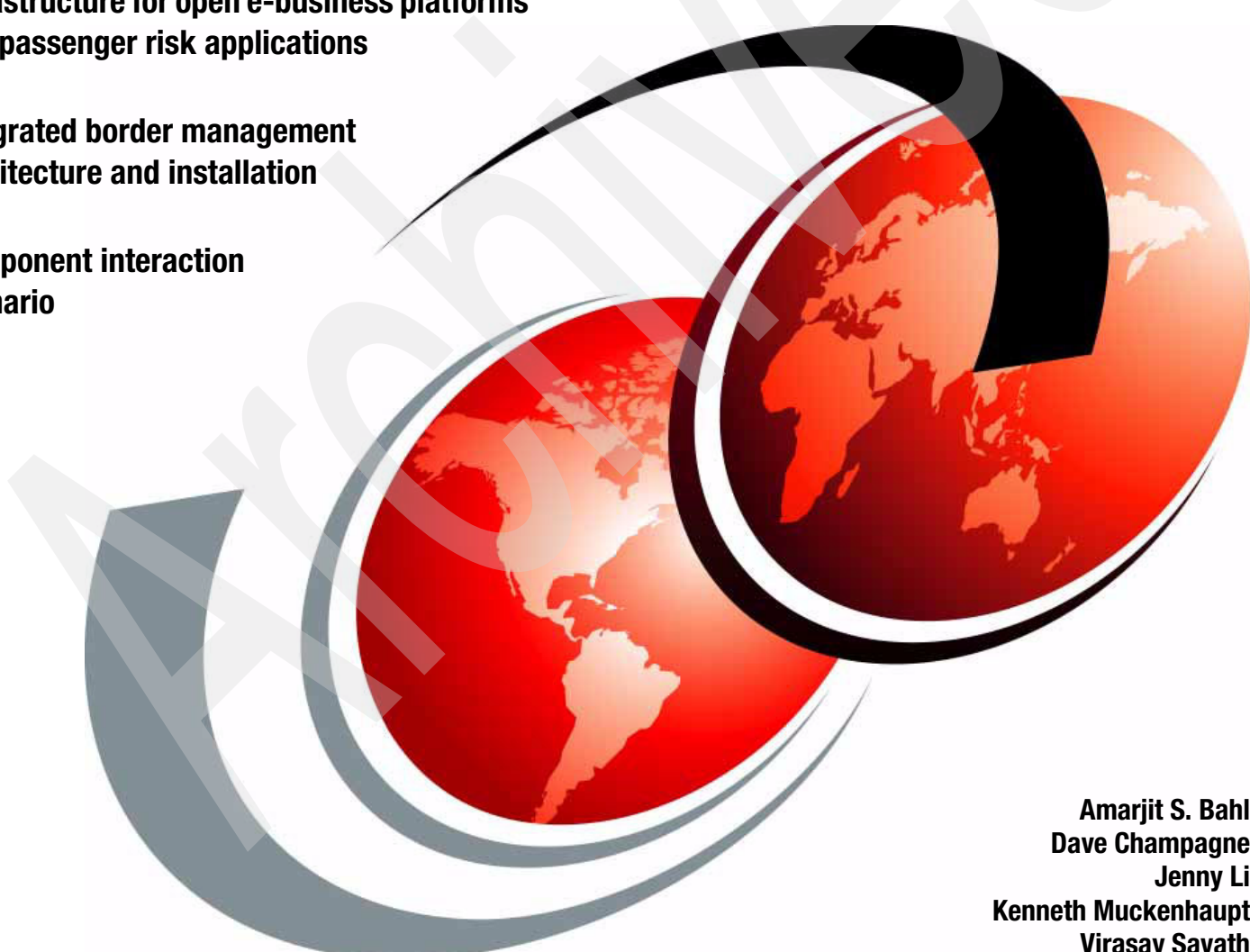**IBM**

Passenger Risk Management
Infrastructure Solution Building Block: Installation and Configuration Guide

Infrastructure for open e-business platforms and passenger risk applications

Integrated border management architecture and installation

Component interaction scenario

Amarjit S. Bahl
Dave Champagne
Jenny Li
Kenneth Muckenhaupt
Virasay Savath

Redbooks

IBM

International Technical Support Organization

**Passenger Risk Management Infrastructure Solution
Building Block: Installation and Configuration Guide**

May 2006

SG24-7201-00

First Edition (May 2006)

Contents

iii

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described 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 Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

vii

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

@server®	BladeCenter®	Lotus®
e-business on demand™	Cloudscape™	Notes®
pSeries®	DB2 Connect™	OS/390®
z/OS®	DB2®	Redbooks™
zSeries®	HACMP™	Redbooks (logo) ™
AIX 5L™	IBM®	Tivoli®
AIX®	Lotus Notes®	WebSphere®

The following terms are trademarks of other companies:

EJB, Java, JDBC, JMX, J2EE, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

In a post 9/11 environment, our government customers are faced with the challenge of optimizing the flow of international commerce while ensuring security and border integrity. Integrated Border Management is one of IBM®'s Selected Business Solutions (SBS) for the Government Industry. The target customers for Integrated Border Management include central government border management and immigration agencies, regional or local port authorities, border police and local law enforcement, national intelligence, agriculture, health, trade regulatory and central government customs agencies worldwide.

Each component of the solution is described in a separate chapter.

► The *Portal Server* provides client browser-based access to the Border Management Passenger Risk applications.

► *WebSphere® Business Integration Server Foundation* (WBISF) V5.1.x provides an environment for services composition, basically a process or workflow within the system.

► *JRules* is a business rules execution product from ILOG that executes business rules on production J2EE™ application servers and databases.

► A *High Availability Clustered Multiprocessor* (HACMP™) configuration monitors customers' IBM @server pSeries® servers and network connections. It performs application failover onto backup servers as necessary.

► *Partition Load Manager* (PLM) allows the system administrator to dynamically allocate processor and memory resources among logical partitions (LPARs) on a pSeries Power5 system without manual intervention.

► *Entity Analytic Server* (EAS) analyzes shipping files and displays any risk relationships that match those in the database.

► *WebSphere Application Server* offers an infrastructure for open e-business platforms. It provides an application deployment environment, including capabilities for transaction management, security, clustering, performance, availability, connectivity, and scalability.

The intent of this IBM Redbook is to provide a framework for building your own similar system, using some or all of the components and suggestions included herein.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Poughkeepsie Center.

Amarjit S. Bahl is an IBM Certified IT Architect and a Certified Project Management Professional (PMP). He has been working at IBM for approximately five years and has filed three patents and published various technical papers on grid and distributed technologies. His areas of expertise are application architecture, application design and implementation. He has worked in various technologies and products including SAP, WebSphere, Tivoli® and DB2®. He started his IBM career in the Webahead lab, which is an applied research powerhouse of knowledge and innovation based in Southbury, CT. He worked on projects which showcase the commitment of IBM to emerging technologies like intraGrid, voiceGrid, IBM Community Tools, Web Services, etc. Presently he is working in the Center for Solution Integration, which is a part of the Design Center in Poughkeepsie, NY. Here he is involved in

designing and architecting business and infrastructure solutions, working with the industry and sector leaders to define reference architectures and building blocks.

Dave Champagne is an Advisory Software Engineer and z/OS® IT Specialist at the IBM STG Center for Solution Integration in Poughkeepsie, NY. He has 28 years of experience in mainframe operating systems, having worked as a MVS-OS/390-z/OS Systems Programmer and Team Lead in a myriad of product development, test, and service organizations, complemented by several years spent as the z/OS Base Lead Planner. In his current assignment, Dave works to build, validate, and document the functionality, reliability, and performance of prototype multi-platform solutions for the marketing and software development community.

Jenny Li is a Certified IT Architect with the Center for Solution Integration (CSI) team in Poughkeepsie, NY. She has worked at IBM for nine years. Her areas of expertise include enterprise solution research, application architecture for on demand e-business, and enterprise architecture and strategy.

Kenneth Muckenhaupt is a Senior Software Engineer and Certified IT Specialist at the IBM STG Center for Solution Integration and has 28 years experience in IBM hardware and software development. His past assignments include microcode development on IBM mainframe processors, management of a microcode development department, technical leadership for the introduction of object-oriented technology on OS/390®, a three year assignment in the development and test of IBM Component Broker on OS/390, and his recent assignment as a Consultant at the IBM Design Center for e-business on demand™, where he is responsible for leading the design and development of industry solutions that focus on cross-platform, e-business on demand applications utilizing grid technology and services oriented architecture.

Virasay Savath is a Senior Consulting IT Architect at IBM Poughkeepsie, NY. He has 27 years of experiences in both hardware servers development and software solutions for industry solutions. Prior to joining the UNIX® Software Services team within IBM, he worked with IBM Business Partners and network equipment providers related to telecommunications. His current area of expertise includes server cluster solutions for disaster recovery running on AIX® and Linux®.

Acknowledgements

- ▶ **Maria Jenny (STG Marketing)** - our Offering Manager who will bring our work to "market"!
- ▶ **Hungtack Kwan (GSC)** for his technical expertise and guidance in setting up our environment
- ▶ **Bob Maher (STG pSeries Benchmark)** for always being there when we needed AIX technical support and expertise including PLM
- ▶ **Krista Morris (STG Center for Solutions Integration)** for unfailing enthusiasm and superb project management
- ▶ **John Mullin (STG zSeries® Benchmark)** for providing workload generator education (twice) and scripting expertise for testing
- ▶ **Rajesh Ramachandran (STG Design Center)** for timely assistance in getting pSeries products to talk to DB2 for z/OS
- ▶ **Bart Tague (STG Design Center)** for developing test servlets that enabled us to execute our integration tests

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

> **ibm.com**/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our Redbooks™ to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- ▶ Use the online **Contact us** review redbook form found at:

    ibm.com/redbooks

- ▶ Send your comments in an email to:

    redbook@us.ibm.com

- ▶ Mail your comments to:

    IBM Corporation, International Technical Support Organization
    Dept. HYJ Mail Station P099
    2455 South Road
    Poughkeepsie, NY 12601-5400

1

Integrated Border Management: Overview

This chapter provides a problem description and solution overview for government customers faced with the challenges of international trade. We discuss the priorities and architecture, management building blocks, proof of concept, and component interactions for Integrated Border Management.

1

Solution industry

Integrated Border Management is one of IBM's Selected Business Solutions (SBS) for the Government Industry; specifically, Customs, Ports and Border Management Solutions (ISA Code PG70). The target customers for Integrated Border Management include central government border management and immigration agencies, regional or local port authorities, border police and local law enforcement, national intelligence, agriculture, health, trade regulatory, and central government customs agencies worldwide.

Problem description

In a post 9/11 environment, government customers worldwide are faced with the challenge of optimizing the flow of international trade and travel while ensuring national security and border integrity. High priorities are to enhance security and ease the burden of compliance while promoting legitimate commerce and authorized border passage. Key government customers' pain points include the need for vigilance and collaboration, the need for embedded security measures, and for efficiency in existing security processes.

Integrated Border Management Reference Architecture

The Integrated Border Management Reference Architecture provides a resilient, adaptive, and integrated IT infrastructure framework for risk management. With this framework, government IT organizations can develop comprehensive border management applications that enable border agents and security personnel to derive non-obvious information about passengers and cargo.

Integrated Border Management Proof of Concept

To test an implementation of the Integrated Border Management Reference Architecture, the IBM STG Center for Solution Integration conducted a Proof of Concept (PoC) that addressed certain architectural components described in the Integrated Border Management Reference Architecture. Figure 1-1 shows this architecture with keys to identify those architectural components that the Center for Solution Integration implemented for the PoC.
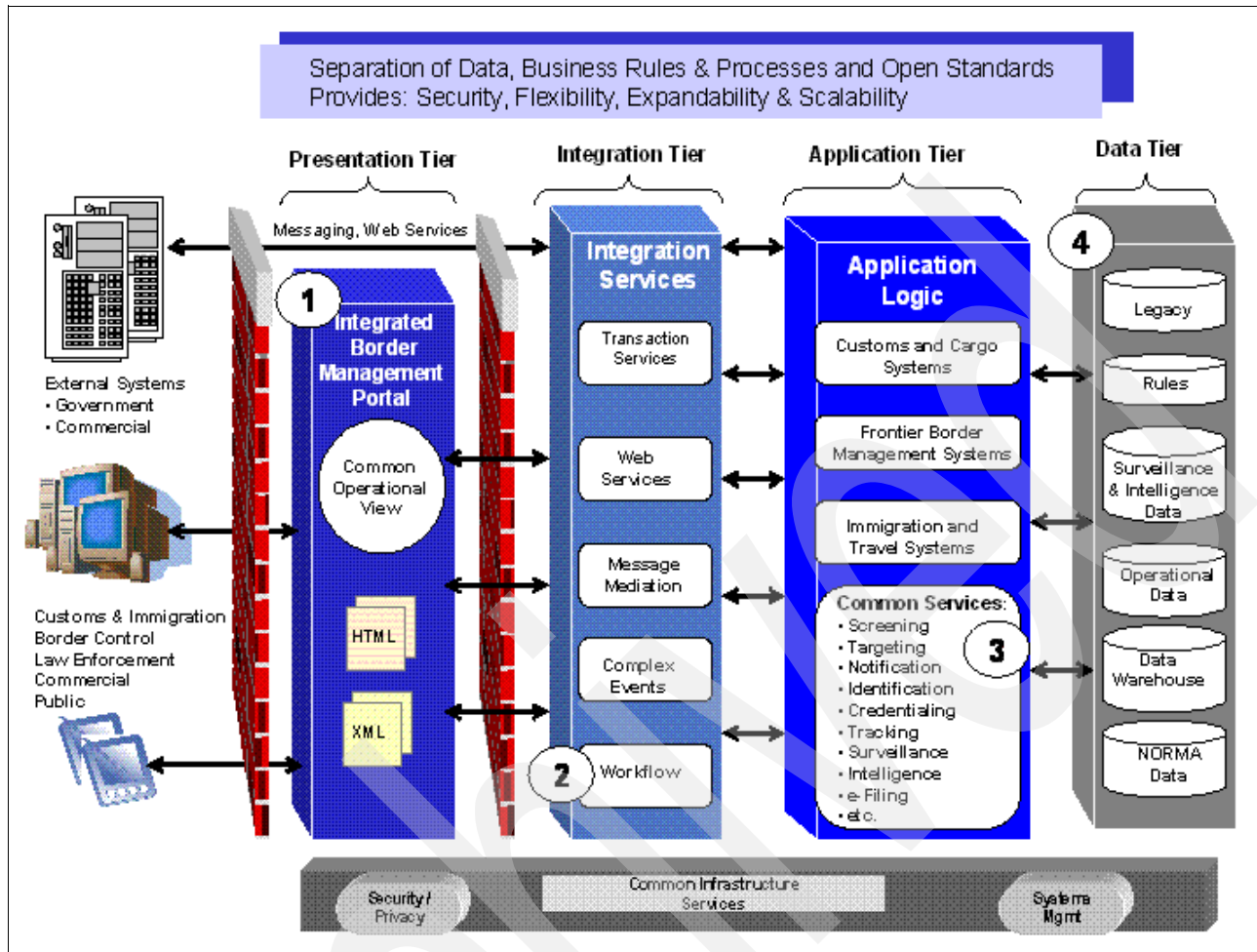
Figure 1-1   Integrated Border Management Reference Architecture

1. Presentation Tier: The PoC development team implemented this tier with WebSphere Portal. Its function was to accept inbound requests from simulated border agents and forward those requests to the Integration Tier.

2. Integration Tier: WebSphere Business Integration Server Foundation provided workflow management for requests received from the Presentation Tier. For the PoC, the development team implemented only the workflow component.

3. Application Tier: The PoC focused on the common services of passenger screening, identification, and screening by implementing a cluster of rules engines to analyze passenger manifest data and risky flight information. This tier logged its result in a database defined in the Data Tier and posted a risk score to the Presentation Tier.

4. Data Tier: This tier contained defined rules and operational databases to support the PoC.

Passenger Risk Management Building Block

Based on the Integrated Border Management Reference Architecture and the architectural components identified for the PoC, the Center for Solution Integration design team specified middleware and application software components that comprise an *Integrated Border Management Passenger Risk Management Building Block*. As a building block, this

aggregation of components can support a larger set of components (hardware and software) that encompass an entire border management infrastructure. This document describes the installation and configuration of these building block components and is intended for IBM Field Technical Specialists who must implement complete IT solutions for managing passenger transit through borders, cargo tracking at ports, and container tracking through secure trade lanes and overland transport. Specifically, the integration of the components described in this document also addresses the following non-functional requirements identified by the IBM Enterprise Business Consulting Service Public Sector:

- Capacity management during peak workloads
  - Use of Partition Load Manager (PLM)
- Process flexibility (Process Integration)
  - Ease of Rules update (see completed Test Plan)
- Availability (Business Continuity)
  - Use of High Availability Clustered MultiProcessor (HACMP)

Required skills

To install, configure, and support the infrastructure solution building block described in this document, the following skills are required:

- Design skills
  - J2EE
  - SOA
  - BPEL and workflow design
  - Business rules policy design
- Hardware management skills
  - IBM @server pSeries Model 590 systems management
  - AIX 5.3 systems management
  - AIX partitioning and Partition Load Manager (PLM) policy definition
  - JS20 BladeCenter® installation and configuration
  - AIX clustering definition with HACMP
  - Cisco network definition
  - SAN and SAN volume controller configuration
  - IBM @server zSeries systems management
- Middleware skills
  - WebSphere Application Server installation and configuration
  - WebSphere Business Integrator Server Foundation installation and configuration
  - WebSphere Portal Server installation and configuration
  - Tivoli Access Manager and Tivoli Identity Manager installation and configuration
  - Security policy definition
  - DB2 for z/OS installation, configuration, and database management

- Applications software
  - ILOG JRules or similar rules server installation and configuration
  - DB2 Relationship Resolution installation and configuration
    - Entity analytics, data mining, and information integration
  - Java™ and J2EE programming
  - XML
  - BPEL

Component interaction scenario

Figure 1-2 illustrates the component interaction scenario that the Center for Solution Integration team used to test the PoC.
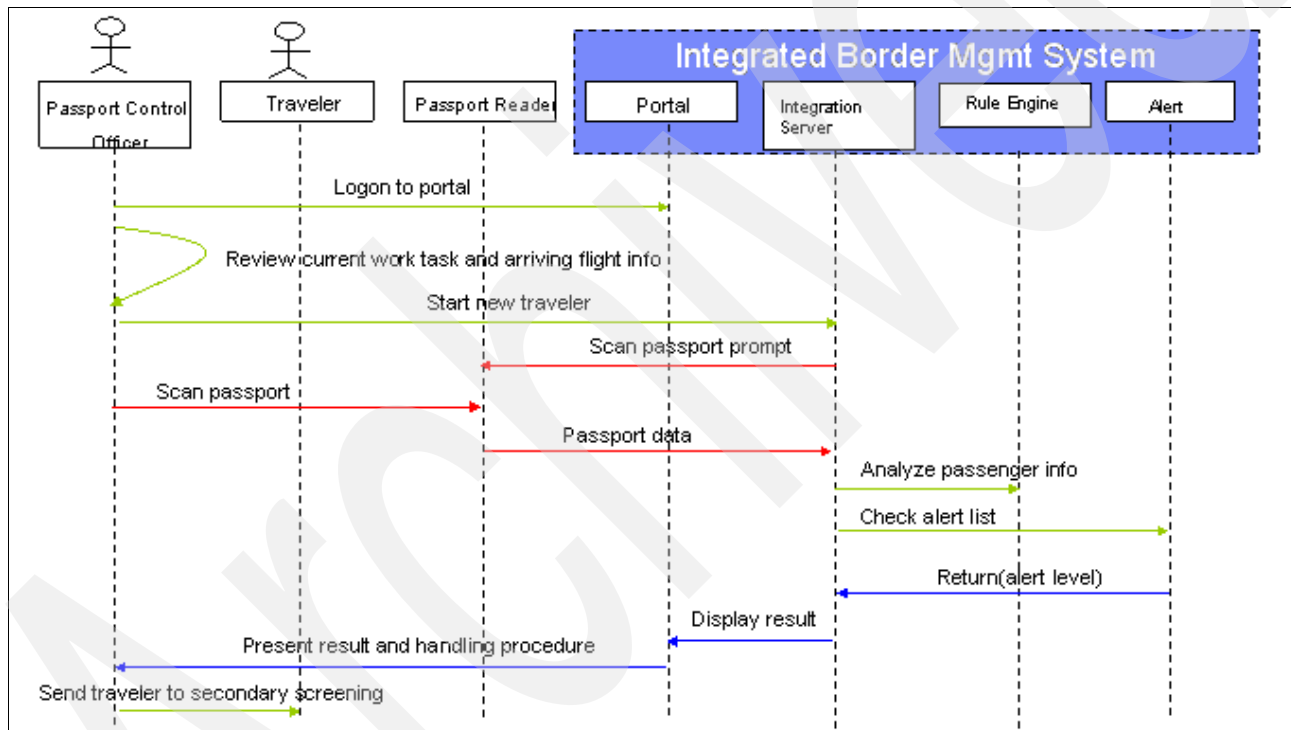
Figure 1-2   Integrated Border Management PoC Component Interaction Diagram

In typical border management scenarios, the Passenger Manifest (PAX List) is actually sent by the flight carriers to the destination country of the flight. The result is delivered to a Passport Control Officer who is on duty at the destination country and the officer determines if any action needs to be taken. Transactions are initiated from a Border Operations Specialist who accesses the system through a Web portal.

For the PoC, the Border Operations Specialist's actions are simulated through a workload generator script that submits a flight manifest file to the Presentation Tier. In turn, the Presentation Tier forwards the flight manifest to the Integration Tier (Integration Server) where a workflow process directs the manifest to the rules engine for risk analysis and scoring. The rules engine produces a risk score that is returned to the originating Border Operations Specialist's portal display and is also recorded in an operational database.

Separately, flight manifest xml can also be submitted to the Entity Analytic Server, where Relationship Resolution analysis can highlight individual passenger data conflicts based on the total amount of cumulative comparison information already resident on the server: passenger names, addresses, or social security or passport ID numbers, for example. The Entity Analytic Server takes input from multiple data sources from private sectors as well as other Government agencies (visa application data, criminal data, customs data declarations, manifests, prior violations, registered trading companies, etc.). This server then correlates this information to discover and illustrate non-obvious relationships with multiple degrees of separations. Results are displayed graphically for further analysis and research at the originating Border Operations Specialist's location.

Component interaction

Figure 1-3 is a component interaction diagram that shows the relationship of the PoC hardware and software components used to implement the Integrated Border Management reference Architecture PoC.
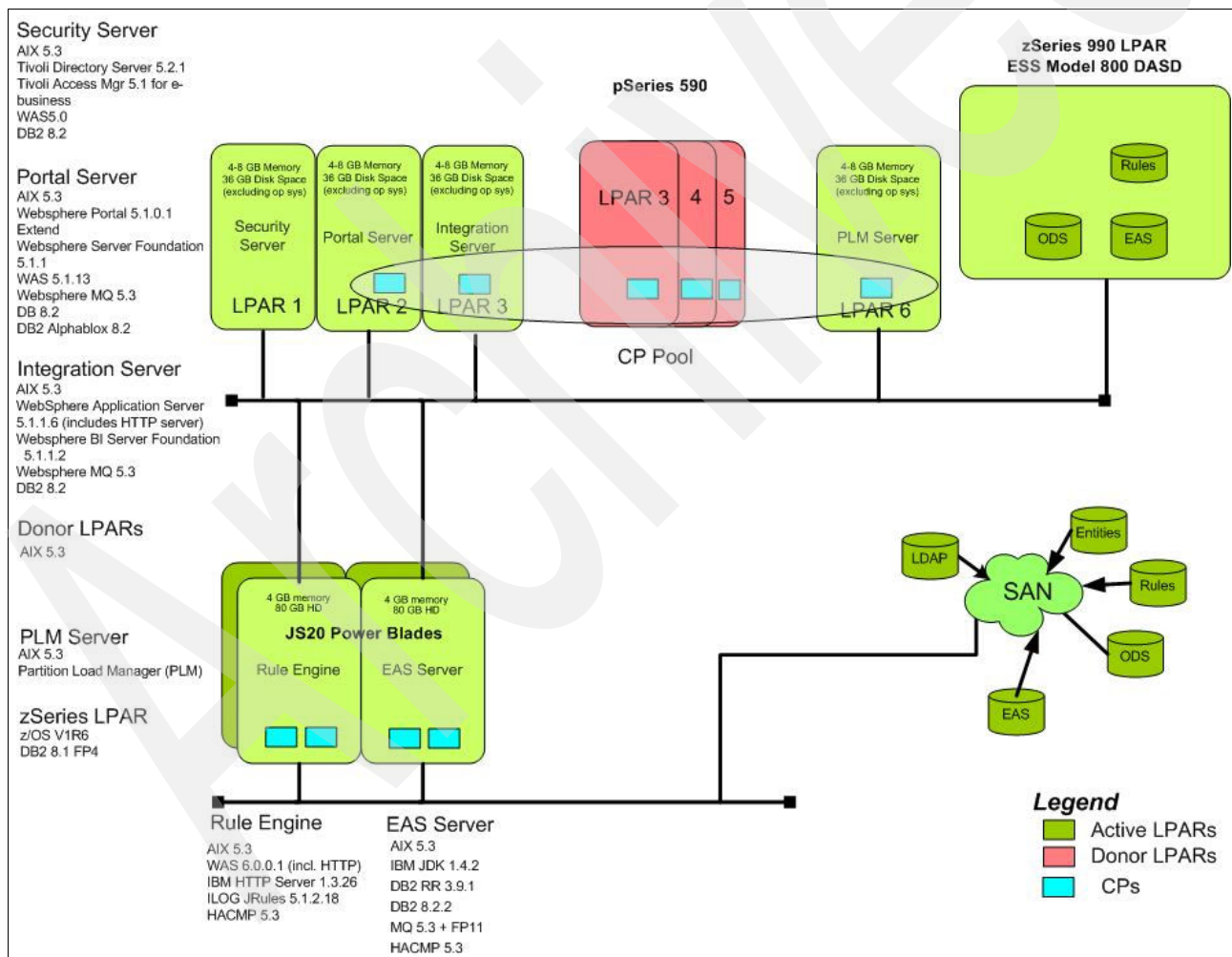
Figure 1-3   Component interaction diagram

To test the component interaction scenario, the PoC design and development defined the following servers:

- **Security Server:** This server performs user authentication operations and controls user access to the Web-based applications running on the Portal Server. It can be configured to flow an identity to the Integration Server.

- **Portal Server:** This server provides client browser-based access to the border management passenger risk applications. Input to this server is a normal HTTP/HTTPS request. The output of this server is a request message that is forwarded to the Integration Server. Specifically, no data is processed or stored at this server.

- **Integration Server:** The Integration Server enables services composition by supporting a process or workflow within the system. The workflow is a sequence of tasks that describes an input to the process (which is the passenger manifest information), how the information flows within the system once it receives the input, and the output of the process. For the PoC, the development team wrote the workflow description in Business Process Execution Language (BPEL) and defined each task within the process as a Web service that can be invoked by a remote process call. To leverage WebSphere Business Integration Server Foundation's process choreography feature, a business process container acts as the process choreography engine within a WebSphere Application Server. The BPEL used during the PoC drives a request to the rules server.

- **Partition Load Manager:** Partition Load Manager (PLM) allows the system administrator to dynamically divide processor and memory resources between logical partitions (LPARs) on a Power5 pSeries system without manual intervention. The allocation of these resources is based on workloads and policies defined by the system administrator. Typically, PLM is set up in a partition or on another system running AIX 5L™ Version 5.2 or 5.3. The PLM server uses a policy file to determine how CPU and memory resources are shared across LPARs. The policy also includes resource shares, group definitions, and tunable parameters. This file defines the managed partitions, their guaranteed entitlements, and their minimum and maximum entitlements. For the PoC, the development team defined PLM policy that directed the PLM server to allocate CPU resources from the Portal Server and three donor LPARs and add them to the Integration Server during periods of peak work load.

- **Rules Server:** The Rules Engine is responsible for analyzing a passenger or set of passengers scheduled on a particular flight. For the PoC, the development team implemented a set of rules that analyzed a passenger manifest against a list of known risky flights. The team used ILOG JRules Rules Builder to create the business rules and deployed them to a JRules Business Rules Execution Server (BRES) running on a cluster of JS20 Blade Servers. The rules application itself was exposed as a Web service that was called by the BPEL executing in the Integration Server. To simulate periods of heavy passenger activity through an airline checkpoint, the integration test team wrote a workload generator script[1] that repeatedly drove requests into the Integration Server. These requests were forwarded to the rules engine through a Web services interface. To ensure the high availability required by border management applications, the test team defined a High Availability Clustered Multiprocessor (HACMP) environment for the rules engine blade servers. Two blades comprised this HACMP cluster with one blade acting as the master server and the other as the backup.

- **Entity Analytic Server:** For Integrated Border Management applications, the Entity Analytic Server discovers relationships between data elements stored across multiple, discrete databases. DB2 Relationship Resolution V3.9.1 is the IBM product used during this PoC. A typical passenger risk management application uses relationship resolution, or entity analytics, to determine the identity of a suspicious traveller. For example, if a certain passenger's personal information is stored in several governmental databases, border agents can use entity analytics to scan those databases based on input criteria to determine if a traveller is known by any aliases or if the passenger's visa number appears

---

[1] Read about Mercury LoadRunner at http://www.mercury.com/us/products/performance-center/loadrunner/

under different names. Additionally, correlation of available information can discover and illustrate non-obvious relationships with multiple degrees of separation.

- **Storage:** The PoC infrastructure supports two storage environments:
  - A DB2 database on z/OS which is used to store passenger risk scores, rules definitions, and Entity Analytic Server user-ID and password information. The use of DB2 on z/OS is not required for all border management implementations; but typically, government border agencies select z/OS for its reliability and availability.
  - A Storage Area Network (SAN), which the PoC development team used to store HACMP heartbeat information. Additionally, the solution implementors can extend the SAN to support the Security Server's LDAP database, the Entity Analytics database, EAS operational data, and the Rules Engine database.

Solution hardware profile

Table 1-1 lists each server and its associated hardware. The memory and CPU values specified in this list are those used by the PoC development team to build the infrastructure depicted in Figure 1-3. Since this hardware list is part of an infrastructure building block, it should be extended to support individual border management solutions.

Table 1-1   Hardware specifications

Server	Hardware
Security Server	pSeries 590 LPAR 1CPU 4-8 GB Memory 36 GB Disk Space (excludes Operating System)
Portal Server	pSeries 590 LPAR 1 CPU 4-8 GB Memory 36 GB Disk Space (excludes Operating System)
Integration Server	pSeries 590 LPAR 1 CPU 4-8 GB Memory 36 GB Disk Space (excludes Operating System)
Donor LPAR #1	pSeries 590 LPAR 1 CPU 4 GB Memory 36 GB Disk Space (excludes Operating System)
Donor LPAR #2	pSeries 590 LPAR 1 CPU 4 GB Memory 36 GB Disk Space (excludes Operating System)
Donor LPAR #3	pSeries 590 LPAR 1 CPU 4 GB Memory 36 GB Disk Space (excludes Operating System)
Partition Load Manager (PLM) Server	pSeries 590 LPAR 1 CPU 4 GB Memory 36 GB Disk Space (excludes Operating System)

Server	Hardware
Rules Engine	JS20 Power Blade 2 CPUs 4 GB Memory 80 GB Disk Space
Rules Engine - HACMP Failover	JS20 Power Blade 2 CPUs 4 GB Memory 80 GB Disk Space
EAS Server	JS20 Power Blade 2 CPUs 4 GB Memory 80 GB Disk Space
EAS Server - HACMP Failover	JS20 Power Blade 2 CPUs 4 GB Memory 80 GB Disk Space
Database Server	zSeries 990 (z990) LPAR 4 Shared CPUs 2 GB Memory
Load Generator	HS20 Power Blade 1 - 2.8 GHz CPU 1 GB Memory 40 GB Disk Space

DISCLAIMER: Any server names or IP addresses appearing in this document were used in the prototype solution detailed herein. These identifiers are to be treated as examples only.

2

Portal Server installation and configuration

WebSphere Portal consists of middleware applications, called portlets, and development tools for building and managing secure business-to-business, business-to-customer, and business-to-employee portals.

WebSphere Portal for Multiplatforms includes two offerings: *Portal Enable* is the base offering and provides personalization, Web content management, document management, productivity functions along with the scalable portal framework. *Portal Extend* adds powerful collaborative, extended search, and Web analysis features to enhance portal effectiveness.

Product description

A portal is a Web site that provides users with a single point of access to Web-based resources by aggregating those resources in one place and by requiring that users log in only to the portal itself, rather than into each portlet they use.

As an administrator, you can customize WebSphere Portal to meet the needs of your organization, users, and user groups. You can adapt the look and feel of the portal to fit the standards of your organization and to customize page content for users and groups in accordance with business rules and user profiles. Users can further customize their own views of the portal. They can also add portlets to pages and arrange them as desired, and control portlet color schemes. By aggregating portlets in one place and giving users the power to customize their own desktops, WebSphere Portal gives users a means for doing business efficiently and with high satisfaction.

Portlets are central to WebSphere Portal. As special reusable Java servlets that appear as defined regions on portal pages, portlets provide access to many different applications, services, and Web content. WebSphere Portal ships a rich set of standard portlets, including portlets for displaying syndicated content, transforming XML, and accessing search engines and Web pages. Portlets for accessing Lotus® Notes®, Microsoft® Exchange, and instant messaging are also included. Several third-party portlets are also available, including Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM). WebSphere Portal also ships an API that developers can use to create custom portlets.

Server definition

The Portal Server provides client browser-based access to the Border Management Passenger Risk applications. Input to this server is normal HTTP/HTTPS requests. The output of this server is a request message that is forwarded to the Integration Server. Specifically, no data is processed or stored at this server.

Server hardware

- IBM @server® pSeries 590
- 4-8 GB Memory
- 36 GB Disk Space

Server software stack

- AIX 5.3
- WebSphere Portal 5.1.0.1 Extend
- WebSphere Server Foundation 5.1.1
- WebSphere Application Server 5.1.13
- WebSphere MQ 5.3
- DB2 8.2

Reference to product installation information

Refer to the installation document in the /documentation/pdf/Install.pdf and the Information Center at:

http://publib.boulder.ibm.com/infocenter/wpdoc/v510/index.jsp

Installation of the portal server

Download the portal server install files to a temporary directory. The files are available in .taz format.

To uncompress the .taz files do the following:

1. mv File.taz File.tar.Z

2. Uncompress File.tar.Z

```
tar xvf File.tar
```

You can also try to use this command:

```
tar Zxf file.tar
```

If the format of the downloaded file is tar.gz:

To uncompress tar.gz files:

```
gunzip —c ese.dbcs.tar.gz | tar xvf —
```

Where:

- -c = output the results
- | = pipe the results
- tar = pipe to tar format
- - = output

In this chapter, we install the WebSphere Portal with WebSphere Application Server and Cloudscape™ database installed locally. See Figure 2-1 on page 14. This scenario focuses on installing and configuring WebSphere Portal only with no options. After you have successfully installed and configured WebSphere Portal, you can add on to it.

Start to execute the setup file.

```
./install.sh
```

Accept the agreement (Figure 2-1 on page 14). Click **Next**.
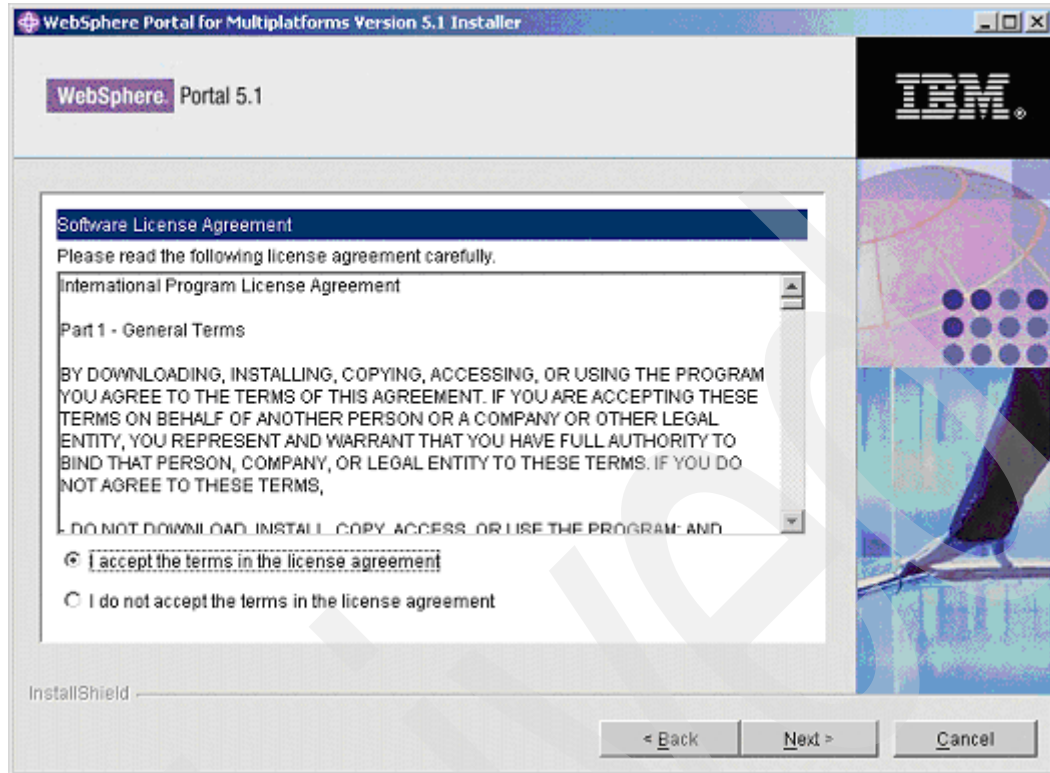
Figure 2-1   Accepting the agreement

The installation program checks the machine for operating system and software prerequisites.

Select **Full install** and click **Next**. See Figure 2-2 on page 15.
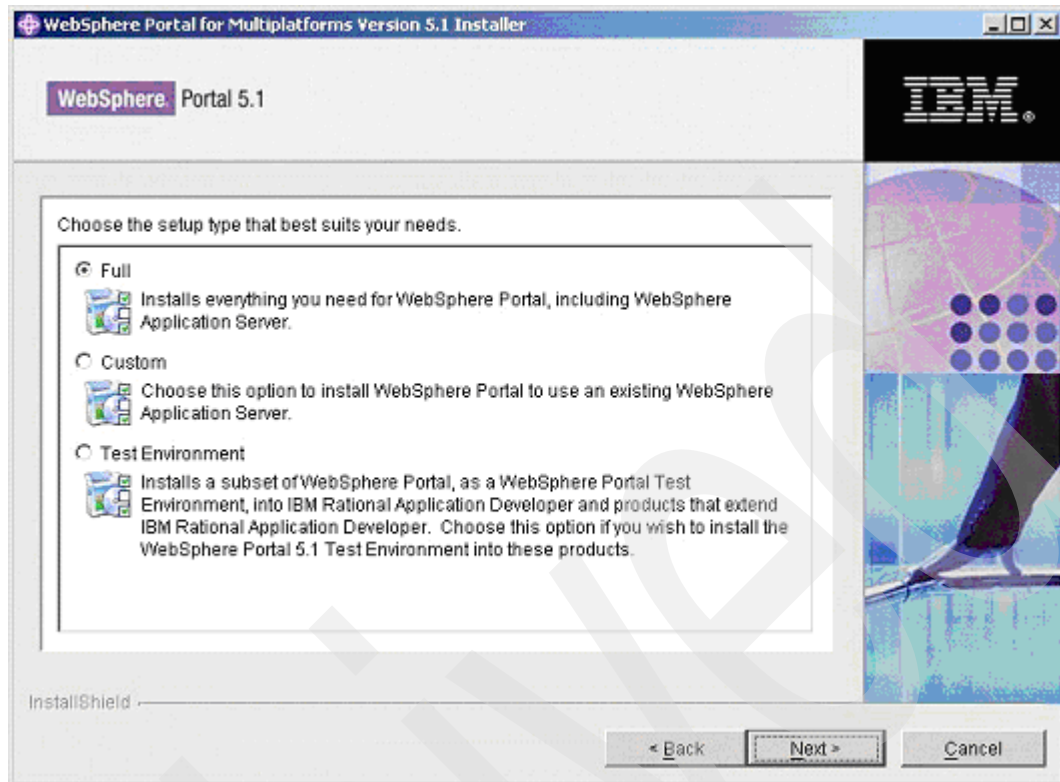
Figure 2-2   Selecting a full install

Enter the directory where you want to install WebSphere Application Server. If the directory that you specify does not exist, it will be created.

Specify the following WebSphere Application Server information, and click Next:

1. The node within the WebSphere Application Server cell where you want the WebSphere Portal application server to be installed. This value must be unique among other node names in the same cell. Typically, this value is the same as the host name for the computer. In our case it was r14n12.pbm.ihost.com

2. The fully qualified host name or IP address of the computer that is running WebSphere Application Server.

Specify the directory where you want to install WebSphere Portal. If the directory that you specify does not exist, it will be created. Click **Next**.

Enter the user ID and password for the WebSphere Portal administrator.

Do not use blanks in either the user ID or the password, and ensure that the password is at least five characters in length. This user ID is used to access WebSphere Portal with administrator authority after installation. Note that this user ID is only used to log in to WebSphere Portal and is not related to any user IDs that are used to access the operating system itself. Click Next. In our case, we created the following:

- WebSphere Portal Admin user = wpadmin
- WebSphere Portal password = wppass

Verify the components to be installed and click **Next**.

The installation program begins installing the selected components. Throughout the installation and configuration process, the program displays progress indicators for the different components.

Note: A full installation, including WebSphere Application Server, can take some hours to complete. Use the progress indicators and the process monitoring facilities of your platform to monitor the overall progress of the installation. See Figure 2-3.
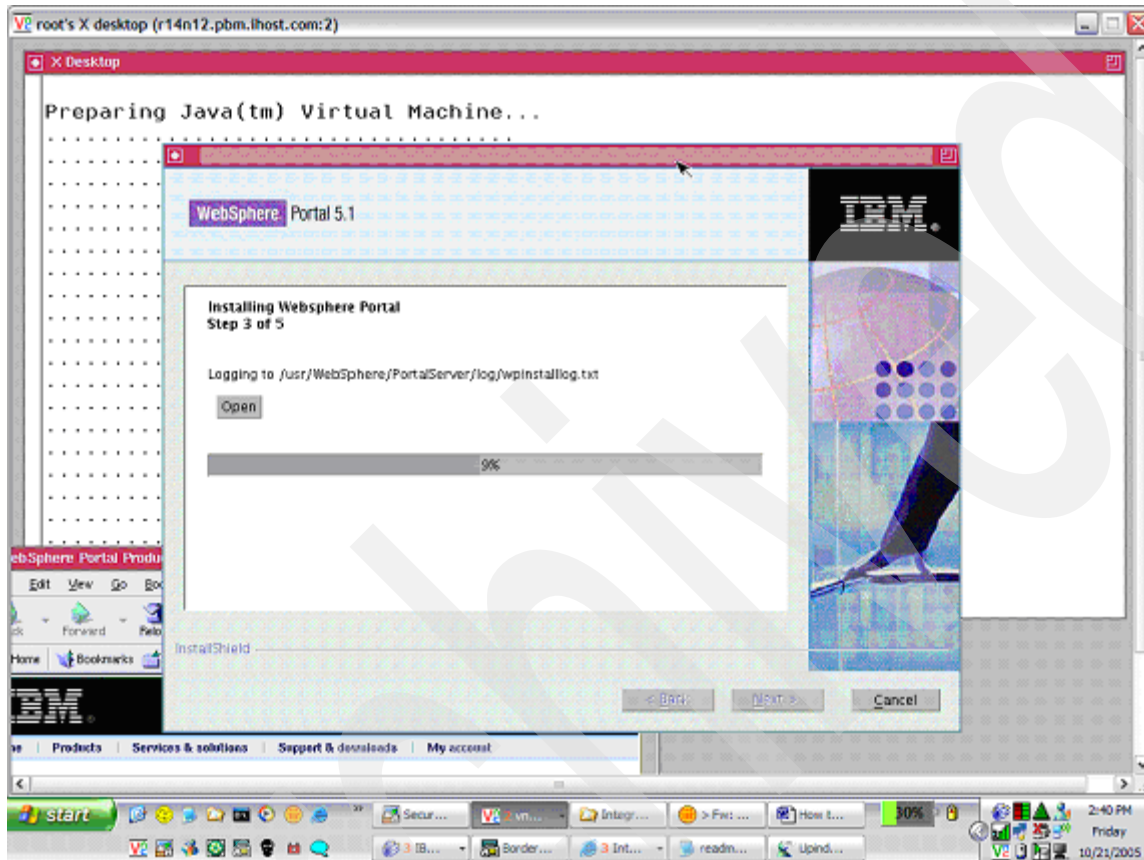
Figure 2-3   Progress indicators for the installation

When the installation is finished, the installation program displays a confirmation panel (Figure 2-4 on page 17) listing the components that have been installed.

Note the following information before clicking Finish:

1. The port number that is used to access WebSphere Portal is displayed on the confirmation panel.

2. Make a note of the port number for use in verifying the WebSphere Portal URL. This value is also stored in the WpsHostPort property in the *<wp_root>*/config/wpconfig.properties file.
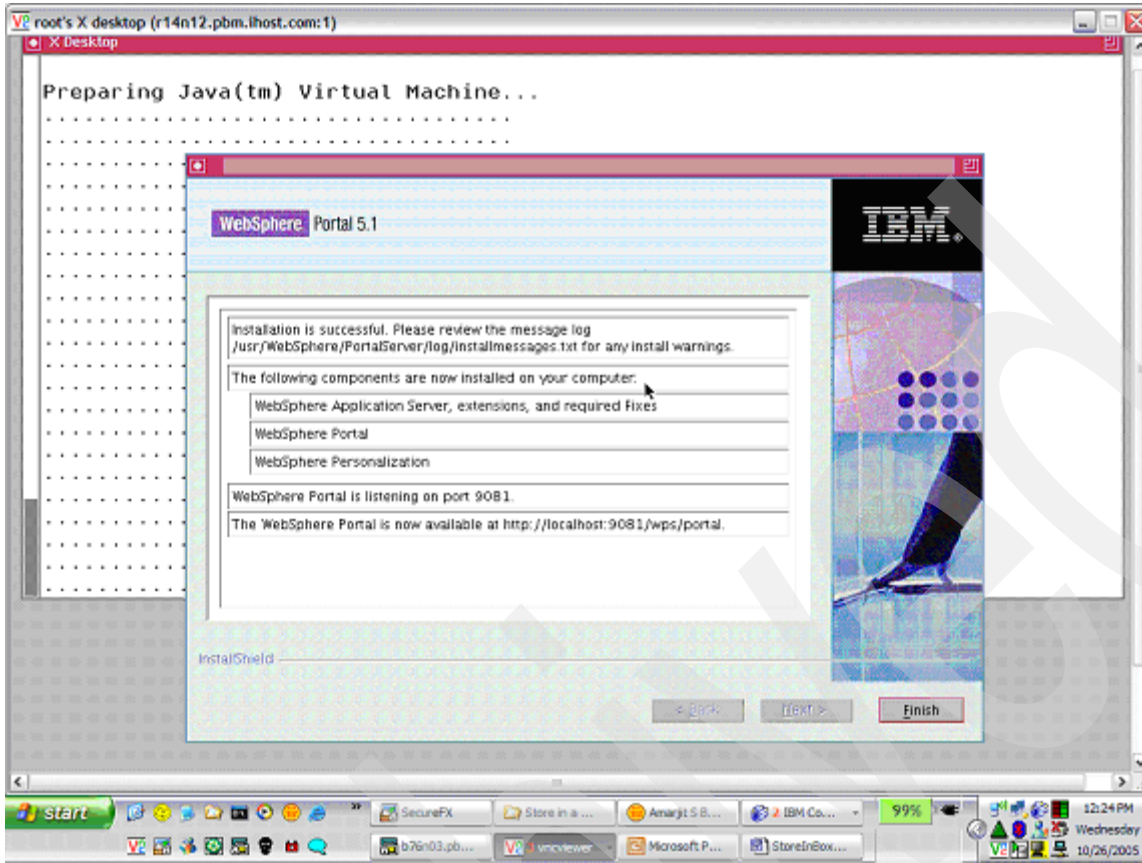
Figure 2-4   The confirmation panel

Click **Finish**.

To log into the portal, use the URL `http://r14n12.pbm.ihost.com:9081/wps/portal/`. This will bring up a Web page that looks like Figure 2-5.
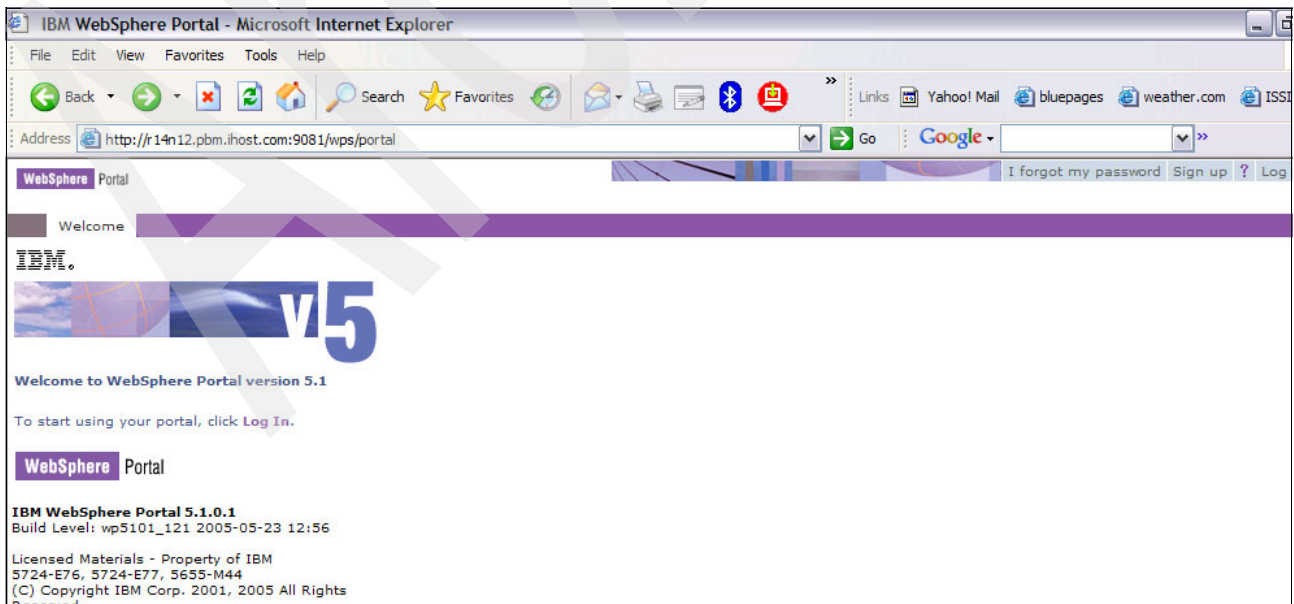
Figure 2-5   Entering the portal

Enter the following information to log on:

    a. User name = wpuser

    b. Password = wpassword

To add a database with greater capability, install DB2, which was not installed with the previous install.

Follow the document on how to install DB2 graphically. Here we explain the IDs that are required and were created for our installation.

1. Create a new user, define group name and home directory (Figure 2-6)

    a. username = dasusr2

    b. password = dasusr2
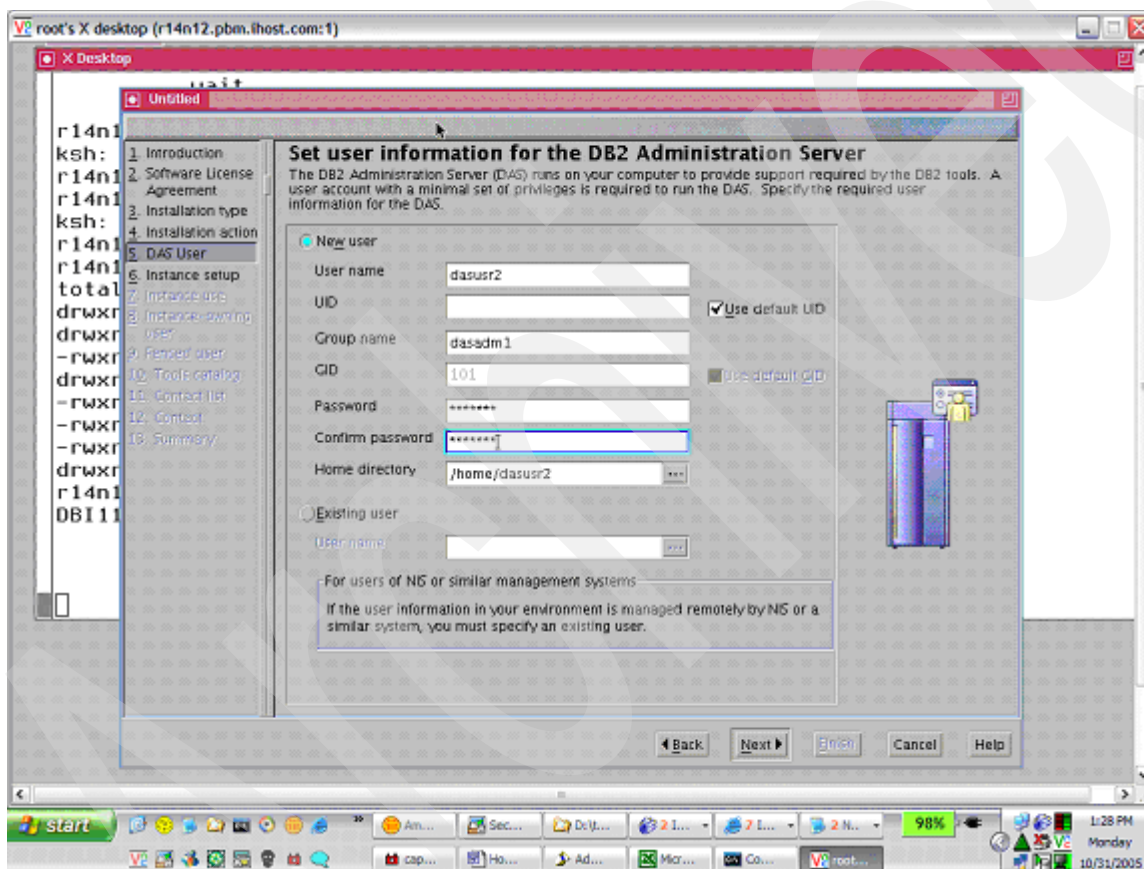
Figure 2-6   Creating a user ID

2. Create DB2 instance (Figure 2-7 on page 19)

    a. user = db2inst2

    b. password = db2inst2
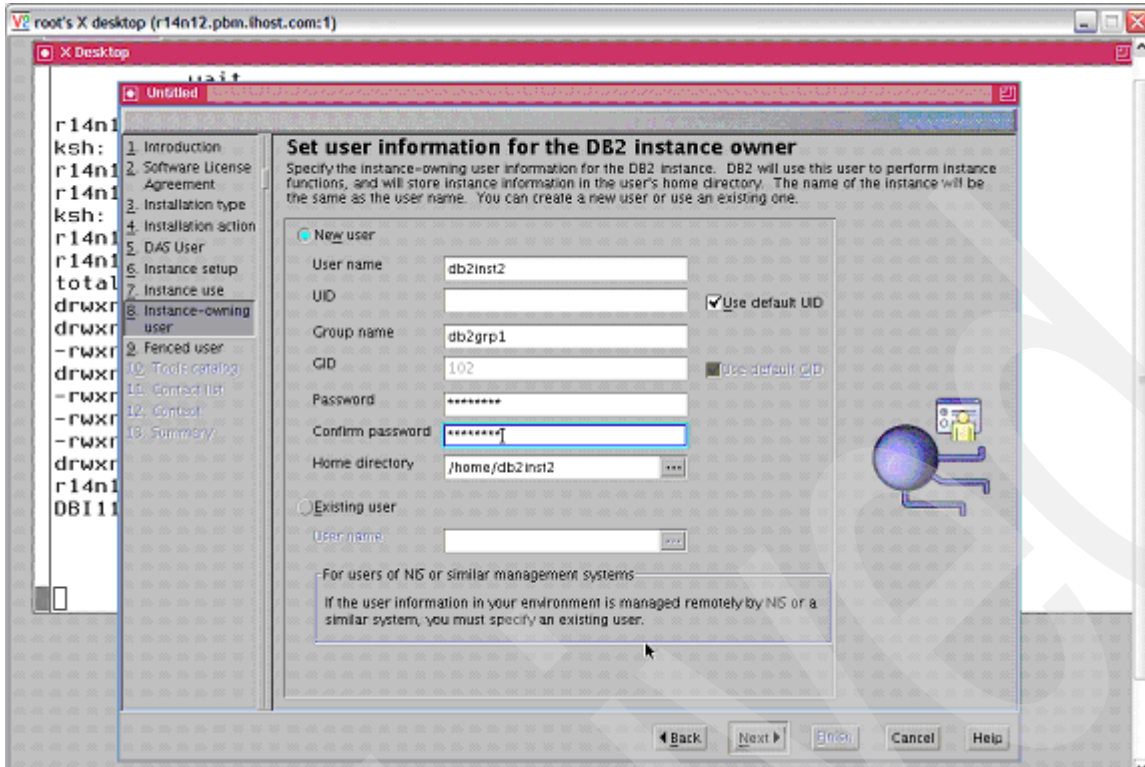
Figure 2-7   Creating a DB2 instance

3. Create DB2 fence user (Figure 2-8)

   a. user = db2fenc2

   b. password = db2fenc2
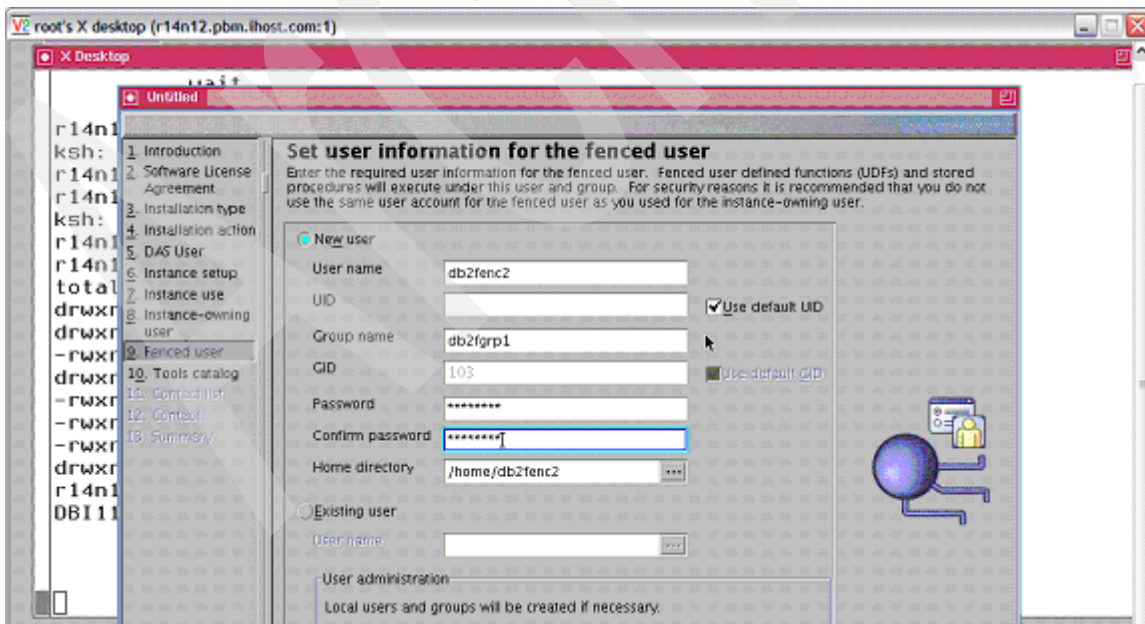
Figure 2-8   Creating a DB2 fenced user

☐ **To create databases and users for DB2 refer to the document:**

`http://publib.boulder.ibm.com/infocenter/wpdoc/v510/index.jsp?topic=/com.ibm.wp.ent.doc/wpf/setup_db2.html`

☐ **To configure the DB2 for the Portal Server refer to the document:**

`http://publib.boulder.ibm.com/infocenter/wpdoc/v510/index.jsp?topic=/com.ibm.wp.ent.doc/wpf/cfg_db2.html`

☐ **Verify the WebSphere Application Server install**

1. Log on to the WebSphere application server administrative console using the URL:

   `http://hostname:9090/admin`

2. Log on to the administrative console using the IDs:

   Username = wsadmin

   Password = wspassword
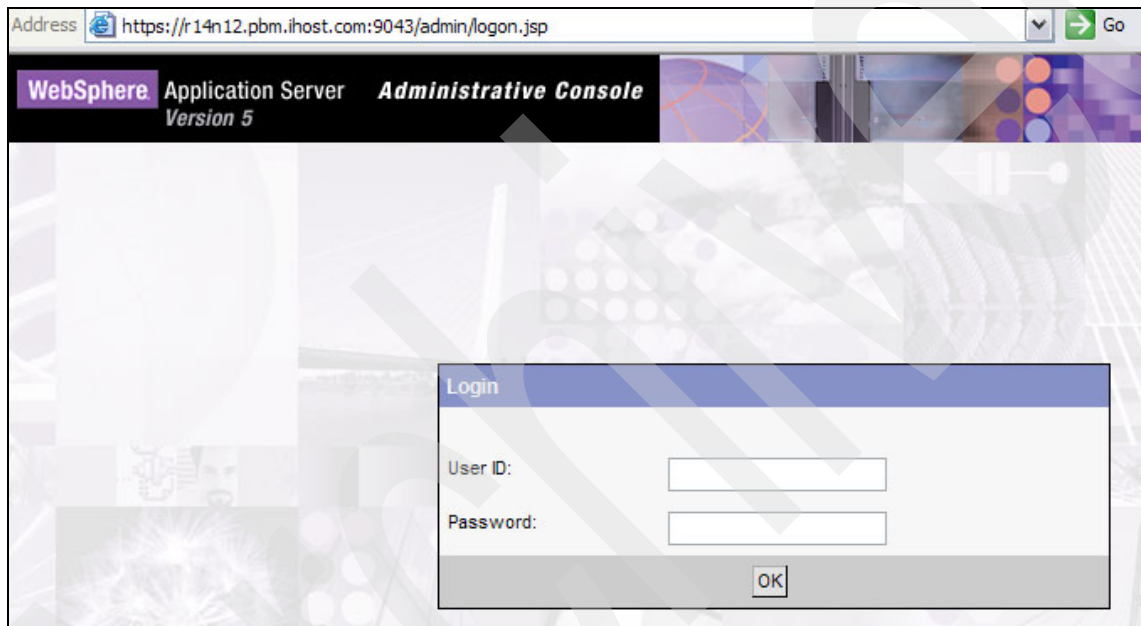
Figure 2-9   Logging on to the administrative console

3. Look at the Enterprise Applications under the Applications tab. See Figure 2-10 on page 21.
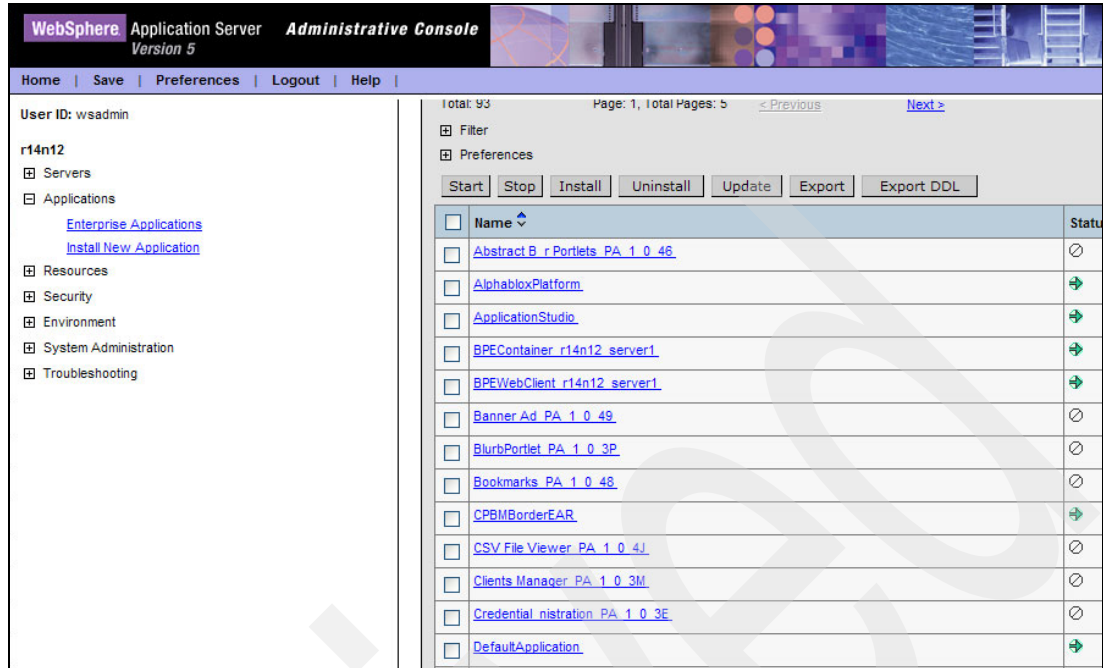
Figure 2-10   Enterprise applications

☐ **Verify the Portal Server install**

1. Log into the portal using the URL: `http://r14n12.pbm.ihost.com:9081/wps/portal`.

2. This will bring up a Web page that looks like Figure 2-11.

Figure 2-11   Logging onto the WebSphere portal

3. Click **Log in** . A window like Figure 2-12 on page 22 appears.

Chapter 2. Portal Server installation and configuration   **21**
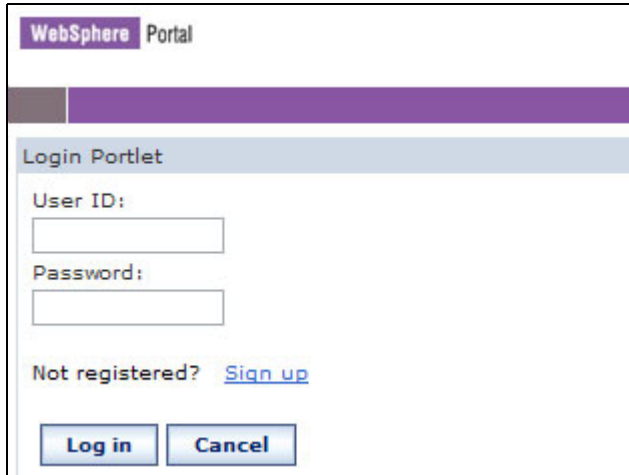
Figure 2-12   Entering your user ID and password

4. Enter the following information to logon:

   User ID = wpuser

   Password = wpassword

5. The portal server will deliver content that you can customize. The basic page looks like Figure 2-13.
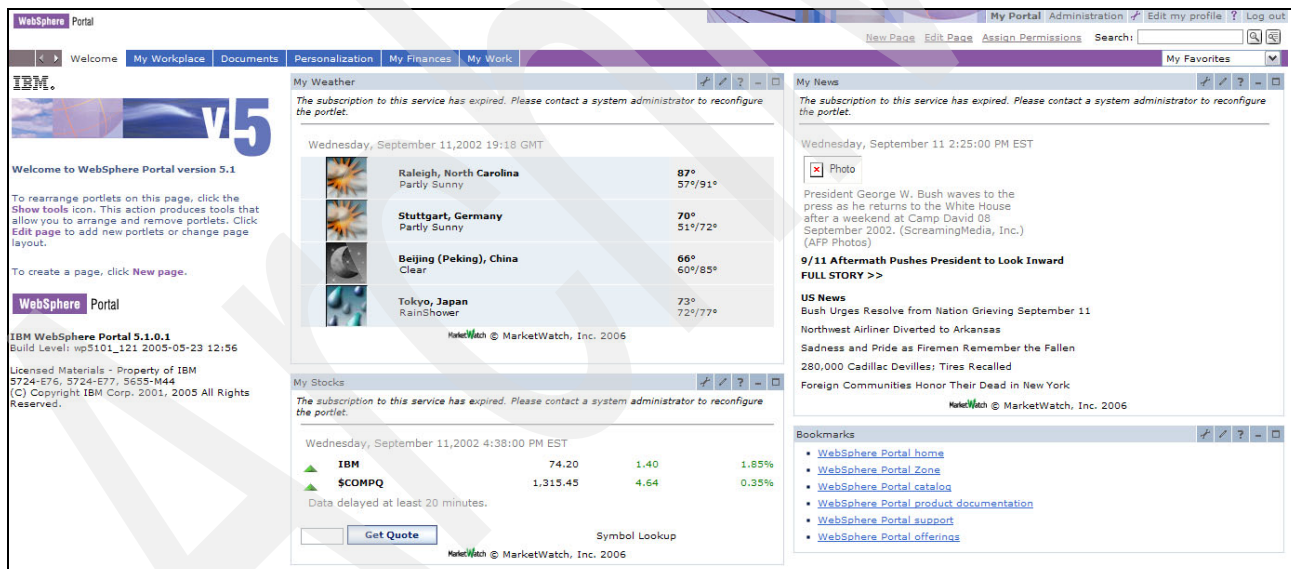
Figure 2-13   Basic portal server content

☐ **Verify the database connection**

1. Log on to the WebSphere application server administrative console as described above.

2. Click **Resources** → **JDBC™ Providers**

3. Select *wpsdbJDBC* . See lower right corner → of Figure 2-14 on page 23.

Figure 2-14   Verifying the connection

4. Select **Data Sources** from **Additional Properties**.

5. Check the data source that you want to test. See Figure 2-15 on page 24.

Figure 2-15   Selecting the data source to test

6. Click **Test Connection** to verify the database connection.

3

WebSphere Business Integration Server Foundation installation and configuration

WebSphere Business Integration Server Foundation (WBISF) lets businesses incorporate business flows or processes within their applications. For this project, WBISF is used in the Integration Server to provide workflow. This chapter lists the steps for installing DB2, WebSphere MQ, WebSphere Application Server, and WebSphere Business Integration Server Foundation.

Product description

WebSphere Business Integration Server Foundation (WBISF) V5.1.x builds on the WebSphere Application Server that supports service oriented architecture-based (SOA) solutions. It provides a J2EE and Web services environment that lets businesses incorporate business flows or processes within their applications, which can be composed of existing or new Web services; leveraging JMS, common event infrastructure or other technologies.

Server definition

For this Government Integrated Border Management project, WebSphere Business Integration Server Foundation is used in the Integration Server to provide an environment for services composition, basically a process or workflow within the system. The process here is a sequence of tasks that describes the input to the process (which is the passenger manifest information), how the information flows within the system once it receives the input, and the output of the process. The process is described in Business Process Execution Language (BPEL), while each task within the process can be defined as a Web service that can be invoked by remote process call (RPC) or other mechanism.

To leverage WebSphere Business Integration Server Foundation's process choreography feature, we have to configure a business process container after the product is installed. Basically, this is the process choreography engine within WebSphere Application Server.

Server hardware

- IBM @server pSeries p590 LPAR with one CPU, 4 GB RAM and 36 GB disk space excluding the operating system.

Server software stack

WebSphere Business Integration Server Foundation 5.1.1.2 requires the following software as prerequisites:

- AIX 5.2 maintenance level 1
- xlC.rte 6.0 run-time code on AIX 5.2 maintenance level 1
- Java 1.3.0
- WebSphere Application Server 5.1.1.6

In addition, the following software is installed as required by the business process container:

- DB2 ESE 8.2.3
- WebSphere MQ 5.3 with Fix Pack 4 or later

Reference to product installation information

The installation and configuration information provided here is a minimal set of information that helps you get started. For details of the WebSphere Business Integration Server Foundation installation and configuration, refer to the Information Center.

Task 0. Planning

☐ **System topology**

The topology for the Integrated Border Management Integration Server is a single server topology. It has the WebSphere Business Integration Server Foundation (WBISF in the diagram), WebSphere Application Server, HTTP Server, DB2, and MQ installed in a single physical node. See Figure 3-1. The Business Process Container is configured in the WebSphere Business Integration Server Foundation to point to DB2 for persistence and use MQ as an external JMS provider. The plugin.xml file is configured automatically during the installation to point to WebSphere Application Server.

Note that WebSphere Business Integration Server Foundation bundles an embedded WebSphere MQ which is a subset of the full version of the MQ product. However, in this setting, we would not use the internal embedded WebSphere MQ; instead, a full version of the MQ is used. Therefore, the WebSphere Business Integration Server Foundation listed here was installed without the embedded messaging feature.
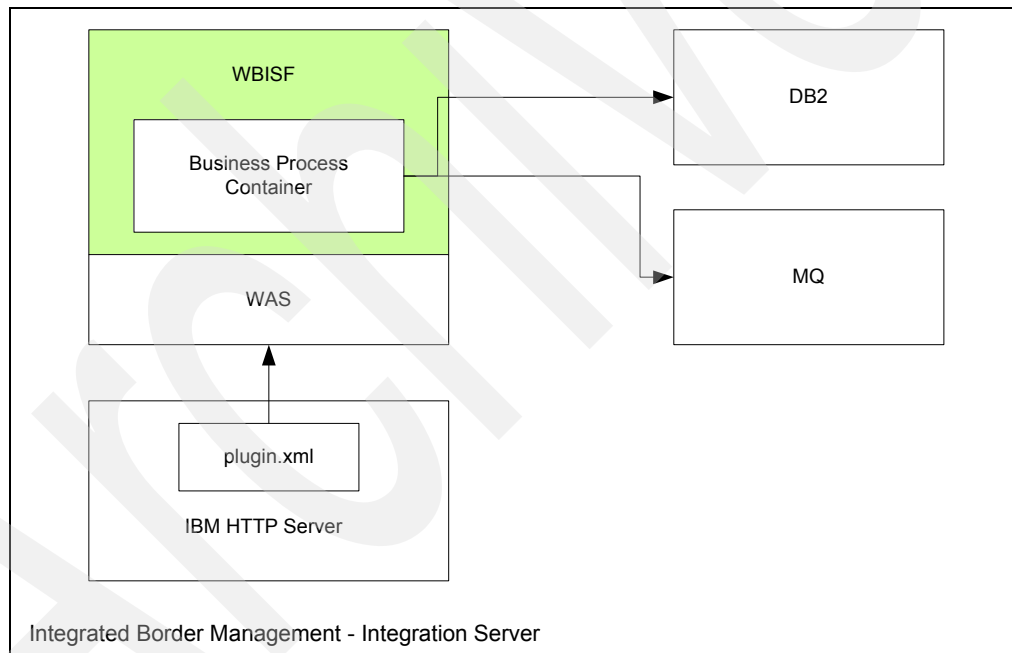
Figure 3-1   Integration server

☐ **Installation sequence**

1. Install DB2 8.1
2. Install DB2 Fix Pack 10
3. Install MQ 5.3
4. Install MQ Fix Pack 11
5. Install WebSphere Application Server 5.1
6. Install WebSphere Application Server Fix Pack 1 and Cumulative Fix Pack 6

7. Install WebSphere Business Integration Server Foundation 5.1 without the embedded message

8. Install the WebSphere Business Integration Server Foundation Fix Pack

☐ **Configuration sequence**

1. Configure WebSphere Application Server to point to MQ.

2. Configure the Business Process Container in the WebSphere Business Integration Server Foundation to point to DB2 for persistence and use an external MQ server (instead of the embedded messaging server) as a JMS server provider.

☐ **How to download WebSphere Business Integration Server Foundation installation bundle**

1. All of the base software that is mentioned in the Installation Sequence above (except the fix packs and cumulative fix packs) are packaged in the WebSphere Business Integration Server Foundation V5.1 e-assembly installation bundle that is available from the product CDs. The e-assembly bundle basically contains multiple components of WebSphere Business Integration Server Foundation V5.1 that are applicable to various operating systems. You should only download the filesets that are applicable for the AIX platform. Any fix packs or cumulative fixes are available from the external IBM product site at: http://www.ibm.com/products.

2. Before you download any fileset, it is important to create a temporary directory on the target AIX machine and give the directory a meaningful name. This is because it is impossible to identify the product you are trying to install from its installation file name. For example, the installation file for WebSphere Application Server 5.1 is called c53ilml.tar. It is important to create a temporary directory, for example "WebSphere Application Server 5.1", on the AIX machine for holding the installation file to avoid any confusion.

3. Remember that all the installation filesets are packaged in compress formats, such as, .tar, .Z, .gz. You will need to uncompress these files in the AIX machine later before the software installation. This will be discussed in detail in each product installation section.

☐ **Provide sufficient disk space**

For WebSphere Application Server, reserve 500 MB for the /tmp directory. During the installation of WebSphere Application Server, the /usr/WebSphere/AppServer directory will be created and it needs at least 1750 MB. For DB2, reserve 1290 MB and for MQ, reserve 55 MB for /usr/mqm (directory for base code) and 13 MB for /var/mqm (directory for base data).

☐ **Target installation paths**

WebSphere Business Integration Server Foundation and its required software will be installed in the default directories shown in Table 3-1. WebSphere Business Integration Server Foundation is installed on top of WebSphere Application Server, so the product code is incorporated under the WebSphere Application Server installation home directory.

Table 3-1   Default directories for WebSphere Business Integration Server Foundation

Software	Directory	Usage
DB2	/usr/opt/db2_08_01	product
DB2	/home/db2inst1	Data for DB2 instance
DB2	/home/dasusr1	Data for DAS user
DB2	/home/db2fenc1	Data for fenced user
WebSphere Application Server	/usr/WebSphere/AppServer	Product and data

HTTP	/usr/IBMHttpServer	Product and data
MQ	/usr/mqm	Base product
MQ	/var/mqm	Data

☐ **Installation prerequisite**

1. Install Java 1.3.0 (package Java130.rte.lib) on AIX. Java 1.3.0 is required by the embedded message feature of WebSphere Business Integration Server Foundation. To download Java130.rte.lib, go to:
   http://www-106.ibm.com/developerworks/java/jdk/aix/index.html, or search for the IBM Developer Kit for AIX if the link is unavailable. To check for the Java version, use this command: `java -version`

2. Install the prerequisite xlC.rte 6.0 runtime code on AIX. You can download the runtime code as a fix from the AIX Support Site at:
   http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp

   To check if xlC.rte is installed, use this command: `lslpp -l | grep xlC.rte`

```
r14n13:/scratch/WBISF511/WBISF_unzip # lslpp -l | grep xlC.rte
  xlC.rte                    7.0.0.0  COMMITTED  C Set ++ Runtime
```

Task 1. DB2 ESE 8.1 installation and configuration

☐ **Planning**

1. You must have root access to the target machine.

2. The final version we need here is DB2 ESE 8.2.3. It can be achieved either by installing DB2 ESE 8.1 and Fix Pack 10 or DB2 ESE 8.2 and Fix Pack 3. Here we installed DB2 ESE 8.1 and Fix Pack 10.

3. Copy the DB2 package Version 8.1 for AIX to a temporary directory, for example /scratch/DB28.1forAIX5, on the Integration Server machine.

4. Use the command `tar -xvf <file.tar>` or `gzip -dv <file.Z>` to uncompress the downloaded package if it is in .tar or .Z file format. Once it is done, you should see the directory /005_ESE_AIX5_3264_SBCS.

5. Decide if you want to use the command line shell script or a graphical installation wizard to install DB2. The command line shell script requires many manual steps including creating users and groups, setting up the database server after the manual installation, configuring TCP/IP communications, etc. The installation wizard is a graphical tool, which is easier for typical users; however it requires Java 1.4.1.

6. The default installed directory for DB2 will be in /usr/opt/db2_08_01. Minimum disk space for DB2 is 1316100 KB.

☐ **Install DB2 ESE base**

1. Change directory to /ese.sbcs. You can run the ./db2_install command to start the installation manually using command line or use the ./db2setup command to install the product using the installation wizard.

2. Follow the DB2 Information Center for the details of a typical DB2 installation:
   http://publib.boulder.ibm.com/infocenter/db2luw/v8//index.jsp

3. During the installation, use these users and groups:
   - Instance user: db2inst1

- – Instance administration group: db2iadm1
- – Fenced user: db2fenc1
- – Fenced administration group: db2fadm1
- – DB2 administration server (DAS) user: dasusr1
- – DB2 administration server (DAS) administration group: dasadm1

☐ **Verify the base installation**

1. Verify if DB2 is up and running:

    a. Log in as db2 instance; in this case **db2inst1**

    b. Start db2 by typing **db2** in the command line.

    c. Create a sample database called sample1. Type: `create database sample1`

    d. Once the database is created, check if the database sample1 is cataloged. Type: list database directory.

    e. Exit db2, type: `quit`

2. Check if any service port is listening to DB2. You can use the netstat command.

    a. First, log in as root.

    b. Type: `netstat –a –f inet | grep LISTEN`

    c. You should be able to find an entry for DB2. If not, you need to configure the TCP/IP communication for the DB2 instance:

        i. Log in as db2inst1.

        ii. View the /etc/services file. You should see these lines from the file:

```
DB2_db2inst1        60000/tcp
DB2_db2inst1_1      60001/tcp
DB2_db2inst1_2      60002/tcp
DB2_db2inst1_END            60003/tcp
```

        iii. Configure the DB2 services: Start DB2. At the db2 prompt, type: `update database manager configuration using svcename DB2_db2inst1`

        iv. Configure the DB2 to listen to the TCP/IP port, and type this at the db2 prompt: `db2set DB2COMM=tcpip.` Exit DB2.

        v. Refresh the db2 profile, type: `. /home/db2inst1/sqllib/db2profile`

        vi. Stop the db2 server; type: `db2stop`

        vii. Refresh the inetd service file. To do so, login as root, then type: `refresh –s inetd`

        viii.Restart the db2 server. Log in as db2inst1, then type: `db2start`

        ix. Use the netstat command above to check again if DB2 is being listened at any port.

Task 2. DB2 ESE 8.1 Fixpak 10 installation and configuration

☐ **Planning**

1. You must have root access.

2. You have verified that the DB2 base product is working.

3. Installed DB2 Fixpak 10 on the ESE 8.1 will bring the DB2 level equivalent to DB2 ESE V8.2.3.

4. Download the DB2 8.1 Fixpak 10 from the external IBM db2 support site at:
   http://www-306.ibm.com/software/data/db2/udb/support/

5. Save the fix pack to a temporary directory and make sure there is no blank character in the directory name and path or the installation will fail. Uncompress the downloaded file with the command: `tar –xvf <file.tar>` or `gzip –dv <file.Z>`

☐ **Stop all DB2 processes prior to the installation**

1. Log in as root.

2. Switch to log in as db2inst1; type: `su – db2inst1`

3. Run the following commands. Press Enter after each command:

```
. $HOME/sqllib/db2profile
db2 force applications all
db2 terminate
db2stop
db2licd –end
exit
```

4. Stop the db2 administration server (DAS). Log in as the DAS administration user. Type the following commands. Press Enter after each command.

```
su – dasusr1
. $HOME/das/dasprofile
db2admin stop
exit
```

5. Unload unused shared libraries from memory. You need to log in as root. Run this command: `/usr/skin/slibclean`

6. Disable the Fault Monitor if it exists and is using DB2 Version 8. Make sure you are root.

   a. Change directory to /usr/opt/db2_08_01/bin where the db2fmcu command will be run from, and then disable the Fault Monitor Coordinator by typing this command: `db2fmcu -d`

   b. Stop the Fault Monitor Daemon, issue the following command. However, you need to make sure the DB2INSTANCE environment is set first: `db2fm -D`

☐ **Install DB2 Fix Pack 10**

1. Login as root.

2. Change directory to which the installation image is located.

3. Launch the installation, type: `./installFixPak –y`

4. Once it is done, you will see a summary of the fix pack installation.

☐ **Configuration after the fix pack installation**

1. Log in as root.

2. You need to perform these four tasks after the fix pack installation:

   a. Run the djxlink command if you have the DB2 Relational Connect installed. Here we do not have DB2 Relational Connect installed, so we can skip this task.

   b. Update instances to use the new level of DB2

   c. Restart the instance

   d. Re-bind the bind files

3. To update the instances to use the new level of DB2:

   a. Log in as root.

    b. Update db2inst1 instance, change directory to /usr/opt/db2_08_01/instance, and type: **./db2iupdt db2inst1**

    c. Update the DB2 Administration Server (DAS). Run this command: **./dasupdt dasusr1**

    d. Update the system catalogs: Run the db2updv8 command to update the system catalogs to support the current level if you have existing databases. For details, use the –h option.

4. Restart the instance:

    a. Log in as the db2 instance (i.e., db2inst1).

    b. Type: db2start.

5. Restart the administration server.

    a. Log in as the DAS owner (i.e., dasusr1).

    b. Type: **db2admin start**

6. Rebind the bind files. This step binds the DB2 utilities against all the existing databases after the installation.

    a. Log in as db2 instance (i.e, db2inst1).

    b. Type: **db2 bind /usr/opt/db2_08_01/bnd/@db2cli.lst blocking all grant public**

☐ **Verification**

1. Log in as db2inst1.

2. Start db2 application by typing db2.

3. Check the database catalog. Type list database directory. You should still see the database name sample1 that you created earlier.

Task 3. WebSphere MQ 5.3.02 for AIX installation

You can refer to the WebSphere MQ for AIX Quick Beginnings Version 5.3 for details on the product installation. The document is available at:
http://publibfp.boulder.ibm.com/epubs/pdf/amqaac06.pdf

Here we provide some basic information about the installation of the product.

☐ **Planning**

1. You must have root access.

2. The WebSphere Business Integration Server Foundation 5.1.x that we are going to install requires MQ 5.3.04 or higher for the external JMS provider. If you have MQ installed, you can check the version with this command: **mqver**.

3. You will be using the AIX smitty tool to install the product. There is no installation script.

4. The MQ 5.3.0.2 is bundled inside the WebSphere Business Integration Server Foundation 5.1 e-assembly for AIX installation files. Copy the installation file to a temporary directory on the target AIX machine.

5. Uncompress the downloaded file using the **tar –xvf <file.tar>** command.

☐ **Create users and groups needed for MQ 5.3**

1. Log in as root.

2. Create these directories for the messaging feature. Use the **mkdir <directory name>** command to do so.

    – /var/mqm for your messaging working data, minimum 50 MB

- /var/mqm/log
- /var/mqm/errors
- /var/mqm/trace for SSL trace

3. Create two groups: mqm and mqbrkrs.

   a. Make sure you are root.

   b. Use the smitty tool. Type `smitty` at command line.

   c. Select **Security & Users** → **Group** → **Add a group**. Then set the Group Name to be `mqm`. Press Enter.

   d. Repeat these steps to create the group mqbrkrs.

4. Create the user mqm.

   a. Make sure you are root.

   b. Use the smitty tool.

   c. Select Security & Users → Users → Add a user.

   d. Set the name field to be `mqm`. Press Enter. Quit the smitty tool.

   e. Set the password for this user. Type `password mqm`. Then enter the new password.

5. Add mqm and root to the mqm group. The users mqm and root would be added to the group mqm so that these users have the authority to run administration commands such as creating or starting the queue manager.

   a. Make sure you are root.

   b. Use the smitty tool.

   c. Select **Security & Users** → **Groups** → **Change/Show Characteristics of a Group**. Then enter **mqm** for the Group Name field. Press Enter. Then enter the users *mqm* and *root* for the USER list. Press Enter.

6. Add root to the mqbrkrs group.

   a. Make sure you are root.

   b. Use the smitty tool.

   c. Select **Security & Users** → **Groups** → **Change/Show Characteristics of a Group**. Then enter *mqbrkrs* for the Group Name field. Press Enter. Then enter the user *root* for the USER list field. Press Enter.

☐ **Install MQ 5.3**

1. Log in as root.

2. Once you downloaded and uncompressed the installation file, you will find the MQ53Server_aix.tar and the readme directory.

3. Uncompress the MQ53Server_aix.tar file with the tar **−xvf <file.tar>** command. When it is done, you will find a list of packages in the directory including the mqm.server package.

```
r14n13:/scratch/MQ5.3.02 # ls
C48UFML.tar          mqm.base.sdk        mqm.msg.Fr_FR      mqm.msg.it_IT
MQ53Server_aix.tar   mqm.client.rte      mqm.msg.It_IT      mqm.msg.ja_JP
READMEs              mqm.dce.samples     mqm.msg.Ja_JP      mqm.msg.ko_KR
gskak.rte            mqm.dce.server      mqm.msg.Zh_CN      mqm.msg.pt_BR
licenses             mqm.java.rte        mqm.msg.Zh_TW      mqm.msg.zh_CN
mqm.Client.Bnd       mqm.keyman.rte      mqm.msg.de_DE      mqm.msg.zh_TW
mqm.Server.Bnd       mqm.man.en_US.data  mqm.msg.en_US      mqm.server
mqm.base.runtime     mqm.msg.De_DE       mqm.msg.es_ES      readme
mqm.base.samples     mqm.msg.Es_ES       mqm.msg.fr_FR
```

4. Use the smitty tool to install the product.

   a. Make sure you are root.

   b. Type `smitty` on the command line.

   c. Select

      • Software Installation and Maintenance

      • Install and Update Software

      • Install and Update from ALL Available Software

   d. Then put a "." to indicate the current directory in the "INPUT device/directory for software".

5. In the next screen in the SOFTWARE to install field, use the function F4 key to browse the list of software that is in the current directory.

6. Then select all the packages that start with "mqm," except the mqm.dce package. If you select the mqm.dce package, you will not be able to use SSL channel. For example, you should include these packages:

   – mqm.Server.Bnd

   – mqm.server

   – mqm.msg.en_US

   – mqm.base

   – mqm.Client.Bnd

   – mqm.client.rte

   – mqm.java.rte

   – mqm.keyman.rte

   Press Enter. In the next screen, make sure these fields are set to YES:

   – AUTOMATICALLY install requisite software = Yes

   – ACCEPT new license agreements = Yes

```
 ● r14n13
                    Install and Update from ALL Available Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                                [Entry Fields]
* INPUT device / directory for software                  .
* SOFTWARE to install                                    [mqm.server                >
  PREVIEW only? (install operation will NOT occur)        no
  COMMIT software updates?                                yes
  SAVE replaced files?                                    no
  AUTOMATICALLY install requisite software?               yes
  EXTEND file systems if space needed?                    yes
  OVERWRITE same or newer versions?                       no
  VERIFY install and check file sizes?                    no
  DETAILED output?                                        no
  Process multiple volumes?                               yes
  ACCEPT new license agreements?                          yes
  Preview new LICENSE agreements?                         no
```

Figure 3-2   Fields to set to Yes

Press Enter when you are ready to start the installation. When the installation is done, you will see a summary of the packages you installed. Exit the tool.

7. Verify the packages are installed by using the `lslpp –l | grep mq` command.

```
r14n13:/scratch/MQ5.3.02 # lslpp -l | grep mq
  mqm.Client.Bnd          5.3.0.2   COMMITTED   WebSphere MQ Client Bundle
  mqm.Server.Bnd          5.3.0.2   COMMITTED   WebSphere MQ Server Bundle
  mqm.base.runtime        5.3.0.2   COMMITTED   WebSphere MQ Runtime for
  mqm.base.samples        5.3.0.2   COMMITTED   WebSphere MQ Samples
  mqm.base.sdk            5.3.0.2   COMMITTED   WebSphere MQ Base Kit for
  mqm.client.rte          5.3.0.2   COMMITTED   WebSphere MQ Client for AIX
  mqm.java.rte            5.3.0.2   COMMITTED   WebSphere MQ Java Client and
  mqm.keyman.rte          5.3.0.2   COMMITTED   WebSphere MQ Support for GSKit
  mqm.msg.en_US           5.3.0.2   COMMITTED   WebSphere MQ Messages - U.S.
  mqm.server.rte          5.3.0.2   COMMITTED   WebSphere MQ Server
  mqm.base.runtime        5.3.0.2   COMMITTED   WebSphere MQ Runtime for
  mqm.man.en_US.data      5.3.0.2   COMMITTED   WebSphere MQ Man Pages - U.S.
```

Figure 3-3   Verifying that packages are installed

☐ **Verify the MQ 5.3 installation**

1. We will use a simple configuration of one queue manager and one queue. Use sample programs to put a message onto the queue and to read the message from the queue. If you have selected the samples during the installation, you should have some samples in the usr/mqm/samp/bin directory.

2. Set up a queue manager and a queue:

    a. Log in as mqm.

    b. Create a default queue manager called venus.queue.manager by typing this command: `crtmqm –q venus.queue.manager`

    c. Start the queue manager. Type: `strmqm`

    d. Run the MQSC command: `runmqsc`

    e. Define a local queue called ORANGE.QUEUE. Type: `define qlocal (orange.queue)`

    f. You will see some messages confirming the creation of the queue. Type **end** to end the session.

```
$ runmqsc
5724-B41 (C) Copyright IBM Corp. 1994, 2002.  ALL RIGHTS RESERVED.
Starting MQSC for queue manager .


define qlocal (orange.queue)
     1 : define qlocal (orange.queue)
AMQ8006: WebSphere MQ queue created.
end
     2 : end
One MQSC command read.
No commands have a syntax error.
All valid MQSC commands were processed.
```

Figure 3-4   Confirming creation of the queue

3. Testing the queue:

    a. Change directory to /usr/mqm/samp/bin.

    b. Run the amqsput sample to put a message to the queue. Type this command: `amqsput ORANGE.QUEUE`

    You will see the confirmation that the amqsput program starts and the target queue is ORANGE.QUEUE. Type a message (one line or multiple lines). Type a blank line afterwards to end the message.

```
$ pwd
/usr/mqm/samp/bin
$ amqsput ORANGE.QUEUE
Sample AMQSPUT0 start
target queue is ORANGE.QUEUE
This is a test for the MQ setup
Bye
```

c. Run the amqsget sample to get the message from the queue. Type this command:
amqsget ORANGE.QUEUE

You should see your message. This verifies the installation is successful.

```
$ amqsget ORANGE.QUEUE
Sample AMQSGET0 start
message <This is a test for the MQ setup>
message <Bye>
```

Task 4. WebSphere MQ 5.3 Fix Pack 11 (CSD11) installation and configuration

☐ **Planning**

1. You must have root access.

2. Required disk space: 21 MB for the installation and 21 MB for saving the previous level.

3. Make sure no queue manager is running while upgrading the fix pack.

4. For the SSL support, if you have installed the IBM GSKit, you have to upgrade this GSKit to the right level first before upgrading the MQ filesets.

Download the WebSphere MQ Fix Pack 11 (CSD11) for AIX 5.3 from the external product support site at:

http://www-1.ibm.com/support/docview.wss?rs=171&context=SSFKSJ&context=SSWHKB&dc=D430&dc=D410&dc=D420&dc=D400&dc=DB550&q1=CSD11&uid=swg24010287&loc=en_US&cs=utf-8&lang=en

If this link is not available, search the fix pack from: http://www.ibm.com/products

☐ **Install MQ 5.3 Fix Pack 11**

1. You must have root access.

2. Download the downloaded fix pack to a temporary directory of the target machine. Uncompress the file with this command: **gzip –dv <file.Z>** or **tar –xvf <file.tar>**.

3. Upgrade the IBM GSKit.

   a. First check the IBM GSKit level by using this command: **lslpp –l | grep gsk***

   b. Here is the list of GSKit levels required for each fix pack level:

   ```
   The level of GSKit which is distributed with fix pack CSD03 is "6.0.3.33".
   The level of GSKit which is distributed with fix pack CSD04 is "6.0.4.37".
   The level of GSKit which is distributed with fix pack CSD06 is "6.0.5.39".
   The level of GSKit which is distributed with fix pack CSD07 is "6.0.5.41".
   The level of GSKit which is distributed with fix pack CSD09 or later is "6.0.5.43".
   ```

   Since we are installing Fix Pack 11 (CSD11), we need to bring the GSKit level to 6.0.5.43.

c. To upgrade the GSKit, change directory to the location of the Fix Pack 11 GSKit fileset, then run this command: `installp –ac –d .gskak.rte`

You should get a confirmation saying the installation is successful.

4. Upgrade the MQ filesets:

   a. Make sure you are root and you are in the MQ fix pack directory. Use the smitty tool.

   b. Select:

   – Install and Upgrade Software

   – Install and Upgrade from ALL Available Software.

   Then type "." for the current directory for the "INPUT device/directory for software" field.

   c. Then under the "Software to install" field, use function F4 key to list the available packages. Select these packages to install:

   • mqm.base (MQ Base Kit, MQ Runtime, MQ Samples)

   • mqm.client (MQ Client for AIX)

   • mqm.java (MQ Java Client and JMS)

   • mqm.keyman (MQ Support for GSKit)

   • mqm.man (MQ man pages—U.S. English)

   • mqm.msg.en_US (MQ Message—U.S. English)

   • mqm.server (MQ Server)

Press Enter to return to the smitty menu. Press Enter again to execute the installation. You should see the summary that confirms the success of the installation.

```
  Selected Filesets
  ----------------
  mqm.base.runtime 5.3.0.11                    # WebSphere MQ Runtime for Cli...
  mqm.base.samples 5.3.0.11                    # WebSphere MQ Samples
  mqm.base.sdk 5.3.0.11                        # WebSphere MQ Base Kit for Cl...
  mqm.client.rte 5.3.0.11                      # WebSphere MQ Client for AIX
  mqm.java.rte 5.3.0.11                        # WebSphere MQ Java Client and...
  mqm.keyman.rte 5.3.0.11                      # WebSphere MQ Support for GSKit
  mqm.man.en_US.data 5.3.0.11                  # WebSphere MQ Man Pages - U.S...
  mqm.msg.en_US 5.3.0.11                       # WebSphere MQ Messages - U.S....
  mqm.server.rte 5.3.0.11                      # WebSphere MQ Server

  << End of Success Section >>
```

☐ **Verify MQ 5.3 Fix Pack 11 installation**

1. You can use the mqver command to determine the current version.

```
r14n13:/scratch/MQ53_FP11 # mqver
Name:          WebSphere MQ
Version:       530.11    CSD11
CMVC level:    p530-11-L050802
BuildType:     IKAP -  (Production)
```

2. You can login as mqm. Start the queue manager, then put and retrieve a message to and from a local queue as we tested the base installation mentioned before.

Task 5. WebSphere Application Server Version 5.1 and HTTP Server installation and configuration

☐ **Planning**

1. You must have root access.

2. Installation of WebSphere Application Server will include the IBM HTTP Server installation.

3. Disk space requirement: At least 700 MB is needed for the default WebSphere Application Server installation directory, which is /usr/WebSphere/AppServer. About 27 MB is needed for the HTTP Server default installation directory, which is /usr/IBMHttpServer.

☐ **Install WebSphere Application Server 5.1 base**

1. Log in as root.

2. Copy the WebSphere Application Server 5.1 installation file to a temporary directory on the target machine. Then uncompress the file using the `tar –xvf <file.tar>` command.

3. Run the launchpad.sh command in that directory.

4. A window pops up, and you can select **Install the product**. Click **Next** on the next screen.

5. Review and accept terms and conditions. Click **Next**.

6. A check of the operating system is made. Click **Next**.

7. Select **custom** instead of typical installation because we will not choose the embedded messaging feature. Click **Next**. Then review the list of components that will be installed. Make sure that the feature embedded messaging is not chosen. Click **Next**.

8. The prompt will ask for the installation paths for the application server and the HTTP server. The default value for the application server path is /usr/WebSphere/AppServer. The default value for the IBM HTTP Server is /usr/IBMHttpServer. Accept both defaults unless you want to change them.

9. The node name and IP are detected. Click **Next**.

10. A summary of the components that will be installed is shown. Click **Next**.

11. It will take a while for the installation to complete. Click **Next** when it is done.

12. You will be prompted to register the product. Click **Finish**.

13. Then the First Steps window appears, as shown in Figure 3-5 on page 39.
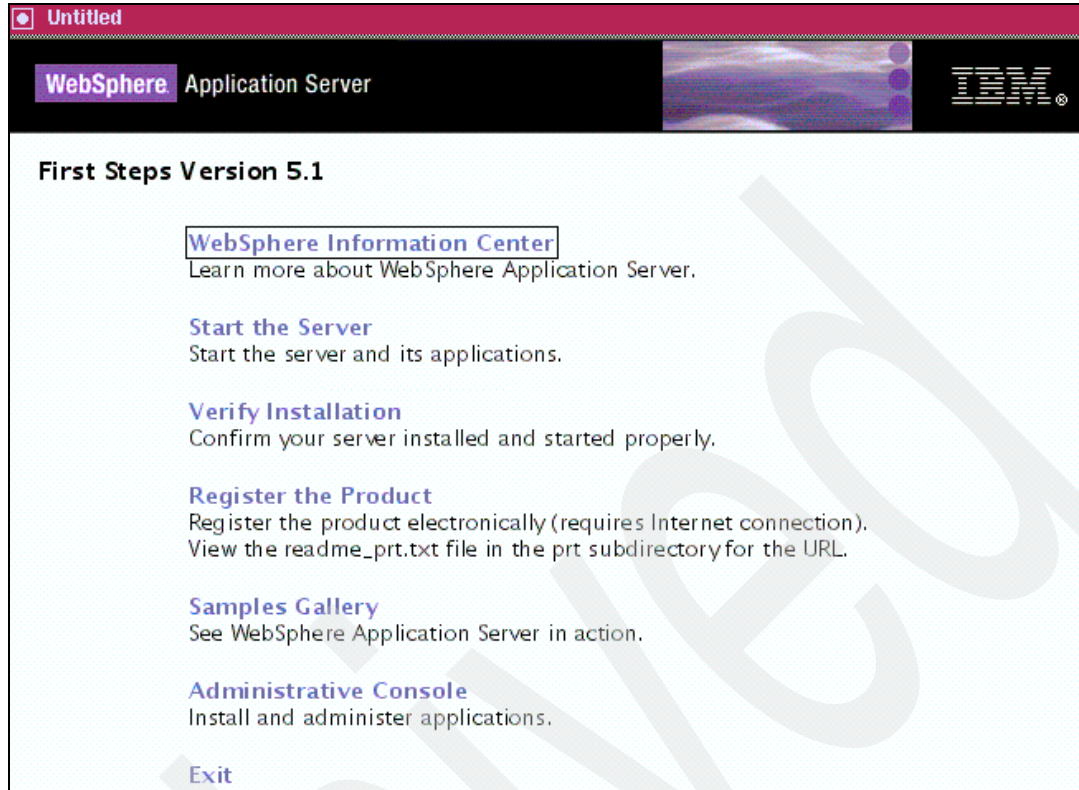
Figure 3-5   The First Steps window

☐ **Verify WebSphere Application Server installation**

1. Make sure you are root.

2. Start the WebSphere Application Server server:

   a. Change directory to the <WebSphere Application Server_install_root>/bin.

   b. Run this command: **`startServer.sh server1`**. It may take a while for the server to start. Wait until it displays a message saying the server is `open for e-business`.

3. From the First Step window, select the Verify Installation menu. The verification test will then run. Messages will be displayed to show the test is complete and successful.
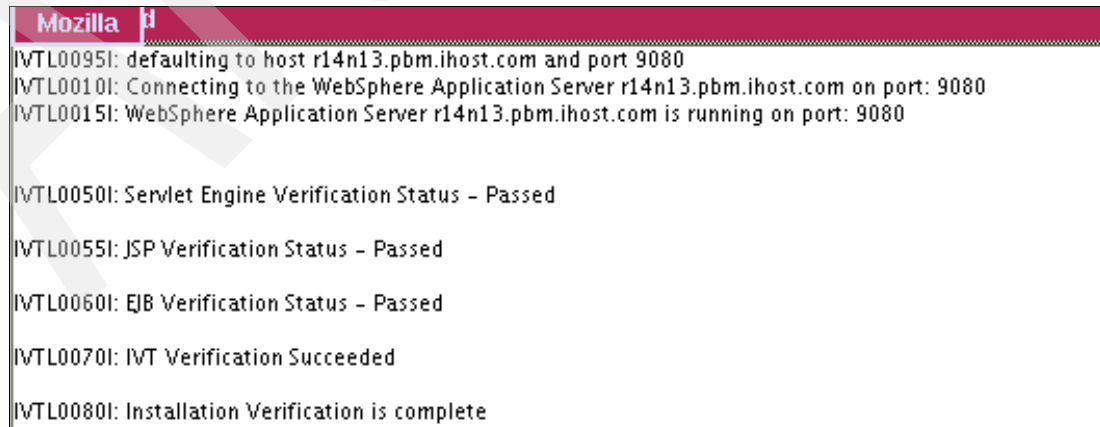
Figure 3-6   Test is complete

4. Now you should be able to open the WebSphere Application Server administration console from the browser:

   `http://<machine IP>:9090/admin`

5. Stop the server using the `stopServer.sh server1` command. We will prepare to install WebSphere Application Server fix pack.

Task 6. WebSphere Application Server 5.1 Fix Pack 1 and Cumulative Fix 6 installation and configuration

☐ **Planning**

1. Make sure you log in as root.

2. Download the WebSphere Application Server 5.1 Fix Pack 1(a zip file) from the support site at: `http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24007195`

   And to a desktop machine, download the WebSphere Application Server 5.1.1. Cumulative Fix 6 from the support site at:
   `http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg27006879#5116`

☐ **Install WebSphere Application Server 5.1 Fix Pack 1**

1. For installing the fix pack, follow the installation information provided on the support site at:
   `http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24007195`

2. In the AIX target machine, create a directory (e.g., /update_fixpack1) for the fix pack 1 under the <WebSphere Application Server_install_home> directory, which is /usr/WebSphere/AppServer.

3. Uncompress the zip file in the desktop machine and then FTP the extracted files to the target AIX machine and put them under /<WebSphere Application Server_install_home>/update. Use the `tar –xvf <file.tar>` command if needed to uncompress any tar files.

4. Run the updateWizard.sh command to start the installation wizard. Choose the **Install Fix Pack** option to install the fix pack.

☐ **Verify the WebSphere Application Server 5.1.1 installation**

1. Start the WebSphere Application Server server:

   a. Change directory to /<WebSphere Application Server_install_home>/bin

   b. Type: `startServer.sh server1`

   c. Wait until the server is `open for e-business`.

2. Start the administration console from a browser. Type this URL:

   `http://<machine IP>:9090/admin`

3. Stop the WebSphere Application Server server and prepare for the cumulative fix installation.

☐ **Install WebSphere Application Server 5.1.1 Cumulative Fix 6**

Please note: You must have installed WebSphere Application Server 5.1 Fix Pack 1 prior to the installation of this cumulative fix.

1. For installing the cumulative fix, follow the installation information provided on the support site at: `http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg27006879#5116`

2. In the AIX target machine, create a directory (e.g., /update_cumulativeFix6) for the Cumulative Fix 6 under the <WebSphere Application Server_install_home> directory, which is /usr/WebSphere/AppServer.

3. Uncompress the zip file in the desktop machine and then FTP the extracted files to the target AIX machine and put them under /<WebSphere Application Server_install_home>/update. Use the `tar –xvf <file.tar>` command if needed to uncompress any tar files.

4. Run the updateWizard.sh command to start the installation wizard. Choose the **Install Fix Pack** option to install the fix pack.

☐ **Verify the WebSphere Application Server 5.1.1.6 installation**

1. Start the WebSphere Application Server server:

   a. Change directory to /<WebSphere Application Server_install_home>/bin

   b. Type: `startServer.sh server1`

   c. Wait till the server is open for e-business.

2. Start the administration console from a browser. Type this URL:

   `http://<machine IP>:9090/admin`

   You should see the version of WebSphere Application Server from the About section on the top right-hand corner, as shown in Figure 3-7.
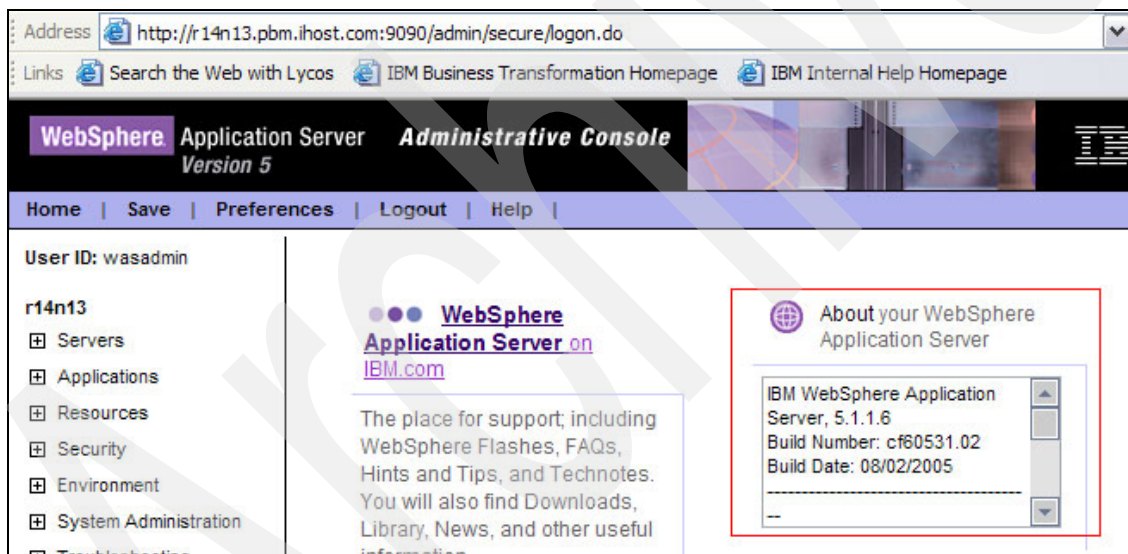
Figure 3-7   Checking the version

Task 7. WebSphere Business Integration Server Foundation V5.1 installation and configuration

☐ **Planning**

1. Make sure you log in as root.

2. Make sure the WebSphere Application Server server is stopped.

3. The WebSphere Business Integration Server Foundation 5.1 installation files are part of the WebSphere Business Integration Server Foundation 5.1 e-assembly bundle that is available from the Xtreme Leverage site.

4. Required disk space: At least 900 MB for WebSphere Business Integration Server Foundation.

☐ **Installing WebSphere Business Integration Server Foundation 5.1 base**

1. Uncompress the WebSphere Business Integration Server Foundation installation files (two files) to a temporary directory on the target AIX machine using the `tar -xvf <file.tar>` command.

2. Run the command `launchpad.sh.`

3. The WebSphere Business Integration Server Foundation menu appears. Select the option **Install the product**. It will take a few minutes before the installation wizard appears. Be patient.

4. The installation wizard appears. Select **Next**.

5. Review and accept the terms and conditions, then click **Next**.

6. The installation wizard checks the operating system level. Click **Next**.

7. It detects an existing WebSphere Application Server. Click **Next**.
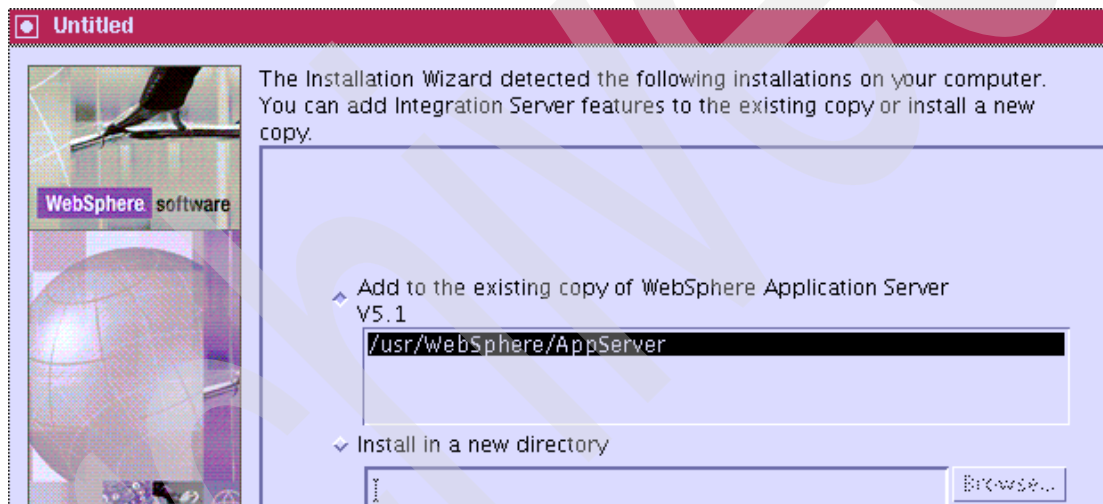
Figure 3-8   Detecting an existing WebSphere Application Server

8. Select custom installation instead of the typical installation. Click **Next**.

9. Review the list of selected components. Make sure that the Embedded Messaging feature is disabled. Then click **Next**.

Figure 3-9   Checking the Embedded Messaging feature

10.Click **Next** in the next window.
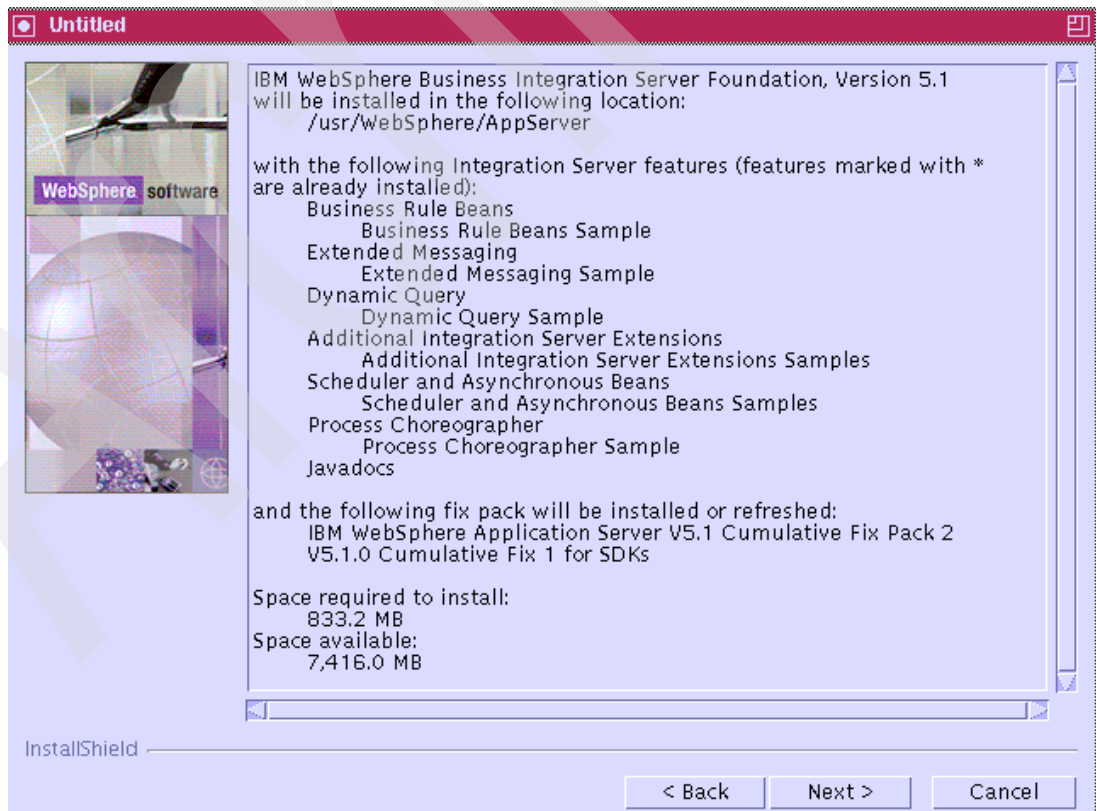
Figure 3-10   List of installed features
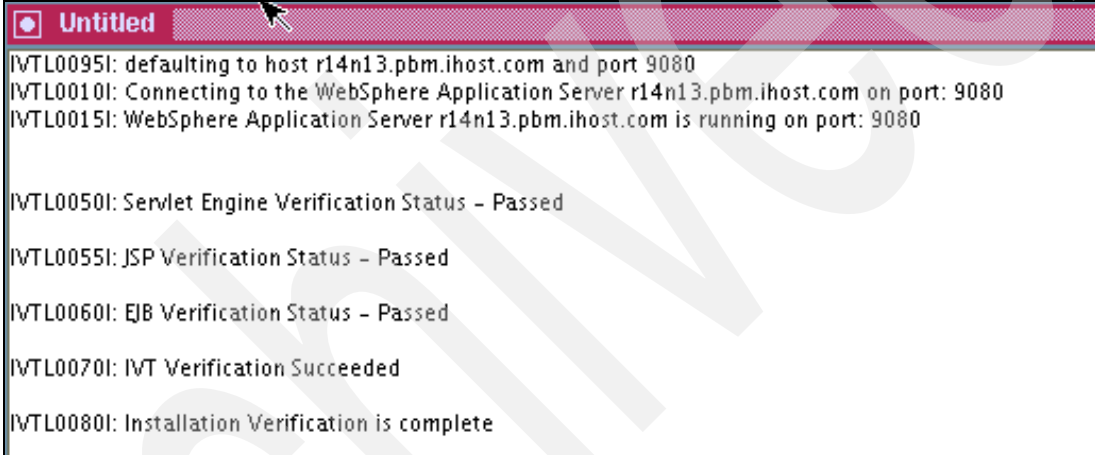
It will take an hour or so to install this.

11. Once the installation is done, it will ask you to register online. Click **Next**.

12. A message will confirm that the installation is complete. Click **Finish**.

☐ **Verify the WebSphere Business Integration Server Foundation base installation**

1. From the <WebSphere Application Server_install_home>/bin directory, start the WebSphere Application Server server with this command: `startServer.sh server1`

2. Wait until the message that server1 is `open for e-business.`

3. Run the verification test from the First Step window:

   a. Change directory to <WebSphere Application Server_install_root>/firststeps

   b. Type: `firststeps.sh`

4. When the First Steps window appears, select the **verify installation** option.

5. Check out the test result in Figure 3-11.

Figure 3-11   Checking the results

6. Start the WebSphere Application Server administration console from a browser. Type this URL: `http://<machine IP>:9090/admin` and log in. Since we have not set up any security in WebSphere Application Server, we can use any login name and it does not matter. From the top right-hand corner of the administration console, you should see the About section that display the WebSphere Application Server and WebSphere Business Integration Server Foundation versions that are installed.

Task 8. WebSphere Business Integration Server Foundation 5.1 Fixpak 1 and Cumulative Fix 2 installation and configuration

☐ **Planning**

1. You must have root access.

2. Both the WebSphere Business Integration Server Foundation 5.1 Fixpak 1 and the Cumulative Fix 2 are available from the external IBM product site. The Fixpak 1 can be found at: `http://www-1.ibm.com/support/docview.wss?rs=1079&uid=swg24007486`.

   The Cumulative Fix 2 is available at:

http://www-1.ibm.com/support/docview.wss?rs=1079&context=SS2KS6&dc=D430&dc=D410
&dc=D420&dc=D400&dc=DB550&q1=fix&uid=swg24009803&loc=en_US&cs=utf-8&lang=en

If these links are unavailable, you can search on the IBM product site at:
http://www-306.ibm.com/software/integration/wbisf/support/

3. Prepare enough disk space. WebSphere Business Integration Server Foundation Fix Pack 1 requires 400 MB disk space minimum on /usr, where WebSphere Application Server is installed, and 400 MB for the /tmp directory. The Cumulative Fix 2 has the same disk space requirement.

4. The installations for WebSphere Business Integration Server Foundation fix pack and cumulative fix are very similar to the ones for WebSphere Application Server. First, you should stop the WebSphere Application Server by running the command:
<WebSphere Application Server_install_home>/bin/stopServer.sh server1

Download each fix to a temporary directory under <WebSphere Application Server_install_home> directory.

☐ **Install WebSphere Business Integration Server Foundation 5.1 Fix Pack 1**

1. For installing the fix pack, follow the installation information provided on the support site at: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24007195

2. In the AIX target machine, create a directory (e.g., /update_WBISF51 fix pack1) for the fix pack 1 under the <WebSphere Application Server_install_home> directory, which is /usr/WebSphere/AppServer.

3. Uncompress the zip file in the desktop machine and then FTP the extracted files to the target AIX machine and put them under /<WAS_install_home>/update_WBISF51fixpak1. Use the **tar –xvf <file.tar>** command if needed to uncompress any tar files.

4. Run the updateWizard.sh command to start the installation wizard; choose the **Install Fix Pack** option to install the fix pack.

☐ **Verify the WebSphere Business Integration Server Foundation 5.1.1 installation**

1. Start the WebSphere Application Server server:

   a. Change directory to /<WebSphere Application Server_install_home>/bin

   b. Type: **startServer.sh server1**

   c. Wait until the server is open for e-business.

2. Start the administration console from a browser. Type this URL:

   http://<machine IP>:9090/admin

3. Stop the WebSphere Application Server server and prepare for the cumulative fix installation.

☐ **Install WebSphere Business Integration Server Foundation 5.1.1 Cumulative Fix 2**

Please note: You must have installed WebSphere Business Integration Server Foundation 5.1 fix pack 1 prior to the installation of this cumulative fix.

1. For installing the cumulative fix, follow the installation information provided on the support site at:

   http://www-1.ibm.com/support/docview.wss?rs=1079&context=SS2KS6&dc=D430&dc=D410
   &dc=D420&dc=D400&dc=DB550&q1=fix&uid=swg24009803&loc=en_US&cs=utf-8&lang=en

2. In the AIX target machine, create a directory (e.g., /update_WBISF51cumulativeFix2) for the Cumulative Fix 2 under the <WebSphere Application Server_install_home> directory, which is /usr/WebSphere/AppServer.

3. Uncompress the zip file in the desktop machine and then FTP the extracted files to the target AIX machine and put them under /<WebSphere Application Server_install_home>/update_WBISF51cumulativeFix2. Use the `tar –xvf <file.tar>` command if needed to uncompress any tar files.

4. Run the updateWizard.sh command to start the installation wizard; choose the **Install Fix Pack** option to install the fix pack.

☐ **Verify the WebSphere Business Integration Server Foundation 5.1.1.2 installation**

1. Start the WebSphere Application Server server:

    a. Change directory to /<WebSphere Application Server_install_home>/bin

    b. Type: `startServer.sh server1`

    c. Wait till the server is `open for e-business`.

2. Start the administration console from a browser. Type this URL:

    `http://<machine IP>:9090/admin`

    You should see information in the About section on the top right-hand corner listing the version of WebSphere Business Integration Server Foundation.
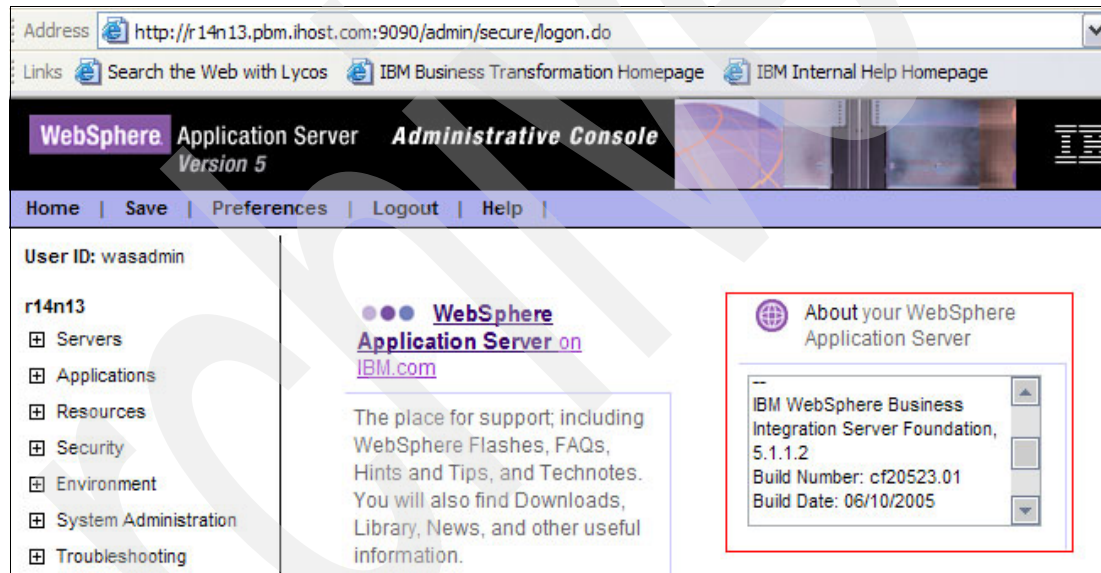
Figure 3-12   Verifying the version

Task 9. Configure WebSphere Application Server to point to MQ

☐ **From a browser, start the WebSphere Application Server administration console**

    `http://<machine IP>:9090/admin`

☐ **Set the MQ_INSTALL_ROOT and the MQJMS_LIB_ROOT environment variables**

1. Click **Environment** → **Manage WebSphere Variables**

2. Set MQ_INSTALL_ROOT to be the fully qualified file path for the WebSphere MQ installation home, which is /usr/mqm for AIX.

3. Set MQJMS_LIB_ROOT to be the relative file path for the WebSphere MQ library.

☐	MQJMS_LIB_ROOT	${MQ_INSTALL_ROOT}/java/lib
☐	MQ_INSTALL_ROOT	/usr/mqm

4. Click **Apply** → **Save** → **Save** to save the changes.

☐ **Restart the WebSphere Application Server server after the configuration changes**

Task 10. Configure a business process container in WebSphere Business Integration Server Foundation

☐ **Planning**

1. You must have root access.

2. Make sure you have installed the correct software: WBSIF without the embedded messaging feature, a full version of WebSphere 5.3 and the fix pack 4 or a later fix pack, and DB2 ESE 8.2.x.

3. In this step, we will configure the business process container, which is the WebSphere Business Integration Server Foundation process choreographer engine to point to DB2 for persistence and the external MQ for JMS provider.

4. Here are the configuration steps required:

   a. Create queue manager, queue and listener in MQ.

   b. Create the BPEDB database in DB2.

   c. Configure the Business Process Container using the WebSphere Application Server Administration Console.

☐ **Create queue manager, queue and listener in MQ**

1. You must have root access.

2. To create the queue manager and queues, change directory to: /usr/WebSphere/AppServer/ProcessChoreographer

   Run the command `createQueues.sh <queueManager>`, where "queueManager" is the name you are going to give, e.g., "WebSphere Application Server_r14n13_server1", where r14n13 is name of the machine.

3. The script will create a default queue manager and define these local queues for the process choreographer:

   a. BPEIntQueue – Internal Queue

   b. BPEApiQueue – API Queue

   c. BPEHldQueue – Hold Queue

   d. BPERetQueue – Retention Queue

4. Once you have created a default queue manager, it will put entries in into the /var/mam/mqs.ini file.

5. To create the queue listener, change directory to /usr/mqm/bin. Run this command:
   `runmqlsr –t tcp –p <port> -m <queueManager> &`

   where, <port> is an available port that the queue manager listens to and <queueManager> is the one you just defined in the previous step. If you are not sure which port it listens to, use the "netstat –an | grep LISTEN" command.

6. Add the port to the /etc/services file. You can add this line to the file:

```
<service name> <port>/tcp
```

where, <service name> is the name of the queue manager service and the <port> is the port that the queue manager listens to. Here is an example:

```
WAS_MQListener   21000/tcp          #MQ listener for WAS BPE
```

7. Add the same service to the /etc/inetd.conf file. You can add this line to the file:

```
<service name> stream tcp nowait mqm /usr/mqm/bin/amqcrsta amqrsta —m
<queueManager>.
```

Here is an example:

```
WAS_MQListener   stream   tcp      nowait   mqm      /usr/mqm/bin/amqcrsta amqrsta —m
WAS_r14n13_server1
```

☐ **Create the BPDB database in DB2**

1. You must have root access.

2. Change the user from root to DB2 instance. You can use the command "su – db2inst1", where db2inst1 is the name of the db2 instance.

3. Start the DB2 server. Run the db2start command.

4. Run the database scripts to create the database called BPEDB:

   a. Make sure you login as the DB2 instance.

   b. Change directory to /usr/WebSphere/AppServer/ProcessChoreographer.

   c. Run this command to create the BPEDB database:

      ```
      db2 —tf createDatabaseDb2.ddl
      ```

   Note: This command will take a while to finish.

5. Bind the CLI packages to the new database by running these commands:

   ```
   db2 connect to BPEDB
   db2 bind <db2 install root>/bnd/@db2cli.lst blocking all grant public
   ```

```
$ db2 connect to BPEDB

   Database Connection Information

 Database server        = DB2/6000 8.2.3
 SQL authorization ID   = DB2INST1
 Local database alias   = BPEDB

$ db2 bind /usr/opt/db2_08_01/bnd/@db2cli.lst blocking all grant public

LINE     MESSAGES FOR db2cli.lst
------   ------------------------------------------------------------
         SQL0061W  The binder is in progress.
         SQL0091N  Binding was ended with "0" errors and "0" warnings.
```

6. Run the database script to create tablespace:

   a. First create the location of the tablespace before we run the script.

      i. Make sure you log in as DB2 instance.

      ii. Change the directory to the home of the instance, e.g., /home/db2inst1.

      iii. Create a directory for the tablespace; for example, /WebSphere Application Server_WBE_tablespace.

b. Log in as root.

   i. Change directory to /usr/WebSphere/AppServer/ProcessChoreographer.

   ii. Modify the createTableDb2.ddl file so that you replace the occurrences of "@location@" with the location of the tablespace you want to create.

c. Log in as the DB2 instance.

   i. Change directory to /usr/WebSphere/AppServer/ProcessChoreographer.

   ii. Run these commands:

   ```
   db2 connect to BPEDB
   db2 —tf createTablespace.Db2.ddl
   ```

7. Create scheme (table and views)

   i. Make sure you log in as DB2 instance owner.

   ii. Change directory to /usr/WebSphere/AppServer/ProcessChoreographer/

   iii. Run these commands:

   ```
   db2 connect to BPEDB
   db2 —tf createSchemaDb2.ddl
   ```

d. Note that you may get several errors because the createSchemaDb2.ddl and the createDatabaseDb2.ddl are almost identical. Therefore, the create table commands are run twice and errors will be generated since the tables already exist. To fix this, run these commands:

   ```
   dropSchemaDb2.ddl
   db2 —tf createSchemaDb2.ddl
   ```

8. Verify the BPEDB database is created correctly. Run these commands:

   i. db2 connect to BPEDB user <db2 user ID>

   ii. db2 connect reset

```
$ db2 connect to BPEDB user db2inst1
Enter current password for db2inst1:

   Database Connection Information

 Database server       = DB2/6000 8.2.3
 SQL authorization ID  = DB2INST1
 Local database alias  = BPEDB

$ db2 connect reset
DB20000I  The SQL command completed successfully.
```

☐ **Configure the Business Process Container in WebSphere Application Server Administration Console**

1. From a browser, open the WebSphere Application Server administration Console:

   ```
   http://<your WebSphere Application Server server IP>:9090/admin
   ```

2. After you log in, select Server →Application Server →server1. In Additional Properties, select **Business Process Container**.

3. Select **Business Process Container Install Wizard**.

   a. Step 1: Database configuration, set these attributes:

      i. JDBC Provider = DB2 UDB 8.1 (DB2 Universal JDBC Driver Provider (XA)

      ii. Data source name = db2inst1

       iii. Data source password = <password of db2inst1>

       iv. Custom properties: Make sure the values are correct, e.g., Check port number, serverName, etc.

  b. Step 2: JMS Provider and Security, set these attributes except the ones that are disabled as shown here:

       i. JMS provider = WebSphere MQ JMS Provider

       ii. Queue Manager = <name of the queue manager> e.g., WebSphere Application Server_r14n13_server

       iii. Classpath = /usr/mqm/java/lib

       iv. JMS User ID =root (this field is disabled)

       v. JMS Password = (this field is disabled)

       vi. Scheduler calendar = (leave it blank and let it use the default)

       vii. Security Role Mapping = root

       viii.JMS API User ID = mqm

       ix. JMS API Password = <password of the mqm user>

  c. Step 3: Create New JMS resources page appears, click **Next** to accept the defaults.

  d. Step 4: The summary page will appear. See Figure 3-14 on page 51. Select **Finish**.

  e. Figure 3-13 displays the log result of the Business Process Container configuration. You should messages at the bottom to confirm the success of the configuration. Remember to save your settings.

AppNotification:task=InstallApplication, taskStatus=Completed, subtask=, subtaskStatus=, properties=
{appname=BPEWebClient_r14n13_server1}, message=ADMA5013I: Application BPEWebClient_r14n13_server1 installed
successfully.

ADMA5013I: Application BPEContainer_r14n13_server1 installed successfully.
ADMA5013I: Application BPEWebClient_r14n13_server1 installed successfully.

Figure 3-13   Configuration log

4. Set these environment variables. Select **Environment** → **Manager WebSphere Variables**.

  a. `UNIVERSAL_JDBC_DRIVER_PATH = ${WebSphere Application Server_INSTALL_ROOT}/universalDriver/lib`

  b. `DB2UNIVERSAL_JDBC_DRIVER_PATH = /usr/opt/db2_08_01/java`

  c. `MQ_INSTALL_ROOT = /usr/mqm`

  d. `DB2_INSTANCE = db2inst1`

→ Step 4   **Summary**

The Business Process container will be installed on application server cells/r14n13/nodes/r14n13/servers/server1 with the following values:

Datasource

Implementation Classname	com.ibm.db2.jcc.DB2XADataSource
Classpath	${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc.jar ${UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cu.jar ${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cisuz.jar
Datasource User Name	db2inst1
Datasource Password	***

Custom Properties		
	databaseName	BPEDB
	driverType	2
	serverName	r14n13.pbm.ihost.com
	portNumber	60000
	description	DataSource for Process Choreographer
	traceLevel	
	traceFile	
	fullyMaterializeLobData	true
	resultSetHoldability	2
	currentPackageSet	
	readOnly	false
	deferPrepares	false
	currentSchema	
	cliSchema	
	enableMultithreadedAccessDetection	false
	retrieveMessagesFromServerOnGetMessage	true
	preTestSQLString	SELECT 1 FROM TABLE1

JMS

JMS Providers	WebSphere MQ JMS Provider
JMS API User ID	mqm
JMS API Password	***

Process Choreographer Web Client

The web client will be installed.

Reminder

You must create the database and the tables yourself. After the Business Process container is installed, you can use the files in /usr/WebSphere/AppServer/ProcessChoreographer

Reminder

The following environment variables need to be set. On the left panel, select Environment --> Manage WebSphere Variables to configure each of the following:
DB2UNIVERSAL_JDBC_DRIVER_PATH
MQ_INSTALL_ROOT
UNIVERSAL_JDBC_DRIVER_PATH

Reminder

Since you are using an external JMS provider, the following resources must be created through your external JMS Provider's interface

Queue Manager	WAS_r14n13_server1
Internal Queue	BPEIntQueue
External Request Processing Queue	BPEApiQueue
Retention Queue	BPERetQueue
Hold Queue	BPEHldQueue

Figure 3-14   Summary page

5. Set the JNDI name of the calendar EJB™ for the process choreographer.

   a. Make sure you log in as root.

   b. Change directory to <WebSphere Application Server_install_home>/ProcessChoreographer.

   c. Run the setCalendar.jacl script:

   ```
   <WebSphere Application Server_install_home>/bin/wsadmin.sh —f setCalendar.jacl
   —jndiName <jndiName> -server <server> -node <node>
   ```

   Where:

   ```
   <jndiName> = com/ibm/websphere/scheduler/calendar/DefaultUserCalendarHome
   ```

   ```
   r14n13:/usr/WebSphere/AppServer/ProcessChoreographer # erver1 -node r14n13    <
   WASX7209I: Connected to process "server1" on node r14n13 using SOAP connector;
   The type of process is: UnManagedProcess
   Set calendar JNDI name to 'com/ibm/websphere/scheduler/calendar/DefaultUserCalen
   darHome' on server1(cells/r14n13/nodes/r14n13/servers/server1:server.xml#Server_
   1).
   ```

6. Activate the Business Process Container:

   a. Make sure you are root.

   b. Change directory to /<WebSphere Application Server_install_home>/bin

   c. Stop the server, run this command: **stopServer.sh server1**

   d. Set the purchased processor allowance, for example, **setmqcap 2**, where two is the number of processors on the machine.

   e. Start the WebSphere Application Server server, run this command: **startServer.sh server1**

☐ **Verify that the Business Process Container works**

1. Install some of the process samples according to the Information Center documentation. See the following link for instructions on how to install the samples:

   ```
   http://publib.boulder.ibm.com/infocenter/adiehelp/index.jsp?topic=/com.ibm.etoo
   ls.ctc.bpel.doc/samples/travelbooking/travelBooking.html
   ```

2. Once the sample process is installed, you can test it with the following link:

   ```
   http://localhost:9080/bpe/webclient/
   ```

4

JRules Server installation and configuration

JRules is a business rules management system (BRMS) product from ILOG that models, manages, and executes business rules on production J2EE application servers. The rules server, or rules engine, analyzes a passenger manifest to determine the risk score of a particular flight. This chapter discusses the installation and configuration of the JRules product.

Product description

JRules is a business rules management system (BRMS) product from ILOG that models, manages, and executes business rules on production J2EE application servers. The Rule Execution Server is a runtime execution component for integrating the JRules engine into the J2EE platform. It includes all the management, monitoring, and logging functionality that J2EE system administrators demand.

The Rule Execution Server's API and notifications conform to the Java Management Extensions (JMX™) standard. Servers can be integrated with enterprise-management tools. The Rule Execution Server also includes a Web-based administration system that provides real-time performance and alert monitoring for critical enterprise applications. [1]

Server definition

The rules server, or rules engine, analyzes a passenger manifest to determine the risk score of a particular flight. This server uses business rules written with ILOG's JRules product to compare passenger information with a known set of risk rules. The rules server requires two input files: a passenger manifest and a flight list. Both of these files reside on the integration server and are passed to the rules engine when the integration server invokes the rules application Web service wrapper application.

Server hardware

- IBM @server BladeCenter JS20

Server software stack

The JRules Server and the JRules Builder require the following software:

- AIX 5.3
- WebSphere Application Server Version 6.0.0 Fixpack 1
- DB2Connect
- HACMP 5.3
- ILOG JRules Version 5.1.2

Reference to product installation information

After you install ILOG JRules, you can find detailed information about configuring the product and creating business rules in the Help panels located on the ILOG Builder toolbar. Further product information is available on the ILOG Web site:

http://www.ilog.com

---

[1] Reference *Rules Execution Server* description on ILOG's Web site: http://www.ilog.com/products/jrules/server.cfm

Task 1. JRules Development Workbench installation

☐ **Log on to the JRules Blade Server as root or an equivalent user ID with root authority.**

☐ **Save the JRules installation executable (jrules.bin) in a temporary directory such as /scratch/jrules_install/.**

☐ **Verify that enough temp space exists on the system disk:**

1. Change to the **/tmp** directory: `cd /tmp`

2. Determine the amount of available temp space: `df -m`

3. If the available temp space is less than 512M, increase its size as follows:

    a. Enter: `smitty`
    b. To increase the available temp space, enter the following selection sequence:
       `System Storage Management > File Systems > Add / Change / Delete / Show /...`
    c. Select: Enhanced Journaled File System
    d. Select: Change / Show /....
    e. Select **/tmp**
    f. In the Unit Size field, tab to **Megabytes**.
    g. In the Number of Units field, delete current value and replace it with the value **512**.
    h. Press Enter and then press F10 to exit.

4. At the prompt, verify that the available temp space is set to 512 MB by entering `df -m`

☐ **Change to the /scratch/jrules_install/ directory.**

☐ **Enter jrules.bin to start the installation. Follow the JRules install shield command prompts. After the installation, JRules resides in /us/ilog/jrules512/.**

☐ **To verify the installation and start the JRules Builder:**

1. Change to the **/usr/ilog/jrules512/bin/RuleBuilder** directory.

2. Enter **brdev** to start the JRules rules builder.

Task 2. Rule Execution Server configuration

The Rule Execution Server, or Business Rules Execution (BRE) Server, is a J2EE application that supports the execution of business rules developed and deployed from the JRules Rule Builder workbench. The procedure to install and configure a BRE Server is described in the JRules documentation. The principle steps for configuring a BRE Server and deploying a rules application onto that server are:

- Installing the BRE Server Execution Stack on a WebSphere Application Server container
- Installing the BRE Server Management Stack on WebSphere Application Server container
- Deploying a rules application in the configured BRE Server

Figure 4-1 on page 56 shows the relationship between the components that comprise a JRules server.
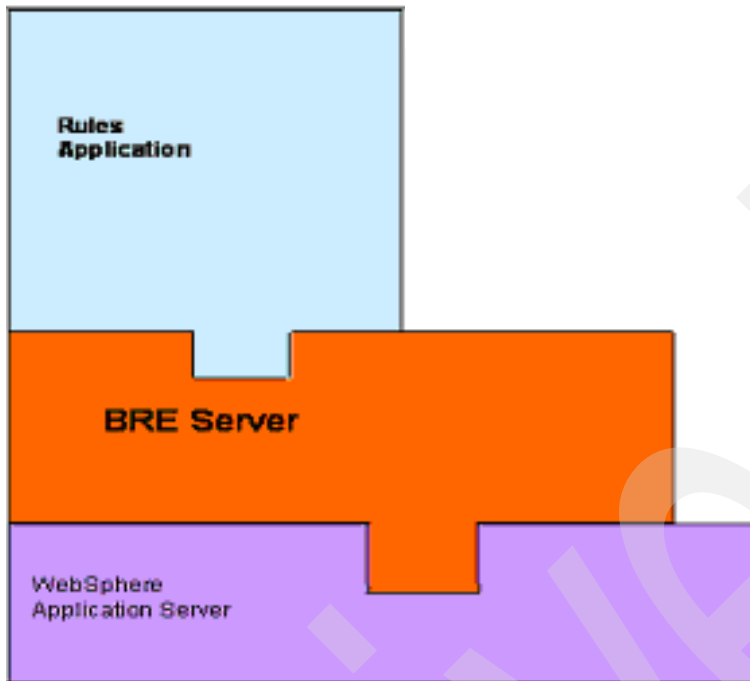
Figure 4-1   Components of a JRules server

DB2 z/OS considerations

JRules requires DB2 definitions contained in the schema_db2.sql member, provided with the product in the /ilog/jRules512/j2ee/databases/db2 directory structure. For z/OS, this SQL needs to have appropriate JCL wrapped around it for execution. Example 4-1 contains sample JCL.

Example 4-1

```
//BRDRDEF    JOB MSGLEVEL=1,CLASS=A,MSGCLASS=H,
//    REGION=0M,NOTIFY=&SYSUID
//****************************************
//*         EXECUTE SQL IN BATCH JOB          *
//****************************************
//JOBLIB  DD  DISP=SHR,DSN=DBT.SDSNLOAD
//STEP1   EXEC PGM=IKJEFT01,DYNAMNBR=20
//SYSTSPRT DD  SYSOUT=*
//SYSPRINT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
//SYSTSIN DD  *
  DSN SYSTEM(DBT1)
  RUN PROGRAM(DSNTIAD)  PLAN(DSNTIA81) PARM('RC0') -
      LIBRARY('DBTG.RUNLIB.LOAD')
  END
//SYSIN    DD *
  SET CURRENT RULES='STD' ;
  SET CURRENT SQLID='<user-ID that owns DB2 database>' ;
```

In addition, when you create a database with DB2 on z/OS, a fourth BRESDATA index needs to be defined. So, at the top of the SQL, a DROP INDEX statement must be added for BRESDATA_IDX_4, along with a statement that says: CREATE UNIQUE INDEX BRESDATA_IDX_4 ON BRESDATA (ID); place this at the bottom of the SQL where all the indexes are defined.

JRules WebSphere Application Server specifications

During the deployment of the BRE Server EAR file, use the following values in the corresponding fields on the WebSphere Application Server Administration Console.

☐ **Application name:** *BRES*

☐ **JDBC and Data Source specifications:**

   – DBC Provider: *DB2 Universal JDBC Provider*

   – JDBC Provider Name: *DB2 Universal JDBC Provider for BRES*

   – Data Source Name: *bresdatasource*

   – JNDI Name: *jdbc/bresdatasource*

   – JNDI Name for XU connectionfactory reference binding *eis/XUConnectionFactory*

   – Database Name: *DBTG*

   – Driver Type: *4*

   – Container Managed Authentication: *Server node name*

   – Server Name (IP Address): *Server IP address*

   – TCP/IP Port: *446*

☐ **Set the following environment variables in the Environment section of the WebSphere Administration Console:**

   – DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH */home/db2inst1/sqllib/lib*

   – DB2UNIVERSAL_JDBC_DRIVER_PATH */home/db2inst1/sqllib/java*

Task 3. Rules application deployment

After the deployment and configuration of the BRE Server, you can deploy a rules application into the same WebSphere Application Server container. A rules application is the executable form of the business rules defined with the JRules Builder. The JRules Builder contains functions which enable you to extract a rules application and deploy it directly into a BRE Server.

To extract and rules application and deploy it into the BRE Server:

☐ **Start the JRules Builder Workbench.**

☐ **Load the business rule to be extracted into the Workbench.**

☐ **Follow the instructions for *Extracting a Rule Application* and *Deploying a RuleApp* that you can find in the JRules documentation.**

Task 4. JRules Server Web service deployment

The rules application is exposed through a Web service and Web service wrapper interface that you must deploy onto the JRules server. Figure 4-2 on page 58 shows the relationship of the Web service and its wrapper to the other JRules server components.
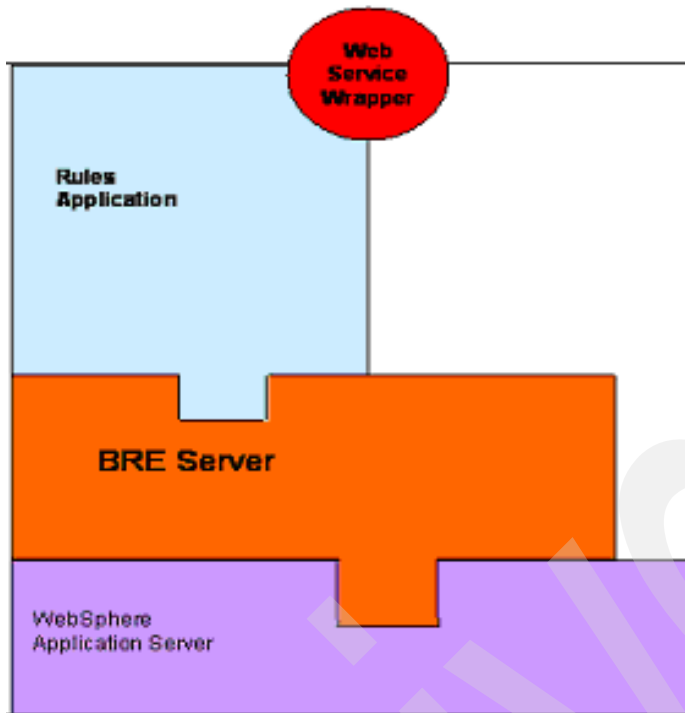
Figure 4-2   Web service and wrapper

☐ **To deploy the Web service and the wrapper on to the JRules Server:**

1. Transfer the Web service EAR file to the JRules server and save it in a temporary directory.

2. From the WebSphere Application Server Administration console:

3. Stop the BRES application.

4. If updating the Web service, stop the Web service application if it is already running.

5. Follow the steps to install or update an EAR file.

6. Specify eis/XUConnectionFactory JNDI name during deployment Step 5, Substep (Apply existing resource JNDI name).

7. Start the BRES application.

8. Start the Web service wrapper application.

5

Entity Analytics Server installation and configuration

This chapter discusses the planning and installation of the Entity Analytic Solution (EAS) component.

59

Product description

Entity Analytic Solution (EAS) is an IBM product that can analyze input manifest files and, based on comparisons with data it has already stored, produce output displaying specific risk relationships that reflect matches with data on file.

Server definition

EAS is included as a separate "stand-alone" piece in this solution—in other words, it is not included in the automated solution that has been verified. It has been tested with input provided by the product's developers and verified to produce the advertised output.

Server hardware

- IBM @server BladeCenter JS20

Server software stack

The EAS server requires the following software:

- AIX 5.3
- DB2 Connect™
- DB2 Relationship Resolution 3.9.1
- HACMP 5.3

z/OS DB2 considerations

The Integrated Border Management Solution Environment as a whole requires a z/OS DB2 back end where output data is recorded in tables. EAS stores user ID and password information in this database as well. In addition, several SQL files are provided with the EAS product, and these must be run against the z/OS DB2 database to provide definitions required to verify the correct installation of the product. These files (CMEAdmin.sql, EAS-Console.sql, and RELRES.sql) include definitions that are referred to during EAS install verification.

Once your DB2 database is created on z/OS, it needs to be defined to, and accessed on, your AIX blades. To perform this task, enter the following commands from a DB2-enabled ID on each blade that requires database access. **Note:** the actual commands and parameters used in prototyping the solution are also included in **bold**).

```
$ db2 catalog tcpip node <node-id you define> remote <z/OS IP-address> server <z/OS DB2
port number>
$ db2 catalog tcpip node DBTG remote 129.40.178.20 server 446
$ db2 catalog database <database name> as <database alias> at node <node-id>
$ db2 catalog database BORDERDB as BORDERDB at node DBTG
$ db2 catalog dcs database <database name> as <z/OS DB2 location name>
$ db2 catalog dcs database BORDERDB as DBTG
$ db2 connect to <database name> user <valid z/OS TSO user> using <valid z/OS TSO password>
$ db2 connect to BORDERDB user <TSO user-ID> using <insert password here>
```

Reference to product installation information

Refer to documentation materials received with the EAS product for specific installation instructions.

Task 1. EAS installation

RELRES 3.9.1 Build 17

Follow the documented process to install this product, providing input parameters as specified below to accommodate definition of the z/OS DB2 back-end environment.

For purposes of this sample, EAS 3.9.1 RELRES code was downloaded and stored in the /scratch/kenjm/EAS391 directory.

- Create the directory to which you will direct the RELRES installation and set the ownership

  ```
  $ mkdir /usr/opt/eas_3.9.1
  $ chown easadmin:easadmin /usr/opt/eas_3.9.1
  ```

- Set easadmin's password to `paidbcd`. You need it for the RR installation.

  ```
  $ passwd easadmin
  ```

- Exit the system and log in as `easadmin`. When prompted to set the password, enter `paidbcd` again.

- Add *bcdhost* entry to /etc/hosts. You can substitute your own hostname here.

- Add entry for *bcdhost* in /etc/hosts to the IP address of the current machine.

> **Important:** Perform the rest of this installation using the easadmin ID. If you SU, then use 'SU –' so that AIX reflects the correct install user ID.

- Change the DB2 environment to the 32-bit DB2 instance since EAS is a 32-bit application and requires the 32-bit DB2 libraries.

  ```
  $ . ~db2i32/sqllib/db2profile
  ```

- Set the following Environment variables.

  ```
  $ export JAVA_HOME=/usr/java14
  $ export DB2DIR=~db2i32/sqllib
  ```

- Go to where you saved the EAS RELRES installer, for example:

  ```
  $ cd /scratch/kenjm/EAS391
  ```

The GUI installer was not used in this sample.

If you need to install using the same options multiple times, you can capture your selections by using the *options-record* option and direct the options selected to a file.

To replay/redo the installation using the options captured during the previous install, you can use the following command:

```
$ RELRES_aix_ppc.bin -silent -options {filename where you wrote the options to}
```

This will re-run the installer with no output to the screen but using your previous options.

Legend for symbols used below:

- *Informational* text—*italics*

- Accept default values shown in brackets [ ] and press Enter—normal text

- Key in **this data** (non-default values)—**bold** type

☐ **$ RELRES_aix_ppc.bin —console**

```
InstallShield Wizard
Initializing InstallShield Wizard...
Searching for Java(tm) Virtual Machine...
--------------------------------------------------------------------------------
Welcome to the InstallShield Wizard for IBM EAS Relationship Resolution
The InstallShield Wizard will install IBM EAS Relationship Resolution on your
computer.
To continue, choose Next.
IBM EAS Relationship Resolution
IBM
http://www.ibm.com
```

☐ **Press 1 for Next, 3 to Cancel or 4 to Redisplay [1]**

```
--------------------------------------------------------------------------------
Software Licensing Agreement

Press Enter to display the license agreement on your screen. Please
read the agreement carefully before installing the Program. After
 reading the agreement, you will be given the opportunity to accept it
 or decline it. If you choose to decline the agreement, installation
 will not be completed and you will not be able to use the Program.

International Program License Agreement

   Part 1 - General Terms

   BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING
     THE PROGRAM YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU
     ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A
     COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT
     THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY,
     OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT AGREE TO
     THESE TERMS,

- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE
     PROGRAM; AND

- PROMPTLY RETURN THE PROGRAM AND PROOF OF ENTITLEMENT TO
     THE PARTY FROM WHOM YOU ACQUIRED IT TO OBTAIN A REFUND OF
     THE AMOUNT YOU PAID. IF YOU DOWNLOADED THE PROGRAM, CONTACT
     THE PARTY FROM WHOM YOU ACQUIRED IT.

"IBM" is International Business Machines Corporation or one
     of its subsidiaries.

"License Information" ("LI") is a document that provides
     information specific to a Program. The Program's LI is
     available at http://www.ibm.com/software/sla/. The LI may
     also be found in a file in the Program's directory, by the
     use of a system command, or as a booklet which accompanies
     the Program.
Press Enter to continue viewing the license agreement, or, Enter 1 to accept the agreement,
2 to decline it, or 99 to go back to the previous screen.
```

☐ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

```
Please read the information below.
Please reference the EAS Product Installation Guide for software and hardware requirements,
prerequisite installation instructions and a step by step guide to the install process.
```

☐ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

Select the features for "IBM EAS Relationship Resolution" you want to install:

● IBM EAS Relationship Resolution

To select/deselect a feature or to view its children, type its number:

1. [x] Relationship Resolution Pipeline
2. [x] EAS Console
3. [x] CME (Central Messaging Engine) Admin
4. [x] EAS Visualizer
5. [x] EAS Web Services

Other options:

0. Continue installing

☐ **Enter command [0]**

☐ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

IBM EAS Relationship Resolution Install Location

Please specify a directory or press Enter to accept the default directory.

☐ **Directory Name: [/opt/IBM/EAS/RELRES] /usr/opt/eas_3.9.1 (*this must ALREADY exist*)**

☐ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

Please select your database type from the list below:

Database type:

```
[ ] 1 - DB2
[X} 2 – DB2 for z/OS
[ ] 3 - Oracle
```

☐ **To select an item enter its number, or 0 when you are finished: [0]**

☐ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

The path to the directory containing the JDBC driver Jar files

☐ **Location of the JDBC driver file(s) [] /usr/opt/db2i32/sqllib/java**

Make sure you pick the 32-bit libs

☐ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

Pipeline Database Settings (DB2)

☐ **Database Server / Hostname [] bcdhost**

Note: This must appear in your etc/hosts file, associated with the IP address of the z/OS system where the DB2 database referred to below resides.

☐ **Database Name [] DBTG**

This is the DB2 LOCATION NAME for the z/OS DB2 system, used above in the CATALOG DCS DATABASE command.

☐ **Username [] (valid TSO user ID on your z/OS system, in CAPS)**

☐ **Password:** *(valid password for TSO user ID—will not be displayed)*

☐ **Database Port [50000] 446**

To determine the database port, execute the NETSTAT command on the z/OS system and use the DB2 port displayed in the resulting list.

☐ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

CME Admin Database Settings (DB2)

☐ **Database Server / Hostname [bcdhost]**

☐ **Database Name [] DBTG**

This is the DB2 LOCATION NAME for the z/OS DB2 system, used above in the CATALOG DCS DATABASE command.

☐ **Username *[<saved valid TSO user-ID>]***

☐ **Password:** *(valid password for TSO user-ID —will not be displayed)*

☐ **Database Port [50000] 446**

Do a NETSTAT on the z/OS system and use the DB2 port displayed in the resulting list.

☐ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

EAS Console Database Settings (DB2)

☐ **Database Server / Hostname [bcdhost]**

☐ **Database Name [] DBTG**

This is the DB2 LOCATION NAME for the z/OS DB2 system, used above in the CATALOG DCS DATABASE command.

☐ **Username *[<saved valid TSO user-ID>]***

☐ **Password:** *<valid password for TSO user-ID – will not be displayed>*

☐ **Database Port [50000]   446**

Do a NETSTAT on the z/OS system and use the DB2 port displayed in the resulting list.

☐ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

CME Admin Transport - Would you like to specify the transport source used by the CME Admin at this time? If you choose not to, you can add it manually, or specify it during initialization of the CME Admin node.

Create CME Admin Transports?

```
[X] 1 - Yes
[ ] 2 - No
```

☐ **To select an item enter its number, or 0 when you are finished: [0]   2**

```
[ ] 1 - Yes
[X] 2 - No
```

☐ **To select an item enter its number, or 0 when you are finished: [0]**

☐ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

Pipeline Transports - Would you like to specify the transport mechanisms used by the Pipeline at this time? If you choose not to, you can add them manually, or specify them during initialization of the Pipeline node.

Create Pipeline Input Transports?

```
[X] 1 - Yes
[ ] 2 - No
```

☐ **To select an item enter its number, or 0 when you are finished: [0]**

☐ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

Please define which transport mechanisms you want to use for Pipeline Input Transports.

Input Transport Modes

```
[ ] 1 - HTTP
[ ] 2 - File
[ ] 3 - Database
[ ] 4 - Message Queue (MQ Series or MSMQ)
```

☐ **To select an item enter its number, or 0 when you are finished: [0]   1**

```
[X] 1 - HTTP
[ ] 2 - File
[ ] 3 - Database
[ ] 4 - Message Queue (MQ Series or MSMQ)
```

☐ **To select an item enter its number, or 0 when you are finished: [0]**

☐ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

Please specify the HTTP Transport source for your Pipeline Input Transport.

☐ **HTTP Transport url: http:// [] washost:8888**

Note: *washost* must be defined in your AIX blade's etc/hosts file, pointing to the IP address of the blade onto which you are installing EAS

☐ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

Please select yes below if you are using a Group 1 server. Group 1 is an address standardization product supplied by Group 1 Software, Inc.

Are you using Group1?

```
[X] 1 - Yes
[ ] 2 - No
```

☐ **To select an item enter its number, or 0 when you are finished: [0]   2 (*You can change this later*)**

```
[ ] 1 - Yes
[X] 2 - No
```

☐ **To select an item enter its number, or 0 when you are finished: [0]**

☐ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

Please enter the SNMP Agent listener port.

☐ **SNMP Agent Port [13516]**

☐ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

Do you want to use full sequential history tracking?

Include sequence tracking?

```
[ ] 1 - Yes
[ ] 2 - No
```

☐ **To select an item enter its number, or 0 when you are finished: [0]   1**

```
[X] 1 - Yes
```

```
                                [ ] 2 - No
```
□ **To select an item enter its number, or 0 when you are finished: [0]**

□ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

WebSphere requires the fully qualified domain name of the installation computer (for example, "host.name.ibm.com"). Please enter this value below.

□ **Fully Qualified Domain Name []   washost**

Note: *washost must be defined in your AIX blade's /etc/hosts file, pointing to the IP address of the blade onto which you are installing EAS*

□ **WebSphere deployment memory (in MB) [1024]**

□ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

Please fill out the following configuration parameters for your CME Admin node.

   □ **Routes Tries [3]**

   □ **Routes Pause [3000]**

   □ **Error Pause (sec.) [0]**

   □ **Error Limit [10]**

   □ **Error Reset Interval [1440]**

   Log All UMF Exceptions

```
   [X] 1 - Yes
   [ ] 2 - No
```

□ **To select an item enter its number, or 0 when you are finished: [0]**

   Stop On All UMF Exception

```
   [ ] 1 - Yes
   [X] 2 - No
```

□ **To select an item enter its number, or 0 when you are finished: [0]**

   RemergeReplication

```
   [ ] 1 - Yes
   [X] 2 - No
```

□ **To select an item enter its number, or 0 when you are finished: [0]**

□ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

Choose how the EAS Console authenticates users.

   Console authentication type

```
   [X] 1 - File Authentication
   [ ] 2 - SQL Authentication
```

□ **To select an item enter its number, or 0 when you are finished: [0]   2**

```
   [ ] 1 - File Authentication
   [X] 2 - SQL Authentication
```

□ **To select an item enter its number, or 0 when you are finished: [0]**

□ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

Enter the WebSphere port numbers:

   □ **Web server port number (http) [13510]**

□ **Secure Web server port number (https) [13511]**

□ **Administration port number (http) [13512]**

□ **Secure administration port number (https) [13513]**

□ **SOAP port number [13514]**

□ **Application server port number [13515]**

□ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

How would you like to create your database schemas?

Automatic	Will create the schemas and tables for you in your database(s).
Advanced	Will generate the SQL necessary to create the schema(s) and write it to a plain text file (one per database).
Nothing	Do nothing at this time.

```
[X] 1 - Automatic
[ ] 2 - Advanced
[ ] 3 - Nothing
```

□ **To select an item enter its number, or 0 when you are finished: [0]**

□ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

IBM EAS Relationship Resolution will be installed in the following location: /usr/opt/eas_3.9.1
with the following features:

● Relationship Resolution Pipeline
● EAS Console
● CME (Central Messaging Engine) Admin
● EAS Visualizer
● EAS Web Services

For a total size of 550 MB

□ **Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]**

```
Installing IBM EAS Relationship Resolution. Please wait...

|----------|----------|----------|----------|

0%      25%      50%      75%      100%

||||||||||||||||||||||||||||||||||||||||||||||

Please read the information below.
Release Notes ----------------
Note: Points to release notes, and actually prints some 'last minute notes' at this
point
```

□ **Press 1 for Next, 3 to Cancel or 4 to Redisplay [1]**

```
The InstallShield Wizard has successfully installed IBM EAS Relationship <- Good
message to see
```

Resolution: Choose **Next** to continue the wizard.

□ **Press 3 to Finish or 4 to Redisplay [3]**

Task 2. Prepare for Web services

You must have a pipeline running as a Web service for the Visualizer. Therefore, create
another ini file just for this purpose.

□ **$ cd /usr/opt/eas_3.9.1/bin**

☐ **$ cp pipeline.ini wspipeline.ini**

☐ **$ vi pipeline.ini**   *and change the entry for InputTransport*

From:

InputTransport=http://localhost:8888

To:

InputTransport=

Task 3. Validate the installation

You can validate the installation by running the pipeline. You will need a copy of the testall_39.xml file that is available in the EAS-ITS teamroom Section 4.2:

☐ **$ cd /usr/opt/eas_3.9.1/bin**

☐ **$ export LIBPATH=${LIBPATH}:/usr/opt/eas_3.9.1/lib**

☐ **$ ./pipeline -d -f ??/testall_39.xml**

  # ?? is wherever you put the testall_39.xml

To validate that Web services is working properly,

☐ **$ cd /usr/opt/eas_3.9.1**

☐ **$ stopEAS.sh**

☐ **$ startEAS.sh**

☐ **$ /usr/opt/eas_3.9.1/bin/pipeline -s -n wspipeline –c /usr/opt/eas_3.9.1/bin/wspipeline.ini**

☐ **$ cd /usr/opt/eas_3.9.1/was_ee/webservice**

☐ **$ $JAVA_HOME/bin/java -jar wsutil.jar --load=http://localhost:13510/easws/services/SRDWebService --input=??/testall_39.xml**

Note: This is all one continuous line (wsutil.jar –load, etc.). Replace the ?? with testall_39.xml

Task 4. Accessing EAS

Once the installation has been validated, enter the IP address of the EAS server with port number 13510 (for example, 129.40.10.105:13510) on a browser. This displays the Relationship Resolution screen. Click the selection that causes the EAS Relationship Resolution code to be downloaded to your client machine. Valid sample user IDs are "admin" and "user", with a sample password of "password". Once logged on, XML manifests can be imported and analyzed. Refer to existing EAS product information for usage instructions.

Enter the IP address of the EAS server with port 13510/console (for example, 129.40.10.105:13510/console) on a browser. This displays the Relationship Resolution console. The user ID and password are whatever was specified during the install steps above. Again, refer to existing product documentation for usage instructions.

6

HACMP configuration

High Availability Cluster Multi-Processing (HACMP) is the solution for the application downtime—downtime that is not caused by processor failures. HACMP helps avoid downtime, enables prompt recovery from any hardware, network and application failures, and allows for taking down an individual server for planned maintenance and upgrades without having to take down the entire cluster. This chapter discusses the configuration of HACMP.

Product description

Most application outages are caused not by hardware failures but by network, application, or external causes. For over a decade, IBM High Availability Cluster Multi-Processing (HACMP) has provided reliable high availability services, monitoring customers' pSeries servers and network connections and dependably performing application failover to backup servers.

Clusters overview
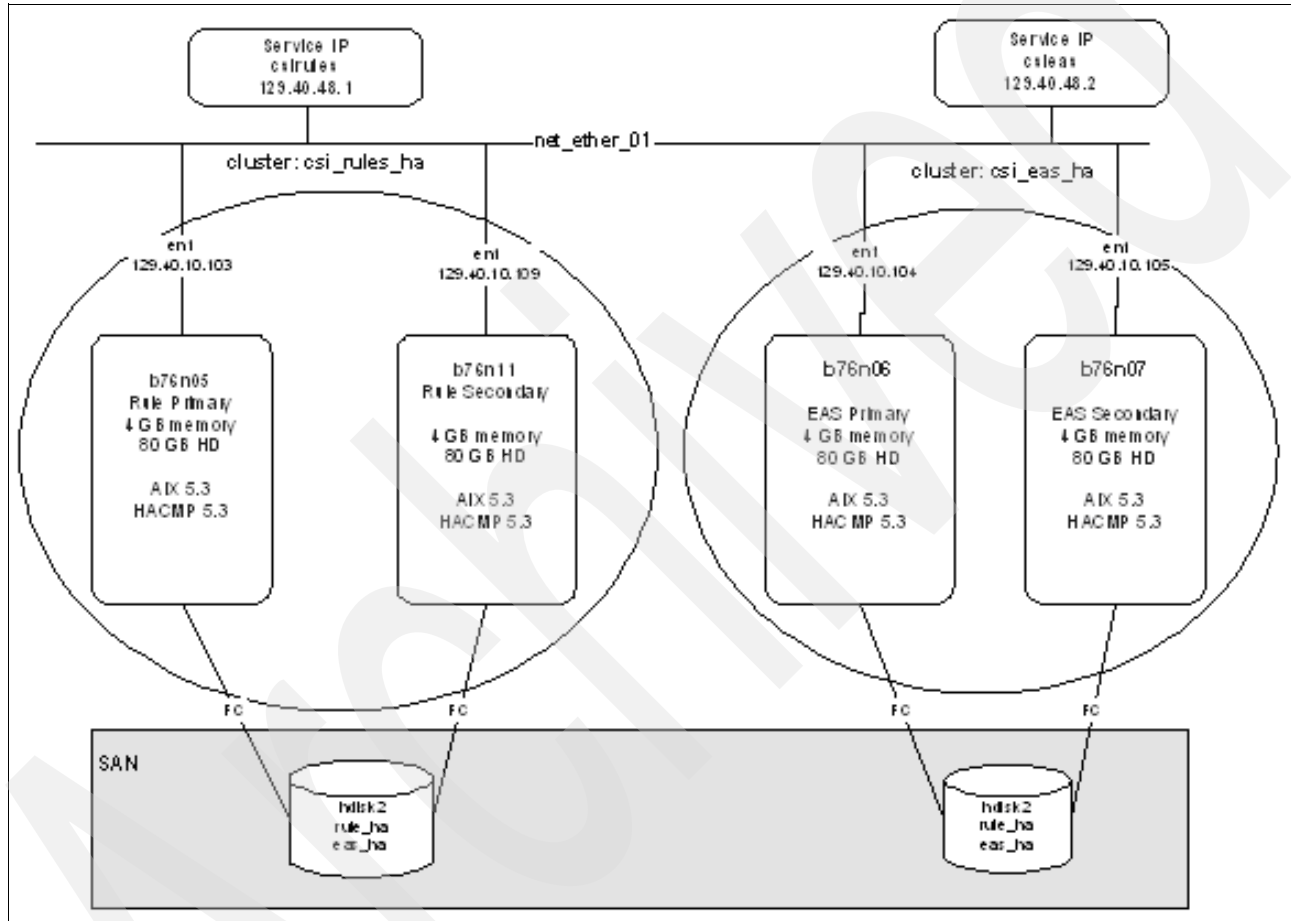
Figure 6-1   Overview

JRules cluster

This cluster consists of two JS20 blades servers as shown above.

The IP heartbeat is the Ethernet network en1 and the non-IP heartbeat is done with a shared disk within the Storage Area Network (SAN).

The service IP for the JRules cluster is named csirules.

Task 1: Configure JRules cluster topology

☐ **Log on to the JRules Blade Server as root or an equivalent user ID with root authority.**

☐ **Enter: smitty hacmp**

```
                              HACMP for AIX
Move cursor to desired item and press Enter.
  Initialization and Standard Configuration

 ‡ Extended Configuration

  System Management (C-SPOC)
  Problem Determination Tools
```

☐ **Select: Extended Configuration**

```
                        Extended Configuration
Move cursor to desired item and press Enter.
  Discover HACMP-related Information from Configured Nodes
 → Extended Topology Configuration
  Extended Resource Configuration
  Extended Cluster Service Settings
  Extended Event Configuration
  Extended Performance Tuning Parameters Configuration
  Security and Users Configuration
  Snapshot Configuration
  Export Definition File for Online Planning Worksheets
  Extended Verification and Synchronization
  HACMP Cluster Test Tool
```

☐ **Select: Extended Topology Configuration**

```
                       Extended Topology Configuration
Move cursor to desired item and press Enter.
  Configure an HACMP Cluster
  Configure HACMP Nodes
  Configure HACMP Sites
  Configure HACMP Networks
  Configure HACMP Communication Interfaces/Devices
  Configure HACMP Persistent Node IP Label/Addresses
  Configure HACMP Global Networks
  Configure HACMP Network Modules
  Configure Topology Services and Group Services
  Show HACMP Topology
```

☐ **The following steps are to assign the cluster name:**

   Select: Configuration an HACMP Cluster

   Select: Add/ Change/Show an HACMP Cluster

   Enter the required Cluster Name: **csi_rules_ha**

☐ **The next step is to assign the nodes or servers to the cluster:**

   Select: Configuration an HACMP Nodes

   Select: Add a Node to HACMP Cluster and enter your server names.

- ☐ **Network Configuration for the cluster:**

    Select: Configuration an HACMP Networks

    Select: Add a Network to the HACMP Cluster

    Select: **net_diskhb_01** for heartbeat network and **net_ether_01** for Ethernet

- ☐ **Configure HACMP Communication Interfaces/Devices:**

    Select: **hdisk2** for heartbeat devices and **en1** for Ethernet for both b76n05 and b76n11 servers.

- ☐ **You can review the cluster topology using the follow steps.**

    Enter: `smitty hacmp`

    Select: Extended Configuration

    Select: Display HACMP Configuration

    The following information displays:

```
                          COMMAND STATUS
Command: OK              stdout: yes              stderr: no
Before command completion, additional instructions may appear below.
[TOP]
Cluster Name: csi_rules_ha
Cluster Connection Authentication Mode: Standard
Cluster Message Authentication Mode: None
Cluster Message Encryption: None
Use Persistent Labels for Communication: No
NODE b76n05:
        Network net_diskhb_01
        Network net_diskhb_02
                b76n05_hdisk2_01         /dev/hdisk2
        Network net_ether_01
                csirules         129.40.48.1
                b76n05  129.40.10.103
NODE b76n11:
        Network net_diskhb_01
        Network net_diskhb_02
                b76n11_hdisk2_01         /dev/hdisk2
        Network net_ether_01
                csirules         129.40.48.1
                b76n11  129.40.10.109

[BOTTOM]
```

Task 2: Configure JRules cluster resource

- ☐ **Log on to the JRules Blade Server as root or an equivalent user ID with root authority.**

- ☐ **Enter: smitty hacmp**

```
                          HACMP for AIX
Move cursor to desired item and press Enter.
  Initialization and Standard Configuration
→ Extended Configuration
  System Management (C-SPOC)
  Problem Determination Tools
```

☐ **Select: Extended Configuration**

```
                        Extended Configuration
Move cursor to desired item and press Enter.
  Discover HACMP-related Information from Configured Nodes
  Extended Topology Configuration
→ Extended Resource Configuration
  Extended Cluster Service Settings
  Extended Event Configuration
  Extended Performance Tuning Parameters Configuration
  Security and Users Configuration
  Snapshot Configuration
  Export Definition File for Online Planning Worksheets


  Extended Verification and Synchronization
  HACMP Cluster Test Tool
```

☐ **Select: Extended Resource Configuration**

☐ **Select: HACMP Extended Resource Configuration**

```
                     Extended Resource Configuration
Move cursor to desired item and press Enter.
 → HACMP Extended Resources Configuration
   Configure Resource Group Run-Time Policies
   HACMP Extended Resource Group Configuration
```

```
                  HACMP Extended Resources Configuration
Move cursor to desired item and press Enter.
  Configure HACMP Applications
  Configure HACMP Service IP Labels/Addresses
  Configure HACMP Tape Resources
  Configure HACMP Communication Adapters and Links
  Configure Custom Disk Methods
  Configure Custom Volume Group Methods
  Configure Custom Filesystem Methods
  Customize Resource Group and Resource Recovery
  Configure Resource Distribution Preferences
```

☐ **Select: Configure HACMP Service IP Labels/ Addresses**

☐ **Select: Add a Service IP Label / Address and make sure to configure for multiple nodes type.**

```
                         Configure HACMP Service IP Labels/Addresses
     Move cursor to desired item and press Enter.
       Add a Service IP Label/Address
       Change/Show a Service IP Label/Address
       Remove Service IP Label(s)/Address(es)


        lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
      x                     Select a Service IP Label/Address type            x
      x                                                                       x
      x Move cursor to desired item and press Enter.                          x
      x                                                                       x
      x  →Configurable on Multiple Nodes                                      x
      x    Bound to a Single Node                                             x
      x                                                                       x
```

☐ **Add the csirules name for the IP Label**

☐ **You can verify as follows.**

```
                Change/Show a Service IP Label/Address (extended)
Type or select values in entry fields.
Press Enter AFTER making all desired changes.


                                                  [Entry Fields]
* IP Label/Address                                csirules
  New IP Label/Address                            []                        +
* Network Name                                    [net_ether_01]            +
  Alternate HW Address to accompany IP Label/Address []
```

☐ **Select: HACMP Extended Resource Group Configuration**

☐ **Select: Add a Resource Group and enter the resource group name.**

☐ **You can verify the resource group as follows.**

```
                    Change/Show a Resource Group
Type or select values in entry fields.
Press Enter AFTER making all desired changes.


                                                  [Entry Fields]
 Resource Group Name                              csi_rules_rg1
 New Resource Group Name                          []
 Participating Nodes (Default Node Priority)      [b76n05 b76n11]           +

 Startup Policy                                   Online On Home Node O> +
 Fallover Policy                                  Fallover To Next Prio> +
 Fallback Policy                                  Fallback To Higher Pr> +
```

☐ **Select: Change / Show Resources and Attributes for a Resource Group.**

Enter the information as follows:

```
        Change/Show All Resources and Attributes for a Resource Group
Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                           [Entry Fields]
  Resource Group Name                           csi_rules_rg1
  Participating Nodes (Default Node Priority)    b76n05 b76n11

  Startup Policy                                Online On Home Node O>
  Fallover Policy                               Fallover To Next Prio>
  Fallback Policy                               Fallback To Higher Pr>
  Fallback Timer Policy (empty is immediate)    []                          +

  Service IP Labels/Addresses                   [csirules]                  +
  Application Servers                           []                          +

  Volume Groups                                 []                          +
  Use forced varyon of volume groups, if necessary  false                  +
  Automatically Import Volume Groups             false                      +
  Filesystems (empty is ALL for VGs specified)   []                         +
  Filesystems Consistency Check                  fsck                       +
  Filesystems Recovery Method                    sequential                 +
  Filesystems mounted before IP configured       false                      +
  Filesystems/Directories to Export              []                         +
                                                                            +
  Filesystems/Directories to NFS Mount           []
  Network For NFS Mount                          []                         +

  Tape Resources                                 []                         +
  Raw Disk PVIDs                                 []                         +

  Fast Connect Services                          []                         +
  Communication Links                            []                         +

  Primary Workload Manager Class                 []                         +
  Secondary Workload Manager Class               []                         +

  Miscellaneous Data                             []
[BOTTOM]
```

Task 3: Verifying and synchronizing the JRules cluster

☐ **Log on to the JRules Blade Server as root or an equivalent user ID with root authority.**

☐ **Enter: smitty hacmp**

☐ **Select: Extended Configuration**

☐ **Select: Extended Verification and Synchronization**

```
      HACMP Verification and Synchronization (Active Cluster Nodes Exist)
Type or select values in entry fields.
Press Enter AFTER making all desired changes.


                                               [Entry Fields]
* Emulate or Actual                            [Actual]                +
* Verify changes only?                         [No]                    +
* Logging                                      [Standard]              +
```

You should review the warnings and the result of the verification, which displays as follows.

```
                            COMMAND STATUS
Command: OK              stdout: yes            stderr: no
Before command completion, additional instructions may appear below.
[MORE...13]
WARNING: There may be an insufficient number of communication interfaces defined
on node: b76n11, network: net_ether_01. Multiple communication interfaces are
recommended for networks that will use IP aliasing.
Verifying Cluster Resources...
Verification has completed normally.
[BOTTOM]
```

Task 4: Start JRules cluster

Log on to the JRules Blade Server as **root** or an equivalent user ID with root authority.

☐ **Enter: smitty hacmp**

☐ **Select: System Management (C-SPOC)**

☐ **Select: Manage HACMP Services**

☐ **Select: Start Cluster Services**

You can start both servers of the cluster at the same time.

```
                          Start Cluster Services
Type or select values in entry fields.
Press Enter AFTER making all desired changes.


                                               [Entry Fields]
* Start now, on system restart or both          now                    +
  Start Cluster Services on these nodes         [b76n05,b76n11]         +
  BROADCAST message at startup?                 false                  +
  Startup Cluster Information Daemon?           true                   +
  Reacquire resources after forced down?        false                  +
  Ignore verification errors?                   false                  +
  Automatically correct errors found during     Interactively          +
  cluster start?
```

Task 5: Stop JRules cluster

☐ **Log on to the JRules Blade Server as root or an equivalent user ID with root authority.**

☐ **Enter: smitty hacmp**

☐ **Select: System Management (C-SPOC)**

☐ **Select: Manage HACMP Services**

☐ **Select: Stop Cluster Services**

```
                      Stop Cluster Services
Type or select values in entry fields.
Press Enter AFTER making all desired changes.


                                              [Entry Fields]
* Stop now, on system restart or both         now                   +
  Stop Cluster Services on these nodes         [b76n05]              +
  BROADCAST cluster shutdown?                  true                  +
* Shutdown mode                                graceful              +
```

Task 6: Show cluster services

☐ **Log on to the JRules Blade Server as root or an equivalent user ID with root authority.**

☐ **Enter: smitty hacmp**

☐ **Select: System Management (C-SPOC)**

☐ **Select: Manage HACMP Services**

☐ **Select: Show Cluster Services to view that status of the subsystems.**

```
                        COMMAND STATUS
Command: OK            stdout: yes            stderr: no
Before command completion, additional instructions may appear below.
[TOP]
Status of the RSCT subsystems used by HACMP:
Subsystem        Group         PID          Status
 topsvcs         topsvcs       1015880      active
 grpsvcs         grpsvcs       1069146      active
 grpglsm         grpsvcs                    inoperative
 emsvcs          emsvcs        1040516      active
 emaixos         emsvcs        1044562      active
 ctrmc           rsct          225426       active
Status of the HACMP subsystems:
Subsystem        Group         PID          Status
 clcomdES        clcomdES      278666       active
 clstrmgrES      cluster       512066       active
Status of the optional HACMP subsystems:
Subsystem        Group         PID          Status
 clinfoES        cluster       1011828      active


[BOTTOM]
```

Task 7: Check for service IP of the JRules cluster

You can verify a successful operation of the cluster manager by checking for the service IP of the cluster using the following command.

```
b76n05:/ # netstat -ni
Name  Mtu    Network      Address            Ipkts Ierrs    Opkts Oerrs  Coll
en1   1500   link#2       0.d.60.1e.e3.2b    9265977   0  5933372   0    0
en1   1500   129.40.10    129.40.10.103      9265977   0  5933372   0    0
en1   1500   129.40.48    129.40.48.1        9265977   0  5933372   0    0
lo0   16896  link#1                          27449564  0 27626804   0    0
lo0   16896  127          127.0.0.1          27449564  0 27626804   0    0
lo0   16896  ::1                             27449564  0 27626804   0    0
```

Note that the *en1* with the IP address 129.40.48.1 is the service IP of the cluster that clients of the operating JRules server use.

Task 8: Takeover with shutdown mode

You can stop a server and verify the IP takeover as follows.

```
                        Stop Cluster Services
Type or select values in entry fields.
Press Enter AFTER making all desired changes.


                                            [Entry Fields]
* Stop now, on system restart or both        now                    +
  Stop Cluster Services on these nodes       [b76n05]                +
  BROADCAST cluster shutdown?                true                   +
* Shutdown mode                              takeover               +
```

EAS servers cluster

This cluster consists of two JS20 blades servers as shown in Figure 6-1 on page 70.

The IP heartbeat is the Ethernet network en1 and the non-IP heartbeat is done with a shared disk within the Storage Area Network (SAN).

The service IP for the EAS cluster is named csieas.

Task 1: Configure EAS cluster topology

☐ **Log on to the EAS Blade Server as root or an equivalent user ID with root authority.**

☐ **Enter: smitty hacmp**

☐ **Select: Extended Configuration**

☐ **Select: Extended Topology Configuration**

The following steps are to assign the cluster name.

Select: Configuration an HACMP Cluster

Select: Add/ Change/Show an HACMP Cluster

Enter the required Cluster Name: **eas_ha**

The next step is to assign the nodes or servers to the cluster

Select: Configuration an HACMP Nodes

Select: Add a Node to HACMP Cluster and enter your server names.

Network Configuration for the cluster

Select: Configuration an HACMP Networks

Select: Add a Network to the HACMP Cluster

Select: **net_diskhb_01** for heartbeat network and **net_ether_01** for Ethernet

Configure HACMP Communication Interfaces/Devices

Select: **hdisk2** for heartbeat devices and **en1** for Ethernet for both b76n06 and b76n07 servers.

You can review the cluster topology using the follow steps.

□ **Enter: smitty hacmp**

□ **Select: Extended Configuration**

□ **Select: Display HACMP Configuration**

```
                          COMMAND STATUS
Command: OK            stdout: yes            stderr: no
Before command completion, additional instructions may appear below.
[TOP]
Current cluster configuration:
Cluster Name: eas_ha_130
Cluster Connection Authentication Mode: Standard
Cluster Message Authentication Mode: None
Cluster Message Encryption: None
Use Persistent Labels for Communication: No
There are 2 node(s) and 3 network(s) defined
NODE b76n06:
        Network net_diskhb_01
        Network net_diskhb_02
                b76n06_hdisk2_01        /dev/hdisk2
        Network net_ether_01
                csieas  129.40.48.2
                b76n06  129.40.10.104
NODE b76n07:
        Network net_diskhb_01
        Network net_diskhb_02
                b76n07_hdisk2_01        /dev/hdisk2
        Network net_ether_01
                csieas  129.40.48.2
                b76n07  129.40.10.105


Resource Group eas_ha
        Startup Policy   Online On Home Node Only
        Fallover Policy  Fallover To Next Priority Node In The List
        Fallback Policy  Fallback To Higher Priority Node In The List
        Participating Nodes      b76n06 b76n07
        Service IP Label                  csieas
[BOTTOM]
```

Task 2: Configure EAS cluster resource

☐ **Log on to the EAS Blade Server as root or an equivalent user ID with root authority.**

☐ **Enter: smitty hacmp**

☐ **Select: Extended Configuration**

```
                      Extended Resource Configuration
Move cursor to desired item and press Enter.
  HACMP Extended Resources Configuration
  Configure Resource Group Run-Time Policies
  HACMP Extended Resource Group Configuration
```

☐ **Select: Extended Resource Configuration**

```
                     HACMP Extended Resources Configuration
Move cursor to desired item and press Enter.
  Configure HACMP Applications
  Configure HACMP Service IP Labels/Addresses
  Configure HACMP Tape Resources
  Configure HACMP Communication Adapters and Links
  Configure Custom Disk Methods
  Configure Custom Volume Group Methods
  Configure Custom Filesystem Methods
  Customize Resource Group and Resource Recovery
  Configure Resource Distribution Preferences
```

☐ **Select: Configure HACMP Service IP Labels/ Addresses**

☐ **Select: Add a Service IP Label / Address**

☐ **Add the csieas name for the IP Label**

☐ **You can verify the Service IP Label as follows.**

```
              Change/Show a Service IP Label/Address (extended)
Type or select values in entry fields.
Press Enter AFTER making all desired changes.


                                               [Entry Fields]
* IP Label/Address                            csieas
  New IP Label/Address                        []                        +
* Network Name                                [net_ether_01]          +
  Alternate HW Address to accompany IP Label/Address []
```

☐ **Select: HACMP Extended Resource Group Configuration**

☐ **Select: Add a Resource Group and enter the follow information.**

```
                   Add a Resource Group (extended)
Type or select values in entry fields.
Press Enter AFTER making all desired changes.


                                              [Entry Fields]
* Resource Group Name                         [eas_rg]
* Participating Nodes (Default Node Priority)  [b76n06 b76n07]        +

  Startup Policy                              Online On Home Node O> +
  Fallover Policy                             Fallover To Next Prio> +
  Fallback Policy                             Fallback To Higher Pr> +
```

☐ **Select: Change / Show Resource and Attributes of a Resource Group**

☐ **Add the resource name and verify as follows.**

```
        Change/Show All Resources and Attributes for a Resource Group
Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                         [Entry Fields]
  Resource Group Name                         eas_rg
  Participating Nodes (Default Node Priority)  b76n06 b76n07

  Startup Policy                              Online On Home Node O>
  Fallover Policy                             Fallover To Next Prio>
  Fallback Policy                             Fallback To Higher Pr>
  Fallback Timer Policy (empty is immediate)  []                        +

  Service IP Labels/Addresses                 [csieas]                  +
  Application Servers                         []                        +

  Volume Groups                               []                        +
  Use forced varyon of volume groups, if necessary  false              +
  Automatically Import Volume Groups          false                     +
  Filesystems (empty is ALL for VGs specified)  []                      +
  Filesystems Consistency Check               fsck                      +
  Filesystems Recovery Method                 sequential                +
  Filesystems mounted before IP configured    false                    +
  Filesystems/Directories to Export           []                        +
                                                                        +
  Filesystems/Directories to NFS Mount        []
  Network For NFS Mount                       []                        +

  Tape Resources                              []                        +
  Raw Disk PVIDs                              []                        +
  Fast Connect Services                       []                        +
  Communication Links                         []                        +

  Primary Workload Manager Class              []                        +
  Secondary Workload Manager Class            []                        +

  Miscellaneous Data                          []
[BOTTOM]
```

Task 3: Verifying and synchronizing the EAS cluster

☐ **Log on to the EAS Blade Server as root or an equivalent user ID with root authority.**

☐ **Enter: smitty hacmp**

☐ **Select: Extended Configuration**

☐ **Select: Extended Verification and Synchronization**

```
        HACMP Verification and Synchronization (Active Cluster Nodes Exist)
Type or select values in entry fields.
Press Enter AFTER making all desired changes.


                                                [Entry Fields]
* Emulate or Actual                             [Actual]                +
* Verify changes only?                          [No]                    +
* Logging                                       [Standard]              +
```

Task 4: Start EAS cluster

☐ **Log on to the EAS Blade Server as root or an equivalent user ID with root authority.**

☐ **Enter: smitty hacmp**

☐ **Select: System Management (C-SPOC)**

☐ **Select: Manage HACMP Services**

☐ **Select: Start Cluster Services**

```
                        Start Cluster Services
Type or select values in entry fields.
Press Enter AFTER making all desired changes.


                                                [Entry Fields]
* Start now, on system restart or both          now                     +
  Start Cluster Services on these nodes         [b76n07]                +
  BROADCAST message at startup?                 true                    +
  Startup Cluster Information Daemon?           true                    +
  Reacquire resources after forced down?        false                   +
  Ignore verification errors?                   false                   +
  Automatically correct errors found during     Interactively           +
  cluster start?
```

Task 5: Stop EAS cluster

☐ **Log on to the EAS Blade Server as root or an equivalent user ID with root authority.**

☐ **Enter: smitty hacmp**

☐ **Select: System Management (C-SPOC)**

☐ **Select: Manage HACMP Services**

☐ **Select: Stop Cluster Services**

```
                       Stop Cluster Services
Type or select values in entry fields.
Press Enter AFTER making all desired changes.


                                              [Entry Fields]
* Stop now, on system restart or both         now                    +
  Stop Cluster Services on these nodes         [b76n07]               +
  BROADCAST cluster shutdown?                  true                   +
* Shutdown mode                                graceful               +
```

Task 6: Show cluster services

☐ **Log on to the EAS Blade Server as root or an equivalent user ID with root authority.**

☐ **Enter: smitty hacmp**

☐ **Select: System Management (C-SPOC)**

☐ **Select: Manage HACMP Services**

☐ **Select: Show Cluster Services to view that status of the Subsystems.**

```
                         COMMAND STATUS
Command: OK            stdout: yes            stderr: no
Before command completion, additional instructions may appear below.
[TOP]
Status of the RSCT subsystems used by HACMP:
Subsystem        Group        PID        Status
 topsvcs         topsvcs      430100     active
 grpsvcs         grpsvcs      348408     active
 grpglsm         grpsvcs                 inoperative
 emsvcs          emsvcs       778278     active
 emaixos         emsvcs       589888     active
 ctrmc           rsct         245920     active
Status of the HACMP subsystems:
Subsystem        Group        PID        Status
 clcomdES        clcomdES     786668     active
 clstrmgrES      cluster      753838     active
Status of the optional HACMP subsystems:
Subsystem        Group        PID        Status
 clinfoES        cluster      659462     active


[BOTTOM]
```

Task 7: Check for service IP of the EAS cluster

You can verify a successful operation of the cluster manager by checking for the service IP of the cluster using the follow command.

```
b76n07:/ # netstat -ni
Name  Mtu    Network      Address          Ipkts Ierrs    Opkts Oerrs  Coll
en1   1500   link#2       0.d.60.1e.de.d9  5926039   0  2488891    0     0
en1   1500   129.40.10    129.40.10.105    5926039   0  2488891    0     0
en1   1500   129.40.48    129.40.48.2      5926039   0  2488891    0     0
lo0   16896  link#1                       13502206   0 13503703    0     0
lo0   16896  127          127.0.0.1       13502206   0 13503703    0     0
lo0   16896  ::1                          13502206   0 13503703    0     0
b76n07:/ #
```

Note that the en1 with the IP address 129.40.48.2 is the service IP of the cluster that clients of the operating EAS server use.

Task 8: Takeover with shutdown mode

You can stop a server and verify the IP takeover as follows.

```
                          Stop Cluster Services
Type or select values in entry fields.
Press Enter AFTER making all desired changes.


                                                [Entry Fields]
* Stop now, on system restart or both           now                    +
  Stop Cluster Services on these nodes          [b76n06]                +
  BROADCAST cluster shutdown?                    true                   +
* Shutdown mode                                  takeover               +
```

Sample /etc/hosts file

A sample /etc/hosts file is attached. The /etc/hosts file for the JRules cluster should be the same as the one for the EAS cluster. See the following figure.

```
# @(#)47        1.1  src/bos/usr/sbin/netstart/hosts, cmdnet, bos520 7/24/91 10:00:46
# IBM_PROLOG_BEGIN_TAG
# This is an automatically generated prolog.
#
# bos520 src/bos/usr/sbin/netstart/hosts 1.1
#
# Licensed Materials - Property of IBM
#
# (C) COPYRIGHT International Business Machines Corp. 1985,1989
# All Rights Reserved
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#
# IBM_PROLOG_END_TAG
#
# COMPONENT_NAME: TCPIP hosts
#
# FUNCTIONS: loopback
#
# ORIGINS: 26  27
#
# (C) COPYRIGHT International Business Machines Corp. 1985, 1989
# All Rights Reserved
# Licensed Materials - Property of IBM
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#
#  /etc/hosts
#
# This file contains the hostnames and their address for hosts in the
# network.  This file is used to resolve a hostname into an Internet
# address.
#
# At minimum, this file must contain the name and address for each
# device defined for TCP in your /etc/net file.  It may also contain
# entries for well-known (reserved) names such as timeserver
# and printserver as well as any other host name and address.
#
# The format of this file is:
# Internet Address        Hostname        # Comments
# Items are separated by any number of blanks and/or tabs.  A '#'
# indicates the beginning of a comment; characters up to the end of the
# line are not interpreted by routines which search this file.  Blank
# lines are allowed.
# Internet Address        Hostname        # Comments
# 192.9.200.1             net0sample      # ethernet name/address
# 128.100.0.1             token0sample    # token ring name/address
# 10.2.0.2                x25sample       # x.25 name/address
127.0.0.1                 loopback localhost     # loopback (lo0) name/address
129.40.10.104    b76n06.pbm.ihost.com     b76n06
129.40.10.103    b76n05.pbm.ihost.com     b76n05
129.40.10.109    b76n11.pbm.ihost.com     b76n11
129.40.10.105    b76n07.pbm.ihost.com     b76n07
129.40.48.2      csieas.pbm.ihost.com     csieas
129.40.106.37    nimserver.pbm.ihost.com
129.40.10.105    washost.pbm.ihost.com    washost
129.40.178.20    bcdhost
```

Reference material

- *The IBM @server BladeCenter JS20*, SG24-6342
- *HACMP Version 5.3 Planning and Installation Guide*, SC23-4861
- *HACMP Version 5.3 Administration Guide*, SC23-4862
- *HACMP Version 5.3 Troubleshooting Guide*, SC23-5177

7

Partition Load Manager configuration

The partition load manager (PLM) server uses a policy file to determine how CPU and memory resources are shared across LPARs. This chapter lists the policy definitions file that we used during our proof of concept.

Product description

Partition Load Manager (PLM) allows the system administrator to dynamically allocate processor and memory resources among logical partitions (LPARs) on a pSeries Power5 system without manual intervention. The allocation of these resources is based on workloads and policies defined by the system administrator. Typically, PLM is set up in a partition or on another system running AIX 5L (Version 5.2 or 5.3).

Server definition

The PLM server uses a policy file to determine how CPU and memory resources are shared across LPARs. The policy also includes resource shares, group definitions, and tunable parameters. This file defines the managed partitions, their guaranteed entitlements, and their minimum and maximum entitlements.

Server hardware

- pSeries Model 595

Server software stack

- AIX 5.3

Reference to product installation information

*Advanced Power Virtualization on IBM @*server *p5 Servers: Introduction and Basic Configuration,* SG24-7940

Task 1: Review policy file concepts

PLM requires a policy file to determine which CPU and memory resources may be managed by the Partition Load Manager server. The policy also includes resource shares, group definitions, and tunable parameters. This file defines the partitions that are to be managed, their guaranteed entitlements, and their minimum and maximum entitlements.

The policy file is divided into stanzas, and each of the stanzas have a type field. Every stanza follows this format:

```
<stanza_label>:
            attribute=<value>
            attribute2=<value>
            type=<value>
```

The policy file has the following format (rules):

- Policy consists of a number of stanzas containing attributes.

- Stanza names may not contain any blanks and must be followed immediately by a colon (:). Nothing but white space or a comment can follow the stanza name. It is suggested that stanza names be placed in column 1 on the line.

The following are the supported stanza types:

   – globals:

   – tunables:

   – group_name:

   – partition_name:

- Attributes consist of a name and a value separated by an equal sign (=). Attribute names and values may not contain any blanks. Nothing but white space or a comment may follow the value. It is suggested that attributes be indented under the containing stanza name.

- Do not repeat attributes in a stanza. Only the first attribute in a stanza is used.

- Comments begin with a pound (#) character. They may be started in any column on the line and continue until end of line.

- Stanzas may be placed in the policy file in any order. However, a suggested order is the following:

   a. globals stanza

   b. tunables stanza

   c. group stanza for first group

   d. partition stanzas for partitions in first group

   e. repeat group/partition stanza for subsequent groups

Review the policy file format rules documented in Chapter 7 in *Advanced Power Virtualization on IBM @server p5 Servers: Introduction and Basic Configuration,* SG24-7940.

Task 2: Create the PLM policy file

☐ **Create the PLM policy file on the PLM server**

1. Edit a new file in directory **/etc/plm/policies/**

2. Enter the policies. Example 7-1 shows the contents of a recommended PLM policy for an Integrated Border Management system.

3. Save the file with the file name **Border_Mgmt.**

☐ **Start the PLM**

See the instructions documented in Chapter 7 in *Advanced Power Virtualization on IBM @server p5 Servers: Introduction and Basic Configuration,* SG24-7940.

Example 7-1   #Integrated Boarder Management PLM Group

```
globals:
        hmc_host_name = hmc14
        hmc_user_name = hscroot
        hmc_cec_name = DesignCenter_p590


Boarder_mgmt_group:
        type = group
        cpu_type = shared
        cpu_maximum = 2
        mem_maximum = 0
        ec_delta = 10
        cpu_intervals = 6
        cpu_load_high = 1
```

```
            cpu_load_low = 0.5
            ec_per_vp_min = 0.5


Boarder_mgmt_group:
            type = group
            cpu_type = shared
            cpu_maximum = 2
            mem_maximum = 0
            ec_delta = 10
            cpu_intervals = 6
            cpu_load_high = 1
            cpu_load_low = 0.5
            ec_per_vp_min = 0.5


r14n12.pbm.ihost.com:
            type = partition
            group = Boarder_mgmt_group
            cpu_guaranteed = 0.5
            cpu_maximum = 1
            cpu_minimum = 0.1
            cpu_shares = 1


r14n08.pbm.ihost.com:
            type = partition
            group = Boarder_mgmt_group
            cpu_guaranteed = 0.5
            cpu_maximum = 1
            cpu_minimum = 0.1
            cpu_shares = 1


r14n09.pbm.ihost.com:
            type = partition
            group = Boarder_mgmt_group
            cpu_guaranteed = 0.5
            cpu_maximum = 1
            cpu_minimum = 0.1
            cpu_shares = 1


r14n11.pbm.ihost.com:
            type = partition
            group = Boarder_mgmt_group
            cpu_guaranteed = 0.5
            cpu_maximum = 1
            cpu_minimum = 0.1
            cpu_shares = 1


r14n13.pbm.ihost.com:
            type = partition
            group = Boarder_mgmt_group
            cpu_guaranteed = 0.5
            cpu_maximum = 1
            cpu_minimum = 0.1
            cpu_shares = 1
```

A

WebSphere Application Server installation and configuration

IBM WebSphere Application Server offers an infrastructure for open e-business platforms. As the foundation of the WebSphere software platform, WebSphere Application Server provides a rich, e-business application deployment environment with a complete set of application services. These include capabilities for transaction management, security, clustering, performance, availability, connectivity, and scalability.

This appendix discusses the installation of IBM WebSphere Application Server.

Reference to product installation information

Refer to the installation document in the /docs/InstallGuide_en.pdf. You can access the Information Center document at:
http://publib.boulder.ibm.com/infocenter/wasinfo/v5r1/index.jsp

How to install WebSphere Application Server

☐ **Download the installation file to a temporary directory.**

1. The installation file is a tar file.
2. Untar the tar file using the command `tar –xvf xxx.tar`

☐ **Modify the execute permission on the Launch.sh file:**

`chmod 766 Launch.sh [This will bring up a GUI for the installation]`

☐ **At the first window, accept the license. Click Next.**

☐ **Choose the typical installation. Click Next.**

☐ **Choose the installation directions for WebSphere Application Server.**

In our case, it is /usr/WebSphere/AppServer. Click **Next**.

1. The installation starts.
2. It could take 15 minutes.

☐ **Click End to close the wizard.**

☐ **Click http://localhost:9090/admin to bring up the administrative console.**

This will confirm the installation.

How to install IBM HTTP Server

☐ **Download the installation file and untar it.**

☐ **Modify the execute permission on the installIHS.sh file:**

`chmod 766 installIHS.sh`

This will bring up a GUI for the installation.

☐ **At the first window accept the license. Click Next.**

☐ **Choose the typical installation. Click Next.**

☐ **Choose the installation direction for WebSphere Application Server, here /usr/HTTPServer. Click Next.**

1. The installation starts.
2. It usually takes 1-2 minutes.

☐ **Click End to close the wizard.**

☐ **Click http://localhost to get the http server page. This will confirm the installation.**

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this document.

IBM Redbooks

These publications can be found at http://www.ibm.com/redbooks/. They can be viewed or downloaded online, or ordered in hardcopy format.

- *The IBM @server BladeCenter JS20,* SG24-6342
- *Advanced Power Virtualization on IBM @server p5 Servers,* SG24-7940

Other publications

These publications are also relevant as further information sources:

- *HACMP Version 5.3 Planning and Installation Guide,* SC23-4861-06
- *HACMP Version 5.3 Administration Guide*, SC23-4862-06
- *HACMP Version 5.3 Troubleshooting Guide*, SC23-5177-00

Online resources

These Web sites and URLs are also relevant as further information sources:

- SSPD entry in Tech Docs: SSPD-KMUT-6MATUA

  http://w3-03.ibm.com/support/techdocs/atsmastr.nsf/Web/TechDocs
- Customs, Ports, and Border Management Solution Catalog on W3 KnowledgeView
  - *GSMethod ARC 101 Integrated Border Management Architecture Overview*
  - *GSMethod ARC 108 Integrated Border Management Component Model*
- ILOG (JRules)

  http://www.ilog.com/products/jrules/server.cfm

Help from IBM

IBM Support and downloads

  ibm.com/support

IBM Global Services

  ibm.com/services

93

Index

    95

S

security   4, 91
Selected Business Solutions (SBS)   2
SOA   4, 26
stanza   88
Storage Area Network (SAN)   8, 70
   volume controller   4

T

Tivoli
   Access Manager   4
   Identity Manager   4

U

user ID   60

V

visa   6

W

WebSphere   12, 26
   Application Server   91
   MQ   12, 26
WebSphere Business Integration Server Foundation (WBISF)   25
WebSphere Portal   3, 11
   administrator   15
workflow management   3

X

xlC   26
XML   5, 68

Z

zSeries   4

Redbooks

Passenger Risk Management Infrastructure Solution Building Block: Installation and Configuration

(0.2"spine)
0.17"<->0.473"
90<->249 pages

Passenger Risk Management
Infrastructure Solution Building Block:
Installation and Configuration Guide

Infrastructure for open e-business platforms and passenger risk applications

Integrated border management architecture and installation

Component interaction scenario

This IBM Redbook describes an Integrated Border Management solution that is passenger-centric. It defines infrastructure solution building blocks, how to install them, how to integrate them with each other, and how to put them into operation. This system design can be used as a template to build other systems with similar requirements.

The target customers for Integrated Border Management include central government border management and immigration agencies, regional or local port authorities, border police and local law enforcement, national intelligence, agriculture, health, trade regulatory and central government customs agencies worldwide.

Each component of the solution is described in a separate chapter:

► Portal Server
► WebSphere Business Integration Server Foundation
► JRules
► High Availability Clustered Multiprocessor
► Partition Load Manager
► Entity Analytic Server
► WebSphere Application Server

The intent of this book is to provide a framework for building your own similar system, using some or all of the components and suggestions included herein.