applications to handle SQL server jobs.

If *NOMAX is not an appropriate setting for your IBM i environment, specify a large enough integer value for the MAXJOBS parameter so that your applications have enough SQL server jobs to handle the maximum number of JDBC connections required at any given time by your applications.

Results

After the maximum number of jobs is successfully changed, the following message is displayed:

```
Program QSQSRVR found in library QSYS.  
Active subsystem description QSYSWRK in QSYS changed.
```

What to do next

Go to “Configuring TCP/IP on IBM i” to continue the installation.

Configuring TCP/IP on IBM i

Configure TCP/IP to run WebSphere Application Server on IBM i.

Before you begin

Before you configure TCP/IP settings, ensure that your user profile has *IOSYSCFG special authority.

About this task

Use the Configure TCP/IP menu to access options that enable you to configure TCP/IP.

Procedure

1. On a Control Language (CL) command line, enter the Configure TCP/IP (**CFGTCP**) command.
2. Verify that your TCP/IP address and LOOPBACK interface are active.
 - a. On the Configure TCP/IP menu, select option **1 (Work with TCP/IP interfaces)**.
 - b. Press **F11** to display the interface status.
 - c. Verify that the TCP/IP address is active. If it is not active, specify option **9 (Start)**.
 - d. Verify that the LOOPBACK interface at IP address 127.0.0.1 is active.
If 127.0.0.1 is not active, specify option **9 (Start)** next to the entry with IP address 127.0.0.1, then press **Enter**.
 - e. Press **F3** to return to the Configure TCP/IP menu.
3. Verify your TCP/IP host name.
 - a. On the Configure TCP/IP menu, select option **12 (Change TCP/IP domain information)**.
 - b. Verify that the TCP/IP host name is correct.
If the host name is not correct, type the correct host name in the Host name field, then press **Enter**. If the host name is correct, press **F3** to return to the Configure TCP/IP menu.
The host name cannot be *NONE.
 - c. Press **F3** to return to the command line.
4. Start TCP/IP.
If TCP/IP is not started or if you do not know if TCP/IP is started, enter the Start TCP/IP (**STRTCP**) command on the CL command line.
5. Verify that the server IP address is associated with the host name.
Issue the following command on the CL command line:

```
ping host_name
```

The following sample output is from a successful **ping** command:

```
Verifying connection to host system MYSYSTEM.MYCOMPANY.COM at address
1.2.3.4.
PING reply 1 from 1.2.3.4 took 0 ms. 256 bytes. TTL 64.
PING reply 2 from 1.2.3.4 took 0 ms. 256 bytes. TTL 64.
PING reply 3 from 1.2.3.4 took 0 ms. 256 bytes. TTL 64.
PING reply 4 from 1.2.3.4 took 0 ms. 256 bytes. TTL 64.
PING reply 5 from 1.2.3.4 took 0 ms. 256 bytes. TTL 64.
Round-trip (in milliseconds) min/avg/max = 0/0/0
Connection verification statistics: 5 of 5 successful (100 %).
```

If the ping fails, follow these steps:

- a. Enter the Configure TCP/IP (**CFGTCP**) command on the CL command line.
- b. On the Configure TCP/IP menu, select Option **10 (Work with TCP/IP host table entries)**.
- c. Configure the IBM i system short name to the active IP address that was listed in step 2:
 - 1) Select Option **2 (Change)** and type your IP address in the Internet address field, then press **Enter**.
 - 2) In the Change TCP/IP Host Table Entry (CHGTCPHTE) menu, edit the **Hostnames: Name** field to match the short name of your IBM i server, then press **Enter**.

Important: The *ADMIN instance of the HTTP server does not start without a host name.

6. Verify your system configuration.

The IPTest Java utility is shipped with the WebSphere Application Server product and can be used to debug TCP/IP configuration problems. To run this utility, run the **IPTest** command from the QShell command line.

The command file is in the *app_server_root/bin* directory:

```
app_server_root/bin/IPTest
```

Results

If TCP/IP has been configured successfully, the **IPTest** command output resembles the following example:

```
Local Address: 12.34.56.78
Local Name: MYSYSTEM.MYCOMPANY.COM
All addresses for MYSYSTEM.MYCOMPANY.COM:
12.34.56.78
```

The *Local Address* is the IP address for your IBM i server. This value must not be blank and must match the IP address verified in step 2. The *Local Name* is the domain-qualified host name for your IBM i server. If this value is blank, see the instructions in step 2. Press **F3** to exit.

If a host name has not been configured for your IBM i server, you receive an UnknownHostException message.

What to do next

Go to “Configuring an HTTP server instance on IBM i” to continue the installation.

Configuring an HTTP server instance on IBM i

Configure your IBM HTTP Server or Lotus Notes® Domino HTTP Server to use either web server with WebSphere Application Server for IBM i.

Before you begin

Decide which HTTP Server you want to use to serve requests to WebSphere Application Server.

The following web servers are supported on IBM i:

- IBM HTTP Server (powered by Apache) (5761-DG1 or 5770-DG1)
- Lotus Domino 8 for System i 8.0 (5733-LD8), versions 8.0.1 and 8.0.2

- IBM Domino 8.5 for i (5733-L85)

The IBM HTTP Server (original) is not supported for WebSphere Application Server. However, you can use the IBM i IBM HTTP Server (Powered by Apache) with your application server. Or, you can configure a remote HTTP server residing on a supported platform to route requests to WebSphere Application Server running on the IBM i server.

About this task

An HTTP server instance is not required to install or use WebSphere Application Server. However, it is recommended to support requests for servlets and JavaServer Pages (JSP) resources managed by WebSphere Application Server.

Procedure

- Configure IBM HTTP Server for IBM i.
Go to “Configuring IBM HTTP Server for IBM i” if you plan to use IBM HTTP Server.
- Configure Lotus Domino HTTP Server.
Go to “Configuring Lotus Domino HTTP Server on IBM i” on page 78 if you plan to use Lotus Domino HTTP Server.

Configuring IBM HTTP Server for IBM i

You must configure IBM HTTP Server for IBM i before using the web server with WebSphere Application Server for IBM i.

Before you begin

This article assumes that you have decided to use the IBM HTTP Server for IBM i to serve requests to WebSphere Application Server. “Configuring an HTTP server instance on IBM i” on page 74 describes the HTTP servers available to WebSphere Application Server users.

About this task

An HTTP server instance is not required to install WebSphere Application Server. However, it is recommended to support requests for servlets and JavaServer Pages (JSP) resources managed by WebSphere Application Server.

Before you can use the IBM HTTP Server for IBM i, you must configure an instance of IBM HTTP Server to communicate with WebSphere Application Server.

Procedure

1. Start the *ADMIN server instance of IBM HTTP Server to use the IBM HTTP Server for IBM i configuration and administration forms.
See “Starting the *ADMIN instance of IBM HTTP Server on IBM i” on page 76 for more information.
2. Create an HTTP server instance or select an existing instance, and configure it to work with WebSphere Application Server.
 - Create an HTTP server instance, and configure it to work with WebSphere Application Server.
Go to “Creating and configuring HTTP server instances on IBM i” on page 76 for more information.
 - Select an existing HTTP server instance, and configure it to work with WebSphere Application Server.
Go to the second step in “Creating and configuring HTTP server instances on IBM i” on page 76 for more information.

Starting the *ADMIN instance of IBM HTTP Server on IBM i

This article describes how to start the *Admin instance of IBM HTTP Server.

Before you begin

This article assumes that you have decided to use the IBM HTTP Server for IBM i to serve requests to WebSphere Application Server.

About this task

Start the *ADMIN server instance of IBM HTTP Server to create, change, or display an IBM HTTP Server instance configuration by using the IBM HTTP Server for IBM i Configuration and Administration forms.

You can start the *ADMIN server instance from a Control Language (CL) command line or from Navigator for i.

Procedure

- Start the *ADMIN server instance from a CL command line.

Type the following command and press **Enter** to start the *ADMIN instance from the CL command line:

```
STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
```

- Start the *ADMIN server instance from the Navigator for i.

The IBM i Navigator is the graphical interface to the IBM i server. The Navigator for IBM i is part of the IBM i Access for Windows product.

For more information about IBM i Access for Windows and Navigator for i, see the IBM i Access Family website.

To start the *ADMIN instance from Navigator for i:

1. Start Navigator for i.
2. Double-click your IBM i server.
3. Click **Network > Servers > TCP/IP**.
4. Right-click **HTTP Administration** in the right frame.
5. Click **Start**.

Do not select the **Start Instance** action from the menu. If the server is already started, the **Start** action is disabled on the menu.

What to do next

Go to “Creating and configuring HTTP server instances on IBM i” to continue the installation.

Creating and configuring HTTP server instances on IBM i

This article describes how to create and configure an IBM HTTP Server instance.

Before you begin

This article assumes that you have started the *Admin instance of IBM HTTP Server. See “Starting the *ADMIN instance of IBM HTTP Server on IBM i” for more information.

About this task

Use this procedure to create and configure an instance of IBM HTTP Server.

If you have an existing instance that you want to use with WebSphere Application Server, skip directly to the configuration step.

Procedure

1. Create a new instance of IBM HTTP Server.

To create a new instance of the IBM HTTP Server (powered by Apache) with a basic configuration, use the IBM HTTP Server for IBM i configuration and administration forms.

Perform the following steps:

a. Using a web browser, go to the IBM HTTP Server for IBM i configuration and administration forms.

1) Open this URL in your browser:

`http://your.server.name:2001/`

The *your.server.name* variable is the name of your IBM i server.

2) Enter a valid user ID and password for your IBM i server.

3) Select **IBM Web Administration for IBM i** at the IBM i Tasks page.

b. The IBM Web Administration for IBM i page is displayed.

1) To create a new HTTP server, click the **Setup** tab.

2) Expand **Common Tasks and Wizards**.

3) Click **Create New HTTP Server**.

c. Select **HTTP server (powered by Apache)**, then click **Next**.

d. In the right frame, type a name for the HTTP server instance and an optional description, then click **Next**.

The name appears in the HTTPSVR subsystem when the job is running.

Write down the HTTP server instance name for use in later steps.

e. Type the server root, then click **Next**.

You can use default values or you can specify another server root or document root directory.

f. Set the document root in the next panel, then click **Next**.

g. Select the IP address and port.

1) Select **All addresses** in the **IP address** field.

2) Accept the default port, 80, for the port number that the HTTP Server instance uses to process requests or type a unique port number, then click **Next**.

If you specify a port other than the default port, you must configure your virtual host Domain Name System (DNS) aliases in the administrative console to reflect your port number.

Write down the internal HTTP port number for use in later steps.

h. Select a logging option.

It is recommended that you select **Yes**. Logs are stored in the `/server_root/logs` directory, where *server_root* is the server root that you set earlier.

i. Specify how long you want to keep the error and access log files, then click **Next**.

j. Review your settings. To create the HTTP server instance, click **Finish**. To make changes, click **Back**.

k. After you click **Finish**, the configuration is created. The Manage Apache Server page is displayed.

2. Configure the HTTP server instance

After you create the HTTP server instance, configure the instance so that it works with WebSphere Application Server.

a. Click the **Manage** tab. In the Server list, select the HTTP server instance that you want to manage.

b. With your HTTP server selected, expand **Server Properties** in the left frame. Click **WebSphere Application Server**. Select the version of WebSphere Application Server to configure, and select the default WebSphere Application Server profile.

c. Click **OK** to write the changes to the configuration file and return to the main configuration page.

What to do next

You have completed step 3 of 5.

Go to Chapter 9, “Starting WebSphere Application Server on IBM i,” on page 81 to continue the installation.

Configuring Lotus Domino HTTP Server on IBM i

You must update the Lotus Domino Web server configuration before you can use the web server with WebSphere Application Server.

Before you begin

See the WebSphere Application Server detailed system requirements page for information on the support levels of Lotus Domino Web Server.

Refer to the Administration Help for your version of Domino for information about installing and setting up Domino servers on IBM i.

The help database is shipped with Lotus Domino and is also available in the Notes.net Documentation Library.

About this task

Configure each instance of a Domino server on your IBM i server.

Procedure

1. Define your web server in the application server configuration.

a. Start Qshell.

On the CL command line, enter STRQSH.

b. Move to the directory where the configuration resides.

At the Qshell prompt, run the command:

```
cd app_server_root/bin
```

c. Specify a name and a port for your Domino Server.

At the Qshell prompt, run the command:

```
configureOs400WebServerDefinition -webservice.name yourDominoServer \  
                                -webservice.type DOMINO \  
                                -webservice.port
```

```
port
```

The *yourDominoServer* variable is the name of your Domino server. The *port* variable is the HTTP port for your Domino Server.

To use a non-default WebSphere Application Server profile, specify the `-profileName myProfile` parameter when you run the `configureOs400WebserverDefinition` script.

d. Generate the `plugin-cfg.xml` file. From the Qshell prompt, run this command:

```
GenPluginCfg -webservice.name yourDominoServer
```

If you specified a profile name in the previous step, specify the `-profileName myProfile` parameter when you run the `GenPluginCfg` script.

e. Write down the location of the `plugin-cfg.xml` file. You need this information in the next step.

2. Update the Domino server `notes.ini` file.

a. Enter the Work with Domino Servers (WRKDOMSVR) command on the CL command line.

b. For the appropriate Domino server instance, specify option 13 (**Edit NOTES.INI**) to edit the server `notes.ini` file.

c. Add this line to the end of the `notes.ini` file:

WebSphereInit=plugin-file

The *plugin-file* variable is the fully-qualified path of the `plugin-cfg.xml` file that you generated in the previous step.

- d. Press **F3** twice to save and exit the `notes.ini` file
3. Start the Domino server.
 - a. Verify that your user profile has *JOBCTL special authority.
 - b. On the CL command line, enter the `strdomsvr` command.
 - c. Press **F4** to have the system prompt you for the server name.
 - d. Type the server name in the field provided.

If you are not sure of the name, press **F4** to display a list of Domino servers on your IBM i server.

- e. Press **Enter**.

While the system is starting the Domino server, you see a message indicating that the server is starting. If the message appears for more than 1 or 2 minutes, the server might be waiting for you to enter a password. To determine if the server is waiting for a password, use the `WRKDOMCSL` command to start a server console session for the server. You can enter the password in this console session.

4. Enable the WebSphere Application Server DSAPI filter.
 - a. From a Lotus Notes client connected to the appropriate Domino server, edit the Domino document. The document is in the Domino server Domino Directory. The name of the file is `names.nsf`. For example, open your browser to `http://your.server.name:port/names.nsf`, where the *your.server.name* variable is the name of your IBM i server and the *port* variable is your web server port.
Enter your Domino administrator user name and password. For additional techniques used to edit the Domino document, refer to the Domino documentation.
 - b. Within the server document, select the **Internet Protocols** tab and then the **HTTP** tab.
 - c. For **DSAPI filter file names**, type:

```
/QSYS.LIB/product_library.LIB/LIBDOMINO.SRVPGM
```

Verify that you do not have a space before or after this command or the filter fails.

- d. Save and exit the Domino server document.
To use the Lotus Domino Web server with WebSphere Application Server, you do not need to change the **Java servlet support** field in the Domino server document.
5. Stop and restart the Domino server HTTP task.
 - a. Enter the Work with Domino Servers (`WRKDOMSVR`) command on the CL command line.
 - b. For your Domino server instance, specify option 8 (**Work console**) to select the Domino server console.
 - c. From the Domino server console, enter the following command to stop the Domino server HTTP task.

```
tell http quit
```
 - d. From the Domino server console, enter the following command to start the Domino server HTTP task.

```
load http
```

What to do next

You have completed step 3 of 5.

Go to Chapter 9, “Starting WebSphere Application Server on IBM i,” on page 81 to continue the installation.

Chapter 9. Starting WebSphere Application Server on IBM i

After installing, start the WebSphere Application Server environment to begin using it.

Before you begin

This article assumes that you have configured your WebSphere Application Server for IBM i installation. See Chapter 8, “Configuring the product after installation on IBM i,” on page 71 if you have not yet configured the product.

About this task

Use this procedure to start the WebSphere Application Server environment.

Procedure

1. Start the default application server profile.

Start the default standalone application server, as described in “Starting default standalone application server profiles on IBM i.”

Choose this task if you intend to run a standalone, unfederated application server.

Start and configure the default deployment manager profile, as described in “Starting and configuring default deployment manager profiles on IBM i” on page 84

Choose this task if you installed WebSphere Application Server Network Deployment and plan to run a deployment manager profile with one or more federated application server nodes.

2. Configure the virtual host, as described in “Configuring virtual hosts on IBM i” on page 88.

If your external HTTP server configuration uses ports other than the default ports, you must update the Host Aliases table for the virtual host to reflect the correct HTTP port number.

3. Start the HTTP server instance, as described in “Starting HTTP server instances on IBM i” on page 89.

Start the HTTP server so that your application server profile can receive and respond to client requests.

4. Start the default application server node, as described in “Starting default application server nodes on IBM i” on page 90.

If you installed WebSphere Application Server Network Deployment and are running a deployment manager profile with one or more federated application server nodes, perform this step to start the default application server node.

What to do next

Go to “Starting default standalone application server profiles on IBM i” to continue the installation.

Starting default standalone application server profiles on IBM i

WebSphere Application Server provides a default application server profile that contains several example applications. The default standalone profile is ready to run after you install, configure, and start WebSphere Application Server. Start the default standalone application server profile to use it.

Before you begin

This article assumes that you have configured your WebSphere Application Server for IBM i installation. See Chapter 8, “Configuring the product after installation on IBM i,” on page 71 if you have not yet configured the product.

About this task

Use this procedure to start the default application server profile.

Procedure

1. Start the default application server profile.
 - a. Run the Start Qshell (**STRQSH**) command from a Control Language (CL) command line.
 - b. At the Qshell prompt, run the following commands:

```
cd app_server_root/bin
startServer server1
```

The **startServer** command starts the QWAS85 subsystem if it is not already started.

2. Start the administrative console, as described in “Starting the administrative console on IBM i” on page 83.

Open the administrative console in a web browser.

What to do next

Go to “Verifying that the application server is running on IBM i” to continue the installation.

Verifying that the application server is running on IBM i

Before you start the administrative console, verify that the application server is running.

Before you begin

This article assumes that you are attempting to start your application server profile. See Chapter 9, “Starting WebSphere Application Server on IBM i,” on page 81 if you have not yet attempted to start the application server.

About this task

When WebSphere Application Server is ready for use, a message is written to the job log of the application server job indicating that WebSphere Application Server is ready for use.

Issue all of the commands in this procedure from the Control Language (CL) command line.

Procedure

1. Run the Work with Active Jobs (**WRKACTJOB**) command from the CL command line, specifying the proper subsystem on the subsystem (SBS) parameter:

```
WRKACTJOB SBS(QWAS85)
```

2. Find your application server job. The application server job for the default application server profile is named SERVER1.
3. Specify option **5 (Work with Job)** on the option line next to the job, then press **Enter**.
4. On the command line of the Work with Job display, specify option **10 (Display job log, if active)**, then press **Enter**.
5. Press **F10** to display all messages.

Look for this message:

```
WebSphere application server application_server ready.
```

The *application_server* variable is the name of your application server. The default application server is named SERVER1.

If the message is not displayed, press **F5** to refresh the job log messages until the message is displayed.

When the message is displayed, WebSphere Application Server has successfully started. It may take up to 20 minutes for the message to be displayed, depending on your IBM i server.

6. To display the port number on which the application server is listening for the administrative console, position the cursor on the last line of the message and press **F1**.

The following message is displayed:

```
WebSphere application server application_server
in job app_server_job is ready to handle administrative
requests on port port_number.
```

The *application_server* variable is the name of your application server, the *app_server_job* variable is the IBM i job name for your application server, and the *port_number* variable is the number of the port used by the administrative console.

If the administrative console application is not installed in the application server profile or if the administrative console port cannot be displayed, the *port_number* is *N.

Press **F3** twice to exit.

What to do next

Go to “Starting the administrative console on IBM i” to continue the installation.

Starting the administrative console on IBM i

The administrative console is a Web-based application that runs on any browser supported by WebSphere Application Server. Start the administrative console to begin administering the system.

Before you begin

This article assumes that you have a running application server profile. See Chapter 9, “Starting WebSphere Application Server on IBM i,” on page 81 if you have not yet attempted to start the application server.

The browser-based administrative console for WebSphere Application Server requires that cookies be enabled in the browser. This article also describes how to enable cookies.

About this task

Use this procedure to start the administrative console on a workstation.

Procedure

1. Open the following web page in your browser:

```
http://your.server.name:port/ibm/console
```

The *your.server.name* variable is the host name of the IBM i server on which your application server is running. The *port* variable is the administrative console port as noted in the ready message in the joblog of your application server.

The administrative console port of the default application server profile is 9060. For more information about the ready message, see “Verifying that the application server is running on IBM i” on page 82.

2. When prompted, enter a user ID.

The administrative console is displayed in the browser window.

The user ID does not need to be an IBM i user profile. This user ID is used only to track which users make changes to the application server configuration.

3. Enable cookies for your web browser.

See your browser documentation for help enabling cookies for other supported web browsers.

Some browsers provide advanced settings so that you can configure cookie settings separately for different domains, such as <http://mycompany.com>. For help with advanced features, see the documentation for your browser.

What to do next

Go to “Configuring virtual hosts on IBM i” on page 88 to continue the installation.

Starting and configuring default deployment manager profiles on IBM i

WebSphere Application Server Network Deployment provides a configurable default deployment manager profile that you create using the `manageprofiles` command after installation.

About this task

After you install WebSphere Application Server Network Deployment, you can start, configure and run the default deployment manager profile.

Procedure

1. Start the default deployment manager.
 - a. On the Control Language (CL) command line, run the Start Qshell (**STRQSH**) command.
 - b. At the Qshell prompt, run the following commands:

```
cd app_server_root/bin
startServer dmgr
```

The `startServer` command starts the QWAS85 subsystem if it is not already started.

2. Verify that the deployment manager is running
Use the Work with Active Jobs (**WRKACTJOB**) command to determine when the deployment manager is ready to accept administrative requests through the administrative console.
3. Add a node to the network deployment profile, as described in “Adding nodes to deployment manager profiles on IBM i” on page 86.
Run the `addNode` command from the Qshell command shell to federate the default application server profile into the Network Deployment cell.
4. Verify that the node agent is running, as described in “Verifying that the node agent is running on IBM i” on page 86.
Use the Work with Active Jobs (**WRKACTJOB**) command to determine when the node agent is ready to accept administrative requests through the administrative console.
5. Start the administrative console for the deployment manager.
Open the administrative console in a web browser, as described in “Starting the administrative console for deployment managers on IBM i” on page 87.
6. Verify that the node exists, as described in “Verifying that nodes exist on IBM i” on page 88.
Use the administrative console to verify that the WebSphere Application Server node was successfully added to the deployment manager domain.

Results

The `addNode` command creates a new server, the node agent, under the application server profile being added to the Network Deployment domain. The node agent server is started as a side effect of adding the node to the domain.

What to do next

Repeat the previous steps for each node (or application server profile) that you want to manage using your deployment manager profile.

Verifying that the deployment manager is running on IBM i

This article describes how to verify that the deployment manager is running before you start the administrative console.

Before you begin

You must install WebSphere Application Server Network Deployment before you can create, start, configure, and run the default deployment manager profile.

See “Starting and configuring default deployment manager profiles on IBM i” on page 84 for more information.

About this task

Before you start the administrative console or add a node to the Network Deployment domain, verify that the Network Deployment environment is running.

When the Network Deployment environment is ready for use, a message is written to the job log of the application server job for the Deployment Manager indicating that the Network Deployment environment is ready. Use this procedure to determine if the Network Deployment environment is running.

Procedure

1. Run the Work with Active Jobs (**WRKACTJOB**) command from the Control Language (CL) command line, specifying the proper subsystem on the subsystem (SBS) parameter:

```
WRKACTJOB SBS(QWAS85)
```

2. Find the server job for your deployment manager profile. For the default deployment manager profile, the server job is named DMGR.
3. Specify option **5 (Work with Job)** on the option line next to the job, then press **Enter**.
4. On the command line of the Work with Job display, specify option **10 (Display job log, if active)**, then press **Enter**.
5. Press **F10** to display all messages.

Look for this message:

```
WebSphere application server application_server ready.
```

The *application_server* variable is the name of your application server. For the default deployment manager profile, the application server for the deployment manager is named dmgr.

If the message is not displayed, press **F5** to refresh the job log messages until the message displays.

When the message is displayed, the Network Deployment environment is successfully running. The message can take up to 20 minutes to display, depending on your IBM i server.

6. To display the port number on which the deployment manager is listening for the administrative console, position the cursor on the last line of the message and press **F1**.

This message is displayed:

```
WebSphere application server application_server  
in job app_server_job is ready to handle  
administrative requests on port port_number.
```

The *application_server* variable is the name of the deployment manager application server. The *app_server_job* variable is the IBM i job name for the deployment manager application server. The *port_number* variable is the number of the port used by the administrative console.

7. Press **F3** twice to exit.

What to do next

Go to “Adding nodes to deployment manager profiles on IBM i” on page 86 to continue the installation.

Adding nodes to deployment manager profiles on IBM i

You can add WebSphere Application Server nodes to the cell that your deployment manager profile is managing.

Before you begin

This article assumes that you are working on the IBM i server that hosts your WebSphere Application Server node.

About this task

Use the **addNode** command to add WebSphere Application Server nodes to the cell which your deployment manager profile is managing.

Procedure

1. Run the Start Qshell (**STRQSH**) command from a Control Language (CL) command line.
2. At the Qshell prompt, issue the **addNode** command.

Specify the host name and Simple Object Access Protocol (SOAP) port for the deployment manager.
For example:

```
app_server_root/bin/addNode  
host_name  
soap_port  
-includeapps
```

The *host_name* variable is the host name of the server on which you installed the Network Deployment product. The *soap_port* variable is the SOAP port for the deployment manager profile. For the deployment manager profile, the default soap port is 8879.

By default, any applications installed on the application server profile are removed from the application server profile when it is added to a cell. If this is the only node that you are adding, or if you know that there are no conflicts with applications installed on other nodes, you can specify the `-includeapps` parameter when invoking the **addNode** command. When this parameter is specified, the **addNode** command does not remove any installed applications.

The *host_name* and the *soap_port* variables are positional and must be the first two parameters. Additional parameters such as `-includeapps` must be specified after the *soap_port* value. See the **addNode** documentation for more information.

Results

The **addNode** command creates a new server, the node agent, under the application server profile being added to the Network Deployment domain. The nodeagent server is started as a side effect of adding the node to the domain.

What to do next

Repeat the previous steps for each node (or application server profile) that you want to manage using your deployment manager profile.

Verify that the node agent is running after adding the node, as described in “Verifying that the node agent is running on IBM i.”

Verifying that the node agent is running on IBM i

Verify that the node agent is running before you start the administrative console.

About this task

Use the **addNode** command to add WebSphere Application Server nodes to the cell which your deployment manager profile is managing.

Procedure

1. Run the Work with Active Jobs (**WRKACTJOB**) command on the CL command line, specifying the proper subsystem on the subsystem (SBS) parameter:

```
WRKACTJOB SBS(QWAS85)
```

2. Find the server job for your deployment manager profile. The node agent job name is the same as the node name for the application server profile. For the default application server profile, the node name is the same as the host name of the IBM i sever.
3. Specify option **5 (Work with Job)** on the option line next to the job, then press **Enter**.
4. On the command line of the Work with Job display, specify option **10 (Display job log, if active)**, then press **Enter**. Press **F10** to display all messages.
5. Look for this message:

```
WebSphere application server nodeagent ready.
```

If the message is not displayed, press **F5** to refresh the job log messages until the message displays.

Results

When the message is displayed, the node agent has successfully started. It can take up to 20 minutes for the message to be displayed, depending on your IBM i server.

What to do next

Start the administrative console for the deployment manager, as described in “Starting the administrative console for deployment managers on IBM i.”

Starting the administrative console for deployment managers on IBM i

The administrative console is a Web-based application that runs on any browser supported by WebSphere Application Server. This article describes how to start the administrative console for the deployment manager.

Before you begin

This article assumes that you have a running deployment manager profile. See “Verifying that the deployment manager is running on IBM i” on page 85 if you have not yet attempted to start the deployment manager.

The browser-based administrative console for WebSphere Application Server requires that cookies be enabled in the browser. This article also describes how to enable cookies.

About this task

Use this procedure to start the administrative console on a workstation.

Procedure

1. Open the following web page in your browser:

```
http://your.server.name:port/ibm/console
```

The *your.server.name* variable is the host name of the IBM i server on which your deployment manager is running. The *port* variable is the administrative console port as noted in the ready message in the joblog of your application server.

The administrative console port of the deployment manager profile is 9060. For more information about the ready message, see “Verifying that the deployment manager is running on IBM i” on page 85.

2. When prompted, enter a user ID.

The administrative console is displayed in the browser window.

The user ID does not need to be an IBM i user profile. This user ID is used only to track which users make changes to the deployment manager configuration.

3. Enable cookies for your web browser.

See your browser documentation for help enabling cookies for other supported web browsers.

Some browsers provide advanced settings so that you can configure cookie settings separately for different domains, such as `http://mycompany.com`. For help with advanced features, see the documentation for your browser.

What to do next

Go to “Verifying that nodes exist on IBM i” to continue the installation.

Verifying that nodes exist on IBM i

This article describes how to verify that the WebSphere Application Server node was successfully added to the deployment manager domain.

Before you begin

This article assumes that you have already started the administrative console for the deployment manager. If you have not yet started the administrative console, see “Starting the administrative console for deployment managers on IBM i” on page 87.

About this task

Use this procedure to verify that the WebSphere Application Server node was successfully added to the Deployment Manager domain.

Procedure

1. Click **System administration > Nodes** in the administrative console of the deployment manager.
2. Verify that the node is listed and that the status is Started. If the node does not exist, go to “Adding nodes to deployment manager profiles on IBM i” on page 86.

Results

Messages in the console panel of the deployment manager show the status of the application server. The **Servers > Application Servers** panel also shows the status of each defined application server.

What to do next

Go to “Configuring virtual hosts on IBM i” to continue the installation.

Configuring virtual hosts on IBM i

A virtual host is a configuration entity that allows WebSphere Application Server to treat multiple host machines or port numbers as a single logical host (virtual host) for configuration purposes. Each virtual host can be associated with multiple aliases. Each alias is a particular host name and port number. Configure the virtual host to make resources available for client requests.

Before you begin

This article assumes that you have started the administrative console. See “Starting the administrative console on IBM i” on page 83 if you have not yet attempted to start the application server.

You can use virtual hosts to combine multiple host machines into a single virtual host or to assign host machines to different virtual hosts. Virtual hosts separate and control WebSphere Application Server resources to make the resources available for client requests.

If your external HTTP server configuration uses ports other than the default ports, you must update the Host Aliases table for the virtual host to reflect the correct HTTP port number.

If your external HTTP server configuration uses the default port (80), skip these steps and go to “Starting HTTP server instances on IBM i” instead.

About this task

Use this procedure to update the Host Aliases table for the default_host virtual host from the administrative console.

Procedure

1. Click **Environment > Virtual Hosts** in the left frame of the administrative console.
2. Click **default_host** in the right frame.
3. Click **Host Aliases**. The settings for default_host are displayed.
4. Click the **asterisk** in the row that has a Port of 80 in the Host Name list.
Host names are set to * when you install WebSphere Application Server.
5. Specify the correct port number for your HTTP server in the Port field.
6. Click **OK**, then click **Save** to save your configuration.
7. After you specify a new port number, you must regenerate the plug-in configuration:
 - a. Click **Servers > Web servers**.
 - b. Select your web server.
 - c. Click **Generate Plug-in**.
 - d. Click **OK**.
8. After configuring the virtual host, start your HTTP server instance.

What to do next

For a standalone application server, restart the application server after you update the virtual host configuration.

Go to “Starting HTTP server instances on IBM i” to continue the installation.

Starting HTTP server instances on IBM i

IBM HTTP Server for IBM i runs in the QHTTSPVR subsystem, and each HTTP Server instance starts multiple jobs. The WebSphere Application Server code that plugs into IBM HTTP Server for IBM i runs in the HTTP Server job that communicates with one or more application servers. Start the HTTP Server instance to enable communication with the application server.

Before you begin

This article assumes that you have already created an HTTP server instance. If you have not yet created an HTTP server instance, see “Configuring IBM HTTP Server for IBM i” on page 75.

About this task

Use this procedure to start the HTTP Server instance for the HTTP Server you are using.

Procedure

- Start IBM HTTP Server.

Enter the following command on the CL command line:

```
STRTCPSVR SERVER(*HTTP) HTTPSVR(myinst)
```

The *myinst* variable is the name of your HTTP server instance. This is the HTTP instance that you configured in “Configuring IBM HTTP Server for IBM i” on page 75.

If you change your HTTP server instance configuration, stop and then start your HTTP server instance.

To stop your HTTP server instance, enter this command from the CL command line:

```
ENDTCPSVR SERVER(*HTTP) HTTPSVR(myinst)
```

The *myinst* variable is the name of your HTTP server instance. This is the HTTP instance that you configured in “Configuring IBM HTTP Server for IBM i” on page 75.

You can also stop and start your HTTP server instance from the IBM HTTP Server for IBM i Configuration and Administration forms in the browser-based interface. For instructions on using the browser-based interface, see “Configuring IBM HTTP Server for IBM i” on page 75.

The Configuration and Administration forms provide the option of restarting, as opposed to starting and stopping, your HTTP server instance. When restarting, the HTTP server recognizes all configuration changes except changes to the Basic and Security configuration forms.

- Start Lotus Domino HTTP Server

If you have not yet configured the Lotus Domino Web server, see “Configuring Lotus Domino HTTP Server on IBM i” on page 78.

Perform the following procedure to start the Domino server web task:

1. Enter the Work with Domino Servers (**WRKDOMSVR**) command on a Control Language (CL) command line.
2. For your Domino server instance, specify option **8** to select the Domino server console.
3. From the Domino server's console, enter this command to restart the Domino server HTTP task:

```
tell http restart
```

Starting default application server nodes on IBM i

Start the default application server node from the deployment manager administrative console.

Before you begin

This article assumes that you have already started the HTTP server instance. If you have not yet started the HTTP server instance, see “Starting HTTP server instances on IBM i” on page 89.

About this task

Use this procedure to start the application server for a node from the administrative console of the deployment manager.

Procedure

1. Click **Servers > Application Servers** in the administrative console of the deployment manager.
2. Select the check box next to the application server you intend to start.
3. Click **Start**.

Results

Messages in the console panel of the deployment manager show the status of the application server. The **Servers > Application Servers** panel also shows the status of each defined application server.

Chapter 10. Installing and uninstalling the DMZ Secure Proxy Server on IBM i systems

IBM Installation Manager is a common installer for many IBM software products that you use to install or uninstall the DMZ Secure Proxy Server for IBM WebSphere Application Server.

Before you begin

Restrictions: You must have Java SE 6 32 bit (option 30 of the IBM Developer Kit for Java) installed on your IBM i system before installing the DMZ Secure Proxy Server. For more information, read “IBM i prerequisites” on page 28.

About this task

Perform one of these procedures to install, update, roll back, or uninstall the product using Installation Manager.

Note: For information on installing and removing fix packs for WebSphere Application Server offerings on IBM i systems using the Installation Manager command line, read the following articles in this information center:

- Installing fix packs on IBM i operating systems using the command line
- Uninstalling fix packs from IBM i operating systems using the command line

For more information on using Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Procedure

- “Installing the DMZ Secure Proxy Server on IBM i operating systems using response files” on page 94
- “Installing the DMZ Secure Proxy Server on IBM i operating systems using the command line” on page 97
- “Installing and removing DMZ Secure Proxy Server features on IBM i operating systems using response files” on page 101
- “Installing fix packs on the DMZ Secure Proxy Server on IBM i operating systems using response files” on page 102
- “Uninstalling fix packs from the DMZ Secure Proxy Server on IBM i operating systems using response files” on page 104
- “Uninstalling the DMZ Secure Proxy Server from IBM i operating systems using response files” on page 105
- “Uninstalling the DMZ Secure Proxy Server from IBM i operating systems using the command line” on page 106

Results

- The following locations are the defaults for Installation Manager files on IBM i systems:
 - **Installation location:** /QIBM/ProdData/InstallationManager
 - **Agent data location:** /QIBM/UserData/InstallationManager
 - **Registry:** /QIBM/InstallationManager/.ibm/registry/InstallationManager.dat
- Logs are located in the logs directory of Installation Manager's agent data location. For example:

/QIBM/UserData/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.

Installing the DMZ Secure Proxy Server on IBM i operating systems using response files

You can install the DMZ Secure Proxy Server using Installation Manager response files.

Before you begin

Prepare for the installation before using this procedure. See Chapter 5, “Preparing the operating system for installation on IBM i,” on page 27 for more information.

Before you install the DMZ Secure Proxy Server, ensure that your user profile has *ALLOBJ and *SECADM special authorities.

Install Installation Manager on the system onto which you want to install the product.

- If you want to use the Installation Manager that comes with this product, perform the following actions:

1. Obtain the necessary files.

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 the product repositories on the product media.

- a. Install Installation Manager on your system.

You can install Installation Manager using the product media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

- b. Use 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 with a Passport Advantage ID and password can download the necessary product repositories from the Passport Advantage site.

- a. Download the files from the Passport Advantage site.

- b. Install Installation Manager on your system.

You can install Installation Manager using the product media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

- c. Use Installation Manager to install the product from the downloaded repositories.

- **Access the live repositories, and use web-based installation**

If you have a Passport Advantage ID and password, you can install the product from the web-based repositories.

- a. Install Installation Manager on your system.

You can install Installation Manager using the product media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

- b. Use Installation Manager to install the product from the web-based repository located at

<http://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v85>

Note: This location does not contain a web page that you can access using a web browser. This is a remote web-based repository location that you must specify in the response file so that the installation can access the files in this repository.

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

Note: If you do not have a Passport Advantage ID and password, you must install the product from the product repositories on the media or local repositories.

2. Install Installation Manager.

- a. Sign on to the IBM i system with a user profile that has *ALLOBJ and *SECADM special authorities.
- b. On a CL command line, run the **STRQSH** command to start the Qshell command shell.
- c. Make sure that the umask is set to 022.

To verify the umask setting, issue the following command:

```
umask
```

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

```
umask 022
```

- d. Change to the temporary directory where you unpacked the Installation Manager files.
- e. Run the following command in the temporary folder:

```
installc -acceptLicense -log log_file_path_and_name
```

Notes:

- For more information on installing Installation Manager, see the IBM Installation Manager Version 1.5 Information Center.
- Use only the **installc** command to install Installation Manager.
- 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.

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 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 with a Passport Advantage ID and password can download the necessary product repositories from the Passport Advantage site.

1. Download the product repositories from the Passport Advantage site.
2. Use Installation Manager to install the product from the downloaded repositories.

– **Access the live repositories, and use web-based installation**

If you have a Passport Advantage ID and password, you can use Installation Manager to install the product from the web-based repositories. Use Installation Manager to install the product from the web-based repository located at

```
http://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v85
```

Note: This location does not contain a web page that you can access using a web browser. This is a remote web-based repository location that you must specify in the response file so that the installation can access the files in this repository.

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

Note: If you do not have a Passport Advantage ID and password, you must install the product from the product repositories on the media or local repositories.

Procedure

1. Optional: If the repository requires a username and password, create a keyring file to access this repository.

For more information on creating a keyring file for Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Tip: When creating a keyring file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

2. Sign on to the IBM i system with a user profile that has `*ALLOBJ` and `*SECADM` special authorities.
3. On a CL command line, run the `STRQSH` command to start the Qshell command shell.
4. Make sure that the `umask` is set to `022`.

To verify the `umask` setting, issue the following command:

```
umask
```

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

```
umask 022
```

5. Use a response file to install the DMZ Secure Proxy Server.

Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and install the DMZ Secure Proxy Server. For example:

```
./imcl -acceptLicense  
input $HOME/WASFiles/temp/install_response_file.xml  
-log $HOME/WASFiles/temp/install_log.xml  
-keyring $HOME/WASFiles/temp/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.
- `/QIBM/ProdData/InstallationManager` is the default installation location for Installation Manager files on IBM i systems.
- The program might write important post-installation instructions to standard output.

Read the IBM Installation Manager Version 1.5 Information Center for more information.

Example

The following is an example of a response file for installing the DMZ Secure Proxy Server with the Administration Thin Client feature into the `/QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ` directory using a web-based repository located at `http://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v85`.

```
<?xml version="1.0" encoding="UTF-8"?>  
<agent-input>  
<server>  
  <repository location='http://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v85' />  
</server>  
<profile id='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ'>  
  <data key='eclipseLocation' value='/QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ' />  
  <data key='was.install.os400.profile.location' value='/QIBM/UserData/WebSphere/AppServer/V85/NDDMZ' />  
  <data key='user.import.profile' value='false' />  
  <data key='cic.selector.nl' value='en, fr, it, zh, ro, ru, zh_TW, de, ja, pl, es, cs, hu, ko, pt_BR' />  
</profile>  
<install modify='false'>  
  <offering profile='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.5' features='core.feature,thinclient' id='com.ibm.websphere.NDDMZ.v85' />  
</install>  
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/QIBM/UserData/InstallationManager/IMShared' />  
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />  
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='30' />  
<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.preserveDownloadedArtifacts' 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' />  
</agent-input>
```

What to do next

You can create a secure proxy profile using the `manageprofiles` command.

The following is an example of using the **manageprofiles** command to create a default secure proxy profile. This example is based on the following assumptions:

- Security is to be enabled.
- The system host name is myhost.abc.com.
- The *appserver_install_root* is /QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ.
- The *user_data_root* is /QIBM/UserData/WebSphere/AppServer/V85/NDDMZ.
- The administrative user name is wasadmin.
- The password is password.

```
manageprofiles -create
-portsFile /QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ/profileTemplates/secureproxy/actions/portsUpdate/portdef.props
-serverName proxy1
-nodeName myhost
-hostName myhost.abc.com
-cellName myhost
-adminUserName wasadmin
-adminPassword password
-templatePath /QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ/profileTemplates/secureproxy
-enableAdminSecurity true
-profileName SecureProxySrv01
```

The following is an example of using the **manageprofiles** command to make profile SecureProxySrv01 the default profile.

```
manageprofiles -setDefaultName -profileName SecureProxySrv01
```

Installing the DMZ Secure Proxy Server on IBM i operating systems using the command line

You can install the DMZ Secure Proxy Server using the Installation Manager command line.

Before you begin

Prepare for the installation before using this procedure. See Chapter 5, “Preparing the operating system for installation on IBM i,” on page 27 for more information.

Important: Before installing the product, you must read the license agreement that you can find with the product files. Signify your acceptance of the license agreement by specifying `-acceptLicense` in the command as described below.

Before you install the DMZ Secure Proxy Server, ensure that your user profile has `*ALLOBJ` and `*SECADM` special authorities.

Install Installation Manager on the system onto which you want to install the product.

- If you want to use the Installation Manager that comes with this product, perform the following actions:

1. Obtain the necessary files.

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 the product repositories on the product media.

- a. Install Installation Manager on your system.

You can install Installation Manager using the product media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

- b. Use 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 with a Passport Advantage ID and password can download the necessary product repositories from the Passport Advantage site.

- a. Download the files from the Passport Advantage site.
- b. Install Installation Manager on your system.

You can install Installation Manager using the product media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

- c. Use Installation Manager to install the product from the downloaded repositories.

– **Access the live repositories, and use web-based installation**

If you have a Passport Advantage ID and password, you can install the product from the web-based repositories.

- a. Install Installation Manager on your system.

You can install Installation Manager using the product media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

- b. Use Installation Manager to install the product from the web-based repository located at

<http://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v85>

Note: This location does not contain a web page that you can access using a web browser. This is a remote web-based repository location that you must specify for the value of the `-repositories` parameter so that the `imcl` command can access the files in this repository to install the product.

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

Note: If you do not have a Passport Advantage ID and password, you must install the product from the product repositories on the media or local repositories.

2. Install Installation Manager.

- a. Sign on to the IBM i system with a user profile that has `*ALLOBJ` and `*SECADM` special authorities.
- b. On a CL command line, run the `STRQSH` command to start the Qshell command shell.
- c. Make sure that the `umask` is set to `022`.

To verify the `umask` setting, issue the following command:

```
umask
```

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

```
umask 022
```

- d. Change to the temporary directory where you unpacked the Installation Manager files.
- e. Run the following command in the temporary folder:

```
installc -acceptLicense -log log_file_path_and_name
```

Notes:

- For more information on installing Installation Manager, see the IBM Installation Manager Version 1.5 Information Center.
- When installing the product on IBM i operating systems, use only the `installc` command to install Installation Manager.

3. If you are using local repositories to install and maintain the product, unpack the compressed file containing the repository to a directory on your system.

- 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.

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 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 with a Passport Advantage ID and password can download the necessary product repositories from the Passport Advantage site.

1. Download the product repositories from the Passport Advantage site.
2. Use Installation Manager to install the product from the downloaded repositories.

– **Access the live repositories, and use web-based installation**

If you have a Passport Advantage ID and password, you can use Installation Manager to install the product from the web-based repositories. Use Installation Manager to install the product from the web-based repository located at

<http://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v85>

Note: This location does not contain a web page that you can access using a web browser. This is a remote web-based repository location that you must specify for the value of the `-repositories` parameter so that the `imcl` command can access the files in this repository to install the product.

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

Note: If you do not have a Passport Advantage ID and password, you must install the product from the product repositories on the media or local repositories.

Procedure

1. Optional: If the repository requires a username and password, create a keyring file to access this repository.

For more information on creating a keyring file for Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Tip: When creating a keyring file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

2. Sign on to the IBM i system with a user profile that has *ALLOBJ and *SECADM special authorities.
3. On a CL command line, run the **STRQSH** command to start the Qshell command shell.
4. Make sure that the `umask` is set to 022.

To verify the `umask` setting, issue the following command:

```
umask
```

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

```
umask 022
```

5. Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.
6. Use the `imcl` command to install the product.

```
./imcl install com.ibm.websphere.NDDMZ.v85_offering_version,optional_feature_ID
-repositories source_repository
-installationDirectory installation_directory
-sharedResourcesDirectory shared_directory
-accessRights access_mode
-preferences preference_key=value
-properties property_key=value
-keyring keyring_file -password password
-acceptLicense
```

Tips:

- 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.

- You can add a list of features that are separated by commas. The feature ID `thinclient` indicates the standalone thin clients and resource adapters.
If a list of features is not specified, the default feature (`thinclient`) is installed.
- The `offering_version`, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to install (8.5.0.20110503_0200 for example).
 - If `offering_version` is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
 - If `offering_version` is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
./imcl listAvailablePackages -repositories source_repository
```

- You can also specify `none`, `recommended` or `all` with the `-installFixes` argument to indicate which interim fixes you want installed with the offering.
 - If the offering version is **not** specified, the `-installFixes` option defaults to `all`.
 - If the offering version is specified, the `-installFixes` option defaults to `none`.
- For initial installations, it is a good practice to specify the `user_data_root`; otherwise, the default value for the `user_data_root`, `/QIBM/UserData/WebSphere/AppServer/V85/NDDMZ`, is used. Use the `was.install.os400.profile.location` property to specify the `user_data_root`. If the `user_data_root` is to be `/QIBM/UserData/WebSphere/AppServer/V85/NDDMZ`, for example, specify `-properties was.install.os400.profile.location=/QIBM/UserData/WebSphere/AppServer/V85/NDDMZ` on the `imcl` installation command.
- The program might write important post-installation instructions to standard output.

For more information on using the `imcl` command to install the product, see the IBM Installation Manager Version 1.5 Information Center.

What to do next

You can create a secure proxy profile using the `manageprofiles` command.

The following is an example of using the `manageprofiles` command to create a default secure proxy profile. This example is based on the following assumptions:

- Security is to be enabled.
- The system host name is `myhost.abc.com`.
- The `appserver_install_root` is `/QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ`.
- The `user_data_root` is `/QIBM/UserData/WebSphere/AppServer/V85/NDDMZ`.
- The administrative user name is `wasadmin`.
- The password is `password`.

```
manageprofiles -create
  -portsFile /QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ/profileTemplates/secureproxy/actions/portsUpdate/portdef.props
  -serverName proxy1
  -nodeName myhost
  -hostName myhost.abc.com
  -cellName myhost
  -adminUserName wasadmin
  -adminPassword password
  -templatePath /QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ/profileTemplates/secureproxy
  -enableAdminSecurity true
  -profileName SecureProxySrv01
```

The following is an example of using the `manageprofiles` command to make profile `SecureProxySrv01` the default profile.

```
manageprofiles -setDefaultName -profileName SecureProxySrv01
```

Installing and removing DMZ Secure Proxy Server features on IBM i operating systems using response files

You can install and remove a DMZ Secure Proxy Server feature using Installation Manager response files.

About this task

Perform this procedure to use Installation Manager to install or remove a DMZ Secure Proxy Server feature using a response file.

Like other Installation Manager operations, you can invoke a modification using the `imcl` command-line tool. Go to the IBM Installation Manager Version 1.5 Information Center for more information.

Procedure

1. Optional: If the repository requires a username and password, create a keyring file to access this repository.

For more information on creating a keyring file for Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Tip: When creating a keyring file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

2. Sign on to the IBM i system with a user profile that has `*ALLOBJ` and `*SECADM` special authorities.
3. On a CL command line, run the `STRQSH` command to start the Qshell command shell.
4. Use a response file to install or remove a DMZ Secure Proxy Server feature.

Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and modify the DMZ Secure Proxy Server. For example:

```
./imcl
input $HOME/WASFiles/temp/modify_response_file.xml
-log $HOME/WASFiles/temp/modify_log.xml
-keyring $HOME/WASFiles/temp/im.keyring
```

Note: The program might write important post-installation instructions to standard output.

For more information on using Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Example

- Here are examples of response files for modifying the features in an installation:
 - Here is a response file that adds the Administration Thin Client feature to an existing DMZ Secure Proxy Server that is installed in the `/QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ` directory:

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<server>
  <repository location='https://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v85'/>
</server>
<profile id='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ'>
  <data key='eclipseLocation' value='/QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ'/>
  <data key='was.install.os400.profile.location' value='/QIBM/UserData/WebSphere/AppServer/V85/NDDMZ'/>
  <data key='user.import.profile' value='false'/>
  <data key='cic.selector.nl' value='en, fr, it, zh, ro, ru, zh_TW, de, ja, pl, es, cs, hu, ko, pt_BR'/>
</profile>
<install modify='true'>
  <offering profile='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.5' features='thinclient' id='com.ibm.websphere.NDDMZ.v85'/>
</install>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/QIBM/UserData/InstallationManager/IMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='30'/>
<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.preserveDownloadedArtifacts' 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'/>
</agent-input>

```

- To alter this response file to remove a feature, simply change the `install` tags to `uninstall`. Here is the same response file modified to remove the Administration Thin Client feature:

```

<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<server>
  <repository location='https://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v85'/>
</server>
<profile id='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ'>
  <data key='eclipseLocation' value='/QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ'/>
  <data key='was.install.os400.profile.location' value='/QIBM/UserData/WebSphere/AppServer/V85/NDDMZ'/>
  <data key='user.import.profile' value='false'/>
  <data key='cic.selector.nl' value='en, fr, it, zh, ro, ru, zh_TW, de, ja, pl, es, cs, hu, ko, pt_BR'/>
</profile>
<uninstall modify='true'>
  <offering profile='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.5' features='thinclient' id='com.ibm.websphere.NDDMZ.v85'/>
</uninstall>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/QIBM/UserData/InstallationManager/IMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='30'/>
<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.preserveDownloadedArtifacts' 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'/>
</agent-input>

```

- Here is an example of the `imcl` command for modifying the features in an installation:

```

./imcl.exe modify com.ibm.websphere.NDDMZ.v85
-addFeatures thinclient
-repositories https://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v85
-installationDirectory /QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ
-keyring /var/keyring_file.keyring -password password

```

Installing fix packs on the DMZ Secure Proxy Server on IBM i operating systems using response files

You can update the DMZ Secure Proxy Server to a later version using Installation Manager response files.

Before you begin

Tip: As an alternative to the procedure that is described in this article, Installation Manager allows you to use the `updateAll` command in a response file or on the command line to search for and update all installed packages. Use this command only if you have full control over which fixes are contained in the targeted repositories. If you create and point to a set of custom repositories that include only the specific fixes that you want to install, you should be able to use this command confidently. If you enable searching service repositories or install fixes directly from other live web-based repositories, then you might not want to select this option so that you can select only the fixes that you want to install using the `-installFixes` option with the `install` command on the command line or the `installFixes` attribute in a response file.

About this task

Perform this procedure to use Installation Manager to update the DMZ Secure Proxy Server using Installation Manager response files.

Note: For information on installing and removing fix packs for WebSphere Application Server offerings on IBM i systems using the Installation Manager command line, read the following articles in this information center:

- Installing fix packs on IBM i operating systems using the command line
- Uninstalling fix packs from IBM i operating systems using the command line

Procedure

1. Optional: If the repository requires a username and password, create a keyring file to access this repository.

For more information on creating a keyring file for Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Tip: When creating a keyring file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

2. Sign on to the IBM i system with a user profile that has `*ALLOBJ` and `*SECADM` special authorities.
3. On a CL command line, run the `STRQSH` command to start the Qshell command shell.
4. Use a response file to update the DMZ Secure Proxy Server.

Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and update the DMZ Secure Proxy Server. For example:

```
./imcl -acceptLicense
input $HOME/WASFiles/temp/update_response_file.xml
-log $HOME/WASFiles/temp/update_log.xml
-keyring $HOME/WASFiles/temp/im.keyring
```

For more information on using Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Example

The following is an example of a response file for updating the DMZ Secure Proxy Server to a later version.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<server>
  <repository location='https://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v85' />
</server>
<profile id='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ'>
  <data key='eclipseLocation' value='/QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ' />
  <data key='was.install.os400.profile.location' value='/QIBM/UserData/WebSphere/AppServer/V85/NDDMZ' />
  <data key='user.import.profile' value='false' />
  <data key='cic.selector.nl' value='en, fr, it, zh, ro, ru, zh_TW, de, ja, pl, es, cs, hu, ko, pt_BR' />
</profile>
<install modify='false'>
  <offering profile='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.5'
    id='com.ibm.websphere.NDDMZ.v85' version='8.5.0.20101025_2108' features='core.feature' />
</install>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/QIBM/UserData/InstallationManager/IMShared' />
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='30' />
<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.preserveDownloadedArtifacts' 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' />
</agent-input>
```

Tips:

- The profile ID (`<profile . . . id='profile_ID'>` and `<offering . . . profile='profile_ID'>`) can be found when you run the `imcl listInstallationDirectories -verbose` command from the `eclipse/tools` subdirectory in the directory where you installed Installation Manager. It is the same as the package group's name.
- The offering ID (`<offering . . . id='offering_ID'>`) can be found in the Install Manager Offering ID section of the report that is generated when you run the `historyInfo` or `genHistoryReport` command from the `app_server_root/bin` directory.
- The *version* is a specific version of the offering to install (8.5.0.20101025_2108 for example). This specification is optional.

- If *version* is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
- If *version* is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
./imcl listAvailablePackages -repositories source_repository
```

- You can also specify *none*, *recommended* or *all* with the `-installFixes` argument to indicate which interim fixes you want installed with the offering.
 - If the offering version is **not** specified, the `-installFixes` option defaults to *all*.
 - If the offering version is specified, the `-installFixes` option defaults to *none*.

Uninstalling fix packs from the DMZ Secure Proxy Server on IBM i operating systems using response files

You can roll back the DMZ Secure Proxy Server to an earlier version using Installation Manager response files.

Before you begin

During the rollback process, Installation Manager must access files from the earlier version of the package. By default, these files are stored on your computer when you install a package. If you change the default setting or delete the saved files, Installation Manager requires access to the repository that was used to install the earlier version.

About this task

Perform this procedure to use Installation Manager to roll back the DMZ Secure Proxy Server to an earlier version using Installation Manager response files.

Note: For information on installing and removing fix packs for WebSphere Application Server offerings on IBM i systems using the Installation Manager command line, read the following articles in this information center:

- Installing fix packs on IBM i operating systems using the command line
- Uninstalling fix packs from IBM i operating systems using the command line

Procedure

1. Optional: If the repository requires a username and password, create a keyring file to access this repository.

For more information on creating a keyring file for Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Tip: When creating a keyring file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

2. Sign on to the IBM i system with a user profile that has `*ALLOBJ` and `*SECADM` special authorities.
3. On a CL command line, run the `STRQSH` command to start the Qshell command shell.
4. Use a response file to roll back the DMZ Secure Proxy Server.

Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and roll back the DMZ Secure Proxy Server. For example:

```
./imcl
input $HOME/WASFiles/temp/rollback_response_file.xml
-log $HOME/WASFiles/temp/rollback_log.xml
-keyring $HOME/WASFiles/temp/im.keyring
```


For more information on using Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Example

The following is an example of a response file for rolling back the DMZ Secure Proxy Server to an earlier version.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<server>
  <repository location='https://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.v85' />
</server>
<profile id='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ'>
  <data key='eclipseLocation' value='/QIBM/ProdData/WebSphere/AppServer/V85/NDDMZ' />
</profile>
<rollback>
  <offering profile='DMZ Secure Proxy Server for IBM WebSphere Application Server V8.5' id='com.ibm.websphere.NDDMZ.v85' version='8.5.0.20101025_2108' />
</rollback>
</agent-input>
```

Tips:

- The profile ID (<profile . . . id='profile_ID'> and <offering . . . profile='profile_ID'>) can be found when you run the `imcl listInstallationDirectories -verbose` command from the `eclipse/tools` subdirectory in the directory where you installed Installation Manager. It is the same as the package group's name.
- The offering ID (<offering . . . id='offering_ID'>) can be found in the Install Manager Offering ID section of the report that is generated when you run the **historyInfo** or **genHistoryReport** command from the `app_server_root/bin` directory.
- The *version* is a specific version of the offering to which to roll back (8.5.0.20101025_2108 for example).

This specification is optional if you are using Installation Manager Version 1.5 or later.

- If *version* is **not** specified, the installation rolls back to the previously installed version of the offering and **all** interim fixes for that version are installed.
- If *version* is specified, the installation rolls back to the specified earlier version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore in the Package section of the report that is generated when you run the **historyInfo** or **genHistoryReport** command from the `app_server_root/bin` directory.

Uninstalling the DMZ Secure Proxy Server from IBM i operating systems using response files

You can uninstall the DMZ Secure Proxy Server using Installation Manager response files.

Procedure

1. Stop all servers and applications on the WebSphere Application Server installations that contain the DMZ Secure Proxy Server.
2. Sign on to the IBM i system with a user profile that has *ALLOBJ and *SECADM special authorities.
3. On a CL command line, run the **STRQSH** command to start the Qshell command shell.
4. Use a response file to uninstall the DMZ Secure Proxy Server.

Complete one of the following actions:

- From a command line on each of the systems from which you want to uninstall the DMZ Secure Proxy Server, run the **uninstall** script (which uses the `uninstall.xml` response file in the same directory) to uninstall the DMZ Secure Proxy Server. For example:

```
app_server_root/uninstall/uninstall
```

- 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 `uninstall.xml` response file in the same directory to uninstall the DMZ Secure Proxy Server. For example:

```
./imcl
input app_server_root/uninstall/uninstall.xml
-log $HOME/WASFiles/temp/uninstall_log.xml
```

- 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 a response file that you created to uninstall the DMZ Secure Proxy Server. For example:

```
./imcl
input $HOME/WASFiles/temp/uninstall_response_file.xml
-log $HOME/WASFiles/temp/uninstall_log.xml
```

Go to the IBM Installation Manager Version 1.5 Information Center for more information.

5. 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 Version 1.5 Information Center for information about using the `uninstall` script to perform this procedure.

Example

The `app_server_root/uninstall/uninstall.xml` file is an example of a response file for uninstalling the DMZ Secure Proxy Server.

Uninstalling the DMZ Secure Proxy Server from IBM i operating systems using the command line

You can uninstall the DMZ Secure Proxy Server using the Installation Manager command line.

Procedure

1. Stop all servers and applications on the WebSphere Application Server installations that contain the DMZ Secure Proxy Server.
2. Sign on to the IBM i system with a user profile that has `*ALLOBJ` and `*SECADM` special authorities.
3. On a CL command line, run the **STRQSH** command to start the Qshell command shell.
4. Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.
5. Use the `imcl` command to uninstall the product.

For example:

```
./imcl uninstall com.ibm.websphere.NDDMZ.v85,optional_feature_ID
-installationDirectory installation_directory
```

You can remove a list of features that are separated by commas—the feature ID `thinclient` indicates the standalone thin clients and resource adapters. If a list of features is not specified, the entire product is uninstalled.

For more information on using the `imcl` command to uninstall the product, see the IBM Installation Manager Version 1.5 Information Center.

Chapter 11. 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.x.

Before you begin

The process for managing Version 7.x and previous versions is different from the process for managing Version 8.x. The following topic explains the different CIM usage scenarios.

About this task

The Version 8.5 Centralized Installation Manager (CIM) can be used to manage Version 8.5 and previous versions of WebSphere Application Server. You can use CIM to install or uninstall Version 8.5 and previous versions of WebSphere Application Server on remote machines and apply maintenance from the administrative console. In Version 8.0 and later, targets can be added outside of the cell. The process for managing Version 7.x and previous versions is different from the process for managing Version 8.x, 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.x, and each process is documented separately in the information center. For Version 8.x, 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.

- **IBM i** To get started using CIM for Version 8.5, see “Submitting Installation Manager jobs” on page 108
- **IBM i** To get started using CIM for Version 6.1.x and 7.x*, see “Getting started with the centralized installation manager (CIM) for previous versions” on page 124.

*(Not supported on z/OS targets.)

Table 6. Differences between CIM for Version 8.x and CIM for Version 6.1.x and 7.x

Function	CIM Version 6.1.x and 7.x	CIM Version 8.x
Scope	Install, update, uninstall Version 7.x. Update Version 6.1.x* *(Not supported on z/OS targets.)	Install, update, uninstall Version 8.x 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.x, 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.x 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 and later, 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 8.5 products.


Before you begin

Note: This topic applies to WebSphere Application Server Version 8.5.

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.

 The user profile must have *JOBCTL authorization in order to use centralized installation manager (CIM) on IBM i targets.

For Version 8.0 and later, 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

For Version 8.x, CIM functions are not compatible with CIM Version 6.x or 7.x.

Note: IBM Installation Manager 1.5.2 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.

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:
- If you are using the command line, run the following command and follow the instructions:

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.

 To perform the installIM job as an administrative user on IBM i , the user profile must have *JOBCTL, *ALLOBJ and *SECADM authorizations.

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 1.5.2 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/CIMJMetadata.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:
- If you are using the command line, run the following command and follow the instructions:

To install Installation Manager so that it can be used by a group of users, specify the **installType** optional parameter. Values for the parameter include:


- **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 you 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 8.5

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:

- If you are using the command line, run the following command and follow the instructions:

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 1.5.2 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.


Installing the Version 8.5 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 8.5. For information about using centralized installation manager (CIM) for Version 6.1.x and 7.x, see the topic about getting started with the centralized installation manager (CIM) for previous versions..

Ensure that you have the administrative console installed on your primary machine.

 The user profile must have *JOBCTL authorization in order to use centralized installation manager (CIM) on IBM i targets.

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 1.5.2 or later 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 8.5 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

Before you install WebSphere Application Server using the job manager, ensure that you have WebSphere Application Server Version 8.5 installed on your primary machine.

 The user profile must have *JOBCTL authorization in order to use centralized installation manager (CIM) on IBM i targets.

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 1.5.2 or later 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.
 - a. 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')
```
 - b. 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.

- a. 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.

- a. 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.

- b. You can edit the response file to include information about your target machine.

- c. 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.

- 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:\\WAS85\\logs\\manageprofiles\\response.log} {destination log}}}
```

- Using Jython:

```
AdminTask.submitJob({'-jobType collectFile -targetList hostname -jobParams  
[[source D:\\WAS85\\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.

Note:  The centralized installation manager can not discover profiles for Application Client and Plugin on IBM i platforms.

- You can submit an 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.
- 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:
 - If you are using the command line, run the following command and follow the instructions:
- 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 8.5, see “Submitting Installation Manager jobs” on page 108.

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 131.

Restriction: This feature is not available in WebSphere Application Server Network Deployment for z/OS.

About this task

Table 7. Differences between CIM versions. This table lists the differences between CIM for Version 8.x and CIM for Version 6.x and 7.x

Function	CIM Version 6.x and 7.x	CIM Version 8.x
Scope	Install, update, uninstall Version 7.x. Update Version 6.x	Install, update, uninstall Version 8.x 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 8.5 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” on page 124.
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 131.
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 143.

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 149.
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 154.
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 156.

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. The IBM 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”
- “Adding installation packages of previous versions to the centralized installation manager (CIM) repository using the Installation Factory” on page 126
- “Special procedures for IBM i operating systems when running the centralized installation manager (CIM) for previous versions” on page 128
- “Installing Version 6.1.x and 7.x customized installation packages (CIPs) using the centralized installation manager (CIM)” on page 134
- “Requirements for using Remote Execution and Access (RXA)” on page 129
- “Additional requirements for installing or uninstalling maintenance to previous versions on AIX as a non-root user” on page 130

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: 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.

Note:

- 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`. If you are using two different users to install and run WebSphere Application Server, the user that runs WebSphere Application Server must have write permission to create the `cimrepos` directory and its content. Otherwise, some functions in the centralized installation manager such as downloading new descriptors or Update Installer will not work. You might see an error in the `SystemOut.log` that is similar to the following:

```
XCIM0903E: Cannot download file 7.0.0.13-WS-UPDI-i50sPPC.zip.part to /QIBM/ProdData/WebSphere/AppServer/cimrepos/UPDI70.  
Reason: /QIBM/ProdData/WebSphere/AppServer/cimrepos/UPDI70/7.0.0.13-WS-UPDI-i50sPPC.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>`, you can relocate the repository location outside of `<WAS_HOME>` by modifying the value in `cimgr.props`.

- When you install WebSphere Application Server version 7.0 to a node using centralized installation manager and you encounter a time out error that is similar to the following,

```
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`. This file is 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). For installation WebSphere Application Server version 7.0 on IBM i nodes, you may change the time out value to 5,400 seconds (90 mins). Save the changes and restart deployment manager.

Procedure

1. Launch the Installation Factory from the following location, where *if_root* is the Installation Factory root directory.
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.

Table 8. *ifcli* command-line options for centralized installation manager.

This table describes command-line options for centralized installation manager.

Option	Description
<code>-wasPath wasInstallationPath</code>	Specifies the directory path of the WebSphere Application Server installation.
<code>-repositoryPath repositoryPath</code>	Specifies the directory path of the repository.
<code>-installationPackagePath installationPackagePath</code>	Specifies the directory path of the installation package.
<code>-overwrite</code>	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 8.5, see “Submitting Installation Manager jobs” on page 108.

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 8.5 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-i50sPPC.zip.part to /QIBM/ProdData/WebSphere/AppServer/cimrepos/UPDI70.  
Reason: /QIBM/ProdData/WebSphere/AppServer/cimrepos/UPDI70/7.0.0.13-WS-UPDI-i50sPPC.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.x and 7.x. 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**.

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**.

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:

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:

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 8.5, see “Submitting Installation Manager jobs” on page 108.

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. As a recommended alternative, 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 on distributed and IBM i systems. You can also use HPEL in conjunction with your 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 8.5, see “Submitting Installation Manager jobs” on page 108.

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 8.5. 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.x or 7.x host in your Version 8.x 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.x 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.x 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.x 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. As a recommended alternative, 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 on distributed and IBM i systems. You can also use HPEL in conjunction with your 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 8.5, see "Submitting Installation Manager jobs" on page 108.

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://public.dhe.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://public.dhe.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://public.dhe.ibm.com/software/websphere/appserv/support/fixpacks/was70/cumulative/
```

Replace it with the following:

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.x, 7.x, and 8.x 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.x deployment manager cannot manage both Version 7.x and 8.x nodes. However, a Version 8.x deployment manager can manage both Version 7.x and 8.x 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.x, 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.x product does not install the Version 6.1.x and 7.x fix-pack descriptors for the centralized installation manager. These steps enable you to obtain those Version 6.1.x and 7.x 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://public.dhe.ibm.com/software/websphere/appserv/support/tools/UpdateInstaller/7.0.x/_yyyymmdd`. If the deployment manager workstation does not have Internet access, an error message is displayed indicating that the host name, `public.dhe.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 8.5, see “Submitting Installation Manager jobs” on page 108.

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.

gotcha: Please use the fully qualified domain name as the hostname when adding remote targets. If you use an IP address for the hostname, it is possible to have the same node name generated for different nodes in the same deployment manager cell.

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

- 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 8.5, see "Submitting Installation Manager jobs" on page 108.

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 8.5 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.

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 8.5, see “Submitting Installation Manager jobs” on page 108.

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 8.5, see “Submitting Installation Manager jobs” on page 108.

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 8.5.
 - 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:
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 8.5, see “Submitting Installation Manager jobs” on page 108.

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 108.

The administrative tasks for the centralized installation manager include the following commands:

- “installWASExtension” on page 157
- “installSoftware” on page 158
- “installWithResponseFile” on page 160
- “installMaintenance” on page 162
- “listPackagesForInstall” on page 163
- “listFeaturesForInstall” on page 163
- “showPackageInfo” on page 164

- “showLicenseAgreement” on page 164
- “getManagedNodesOnHostByInstallLoc” on page 165
- “listManagedNodesOnHost” on page 166
- “testConnectionToHost” on page 166
- “testConnectionToHostUsingSSHKey” on page 167
- “installSSHPublicKeyOnHost” on page 168
- “listKeyInstallationRecords” on page 168
- “updateKeyInstallationRecords” on page 169
- “listPendingRequests” on page 169
- “listInProgressRequests” on page 170
- “listRequestsForTarget” on page 170
- “showLatestInstallStatus” on page 171
- “showLatestUninstallStatus” on page 172
- “uninstallSoftware” on page 172
- “uninstallMaintenance” on page 173

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 installWASEExtension {-packageName XD0ps -hostName river.com  
-augment ALL_NODES -adminName admin1  
-adminPassword passw0rd1 -acceptLicense true}
```

• Using Jython:

```
AdminTask.installWASEExtension ('[-packageName XD0ps -hostName river.com  
-augment ALL_NODES -adminName admin1  
-adminPassword passw0rd1 -acceptLicense true]')
```

Interactive mode example usage:

• Using Jacl:

```
$AdminTask installWASEExtension {-interactive}
```

• Using Jython:

```
AdminTask.installWASEExtension ('[-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 8.5, 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 8.5:

- **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-WAS-WAS-IFPKxxxx.pak,8.0.0.5-WAS-WAS-IFPKyyyy.pak" -hostName  
river.com -installLocation D:/WAS80 -adminName admin1 -adminPassword  
passw0rd1 -acceptLicense true}
```

- Using Jython:

```
AdminTask.installMaintenance ('[-packageName ND80Maintenance -fileList
"8.0.0.5-WAS-WAS-IFPKxxxxx.pak,8.0.0.5-WAS-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 passwd0rd3 -publicKeyStore /root/.ssh/id_rsa.pub}
```

- Using Jython:

```
AdminTask.installSSHPublicKeyOnHost ('[-hostName abc.com -adminName  
root -adminPassword passwd0rd3 -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

A

- administrative console
 - deployment managers 87
 - starting
 - IBM i 83
- application server
 - install
 - environment 3
 - verification
 - IBM i 82

C

- centralized installation manager (CIM)
 - AdminTask 156
 - descriptors and binary files 143
 - getting started 124
 - IBM i 128
 - installation
 - previous versions 138
 - Installation Factory
 - previous versions 126
 - interim fix 135
 - Internet 145
 - managing 149
 - managing cells 155
 - monitoring
 - previous versions 141
 - previous versions 123, 131
 - uninstallation 142
 - updating versions 156
 - usage 154
 - usage scenarios 154
- CIM
 - using 154

D

- default standalone application server
 - starting
 - IBM i 81
- deployment manager profiles
 - IBM i 84
- deployment managers
 - verification
 - IBM i 85
- directory
 - installation
 - conventions 17
- DMZ Secure Proxy Server
 - installation 93
 - IBM i 94, 101
 - uninstallation 93

H

- HTTP server
 - configuring 74
 - IBM i 76, 89
- HTTP Server
 - configuring 75

I

- IBM HTTP Server
 - *ADMIN 76
- IBM i
 - installation 53
 - planning 27
 - prerequisites 28
 - rolling back 64, 65
 - starting 81
 - uninstallation 53
 - updating 58
 - installation
 - configuration
 - IBM i 71
 - IBM i 7, 35, 43
 - learning 24
 - product 7
 - requirements 18
 - verification 69
 - installing
 - checklist 5
 - iRemoteInstall
 - installation
 - IBM i 48

J

- job managers
 - submitting Installation Manager jobs 108

L

- license
 - installation 71
- Lotus Domino HTTP Server
 - IBM i 78

M

- maintenance
 - installation 33
 - IBM i 32
 - requirements 131

N

- node agent
 - verification
 - IBM i 87
- nodes
 - default application server
 - IBM i 90
 - deployment managers
 - IBM i 86
 - verification
 - IBM i 88

P

- ports
 - updating
 - IBM i 19
- prerequisites 31

R

- requirements
 - installation 18
- response files
 - installation 37

S

- Secure Shell (SSH)
 - authentication method 153
 - installation
 - public key 151
- SQL
 - installation
 - IBM i 72

T

- TC/IP
 - IBM i 73

U

- uninstallation
 - DMZ Secure Proxy Server
 - IBM i 105
 - IBM i 35, 67
 - installation manager
 - IBM i 67