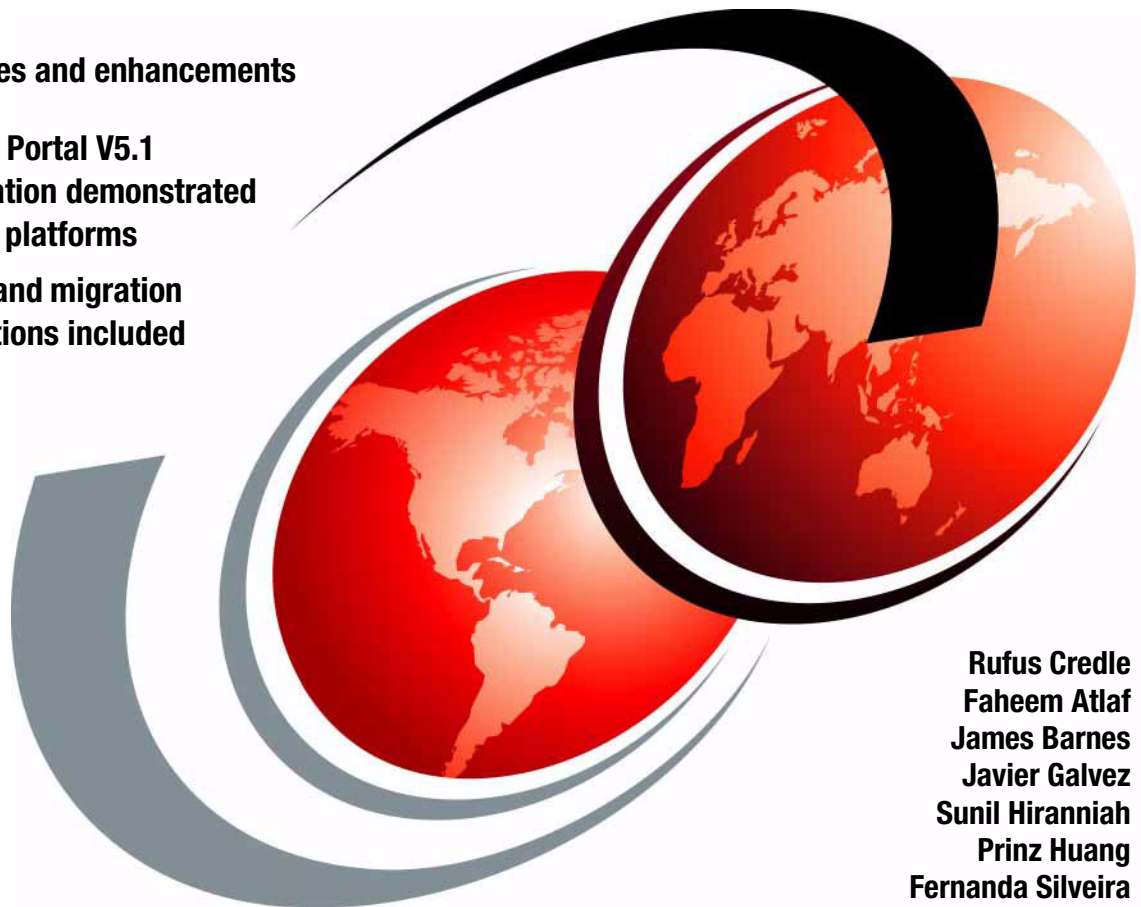


IBM WebSphere Portal for Multiplatforms V5.1 Handbook

New features and enhancements

WebSphere Portal V5.1
implementation demonstrated
on multiple platforms

Clustering and migration
demonstrations included



Rufus Credle
Faheem Atlaf
James Barnes
Javier Galvez
Sunil Hirannah
Prinz Huang
Fernanda Silveira



International Technical Support Organization

**IBM WebSphere Portal for Multiplatforms V5.1
Handbook**

April 2005

Note: Before using this information and the product it supports, read the information in “Notices” on page ix.

First Edition (April 2005)

This edition applies to IBM WebSphere Portal for Multiplatforms Version 5.1.

© Copyright International Business Machines Corporation 2005. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	ix
Trademarks	x
Preface	xi
The team that wrote this Redbook	xi
Become a published author	xiv
Comments welcome	xiv
Chapter 1. WebSphere Portal V5.1: New features and enhancements . . .	1
1.1 Introduction	2
1.2 Installation and configuration enhancements	2
1.3 Virtual portals	4
1.4 Business process integration	6
1.5 Search enhancements	8
1.6 WebSphere Portal Document Manager	13
1.7 Security enhancements	16
1.8 Administration, operations, and deployment enhancements	18
1.9 Personalization	20
1.10 Web Content Management	21
1.11 Programming model enhancements	22
1.12 Summary	24
Chapter 2. WebSphere Portal V5.1 planning and requirements	25
2.1 Hardware requirements	26
2.2 Software requirements	26
Chapter 3. WebSphere Portal: Microsoft Windows Server 2003 install . .	29
3.1 Using install logs	35
3.2 Base installation	37
3.3 Migrating the database from Cloudscape to DB2	53
3.3.1 Installing IBM DB2 UDB Enterprise Server Edition V8.1.1.94.	55
3.3.2 Configuring WebSphere Portal for DB2	61
3.4 Adding an LDAP to the portal	71
3.4.1 Installing Domino Enterprise Server 6.5.3.	72
3.4.2 Setting up Domino LDAP	77
3.4.3 Updating the access control list of Domino Directory	81
3.4.4 Specifying Domino LDAP configuration settings	82
3.4.5 Completing the configuration	83
3.5 Creating the Web SSO configuration	87

3.6	Installing Lotus Team Workplace 6.5.1	90
3.7	Specifying Lotus Team Workplace 6.5.1 server settings	92
3.7.1	Adding QPServlet and configuring for Team Workplace.	98
3.7.2	Configuring Domino Web server	99
3.7.3	Enabling Lotus Team Workplace search	100
3.8	Installing Lotus Instant Messaging and Web Conferencing 6.5.1	102
3.8.1	Modifying Domino after Lotus Instant Messaging installation	104
3.8.2	Setting up Instant Messaging and Web Conferencing awareness and chat	104
3.8.3	Editing the Sametime.ini file to set the security level	107
3.9	Configuring WebSphere Portal for Domino Directory	108
3.10	Deploying Lotus Collaborative Components	117
Chapter 4. WebSphere Portal: Clustering		131
4.1	WebSphere Application Server Network Deployment.	135
4.1.1	Installing WebSphere Application Server Network Deployment	135
4.1.2	Installing the Enterprise extensions on Network Deployment	137
4.1.3	Installing Network Deployment Fix Pack 1	138
4.1.4	Installing WebSphere Business Integration Server Foundation Fix Pack 1	140
4.1.5	Installing Network Deployment Cumulative Fix 1	140
4.1.6	Validating the Network Deployment installation	141
4.2	Installing and configuring IBM WebSphere Portal on node 1	141
4.2.1	Configuring WebSphere Portal node 1 to a Web server.	142
4.2.2	Configuring to optimize for clustering	145
4.2.3	Federating node 1 to the deployment manager using the -includeapps option	146
4.2.4	Starting WebSphere Portal and running the post-federation task.	147
4.2.5	Updating virtual host entries and Web server plug-in	148
4.2.6	Configuring WebSphere Portal node 1 and Network Deployment for security	149
4.2.7	Final steps to complete node 1 federation	150
4.3	Installing and configuring WebSphere Portal on node 2	150
4.3.1	Connecting WebSphere Portal node 2 to the external database	151
4.3.2	Configuring WebSphere Portal node 2 for security.	152
4.3.3	Configuring to optimize for clustering	153
4.3.4	Federating node 2 to the deployment manager	153
4.3.5	Starting WebSphere Portal and running the post-federation task.	154
4.4	Adding WebSphere Portal nodes to the cell	155
4.5	Creating the cluster	156
4.5.1	Editing the WebSphere Portal configuration on each node	161
4.5.2	Enabling dynamic caching	162
4.5.3	Starting the cluster	164

4.5.4	Regenerating the Web server plug-in	164
4.5.5	Validating the cluster configuration	165
4.6	Deploying portlets	166
4.7	Deploying themes and skins	169
4.8	Removing the WebSphere Portal node from deployment manager	170
4.8.1	Removing the node from the cell	171
4.8.2	Removing all enterprise application instances from bc3srv6	171
Chapter 5.	WebSphere Portal: SUSE LINUX Enterprise Server 9 (SLES9) installation	175
5.1	Overview of WebSphere Portal installation on Linux	177
5.2	Preparing the machines for installation	178
5.3	Installing WebSphere Portal	179
5.4	Installing IBM HTTP Server.	190
5.4.1	Installing IBM HTTP Server.	190
5.4.2	Verifying the installation	195
5.4.3	Configuring WebSphere Portal with a remote IBM HTTP Server	196
5.5	Installing IBM DB2 V8.2 for WebSphere Portal.	199
5.5.1	Installing IBM DB2 UDB Enterprise Server V8.2.	199
5.5.2	Installing IBM DB2 Administration Client V8.2	203
5.5.3	Creating remote databases	203
5.5.4	Configuring the connection to remote databases	206
5.5.5	Transferring data to the DB2 database	208
5.6	Installing Lotus Domino 6.5.3	213
5.6.1	Installing Lotus Domino Enterprise Server 6.5.3.	214
5.6.2	Installing Domino Administrator	223
5.6.3	Configuring the Domino server settings	223
5.6.4	Configuring Domino Administrator	235
5.6.5	Setting up Domino Directory	237
5.6.6	Updating the access control list of Domino Directory	240
5.6.7	Specifying Domino LDAP configuration settings.	241
5.6.8	Creating the Web SSO configuration (optional)	245
5.6.9	Configuring WebSphere Portal for Domino Directory	247
5.6.10	Verifying the LDAP configuration	251
5.6.11	Configuring WebSphere Portal Web SSO (optional)	251
Chapter 6.	WebSphere Portal: IBM AIX 5L V5.2 installation	257
6.1	Installing WebSphere Portal in a multi-tier environment	260
6.2	Installing WebSphere Portal	260
6.3	Installing a remote HTTP server	269
6.4	Configuring the remote HTTP server	273
6.4.1	Configuring the plug-in	274
6.4.2	Adding a new host alias	274

6.4.3	Updating and copying the Web server plug-in configuration	276
6.4.4	Disabling access to port 9081 (optional)	277
6.5	Installing and configuring DB2 UDB Enterprise Server Edition	278
6.5.1	Installing IBM DB2 UDB Enterprise Server	278
6.5.2	Installing the IBM DB2 fix pack	284
6.5.3	Installing IBM DB2 Administration Client.	287
6.5.4	Creating remote databases	289
6.5.5	Configuring the connection to remote databases	291
6.5.6	Transferring data to the DB2 database	294
6.6	Installing and configuring LDAP	298
6.6.1	Installing IBM Tivoli Directory Server	299
6.6.2	Configuring the administrator DN	302
6.6.3	Configuring the LDAP database	303
6.6.4	Configuring the Web Administration Tool	310
6.6.5	Configuring the LDAP server for Web Administration Tool	312
6.6.6	Installing IBM Tivoli Directory Server V5.2 client	315
6.6.7	Preparing the LDAP server for WebSphere Portal	316
6.6.8	Creating the required users and group	318
6.6.9	Configuring WebSphere Portal with the LDAP settings	318
6.7	Validating the overall configuration	321
6.7.1	Validating the database configuration	321
6.7.2	Validating the LDAP configuration	325

Chapter 7. WebSphere Portal: SUSE LINUX Enterprise Server 8 (SLES8) installation on zSeries	327
7.1 Prerequisites	328
7.1.1 SLES8 operating system requirements.	328
7.1.2 IBM hardware requirements	328
7.1.3 IBM Middleware component space requirements	328
7.1.4 WebSphere Portal installation CD requirements.	329
7.2 Installing WebSphere Portal V5.1	329

Chapter 8. WebSphere Portal V5.0.2 to V5.1 migration	343
8.1 WebSphere Portal V5.1 migration overview	345
8.2 Migration process overview.	346
8.3 Prerequisites and preparing for the migration	347
8.4 Portal migration process	351
8.4.1 Migrating access controls on user groups.	351
8.4.2 Migrating virtual resources	354
8.4.3 Migrating credential slots and segments.	354
8.4.4 Migrating pages, themes, skins, and applications.	356
8.4.5 Migrating all the user customizations	363
8.4.6 Migrating credential vault data	365

Appendix A. Identity management	369
WebSphere Member Manager	370
WebSphere Member Manager supported configuration	371
Appendix B. Preparing the AIX machine	375
Increasing the size of an existing file system	376
Creating a new file system	376
Creating a CDROM file system	377
Appendix C. Creating users on AIX	379
Creating DB2 groups	380
Creating DB2 users	380
Setting user passwords	380
Related publications	381
IBM Redbooks	381
Other publications	382
Online resources	382
How to get IBM Redbooks	383
Help from IBM	383
Index	385

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.

Trademarks

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

AIX 5L™	Lotus Discovery Server™	RS/6000®
AIX®	Lotus Notes®	S/390®
Cloudscape™	Lotus®	Sametime®
DB2 Universal Database™	Notes®	Tivoli®
DB2®	OS/390®	WebSphere®
Domino®	POWER3™	Workplace Web Content
@server®	PowerPC®	Management™
ibm.com®	pSeries®	Workplace™
IBM®	QuickPlace®	xSeries®
Informix®	Rational®	z/OS®
iNotes™	Redbooks (logo)  ™	zSeries®
iSeries™	Redbooks™	

The following terms are trademarks of other companies:

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

Intel, Intel Inside (logos), MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

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

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

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

Preface

This IBM Redbook positions the new features and enhancements of IBM WebSphere® Portal for Multiplatforms Version 5.1 and serves as a follow-up to the IBM Redbook, *IBM WebSphere Portal for Multiplatforms V5 Handbook*, SG24-6098.

This *IBM WebSphere Portal for Multiplatforms V5.1 Handbook* will help you to understand how to install, tailor, and configure WebSphere Portal V5.1 within the Microsoft® Windows® Server 2003, SUSE LINUX Enterprise Server 9 (SLES9), IBM AIX® 5L™, and Linux® on zSeries®/SUSE LINUX Enterprise Server 8 (SLES8) environments. We provide instructions to set up a clustered environment and also provide a demonstration of migrating from WebSphere Portal Version 5.0 to Version 5.1.

Although this book includes the steps for configuring WebSphere Portal V5.1 on the latest operating systems, we recommend that you refer to the IBM Redbook *IBM WebSphere Portal for Multiplatforms V5 Handbook*, SG24-6098, when you seek administrative and customization examples.

Other examples provided in this book include the implementation of IBM Lotus® Domino® Enterprise Server, Lotus Team Workplace™, Lotus Collaborative Components, and IBM Tivoli® Directory Server.

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, Raleigh Center.



Rufus Credle is a Senior I/T Specialist and certified Professional Server Specialist at the International Technical Support Organization, Raleigh Center. He conducts residencies and develops Redbooks™ about network operating systems, ERP solutions, voice IBM @server® technology, high availability and clustering solutions, Web application servers, pervasive computing, and IBM and OEM e-business applications, all running IBM @server xSeries® systems. Rufus's various positions during his IBM career have included assignments in administration and asset management, systems engineering, sales and marketing, and IT services. He holds a B.S. degree in business management from Saint Augustine's College. Rufus has been employed at IBM for 25 years.



Faheem Atlaf is an IT Professional with the IBM Linux Integration Center in Austin, TX, working as a Sales Engagement Specialist on the pre-sales support initiative. The Linux Integration Center is a worldwide team dedicated to assisting the IBM Sales team with technical issues concerning IBM Middleware, and ultimately driving Linux solutions into the marketplace. Recently, Faheem has been focused on single sign-on solutions in Linux that include IBM WebSphere Portal, WebSphere Application Server, DB2®, Tivoli Access Manager, IBM Directory Server and open source components, such as OpenLDAP and Samba. Faheem has previously contributed to the Redpaper *WebSphere Portal Installation for Linux on zSeries*, REDP-3699.



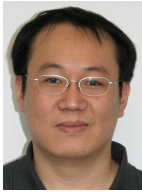
James Barnes works as a Team Lead for the Portal Level 2 development and runtime team in the U.S. He has two years experience working with WebSphere Portal support and previously worked on the Lucent account as a Java™ and Cobol Programmer for four years. His areas of expertise include Java, portals, WebSphere Portal tools, runtime and crash issues, network topology, and performance. He writes extensively about WebSphere Portal performance and runtime issues. He holds a degree in Agriculture and Applied Economics from Virginia Tech.



Javier Galvez works for Itecsa in the Business Partner Innovation Center (BPIC) in Buenos Aires, Argentina. He is an IT Professional and works as a sales engagement specialist on the pre-sales IBM software support initiative. He has 10 years of experience in the IT field. He is MSCE certified in Microsoft Windows NT® and Windows 2000 and received GIAC Security Certification from the SANS Institute. His areas of expertise include cryptography, information security, WebSphere Portal, and Lotus Workplace. Javier is a student at UADE University majoring in Systems Engineering.



Sunil Hirannah works for IBM Developer Relations Technical Support Center in Dallas, Texas as an Advisory Software Engineer. He has worked as a software engineer, developer, and analyst in various commercial projects since 1997. He has ample experience and has published extensively on the WebSphere family of products, J2EE, databases, and security. He is WebSphere Portal product certified as both a Solution Developer and System Administrator. Sunil has been a coauthor for more than four WebSphere Portal Redbooks and has published more than 60 articles about IBM Middleware products. His current and most interesting job involves providing enablement assistance to Business Partners and customers on WebSphere Portal and Collaboration components. Sunil can be reached at <mailto:sunilh@us.ibm.com>.



Prinz Huang is a Staff Software Engineer and works for the IBM China Software Development Lab in Taiwan. He has five years of experience in Java application development including DB2, J2SE/J2EE, and WebSphere Commerce and WebSphere Portal applications. He holds a M.S. degree in Electronic Engineering from National Sun Yat-Sen University in Kaohsiung, Taiwan. His areas of expertise include J2SE/J2EE, databases, e-business, portal solutions, and High Performance Computing.



Fernanda Silveira is a Certified Sun Java Programmer and IBM Certified System Administrator for WebSphere Portal. She is a Solutions Developer for Dualline Solutions, an IBM Premier Business Partner. As a developer, she has extensive experience with Java systems with database access and distributed systems with RMI and FTP communication. She has worked in projects using WebSphere Portal Versions 4.2 and 5.0 on both Microsoft Windows and Linux, using DB2 and Oracle. In those projects, she configured single sign-on between WebSphere, Domino, Lotus Instant Messaging and Web Conferencing (formerly Sametime®) and Lotus Team Workplace (formerly QuickPlace®), and she also developed portlets to access Web services and enterprise applications, such as SAP and Cognos. Fernanda earned her BSc in Computer Science from the Federal University of Santa Catarina in Florianopolis, Brazil.

Thanks to the following people for their contributions to this project:

Tamikia Barrow, Jeanne Tucker, Diane O'Shea,
International Technical Support Organization, Raleigh Center

Charles Price, Software Engineer, Lotus Technical Support/Collaboration Center
IBM Atlanta

William Ding, Staff Software Engineer, Business Integrations and Testing, China
Software Development Lab
IBM Taiwan

Libra Huang, Manager, eSupport Development, China Software Development
Lab
IBM Taiwan

Elaine Lee, Software Engineer, Business Integrations and Testing, China
Software Development Lab
IBM Taiwan

Jeanne Lee, Staff Software Engineer, eSupport Development, China Software
Development Lab
IBM Taiwan

Michael Chen, Software Engineer
Shinewave International, Taiwan

Jerry Dancy, WebSphere Portal Server Level 2 Support Specialist
IBM Research Triangle Park

Thomas Hurek, IBM WebSphere Portal Security Development
IBM Germany

Stefan Liesche, WebSphere Portal Architect
IBM Germany

Rob Will, Distinguished Engineer, WebSphere Portal, Document Management,
and Web Content Management
IBM Research Triangle Park

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 e-mail to:

redbook@us.ibm.com

- ▶ Mail your comments to:

IBM® Corporation, International Technical Support Organization
Dept. HQ7 Building 662
P.O. Box 12195
Research Triangle Park, NC 27709-2195



WebSphere Portal V5.1: New features and enhancements

This chapter highlights the new features and enhancements of IBM WebSphere Portal for Multiplatforms Version 5.1. Some of the new features and enhancements that we cover in this chapter include virtual portals, business process integration, installation, and administration.

1.1 Introduction

Before immersing yourself into any new product version, it is important to have a good understanding of its new capabilities and features. In this chapter, we discuss some of the major highlights and enhancements that come with WebSphere Portal V5.1. This chapter will give you an overview understanding of the new features and enhancements, which will help you plan your environment with WebSphere Portal V5.1. Some of the new features and enhancements that we cover in this chapter include:

- ▶ Installation and configuration enhancements
- ▶ Virtual portals
- ▶ Business process integration
- ▶ Search enhancements
- ▶ Document Manager
- ▶ Security enhancements
- ▶ Administration, operations, and deployment enhancements
- ▶ Personalization
- ▶ IBM Workplace Web Content Management
- ▶ Programming model enhancements

1.2 Installation and configuration enhancements

WebSphere Portal V5.0 had major enhancements with regards to installation. Installation was much simpler and more reliable by installing a working WebSphere Portal infrastructure based on an IBM Cloudscape™ configuration. Users had the option to configure their choice of database and LDAP when they were ready. This helped smooth the way for additional enhancements with the current version.

The WebSphere Portal V5.1 installation has continued in this path with further enhancements. The initial installation now uses the archive-based install. Basically, the archive install copies a working image to the location of your choice and then does the necessary customizations, such as host name and administrative passwords. For problem determination, informative messages will be logged during the installation and configuration processing.

A configuration wizard is now available with WebSphere Portal V5.1 to help configure LDAP and databases instead of having to edit the ANT scripts directly. After installing WebSphere Portal, there are usually several configuration steps

that need to be run, depending on your environment. In the past, this required you to edit the WebSphere Portal properties file for which it proved difficult to determine exactly what should be edited for a particular task. In addition, you then had to run a sequence of ANT tasks to configure your system. The sequence of these tasks and the syntax to execute them was not always readily apparent. Now with WebSphere Portal V5.1, there is an alternative to running these tasks through the command line. The new WebSphere Portal installation configuration wizard gives you a GUI front end to the most commonly run tasks. The configuration wizard will install automatically during the WebSphere Portal installation and has been built using Install Shield Multiplatform (ISMP), which gives the new GUI an *install-like* look and feel. This allows the wizard to look like a WebSphere Portal component. The wizard uses existing mechanisms for the configuration. Just as in running scripts, the wizard will update a properties file and execute the WPSconfig script.

Some of the benefits of the configuration wizard include:

- ▶ Ability to set up a production environment without manually editing property files.
- ▶ Users should not have to edit any property files or execute scripts to do the most common tasks they are likely to need to create a production WebSphere Portal environment.
- ▶ Additional validation of property values is possible prior to execution of the configuration task or tasks.
- ▶ Some of the most important tasks will be presented to the user without them having to look for the script files.
- ▶ Any errors that occur can be presented directly to the user without them having to look in the logs.

One of the issues we had in WebSphere Portal V5.0 was the time it took to transfer data from the base install Cloudscape database to the selected database and LDAP. This issue has been solved with the current release. Another important enhancement is the database transfer performance by creating a direct connection between the Cloudscape database and the selected database, which removes the intermediate copy to disk.

Previous versions of WebSphere Portal did not have WebSphere Application Server deployment manager, which required a complex manual cluster setup procedure. Support has been added to the installer to simplify the installation and configuration in a federated node. Now, it will be possible to perform post-configuration on WebSphere Portal on either non-federated or federated node.

To summarize the enhancements to the WebSphere Portal V5.1 installation and configuration tasks:

- ▶ Archive install:
 - Dramatically improve install time.
 - Fewer install steps lead to improved install reliability. All you will need is to answer a couple of questions, providing information such as the WebSphere Portal administrator ID and password.
- ▶ Install into cell (install support for Network Deployment):
 - No need to remove node prior to installing WebSphere Portal.
 - Easier to create WebSphere Portal clusters.
- ▶ Post-install configuration wizard: Security and database tasks that are most often used.
- ▶ Improved DB transfer performance and usability: Two-step process eliminated, so no more export, change properties, or import steps.
- ▶ Platform support: Microsoft Windows, IBM AIX, Sun Solaris, Linux, HP-UX.

1.3 Virtual portals

In WebSphere Portal V5.0 and earlier, each unique portal required its own WebSphere Portal installation: a WebSphere Application Server install, a WebSphere Portal install, a set of installed portlets, and so on. As users build a WebSphere Portal implementation, they can see how it can be leveraged in other areas of their business. In some cases, it just means adding more user communities to their WebSphere Portal rollout. But there are cases where users want and need distinct portals. For example, one of our users is an insurance company that has deployed WebSphere Portal for their employees. It has been so successful that they have been asked to roll out a similar solution for the insurance agents. While there are some similar capabilities that they want to offer the agents, there are differences in terms of the anonymous pages and the overall site navigation and style. So, this really is a second portal. However, they do not want to have to maintain a second portal infrastructure. How will the user solve this problem? Virtual portals are the solution to this problem.

With WebSphere Portal V5.1, we introduce virtual portals. Virtual portals are entities that act like distinct WebSphere Portal instances, but run on a shared infrastructure. By *distinct*, we mean that they have their own URI, places, pages, and set of users. They can have their own set of anonymous pages, their own login pages, and sign up pages. Therefore, from the user perspective, they cannot tell that these virtual portals are running on the same infrastructure.

Figure 1-1 shows the various virtual portals using the same WebSphere Portal infrastructure. Notice the different URIs representing various virtual portals.

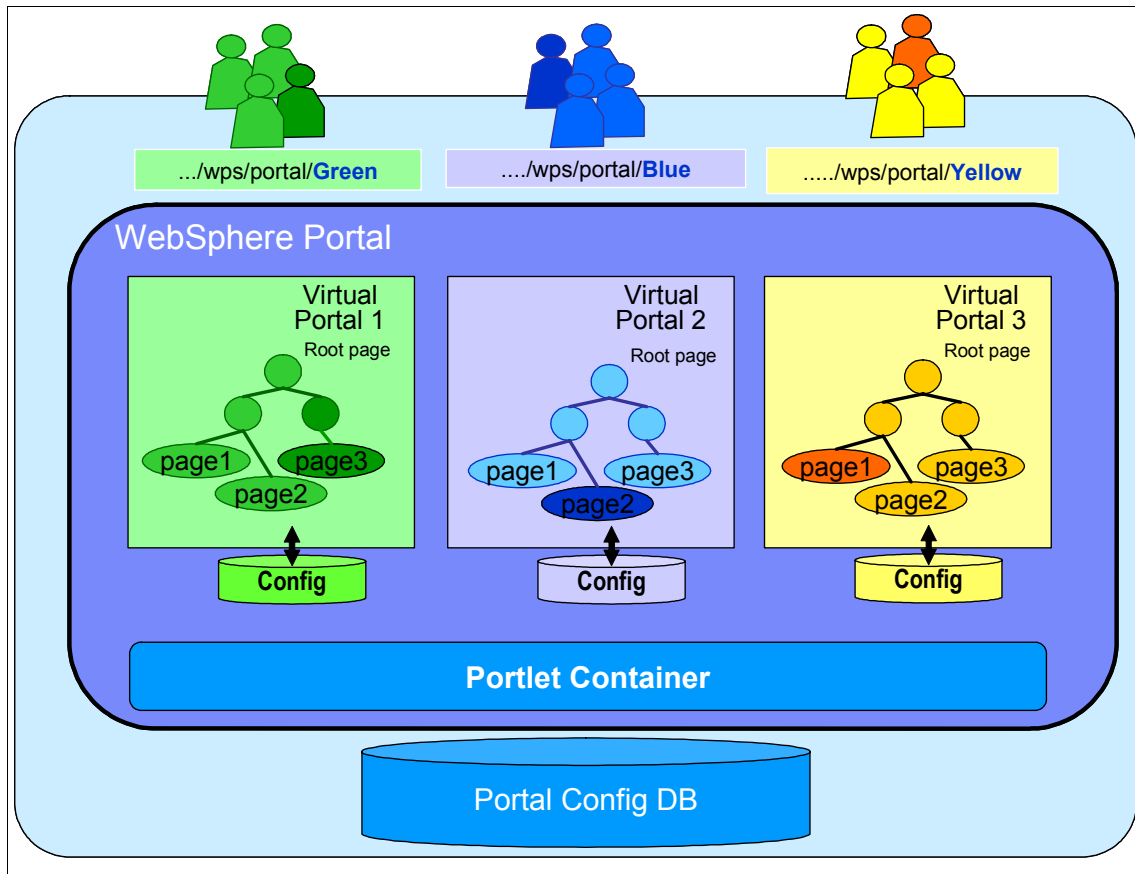


Figure 1-1 An example of virtual portals

The virtual portal administrators can more or less manage their virtual portal independently. There are some things that are shared between the virtual portals. For example, portlet applications need to be installed once, and then all virtual portals can use them. The portlet data can be specific to each virtual portal. Themes and skins are common to all virtual portals, but each virtual portal can be assigned its own unique set of themes and skins.

With virtual portals, you can use a single installation of WebSphere Portal to deploy multiple portals with different URLs, anonymous pages, user groups, and themes and skins. Virtual portals enable you to quickly deploy additional portals on an existing infrastructure.

The advantages of using virtual portals are that they can be created on the same hardware system, without repeating the software installation procedure, by partitioning an existing WebSphere Portal installation into logical portals, thereby enabling simplified administration of multiple portals.

To summarize, the highlights of virtual portals include:

- ▶ Virtual portals are virtual entities, each representing the logical behavior of a distinct WebSphere Portal, but running on a shared infrastructure.
- ▶ Characteristics of a virtual portal include:
 - Each has a unique URI.
 - Each has its own unique set of places, pages, and users.
 - Each has its own set of anonymous pages, login and sign up pages, and themes and skins.
 - Each has its own user community.
- ▶ Virtual portal administrators:
 - Manage each virtual portal individually.
 - Have some shared resources (such as portlet applications).

1.4 Business process integration

WebSphere Portal provides the user interface to achieve integration with business processes. Some of the business benefits include increased application usage, reduced IT support, and wide use of collaboration tools.

Business processes are a set of activities carried out in an order. So, for example, when ordering a product, the steps would be:

1. Check product availability.
2. Take payment.
3. Confirm delivery date.

Services are choreographed to provide the technical implementation of a business process, that is, each step or activity in a business process is implemented by a service. This service choreography is described by the Business Process Execution Language (BPEL).

In Figure 1-2 on page 7, you notice an employee trying to book a flight ticket and the processes involved.

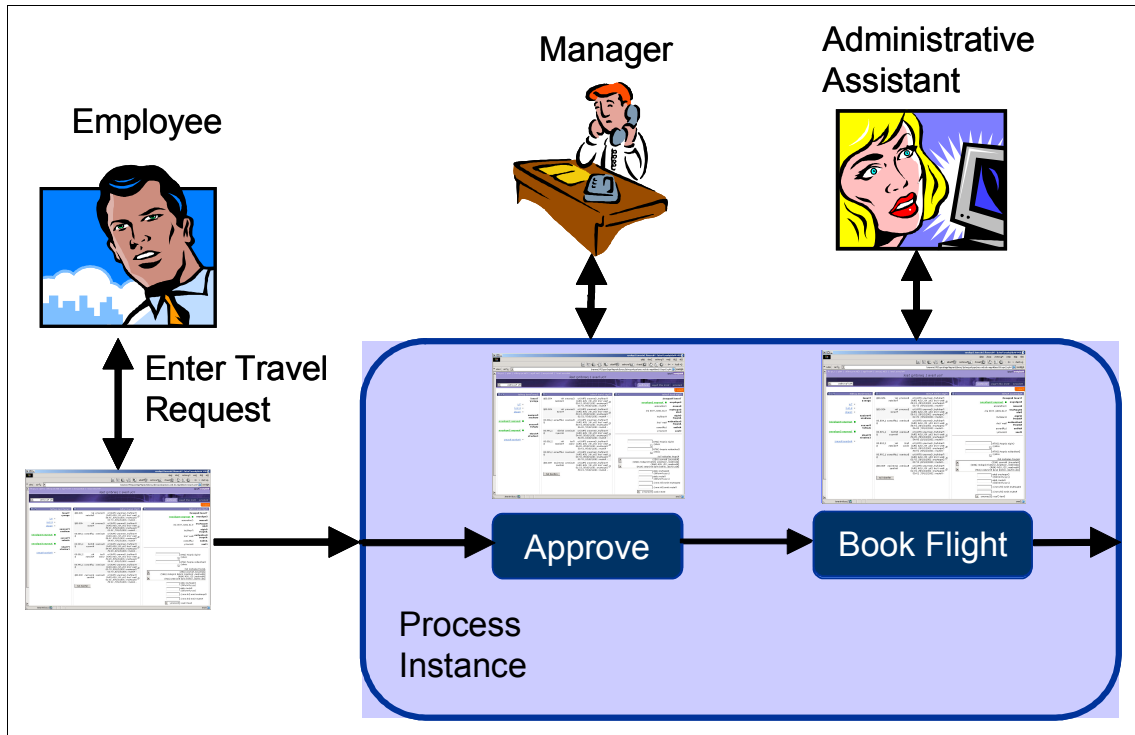


Figure 1-2 Employee booking a flight ticket and the processes involved before booking the flight ticket

More and more customers are adopting a service-oriented architecture (SOA) approach to their IT infrastructure. What this means is that they expose their infrastructure as a set of standards-based Web services connected together by an *enterprise service bus* that enables applications to connect to these services as needed. As that implementation matures, they are able to combine these services into business processes to meet their business needs. IBM is one of many companies behind the Business Process Execution Language (BPEL) standard, which is a standardized way to define and execute business processes composed of Web services. The IBM BPEL implementation is known as IBM WebSphere Process Choreographer. WebSphere Process Choreographer ships as part of IBM WebSphere Portal and IBM WebSphere Business Integrator.

With WebSphere Portal V5.1, we introduce an important integration with WebSphere Process Choreographer and the Business Process Execution Language. First, there is the My Tasks portlet. The My Tasks portlet enables users to claim and process WebSphere Process Choreographer tasks assigned to them. As each task is selected for processing, WebSphere Portal launches the corresponding *page application instance*. By page application instance, we mean a portal page that has been defined to contain the set of portlets necessary for

the user to complete a specific task. This page passes the context necessary for the portlets that are deployed on the page and presents the appropriate information to the user. For example, the task can be an approval of a travel request. The task context might include the ID of the traveler and the destination. The portlets on the page could then display the traveler's past trips, manager information, lowest cost airfares to the selected destination, and other information necessary to approve or reject the travel request. Because the user might have to work on multiple tasks at once, suspending work while waiting for more information, for example, the WebSphere Portal My Task portlet instantiates an instance of the appropriate page for each task being processed. The page instances remain until the user completes the task or logs off (when the user logs on later, and clicks the items in the My Tasks portlet, the pages can be instantiated again).

This is a significant enhancement to WebSphere Portal. Not only does it provide a way to provide a consistent user interface in front of an enterprise's diverse applications, the WebSphere Portal navigation paradigm has been extended from role-based navigation selection to enable navigation to change based on the current task. This is important, because companies have many, many processes and some are rarely used by any one employee. With just a role-based paradigm, the user would be exposed to all of these pages all the time. With task-oriented navigation, these extra pages are only visible when needed. This helps make the user more productive and improves the flows throughout your site.

To summarize some of the highlights of business portals:

- ▶ WebSphere Portal becomes the user interface for user-facing activities in business processes.
- ▶ WebSphere Portal displays alerts for users when tasks are pending. When a user clicks the alert, the portal displays the user's task list, which lets the user launch task pages.
- ▶ Alternatively, the portal can send e-mail task notifications with URLs, which will launch the corresponding task page automatically.
- ▶ Advantage: A consistent user interface in front of an enterprise's diverse applications.

1.5 Search enhancements

When we talk about WebSphere Portal search feature enhancements, some of the enhancements include:

- ▶ Enhanced administration and search features with a new set of portlets

- ▶ Enhanced security
- ▶ Support for additional document formats (Adobe PDF, Microsoft Word, Microsoft PowerPoint, and so on)
- ▶ Employs the Stellent *Outside In* filtering technology
- ▶ Categorization
- ▶ Static and user-definable rules-based taxonomy
- ▶ Automatic categorization of indexed documents
- ▶ Summarization
- ▶ Enhanced crawler (multisite crawling, start/stop, progress information, filters)
- ▶ Improved languages support (additional stemmers for languages other than English)
- ▶ Enhanced search support (phrases, wildcards, fielded search)
- ▶ Organized search collections

There are three major enhancements in the search capabilities for WebSphere Portal V5.1: enhanced crawling and searching, the addition of a search center, and the ability to remotely invoke the Portal Search Engine.

It is easier to crawl and search the portal itself. A search bar, as shown in Figure 1-3 on page 10, has been provided within the default themes so that the search bar can appear on every page of the portal. When indexing the portal, you select a specific user ID to crawl the portal and the index is developed using that level of security. When a user subsequently searches the portal, the results are filtered based on the searching user's authorities and the results shown in the context of the portal page on which they reside. You can define which portlets on which pages you want to make searchable. You do this by granting the required access permissions to a crawler user. Only the main panels of portlets are available for indexing and search.

This enhances security, because:

- ▶ Users see only the tabs for search collections for which they have access.
- ▶ A search by a user on a WebSphere Portal search collection returns only documents to which the user has access permission.
- ▶ A search by a user on a portal site returns only portal resources to which the user has access permission.

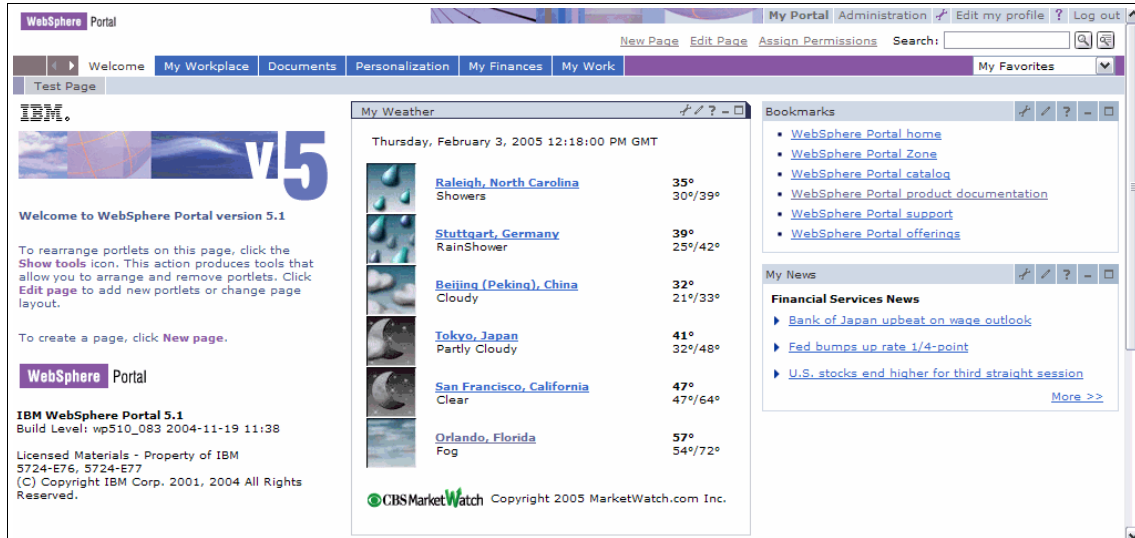


Figure 1-3 Search bar provided with default themes with WebSphere Portal V5.1

The second major search enhancement is the introduction of the Search Center, as shown in Figure 1-4 on page 11. The Search Center enables an administrator to define a set of search targets within a single portlet. Using this portlet, the user can go to one central place and search multiple repositories. In addition, users can search multiple repositories at one time. The Search Center does not have to be deployed on a portal page to be available for users. When users click the Search option, they are taken to the Search Center.

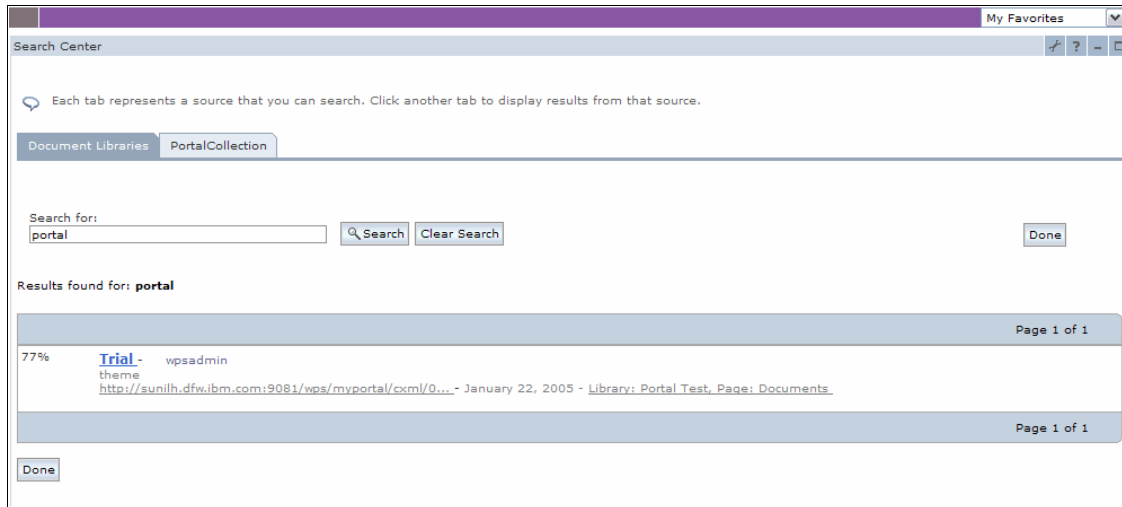


Figure 1-4 The new Search Center with WebSphere Portal V5.1

The content sources are organized by tabs. These sources can be, for example:

- ▶ Search collections that you administer using the Portal Search Engine
- ▶ Portal document management libraries

These can be internal or external Web sites, or IBM Lotus Extended Search, if available, as specified by an administrator.

Finally, the Portal Search Engine is now enabled to be remotely invoked. This means that the indexing and search can be run on a separate server. This takes load off of the portal server, and it allows a cluster of portal servers to share a single search index for more consistent search results and less overhead.

Comparing the various WebSphere Portal Search portlets that are available:

- ▶ WebSphere Portal V5.0 Search portlets

In WebSphere Portal V5.0, we had the following Search portlets:

- Manage Search Collections portlet was the only Search portlet available. The Manage Search Collections portlet features have been enhanced with WebSphere Portal V5.1, and it has two sub-portlets.
- *Search and Browse* used to be called *Document Search* in Portal V5. However, the portlet is basically the same.

► WebSphere Portal V5.1 Search portlets

WebSphere Portal V5.1 has the following Search portlets:

- Search Administration Portlet Taxonomy Manager
The WebSphere Portal Taxonomy Manager portlet helps you manage the search taxonomy.
- Search Administration Portlet Manage Search Collections
Helps perform administrative tasks, which are required as preparatory steps for the search feature, such as indexing.
- Search Administration Portlet Pending Search Collection Items
- Search Administration Portlet Search and Browse
This is similar to the user portlet Search and Browse, but provides additional administrative functions for editing and deleting search items.
- Search Administration Portlet Seed List
The Seed List portlet provides the crawler with an entry point to the portal.
- Search Center Portlet for Search by Users
The Search Center provides a central starting point to all searchable content sources made available to the portal. Users can use the WebSphere Portal Search Center portlet to search documents and content. The available search collections are organized by tabs.
The Search Center is installed as part of the default portal installation, but it is not deployed and placed on a portal page.
- Search and Browse Portlet for Search by Users
Users can use the Search and Browse portlet for more advanced searches. For example, they can refine their search by restricting it to specific document types or by searching in the document fields.

To summarize, the new search features in WebSphere Portal V5.1 include:

- Portal site search:
 - Enables crawling and indexing portal pages.
 - Crawler can fetch all pages with searchable portlets and index those pages.
 - You can define which portlets on which pages you want to make searchable. You do this by granting the required access permissions to a crawler user.
 - Only the main panels of portlets are available for indexing and search.

- ▶ Enhanced security:
 - Users see only the tabs for search collections for which they have access.
 - A search by a user on a portal search collection returns only documents to which the user has access permission.
 - A search by a user on a portal site returns only portal resources to which the user has access permission.
- ▶ Search Center: Sample themes that are shipped with the product provide ability to have a search box on every portal page.
- ▶ Remote search service: The Portal Search Engine service can reside on a different machine.
- ▶ Portal cluster search is possible by implementing Portal Search Engine as a remote service either through Web services or EJB Interface.
- ▶ Portal search results can be displayed to the user within the context of the portlet as personalized for that user.
- ▶ Portal search results can be displayed to the user within the context of the portlet as personalized for that user.

1.6 WebSphere Portal Document Manager

WebSphere Portal Document Manager has been enhanced in WebSphere Portal V5.1.

A tree control has been added to the left side, providing a Microsoft Windows Explorer look, as shown in Figure 1-5 on page 14. The users and administrators have the ability to configure the tree control on or off, so if you want a more classic Document Manager look, where there were tables and folders and documents, you can turn the tree off and obtain them.

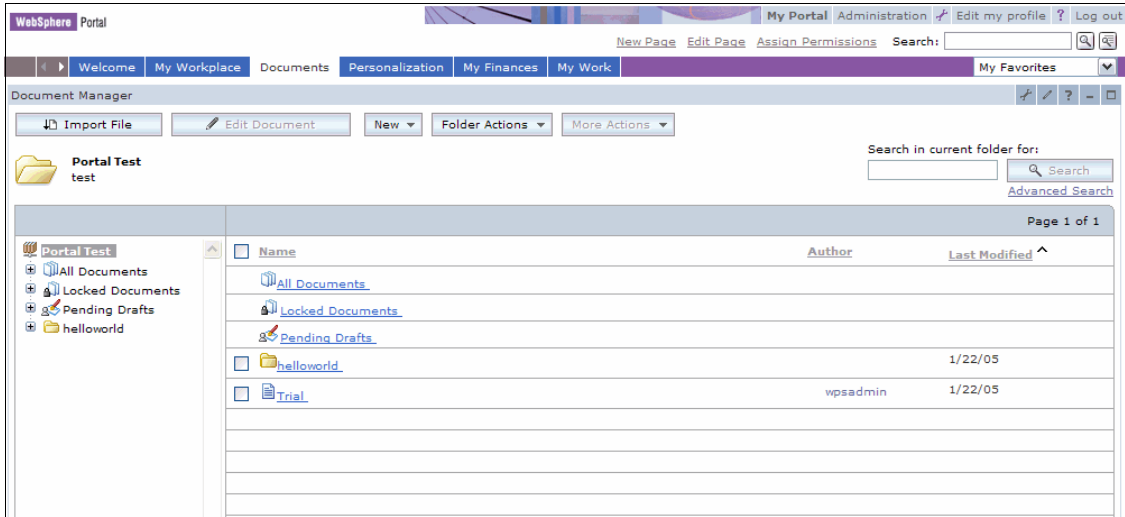


Figure 1-5 New user interface for WebSphere Portal Document Manager in WebSphere Portal V5.1

The round-trip editing process has been streamlined. By round-trip editing, we mean launching a client-side editor, as shown in Figure 1-6 (such as Microsoft Excel) and editing a file locally and then storing the result back into WebSphere Portal Document Manager. With WebSphere Portal V5.1, this requires fewer clicks and is more seamless.

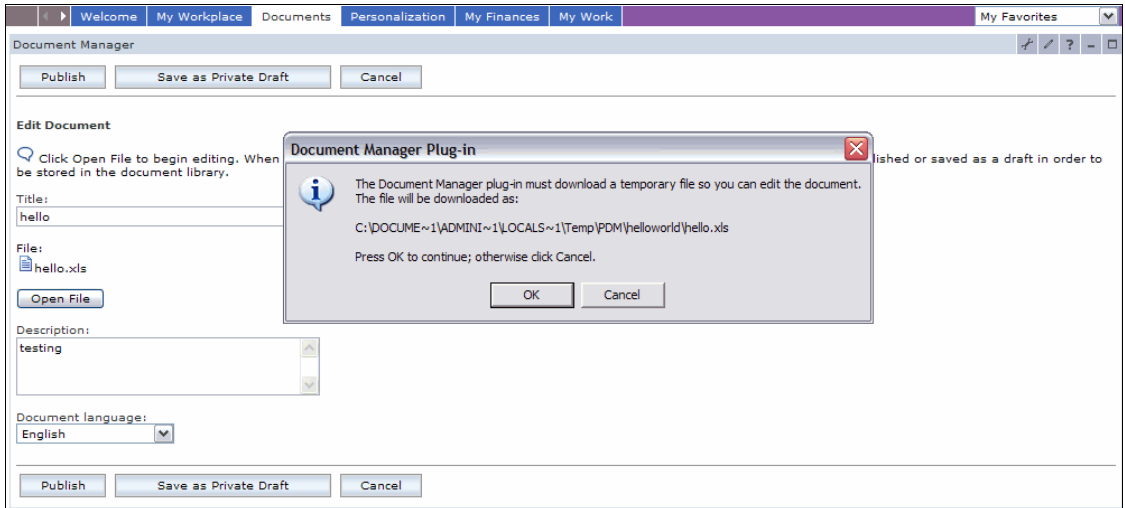


Figure 1-6 Round-trip editing in Portal Document Manager

In WebSphere Portal V5.1, Document Manager includes the following features:

- ▶ Document Manager uses extensions defined by JSR 170. JSR 170 will be the basis for the new content repository. JSR 170 is an API that provides standard access to data in different content management repositories. A short-term benefit is that it aligns all of the IBM repositories so that applications with various databases can leverage one search. JSR 170 is an emerging standard for content stores.
- ▶ Presence awareness can be built into the Document Manager portlet.
- ▶ The cross-project search will expand the current search capability available in WebSphere Portal 5.0.x, supporting the search of individual Document Manager projects to enable searches across multiple Document Manager projects from the Document Manager portlet interface.
- ▶ Improved workflow: Uses WebSphere Process Choreographer as the underlying workflow engine.
- ▶ Improved folder structure presentation/control: Administrators will be able to restrict the ability of end users to create document folders.
- ▶ Multifile import: Administrators will have the ability to import large numbers of documents either from a file system, or from a Web site. Imports can be scheduled.
- ▶ Document change notifications: Users will be able to push out e-mail or Lotus Instant Messaging and Web Conferencing (formerly called Sametime) notifications when a document is changed.
- ▶ Uses productivity components:
 - Portal users can view, edit, and share basic documents, spreadsheets, and presentations through a portal interface.
 - Editing components have been added to the portal framework so that they can be used by other portlets.
 - Advanced browser features can deliver a richer portal experience without any client-side installation or browser plug-ins.

To summarize some of the new features included with Portal Document Manager for WebSphere Portal V5.1:

- ▶ Document management within WebSphere Portal:
 - Navigate the customer-defined folder hierarchy.
 - View, add, delete, and modify documents and folders.
- ▶ Control access on folders and documents.
- ▶ Document versioning.
- ▶ Approve changes through a workflow.

- ▶ Search folders and documents.
- ▶ Subscribe to folders and documents.

1.7 Security enhancements

WebSphere Portal security is based on IBM WebSphere Application Server security. When we talk about WebSphere Portal security, three important concepts are involved:

- ▶ Authentication: Who are you?
- ▶ Single sign-on (SSO): I will accept you as a person because I have your credential information.
- ▶ Authorization: What you are allowed to see and do?

WebSphere Portal security basics include:

- ▶ WebSphere Portal leverages WebSphere Application Server authentication and thus requires WebSphere Application Server security to be activated in production setups.
- ▶ WebSphere Portal does its own access control on portal resources for its instance-level authorization.
- ▶ WebSphere Portal is a Java 2, Enterprise Edition (J2EE) application leveraging WebSphere Application Server SSO.
- ▶ WebSphere Portal features a Credential Vault for back-end SSO.

New features in WebSphere Portal V5.1 include:

- ▶ WebSphere Portal supports Java 2 Security:
 - Protection of system resources and APIs through policy-based, fine-grained access control mechanism.
 - Policy files define the privileges of the code to be executed.
 - Java Access Controller prevents unauthorized access through security exceptions.
 - Global setting in WebSphere Application Server.
- ▶ Multiple realm features:
 - Realms represent a set of users and groups.
 - Realms can aggregate partitions of user repositories, as well as multiple user repositories as an entity.
 - Configuration in the WebSphere Member Manager XML files.

- Required for the virtual portal feature to have different user/group populations per virtual portal.
- ▶ Login page with portlet:
 - Replaces window (JSP) solution (still possible to use legacy window).
 - Login page and portlet specific per virtual portal.
- ▶ Login functions while in a portlet:
 - Possible to generate URLs to the protected area of the portal within a portlet from the unprotected area.
 - When a user clicks a URL:
 - i. Interception with Login form.
 - ii. After successful login, redirect to URL.
- ▶ Login URL:
 - URL for login without being prompted by form to authenticate still exists but has changed:
 - Old URL:


```
http://<server>:<port>/wps/portal/!ut/p/.cmd/LoginUserAuth?userid=<userid>&password=<password>
```
 - New URL:


```
http://<server>:<port>/wps/portal/cxml/04_Sj9CPMtCP1I800I_KydQvyHFUBACnPpvE?userid=<userid>&password=<password>
```
- ▶ Security effects of virtual portal: Security scoped to virtual portal resources and user populations.
- ▶ Credential Vault in JSR168 container.
- ▶ Usability enhancements to the Access Control portlets.
- ▶ WebSphere Member Manager enhancements: *Realms* for virtual portal.

To summarize, some of the new features with WebSphere Portal V5.1 security include:

- ▶ Improved User and Group Permissions portlet
- ▶ Ability for specific login customization
- ▶ Login portlet
- ▶ Java 2 Security

For more information, see the IBM WebSphere Portal security solutions white paper, *Integrating WebSphere Portal software with your security infrastructure*, G325-2090-01, available at:

ftp://ftp.software.ibm.com/software/websphere/pdf/WS_Portal_Security_G325-2090-01.pdf

1.8 Administration, operations, and deployment enhancements

There are number of enhancements of the administration, operations, and deployment of WebSphere Portal V5.1. Some of the major enhancements include:

- ▶ Portal navigation
Users can now use the Back button of the browser to navigate back through the recent history of the views of the portal pages.
- ▶ Reverse caching of portal pages
You can deliver information-centric portal pages (for example, News Pages) from page caches.
- ▶ Move pages
You can move pages and their child pages to any destination within the portal that you need. This is similar to the *cut and paste* functionality.
- ▶ Enhanced access control management
 - User and Group Permissions portlet now displays all role assignments for the selected user and all child resources of a selected parent resource in one view.
 - Support for custom action sets and custom resource types.
- ▶ Import XML portlet
The purpose of this portlet is to enable the user to point to an XMLAccess file and have it executed. This is very similar to the command-line way of executing xmlaccess. When executing the XMLAccess file here or in a command line, the exact same results occur.
- ▶ Export option
The option enables you to move a particular portal resource into XML format, which can be imported later. This is beneficial if you are developing your portal application remotely across number of centers. You can export an XML resource and easily import the resource.

- ▶ Administrative performance enhancements
 - Search users/groups.
 - Search portlet/pages.
- ▶ Administrative portlets enhancements
 - JSR 168 portlet management including portlet wiring for JSR 168 portlets.
 - Web Services for Remote Portlets (WSRP) consuming and producing support.
 - Taxonomy Manager and Search Administration.
 - XMLAccess import and export through a portlet UI.
 - Ability to move pages and page hierarchies.
 - Caching: Ability to set portlet and page caching properties.
- ▶ Another operations enhancement is scripting support for key administration functions.

The Portal Scripting Interface enables you to create scripts that portal administrators can use to perform administrative tasks from a command line. The Portal Scripting Interface enables portal solution development teams to write scripts that are later executed by operation teams for solution deployment. These scripts have the same functionality as the portal administration user interface. This enables you to implement automated configuration management for various kinds of configuration changes. Scripts provide repeatability and avoid user errors that are likely in manual administration procedures.

The scripting syntax is based on JACL, which is the scripting language supported by the wsadmin tool of WebSphere Application Server. The portal scripting component is an extension to the wsadmin tool of the WebSphere Application Server. Example 1-1 shows an example of using the scripting syntax.

Example 1-1 Create new content tree with pages

```
$Content select the root
$Content select [$Content create label Test]
$Content select [$Content create label Trial]
$Content create page abcAtTest
$Content create page zzzAtTest
$Content select the parent
$Content select [$Content create label Office]
$Content create page vvvInOffice
$Content create page mmmInOffice
```

With WebSphere Portal V5.0, WebSphere Portal did a good job supporting the movement of full WebSphere Portal configurations from staging to production;

however, it did not provide automated support for the staging of incremental and differential releases of WebSphere Portal. That is, after moving to a running portal on a staging and production environment, you need to be able to make and test changes on the staging server. When these changes were modifications or additive, everything was fine, but when it included deletions, the deletions had to be done manually on the production server. With WebSphere Portal V5.1, we have the release manager to aid in this process.

WebSphere Portal V5.1 provides support for WebSphere Application Server Network Deployment Manager. Specifically, we now enable WebSphere Portal to be installed into an existing WebSphere Application Server V5 cell and allow configuration changes to WebSphere Portal without first taking the node out of the cell.

To summarize some of the administration and operation enhancements with WebSphere Portal V5.1:

- ▶ Staging to production:
 - Currently, WebSphere Portal does not provide automated support for staging of differential releases of portals.
 - Developed the *release manager* to automate and simplify the process.
- ▶ Scripting interface for administration:
 - Support for delegated administration using scriptable interfaces for integration tasks (for example, during release construction or operation).
 - Basically, enable portal administration through a command-line interface.
- ▶ Log message explanations and user actions:
 - Integrated with the *Information Center*.
 - Continuously enhanced and provided on the Web.

1.9 Personalization

With Personalization, Web sites customize content automatically for each user based on their profile information. With WebSphere Portal V5.1, the Personalization interface consists of three portlets:

- ▶ Personalization Navigator: The main navigation interface.
- ▶ Personalization Editor: The portlet where users edit element content or information.
- ▶ Personalized List: Enables users to display personalized content without having to build a custom JSP portlet.

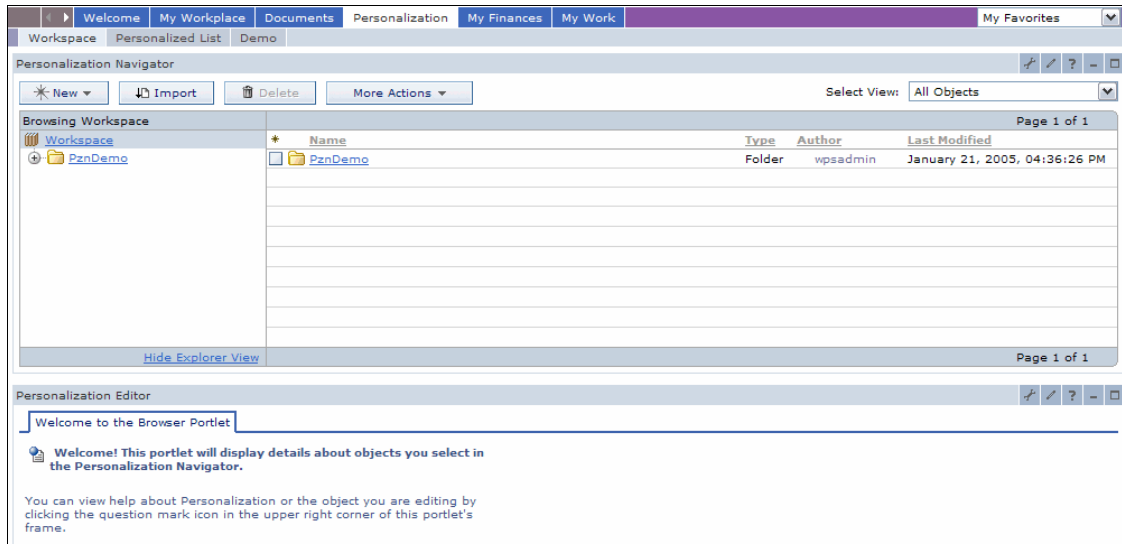


Figure 1-7 Out-of-the-box Personalization portlets

Some of the features of Personalization and the tasks that you can perform using these Personalization portlets include:

- ▶ Match users to the best content for their interests and needs.
- ▶ Business experts create the rules for classifying users and selecting content.
- ▶ Campaign manager applies special rules during specific time periods.
- ▶ Send personalized, targeted e-mail to a set of users.
- ▶ Targeted by a selection rule.
- ▶ Personalized by a JSP e-mail body with embedded rules.
- ▶ Send e-mail once or on a recurring basis.

1.10 Web Content Management

IBM Workplace Web Content Management has changed from an applet-based user interface to a portlet-based user interface and makes use of WebSphere Member Manager for storing its users and groups. These two items help Web Content Management integrate much better with WebSphere Portal. In addition, Web Content Management will be able to reference Document Manager documents within Web Content Management presentation templates and Personalization rules will be able to be used to display Web Content Management content within Web Content Management templates.

To highlight some of the Web Content Management features:

- ▶ Lightweight versioning
- ▶ Portlet Secure Sockets Layer (SSL) support
- ▶ Group 2 languages (except Bidi), enablement and translation

There are many enhancements to the user interface, including:

- ▶ Ordering and filtering of content. This can be useful when finding content in a large repository.
- ▶ Rich text editor enhancements.
- ▶ Multi-object actions, for example, deleting, moving, and versioning multiple objects.
- ▶ Enhanced access control, using new view privileges to hide sections of the UI.
- ▶ People awareness.
- ▶ Managed reuse of WebSphere Portal documents.
- ▶ Workflow enhancements, for example, use Portal or LDAP groups, or both, for Web Content Management workflow.
- ▶ Enterprise user management and directory support.
- ▶ Advanced Personalization and conditional presentation of external content.
- ▶ Ability to use the site search capabilities to search for Web Content Management content.

1.11 Programming model enhancements

With WebSphere Portal V5.1, there are enhancements to the general programming model to make it easier to create portlets and customize the portal. The biggest change in this area is in providing consistent support for the navigation state within portal. The navigation state concerns *where in the portal you are versus the application state*. By formally defining the navigation state and how deal to with it in your portlets, WebSphere Portal can provide consistent Back button behavior.

Programming model enhancements include:

- ▶ Portlet services for standard portlets: Allow standard and legacy portlets to use standards-based portlet services.
- ▶ Struts portal framework support for JSR168 API.
- ▶ Public APIs: More public APIs.

- ▶ CreateURL:
 - Page, Portlet, NavState
 - Login, SelfCare, Enrollment portlets
- ▶ Portal tools are fully integrated to support portal and portlet development. No Portal Toolkit exists on IBM Rational® Application Developer Version 6.0. There are new tools for WebSphere Portal support called *Portal Tools* in Rational Application Developer V6.0. New features include:
 - Portal site development
 - Portal Designer: New tool for customizing portal pages (layout, navigation links)
 - Visual themes and skins development
- ▶ JSR 168 Extensions:
 - Functionality provided in addition to the standard in WebSphere Portal V5.0.2.1:
 - Parallel portlet rendering.
 - Markup property provided in order to handle markups that are not distinguishable through the MIME type, such as cHTML.
 - Enhanced administrative capabilities, for example, you can clone portlet applications.
 - Functionality provided in addition to the standard in WebSphere Portal 5.1:
 - Portlet services concept (based on JNDI lookup):
 - Credential Vault service.
 - Content access service.
 - URL generation service.

Create action or render links to other portlets on the same or on different pages, and create links to portal resources, such as icons.
 - Inter-portlet communication for JSR 168 portlets:
 - Portlets can send events to other portlets on the same page.
 - Based on the property broker infrastructure.
 - Support of Struts V1.1: Struts portlet framework that integrates JSR 168 portlets into the Struts framework.
 - Advanced caching support:
 - Support for remote caching in edge servers.
 - Portlets can set the cache scope (shared or non-shared) and an expiration time.

- Support of sessions for anonymous users.

1.12 Summary

In this chapter, we described some of the new features and enhancements of WebSphere Portal V5.1. You now should have a good understanding of the new features of WebSphere Portal V5.1 before you begin the product installation.



WebSphere Portal V5.1 planning and requirements

In the following chapters, we describe the lab environments for Microsoft Windows, Linux, IBM AIX, and Linux on zSeries and the hardware and software used to set up and configure IBM WebSphere Portal solutions running on these platforms. However, depending on your particular WebSphere Portal business solution, we suggest that you visit the *IBM WebSphere Portal for Multiplatforms Version 5.1 Information Center* to view the complete information about planning activities for WebSphere Portal:

<http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/index.html>

This *Information Center* provides information about the following subjects:

- ▶ Planning considerations
- ▶ Supported hardware and software
- ▶ Software and hardware topologies
- ▶ Additional resources for planning

2.1 Hardware requirements

The Supported hardware and software section of the *IBM WebSphere Portal for Multiplatforms Version 5.1 Information Center* provides data for hardware configurations that have been tested by IBM. You should use the information found here as a guide for your installation of WebSphere Portal. Also refer to “Preparing your operating system for WebSphere Portal” in the “Installing” section for more information about the following topics:

- ▶ IBM AIX systems
- ▶ HP-UX systems
- ▶ Linux Intel® systems
- ▶ Linux on iSeries™ systems
- ▶ Linux on pSeries® systems
- ▶ Linux on S/390® systems
- ▶ Linux on zSeries systems
- ▶ Sun Solaris systems
- ▶ Microsoft Windows systems

2.2 Software requirements

The Supported hardware and software section of the *IBM WebSphere Portal for Multiplatforms Version 5.1 Information Center* provides the minimum product levels that you should install for WebSphere Portal. Because other products frequently ship fixes, updates, and new releases, every possible configuration has not been tested, for example:

- ▶ Supported operating systems (required on the WebSphere Portal machine)
- ▶ Supported application servers (required on the WebSphere Portal machine)
- ▶ Supported Web servers (Windows/UNIX®, optional)
- ▶ Supported databases (required)
- ▶ Supported LDAP directories (optional)
- ▶ Supported Web browsers (required)
- ▶ Supported software for collaboration (optional)
- ▶ Supported software for content management (optional)
- ▶ Supported external security software (optional)
- ▶ Supported software for portlet development (optional)

- ▶ Other supported software (optional)

Note: In the following chapters, we use the CD set from *WebSphere Portal V5.1 - WebSphere Portal Extend for Multiplatforms, V5.1*. Therefore, if you are using another set of CDs from a different shrink-wrap or download, there might be a difference in the CD numbering and naming systems.



WebSphere Portal: Microsoft Windows Server 2003 install

This chapter describes the installation and configuration of IBM WebSphere Portal for Multiplatforms V5.1 on Microsoft Windows Server 2003 in a single-tier environment.

The installation configuration includes the following components (as shown in Figure 3-1 on page 30):

- ▶ Server 1:
 - WebSphere Application Server V5.1.1.1
 - WebSphere Business Integration Server Foundation V5.1.1
 - WebSphere Portal V5.1
 - Migrates the data store from IBM Cloudscape to IBM DB2 UDB Enterprise Server Edition V8.1.1.94
 - Collaborative portlets
 - WebSphere MQ
- ▶ Server 2:
 - Lotus Domino as LDAP Release 6.5.3
 - Lotus Team Workplace Release 6.5.1

- ▶ Server 3:
 - Lotus Domino as LDAP Release 6.5.3
 - Lotus Instant Messaging and Web Conference Release 6.3.1

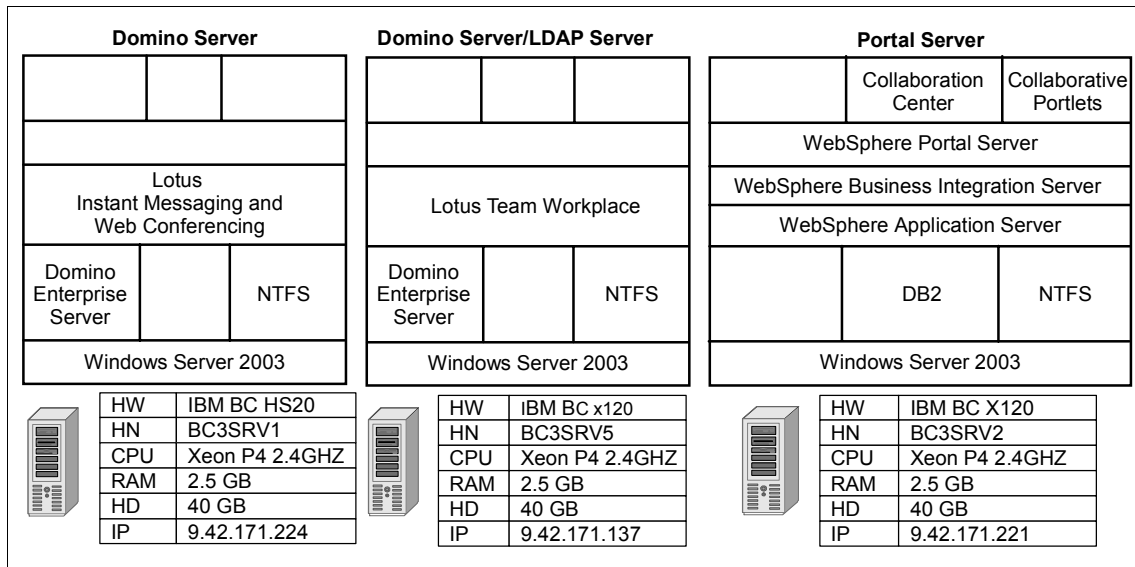


Figure 3-1 Lab configuration for Windows Server 2003 installation

Note: In previous versions, it was possible to have Lotus Instant Messaging and Team Workplaces on the same Lotus Domino server. In the current release, the install can be problematic when installing them onto the same server. That is why in Figure 3-1, we separated them out and linked the Domino servers.

This section depicts the lab configuration of the WebSphere Portal Extend offering in V5.1. WebSphere Portal is shipped with multiple software components. It provides the clients with an open architecture framework and the flexibility to integrate with other software components.

WebSphere Portal provides additional services such as single sign-on, security, directory services, content management, collaboration, search and taxonomy, support for mobile devices, accessibility support, internationalization, and site analytics. Updates in the 5.1 release include enhanced search capabilities, virtual portals, a new configuration wizard, and expanded development tools. Clients can further extend the WebSphere Portal solution to provide host integration and e-commerce (see the context diagram in Figure 3-2 on page 31).

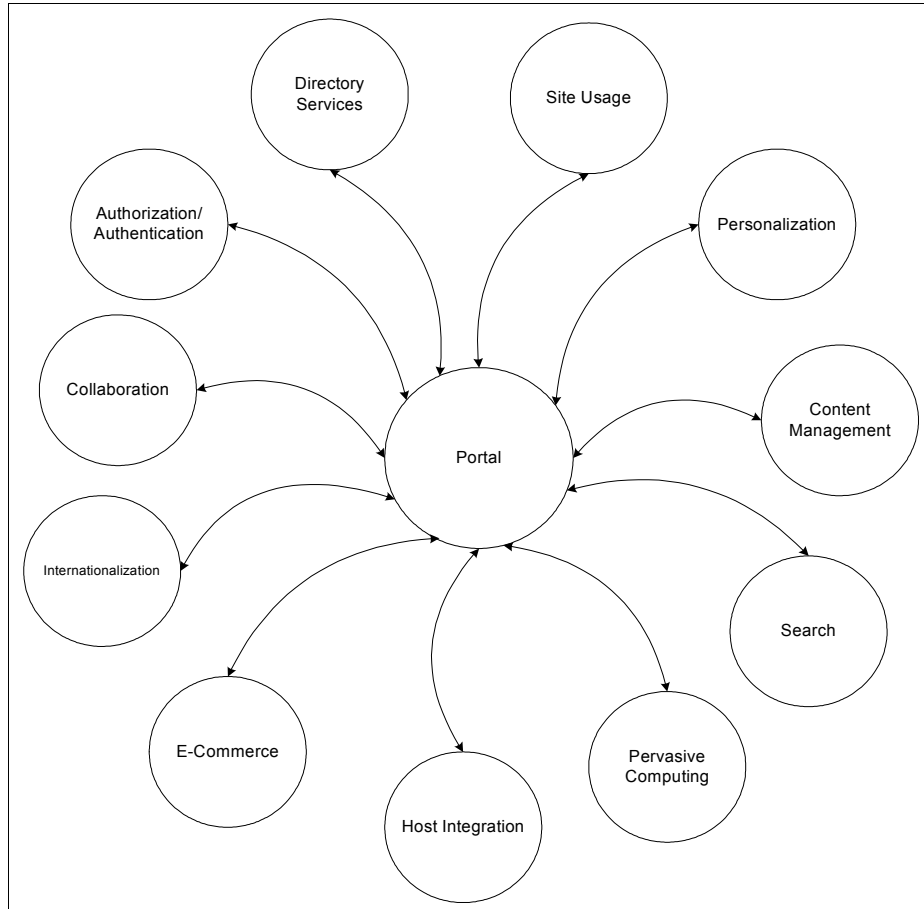


Figure 3-2 Context diagram

We conducted a proof of concept in the ITSO Raleigh lab environment. We depicted a distributed architecture in the Windows environment and a demilitarized zone architecture for the Linux and AIX environments. For demonstration purposes, integration to external directory services, Web Content Management and Collaboration Center, is depicted in the Windows environment only. Clustering will be demonstrated in the Windows configuration only.

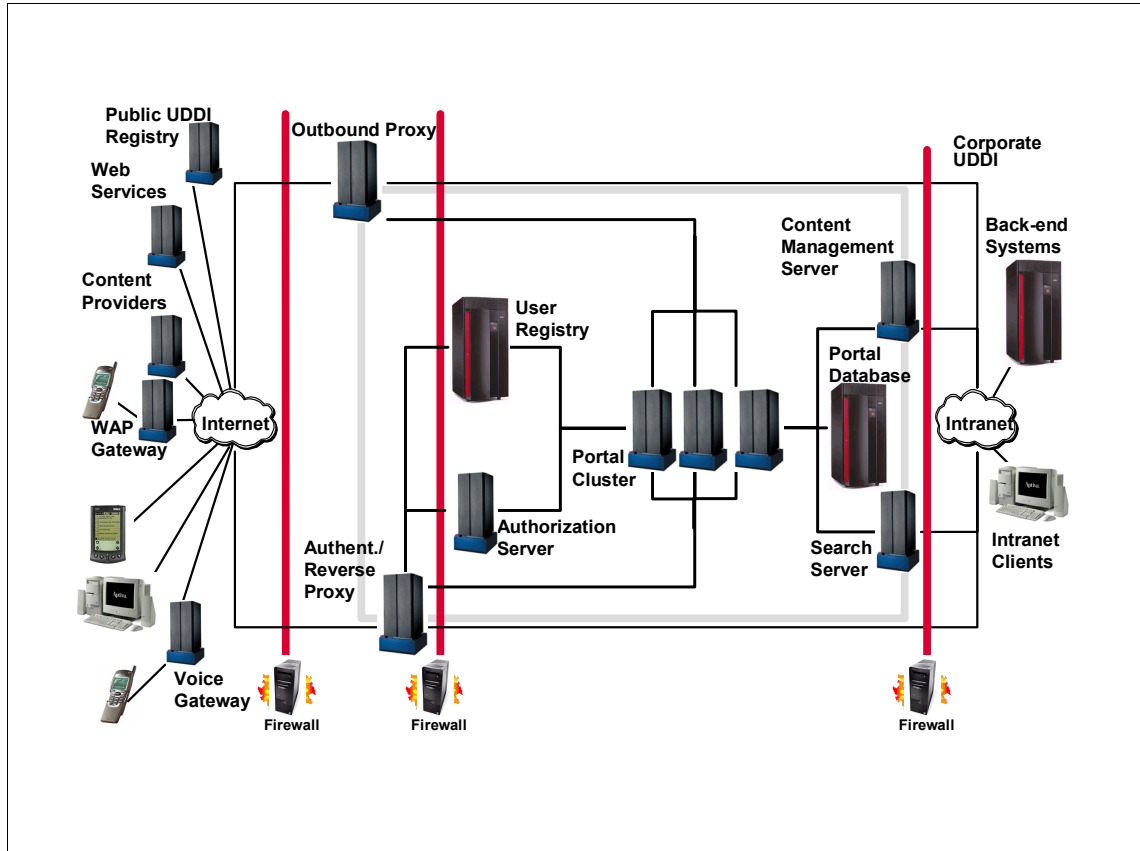


Figure 3-3 Distributed multi-tier portal architecture

WebSphere Portal V4.x addresses most WebSphere Portal requirements in a client environment and results in a relatively complex install. WebSphere Portal V5.1 is based on a modular approach. The base configuration installs WebSphere Application Server V5.1.1.1, WebSphere Business Integration Server Foundation V5.1.1, the Cloudscape database, and WebSphere Portal software. The client can then tailor the WebSphere Portal solution to best fit the requirements by changing the database used by the portal, switching to a custom user registry, using one of the supported LDAP servers, using integration to host systems, enabling a proxy for access of remote content through the portal, and so on. IBM is one of the few vendors that provides not only an open architecture but also an end-to-end solution in the portal solution space. IBM provides IBM Tivoli Access Manager and IBM Tivoli Identity Manager from the Tivoli family of products to handle advanced authentication and authorization, WebSphere Application Server Network Deployment from the WebSphere family to provide an application server and clustering, messaging queue service from the

WebSphere MQ family, Host-on-Demand for host integration, WebSphere Commerce for e-commerce, directory services such as IBM Tivoli Directory Server or Domino, a database such as DB2, Site Analyzer for site usage, and so on. This gives the client the flexibility and options to integrate with the best-of-breed software to create the end-to-end portal solution. Refer to Figure 3-3 on page 32 when planning for a client implementation.

A base configuration installs Cloudscape as the database repository. Clients planning to pursue better database performance should upgrade to a more robust database. The steps to migrate the database repository from Cloudscape to DB2 is demonstrated in the proof of concept.

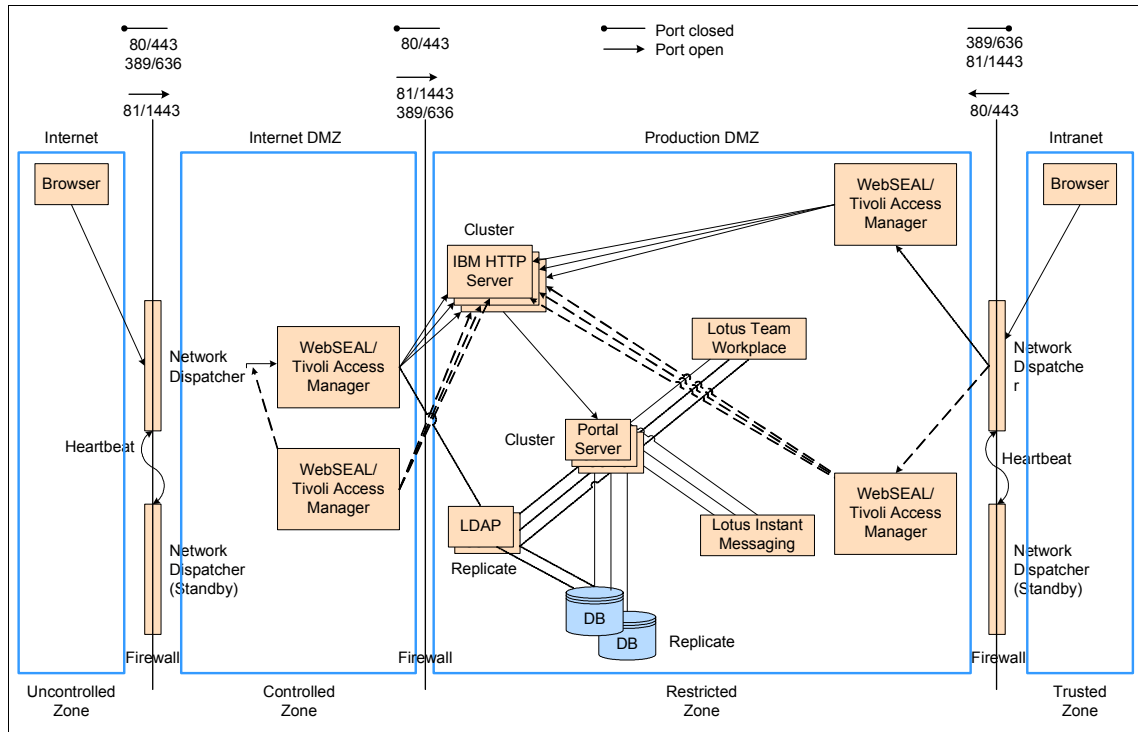


Figure 3-4 Example WebSphere Portal architecture with high availability

In Figure 3-4, we depict a sample architecture deploying WebSphere Portal in a multi-tier demilitarized zone (DMZ) configuration with high availability. This configuration can be used for an Internet/extranet portal solution.

In this configuration, Tivoli Access Manager WebSEAL is used to shield the Web server from unauthorized requests for external facing users. This approach is desirable when the Web server might contain sensitive data and direct access to it is not desirable.

WebSEAL is a reverse proxy security server (RPSS) that uses Tivoli Access Manager to perform coarse-grained access control to filter out unauthorized requests before they reach the domain firewall. WebSEAL uses Tivoli Access Manager to perform access control, as illustrated in Figure 3-4 on page 33. In the particular example of integrating with WebSEAL, you can configure WebSphere Application Server to use the LDAP user registry, which can be shared with WebSEAL and Tivoli Access Manager. Replicated front-end WebSEAL provides the portal site with load balancing during periods of heavy traffic and failover capability. The load balancing mechanism is handled by a Network Dispatcher such as IBM WebSphere Edge Server. If the Network Dispatcher fails for some reason, the standby Network Dispatcher will continue to provide access to the portal. In our sample configuration, HTTP servers and WebSphere Portal are clustered to provide additional redundancy.

The directory server can be replicated to one or more replica LDAP servers to provide redundancy. WebSphere Application Server uses LDAP to perform authentication. The client ID and password are passed from WebSphere Application Server to the LDAP server. Replication can be turned on in the database server that is used by the portal.

In this configuration, you can optionally use a separate WebSEAL for the internal users for better performance.

3.1 Using install logs

Important: For information pertaining to the hardware and software prerequisites for a WebSphere Portal for Windows installation, refer to the *IBM WebSphere Portal for Multiplatforms Version 5.1 Information Center* at:

<http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/index.html>

This section contains information to assist an administrator in preventing, identifying, and correcting problems with WebSphere Portal.

Using WebSphere Portal log files

WebSphere Portal has log files that are created during the installation and runtime. This section describes the content of the log files and includes recommendations as to when to check the log files.

Installation log files

The installation log files (Table 3-1 on page 36) are in the directory <wp_root>/log, where <wp_root> is the directory where WebSphere Portal is installed. The table lists each file, describes the file content, and recommends when to check the file for information that might assist in troubleshooting installation problems. Not all of the files will be present, because in the new WebSphere Portal V5.1 InstallShield, there are two paths that it can take. One is a regular install, and the second is an archive install. The second installation path takes considerably less time. The InstallShield will survey your system, and depending on various items, will decide which path to take.

Table 3-1 Log files under the <wp_root>/log directory

Log file name	Description	Problem symptoms
wpinstallog.txt	Contains trace information generated by the installation program.	Check this log if the WebSphere Portal installation stops before successful completion.
installmessages.txt	Contains messages generated during the installation. The messages in this file are translated for the language specified during the installation.	Check this log for errors generated during the installation.
portletinstall.txt	Contains messages generated during the portlet installation.	Check this log if problems occur with portlets being deployed during installation.
mq_install.log	Contains messages generated during the silent WebSphere MQ installation.	Check for problems if WebSphere MQ fails to install.
jcrdb.log	Contains messages generated during JCR database configuration.	Check for errors during the database transfer.
cmlnit.log	Contains messages for the IBM Lotus Workplace Web Content Manager installation.	Check for errors during the IBM Lotus Workplace Web Content Manager installation.
wpwasfp1.txt	Contains trace information generated during the installation of WebSphere Application Server Fix Pack 1.	Check this log if you have problems with the installation of WebSphere Application Server Fix Pack 1.
wppmefp1.txt	Contains trace information generated during the installation of WebSphere Application Server Enterprise Edition Fix Pack 1.	Check this log if you have problems with the installation of WebSphere Application Server Enterprise Edition Fix Pack 1.
log.txt	Contains trace information generated during the installation of WebSphere Application Server. Note: Located in the <was_root>/logs directory.	Check this log if you have problems with the installation of WebSphere Application Server.
WAS.PME.install.log	Contains trace information generated during the installation of WebSphere Application Server Enterprise Edition. Note: Located in the <was_root>/logs directory.	Check this log if you have problems with the installation of WebSphere Application Server Enterprise Edition.

The following log files (Table 3-2 on page 37) are located in the <temp> directory and are used during the installation. Note that the wpinstallog.txt and wpsinstallog.txt log files previously described begin in the <temp> directory and

are moved to <wp_root>/log early in the installation.

Table 3-2 Log files under the <temp> directory

Log file name	Description	Problem symptoms
installtraces1.txt installtraces2.txt installtraces3.txt	Contain trace information generated by the dependency checking function. Output is added to installtraces1.txt until it reaches a predefined size, at which point output goes into installtraces2.txt and then into installtraces3.txt. When installtraces3.txt is full, output reverts to installtraces1.txt and overwrites previous trace information.	Check these files if there are problems with component discovery and dependency checking.
LocalizeConfigMessages.log LocalizeConfigTrace.log LocalizeConfigtrace1.log LocalizeProgress.log LocalizeTrace.log	Contain information used by the archive install. Output is added to all files, and then at the end, they are copied to wp_root\log.	Check these files if there are problems with the archive install of WebSphere Application Server or WebSphere Portal.

3.2 Base installation

Note: In lab, to speed up the installation, we put all of the CDs in a network share point. You would need the following CDs located there for the base install:

- ▶ Setup
- ▶ CD1-1
- ▶ CD4-1
- ▶ CD5-1
- ▶ CD5-3

For our lab installation, Table 3-3 on page 38 specifies the CDs that are required for the installation of the WebSphere Portal components in this chapter.

Table 3-3 Installation CDs

Disk	Description
CD Setup	WebSphere Portal V5.1 - Portal Install (Setup), V5.1
CD #1-1	WebSphere Business Integration Server Foundation for Windows V5.1
CD #4-1	WebSphere Application Server Archive Install for Windows
CD #4-3	WebSphere Application Server Archive Install for AIX
CD #5-1	Portal Server Archive Install, Windows, V5.1
CD #5-3	Portal Server Archive Install, Windows, AIX, Linux zSeries, Linux Intel
CD #9-1	DB2 UDB Enterprise Edition for Windows V8.1
CD #9-10	DB2 UDB Enterprise Edition Fix Pack 6 for Windows V8.1
CD #12-1	Lotus Domino Enterprise Server for Windows Release 6.5.3
CD #12-6	Lotus Notes®, Designer, and Admin Clients for Windows
CD #13-1	Lotus Instant Messaging and Web Conferencing for Windows V6.5.1
CD #14-1	Lotus Team Workplace for Windows SBCS Group 1 V6.5.1

This scenario takes you through a basic installation of WebSphere Portal, with an emphasis on getting it up and running quickly. At the end of the scenario, you can follow the links to information describing additional functions you can add to your WebSphere Portal environment, such as the use of an LDAP directory for user authentication, or a collaboration function, such as Lotus Instant Messaging and Web Conferencing.

The installation requires you to log on with an ID with sufficient user privileges on the system. The user account must be part of the local Administrators group and must have the following user rights assigned to it:

- ▶ Act as part of the operating system
- ▶ Log on as a service

You can change user privileges by going to **Start** → **All Programs** → **Administrative Tools** → **Local Security Policy**.

This will then open a new window. In this window, expand **Security Settings** → **Local Policies** → **User Rights Assignment**.

Note: After assigning user privileges, you should log off from Windows and log on again for the changes to become effective.

For the base installation of WebSphere Portal, complete the following steps:

1. Run **install.bat** from the setup folder in the Setup CD.
2. Choose your preferred language and click **OK**.
3. Click **Next** and you will have the option to launch the *Information Center* (Figure 3-5).

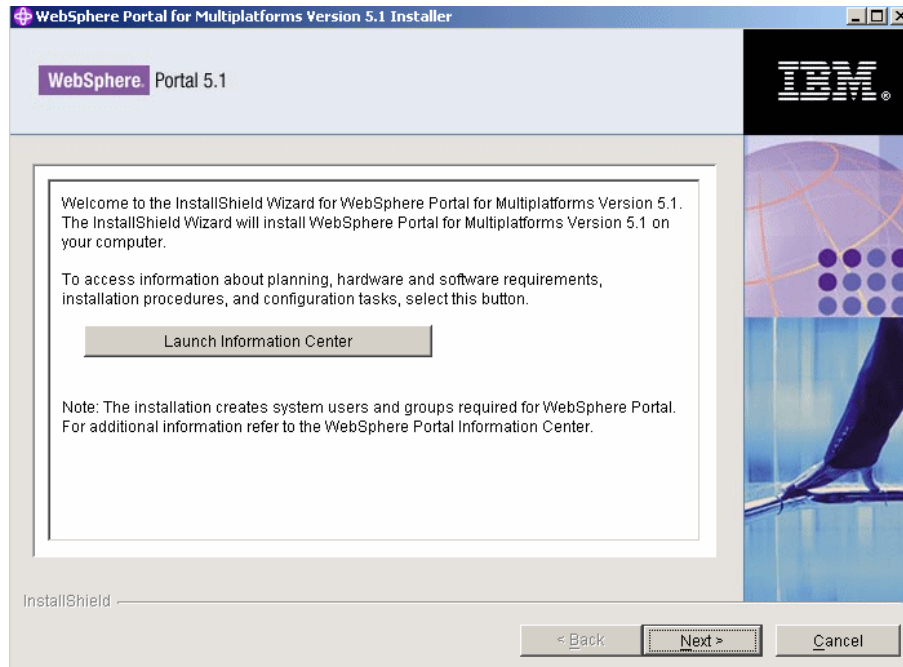


Figure 3-5 Launch Information Center window

4. Click **Next**.
5. Read and the license agreement, and if in agreement, click **Next**.

Note: If you have firewall applications running on the server, a warning message similar to the one shown in Figure 3-6 will be presented. Disable any firewall applications before you proceed.

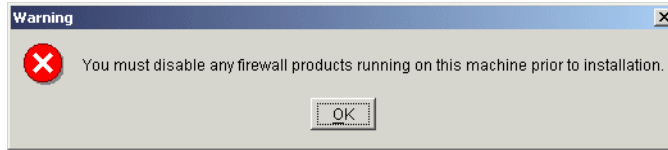


Figure 3-6 Warning message detecting firewall application

6. Select a **Full** installation, as shown in Figure 3-7, and proceed to the next window.

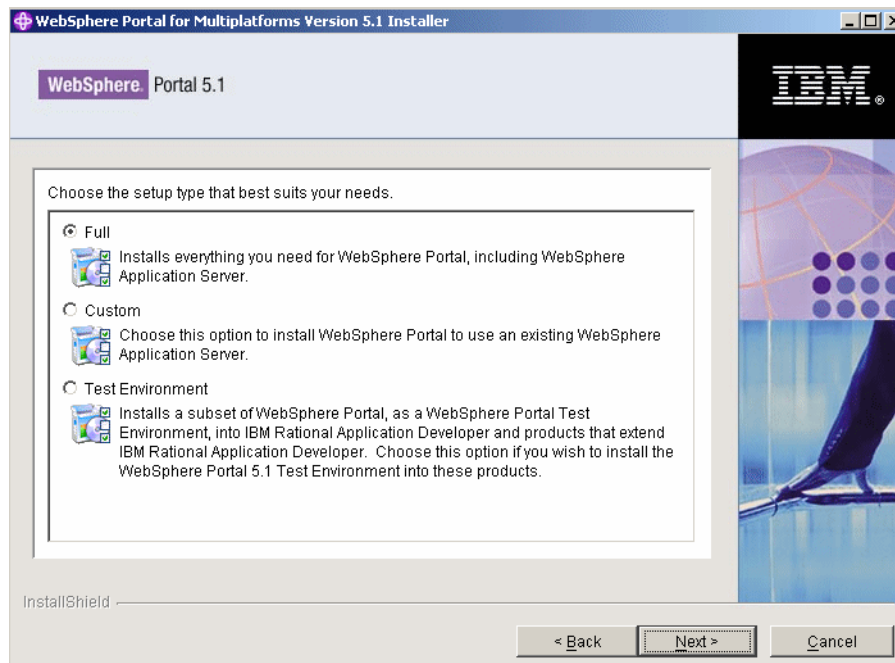


Figure 3-7 Select Full installation

7. Enter your choice for the WebSphere Application Server installation directory (Figure 3-10 on page 43), for example, C:\WebSphere\AppServer, and click **Next**.

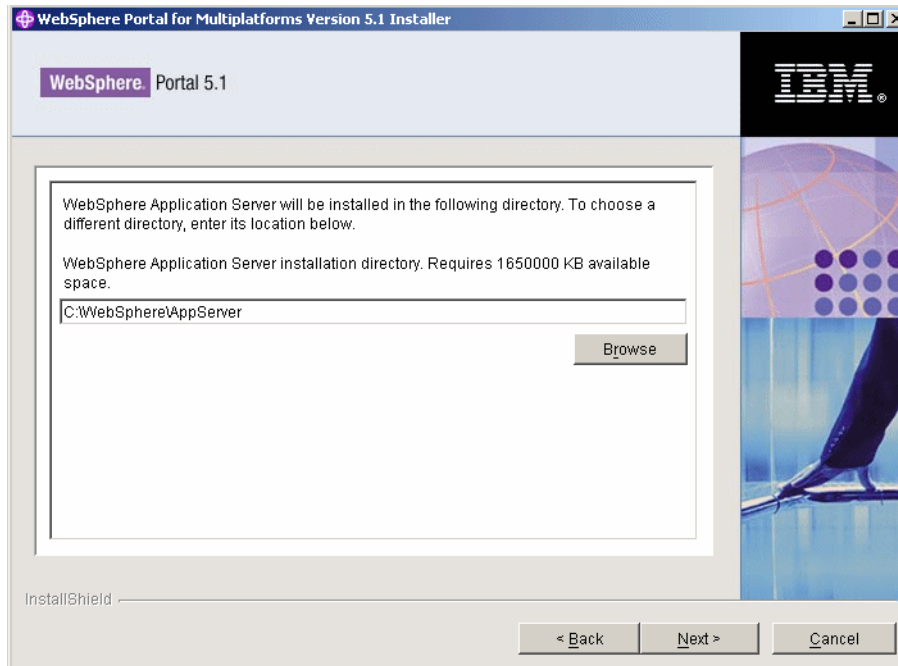


Figure 3-8 WebSphere Application Server installation directory

8. Enter or accept the Node name (for example, top440) and the fully qualified host name (for example, bc3srv2.itso.ra1.ibm.com). See Figure 3-9. Click **Next** to proceed to the next window.

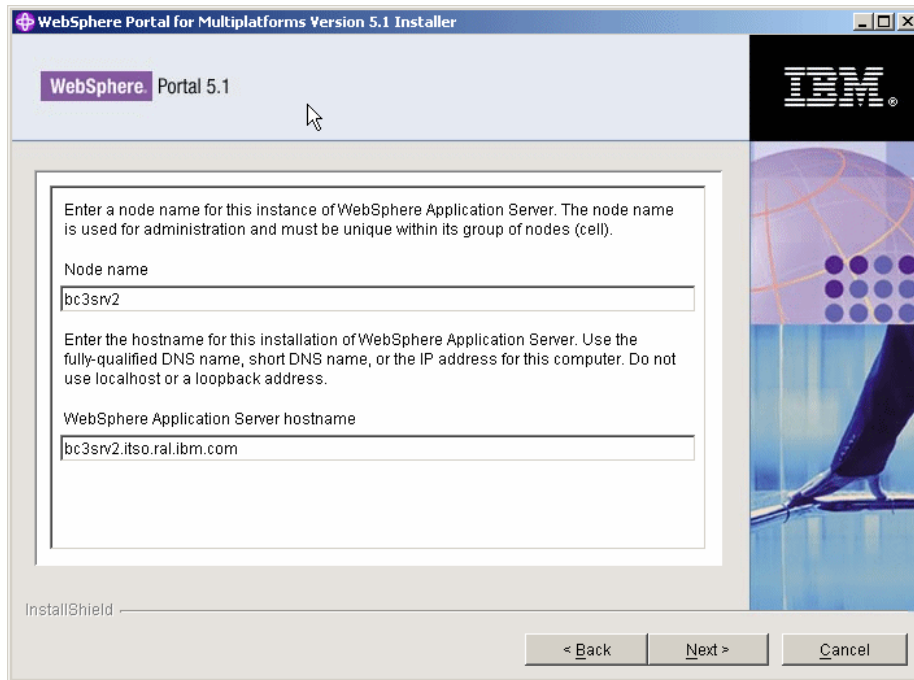


Figure 3-9 Confirm Node name and fully qualified hostname

9. Confirm your choice for the installation directory for WebSphere Portal (Figure 3-10). For our example, we entered C:\WebSphere\PortalServer.

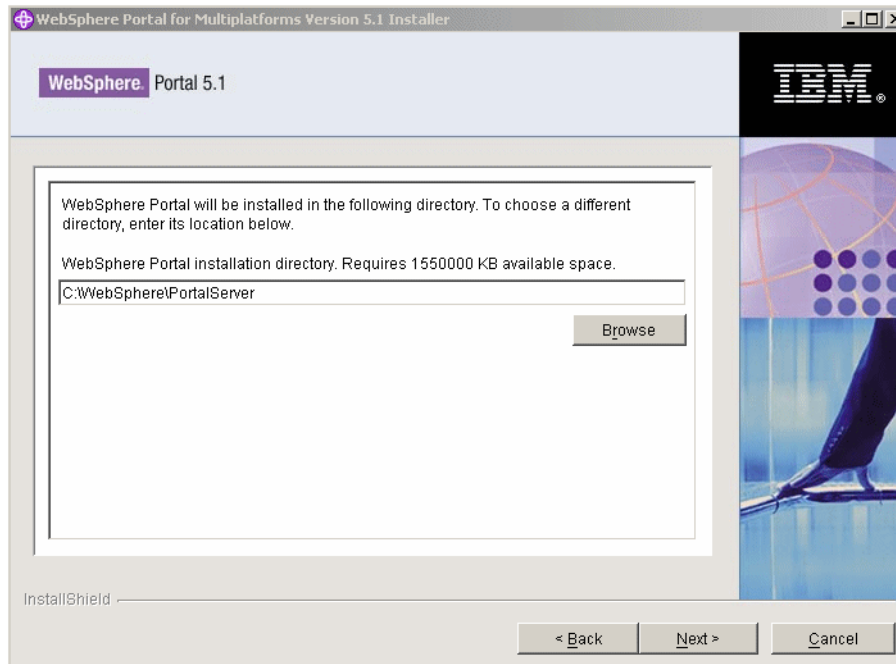


Figure 3-10 WebSphere Portal installation directory

10. Enter the System Logon User ID and Password (Figure 3-11) and accept the default values for the other fields. Click **Next**.

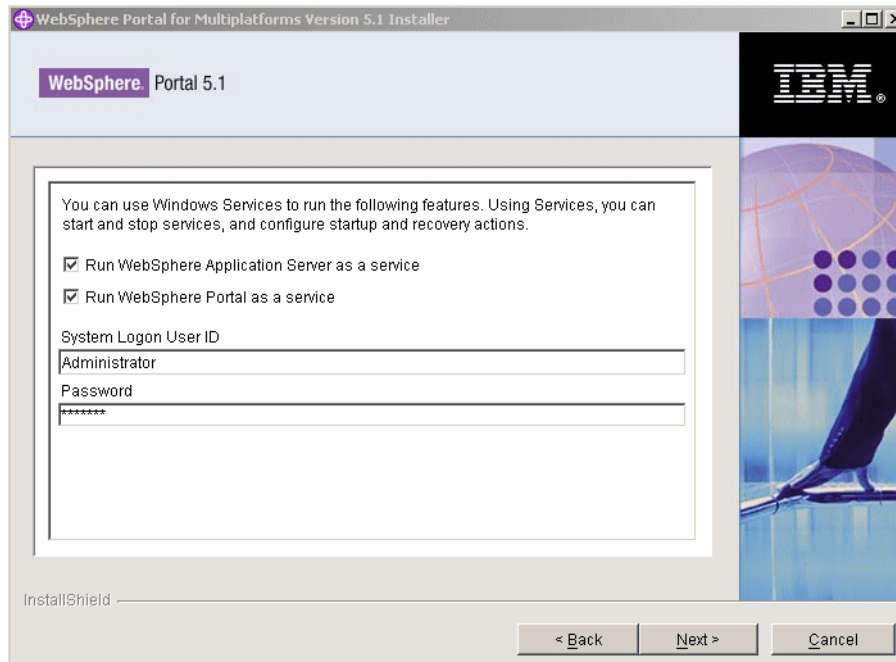


Figure 3-11 Run as a service on Windows

11. Enter your choice of Portal administrative user name and password (Figure 3-12). Do not use blanks in either the user ID or the password fields, 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 the installation. Note that this user ID is only used to log in to WebSphere Portal and is not related to any user IDs used to access the operating system itself. Click **Next**.

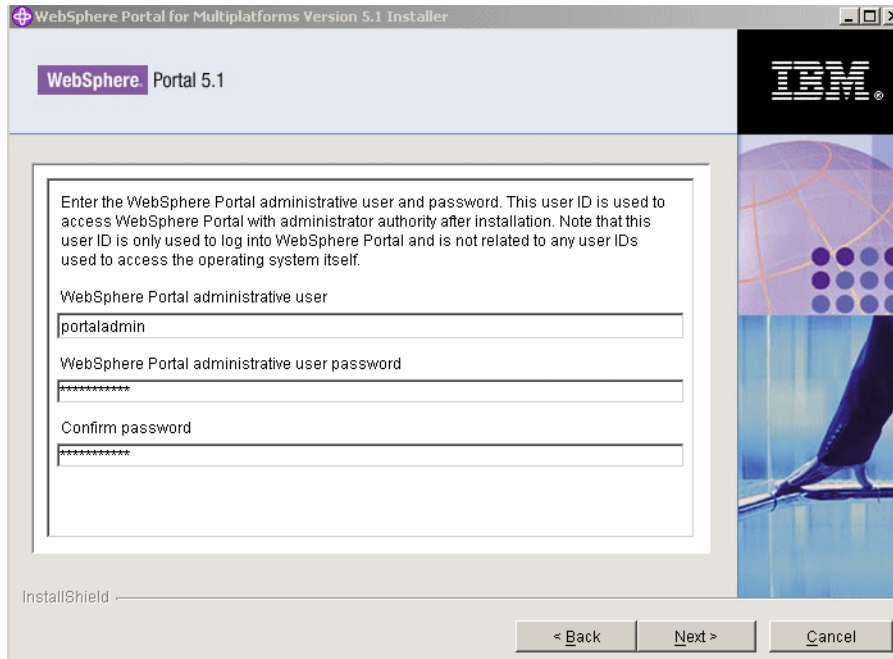


Figure 3-12 WebSphere Portal administrative user name and password

12. Confirm your choices and click **Next** on the summary information window (Figure 3-13).

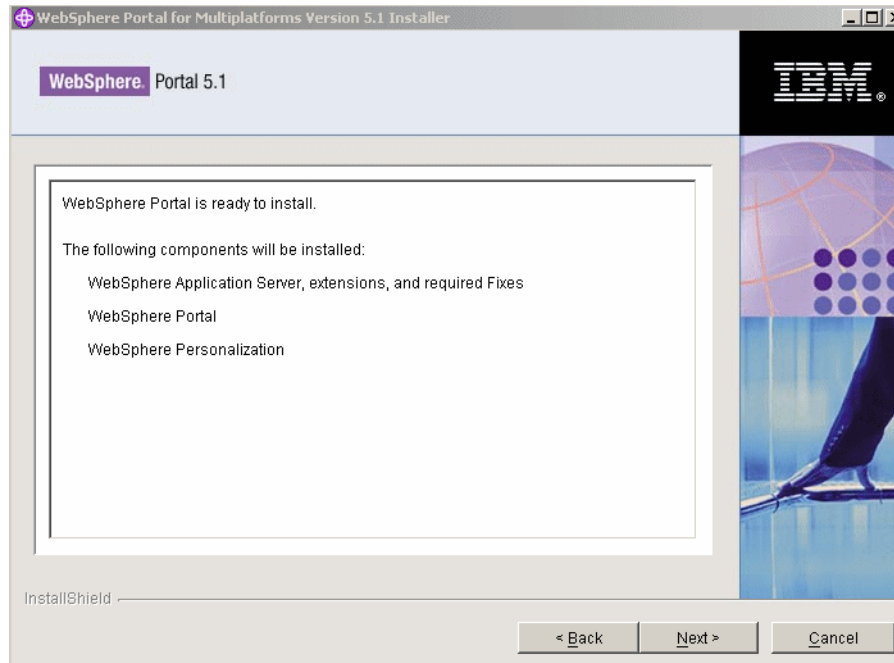


Figure 3-13 Summary information for the installation

13. When prompted, browse to the location of Disk 1-1 (WebSphere Application Server Enterprise for Windows) to continue the installation (Figure 3-14).

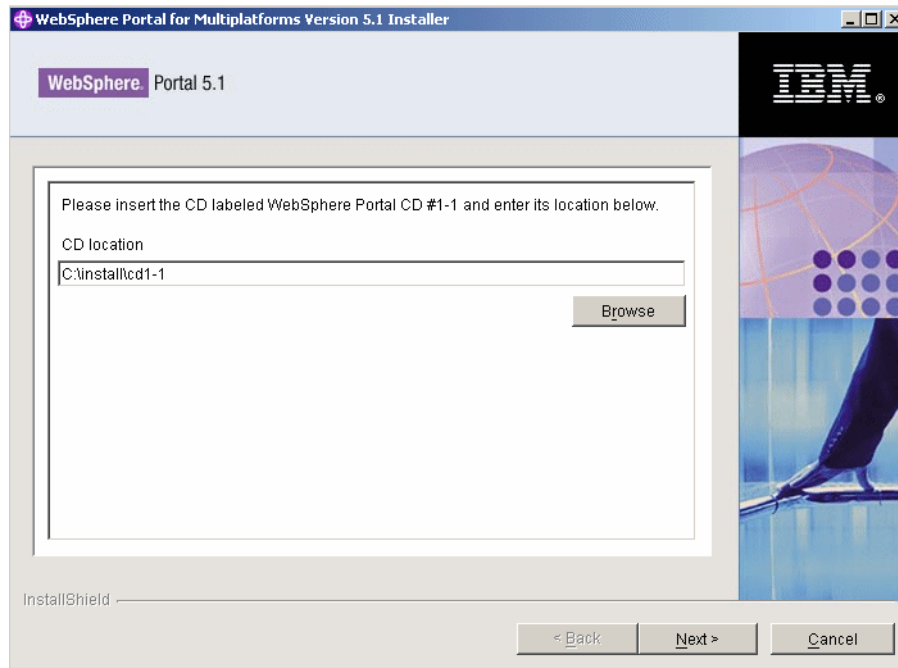


Figure 3-14 Insert Disk 1-1

14. The installer will then proceed with the installation of WebSphere MQ.
15. When prompted, browse to the location of CD 4-3 (WebSphere Application Server Archive Install for Windows). Click **Next**.
16. The installer will then proceed with the installation of WebSphere Application Server and WebSphere Business Integration Server Foundation.
17. When prompted, browse to the location of CD 5-1 (Portal Server Archive Install, Windows, V5.1). Click **Next**.
18. The installer will then install WebSphere Portal and WebSphere Portal Web Content Manager.
19. When prompted, browse to the location of CD 5-3 (Portal Server Archive Install, Windows, AIX, Linux zSeries, Linux Intel). Click **Next**.

Note: The progress bar on the install will reset several times; this is normal.

20. Clear the **Launch First Steps** option.
21. Click **Finish** to complete the installation (Figure 3-15).

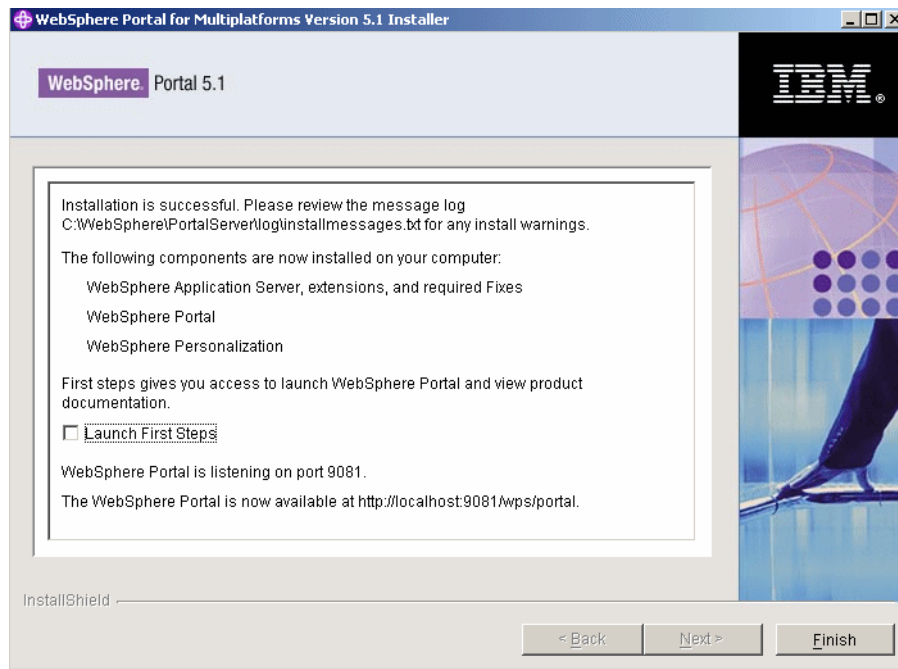


Figure 3-15 Installation complete

Note: Checkpoint for WebSphere Portal

At this point, WebSphere_Portal and server1 are not started. Before continuing, you will need to start them.

To start them, complete the following steps:

1. Open a command prompt.
2. Change the directory to <was_root>\bin (where <was_root> is where you installed WebSphere Application Server, in our example, C:\WebSphere\AppServer).
3. Issue the **startserver.bat server1** command.
4. Wait for it to finish and start up.
5. Then, issue the **startserver.bat WebSphere_Portal** command.

The capitalization is important in the server name. Additionally, for the My Tasks portlet to work, server1 must be running.

To verify that the installation is successful, go to a browser and type in the following URL:

```
http://<fully_qualified_host_name>:9081/wps/portal
```

For example, in our scenario, the URL of the portal will be `http://bc3srv2.itso.ra1.ibm.com:9081/wps/portal`. The Welcome to WebSphere Portal V5.0 portlet will open, as shown in Figure 3-16 on page 50.

Note: Checkpoint for the servlet engine

To verify that the servlet engine is up and running, go to a browser and type in the following URL:

```
http://<fully_qualified_hostname>:9080/snoop
```

Where the <fully_qualified_host_name> in the example is `bc3srv2.itso.ra1.ibm.com`.

See Figure 3-17 on page 51.

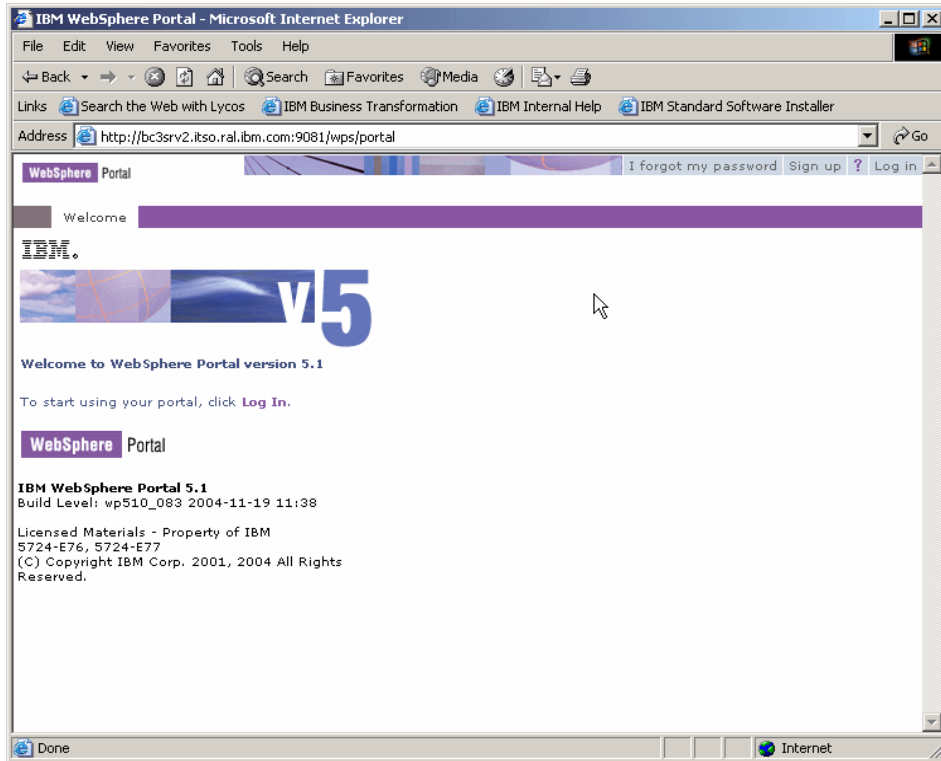


Figure 3-16 Welcome to WebSphere Portal Version 5.1 window

The portal is now up and running.

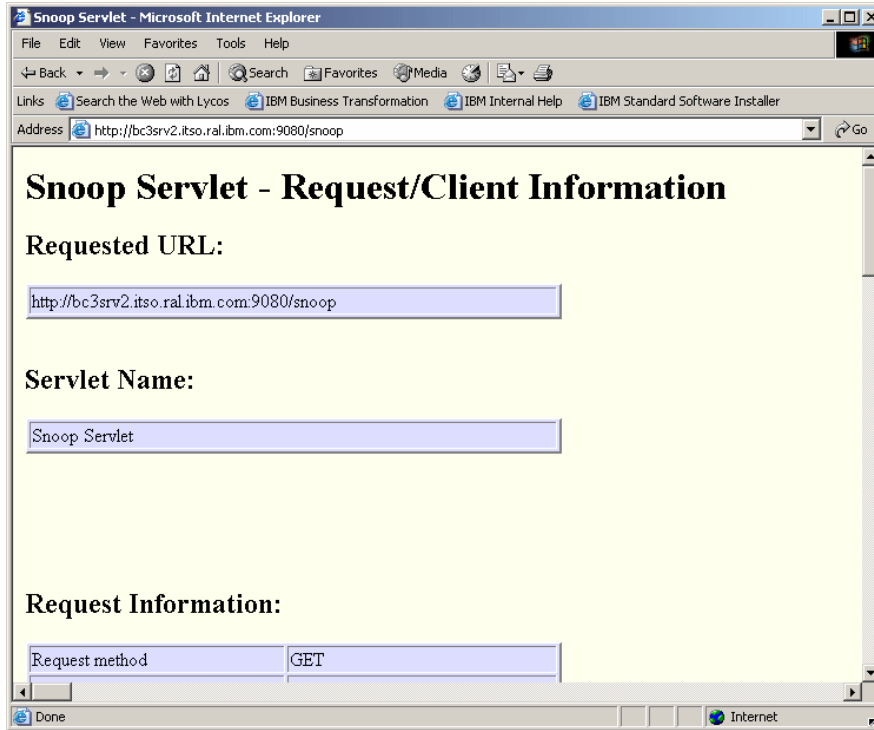


Figure 3-17 Checkpoint for snoop servlet

After completing the checkpoint procedure for the servlet engine, perform the following steps:

1. Click **Sign in** and enter the WebSphere Portal administrator ID and password, as shown in Figure 3-18 on page 52.

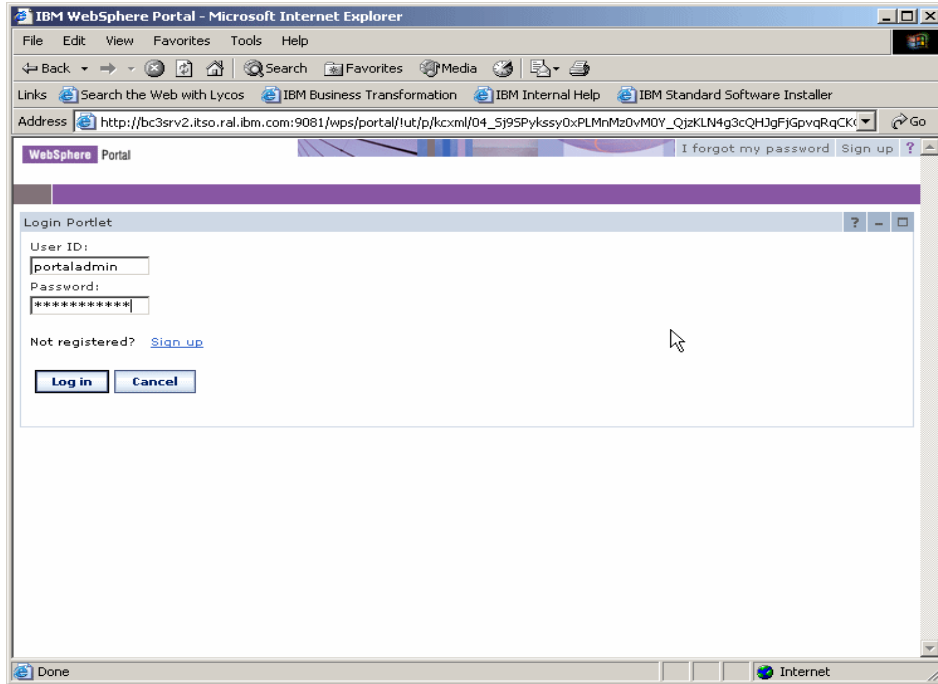


Figure 3-18 Logging in using the WebSphere Portal administrator ID

Note: One of the first differences you will see is that the windows used for the login are gone and it is now a portlet.

2. You are now logged in to WebSphere Portal, as shown in Figure 3-19.

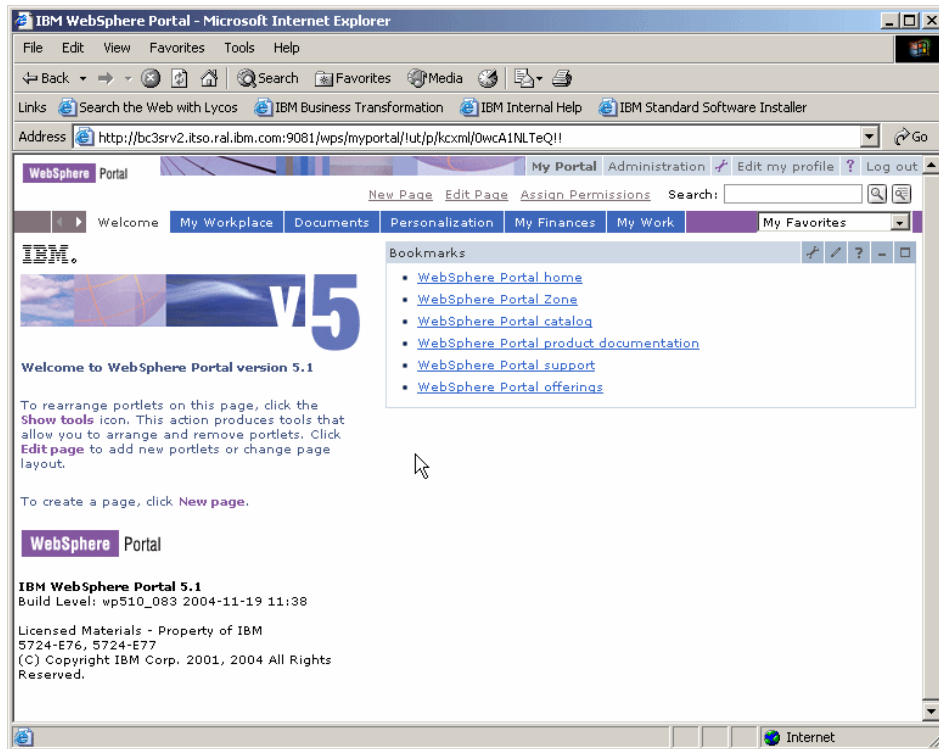


Figure 3-19 WebSphere Portal

The base installation is now complete.

Note: In our installation, we were behind a firewall, so we removed the Screaming Media portlets from the Welcome page because this can impact the login performance (20 minute delay).

3.3 Migrating the database from Cloudscape to DB2

By default, WebSphere Portal installs and uses an IBM Cloudscape database to store information about user identities, credentials, and permissions for accessing portal resources. Cloudscape is a built-in Java database that is well-suited to basic portal environments. However, if the demands of your portal environment include database software with greater capability and scalability, you can also configure WebSphere Portal to use a more robust database, such as IBM DB2 UDB Enterprise Server Edition. For example, Cloudscape does not

support vertical cloning or a cluster environment, nor does it support enabling security in a database only mode. Performance gains might also be possible by moving to a more robust database. If you want to use another database, you must transfer data from the Cloudscape database to your preferred database.

For the purpose of the proof of concept, we illustrate the migration of Cloudscape to a local DB2 database here.

You first need to create a database user on the Microsoft Windows operating system. The user should be defined locally and belong to the local Administrators group. The user ID should have the following user rights:

- ▶ Act as part of the operating system
- ▶ Adjust memory quotas
- ▶ Create a token object
- ▶ Lock pages in memory
- ▶ Log on as a service
- ▶ Replace a process level token

The limitations of the choice of the database ID are as follows:

- ▶ User names in Windows can contain 1 to 30 characters. The Windows NT and Windows 2000 operating systems currently have a limit of 20 characters.
- ▶ Group and instance names can contain 1 to 8 characters.
- ▶ Names cannot be any of the following:
 - users
 - admins
 - guests
 - public
 - local
- ▶ Names cannot begin with:
 - IBM
 - SQL
 - SYS
- ▶ Names cannot include accented characters.

You can assign or change user privileges by going to **Start** → **Administrative Tools** → **Local Security Policy**. Then, expand **Local Policies** → **User Rights Assignment**.

Note: If an earlier version of WebSphere Portal coexists on the same server, the database user ID for WebSphere Portal V5 must be different from the one in the earlier version to avoid conflicts during the installation.

We recommend the database user `wpsdbusr`, with administrative rights.

3.3.1 Installing IBM DB2 UDB Enterprise Server Edition V8.1.1.94

In this section, we install the database to support our WebSphere Portal installation. Complete the following steps:

1. Insert CD 9-1 (DB2 Enterprise Edition for Windows V8.1) and run **Setup.exe** to start the DB2 on Windows installation.
2. Click **Install Products**, as shown in Figure 3-20.

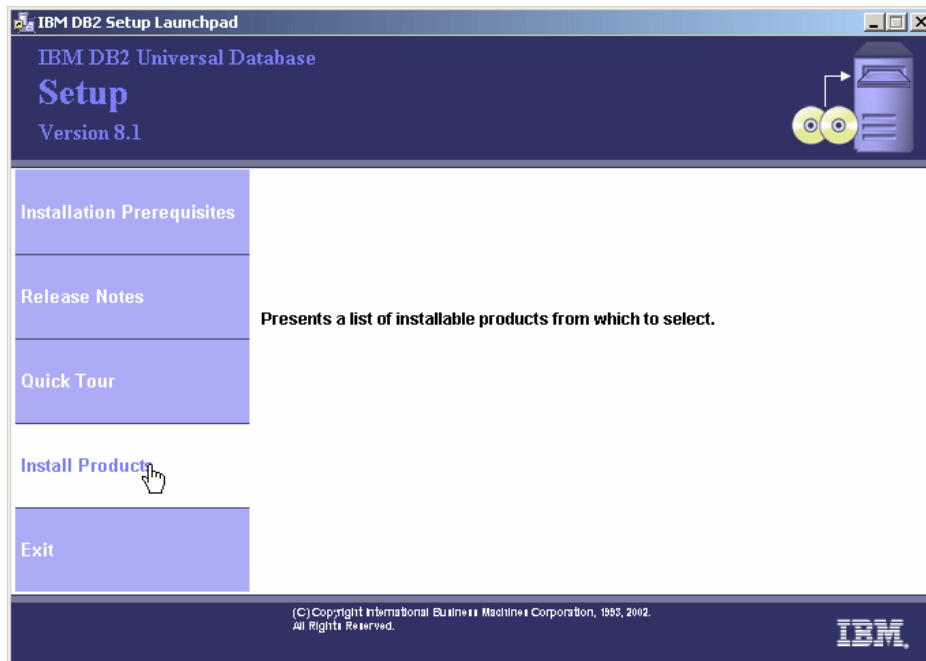


Figure 3-20 Select Install Products

3. Select **DB2 UDB Enterprise Server Edition** to install, as shown in Figure 3-21. Click **Next**.

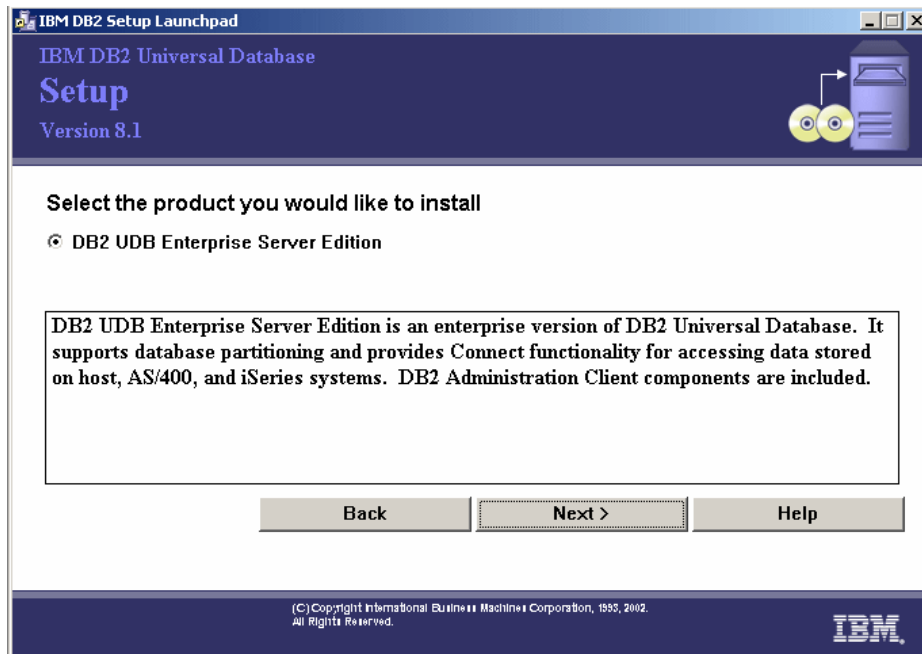


Figure 3-21 Select the product you want to install

4. Click **Next** in the Welcome window.
5. Read and accept the license agreement. Click **Next**.

6. Select **Typical** as the installation type, as shown in Figure 3-22. Click **Next**.

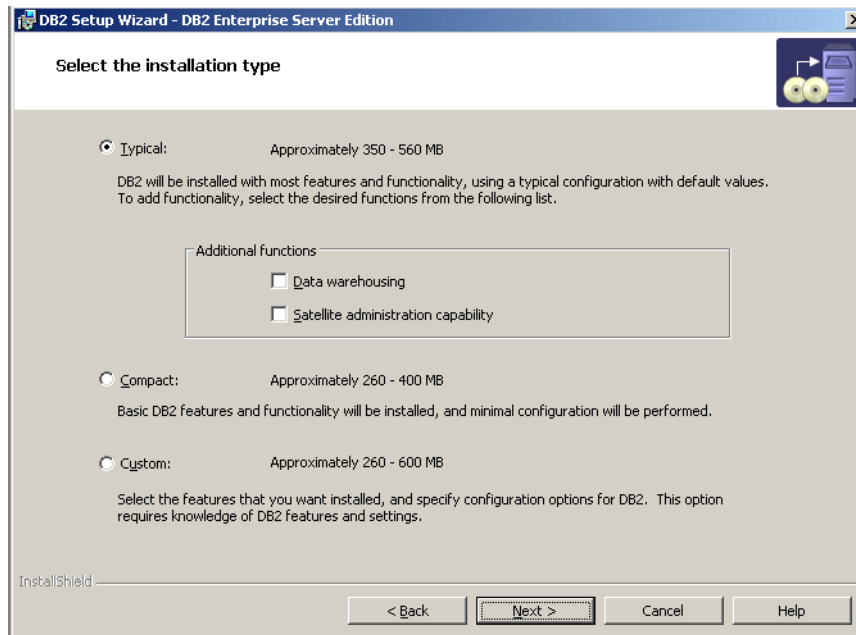


Figure 3-22 Select Typical installation

7. If you receive a warning message for APPC support, click **OK**.
8. Select **Install DB2 UDB Enterprise Server Edition on this computer**. Click **Next**.
9. Confirm the installation directory. Click **Next**.

10. Enter the user information for the DB2 Administration Server (Figure 3-23).
For example, the user name is wpsdbusr and the password is password. If you are installing DB2 in a domain environment, enter the Domain name.

DB2 Setup Wizard - DB2 Enterprise Server Edition

Set user information for the DB2 Administration Server

Enter the user name and password that the DB2 Administration Server (DAS) will use to log on to your system. You can use a local user or a domain user.

User information

Domain

User name: wpsdbusr

Password: *****

Confirm password: *****

Use the same user name and password for the remaining DB2 services

InstallShield

< Back Next > Cancel Help

Figure 3-23 Database user ID and password

11. On the Setup the administration contact list window, make sure that you enter a valid SMTP server name and valid e-mail address. Otherwise, you will receive a warning message. Click **OK** on the warning message if you do not want to specify it.
12. On the Configuring DB2 Instances window, accept the default and click **Next**.
13. On Prepare the DB2 tools catalog window, accept the default and click **Next**.
14. Specify a contact for the Health Monitor Notification (in our example, we deferred this until later).

15. Click **Install** when you reach the window shown in Figure 3-24.

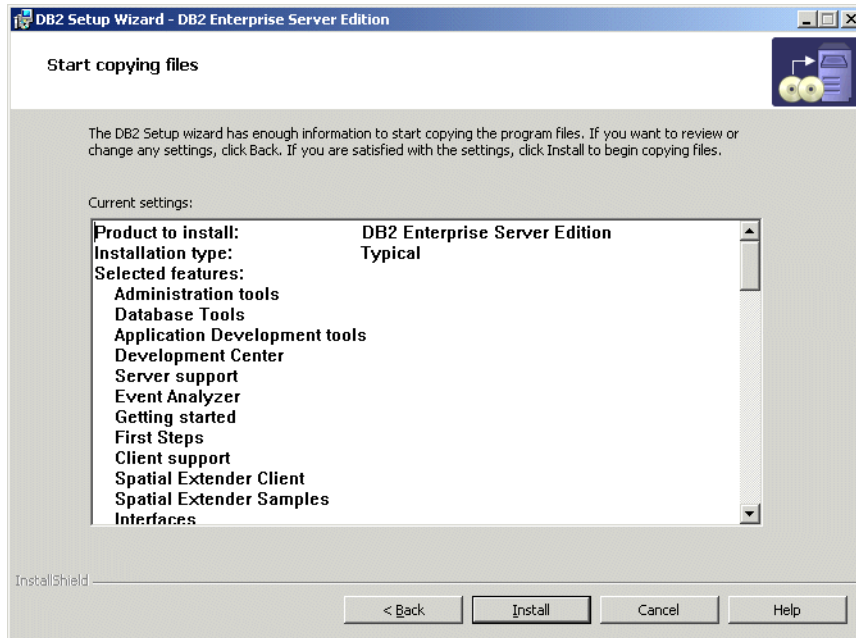


Figure 3-24 Start copying files

Note: If you selected the response file options, the Start copying files window would show the Finish button instead of the Install button.

16. Click **Finish** when the setup is complete (Figure 3-25). A congratulation window will open.

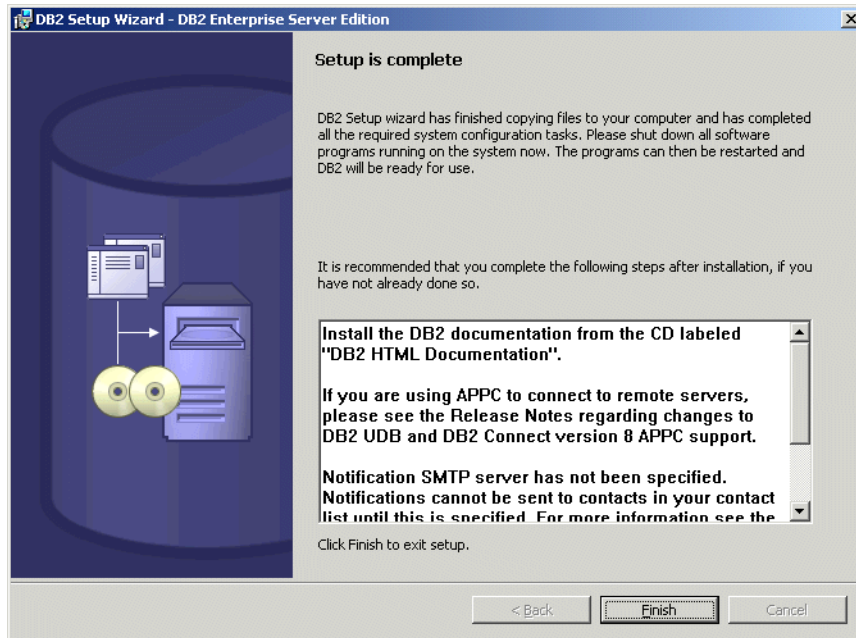


Figure 3-25 Setup is complete

17. Reboot the machine.
18. Shut down all the DB2 services.
19. Insert CD 9-10 (DB2 Enterprise Edition Fix Pack 6 for Windows V8.1) to apply the DB2 Fix Pack 6.
20. Click through the windows and accept all the defaults.

Notes:

The configuration wizard does not transfer IBM Lotus Workplace Web Content Manager data. Therefore, after doing a DB2 configuration wizard DB transfer, IBM Lotus Workplace Web Content Manager still points to the Cloudscape database.

To solve this, follow these steps to transfer the IBM Lotus Workplace Web Content Manager data:

1. Modify the wpconfig.properties file for the Web Content Management DB section according to your setup.
2. Run the following tasks:
 - WPSConfig.bat config-wcm-repository
-DPortalAdminPwd=your-portal-admin-password
 - WPSConfig.bat configure-wcm
-DPortalAdminPwd=your-portal-admin-password

You must set the value for JcrDbUnicode.

Set JcrDbUnicode value to Y if the database was created using the codeset UTF-8.

This information is documented in the *IBM WebSphere Portal for Multiplatforms Version 5.1 Information Center*.

For database transfers, all databases must use the same database user name and password.

For example, if you use db2admin for the wpsdb user name, you must also use db2admin for the fdbkdb, lmdb, and jcrdb user names.

For more information, see the *IBM WebSphere Portal for Multiplatforms Release Notes - Version 5.1.0*, available at:

http://pvcid.raleigh.ibm.com/wpf/ic/510/ent/en/beta/wp_release_notes.html#ilwcm

3.3.2 Configuring WebSphere Portal for DB2

In this section, we configure WebSphere Portal to support DB2 UDB Enterprise Server Edition. Complete the following steps:

1. Open a command prompt and change the current directory to <wp_root>/config.

2. Create a backup copy of the <wp_root>/config/wpconfig.properties file and update the fields applicable to your environment. In the lab example, we updated the properties shown in Table 3-5.

Note: We recommend the following databases; refer to Table 3-4 for the database functions:

- ▶ wps51: To be shared by WebSphere Portal and Member Manager.
- ▶ lm51: The database used by LikeMinds.
- ▶ fdbk51: Feedback database used by WebSphere Portal content publishing.
- ▶ jcr51: Stores the data for DB2 Content Manager Runtime Edition.

Table 3-4 Database functions

Database	Database function
wps51	Stores information about user customizations, such as pages, and user and login information.
fdbk51	Contains the information logged by your Web site for generating reports for analysis of site activity, including information about campaigns and personalized resources.
jcr51	Contains the information to be stored for DB2 Content Manager.
lm51	Contains information used to analyze the user activities and make recommendations for Personalization.

Table 3-5 Values used in the database configuration

Property	Value used
DbType	db2
wpsDbName	wps51
DbDriver	COM.ibm.db2.jdbc.app.DB2Driver
DbDriverDs	COM.ibm.db2.jdbc.DB2XADataSource
JdbcProvider	wps51JDBC
DbUrl	jdbc:db2:wps51
DbUser	wpsdbusr
DbPassword	test123
DbLibrary	C:/Program Files/ibm/SQLLIB/java/db2java.zip

Property	Value used
jcrDbName	jcr51
jcrDbUser	wpsdbusr
jcrDbPassword	test123
jcrDbUrl	jdbc:db2:jcr51
FeedbackDbName	fdbk51
FeedbackDbUser	wpsdbusr
FeedbackDbPassword	test123
FeedbackDbUrl	jdbc:db2:fdbk51
LikemindsDbName	lm51
LikemindsDbUser	wpsdbusr
LikemindsDbPassword	test123
LikemindsDbUrl	jdbc:db2:lm51
WmmDbName	wps51
WmmDbUser	wpsdbusr
WmmDbPassword	test123
WmmDbUrl	jdbc:db2:wps51

3. Save the file.
4. From a command prompt, type `WPSconfig.bat create-local-database-db2` from the `<wp_root>/config` directory.

You should see the message `BUILD SUCCESSFUL` after successfully running the command.
5. From a command prompt, type `WPSconfig.bat validate-database-connection-wps` from the `<wp_root>/config` directory.

You should see the message `BUILD SUCCESSFUL` after successfully running the command.
6. From a command prompt, type `WPSconfig.bat validate-database-connection-wmm` from the `<wp_root>/config` directory.

You should see the message `BUILD SUCCESSFUL` after successfully running the command.

7. From a command prompt, type `WPSconfig.bat validate-database-connection-likeminds` from the `<wp_root>/config` directory.
You should see the message `BUILD SUCCESSFUL` after successfully running the command.
8. From a command prompt, type `WPSconfig.bat validate-database-connection-feedback` from the `<wp_root>/config` directory.
You should see the message `BUILD SUCCESSFUL` after successfully running the command.
9. From a command prompt, type `WPSconfig.bat validate-database-connection-jcr` from the `<wp_root>/config` directory.
You should see the message `BUILD SUCCESSFUL` after successfully running the command.
10. Make sure that `server1` is started and that `WebSphere_Portal` is stopped:
 - a. Open a command prompt and change to the `<was_root>\bin` directory.
 - b. Issue the `serverstatus.bat -all` command.
 - c. If `server1` is stopped, issue the `startserver.bat server1` command.
 - d. If `WebSphere_Portal` is running, issue the `stopserver.bat WebSphere_Portal` command.
11. From a command prompt, change to the `<wp_root>\config\wizard` directory and then execute the `configwizard.bat` command.
12. For the language, select **English**.
13. Click **Next** on Welcome window.

14. Make sure that the **Transfer data to another database** option is selected, as shown in Figure 3-26. Click **Next**.

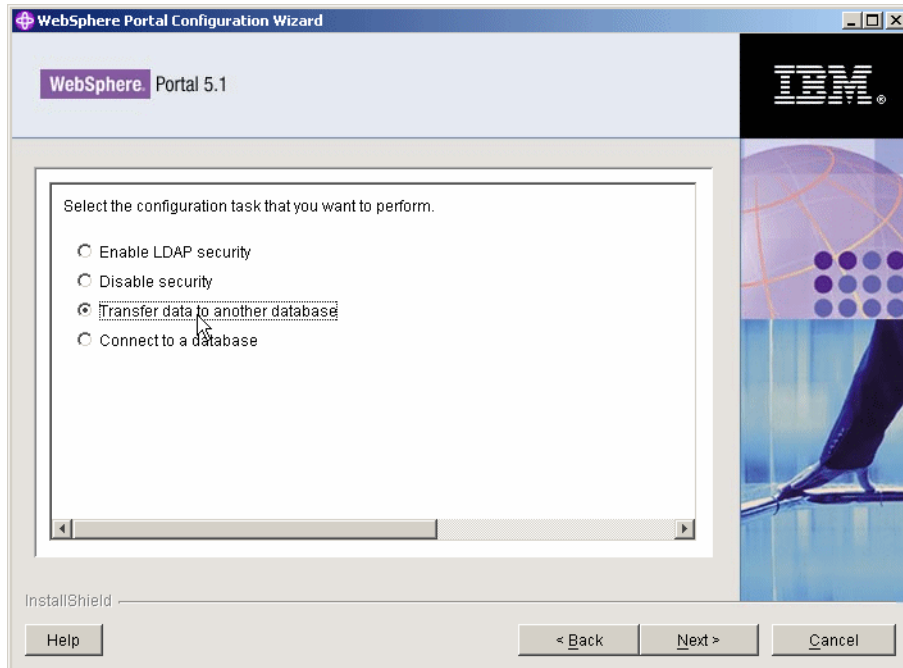


Figure 3-26 Transfer data to another database

15. Ensure that **IBM DB2 Universal Database** is selected, as shown in Figure 3-27. Click **Next**.

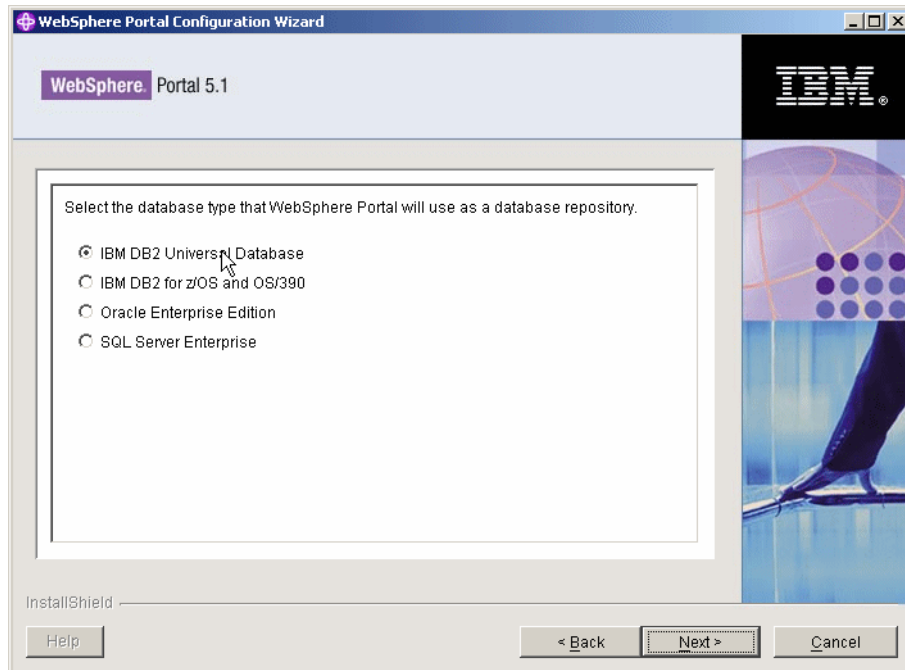


Figure 3-27 Select IBM DB2 Universal Database

16. If we had not already edited the `wpconfig.properties` file, you could choose one of the config helper files, but here we choose `wpconfig.properties`, as shown in Figure 3-28. Click **Next**.

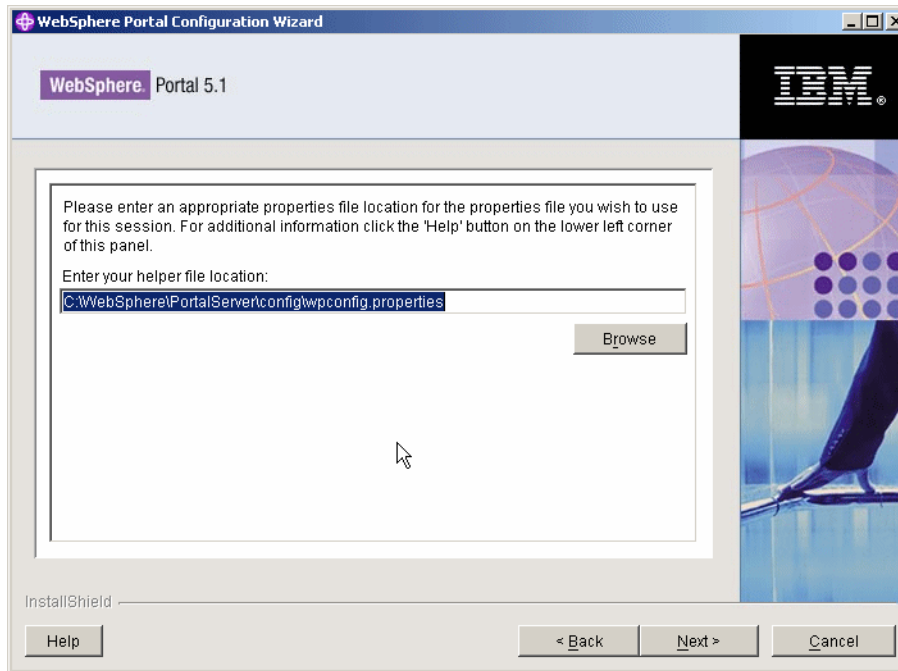


Figure 3-28 Choose the `wpconfig.properties` file

17. You will be taken through several windows, such as the one shown in Figure 3-29. Verify the entries and click **Next**.

Note: These values are pulled from the wpconfig.properties file, so verify them if you have not already updated them. It is possible that you could have chosen the helper file transfer_db2.properties from wp_root\config\helpers.

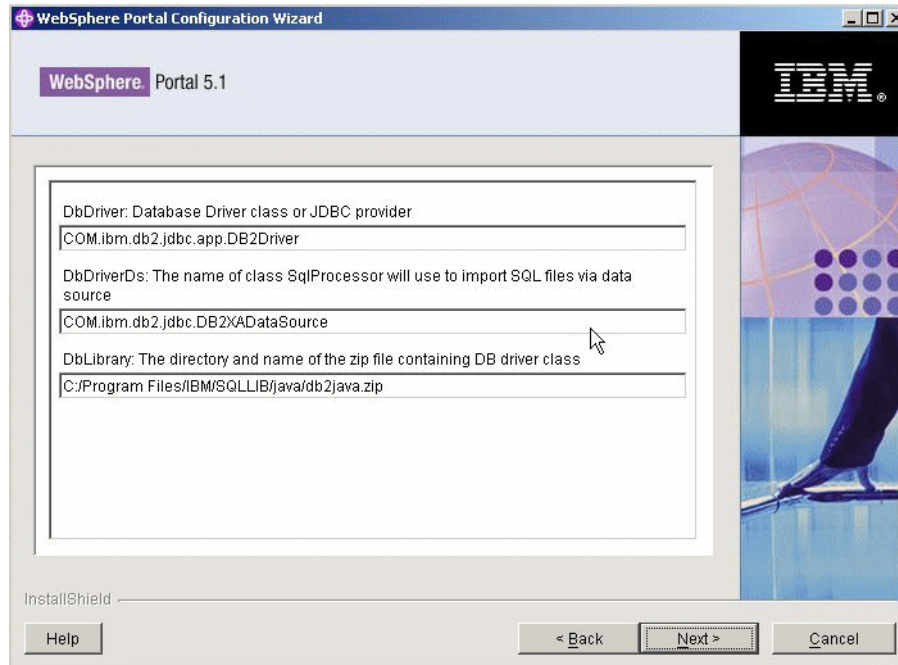


Figure 3-29 Verify the populated entries

18. After verifying all the inputs, the window shown in Figure 3-30 opens. Click **Next** to start the transfer process.

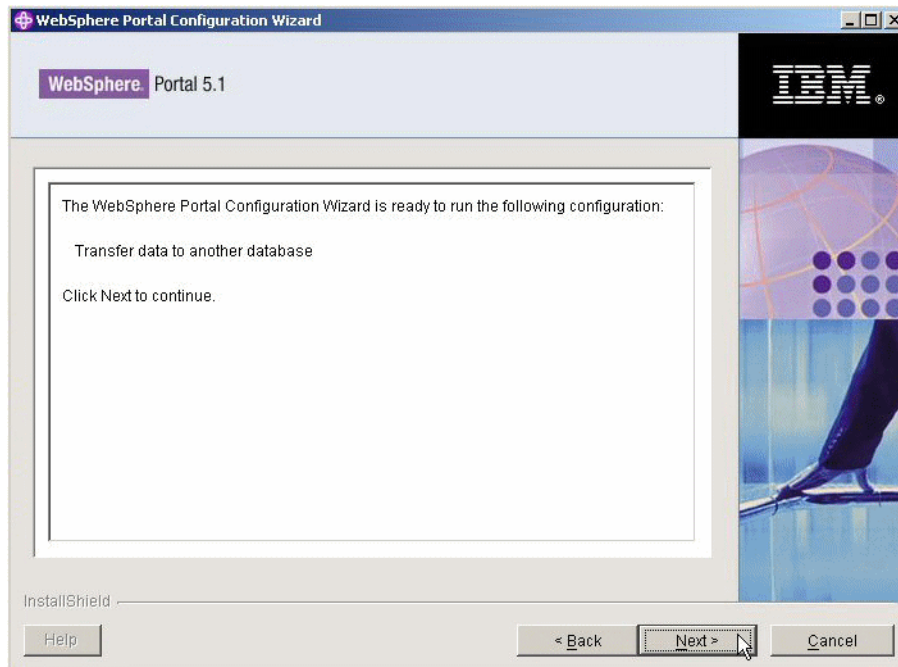


Figure 3-30 Transfer the data

19. The transfer process immediately starts and takes between 15-30 minutes to complete. The window shown in Figure 3-31 opens. Click **Finish** to end the configuration wizard.

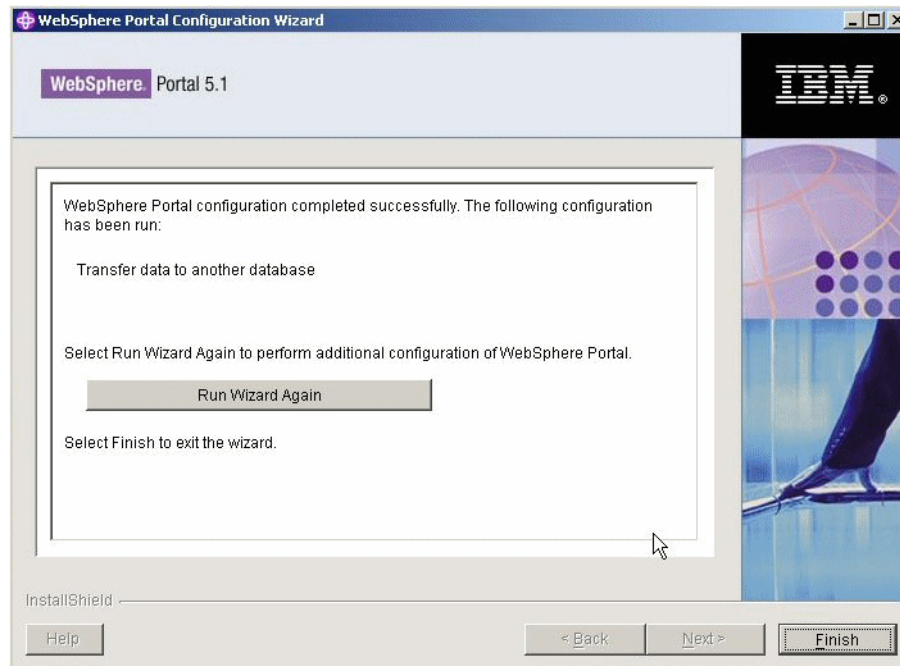


Figure 3-31 Process finished

20. We recommend that you perform a reorg check to improve performance. Open a DB2 command prompt. Connect to each database (wps51, jcr51, 1m51, and fdbk51) and run the following commands:
- ```
db2=>reorgchk update statistics on table all
db2=>terminate
```
- Go to a command prompt and type `c:\> db2rbind <database_name> -l db2rbind.out -u <db2_admin> -p <password>`. Repeat for each database.
21. Start WebSphere Portal by opening a command prompt and navigating to the `<was_root>\bin` directory. Issue the **startserver.bat WebSphere\_Portal** command.
22. Verify the portal by typing in the URL of the portal, for example, `http://<fully_qualified_hostname_name>:9081/wps/portal`.
- You have now migrated the WebSphere Portal database from Cloudscape to DB2.

**Note:** Checkpoint for WebSphere Portal

Make sure that WebSphere Portal is started and verify that you can log in to Portal.

Logs to check are configwizard.log, configwizardlog.txt, and configtrace.log (these can be found in <wp\_root>\log). Additionally, you can check the system, and if you see the lines shown in Example 3-1, you can verify that DB2 is being used correctly.

*Example 3-1 configwizard.log example*

---

```
[1/4/05 13:45:09:781 EST] 71d9b471 WSRdbDataSour I DSRA8203I: Database product
name : DB2/NT
[1/4/05 13:45:09:797 EST] 71d9b471 WSRdbDataSour I DSRA8204I: Database product
version : 08.01.0006
[1/4/05 13:45:09:797 EST] 71d9b471 WSRdbDataSour I DSRA8205I: JDBC driver name
: IBM DB2 JDBC 2.0 Type 2
[1/4/05 13:45:09:797 EST] 71d9b471 WSRdbDataSour I DSRA8206I: JDBC driver
version : 08.01.0006
```

---

**Note:** Checkpoint for database migration

Refer to 6.7.1, “Validating the database configuration” on page 321 for the steps necessary to verify the database configuration.

## 3.4 Adding an LDAP to the portal

WebSphere Portal and WebSphere Application Server require some form of user registry. There are several possible ways to provide WebSphere Application Server and WebSphere Portal with access to a user registry:

- ▶ Lightweight Directory Access Protocol (LDAP) directory
- ▶ Custom user registry
- ▶ MemberRepository (for WebSphere Portal/WebSphere Member Manager)

By default, WebSphere Portal installs a Cloudscape database and uses it as a custom user registry (CUR) for authentication.

WebSphere Portal can be configured to use an LDAP directory to store user information and to authenticate users. This section discusses the issues to consider and the procedures to follow if you plan to use an LDAP directory with WebSphere Portal.

In the lab proof of concept, a Domino server is configured as an LDAP directory for WebSphere Portal. We recommend that you use Domino as the LDAP server if no existing directory is already in place if you intend to make use of Lotus Collaborative Components. If there is already a non-Domino Directory server in place, you might want to use the Domino Directory Assistance feature to incorporate the existing directory with Domino. If you intend to use Domino as the LDAP server for WebSphere Portal, you should configure Domino Directory in Domino Administrator or the Lotus Notes client before you configure security in WebSphere Portal.

### 3.4.1 Installing Domino Enterprise Server 6.5.3

You can install and configure Lotus Domino as an LDAP directory (Domino Directory) for WebSphere Portal (including Lotus Collaborative Components), Lotus Instant Messaging and Web Conferencing and Team Workplace, and as prerequisite software for the same. The following information is specific to installing Domino 6.5.3, which is included with WebSphere Portal. Usage restrictions apply when installing Domino. You are authorized to install and use Domino solely and exclusively in connection with your use of Lotus Instant Messaging and Team Workplace. Consult the product license for details.

In this section, we perform the steps to install a basic Domino server. We install the most basic installation of Domino, and only the absolute necessary tasks are left running. Later, when we configure the servers to work with WebSphere Portal, we run the tasks that could have been enabled during the install. We did this for two reasons. First, if you already have your Domino servers installed, you can skip this step and not miss enabling any Domino tasks necessary to work with WebSphere Portal. Second, we believe that by enabling the tasks on the Domino server only when necessary, this will help explain how certain features work and let you choose what you want and do not want to run on Domino.

For more information about installing Lotus Domino and all the Domino tasks, see the *Lotus Domino Administrator Help*, available at:

<http://www.lotus.com/1dd/notesua.nsf/find/domino>

#### Installing the first server

In these steps, we install the first Domino server, which we refer to as the primary server. Complete the following steps:

1. Insert CD 12-1 (Lotus Domino Enterprise Server for Windows Release 6.5.3) and run the **Setup.exe** program in the \server directory. Follow the installation wizard using the following options:
  - We did not select Partitioned Server Install.

- We used the defaults for the installation folders: C:\Lotus\Domino and C:\Lotus\Domino\Data.

2. Select **Domino Enterprise Server** as the installation type.

Next, we need to configure the server. There are two types of Domino server configurations: one for the first Domino server and another for additional Domino servers. In our environment, bc3srv5 is the first Domino server, and bc3srv1 is configured as an additional Domino server.

For the first Domino server, bc3srv5, we performed the following steps:

1. Start the server by selecting **All Programs** → **Lotus Applications** → **Lotus Domino Server**.
2. You will be prompted to start it as a Windows Service (in our example, we choose to always start as a service and not to ask again). Click **OK**.
3. In the Welcome to Domino Server Setup window, click **Next**.
4. In the First or additional server window, select **Set up the first server** or a **stand-alone server**, and then click **Next**.
5. In the Provide a server name and title window, enter your Server name (in our case, bc3srv5) and a title if you want (Workplace Server in our case). Click **Next**.
6. In the Choose your organization name window, enter an Organization name (in our case, itso) and type a password (password in our example). Click **Next**.
7. In the Choose the Domino domain name window, enter a Domino domain name (in our case, itso) and click **Next**.
8. In the Specify an Administrator name and password window, enter a Domino Administrator name and password (itsoadmin for the last name in our example). We also chose to save a local copy of the ID file. Click **Next**.
9. Select **Web** and **LDAP** from the options under **Setup Internet services for**. We will configure these as needed. Click **Next**.
10. In the Domino network settings window, click **Customize**. In the window that opens:
  - a. Ensure that the **TCP/IP** option is selected.
  - b. Under Type the fully qualified Internet host name for this Domino server, we entered bc3srv5.itso.ra1.ibm.com.
  - c. Click **OK**.
11. Back in the Domino network setting window, click **Next**.
12. In the Secure your Domino Server window, clear the Prohibit Anonymous option and leave the other option selected. Click **Next**.

13. Click **Setup** to configure your Domino server.
14. Click **Finish** in the Successful configuration window.
15. Start the Domino server by selecting **Start** → **All Programs** → **Lotus Applications** → **Lotus Domino Server**.

### Installing Domino Administrator Release 6.5.3

Domino Administrator is required in order to administer Domino. In this instance, you will need to install it on a desktop, because Windows Server 2003 is not a supported operating system for the admin client. Complete the following steps:

1. Insert CD 12-6 (Lotus Notes, Designer and Admin Clients for Windows) and start the **Setup.exe** program in the lotusnotes\win\English directory.
2. Click **Next** in the welcome window.
3. Read and accept the license agreement.
4. Enter the name and company name.
5. Confirm the install folder.
6. On the Custom Setup window, make sure to select Domino Administrator, because it is not selected by default. Click **Next**.
7. Choose if you want it to be your default e-mail program and click **Install**.
8. Click **Finish** to complete the installation.

### Configuring Domino Administrator Release 6.5.3

The Lotus Notes client software provides a wizard to step you through the configuration. The following steps provide general information for setting up Domino Administrator:

1. Start the Domino server on the primary server if it is not already started by going to **Start** → **All Programs** → **Lotus Applications** → **Lotus Domino Server**.
2. On the client machine, start Domino Administrator by going to **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Administrator**.
3. Click **Next** in the Welcome window.
4. On the User Information window:
  - For Your Name, enter the Domino Administrator name you entered above. (itsoadmin in our example).
  - For Domino Server, enter the Domino server of your primary server. This name is a combination of the server name and the organization you created in the previous steps (bc3srv5/itso in our example).
  - Ensure that the **I want to connect to a Domino Server** option is selected. Click **Next**.



5. On the How do you want to connect to a Domino Server window, choose **Set up a connection to a local area network**.
6. On the Domino Server Network information window, the server should be filled in. Select **TCP/IP** and enter the server's fully qualified host name (bc3srv5.itso.ra1.ibm.com in our example).
7. Depending on how you have it set up, it might pull the admin ID off the server. If it does not, browse to the location of the admin ID file.
8. Enter the password you chose in for the administrator (itsoadmin in our example) and click **OK**.
9. Clear the Setup instant messaging option in the Instant Messaging Setup window. Click **Next**.
10. Under Additional Services, leave all the options cleared. Click **Finish**.

The Domino Administrator interface opens.

### Registering the second server

To register the second server so that it is in the same Domino domain, complete the following steps:

1. Click **Configuration**.
2. On the right side, expand **Tools** → **Registration** → **Server**.
3. If this is the first time you have done this, complete the following steps (otherwise, skip to the next step):
  - a. Click the **Server** button on the Choose a Certifier window.  
For the Registration Server, chose your first Domino server. Click **OK**.
  - b. Click **Certifier ID**.  
Browse to the certifier ID (located in C:\Lotus\Domino\Data on the first server install by default).
  - c. Click **OK** and enter the certifier password (password in our example).
4. Click **OK** on the Certifier Recovery Information Warning window if it opens.
5. Ensure that the registration server is your first Domino server, and the certifier is the organization you created when installing that server. Click **Continue** on the Register Servers window.
6. On the Register New Server(s) window:
  - a. Enter the additional server's host name (bc3srv1 in our example).
  - b. Enter an ID password.

**Note:** In our example, we left the Password quality scale set to Password is optional (0) so that we could clear the password and not have to enter it every time the Domino server was restarted. With this option, you cannot store the server ID in the Domino Directory and you will have to save the ID file. In our example, we called it bc3srv1.id.

- c. Select the green check box.
  - d. Select the server and click **Register** to register this new server.
  - e. Click **Done**.
7. It is good practice to configure scheduled replication between the first server and this additional Domino server at this point to keep the important databases synchronized.

**Note:** We set this up at this point as well. You might see errors until the second server is actually up and running as it tries to replicate with it. To set up this replication now, follow these steps.

1. Open Domino Administrator if not already started by going to **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Administrator**.
2. Make sure to open up the domain on the primary server (itso domain in our example).
3. Click the **Configuration** tab.
4. Expand **Replication**.
5. Click **Connections**.
6. Click **Add Connection**.
7. Then, use the following parameters for the connection:
  - Connection Type: **Local Area Network**
  - Source Server: Primary server (bc3srv5/itso in our example)
  - Destination Server: The name of the other registered server (bc3srv1/itso in our example)
  - Click **Schedule** tab and choose the appropriate schedule.
  - Click **Save & Close**.

## Installing and configuring the second server

For additional Domino servers, install as described in the previous steps and then complete the following configuration procedure:

1. Start the server by selecting **Start** → **All Programs** → **Lotus Applications** → **Lotus Domino Server**.
2. Click **Next** on the Welcome to Domino Server Setup window.
3. On the First or additional server window, select **Set up an additional server**, and then click **Next**.

4. Select **The server ID file is stored in the Domino Directory** option, and enter the password. Click **Next**.

**Note:** In our case, because we did not use a password, it was a separate ID file, but we had tried both ways and they worked the same.

5. On the Provide the registered name of this additional Domino Server window, enter this additional server name (in our case, bc3srv1/its0); this should already be populated. Click **Next**.
6. Select only the Web options under Setup Internet services for. We will configure these as needed. Click **Next**.
7. Click **Customize** on the Domino network settings window. In the window that opens:
  - a. Ensure that the **TCP/IP** option is selected.
  - b. Under Type the fully qualified internet host name for this Domino Server, make sure that it is the fully qualified Internet host name for this server (in our case, bc3srv1.itso.ra1.ibm.com).
  - c. Click **OK**.
8. When you return to the Domino network settings window, click **Next**.
9. On the Provide the system databases for this Domino Server window:
  - a. For the Other Domino Server name, type your first Domino server's name (bc3srv5/its0 in our example).
  - b. For the Optional network address, type the fully qualified Internet host name for that server (in our case, bc3srv5.itso.ra1.ibm.com).
  - c. Click **Next**.
10. Select **Set up as a primary Domino Directory (Recommended)** and click **Next**.
11. On the Secure your Domino Server window, clear the Prohibit Anonymous option. Click **Next**.
12. Click **Setup** to configure your Domino server.
13. Click **Finish** in the Successful configuration window.
14. Start the Domino server by selecting **Start** → **All Programs** → **Lotus Applications** → **Lotus Domino Server**.

### 3.4.2 Setting up Domino LDAP

The following section describes how to set up the Domino LDAP.

## Adding Portal administrators to the Domino Directory

You need to create two users in your Domino Directory to work with WebSphere Portal. Complete the following steps:

1. Open Domino Administrator. Click **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Administrator**.
2. Go to the People tab of the Domino Directory, click **People**, and click **Add Person**.
3. You will create two users. To create the wpsbind user, in the Person form, enter the values from Table 3-6 that coincide with the respective Person fields.

Table 3-6 Person form values: wpsbind user

| Field             | Value                   |
|-------------------|-------------------------|
| Last name         | wpsbind                 |
| User name         | wpsbind/itso<br>wpsbind |
| Short name/UserID | wpsbind                 |
| Domain            | itso.ral.ibm.com        |
| Internet password | wpsbind                 |

4. Click **Save & Close** to save the entries for the administrators and return to the People view of the Domino Directory.
5. Repeat using the values for the portaladmin user, as shown in Table 3-7.  
In the end, you will have the two users wpsbind and portaladmin.

Table 3-7 Person form values: portaladmin user

| Field             | Value                           |
|-------------------|---------------------------------|
| Last name         | portaladmin                     |
| User name         | portaladmin/itso<br>portaladmin |
| Short name/UserID | portaladmin                     |
| Domain            | itso.ral.ibm.com                |
| Internet password | portaladmin                     |

**Important:** If you want to have the users you create also be able to use the mail portlet, you need to create a mail database for them and specify it in the Person document in Domino Directory. Follow these steps:

1. Start Domino Administrator.
2. Click **File** → **Database** → **New**.

Create the database with the following options:

- Server: Primary server (bc3srv5/itso in our example)
- Title: *user mail file*
- File name: mail\Auto Generated.nsf

Template information:

- Server: As above.
- Select **Domino Web Access (6) inotes6.ntf**.
- Click **OK**.

3. The mail file will then open. Click **File** → **Database** → **Access Control** to open the access control list and give that specific user the following rights.
  - User Type: **Person**.
  - Access: **Editor**.
  - Select all of the attributes.
4. Close the mail file.
5. Edit the Person document and enter the mail server and mail file names:
  - Mail server: primary mail server (bc3srv5/itso in our example)
  - Mail file: mail\*mailfilenamefromabove.nsf*
6. From the Server view, click the **Files** tab.
7. Right-click the **mail** directory, and select **Manage Directory ACL**, as shown in Figure 3-32 on page 80.
8. Add the newest user whose mail file you created to the list Who should be able to access this directory?

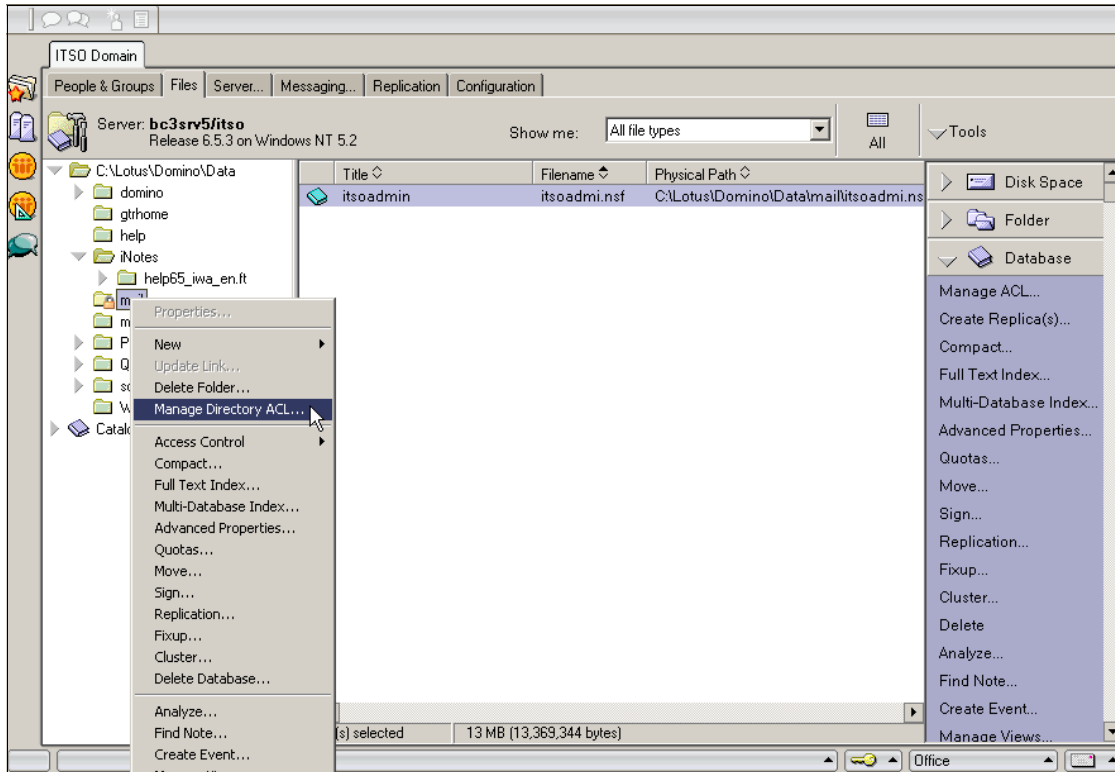


Figure 3-32 Set mail directory ACL

9. Go to the Groups view and click **Add Group**.
10. In the New Group form, create a new group called wpsadmins. Select **Multi-purpose** for the Group type.
11. Add wpsbind and the portal administrator user as members from the portal's address book. wpsbind is the user ID for LDAP bind authentication.
12. Click **Save & Close** to save the wpsadmins group.
13. Repeat this to create groups called wpscontentadministrators and wpsdocreviewers.

**Note:** Checkpoint for LDAP

To check LDAP:

1. Open a browser.
2. Enter the following to the URL:  
ldap://<fully\_qualified\_hostname>/cn=wpsbind,o=itso

For example:

ldap://bc3srv5.itso.ral.ibm.com/cn=wpsbind,o=itso

3. You should see a window similar to the one shown in Figure 3-33.

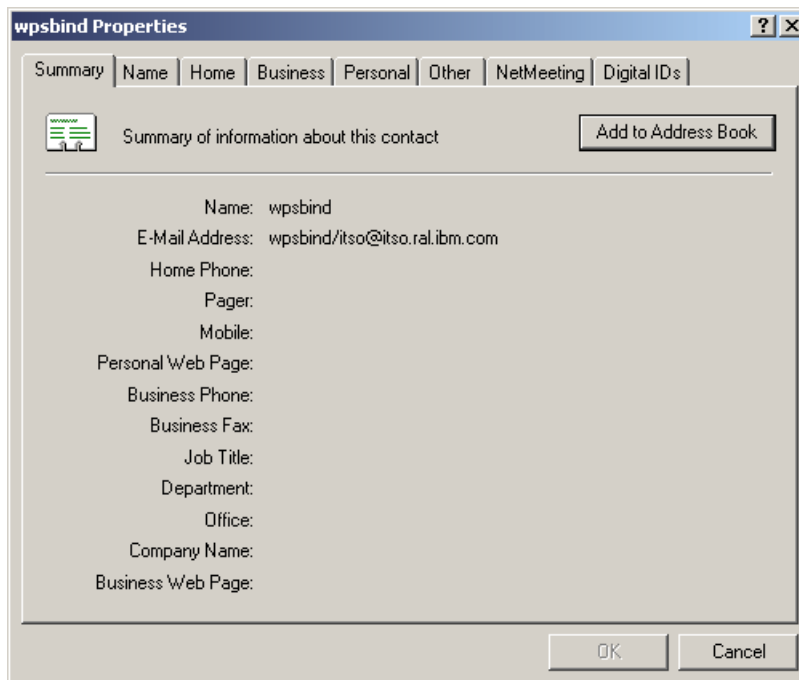


Figure 3-33 Checkpoint for LDAP

### 3.4.3 Updating the access control list of Domino Directory

These steps will be necessary so that the wmm user can add information to the Domino Directory. Complete the following steps:

1. Open Domino Administrator. Click **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Administrator**.

2. From the Domino Administrator, open the server's Domino Directory. Go to **File** → **Database** → **Access Control** to open the names.nsf database.
3. Click **Add**, and then click the people icon, and select **wpsadmins**.
4. In the Basic panel, make sure that the Portal administrator group wpsadmins has either Author access or Editor access for all roles available by selecting **wpsadmins**, changing the access to **Manager** and selecting the **Delete documents** option.
5. Assign the following Role types to the wpsadmins group:
  - GroupCreator
  - GroupModifier
  - UserCreator
  - UserModifier
6. Click **OK** to save the settings.
7. Push the settings by issuing this command from the Domino Console:

```
push bc3srv1/itso names.nsf
```

### 3.4.4 Specifying Domino LDAP configuration settings

In this section, we discuss the setting selections for the Domino LDAP configuration.

#### Adding the HTTP\_HostName attribute

Perform the following steps to add the HTTP\_HostName attribute.

**Note:** You might not have to do this step depending on the configuration you chose for your Domino server. Every time we checked, it was already populated.

1. Make sure that you have Manager access to the Schema database (schema.nsf) on the primary server (bc3srv5/itso in our example).
2. Open the Schema database on any server in the domain that runs the LDAP service.
3. Select the **All Schema Documents** view, and then click **New Document** → **Add Attribute Type**.
4. Complete the fields specified in Table 3-8 on page 83 on the Basics tab.



Table 3-8 Values for the HTTP\_HostName attribute

| Field                | Action                                                                                                                                                                              |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LDAP name            | Enter HTTP-HostName for the attribute.                                                                                                                                              |
| OID                  | Enter the object identifier: 2.16.840.1.113678.2.2.2.2.461                                                                                                                          |
| Syntax name          | Select <b>Directory String</b> .                                                                                                                                                    |
| Description          | (Optional) Enter a description for the attribute.                                                                                                                                   |
| Equality match       | (Optional) Select a matching rule to apply when the equality operator is used to search for this attribute.                                                                         |
| Ordering match       | (Optional) Select a matching rule to apply when an ordering operator is used to search for this attribute.                                                                          |
| Substrings match     | (Optional) Select a matching rule to apply when a substring operator is used to search for this attribute.                                                                          |
| Single valued        | Choose one: <ul style="list-style-type: none"> <li>▶ Yes to allow more than one value for the attribute (default)</li> <li>▶ No to allow only one value</li> </ul>                  |
| Collective           | Choose one: <ul style="list-style-type: none"> <li>▶ Yes to allow the values for this attribute to be shared</li> <li>▶ No to prevent values from being shared (default)</li> </ul> |
| No user modification | Choose one: <ul style="list-style-type: none"> <li>▶ Yes to prevent users from modifying the values</li> <li>▶ No to allow users to modify values (default)</li> </ul>              |

5. Click **Save & Close**. A draft document for the HTTP-HostName attribute appears in the Draft Documents - Draft Attribute Types view.
6. Select the **HTTP-HostName** draft documents, and click **Approve** → **Approve Selected Drafts**.

### 3.4.5 Completing the configuration

These steps will enable the Domino Directory to be searched correctly by WebSphere Member Manager:

1. Use the Domino Administrator interface to open the Domino Directory, names.nsf, on the primary server (bc3srv5/itso in our example).
2. Navigate to the view **Configuration - Servers**.

3. Highlight **Configurations** and then open the Configuration Settings document. If a global configuration document does not exist, click **Add Configuration** to create a new configuration document and display the Configuration Settings.
4. On the Basics tab, for the **Use these settings as the default settings for all servers** option, click **Yes**.

**Note:** You must select **Yes** to cause the LDAP tab to appear for use in the next step.

5. On the LDAP tab, click the button next to **Select Attribute Types** to open the LDAP Attribute Type Selection dialog box.
6. From the Object Classes drop-down list, select \*, and then click **Display Attributes**.
7. From the Selectable Attribute Types box, select the following fields, and then click **Add** to add them to the Queriable Attribute Types box:
  - AltFullName
  - dominoCertificate
  - FullName
  - givenName
  - HTTP\_HostName
  - Location
  - mail
  - MailAddress
  - MailDomain
  - MailFile
  - MailServer
  - member
  - NetAddresses
  - PublicKey
  - Sametime
  - sn
  - uid
  - userCertificate
8. Click **OK** to close the LDAP Attribute Type Selection dialog box and return to the Configuration Settings document.
9. Ensure that the Anonymous users can query field displays the following attributes:
  - AltFullName
  - dominoCertificate
  - givenName

- FullName
- HTTP\_HostName
- InternetAddress
- Location
- mail
- MailAddress
- MailDomain
- MailFile
- MailServer
- member
- NetAddresses
- PublicKey
- Sametime
- sn
- uid
- userCertificate

10. For the **Allow LDAP users write access** option, click **Yes**. This setting ensures that portal users can use the self-care and self-registration features of WebSphere Portal.

11. Keep all the other default LDAP settings in the Configuration Settings document.

12. Click **Save & Close** to close the Configuration Settings document.

### **Additional Domino configuration**

To enable the database drop-down list, you need to complete two tasks: enable the DIOP task and allow users the ability to run Java agents.

To enable the DIOP task to load automatically every time the Domino server starts, perform the following steps:

1. Open the notes.ini in the Domino program directory.
2. Locate the line ServerTasks= and add di iop to the end of the line if it is not already there.
3. Save and close the file.

For more information about the DIOP task, refer to the *Lotus Domino Administrator Help*.

Next, perform the following steps to allow users the ability to run Java agents:

1. Start the Domino Console.
2. Open the names.nsf database on the primary server (bc3srv5/itso in our case).

3. Navigate to **Configuration** → **Servers** → **All Server Documents**.
4. Double-click the Server document that you want to configure (bc3srv5/itso in our example).
5. Make the following configuration changes to the Server document:
  - a. On the Basics tab, make sure that the Fully Qualified Internet Host Name field contains the fully qualified name that you enter in the browser to access this server.
  - b. Switch to the Ports tab. On the Notes Network Ports subtab, make sure that the top line has the Port set to **TCPIP** and the Net Address set to the fully qualified name of the server. Make sure this port is set to **Enabled**.
  - c. Switch to the Internet Protocols tab. On the HTTP subtab, select **Yes** for the option **Allow HTTP Clients To Browse Databases**.
  - d. Switch to the Security tab. For troubleshooting and development purposes, set the following three fields to \* under the Programmability Restrictions section:
    - Run restricted LotusScript/Java agents
    - Run restricted Java/JavaScript/COM
    - Run unrestricted Java/JavaScript/COM

**Note:** You might want to restrict these fields to a subset of users. If you do this, note the following information:

- ▶ The Domino server to which you are connecting must be included with the full canonical name (for example, bc3srv5/itso). Next, add any users or groups that you want to receive a list of databases when placing a portlet in edit mode. You can also use an asterisk (\*) as a wild card.
- ▶ If you want to add the user wpsadmin, add the following information to the field: uid=wpsadmin/cn=users/o=ibm/c=us. To add all of the members in the /o=ibm/c=us organization, add the following value to the field: \*/o=ibm/c=us.

6. Click **Save & Close**.
7. Open the other server's Server document and repeat these steps.
8. Push the changes to the other server with the following command issued from the Domino Console:

```
push bc3srv1/itso names.nsf
```

## 3.5 Creating the Web SSO configuration

The Web single sign-on (SSO) configuration document is a domain-wide configuration document stored in the Domino Directory. You must create the Web SSO configuration document prior to enabling multiserver single sign-on. Complete the following steps:

1. Start Domino Administrator by clicking **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Administrator**.
2. Open the names.nsf database on the primary server.
3. Select **Configuration** → **Server** → **All Server Documents**.
4. Select the server (primary server bc3srv5/itso in our example) and click **Web** → **Create Web SSO Configuration** (Figure 3-34).

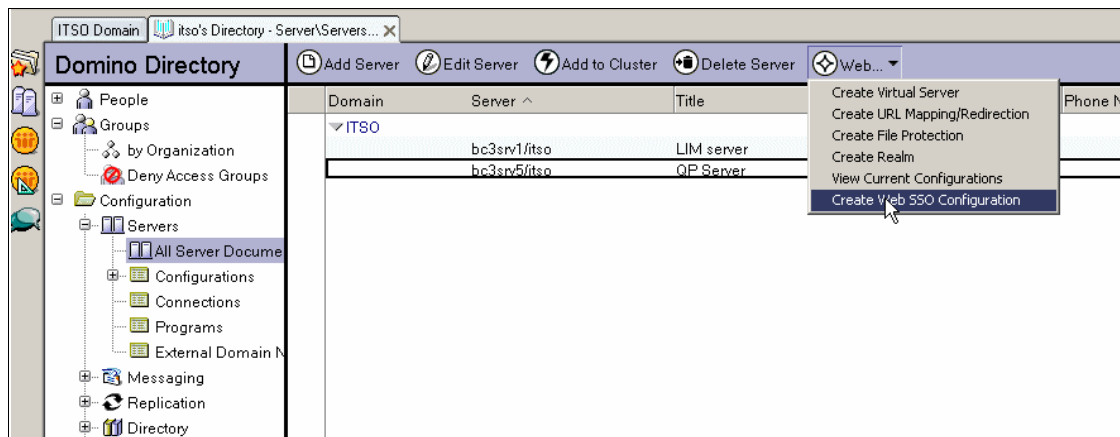


Figure 3-34 Create Web SSO Configuration

5. Enter the domain suffix for the DNS Domain and select both servers in Domino Server Names field (Figure 3-35).

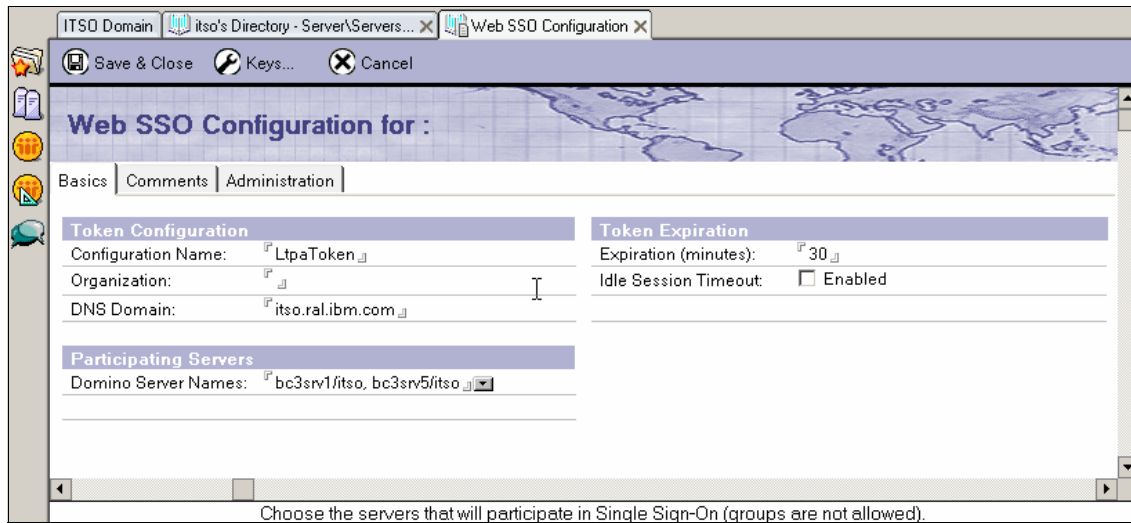


Figure 3-35 Modify settings for SSO

6. From the Keys menu, select **Create Domino SSO Key** (Figure 3-36).

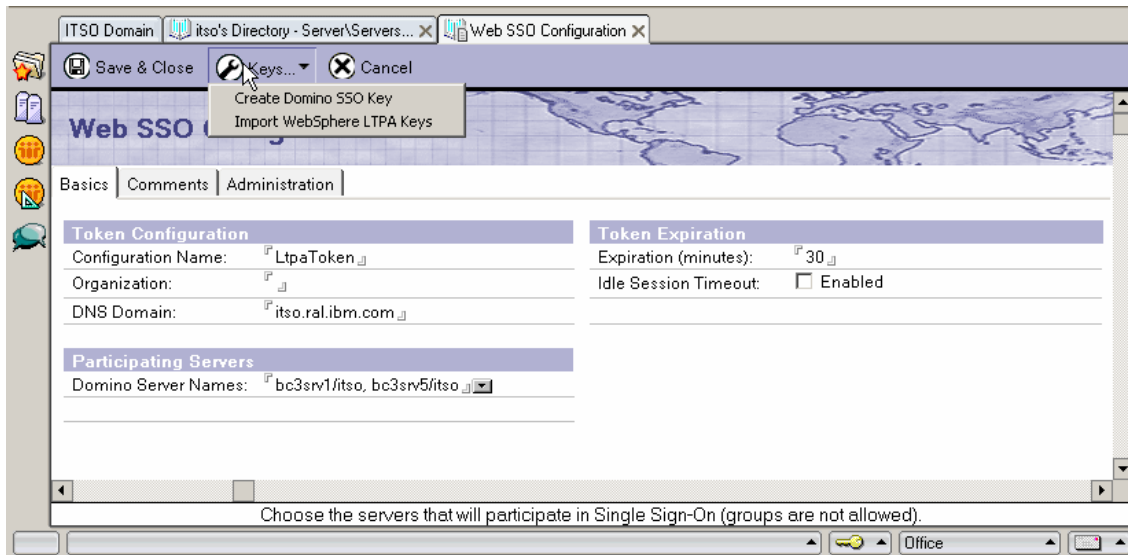


Figure 3-36 Create Domino SSO Key

7. Click **OK**.
8. Click **Save & Close**.
9. Close the Domino Administrator interface.
10. From the Domino Console, issue the command to push names.nsf to the secondary server, in our example, push bc3srv1/itso names.nsf.
11. Restart both Domino servers. To restart the servers, issue the following command from the Domino Console:  

```
restart server
```

**Note:** Checkpoint for Domino

You should be able to open the Domino home page using a browser by typing in `http://<fully_qualified_domino_server>`. Port 80 is the default port number for the Domino Web server. For example, in our lab configuration, the URL of the Domino home page is `http://bc3srv5.itso.ral.ibm.com` and `http://bc3srv1.itso.ral.ibm.com`.

## 3.6 Installing Lotus Team Workplace 6.5.1

In this section, we take you through the steps to install a Lotus Team Workplace (formerly called QuickPlace) server. The Lotus Team Workplace server installs on top of a Domino server, so prior to installing Lotus Team Workplace, make sure that you complete the steps in 3.4.1, “Installing Domino Enterprise Server 6.5.3” on page 72 for the Team Workplace server. In our example, we will be installing this onto bc3srv5.

To install Lotus Team Workplace V6.5.1, complete the following steps:

1. Stop the Domino server on which Lotus Team Workplace will be installed by issuing the **quit** command from the Domino Console.
2. Run **Setup.exe** from the directory of the preferred language on the Lotus Team Workplace CD (CD14-1 from the WebSphere Portal bundle).
3. Accept the license agreement. Click **Next**.
4. Verify that the installation directories match the Domino server directories and click **Next**.
5. Click **Next** to start the installation.
6. When finished copying files, click **Next**.
7. When prompted, enter the name and password for a Team Workplace administrator, as shown in Figure 3-37 on page 91. The user name and password are local to the Team Workplace server and should not be the same user as anyone listed in the Domino Directory on which Team Workplace is installed or the LDAP directory with which Team Workplace will work. (We used twadmin in our example.)





Figure 3-37 Administrator ID for Team Workplace server

8. When prompted, click **Finish** to complete the installation.
9. Open the notes.ini file from the Team Workplace server in a text editor. The notes.ini file is located in the Domino program directory.
10. The Team Workplace server loads when the HTTP task loads in Domino. After installing Team Workplace, ensure that the HTTP task is set to automatically load in Domino. Find the ServerTasks= line and add ,http to the end if it does not already exist.
11. Restart the Team Workplace server by selecting **Start** → **All Programs** → **Lotus Applications** → **Lotus Domino Server**.

When the HTTP task loads, you should see the text shown in Example 3-2 in the Domino Console.

*Example 3-2 Console of Team Workplace starting successfully*

---

```
01/17/2005 11:19:48 AM HTTP Server: DSAPI Domino Off-Line Services HTTP
extension Loaded successfully
01/17/2005 11:19:49 AM HTTP Server: DSAPI QuickPlace DSAPI Filter Loaded
successfully
01/17/2005 11:19:49 AM LDAP Server: Started
01/17/2005 11:19:50 AM Attempt by CN=bc3srv5/0=itso to create duplicate
template Place Catalog in database C:\Lotus\Domino\Data\PlaceCatalog.nsf -
rejected.
01/17/2005 11:20:00 AM QuickPlace Server started. 350172.00
01/17/2005 11:20:01 AM HTTP Server: Started
```

---

### 3.7 Specifying Lotus Team Workplace 6.5.1 server settings

To set up the Lotus Team Workplace server for use with WebSphere Portal, follow these general steps:

1. Start the Domino server if not already started by clicking **Start** → **All Programs** → **Lotus Applications** → **Lotus Domino Server**.
2. Open a browser and enter `http://<domino_server>/QuickPlace` where `<domino_server>` is the fully qualified host name. For example, in our case, this would be `http://bc3srv5.itso.ra1.ibm.com/Quickplace/`.
3. Click **Sign in**.
4. Enter the administrator ID and password that you specified during the installation. For example, in our lab configuration, we used `twadmin`.
5. Select **Server Settings**.
6. Select **User Directory**.
7. Click the **Change Directory** button.

8. Select **LDAP Server** as the server type.
9. Enter the fully qualified host name of the Domino LDAP Server (Figure 3-38) in the Name field (bc3srv5.its.o.ra.l.ibm.com in our example).
10. Select **Disallow new users** in the bottom part of the window.

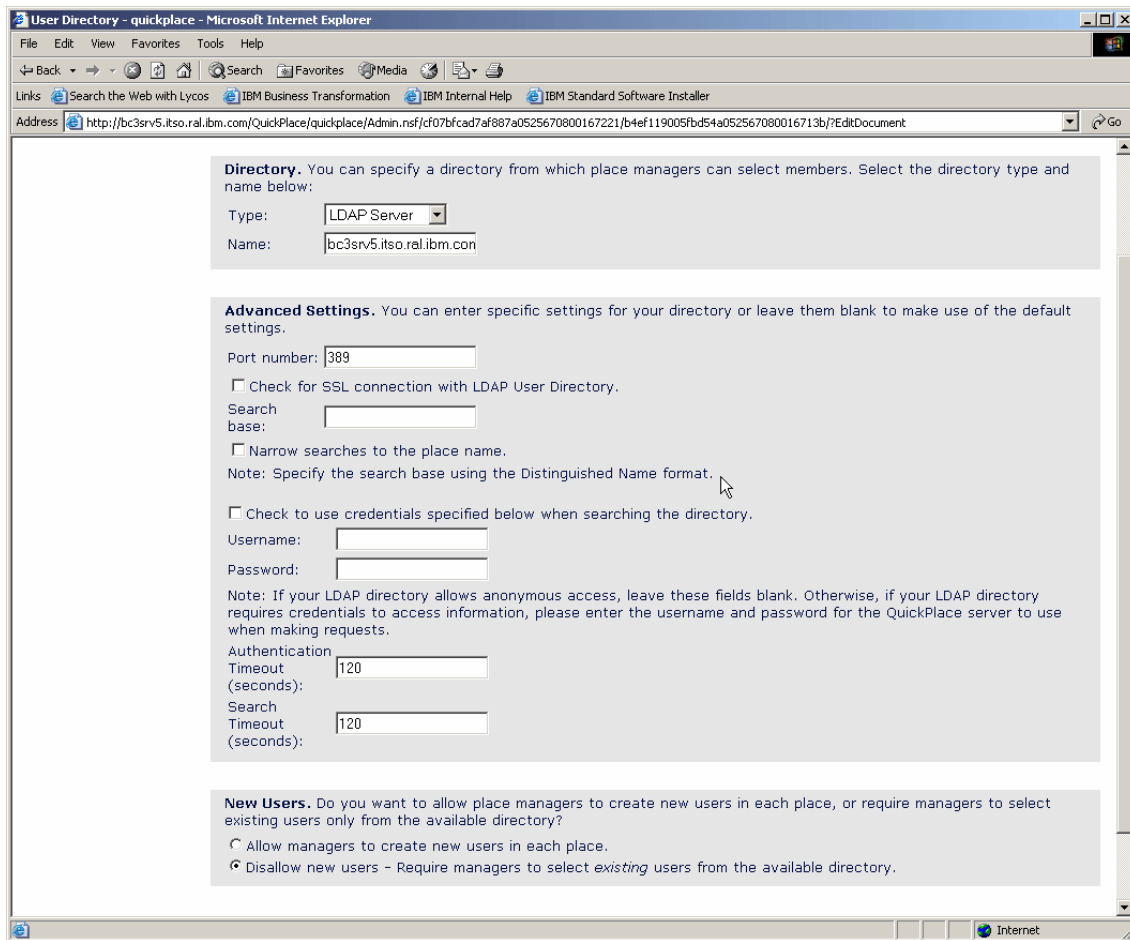


Figure 3-38 Change the user directory

11. Confirm your choices by clicking **Next** (Figure 3-39).

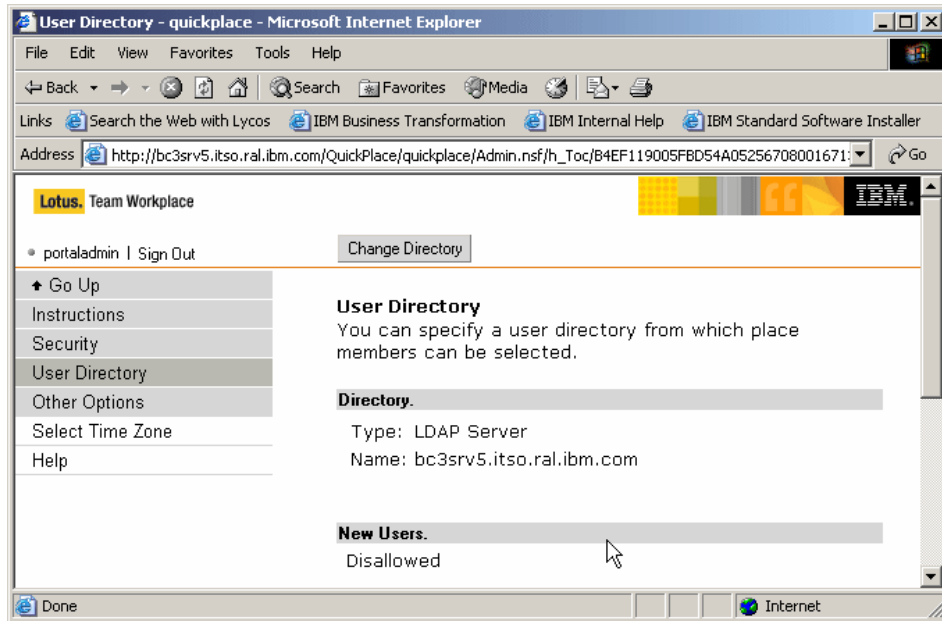


Figure 3-39 Confirm configuration of user directory

12. Select **Security**.

13. Under **Who can administer this server?**, click the **Add** button (Figure 3-40).

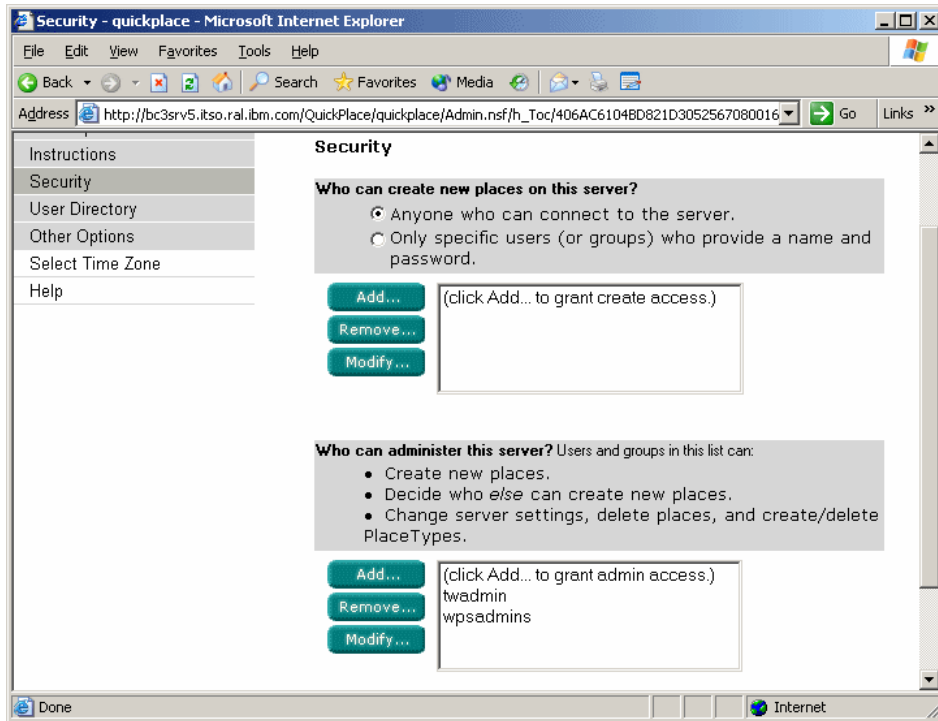


Figure 3-40 Who can administer this server?

14. Click **Directory**.

15. Select **Group** and enter an asterisk (\*) to search.

16. Check the group for the Portal administrators (wpsadmins) and then click **Add**.

17. Click **Close**.

18. Click **Next**.

19. Sign out.

20. Restart the Domino server by issuing the following command from the Domino Console:

```
restart server
```

21. Start the Domino Administrator on the client machine if it is not running.

22. Select the itso domain and choose the primary server (in our example, bc3srv5).

23. Select the **Configuration** tab.

24. Expand **Server**.
25. Select **Current Server Document**.
26. Click **Edit Server**.
27. Go to **Internet Protocols** → **Domino Web Engine**. Change the Session authentication to **Multiple Servers (SSO)** (Figure 3-41). Domino is a prerequisite for the Team Workplace and Instant Messaging and Web Conferencing servers, and if you plan to use those servers, multiserver single sign-on must be enabled. Enabling single sign-on allows Web users who log on once to a server to automatically access any other server in the DNS domain that is enabled for single sign-on.
28. Select **LTPA** as the Web SSO Configuration.

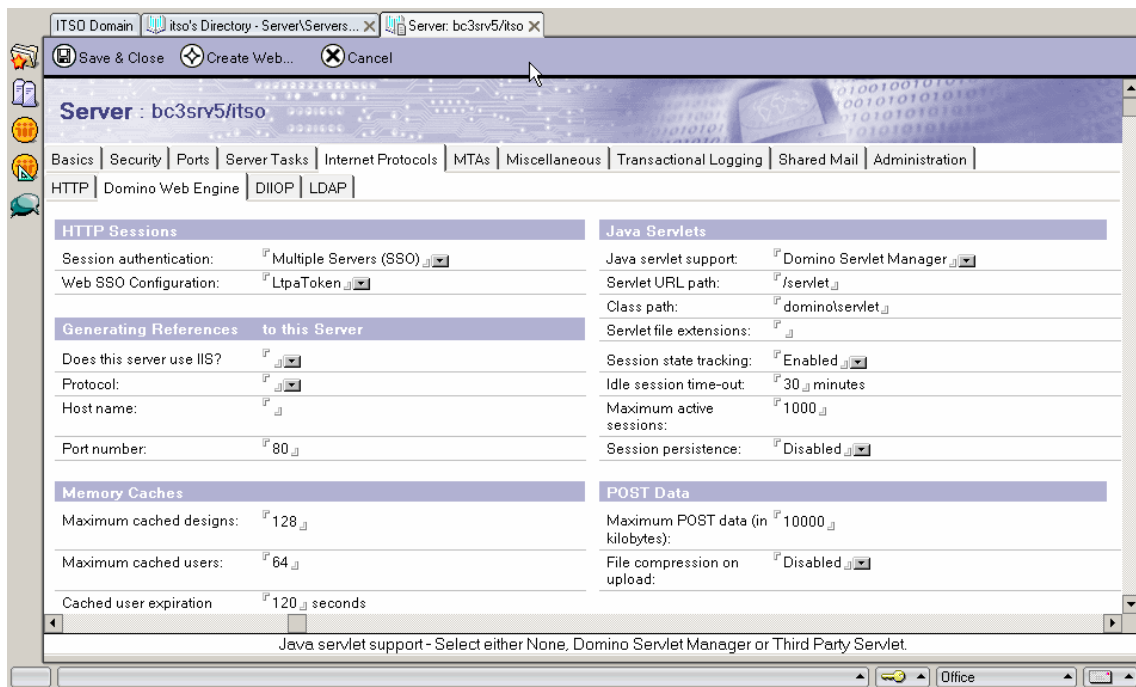


Figure 3-41 Change Session Authentication

29. Change the Java servlet support to **Domino Servlet Manager**.
30. Click **Save & Close**.
31. Open the second Server document and repeat steps 24 through 30 on the second server.
32. Close Domino Administrator.

33. Push names.nsf to the secondary server by issuing the following command from a Domino Console on the primary server, in our example, issued from bc3srv5:

```
push bc3srv1/itso names.nsf
```

34. Restart both of the Domino servers.

You should see messages as shown in Example 3-3.

*Example 3-3 Web SSO configuration messages*

---

```
01/17/2005 11:33:03 AM HTTP Server: Java Virtual Machine loaded
01/17/2005 11:33:03 AM HTTP Server: DSAPI Domino Off-Line Services HTTP
extension Loaded successfully
01/17/2005 11:33:03 AM HTTP Server: DSAPI QuickPlace DSAPI Filter Loaded
successfully
01/17/2005 11:33:03 AM Servlet engine initialization was successful
01/17/2005 11:33:03 AM DIIOP Server: Started
01/17/2005 11:33:03 AM HTTP JVM: File or directory
C:\Lotus\Domino\Data\domino\servlet does not exist
01/17/2005 11:33:03 AM QuickPlace: Successfully loaded Web SSO Configuration.
01/17/2005 11:33:04 AM LDAP Server: Started
01/17/2005 11:33:05 AM QuickPlace Server started. 350172.00
01/17/2005 11:33:05 AM HTTP Server: No Web SSO Configuration specified, using
default ('LtpaToken').
01/17/2005 11:33:06 AM HTTP Server: Started
```

---

**Important:** In our example, we did not choose the Web SSO Configuration so that you would see what configuration is being loaded as shown Example 3-3.

**Note:** Checkpoint for SSO

At this point, single sign-on should be working. To verify this, complete the following steps:

1. In a browser, go to the primary server by typing in the following URL:

```
http://<domino_server>/quickplace
```

In our example: <http://bc3srv5.itso.ra1.ibm.com/quickplace>

2. Log in as portaladmin/portaladmin.

3. After logging in, type the following URL in your browser:

```
http://<domino_server>/names.nsf
```

In our example: <http://bc3srv1.itso.ra1.ibm.com/names.nsf>

You should not be prompted for a password, and if you are not prompted, SSO is working.

### 3.7.1 Adding QPServlet and configuring for Team Workplace

To enable Lotus Team Workplace to work in your Collaborative portal, you need to add the QPServlet (stored in the Java archive file cs.jar) to your Lotus Team Workplace server. The QPServlet ensures that the records of portal users who are registered in portal are synchronized with Team Workplace membership records. Complete the following steps:

1. If it does not already exist, create a directory named Servlet in the C:\Lotus\Domino\Data\domino directory in our example.
2. Find the Domino Data servlets.properties file, typically in the default location C:\Lotus\Domino\Data\servlets.properties. If this file does not exist, create it with a text editor.

Open the servlets.properties file in a text editor and add this line (Figure 3-42):

```
servlet.QPServlet.code=com.lotus.cs.util.QPServlet
```

**Note:** The preceding line is case-sensitive, and you must add a hard return at the end of the line.

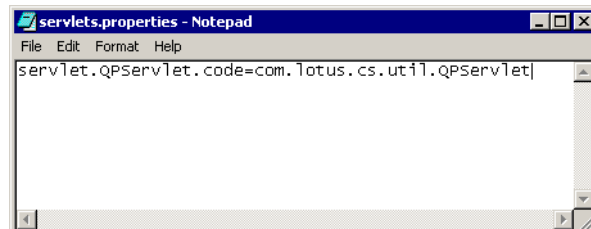


Figure 3-42 The servlet.properties file

3. Save and close the file.
4. Copy the Collaborative Services Java archive file (cs.jar) from <wp\_root>\shared\app into the C:\Lotus\Domino\Data\domino\java directory.

**Note:** Do not create subdirectories, such as WEB-INF, in the Lotus\Domino\Data\domino\java directory in which to store the cs.jar file.

5. Edit the notes.ini file to add cs.jar to notes.ini. For the Lotus Team Workplace server, making the following changes:
  - a. Locate the JavaUserClassesExt line.
  - b. Append WPS1 to the JavaUserClassesExt line (use a comma as a delimiter).



- c. Add the following line below the `JavaUserClassExt` line:  
`WPS1=c:\Lotus\Domino\data\domino\java\cs.jar`
6. Follow these steps to ensure that Domino Servlet Manager is set for Java servlet support:
  - a. Start Domino Administrator and type the password for the administrator.
  - b. Open the `names.nsf` database of the Lotus Team Workplace server.
  - c. Edit the Lotus Team Workplace Server document (`bc3srv5/itso` in our example).
  - d. Go to **Internet Protocols** tab and click **Domino Web Engine**.
  - e. Set Java Servlet Support to **Domino Servlet Manager**.
  - f. Click **Save & Close**.

### 3.7.2 Configuring Domino Web server

These steps will create the mapping for the correct login form to be used on the Lotus Team Workplace server. Complete the following steps:

1. Create the Domino Web Server Configuration database, `domcfg.nsf`:
  - a. From Domino Administrator, select **File** → **Database** → **New**.
  - b. We use the following properties:
    - Server: `bc3srv5/Itso` (Team Workplace server)
    - Title: `Web Server Configuration`
    - File name: `domcfg.nsf`
    - Template: **Domino Web Server Configuration (6) (domcfg5.ntf)**; this template is shown with the Advanced templates.
  - c. Click **OK**.
  - d. Open the newly created Web Server Configuration database if it does not open by itself.
  - e. Click **Add Mapping**.
  - f. In the Mapping document, fill in the following:
    - Applies to: **All Web Sites/Entire Server**  
(You can also restrict SSO to specific virtual servers.)
    - Target Database: `quickplace/resources.nsf`
    - TargetForm: `QuickPlaceLoginForm`
  - g. Click **Save & Close**.
  - h. Close the database.
2. Update the `notes.ini` file:
  - a. Open the `notes.ini` file in the `\Lotus\Domino` Directory of your Team Workplace server in a text editor.
  - b. Add the directive `NoWebFileSystemACLs=1` to the file. Do not place this as the last line of the file.

3. Push the changes to the other server by issuing the following command from the Domino Console on the primary server:

```
push bc3srv1/itso names.nsf
```

4. Restart the Domino server for the changes to take effect.

### 3.7.3 Enabling Lotus Team Workplace search

Enabling search will enable users to search through the index for places at much faster speeds. To enable search, configure the Search Places settings in the qpconfig.xml file by completing the following steps:

1. Copy the qpconfig\_sample.xml file to the qpconfig.xml file if it does not already exist (this existed in C:\Lotus\Domino\Data in our example).
2. Open the qpconfig.xml file using a text editor.
3. Scroll down to the Search Places section and remove the following lines from the beginning and end of Search Places section, respectively:

```
<!-- ===== START OF SAMPLE =====
===== END OF SAMPLE ===== -->
```

4. Modify the Search Places tags for your environment. Example 3-4 shows our configuration.

*Example 3-4 Search Places section of the qpconfig.xml file*

---

```
<search_places enabled="true" log_level="0" anonymous="true">
<domain_catalog_server ssl="false">
<port>80</port>
<domino_server_name>bc3srv5/itso</domino_server_name>
<path_prefix></path_prefix>
<hostname>bc3srv5.itso.ra1.ibm.com</hostname>
</domain_catalog_server>
</search_places>
```

---

5. Restart the Domino server for these settings to take effect.

#### **Note:** Checkpoint for Lotus Team Workplace

To check Team Workplace, complete the following steps:

1. Open a browser and enter `http://<server_name>/quickplace`.
2. Log in to Team Workplace with `portaladmin`.
3. Create a place.
4. Log in to the place you created.
5. You should see the place you created, as shown in Figure 3-43 on page 101.

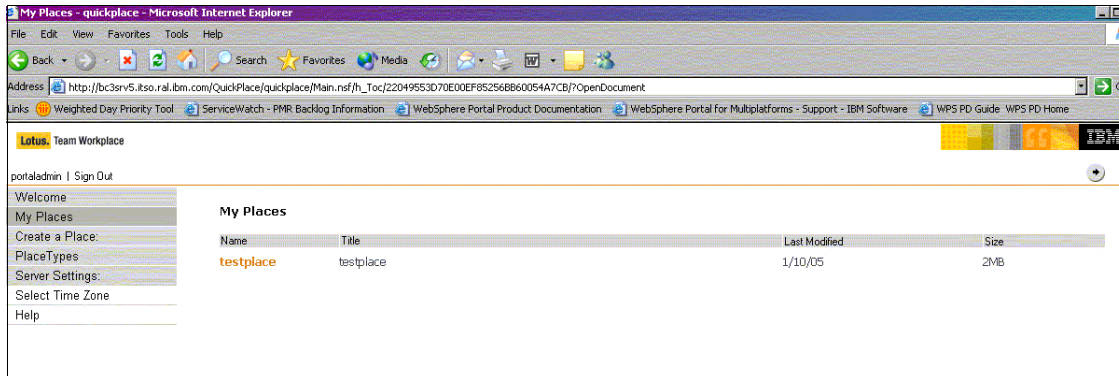


Figure 3-43 Checkpoint for Lotus Team Workplace

**Note:** Checkpoint for QPServlet

To check QPServlet, complete the following steps:

1. Open a browser and enter the following URL:  
[http://<fully\\_qualified\\_domino\\_server\\_host\\_name>/servlet/QPServlet?actionType=69](http://<fully_qualified_domino_server_host_name>/servlet/QPServlet?actionType=69)  
 In our example:  
<http://bc3srv5.itso.ra1.ibm.com/servlet/QPServlet?actionType=69>
2. You should see the return message, as shown in Figure 3-44 on page 102.
3. Enter the following in the URL:  
[http://<fully\\_qualified\\_domino\\_server\\_host\\_name>/servlet/QPServlet?actionType=68](http://<fully_qualified_domino_server_host_name>/servlet/QPServlet?actionType=68)  
 In our example:  
<http://bc3srv5.itso.ra1.ibm.com/servlet/QPServlet?actionType=68>
4. You should see the return message, as shown in Figure 3-45 on page 102.

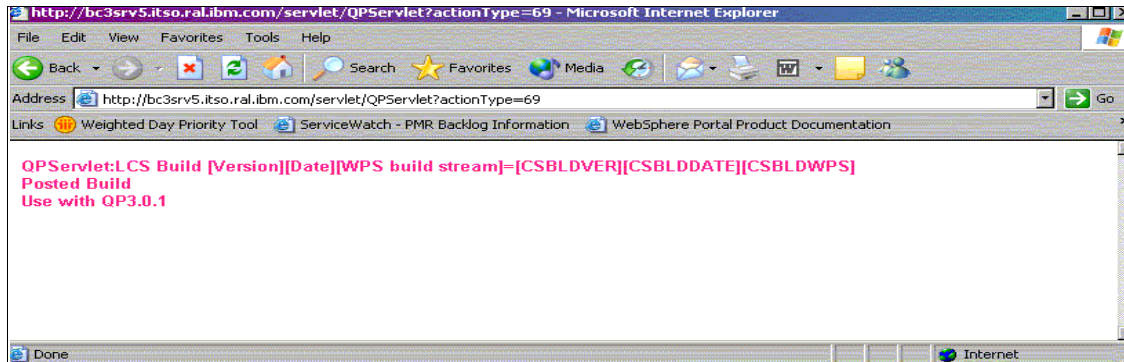


Figure 3-44 Checkpoint for QPServlet

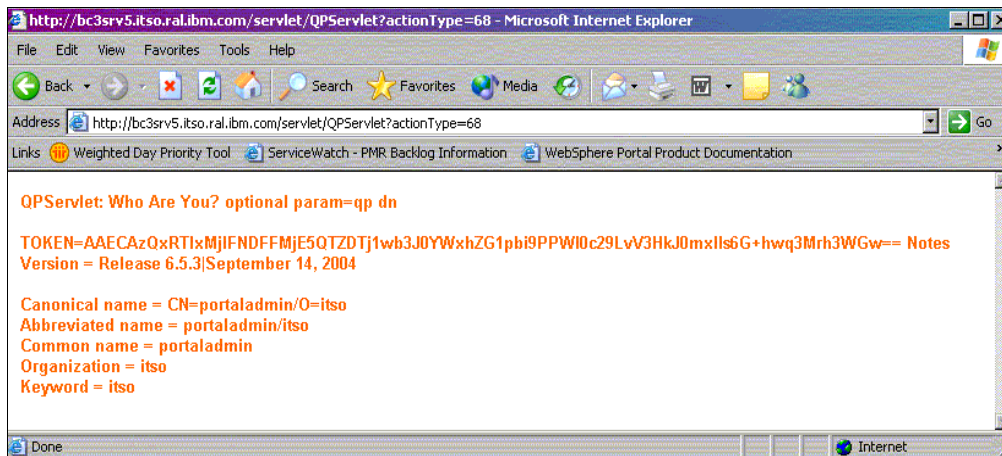


Figure 3-45 Who Are You?

## 3.8 Installing Lotus Instant Messaging and Web Conferencing 6.5.1

Setting up Lotus Instant Messaging and Web Conferencing (formerly called Sametime) to work with WebSphere Portal offers portal users the complete set of people awareness features available in Collaborative portlets. In our example, this software is installed on bc3srv1.

**Important:** Do not install the Instant Messaging and Web Conferencing server and Team Workplace server on the same Domino server. These should be on two separate Domino servers.

Complete the following steps:

1. Shut down the Domino server by issuing the **quit** command from the Domino Console on the secondary server (in our example, bc3srv1/itso).
2. Run **demo32** from CD 13-1 (Lotus Instant Messaging and Web Conferencing for Windows V6.5.1).
3. Click **English**.
4. Click **Install Sametime Server**.
5. Accept the license agreement and click **Next**.
6. On the Welcome window, click **Next**.
7. Click **Yes** to install to the existing Domino server.
8. Verify that the installation directories match the Domino server directories and click **Next**.
9. When the installation completes, click **Finish**.
10. When prompted, browse to and select the server.id file in C:\Lotus\Domino\Data\server.id (bc3srv1.id in our example). Click **Next**.
11. Select **LDAP** from the drop-down list and enter the host name and port in the required fields (bc3srv5.itso.ra1.ibm.com and 389 in our example). Click **Next**.
12. In the HTTP tunnelling window, select the option to allow HTTP tunnelling and click **Next**.

**Note:** If you are planning to integrate with Tivoli Access Manager, you must enable HTTP tunneling by selecting this option. If, however, you are not going to use Tivoli Access Manager or any other type of reverse proxy, you can leave this option cleared, and users will need to have access to the Instant Messaging and Web Conferencing server through these default ports:

- ▶ 1533: For Instant Messaging
- ▶ 8082: For chat
- ▶ 8081: For Web conferences
- ▶ 554: For real-time streaming

13. Click **OK** to complete the installation of Instant Messaging and Web Conferencing.
14. Start the Instant Messaging and Web Conferencing server by selecting **Start** → **All Programs** → **Lotus Applications** → **Lotus Domino Server**.

15. When all the Instant Messaging and Web Conferencing services start, you will see the following message:

Sametime Server: Running on the Domino Console.

### 3.8.1 Modifying Domino after Lotus Instant Messaging installation

Here, we disable the directory assistance to prevent problems from arising down the installation path. Complete the following steps:

1. On the machine with Domino Administrator, start it by clicking **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Administrator**.
2. Enter the password.
3. Select **File** → **Database** → **Open**.
4. Browse to primary server (bc3srv5/itso in our example), and select **names.nsf**.
5. Close the About window if it opens.
6. Expand **Configuration** → **Servers** → **All Server Documents**.
7. Open the Server document for the primary server (bc3srv5/itso in our example).
8. Edit the server. Under the Basics tab, remove da.nsf (if it is there) as the directory assistance database name if it exists.
9. Click **Save & Close**.
10. Repeat these steps on the second Server document (bc3srv1/itso in our example).
11. In if you made any changes, perform the following steps (however, you might not have to do this task):
  - a. Force a push of names.nsf by issuing this command from the Domino Console:

```
push bc3srv1/itso names.nsf
```
  - b. Restart both servers.

### 3.8.2 Setting up Instant Messaging and Web Conferencing awareness and chat

To enable online awareness and chat for Team Workplace users, complete the following steps:

1. Copy the Java files required for Lotus Instant Messaging and online awareness.
2. Specify the Sametime Community server for Team Workplace to use.

## Copying Java files required for chat

To copy the Java files required for chat and online awareness, complete the following steps:

1. Install the Sametime Java Toolkit on the Instant Messaging server:
  - a. Download the Lotus Instant Messaging and Web Conferencing Java toolkit from the following URL:  
<http://www.lotus.com/idd/down.nsf>
  - b. Extract the downloaded file into the directory <dominodata>\domino\html\sametime\toolkits\st651javatk on the Instant Messaging server  
(C:\Lotus\Domino\Data\domino\html\sametime\toolkits\st651javatk in our example).
2. In the Domino data directory of the Instant Messaging server, create the subdirectory <domino data>\Domino\html\QuickPlace\peopleonline (C:\Lotus\Domino\Data\domino\html\QuickPlace\peopleonline in our example).
3. Copy the STComm.jar, CommRes.jar, and PeopleOnline31.jar files to the QuickPlace\peopleonline subdirectory you created in the previous step. These files can be found in the following locations:
  - Files from the Instant Messaging and Web Conferencing server:  
STComm.jar and CommRes.jar:  
<dominodata>\domino\html\sametime\toolkits\st651javatk\bin  
(C:\Lotus\Domino\Data\domino\html\sametime\toolkits\st651javatk\bin in our example).
  - Files from the Team Workplace server:  
PeopleOnline31.jar: <Domino data>\QuickPlace  
(C:\Lotus\Domino\Data\QuickPlace in our example).

## Specifying the Instant Messaging server in Team Workplace

**Note:** From this point, when restarting the Domino servers, make sure to start the server with Instant Messaging first. You will receive errors about not finding the LDAP server on the primary server, but that is okay and can be ignored. The procedure we used here was to restart the secondary server and wait for it to come up and then restart the primary server (awareness could fail to function if it is unable to detect the Instant Messaging and Web Conferencing server at startup).

Complete the following steps:

1. Open a browser and enter `http://<server_name>/quickplace` as the URL.

2. Click **Sign in**. Use a user that has administrative access to Team Workplace (portaladmin in this case).
3. Select **Server Settings** → **Other Options** and click **Edit Options**.
4. Under the Sametime Servers heading, make sure that the Sametime Instant Messaging server is in the community field. Use the full name of the server (http://bc3srv1.itso.ra1.ibm.com in our example).
5. Click **Next**.
6. Sign out of Team Workplace.
7. Restart the Domino server with Team Workplace.

**Note:** Checkpoint for Lotus Instant Messaging and Web Conferencing online awareness

To check Lotus Instant Messaging and Web Conferencing online awareness, complete the following steps:

1. Open a browser and enter:  
`http://<sametime_server_name>/sametime/toolkits/st651javatk/index.html`  
For example, in our configuration, the URL is:  
`http://bc3srv1.itso.ra1.ibm.com/sametime/toolkits/st651javatk/index.html`
2. Log in to Team Workplace and see if the awareness icon turns green (it sometimes took 20 seconds for this to happen).
3. The sample page with online awareness opens, as shown in Figure 3-46 on page 107. You should see an online awareness indicator in green besides the ID you entered in the previous window.



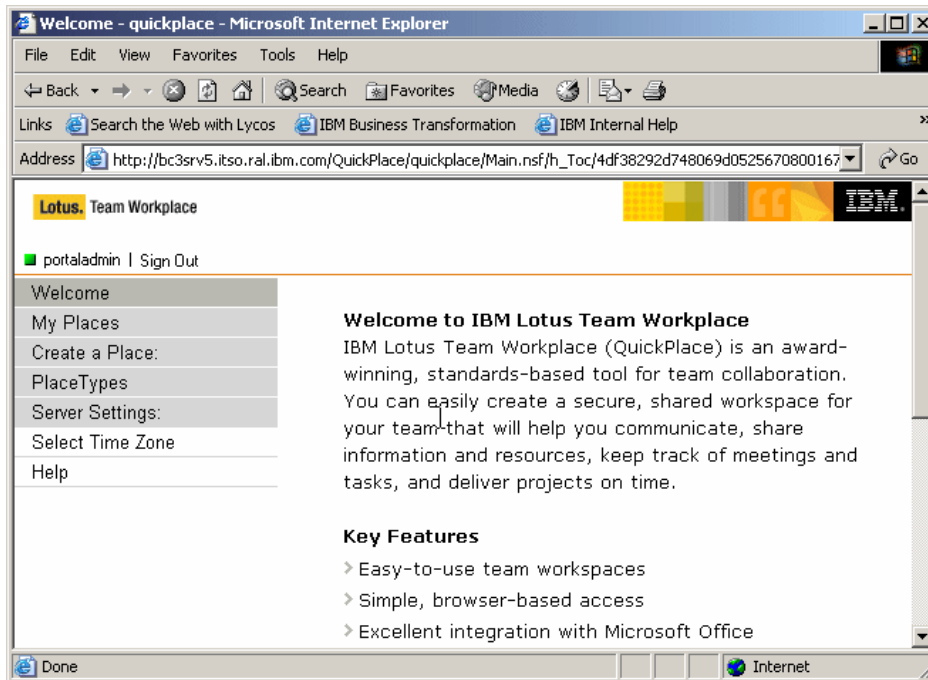


Figure 3-46 Lotus Instant Messaging online awareness

### 3.8.3 Editing the Sametime.ini file to set the security level

Before you perform the configuration task, set the security level. WebSphere Portal uses a Lotus Instant Messaging server application to enable Lotus Instant Messaging connectivity or people awareness. To allow this connectivity to work, you must set a security level by editing the Sametime.ini file. Complete the following steps:

1. Go to the Lotus Instant Messaging server (bc3srv1 in our example).
2. Locate the C:\Lotus\Domino\sametime.ini file to grant portal access to the Lotus Instant Messaging server.
3. Create a backup copy of the file.
4. Add the following line to the top of the file using a text editor. This is to configure the Lotus Instant Messaging server to accept all IPs as trusted. Add the following line to the Debug section:

```
[Debug]
VPS_BYPASS_TRUSTED_IPS=1
```

5. Change VPS\_IGNORE\_UNKNOWN\_CLIENT\_IP to equal 0.

6. Save and close the file.
7. Restart both Domino servers.

## 3.9 Configuring WebSphere Portal for Domino Directory

Follow these steps to edit the `wpconfig.properties` file and run the appropriate configuration tasks so that WebSphere Portal can work with the Domino LDAP server:

1. Locate the `<wp_root>/config/wpconfig.properties` file and create a backup copy.
2. Update the file property values under the WebSphere Application Server and Domino sections applicable to your environment using the values in Table 3-9 as a basis. For the purpose of the proof of concept, the fields shown in Table 3-9 were updated.

*Table 3-9 Values used in the lab*

| Property                      | Value used                  |
|-------------------------------|-----------------------------|
| WasUserId                     | cn=wpsbind,o=itso           |
| WasPassword                   | wpsbind                     |
| PortalAdminId                 | cn=portaladmin,o=itso       |
| PortalAdminIdShort            | portaladmin                 |
| PortalAdminPwd                | portaladmin                 |
| PortalAdminGroupId            | cn=wpsadmins                |
| PortalAdminGroupIdShort       | wpsadmins                   |
| WpsContentAdministrators      | cn=wpscontentadministrators |
| WpsContentAdministratorsShort | wpscontentadministrators    |
| WpsDocReviewer                | cn=wpsdocreviewer           |
| WpsDocReviewerShort           | wpsdocreviewer              |
| LTPAPassword                  | password                    |
| SSODomainName                 | itso.ra1.ibm.com            |
| LDAPHostName                  | bc3srv5.itso.ra1.ibm.com    |
| LDAPPort                      | 389                         |

| Property             | Value used                           |
|----------------------|--------------------------------------|
| LDAPAdminUIId        | cn=wpsbind,o=itso                    |
| LDAPAdminPwd         | wpsbind                              |
| LDAPServerType       | DOMINO502                            |
| LDAPBindID           | cn=wpsbind,o=itso                    |
| LDAPBindPassword     | wpsbind                              |
| WmmSystemId          | cn=wpsbind,o=itso                    |
| WmmSystemIdPassword  | wpsbind                              |
| LDAPSuffix           | <blank>                              |
| LDAPUserPrefix       | cn                                   |
| LDAPUserSuffix       | o=itso                               |
| LDAPGroupPrefix      | cn                                   |
| LDAPGroupSuffix      | <blank>                              |
| LDAPUserObjectClass  | inetOrgPerson                        |
| LDAPGroupObjectClass | groupOfNames                         |
| LDAPGroupMember      | member                               |
| LDAPGroupFilter      | (&(cn=%v)(objectclass=groupOfNames)) |

3. Ensure that the Domino servers are started. If not, start the Domino servers by clicking **Start** → **All Programs** → **Lotus Applications** → **Lotus Domino Server** on both machines.
4. Open a command prompt and change the current working directory to <was\_root>/bin.
5. Enter the following commands:

```
startServer server1
stopServer WebSphere_Portal
```
6. From a command prompt, type `WPSconfig.bat validate-wmmur-ldap` from the <wp\_root>/config directory.  
You should see the message `BUILD SUCCESSFUL` after successfully running the command.

**Note:** If the configuration task fails, verify the values in the `wpconfig.properties` file and also check the output, as specified in step 8 on page 110. Before running the task again, be sure to stop the WebSphere Portal application server by entering the following command from the `<was_root>/bin` directory and specifying the WebSphere Application Server user ID and password (as defined by the `WasUserid` and `WasPassword` properties):

```
stopServer WebSphere_Portal -user was_admin_userid -password
was_admin_password
```

7. From a command prompt, type `WPSconfig.bat enable-security-wmmur-ldap` from the `<wp_root>/config` directory.

You should see the message `BUILD SUCCESSFUL` after successfully running the command.

**Note:** In our setup, here we choose to enable security with realm support. You can also enable security without realm support and use the configuration wizard, but you will not get the full functionality of the virtual portals as provided in V5.1

8. Check the output for any error messages before proceeding with any additional tasks. Output is in `configtrace.log` and `configtrace1.log` in `wp_root\log`.
9. Stop the servers:

```
stopServer WebSphere_Portal -user was_admin_userid -password
was_admin_password
```

After this completes, also make sure that `server1` is stopped by issuing:

```
stopServer server1 -user was_admin_userid -password was_admin_password
```

**Note:** After you have enabled security with your LDAP directory, you will need to provide the user ID and password required for security authentication on WebSphere Application Server when you perform certain administrative tasks with WebSphere Application Server.

In our configuration, the command is as follows:

```
stopServer WebSphere_Portal -user wpsbind -password wpsbind
```

10. Open the `PumaService.properties` file found in the `wp_root\shared\app\config\services` directory:
  - a. Add `user.sync.remove.attributes=cn,CN`.

- b. Save the file.
11. Open the wmm.xml file in a text editor (file is found at wp\_root\wmm):
  - a. Locate the <ldapRepository .. > section of the file.
  - b. Change the adapterClassName= value to:

```
adapterClassName="com.ibm.ws.wmm.ldap.Domino.Domino6LdapAdapterImpl"
```
12. Start both the servers by running these commands in a command prompt from was\_root\bin:

```
startServer server1
```

After this has completed, also make sure that WebSphere Portal is started by issuing:

```
startServer WebSphere_Portal
```
13. Open the WebSphere Application Server administrative console by clicking **Start** → **All Programs** → **IBM WebSphere** → **Application Server v5.1** → **Administrative Console**.

**Note:** The SSO mechanism requires the use of a token. This token, referred to as a Lightweight Third Party Authentication (LTPA) token, contains data that uniquely identifies the user, such as the user's ID and a digital signature used to authenticate the token by the application server.

If you have already configured SSO between Domino LDAP and WebSphere Application Server, use the same LTPA token that was created by WebSphere Application Server and imported by Domino LDAP.

14. Select **Security** → **User Registry** → **Custom**.
15. Click **Custom Properties**.
16. Check if the property userRegistryRealm already exists. If yes, select the property and edit. Otherwise, click **New**.
17. Set the following parameters:
  - Name: userRegistryRealm
  - Value: <ldap fully qualified host name>:<port>In our example, this is bc3srv5.itso.ra1.ibm.com:389.

**Note:** The previous steps 14-17 are not documented in the *Information Center* at the time of writing and must be done for SSO to work between Domino and WebSphere Portal with realm support.

18. Select **Security** → **Authentication Mechanisms** → **LTPA**.

19. Enter a name for the key file, for example, C:\domwas.key.

20. Click **Export Keys** (Figure 3-47).

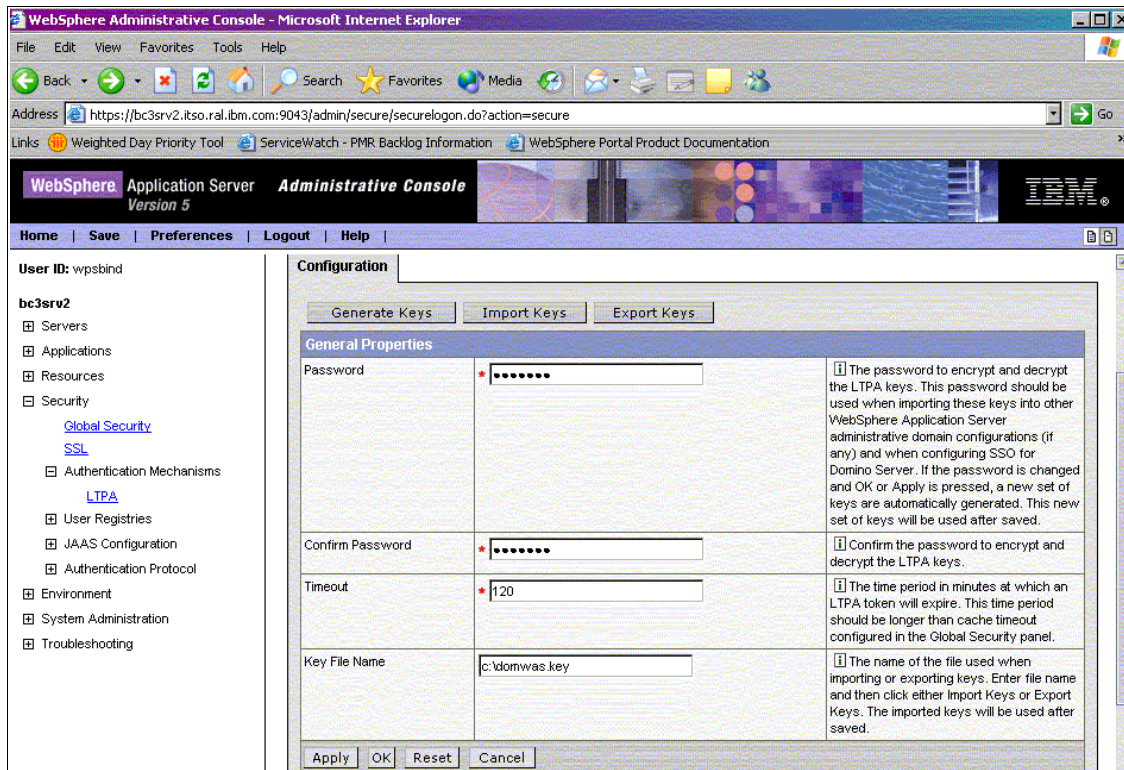


Figure 3-47 Export LTPA token from WebSphere Portal

21. Click **Save** (Figure 3-48 on page 113).

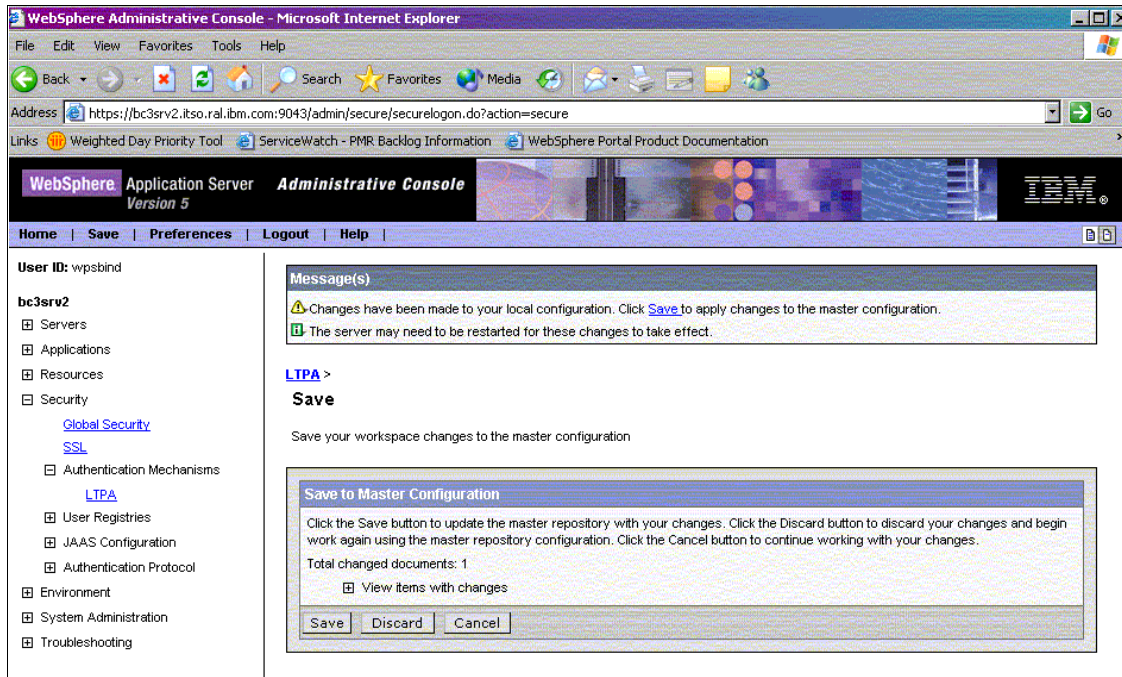


Figure 3-48 Save window

22. Stop both servers:

```
stopServer WebSphere_Portal -user was_admin_userid -password
was_admin_password
```

After this completes, also make sure that server1 is stopped by issuing:

```
stopServer server1 -user was_admin_userid -password was_admin_password
```

23. Open Domino Administrator.

24. Open the names.nsf database on the primary server (bc3srv5/itso in our example) by clicking **File** → **Database** → **Open**.

25. Make sure it is on the primary server (bc3srv5/itso in our example).

26. Click the **Configuration** tab.

27. Expand **Web**.

28. Click **Web Configuration**.

29. Expand \*- **Web SSO Configurations**.

30. Open the **Web SSO Configuration for Ltpa token** (Figure 3-49 on page 114).

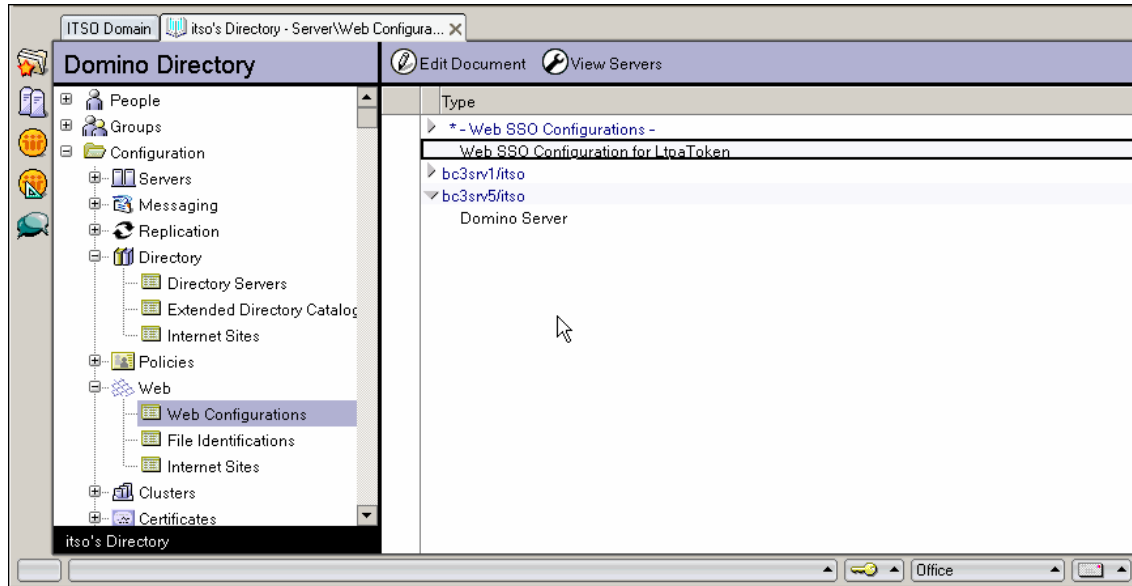


Figure 3-49 Import the LTPA token on the Domino server

31. Edit the document.

32. Click **Keys** → **Import WebSphere LTPA Keys** (Figure 3-50).

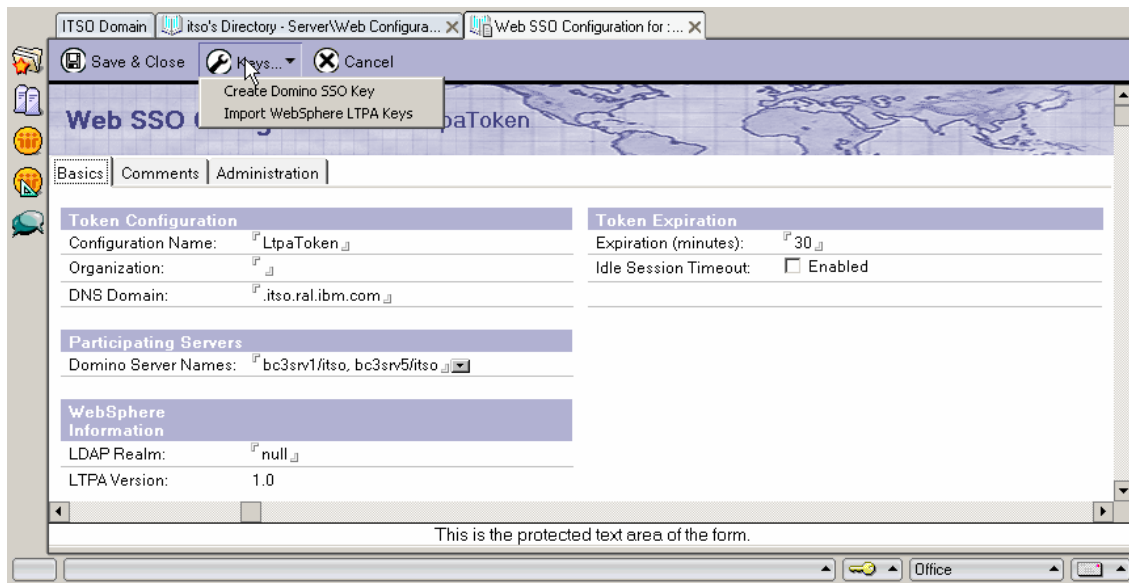


Figure 3-50 Import the LTPA token



33. Ignore the warning message that SSO configuration has already been initialized. Click **OK**.
34. Enter the path of the key (Figure 3-51). For example, in the lab, the key was copied to C:\ltpa\domwas.key. Click **OK**.

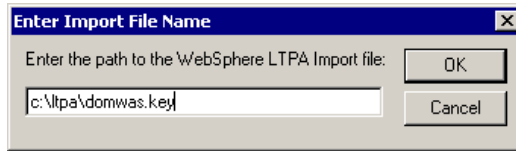


Figure 3-51 Path to the LTPA token

35. Type the LTPA password, for example, password (Figure 3-52). Click **OK**.

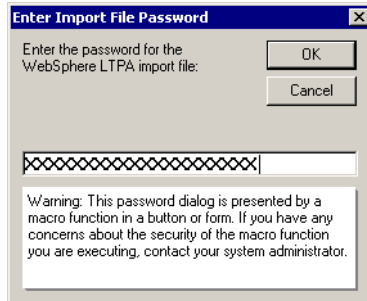


Figure 3-52 Enter the LTPA password

36. You will see the message Successfully imported WebSphere LTPA keys. Click **OK**.
37. Enter <server\_name>\:389 as the LDAP realm (Figure 3-53 on page 116). It is important to enter the slash and colon (\:) before the port number.

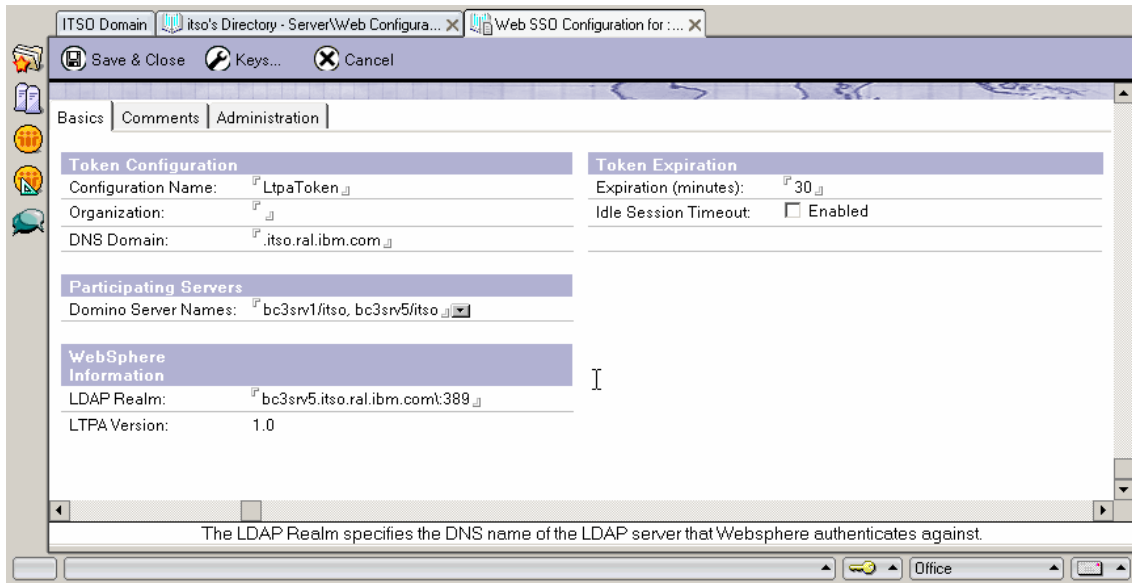


Figure 3-53 Finish Importing LTPA token

38. Click **Save & Close**.

39. Push the names.nsf file from bc3srv5 to bc3srv1 with the following command in the Domino Console:

```
push bc3srv1/itso names.nsf
```

40. Restart both Domino servers.

41. Start both the servers by running these commands in a command prompt from was\_root\bin:

```
startServer server1
```

After this completes, start WebSphere Portal by issuing:

```
startServer WebSphere_Portal
```

**Note:** Checkpoint for single sign-on

To check single sign-on, complete the following steps:

1. Log in to the portal by entering the following URL:  
`http://<fully_qualified_server_name>:9081/wps/portal`  
In our example: `http://bc3srv2.itso.ra1.ibm.com:9081/wps/portal`
2. Point the same browser to `http://<domino_server>/names.nsf`.  
In our example: `http://bc3srv1.itso.ra1.ibm.com/names.nsf`
3. You should see the Domino address book without being challenged for a user name and password if single sign-on is working properly.

## 3.10 Deploying Lotus Collaborative Components

IBM Lotus Collaborative Components provide the building blocks for integrating the functionality of IBM Lotus Domino, Lotus Instant Messaging and Web Conferencing (formerly called Sametime), Lotus Team Workplace (formerly called QuickPlace), and Lotus Discovery Server™ into portals and portlets. To use Lotus Collaborative Components, you must use the Lotus companion products (Lotus Instant Messaging and Web Conferencing, Lotus Team Workplace, and Lotus Discovery Server). In addition, you can configure Lotus Collaborative Components to use Domino Directory as the LDAP server.

**Note:** In WebSphere Portal V5.1, the Collaborative portlets that are most common are deployed by default and only need to be configured.

To enable the Lotus Collaborative Components, perform the following steps:

1. Stop the server by issuing:  

```
stopServer WebSphere_Portal -user was_admin_userid -password
was_admin_password
```
2. Locate the `<wp_root>/config/wpconfig.properties` file and make a back up of it before making any changes. Then, open in your favorite text editor use Table 3-10 on page 118 as a guide for the values you should modify.

Table 3-10 Lotus Collaborative Components values used in this example

| Property                    | Value used               |
|-----------------------------|--------------------------|
| LCC.DominoDirectory.Enabled | true                     |
| LCC.DominoDirectory.Server  | bc3srv5.itso.ra1.ibm.com |
| LCC.DominoDirectory.port    | 389                      |
| LCC.DominoDirectory.SSL     | false                    |
| LCC.QuickPlace.Enabled      | true                     |
| LCC.QuickPlace.Server       | bc3srv5.itso.ra1.ibm.com |
| LCC.QuickPlace.Protocol     | http                     |
| LCC.QuickPlace.Port         | 80                       |
| LCC.Sametime.Enabled        | true                     |
| LCC.Sametime.Server         | bc3srv1.itso.ra1.ibm.com |
| LCC.Sametime.Protocol       | http                     |
| LCC.Sametime.Port           | 80                       |

3. Save the file.
4. Open a command prompt and navigate to the wp\_root\config directory and run the following configuration tasks:

```
wpsconfig.bat lcc-configure-dominodirectory
wpsconfig.bat lcc-configure-quickplace
wpsconfig.bat lcc-configure-sametime
```

### Configuring the Collaborative portlets to bind to LDAP

In this step, we set up LDAP binding for the Collaborative portlets, which will give us faster access to the information we need for the Collaborative portlets.

Perform the following steps:

1. Locate the CSEnvironment.properties file in the Windows/UNIX <wp\_root>\shared\app\config directory.
2. Open the file in a text editor.
3. Remove the comment tag (#) from the beginning of the line that contains CS\_SERVER\_DOMINO\_DIRECTORY\_1.userid=.
4. At the end of the line, add a user ID that has at least reader access to the address book (names.nsf) of your Domino LDAP server. Type the Domino LDAP canonical name for the user (cn=wpsbind,o=itso in our example).

5. Go to the line that contains `CS_SERVER_DOMINO_DIRECTORY_1.encryptedpwd=` and remove the comment tag (`#`) from the beginning of this line.
6. Copy the line that contains `CS_SERVER_DOMINO_DIRECTORY_1.encryptedpwd=` and paste it into a new file.
7. In the new file, at the end of the line, add the Internet password for the user ID that was entered for `CS_SERVER_DOMINO_DIRECTORY_1.userid=` (`wpsbind` in our example).
8. Save this new file as `dominobind.txt` in the `<was_root>\bin` directory.
9. Open a command prompt in the `<was_root>\bin` directory, and run the following command:

```
PropFilePasswordEncoder dominobind.txt
CS_SERVER_DOMINO_DIRECTORY_1.encryptedpwd
```
10. Open the `dominobind.txt` file, and copy the encrypted password after `CS_SERVER_DOMINO_DIRECTORY_1.encryptedpwd=`.
11. Go back to the `CSEnvironment.properties` file.
12. Paste the encrypted password after `CS_SERVER_DOMINO_DIRECTORY_1.encryptedpwd=`.
13. Save and close the `CSEnvironment.properties` file.
14. Close the `dominobind.txt` file, and then delete `dominobind.txt` and `dominobind.txt.bak` from the `<was_root>\bin` directory.

**Note:** This step allows server names to appear in the server drop-down list, and users should be able to automatically detect the mail database for the Domino Web Access (formerly called iNotes™ Web Access) and Notes mail portlets. If you continue to experience problems with the drop-down (picker) list or auto-detection of the mail database, see the following troubleshooting Technotes:

- ▶ *Troubleshooting Pickers in Collaborative Portlets*, Technote 1157249.
- ▶ *Troubleshooting Automatic Detection of your Mail File with the Different Collaborative Portlets*, Technote 1157029.

15. Start both the servers by running these commands in a command prompt from the `was_root\bin` directory:

```
startServer server1
```

After this completes, make sure that WebSphere Portal is started by issuing:

```
startServer WebSphere_Portal
```

## Configuring the Collaborative portlet

For the Team Workplace and Web Conferencing portlet to work, you must perform the following steps:

1. Log in to WebSphere Portal as the administrator (portaladmin in our example).
2. Click **Administration**.
3. Click **Portlet Management** → **Portlets**.
4. Search for the portlet using Title Contains and work.
5. Choose the Wrench icon for My Lotus Team Workplaces.
6. On the next window, which looks similar to Figure 3-54, for the New parameter, enter QuickPlaceHostname, and the New value is the Team Workplace server (in our example, bc3srv5.itso.ral.ibm.com).

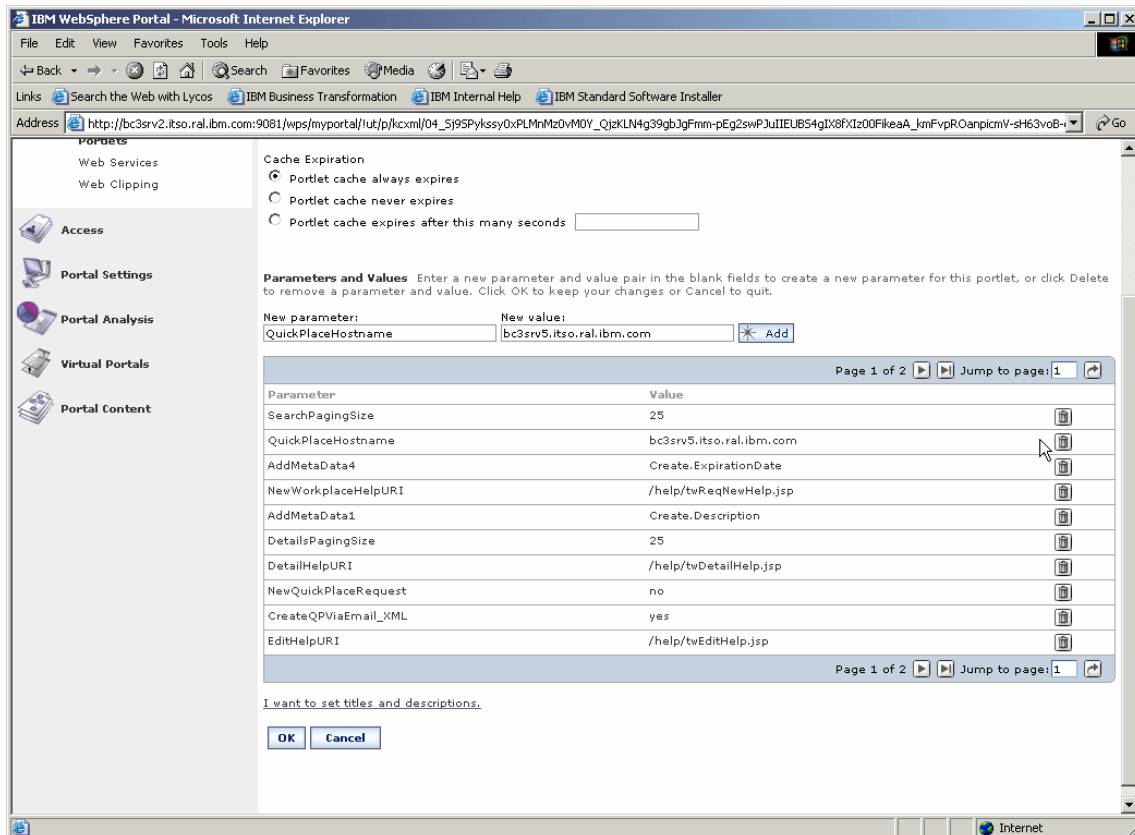


Figure 3-54 Configuring the My Lotus Team Workplaces portlet

7. Then, click the Delete icon on the existing parameter of the same name (QuickPlaceHostname; your form data will be kept).
8. Click **Add**.
9. Click **OK**.
10. Next, search for and select the Lotus Web Conferencing portlet.
11. Click the Wrench icon for that portlet, and there, update three parameters (see Table 3-11 for the values used). Delete them and then add them back with the appropriate value, as we did for the previous portlet.

*Table 3-11 Values used in the lab*

| <b>New parameter</b> | <b>New value</b>         |
|----------------------|--------------------------|
| SametimeServerName1  | bc3srv1.itso.ral.ibm.com |
| SametimeUserName1    | portaladmin              |
| SametimePassword1    | portaladmin              |

12. Click **OK**.
13. Log out of WebSphere Portal.

**Note:** Checkpoint for the Collaborative portlets

To check the Collaborative portlets, complete the following steps:

1. Log onto WebSphere Portal.
2. Click the **My Workplace** tab.
3. Click **Team Spaces**. You should see a window similar to the one shown in Figure 3-55.
4. Click **Web Conferences**. You should see a window similar to the one shown in Figure 3-56 on page 124.
5. To check the chat features, double-click a name from the Sametime Contact List (we clicked ourselves). You should see a window similar to the one shown in Figure 3-57 on page 125.
6. If you also configured the mail files, before clicking **Mail**, you should see a window similar to the one shown in Figure 3-58 on page 126. You might receive an error with Internet Explorer, but the error does not occur with Mozilla.
7. To check the People Finder, enter a name (`wpsbind` in our example) and click **Search**. You should get a result similar to the one shown in Figure 3-59 on page 127.
8. Click **Domino Databases**, and then click the Edit icon for the portlet. On the next page, if after entering your server (`bc3srv5.itso.ra1.ibm.com` in our example) and clicking the black check mark, the drop-down lists are populated (as shown in Figure 3-60 on page 128), the binding to LDAP is working. Having chosen the Inbox, it will look similar to the window shown in Figure 3-61 on page 129.



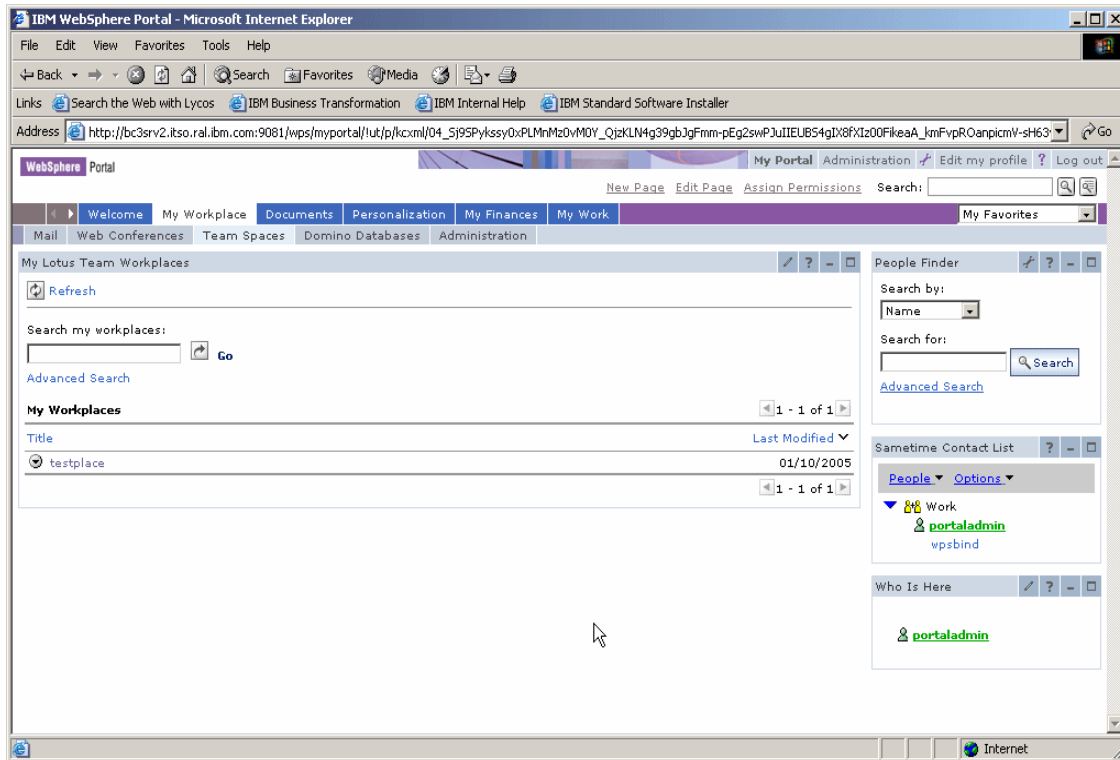


Figure 3-55 Checkpoint For My Team Workplaces portlet

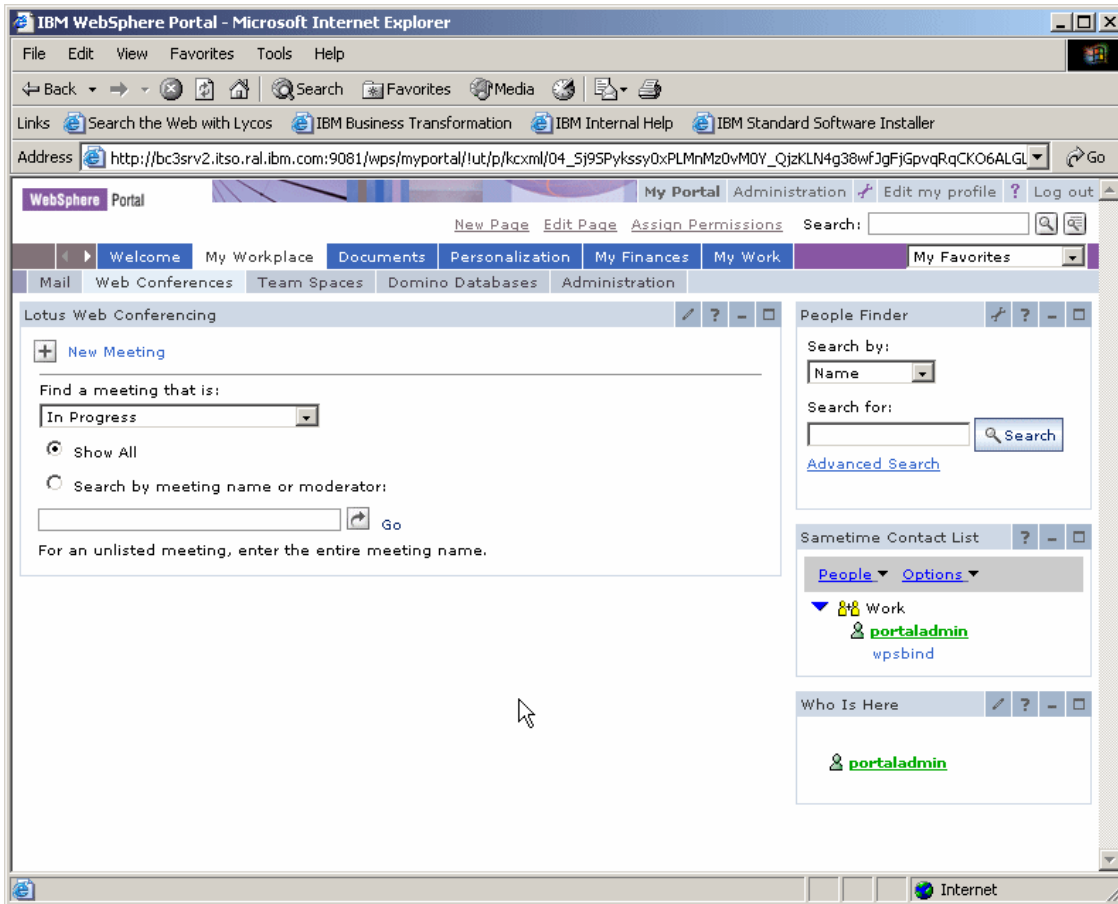


Figure 3-56 Checkpoint for the Web Conferencing portlet

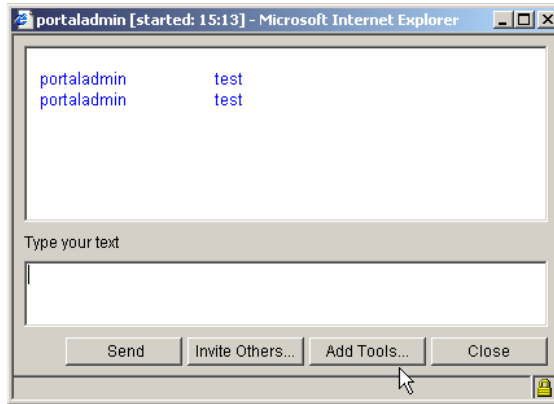


Figure 3-57 Instant Messaging chat

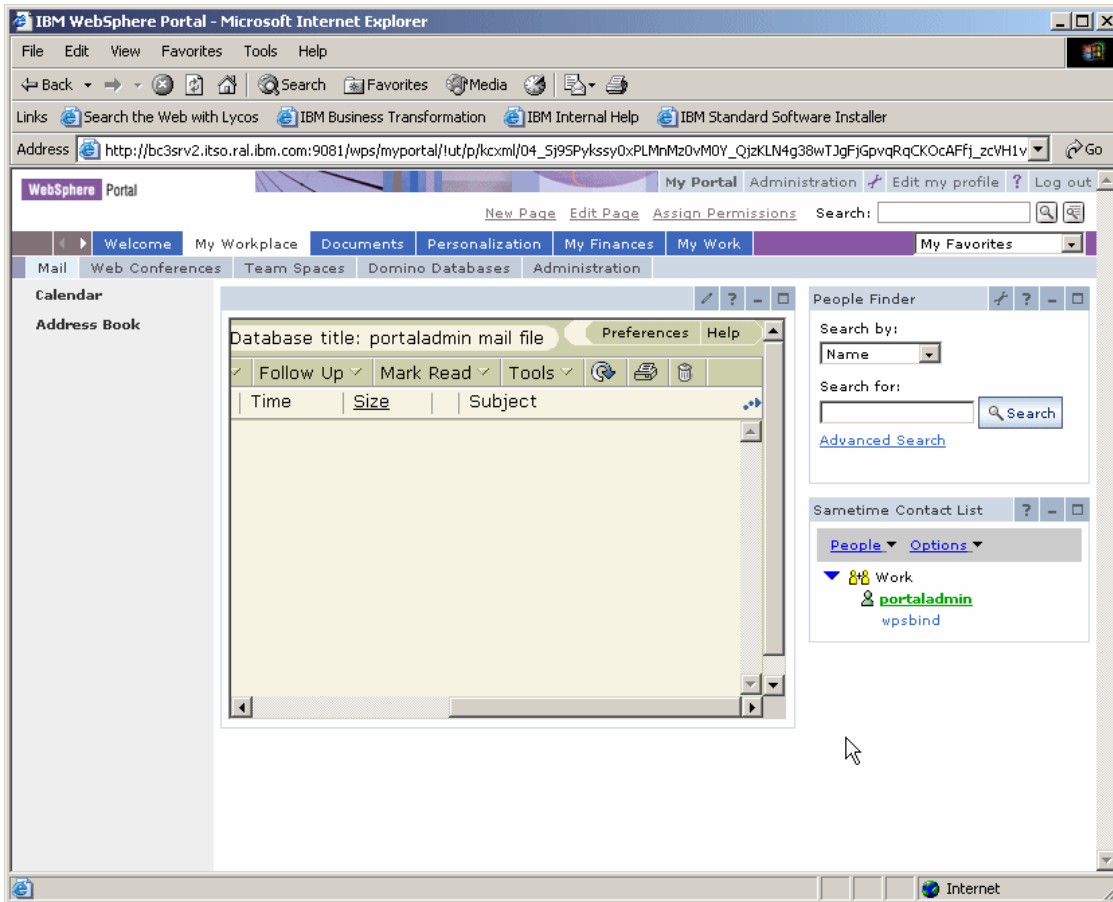


Figure 3-58 Checkpoint for mail functions

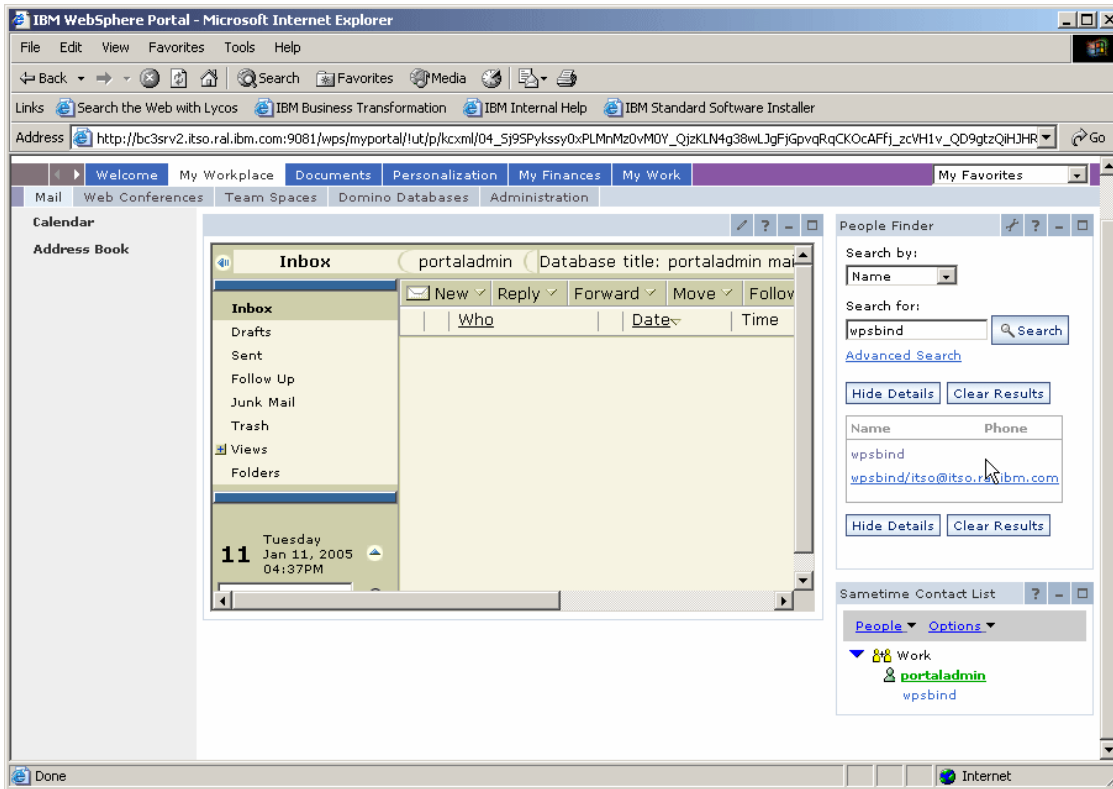


Figure 3-59 Checkpoint for People Finder

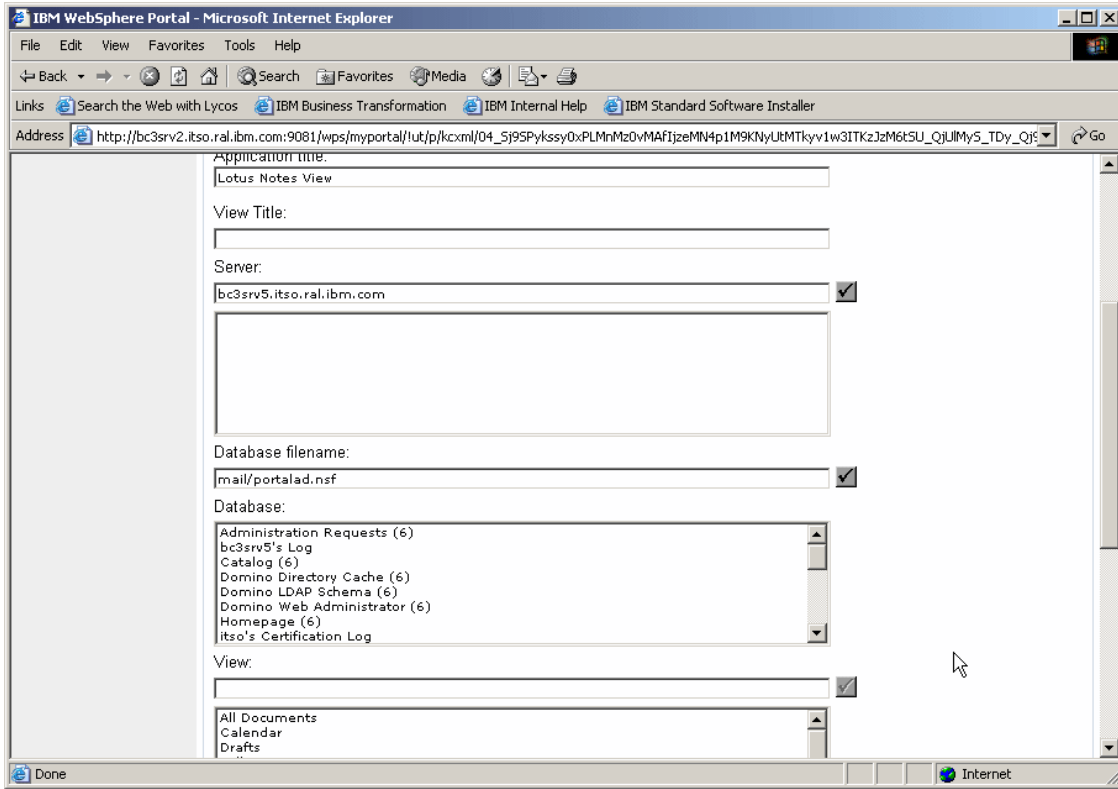


Figure 3-60 Checkpoint for Lotus Notes View portlet with drop-down list

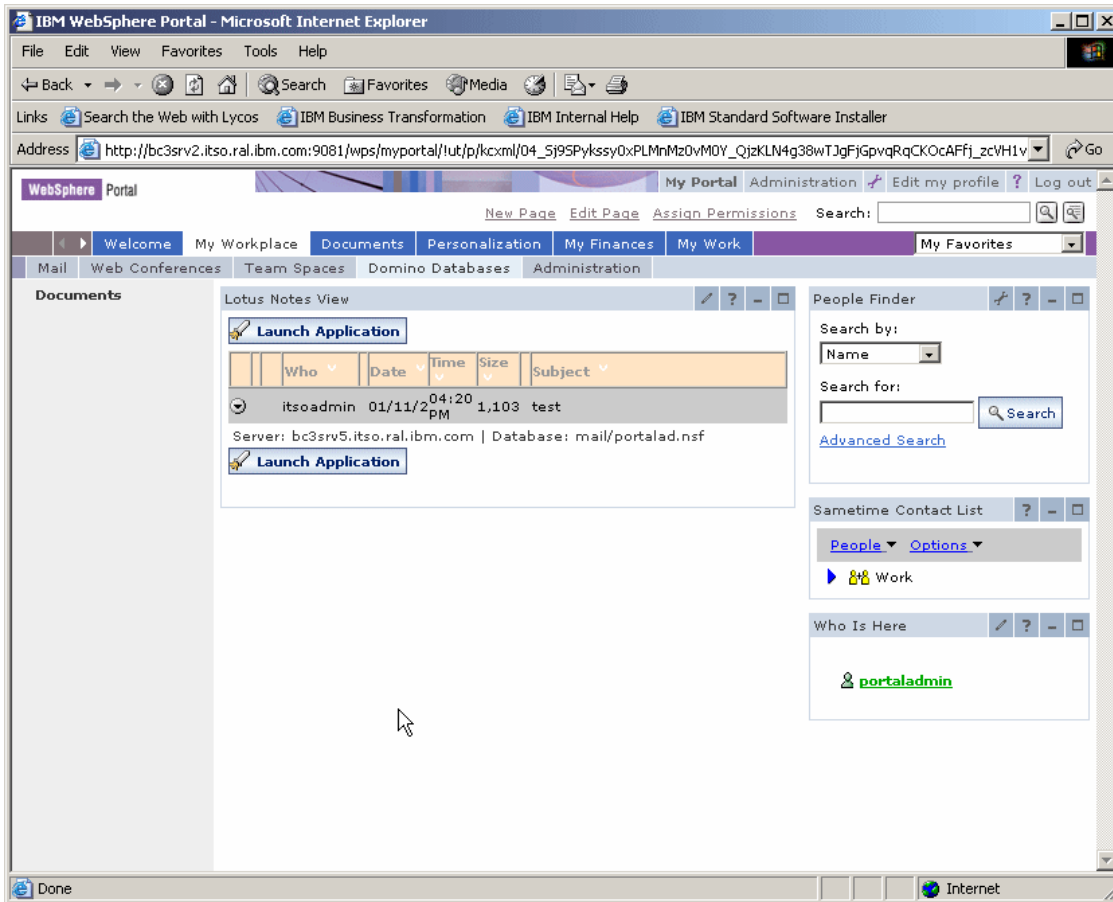


Figure 3-61 Checkpoint for Notes View portlet







## WebSphere Portal: Clustering

This chapter guides you through the configuration of IBM WebSphere Portal in a clustered environment.

Our example is based on the topology shown in Figure 4-1 on page 133, but we do not cover the installation and configuration of the reverse proxy and dispatcher components. Those components are already included in the WebSphere Application Server Network Deployment V5.1 product. You can find information about installing and configuring the Edge components in *IBM WebSphere V5.1 Performance, Scalability, and High Availability, WebSphere Handbook Series*, SG24-6198.

The topology shown in Figure 4-1 on page 133 includes:

- ▶ Machine 1: This is the Web server. This machine runs IBM HTTP Server V1.3.28.
- ▶ Machine 2: The deployment manager machine is responsible for managing all WebSphere Application Server nodes in the cell. This machine runs IBM WebSphere Application Server Network Deployment V5.1.1.1 and IBM WebSphere Business Integration Server Foundation V5.1.1. The WebSphere Portal nodes are members of the cluster managed by the deployment manager named WP51.

- ▶ Machine 3: This is node 1 of the IBM WebSphere Portal server cluster. This machine runs the following products:
  - WebSphere Business Integration Server Foundation V5.1.1
  - WebSphere Portal V5.1
  - IBM DB2 UDB Enterprise Server Edition V8.1
- ▶ Machine 4: This is node 2 of the IBM WebSphere Portal server cluster. This machine runs the following products:
  - WebSphere Business Integration Server Foundation V5.1.1
  - WebSphere Portal V5.1
  - IBM DB2 UDB Enterprise Client V8.1
- ▶ Machine 5: This is the LDAP server machine. This machine runs Domino Enterprise Server V6.5.3.
- ▶ Machine 6: This is the Domino Administrator. This machine runs Domino Administrator V6.5.3.

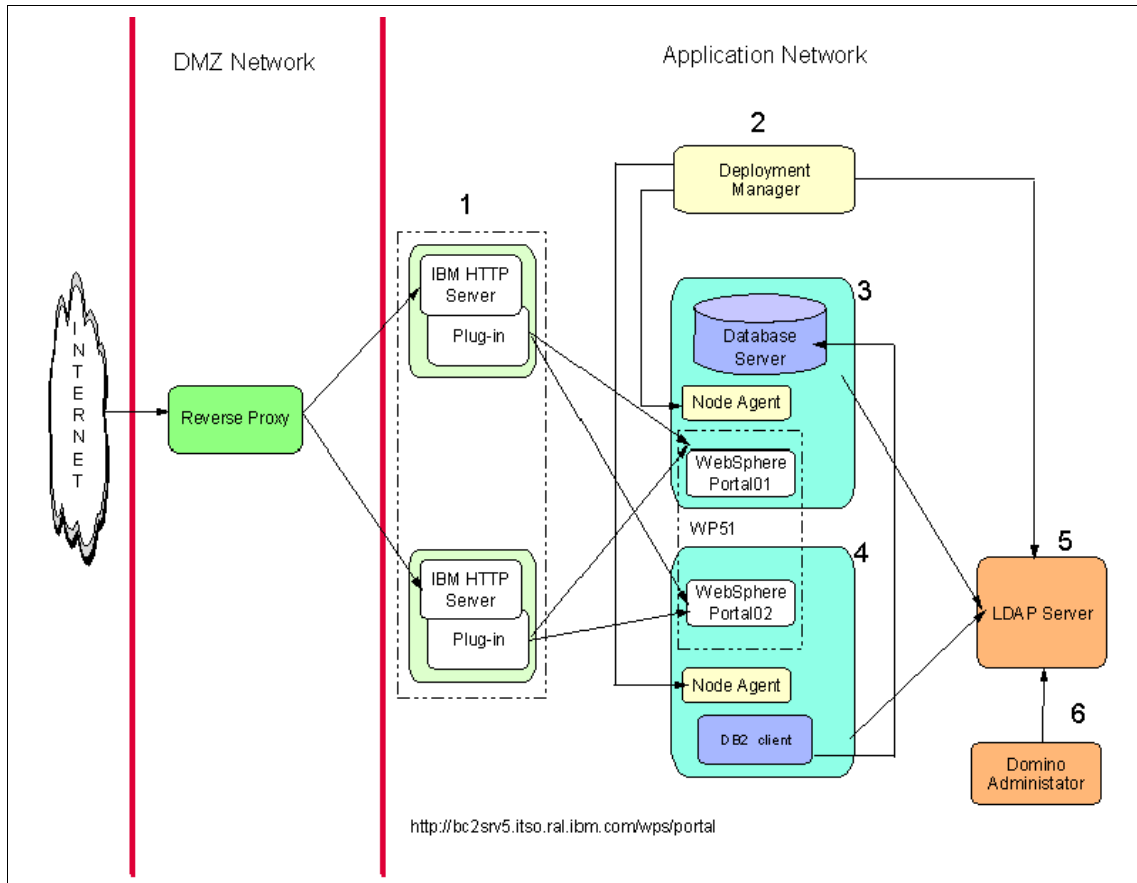


Figure 4-1 Clustering topology

The WebSphere Application Server Network Deployment V5.1 enables you to run applications on multiple servers and on multiple physical nodes.

You will be using terms that are only used by WebSphere Application Server Network Deployment. This is a brief description of a few of them:

- ▶ Cell

A cell is a group of nodes in a single administrative domain. The deployment manager manages the cell master configuration repository. This repository stores the configuration for all nodes included in the cell.

- ▶ **Deployment manager**  
The deployment manager process provides a single point of administration for all nodes of the cell. The deployment manager manages the communication with the node agent process presented on each node added to the cell.
- ▶ **Master configuration repository**  
The master configuration repository contains the configuration data of the cell. The deployment manager is responsible for the updates to the configuration repository. Only the deployment manager can update the node repository.
- ▶ **Node agent**  
The node agent resides in each node. It is responsible for the communication with the deployment manager, file transfer services, configuration synchronization, and performance monitoring.
- ▶ **Cluster**  
A cluster is a logical collection of application server processes. It provides the load balance, fail-over, and scalability between application servers that are part of the cluster.

For a detailed description of the Network Deployment components, read *IBM WebSphere Application Server V5.1 System Management and Configuration, WebSphere Handbook Series, SG24-6195*.

For our lab installation, Table 4-1 specifies the CDs that are required for the installation of the WebSphere Portal components in this chapter.

*Table 4-1 Installation CDs*

| <b>Disk</b> | <b>Description</b>                                                                                         |
|-------------|------------------------------------------------------------------------------------------------------------|
| CD Setup    | WebSphere Portal V5.1 - Portal Install (Setup), V5.1                                                       |
| CD #1-1     | WebSphere Business Integration Server Foundation for Windows V5.1                                          |
| CD #1-2     | WebSphere Business Integration Server Foundation for AIX, V5.1                                             |
| CD #1-15    | WebSphere Business Integration Server Foundation - WebSphere Application Server V5.1 Fix Pack1 for Windows |
| CD #6-1     | WebSphere Server Network Deployment for Windows                                                            |
| CD #6-8     | Network Deployment Fix Pack                                                                                |

## 4.1 WebSphere Application Server Network Deployment

This section explains how to install and configure IBM WebSphere Application Server Network Deployment Version 5.1.1.1 on Microsoft Windows Server 2003.

### 4.1.1 Installing WebSphere Application Server Network Deployment

This section provides instructions about how to install a base installation of IBM WebSphere Application Server Network Deployment V5.1.

We refer to this machine as *bc3srv6*.

Before installing WebSphere Application Server Network Deployment, you must perform the following steps:

1. Create a group named `mqm`.
2. Create a group named `mqbrkr`.
3. Create a user `mquser`.
4. Make the user `mquser` a member of the group `mqm`.
5. Make the user administrator a member of groups `mqm` and `mqbrkr`.
6. The installation requires you to log on with an ID with sufficient user privileges on the system. The user account must be part of the local administrators group and have the following user rights assigned to it:
  - Act as part of the operating system
  - Log on as a service

You can change user privileges by clicking **Start** → **All Programs** → **Administrative Tools** → **Local Security Policy**.

This will then open a new window in this window. Expand **Security Settings** → **Local Policies** → **User Rights Assignment**.

**Note:** After assigning user privileges, you should log off from Windows and log on again for the changes to become effective.

To install the Network Deployment machine, complete the following steps:

1. Insert CD #6-1. It contains the IBM WebSphere Application Server Network Deployment product.
2. Launch the installation wizard with the command:  

```
\cdrom\win\install.bat
```
3. Select the desired language. Click **OK**.

4. Click **Next** on the Welcome page.
5. Accept the license terms. Click **Next**.
6. Select the components to be installed. Click **Next**.
7. Enter the Network Deployment installation directory. We suggest that you use C:\WebSphere\DeploymentManager. Click **Next**.
8. Enter the Network Deployment Node Name, Host Name, and cell name or accept the defaults. You will see a window similar to the one shown in Figure 4-2.

**Important:** We recommend that you use the default values on this window. If you enter a node name that is already in use, you will have problems when trying to add a node to the cell.

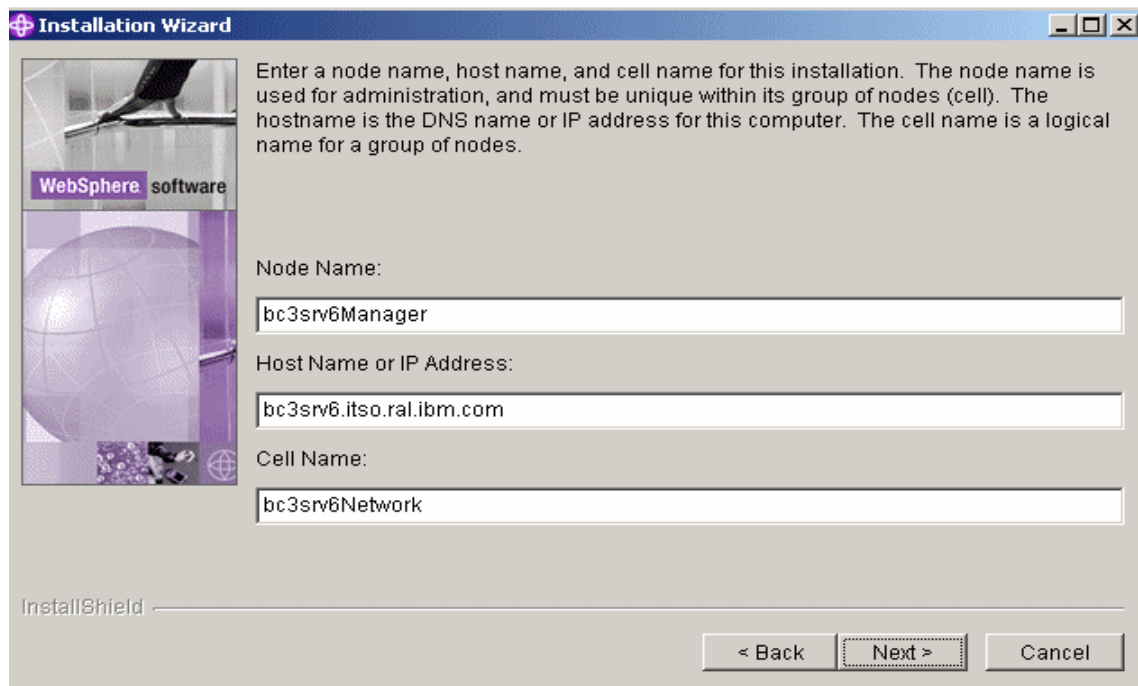


Figure 4-2 Accept the defaults for the node name and cell name

9. The Summary window opens. Verify that the features to be installed are correct and click **Next** to continue.

Wait for the process to finish.

10. You have the option to register now or later. Choose the desired option. Click **Next**.
11. Click **Finish**. The installation is complete.
12. Click **Exit** to close the WebSphere Application Server LaunchPad.
13. The WebSphere Application Server - First Steps window might launch automatically. We will not start the server at this time. Click **Exit** to close the window.

## 4.1.2 Installing the Enterprise extensions on Network Deployment

This section describes how to upgrade WebSphere Application Server Network Deployment to the Enterprise level. It is required that Network Deployment and all WebSphere Application Server nodes be on the same level.

Table 4-2 shows the required levels of WebSphere products in this WebSphere Portal solution.

*Table 4-2 Required versions for a clustering solution on WebSphere Portal*

| Product                                         | Required version                                                                                                          |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| WebSphere Portal node                           | IBM WebSphere Application Server V5.1.1 plus IBM WebSphere Business Integration Server Foundation V5.1.1                  |
| WebSphere Application Server Network Deployment | WebSphere Application Server Network Deployment V5.1.1.1 plus IBM WebSphere Business Integration Server Foundation V5.1.1 |

If you completed 4.1.1, “Installing WebSphere Application Server Network Deployment” on page 135, this is the level of Network Deployment: WebSphere Application Server Network Deployment V5.1.

Now, you have to install IBM WebSphere Business Integration Server Foundation on the WebSphere Application Server Network Deployment machine:

1. Insert CD #1-1, which contains WebSphere Business Integration Server Foundation V5.1.
2. Start the installation wizard by running:
 

```
\cdrom\win\install.bat
```
3. Select the language. Click **OK**.
4. The Welcome page opens. Click **Next**.
5. Accept the license terms. Click **Next**.
6. Select the **Typical** setup type.

7. The installation wizard detects the installation of the Network Deployment. Click **Next**.
8. You can select **Run WebSphere Application Server as a Service**.
9. Select the user ID and the password. Click **Next**.
10. Insert the WebSphere Business Integration Server Foundation Disk 2 or specify the location of the WebSphere update directory.
11. Click **Next**. This process might take a while. Wait for the process to complete.
12. Verify the features that will be installed. Click **Next**.  
The installation starts. Wait for the process to finish.
13. You have the option to register now or later; choose the desired option. Click **Next**.
14. Click **Finish** to complete the installation.
15. We will not start the server at this time.

You have now upgraded WebSphere Application Server Network Deployment with Enterprise extensions.

### 4.1.3 Installing Network Deployment Fix Pack 1

Table 4-2 on page 137 shows the required versions for the WebSphere Portal nodes and WebSphere Application Server Network Deployment. After completing the steps in 4.1.2, “Installing the Enterprise extensions on Network Deployment” on page 137, this is the version of WebSphere Application Server Network Deployment: WebSphere Application Server Network Deployment V5.1 plus WebSphere Business Integration Server Foundation V5.1.

To upgrade WebSphere Application Server Network Deployment, complete the following steps:

1. Before you update Network Deployment, the JAVA\_HOME environment setting must point to the IBM software development kit (SDK) for WebSphere Application Server products. Source the appropriate command. For the Windows platform, it is:

```
install_root\bin\setupCmdLine.bat
```

1. Insert CD #6-8. It contains the Network Deployment Fix Pack and the was51\_nd\_fp1\_win.jar file.
2. Run the Update Installation Wizard tool:  

```
\cdrom\was51nd_fp1\updateWizard.bat
```
3. The Update Installation Wizard Welcome window opens. Click **Next**.



4. Select **Specify Product Information**. Click **Next**.
5. Select **Install fix packs**. Click **Next**.
6. Enter the path where the fix pack is located. Click **Next**. You will see a window similar to the one shown in Figure 4-3.
7. Select the fix pack name and click **Next**.

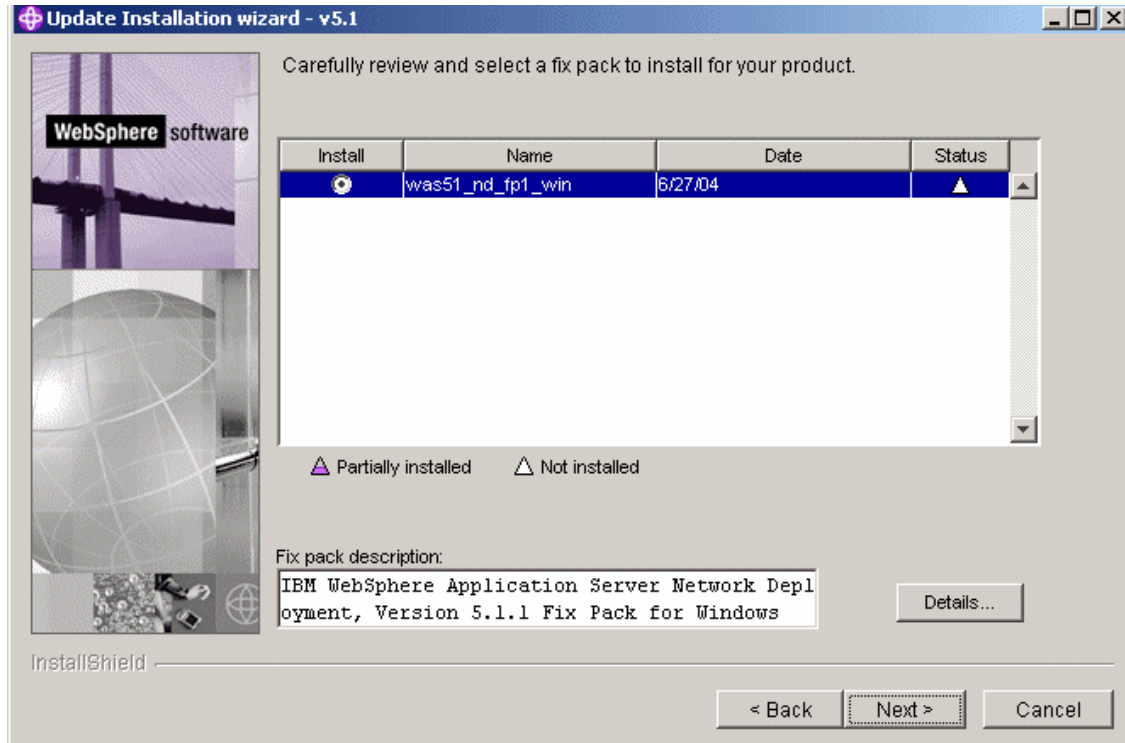


Figure 4-3 Select the fix pack name

8. The Summary window opens. The Update Installation Wizard will remove any interim fixes that you might have applied earlier and install the new fix pack. Click **Next**.
9. Verify that the fix pack was installed successfully. Click **Finish**.  
The version of WebSphere Application Server Network Deployment has changed to V5.1.1.  
We will not start the server at this time.

## 4.1.4 Installing WebSphere Business Integration Server Foundation Fix Pack 1

This section provides the instructions to install WebSphere Business Integration Server Foundation V5.1 Fix Pack 1 for WebSphere Application Server Network Deployment. You have already applied the Network Deployment Fix Pack 1; the same procedure must be followed for the Enterprise extensions. Complete the following steps:

1. Insert CD #1-15. It contains Fix Pack 1 for WebSphere Business Integration Server Foundation and the `wbisf51_nd_fp1_win.jar` file.
2. Run the Update Installation Wizard tool:  

```
\cdrom\wbisf51_fp1\updateWizard.bat
```
3. The Welcome window opens. Click **Next**.
4. Select **Specify Product Information** and enter the Network Deployment installation directory (in our environment, `C:\WebSphere\DeploymentManager`). Click **Next**.
5. Select **Install fix packs**. Click **Next**.
6. Enter the directory where the fix pack is located.
7. The Summary window shows the features that will be installed. Click **Next**.
8. Verify that the fix pack was installed successfully. Click **Finish**.

We will not start the server at this time.

## 4.1.5 Installing Network Deployment Cumulative Fix 1

This section provides the instructions to install WebSphere Application Server Network Deployment V5.1 Cumulative Fix 1. You have already applied the Network Deployment Fix Pack 1 and WebSphere Business Integration Server Foundation Fix Pack 1; the same procedure must be followed for Network Deployment Cumulative Fix 1. Complete the following steps:

1. Insert CD #6-8. It contains the CF1 for the Network Deployment server and the `was511_nd_cf1_win.jar` file.
2. Run the Update Installation Wizard tool:  

```
\cdrom\was511nd_cf1\updateWizard.bat
```
3. The Welcome window opens. Click **Next**.
4. Select **Specify Product Information** and enter the Network Deployment installation directory (in our environment, `C:\WebSphere\DeploymentManager`). Click **Next**.
5. Select **Install fix packs**. Click **Next**.

6. Enter the directory where the fix pack is located.
7. The Summary window shows the features that will be installed. Click **Next**.
8. Verify that the fix pack was installed successfully. Click **Finish**.

#### 4.1.6 Validating the Network Deployment installation

Verify that the WebSphere Application Server Network Deployment is working properly by completing the following steps:

1. Start the deployment manager:

```
\WebSphere\DeploymentManager\bin\startManager.bat
```

2. Open the startServer.log file in the \WebSphere\DeploymentManager\logs\dmgr directory. If the server was started successfully, you should see the following message:

```
Server dmgr open for e-business.
```

3. Open the deployment manager administrative console. Enter the following URL in your browser window:

```
http://<nd_hostname>:9090/admin
```

Where <nd\_hostname> is the Network Deployment fully qualified host name.

## 4.2 Installing and configuring IBM WebSphere Portal on node 1

The information in this section is described in detail in Chapter 3, “WebSphere Portal: Microsoft Windows Server 2003 install” on page 29.

In this chapter, we refer to this machine as *bc3srv3*.

To complete the installation and configuration of *bc3srv3*, complete the following steps:

1. Install a base WebSphere Portal installation using Cloudscape. For details, see 3.2, “Base installation” on page 37.
2. Install DB2 and export the data from Cloudscape to DB2. For details, see 3.3, “Migrating the database from Cloudscape to DB2” on page 53 or refer to the following *Information Center* link for the details about database configuration:

[http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/wpf/intr\\_db.html](http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/wpf/intr_db.html)

## 4.2.1 Configuring WebSphere Portal node 1 to a Web server

This section explains how to set up the WebSphere Application Server plug-in for use with your IBM HTTP Web server on Microsoft Windows Server 2003.

We refer to this machine as *bc2srv5*.

Complete the following steps:

1. Ensure that the Web server is installed and configured. Refer to the Web server documentation for more information.
2. After the Web server is successfully installed and running, stop the Web server.
3. Install the plug-in on the machine where the Web server is located.
4. Launch the WebSphere Application Server installation program. The installation program is located in the `<was_cd_root>/<operating_system>/WAS` directory, where `<was_cd_root>` is the root directory of the CD containing the WebSphere Application Server component for your operating system, and where `<operating_system>` indicates the operating system of the machine where you are installing the plug-in.
5. Click **Next** on the Welcome panel. Accept the license agreement, and click **Next**.
6. Select **Custom**.
7. On the Features panel, clear all the features except the Web server plug-ins and the entry for the specific Web server for which you are installing the plug-in, such as IBM HTTP Server. Click **Next**.
8. Specify the directory path where you want to install the WebSphere Application Server files. This path must be the same that you used for the WebSphere Application Server that you are using with the Web server. Click **Next**.
9. Specify the location of the Web server configuration file or other required files if appropriate. For example, the configuration file for IBM HTTP Server (`httpd.conf`) is located in the `<ihs_root>/conf` directory. Click **Next**.
10. Complete the installation.

11. Verify the WebSphere Application Server plug-in installation by checking the Web server configuration. For example, if you install the IBM HTTP Server plug-in on a machine that is running the Windows operating system, the plug-in installation updates the <ihs\_root>/conf/httpd.conf file with the following lines:

```
LoadModule ibm_app_server_http_module
"C:\WebSphere\AppServer\bin\mod_ibm_app_server_http.dll"
WebSpherePluginConfig "C:\WebSphere\AppServer/config/cells/plugin-cfg.xml"
```

Update the WebSphere Application Server plug-in settings by completing the following steps:

- a. Ensure that the WebSphere Application Server administrative server is running by entering the following command from the Windows directory <was\_root>/bin:

```
startServer server1
```

- b. Configure the WebSphere Application Server virtual host:

- i. Open the administrative console by accessing the following URL in a browser:

```
http://<hostname.yourco.com>:9090/admin
```

Where <hostname.yourco.com> is the host name of the local machine.

In our example, this is `http://bc3srv3.itso.ral.ibm.com:9090/admin`.

- ii. After logging on, click **Environment** → **Virtual Hosts**, and then click **default\_host** from the list of virtual hosts.
- iii. Click **Host Aliases** from the list of additional properties.
- iv. On the Host Aliases page, click **New**.
- v. Enter the host name and port number of the machine where the Web server is installed. Click **OK**.
- vi. Click **Save**.

Regenerate the Web server plug-in settings:

- a. In the administrative console, click **Environment** → **Update Web Server Plugin**.
- b. Click **OK**.

12. Remote Web server only: Copy the plug-in file (<was\_root>/config/cells/plugin-cfg.xml) to the machine where the Web server is installed. Ensure that you copy the file to same directory on the remote Web server machine. This step is not necessary if the Web server and WebSphere Application Server are installed on the same machine.

13. Restart the Web server.

14. Verify the Web server plug-in configuration:

- a. Check the plug-in logs (the location of logs is specified in the plugin-cfg.xml file).
- b. Check the connection to WebSphere Application Server: Using a Web browser, request a URL to be served by WebSphere Application Server (for example, `http://<webserver_hostname>:<port_number>/snoop`).

15. Ensure that WebSphere Portal is running by entering the following command from the Windows directory `<was_root>/bin`:

```
startServer WebSphere_Portal
```

16. Verify that WebSphere Portal can be accessed from the Web server. For example, open a browser to:

```
http://<webserver_hostname>:<port_number>/wps/portal
```

After configuring WebSphere Portal to use an external Web server, you will access the portal with the Web server host name and port (80). In addition, you will be unable to access the portal using the WebSphere Portal host name and port (9081), unless there is a corresponding virtual host definition for port 9081 in the WebSphere Application Server configuration.

Many of the WebSphere Portal configuration tasks rely on the `WpsHostName` and `WpsHostPort` properties from the `wpconfig.properties` file. You must ensure that WebSphere Portal can be accessed using the host name and port specified by these property values. You can do this in one of two ways:

- ▶ Modify the `WpsHostName` and `WpsHostPort` property values to specify the Web server host name and port.
- ▶ Add the appropriate virtual host definition, as described in the following steps.

If you want to access WebSphere Portal using a host name and port different from your Web server, add the required virtual host definition using the WebSphere Application Server administrative console. Note, in a clustered environment, use the deployment manager administrative console to perform these steps. Complete the following steps:

1. Click **Environment** → **Virtual Hosts**.
2. Click the **default\_host** entry or the entry for the virtual host that is being used to access the WebSphere Portal application.
3. Click **Host Aliases**, and verify whether there is a host name and port entry corresponding to the values used to access WebSphere Portal (for example, `*:9081`). If the entry does not exist, click **New**, and enter the information for the host name and port you want to use.
4. Save your changes.

5. Regenerate the Web server plug-in.
6. If you are using a remote Web server, copy the updated plugin-cfg.xml file to the Web server machine.

Refer to the following *Information Center* link for the details of the Web server configuration:

[http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/wpf/inst\\_ihs.html](http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/wpf/inst_ihs.html)

After completing the steps, verify WebSphere Portal by rendering WebSphere Portal from a browser using the Web server, for example:

<http://bcr2srv5.itso.ra1.ibm.com/wps/portal>

## 4.2.2 Configuring to optimize for clustering

This section provides the instructions to modify the configuration of the WebSphere Business Integration Server Foundation and WebSphere Portal to optimize for clustering.

Edit the following file:

```
<was_root>/config/cells/<cell_name>/nodes/<node_name>/servers/WebSphere_Portal/server.xml
```

Within the opening and closing tags of each HTTP transport section (xmi:id="HTTPTransport\_<x>", where <x> is a unique number), add the following line:

```
<properties xmi:id="Property_10" name="ConnectionIOTimeout" value="180" required="false"/>
```

The following is an example of a HTTP transport section with the line added:

```
<transports xmi:type="applicationserver.webcontainer:HTTPTransport" xmi:id="HTTPTransport_1" sslEnabled="false">
<address xmi:id="EndPoint_1" host="" port="13975"/>
<properties xmi:id="Property_10" name="ConnectionIOTimeout" value="180" required="false"/>
</transports>
```

Edit the <was\_root>/properties/soap.client.props file. Increase the SOAP request timeout to 6000:

```
com.ibm.SOAP.requestTimeout=6000
```

### 4.2.3 Federating node 1 to the deployment manager using the `-includeapps` option

This node will be used as the primary node in the cluster and the cluster definition will be based on this node, so the node should be added to the cell using the `-includeapps` option when issuing the `addNode.bat` command.

The deployment manager should also be started before issuing the `addNode.bat` command.

To add a node to the deployment manager cell, issue the `addNode` command (on one line) on the command line of the node to be added (bc3srv3). For Windows:

```
<was_root>\bin\addNode.bat <deployment_manager_host> <deployment_manager_port>
-username <admin_user_id> -password <admin_password> [-includeapps] [-trace]
```

Where:

- ▶ `<was_root>` is the root directory on WebSphere Application Server.
- ▶ `<deployment_manager_host>` is the deployment manager host name.
- ▶ `<deployment_manager_port>` is the deployment manager SOAP connector address. The default value is 8879.
- ▶ `<admin_user_id>` is the WebSphere Application Server administrative user name. This parameter is optional, but it is required if security is enabled.
- ▶ `<admin_password>` is the administrative user password. This parameter is optional, but it is required if security is enabled.

For example:

```
addNode.bat bc3srv6.itso.ral.ibm.com 8879 -includeapps
```

The parameters are:

- ▶ `includeapps`:

The `-includeapps` parameter is optional. This parameter should only be used if there are enterprise applications already installed on this node that need to be added to the deployment manager master configuration. If you do not specify this flag, any application servers that are defined on this node will be included in the deployment manager configuration, but they might not be functional without their corresponding enterprise applications. If the application already exists in the cell, a warning is generated, and the application is not installed into the cell.

- ▶ `trace`

The `-trace` parameter is optional. This parameter generates trace information that is stored in the `addNode.log` file for debugging purposes.



Refer to the appropriate *Network Deployment Information Center* for details about the **addNode** command.

## 4.2.4 Starting WebSphere Portal and running the post-federation task

Start nodeagent on the WebSphere Portal node, node 1, by issuing this command:

```
<was_root>/bin/startServer.bat nodeagent
```

Start WebSphere Portal from deployment manager administrative console by selecting the **WebSphere\_Portal** server and clicking the **Start** button.

After WebSphere\_Portal is started, you will see a green arrow, as shown in Figure 4-4.

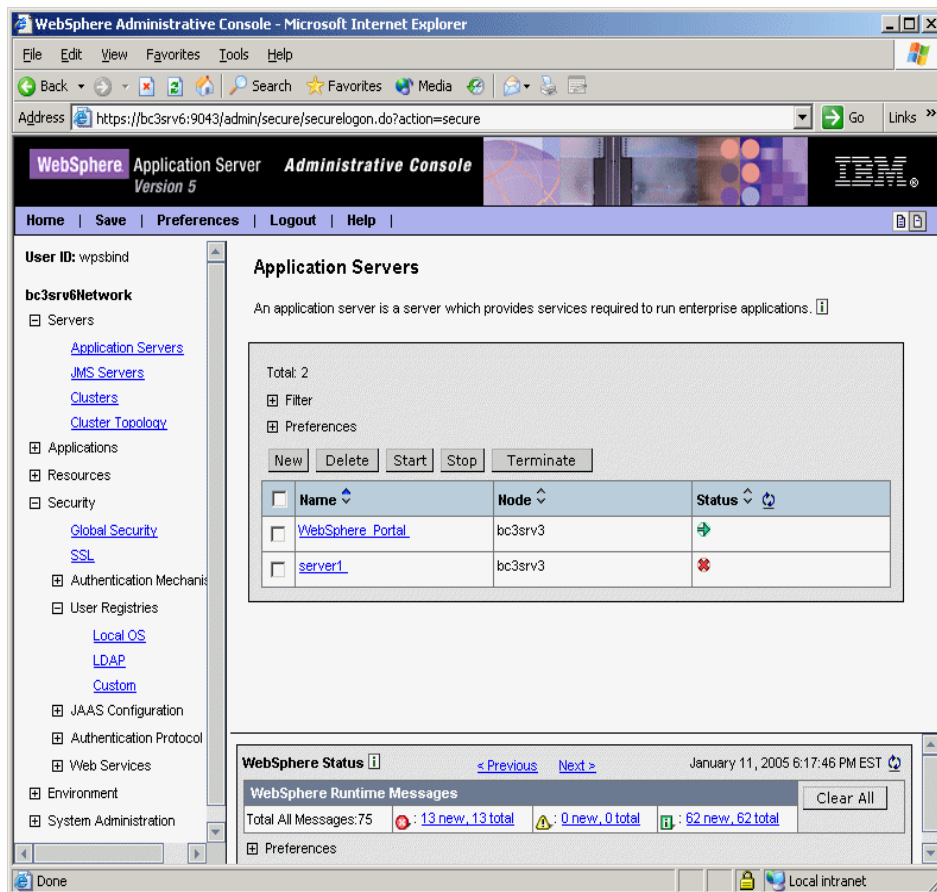


Figure 4-4 Application Servers

In the WebSphere Portal node 1 (bc3srv3), edit the <wps\_root>/config/wpconfig.properties file and change the CellName property:

```
CellName=<cell_name>
```

For example:

```
CellName=bc3srv6Network
```

The cell name changed during federation of node 1. To verify the cell name, you can identify it by <was\_root>/config/cells/<cell\_name>.

Run the post-portal-node-federation-configuration task by issuing the following command:

```
<wps_root>/config/WPSconfig.bat post-portal-node-federation-configuration
```

Verify WebSphere Portal by rendering it through a browser.

## 4.2.5 Updating virtual host entries and Web server plug-in

Perform the following steps to update the virtual host entries:

1. Check the virtual host entry in deployment manager administrative console by navigating to **Environment** → **Virtual Hosts** → **default\_host** → **Host Aliases**. Make sure that an entry exists for port 9081. If one does not exist, click **New** and add an entry by defining the Host Name as "\*" and the Port as 9081.
2. Update the plugin-cfg.xml file by navigating to **Environment** → **Update Web Server Plugin**. Click **OK**.
3. Edit the <dmgr\_root>/config/cells/plugin-cfg.xml file and change any directory structure occurrences specific to the Network Deployment machine to match the directory structure used on the Web server. For example, references to install\_dir/WebSphere/DeploymentManager might need to be replaced with install\_dir/WebSphere/AppServer.

If you are using a remote Web server (bc2srv5), copy the updated plug-in configuration file (<dmgr\_root>/config/cells/plugin-cfg.xml) to the Web server's plug-in configuration directory.

4. Stop and start IBM HTTP Server.
5. Edit the wpsHostName and wpsHostPort properties in the wpconfig.properties file to match the host name and port that are being used to render WebSphere Portal from a browser.
6. Verify WebSphere Portal by rendering it through a browser.

## 4.2.6 Configuring WebSphere Portal node 1 and Network Deployment for security

The configuration and settings of the LDAP server in this section is described in detail in 3.4, “Adding an LDAP to the portal” on page 71.

This section guides you through the configuration of WebSphere Portal and WebSphere Application Server Network Deployment in a clustered environment with the helper file.

**Note:** Because we have already federated the Portal node 1 into the deployment manager, this procedure will configure security on the Portal node 1 and the deployment manager with the same security settings. If you use this process, you now no longer are required to manually configure security on the deployment manager as was required with WebSphere Portal 5.0.x Versions.

In this example, we use the configuration wizard (a tool introduced with WebSphere Portal V5.1).

Using the configuration wizard, complete the following steps:

1. Locate the appropriate configuration helper file located at `<wps_root>/config/helper`.
2. Make copy of original helper file.
3. Edit the helper file with the proper LDAP values to use with the configuration wizard.
4. Start the configuration wizard from `<wps_root>/config/wizard/configwizard.bat`.
5. Click **Next** on Welcome window.
6. Select **Enable LDAP security** and click **Next**.
7. Select **Lotus Domino Enterprise Server** and click **Next**.
8. Select the helper file you edited previously and click **Next**.
9. Verify the values and click **Next**.
10. Verify the values and populate the DbPassword and WmmDbPassword fields because they are not in the helper and click **Next**.
11. On the final window, click **Next** to begin the task to enable security.

After the task completes successfully, restart the deployment manager to activate the new security settings.

Verify the new security settings by rendering the deployment manager administrative console and WebSphere Portal from a browser. You should now be prompted for a password when accessing the deployment manager administrative console.

## 4.2.7 Final steps to complete node 1 federation

Make sure that the `wp.wire.jar` is present on the deployment manager node.

Verify whether the `wp.wire.jar` file is present in the `<dmgr_root>/lib/ext` directory on the Network Deployment machine.

If the file is not present, copy the file from the `<was_root>/lib/ext` directory on any WebSphere Portal node to the `<dmgr_root>/lib/ext` directory on the Network Deployment machine.

Restart the deployment manager.

Verify WebSphere Portal by rendering it through a browser and making sure the federated servers are visible in the **Servers** → **Application Server** view through the deployment manager administrative console.

## 4.3 Installing and configuring WebSphere Portal on node 2

In this chapter, we refer to this machine as *bc3srv4*.

First, install a base WebSphere Portal installation using Cloudscape. For details, see the steps in 3.2, “Base installation” on page 37. Next, install IBM DB2 UDB Enterprise Client and export the data from Cloudscape to the external IBM DB2 UDB Enterprise Server Edition.

This section guides you through the installation and configuration of the second WebSphere Portal node that will be part of the cluster and its prerequisites.

The configuration procedure for the second node, *bc3srv4*, is different from what was used for *bc3srv3*. At this point, we expect that you have installed and configured *bc3srv3*.

**Important:** Use the same directory structure you used for *bc3srv3*, that is, if you installed WebSphere Portal on `\WebSphere\Portal`, do the same for the subsequent WebSphere Portal machines.

If you are planning on adding more than two machines to a cluster, follow the steps provided in this section for every node you want to add in the cluster.

### 4.3.1 Connecting WebSphere Portal node 2 to the external database

This section provides the instructions to configure the second node (bc3srv4) of WebSphere Portal.

Refer to the following *Information Center* link for the details about the database configuration:

[http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/wp/intr\\_db.html](http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/wp/intr_db.html)

**Note:** To perform this task, you will edit the configuration helper file with the same database values as from the previous configuration helper used on node 1. Then, use the configuration wizard to run the connect-database task to build the data sources on node 2 to point to the databases that have already been initialized for node 1. The end result will be that node 2 and node 1 will use the same database repository.

In this example, we use the configuration wizard (a tool introduced with WebSphere Portal V5.1).

Using the configuration wizard, complete the following steps:

1. Locate the appropriate configuration helper file on node 2 located at `<wps_root>/config/helper`.
2. Make a backup copy of original helper file on node 2.
3. Make a copy of the configuration helper file used on node 1 and move it to node 2.
4. Verify the DbLibrary property to make sure the driver location is valid on node 2.
5. Start the configuration wizard on node 2 from `<wps_root>/config/wizard/configwizard.bat`.
6. Click **Next** on Welcome window.
7. Select appropriate database and click **Next**.
8. Select the helper file you copied previously from node 1 and click **Next**.
9. Verify the values (especially the location of the DbLibrary property) and click **Next**.
10. Click **Next** on the final window to start the connect-database task.

**Important:** Do not verify the WebSphere Portal operation on node 2 at this time and do not log in. This could cause database corruption, because node 2 is now pointing to the cluster database; however, node 2 has not been configured with security. After security is configured, we validate the WebSphere Portal operation.

### 4.3.2 Configuring WebSphere Portal node 2 for security

When configuring the WebSphere Portal node 2, check the following information:

- ▶ Make sure that you use the identical security settings that were used on node 1 to configure security on node 2.
- ▶ Make sure that you edit the `wpsconfig.properties` file on node 2 to change the `DbSafeMode` property value to `True`. By default, `enable-security-ldap` and `disable-security` write entries into the WebSphere Portal tables on the cluster database. Because this database is already configured with production settings, you do not want to make any writes to the database, because any typographical errors in the `wpsconfig.properties` or helper files might result in database corruption. By setting the `DbSafeMode` to `True`, you will ensure that no database writes will occur.
- ▶ The `WpsHostName` value must also be changed here because node 2 has not been configured to use a Web server as node 1 was, so the entry is incorrect for node 2. If this is not changed, it will cause a failure in the `enable-security-ldap` task. This value needs to be the fully qualified domain name that is used to render WebSphere Portal.

In this example, we use the configuration wizard (a tool introduced with WebSphere Portal V5.1).

Using the configuration wizard, complete the following steps:

1. Locate the appropriate configuration helper file located at `ps_root>/config/helper`.
2. Make a backup copy of original helper file on node 2.
3. Make a copy of the configuration helper file used on node 1 and move it to node 2.
4. Edit the `<wps_root>/config/wpsconfig.properties` file and change `DbSafeMode` to `True`.
5. Edit the helper file to change the `WpsHostName` property to the host name of the Portal node 2.
6. Start the configuration wizard from `<wps_root>/config/wizard/configwizard.bat`.

7. Click **Next** on Welcome window.
8. Select **Enable LDAP security** and click **Next**.
9. On the final window, click **Next** to begin the task to enable security on node 2.  
After the task completes successfully, edit the `<wps_root>/config/wpconfig.properties` file and change the `DbSafeMode` property back to `False`.
10. Verify the new security settings by rendering the deployment manager administrative console and WebSphere Portal from a browser. You should now be prompted for a password when accessing the deployment manager administrative console.

### 4.3.3 Configuring to optimize for clustering

To optimize the cluster, edit the `<was_root>/properties/soap.client.props` file. Increase the SOAP request timeout to 6000:

```
com.ibm.SOAP.requestTimeout=6000
```

### 4.3.4 Federating node 2 to the deployment manager

Because this is a secondary node, the node should be added to the cell without using the `-includeapps` option when issuing the `addNode.bat` command.

The deployment manager should also be started before issuing the `addNode.bat` command.

To add a node to the deployment manager cell, issue the `addNode` command (on one line) on the command line of the node to be added, for Windows:

```
<was_root>\bin\addNode.bat <deployment_manager_host> <deployment_manager_port>
-username <admin_user_id> -password <admin_password>
```

Where:

- ▶ `<was_root>` is the root directory on WebSphere Application Server.
- ▶ `<deployment_manager_host>` is the deployment manager host name.
- ▶ `<deployment_manager_port>` is the deployment manager SOAP connector address. The default value is 8879.
- ▶ `<admin_user_id>` is the WebSphere Application Server administrative user name. This parameter is optional, but it is required if security is enabled.
- ▶ `<admin_password>` is the administrative user password. This parameter is optional, but it is required if security is enabled.

For example:

```
addNode.bat bc3srv6.itso.ra1.ibm.com 8879 -username wpsbind -password wpsbind
```

Refer to the appropriate *Network Deployment Information Center* for details about the **addNode** command.

### 4.3.5 Starting WebSphere Portal and running the post-federation task

Perform the following instructions to start Portal and run post-federation:

1. Start nodeagent on the WebSphere Portal node, node 2, by issuing this command:  

```
<was_root>/bin/startServer.bat nodeagent
```
2. Start WebSphere Portal from the deployment manager administrative console by selecting the **WebSphere\_Portal** server on node 2 and clicking the **Start** button.

After WebSphere Portal is started, you will see a green arrow, as shown in Figure 4-5. At this point, you can see that both WebSphere Portal nodes that have been federated to the deployment manager are started.

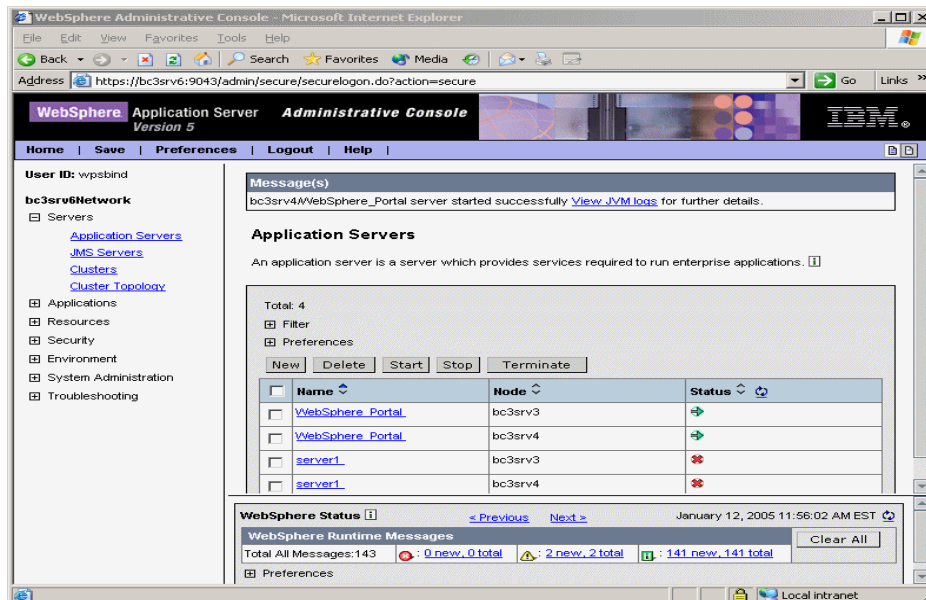


Figure 4-5 Application Servers



3. Edit the `<wps_root>/config/wpconfig.properties` file and change the *CellName* and *PrimaryNode* properties:

```
CellName=<cell_name>
```

For example, `CellName=bc3srv6Network`.

4. The cell name changed during federation of node 2. To verify the cell name, you can identify it by `<was_root>/config/cells/<cell_name>`:

```
PrimaryNode=<true or false>
```

For example, `PrimaryNode=false`.

This is the second node added to the deployment manager, so it is considered a secondary node.

5. Run the `post-portal-node-federation-configuration` task by issuing the following command:

```
<wps_root>/config/WPSconfig.bat post-portal-node-federation-configuration
```

At this point, if you try to render WebSphere Portal through a browser, you will get a “Page Cannot be Displayed” error because the node was added without the `-includeapps` option and, therefore, is not associated with the `wps.ear` file. After creating the cluster, the node 2 will share the `wps.ear` file that is associated with node 1.

## 4.4 Adding WebSphere Portal nodes to the cell

Before adding a WebSphere Portal node to a cell, verify the following information:

- ▶ The cell must already exist, that is, you have to install and validate WebSphere Application Server Network Deployment before adding nodes to a cell.
- ▶ The date and time between the deployment manager machine and the nodes must be the same or within five minutes. All machines must be set using the same time zone.
- ▶ Cloudscape cannot be used in a clustered environment. You must transfer the data to a more robust database, such as DB2 *before* adding the node to a cell.
- ▶ You cannot install WebSphere Portal into an existing cluster environment.
- ▶ All WebSphere Portal configurations must be done outside the cell. This means that if you need to change the configuration of a WebSphere Portal node that was added to a cell, you have to remove it from the cell, configure it, and then add it back into the cell.

- ▶ On all nodes, install a sample portlet to validate the Deployment portlet configuration and avoid problems after creating the cluster.
- ▶ Deployment manager must be running.
- ▶ The node name must be unique in the cell.
- ▶ Both server1 and WebSphere Portal must be running on each node.

## 4.5 Creating the cluster

This section provides instructions about how to create a cluster and include members into a WebSphere Application Server Network Deployment cell.

This example describes how to create a cluster using horizontal scaling; the WebSphere Portal application existing on the bc3srv3 machine will be the clone template that we use to create a new cluster member on the bc3srv4 node.

You can find detailed information about clustering and horizontal and vertical scaling in *IBM WebSphere V5.1: Performance, Scalability, and High Availability, WebSphere Handbook Series*, SG24-6198.

To create a cluster, complete the following steps:

1. Open the bc3srv6 Network Deployment administration console:  
`http://bc3srv6.itso.ra1.ibm.com:9090/admin`
2. Expand **Servers**. Select **Clusters**, as shown in Figure 4-6 on page 157.

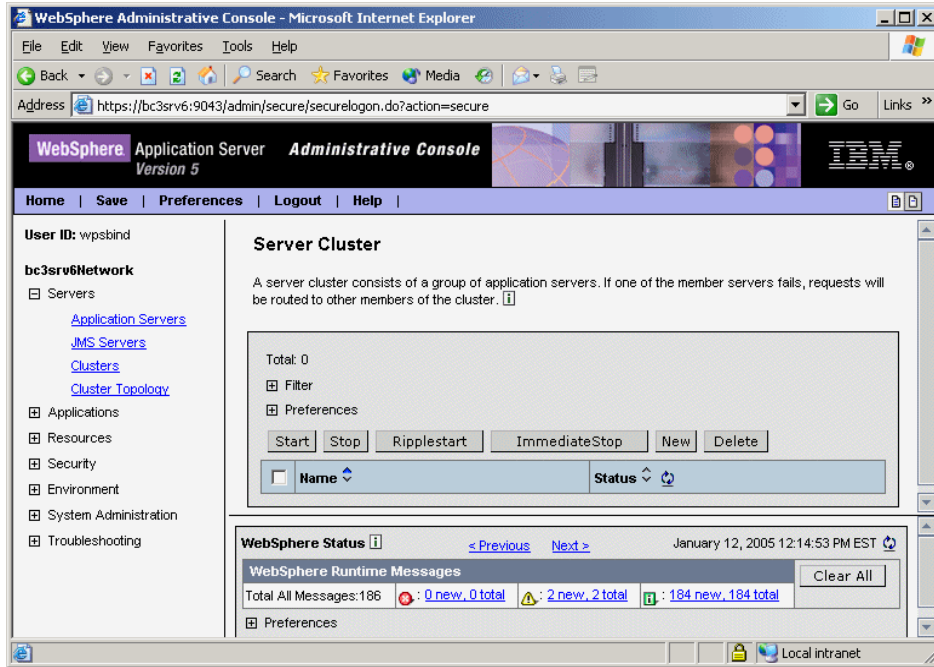


Figure 4-6 Server Cluster

3. The Create New Cluster panel opens on the right side of the window, as shown in Figure 4-7 on page 158. Enter the value for the Cluster name. In this example, we use WP51.
4. Select **Prefer local enabled**.
5. Select **Create Replication Domain for this cluster**.
6. Select **Select an existing server to add to this cluster**.
7. Choose the server **WebSphere\_Portal** from the node bc3srv3 (node 1).

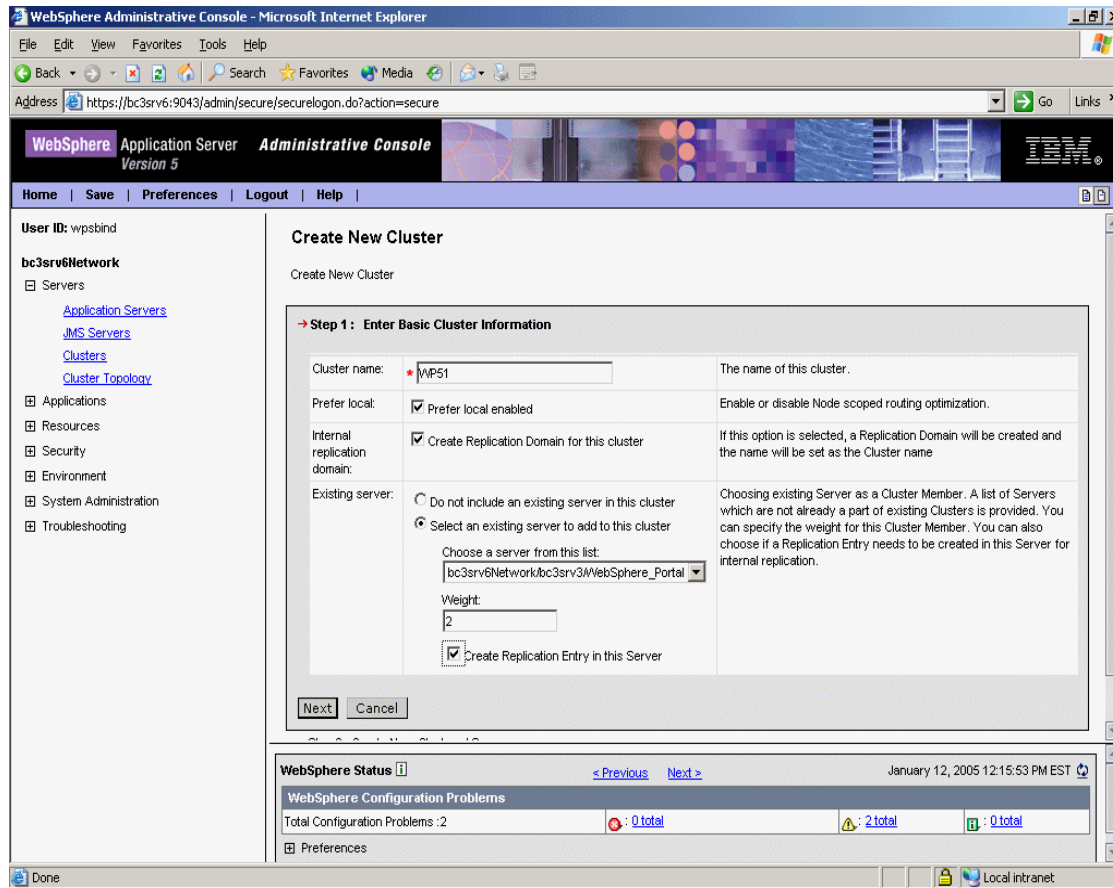


Figure 4-7 Create New Cluster

8. Click **Next**.

Follow these steps to create a cluster member on Portal02:

1. Enter the name of the new cluster member.

**Note:** Cluster members cannot have the same name. Because you already added bc3srv3 (node 1), its name by default is WebSphere\_Portal. Therefore, here you need to use a different name. In this example, we used WebSphere\_Portal\_2 for the name of the cluster member on bc3srv4 (node 2).

2. Select the appropriate node depending on the cluster topology you are using:
  - Horizontal: Server name of node 2
  - Vertical: Server name of node 1

In this example, select **bc3srv4**.

3. Select the appropriate HTTP port setting depending on the cluster topology you are using:
  - Horizontal: Clear the Generate Unique HTTP Ports option.
  - Vertical: Select the Generate Unique HTTP Ports option.

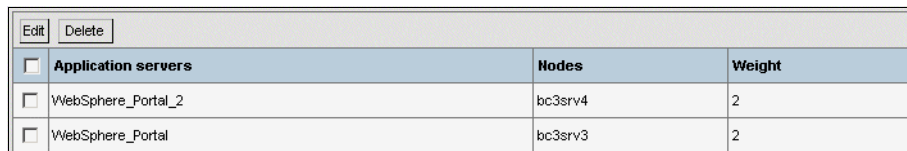
In this example, select the **Generate Unique HTTP Ports** option.

**Note:** This option will create a unique port number for the next cluster members. For example, the WebSphere Portal application uses port 9081 by default; if you select the above option, the second clustered server will use a different port than 9081. This is not required for a horizontal scaling with clusters unless you are creating a vertical clustered environment, that is, multiple clustered servers on a single WebSphere Portal machine.

For more information about horizontal and vertical scaling with clusters, see *IBM WebSphere Application Server V5.1 System Management and Configuration, WebSphere Handbook Series, SG24-6195*.

4. Select **Create Replication Domain for this cluster**.
5. Click **Apply**.

The cluster member will appear in the Application servers list on the bottom on the window, similar to the list shown in Figure 4-8.



<input type="checkbox"/>	Application servers	Nodes	Weight
<input type="checkbox"/>	WebSphere_Portal_2	bc3srv4	2
<input type="checkbox"/>	WebSphere_Portal	bc3srv3	2

Figure 4-8 The Application servers list

Notice at the bottom of the window that it lists your application servers that will become members of your cluster. We have no other cluster members to add. If you had additional cluster members to add, you would just repeat this process until all the cluster members are added.

6. Click **Next**. The Summary window opens.

7. Click **Finish** (Figure 4-9) to create the cluster.

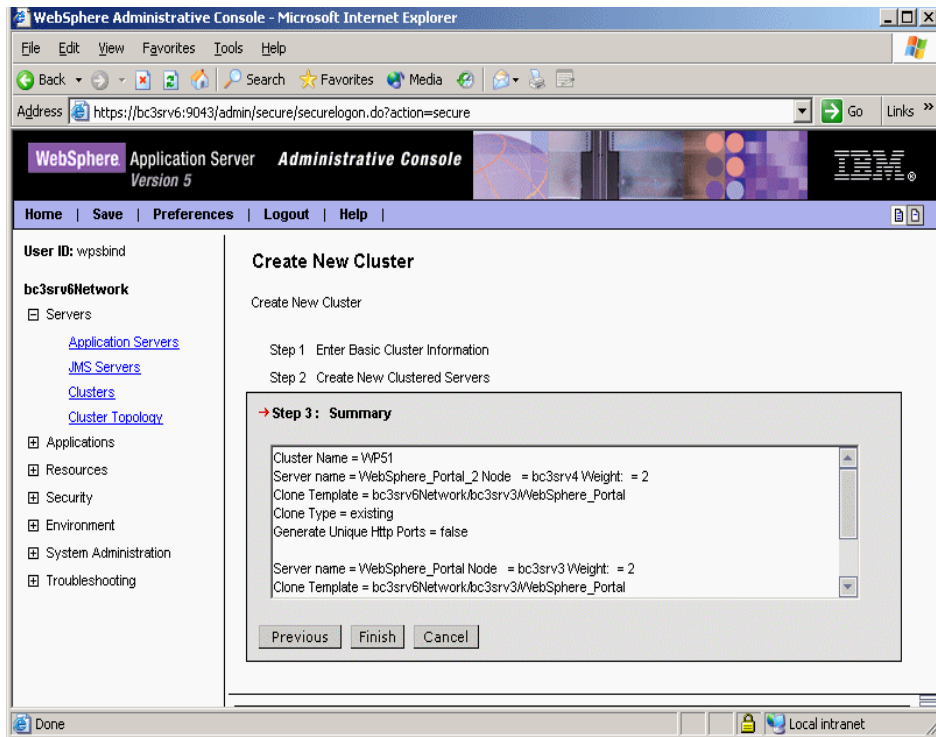


Figure 4-9 Create New Cluster

8. Save the changes to the master configuration.
9. Select the **Synchronize changes with Nodes** option and click **Save**.
10. After the configuration has been saved, navigate to **Servers** → **Cluster Topology** for a graphical view of the clusters topology (Figure 4-10 on page 161).

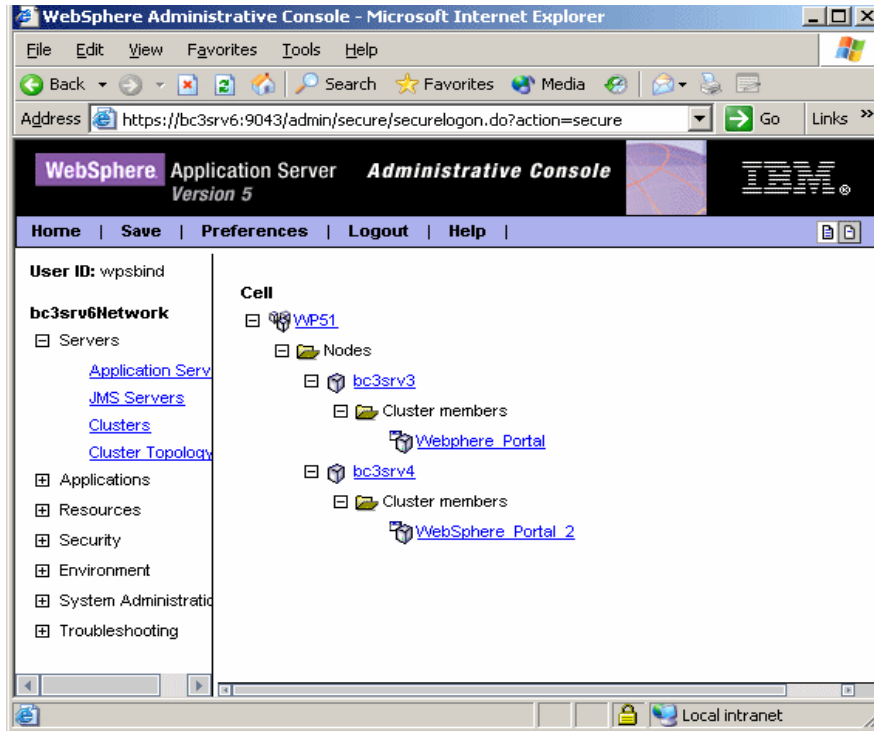


Figure 4-10 Cluster topology

#### 4.5.1 Editing the WebSphere Portal configuration on each node

To enable portlet deployment in the cluster, you must edit the following file on each WebSphere Portal node:

```
<wps_root>/shared/app/config/services/DeploymentService.properties
```

Set the `wps.appserver.name` property to the name of the cluster you defined previously, for example, `wps.appserver.name=WP51`.

Each node in the cluster should have the same synchronization settings to ensure consistency between the WebSphere Portal server configurations on each node. By default, automatic synchronization will occur between every node when a change is made to the configuration of the cell. This is checked for updates once per minute. To view the synchronization settings in the deployment manager administrative console, click **System Administration** → **Node Agents** and select the desired node agent.

The configuration on each WebSphere Portal node must be updated with the appropriate cluster member information. Use a text editor to open the following file on each WebSphere Portal node:

```
<wps_root>/config/wpconfig.properties
```

Ensure that the `ServerName` property is uncommented and specify appropriate values. For `ServerName`, make sure that this value still reflects the WebSphere Portal server name in the cluster specifically on the non-primary nodes, because the WebSphere Portal server name was changed when adding the server to the cluster, because no two servers can have the same name. The primary node, or first node added, was named `WebSphere_Portal` by default. The remaining non-primary nodes must be renamed with a unique server name for the cluster. For example on `bc3srv4` (node 2), use the following value:

```
ServerName=WebSphere_Portal_2
```

Update this property to match the cluster member name used to identify the node to the deployment manager. To determine the cluster member name, click **Servers** → **Cluster Topology** in the administrative console for the deployment manager and expand the cluster you are working with to view the cluster members.

## 4.5.2 Enabling dynamic caching

You must enable dynamic caching on the cluster member nodes to correctly validate the portal caches. If dynamic caching is not enabled, situations could arise where users have different views or different access rights, depending on which cluster node handles the user's request.

To enable dynamic caching on the first cluster member node (node 1), run the following command in the Windows `<wps_root>/config` directory:

```
WPSconfig.bat action-set-dynacache -DServerName=<ClusterMemberName>
-DReplicatorName=<ReplicatorName>
```

Where `<ClusterMemberName>` is the name of the cluster member you want to update with the replicator setting, and `<ReplicatorName>` is the name of the cluster member to be used as the replicator.

**Note:** We recommend that you create a replicator entry on each node. This will provide replicator failover. With this architecture, you will prevent the scenario where the node with the replicator goes down and thus prevents the other nodes from being able to start because they cannot access the replicator.



## Performance and failover considerations when using replicators

Because a replicator runs within an existing application server instance process, there is a performance impact from defining the replicator on a WebSphere Portal server instance. All replicators within a replication domain connect to each other, forming a network of replicators. WebSphere Application Server processes can connect to any replicator within a domain to receive data from other processes connected to any other replicator in the same domain. If a WebSphere Application Server process is connected to a replicator, and the replicator goes down, the process automatically attempts to reconnect to another replicator in the domain and recover any data missed while unconnected.

The more replicators you have defined in your environment, the better the replication failover capability will be. In the event that an application server process on which the replicator is defined is unavailable or goes down, there will be other replicators available to fill the gap. However, because additional replicators will impact the overall performance of your environment, you should carefully plan the total number of replicators needed.

For best performance, you can also provide a completely separate system running a dedicated application server instance as the replicator host. This dedicated application server instance need not have WebSphere Portal installed on it, although it must be in the same cell and in the same replication domain as the WebSphere Portal cluster.

For more information about using replicators, refer to the WebSphere Application Server documentation.

For example, to enable dynamic clustering on bc3srv3, node 1, use:

```
WPSconfig.bat action-set-dynacache -DServerName=WebSphere_Portal
-DReplicatorName=WebSphere_Portal
```

Then, enable dynamic caching for the second cluster member by repeating the previous step on node 2.

For horizontal or vertical scaling, consider the following information:

- ▶ Horizontal scaling: When running the action-set-dynacache task, ensure that you run the task on node 2.
- ▶ Vertical scaling: When running the action-set-dynacache task, ensure that you specify the name of the second cluster member with the ServerName property and run the task on node 1.

For example on bc3srv4, node 2, use:

```
WPSconfig.bat action-set-dynacache -DServerName=WebSphere_Portal_2
-DReplicatorName=WebSphere_Portal_2
```

### 4.5.3 Starting the cluster

This section describes the process of starting a cluster on WebSphere Application Server Network Deployment V5.0.

To start a cluster, complete the following steps:

1. In the administrative console, expand **Servers** and select **Clusters**.
2. Select the cluster name, **WP51** in our example. Click **Start**.

This process might take a while because it will start all applications under this cluster.

3. Check that the cluster members are started:
  - a. Expand **Servers** and select **Application Servers**.
  - b. Verify the status of the applications. You might have to click the **Refresh** icon to check the latest status of the applications, as shown in Figure 4-11.

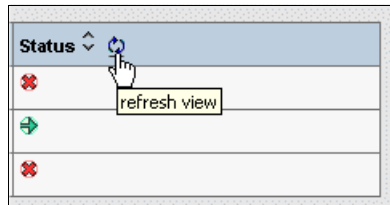


Figure 4-11 Click refresh view

4. Save your changes and resynchronize the nodes:
  - a. In the deployment manager administrative console, click **Save** on the taskbar, and save your administrative configuration.
  - b. Select **System Administration** → **Nodes**, select the node from the list, and click **Full Resynchronize**.

### 4.5.4 Regenerating the Web server plug-in

This section describes the procedure to regenerate the plug-in configuration on the deployment manager machine and transfer it to the remote HTTP server.

When you add a node to a deployment manager cell, you no longer use the plug-in configuration residing on the node machine. You have to work on the

plug-in configuration located in the Network Deployment machine. For this reason, all ports in use by the node applications must be added to the virtual host on the deployment manager machine, in this example, what we call the bc3srv6 machine.

The procedure that follows will add the remote HTTP server host name and port to the Host Alias list. This action will enable the user to access the clustered portal application. Complete the following steps:

1. In the deployment manager administrative console, expand **Environment** and select **Update Web Server Plugin**.
2. Click **OK** to regenerate the plug-in.
3. Edit the `<nd_root>/config/cells/plugin-cfg.xml` file and change any directory structure occurrences specific to the Network Deployment machine to match the directory structure used on the Web server. For example, references to `<install_dir>/WebSphere/DeploymentManager` would be replaced with `<install_dir>/WebSphere/AppServer`.
4. Copy the `plugin-cfg.xml` file located in the `/usr/WebSphere/DeploymentManager/config/cells` directory to the remote Web server machine:
  - a. The file should be copied to the `<was-root>/config/cells` directory in the Web server machine
  - b. Stop and start the Web server.
  - c. Restart all nodes in the cluster.

#### 4.5.5 Validating the cluster configuration

This section explains how to validate a cluster configuration on WebSphere Application Server Network Deployment V5.0.1.

You can validate a cluster configuration by testing the fail-over functionality.

In this example, the WebSphere Portal application is a cluster member residing in the bc3srv3 node, while WebSphere Portal 2 is the second cluster member and resides on the node bc3srv4.

If the WebSphere Portal application fails, all the incoming requests will be automatically handled by the application on Portal02 without errors or logging in again. To validate the cluster configuration, complete the following steps:

1. Start the cluster. Follow the steps in 4.5.3, “Starting the cluster” on page 164.

When you start the cluster, all application members of this cluster will be automatically started. Make sure that all applications are started before you continue.

2. Stop the clustered application on Portal02:
  - a. Open the bc3srv6 administrative console.
  - b. Log in using `wpsbind` and its password.
  - c. Expand **Servers** and select **Application Servers**.
  - d. Select the **WebSphere\_Portal\_2** application check box. Click **Stop**.
3. Log in to the WebSphere Portal application using `portaladmin` and its password:

```
http://<webserver_hostname>/wps/myportal
```

Currently, the remote HTTP server receives and uses the plug-in to send the incoming requests to the available clustered application; because we have stopped the application on node Portal02, we ensure that the application receiving and processing requests is the one residing on node bc3srv3.

4. Do *not* log off the WebSphere Portal application. Do *not* close the browser window.
5. Start the clustered application on bc3srv4, that is, WebSphere Portal 2.
6. Stop the application previously running, WebSphere Portal on the bc3srv3 node.
7. Go back to the WebSphere Portal browser window you opened in step 3.
8. Select the **Administration** link.

If the Administration page opens without interruption, the fail-over validation successfully completed.

## 4.6 Deploying portlets

In this section, we explain the deployment of portlets in a clustered environment.

When you install a new portlet on WebSphere Portal, the portlet information is stored into the WebSphere Portal database. In a cluster environment, the database is shared across the cluster members, meaning that all portlets installed on the bc3srv3 application will also be available on bc3srv4 and vice

versa. The deployment manager is responsible for keeping all cluster members synchronized.

Ensure that you have made the following changes before deploying a portlet:

- ▶ Change the application name in the `DeploymentService.properties` file. Refer to 4.5.3, “Starting the cluster” on page 164, step 4 on page 144.
- ▶ Add the Portal administrator user to the Console Users list:
  - a. Set the required authority for `portaladmin`.
  - b. After enabling security, you have to give the Portal administrator user the authority to deploy portlets in a clustered environment. This privilege can also be set for other users other than the Portal administrator.

In this chapter, we use `portaladmin` as the Portal administrator user. To set the privilege to this user, complete the following steps:

1. Open the deployment manager administrative console and log in as `portaladmin`:  
`http://<dm_hostname>:9090/admin`
2. Expand **System Administration** and select **Console Users**. The console user properties are displayed on the right.
3. Click **Add** to add a new user.
4. Enter `portaladmin` in the User field.
5. Select the **Administrator** role. Click **OK**.
6. Save changes to the master configuration.

To install a new portlet and synchronize the change across all WebSphere Portal nodes, complete the following steps:

1. Open the WebSphere Portal Web page.
2. Log in as the Portal administrator, in this example, `portaladmin`.
3. Click **Administration**.
4. Click the **Portlets** icon on the left. Select **Install**.
5. Browse for the portlet WAR file. Click **Next**.
6. You will be shown the portlets included in the WAR file. Click **Next**.
7. Click **Install**. Wait for the installation process to finish.

As soon as the portlet installation process is over, you will see a message similar to the one shown in Figure 4-12 on page 168.

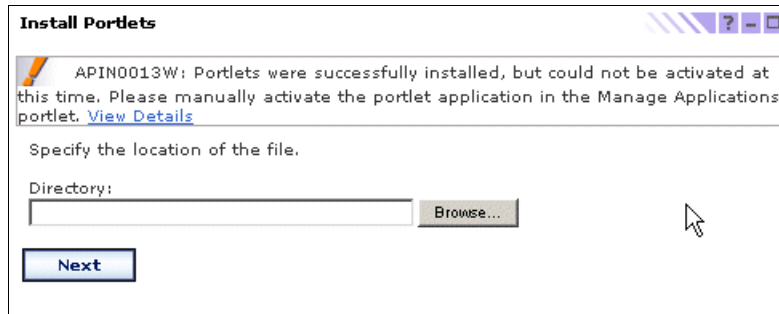


Figure 4-12 Could not activate the portlet

The auto-synchronization might not occur as soon as you install a new portlet; this will depend on how the auto-synchronization is configured on the deployment manager. We recommend that you manually synchronize all nodes just after installing or removing portlets.

When you install a portlet, an enterprise application is created under the deployment manager topology. This enterprise application must be started manually in order to be able to activate the portlet.

The following steps will guide you through this configuration:

1. Open the deployment manager administrative console:  
`http://<dm_hostname>:9090/admin`
2. Expand **System Administration** and select **Nodes**.
3. Select all the nodes that are members of the cluster. Click the **Synchronize** button. Check that you see a successful synchronization message for each node.
4. Expand **Applications** and select **Enterprise Applications**.
5. Select the enterprise application of your portlet. You can use the Filter to search applications. Click **Start**.
6. Open the Portal Administration page and log in as `portaladmin`:  
`http://<portal_hostname>/wps/myportal`
7. Click **Administration** at the top right of the window.
8. Click the **Portlets** icon on the left. Select **Manage Applications**.
9. Select the portlet application under the **Web modules** box. Then, select the portlet name you have just installed and click **Activate/Deactivate** to activate the portlet.

## 4.7 Deploying themes and skins

This section give you instructions about how to deploy a new theme and skin into the cluster. Themes and skins are stored in the WebSphere Portal enterprise application. In a cluster environment, you must export the Portal EAR file from deployment manager, update the EAR file with the new theme and skin directories, and import the enterprise application file back to the deployment manager cell.

To deploy themes and skins, complete the following steps:

1. Export the WebSphere Portal EAR file from the deployment manager:
  - a. On the deployment manager machine, go to the <nd-root>/bin directory.

- b. Enter the following command:

```
wsadmin.bat -user <was_user> -password <password>
$AdminApp export wps /tmp/wps_orig.ear
```

Where <was\_user> is the administrator ID, such as wpsbind and <password> is the administrator password.

- c. Enter **quit** to exit the portaladmin command line.

A wps\_orig.ear file will be created in the /tmp directory.

2. Expand the wps\_orig.ear file:
  - a. Create the directory /tmp/wps\_files.
  - b. Go to the <nd-root>/bin directory.
  - c. Expand the wps\_orig.ear file using the following command (make sure that you type the command on one line):

```
EARExpander.bat -ear /tmp/wps_orig.ear -operationDir /tmp/wps_files/
-operation expand
```

3. Copy the new theme and skin JSP files to the following locations:

- Theme: /tmp/wps\_files/wps.war/themes/<markup>/
- Skin: /tmp/wps\_files/wps.war/skins/<markup>/

4. Collapse the files back to an EAR file. Enter the following command:

```
/EARExpander.bat -ear /tmp/wps.ear -operationDir /tmp/wps_files/ -operation
collapse
```

5. Import the new wps.ear file to the deployment manager:

- a. Use **wsadmin** to import an EAR file:

```
/wsadmin.bat -user <was_user> -password <password>
wsadmin>$AdminApp install /tmp/wps.ear {-update -appname wps}
```

Wait for the message Application wps installed successfully.

- b. Save the changes to the master configuration, and then quit the wsadmin command line:

```
wsadmin>$AdminConfig save
wsadmin>quit
```

6. Add the new skin and theme to the Portal Administration page:
  - a. Log in to the Portal page using the Portal administrator user, such as portaladmin:  
`http://<hostname.com>/wps/myportal`
  - b. Click **Administration** and select **Portal User Interface**.
  - c. Select the **Themes and Skins** view.
  - d. Click **Add new skin**.
  - e. Enter the skin name and default locale title.
  - f. Enter the skin directory name. The directory name must match the one you have created in step 3 on page 169. Click **OK**.
  - g. Click **Add new theme**.
  - h. Enter the theme name in the Theme name and default locale title field.
  - i. Enter the theme directory name. The directory name must match the one you have created in step 3 on page 169.
  - j. Select the desired skins to be used in this theme. Click **OK**.

You are now ready to use the new theme and skin in WebSphere Portal.

## 4.8 Removing the WebSphere Portal node from deployment manager

In this section, we provide you with the instructions for removing a WebSphere Portal node from a deployment manager cell.

You might have to remove a WebSphere Portal node from a cell when:

- ▶ Upgrading the product level of WebSphere Portal components
- ▶ Installing an interim fix or fix pack on WebSphere Portal components, such as WebSphere Application Server
- ▶ Adding any configuration to the WebSphere Portal node
- ▶ Changing any existing configuration, such as LDAP or database properties

We *strongly* recommend that you increase the maximum heap size of the removeNode script. If you do not increase this value, you might run into a



java.lang.OutOfMemoryError error message during the remove process, and this will cause you problems when restoring the original configuration of the node.

To increase the maximum heap size of removeNode.bat, complete the following steps:

1. In the machine where the node you want to remove resides, go to the <was\_root>/bin directory.
2. Edit the removeNode.bat file.
3. In the Java command, include an additional line with the option:  
`-Xmx512 \`
4. Save and close the file.

### 4.8.1 Removing the node from the cell

You can choose to remove a node using the deployment manager administrative console or by using the removeNode script on the WebSphere Portal node machine.

To remove a node using the administration console, follow these steps:

1. Open the deployment manager administrative console:  
`http://<nd_hostname>:9090/admin`
2. Stop the cluster member:
  - a. Expand **Servers** and select the **Clusters** link.
  - b. Select the cluster name. The cluster properties window opens.
  - c. In the Additional Properties, select **Cluster members**.
  - d. Select the cluster member you want to remove. Click **Stop**.
3. Remove the node from the cell:
  - a. Expand **System Administration** and select the **Nodes** view.
  - b. Select the node name you want to remove. Click **Remove Node**.  
This task will take several minutes to finish. Wait until the task has completed.

### 4.8.2 Removing all enterprise application instances from bc3srv6

When the first WebSphere Portal node is added to the cell using the **addNode** command with the **-includeapps** option, all of the product's applications (portlets and servlets) and their associated resources (shared libraries, data source

providers, and variable definitions) are added to the deployment manager master configuration as well. Removing a WebSphere Portal node from the cell will cause the removal of its resources, but not its enterprise applications. Therefore, to completely remove the product from the deployment manager configuration, additional steps are needed to remove these items. If these items are not removed and the product is added back into the cell, there could be configuration conflicts.

**Note:** Do not perform these steps unless you have removed all instances of WebSphere Portal from the deployment manager.

Perform the following steps to completely remove WebSphere Portal from the deployment manager configuration:

1. There is a separate enterprise application definition for each portlet application, as well as several additional enterprise applications for other Portal services. All of these must be removed. In the deployment manager administrative console, navigate to the **Applications** → **Enterprise Applications** view.
2. Using the Filter, search for all enterprise applications using the string "`*(PA_*)`", because all portlet applications are deployed with a naming convention that includes this string. Apply the filter, and then select all enterprise application entries in the resulting table and click **Uninstall**.
3. The remaining enterprise applications must be identified and uninstalled manually. Use the following list as a reference:
  - `Presentation.war`
  - `RichTextEditor.war`
  - `SpreadsheetBlox.war`
  - `Pdmauthor`
  - `wmmApp`
  - `wps`
4. If you have deployed your own enterprise applications, these should be uninstalled as well.
5. In case of an installation or configuration problem, some of the WebSphere Portal resources might exist in the deployment manager configuration. It is a good idea to ensure that these are cleaned up before attempting to add a WebSphere Portal node back into the cell.

The following steps are only required if you had problems adding or removing a node to a cell:

1. Remove the JDBC providers. These JDBC providers are specified in the `wpconfig.properties` file by the values of the following properties:

- `JdbcProvider`
- `JcrJdbcProvider`
- `WcmJdbcProvider` (z/OS® only)

Note that by default these properties are set to use the same JDBC provider. To remove the JDBC providers, navigate to the **Resources** → **JDBC Providers** view and browse all nodes in the cell's scope looking for the JDBC provider definitions. Select the providers and click **Delete**.

2. Remove the shared library definitions. Navigate to the **Environment** → **Shared Libraries** view and browse all nodes in the cell's scope looking for the following shared library definitions:

- `CloudScapeLib`
- `WPSLib`
- `SDOMediatorsLib`
- `LotusWorkplaceLib`
- `JcrLib`
- `contentlib`
- `WcmLib`

Select the libraries and click **Delete**.

3. Remove the variable definitions. Navigate to the **Environment** → **Manage WebSphere Variables** view and browse all nodes in the cell's scope looking for the `<WPS_HOME>` variable. Select the variable and click **Delete**.

4. Remove the J2C authentication data entries associated with WebSphere Portal. Navigate to the **Security** → **JAAS Configuration** → **J2C Authentication Data Entries** view and browse the authentication data entries looking for the following aliases:

- `fbkDBAuth`
- `jcrDBAuth`
- `lmdBAuth`
- `node/BPEAuthDataAliasEmb_node_server1`
- `wmmDBAuth`
- `wpsDBAuth`

Select the entries and click **Delete**.

5. After all changes have been made, click **Save** from the last change to commit the changes to the cell's master configuration.



# WebSphere Portal: SUSE LINUX Enterprise Server 9 (SLES9) installation

This chapter describes the installation and configuration of IBM WebSphere Portal V5.1 for SUSE LINUX Enterprise Server 9 (SLES9) in a multi-tier environment.

The installation includes five machines, where:

- ▶ Machine one with Microsoft Windows Server 2003 has IBM HTTP Server V1.3.28.1.
- ▶ Machine two with SLES9 has:
  - WebSphere Application Server V5.1
  - WebSphere Portal V5.1
  - Cloudscape V5.1.60.12
  - IBM DB2 Administration Client V8.2
- ▶ Machine three with SLES9 has Lotus Domino Application Server 6.5.3.
- ▶ Machine four with SLES9 has IBM DB2 UDB Enterprise Server V8.2.

- ▶ Machine five with Windows 2000 Professional (desktop) has Lotus Domino Administrator 6.5.3.

This chapter is organized as follows:

- ▶ Overview of WebSphere Portal installation on Linux
- ▶ Preparing the machines for installation
- ▶ Installing WebSphere Portal V5.1
- ▶ Installing IBM HTTP Server V1.3.28.1
- ▶ Installing IBM DB2 V8.2
- ▶ Installing Lotus Domino V6.5.3

For our lab installation, Table 5-1 specifies the CDs that are required for the installation of the WebSphere Portal components in this chapter.

*Table 5-1 Installation CDs*

<b>Disk</b>	<b>Description</b>
CD Setup	WebSphere Portal V5.1 - Portal Install (Setup), V5.1
CD #1-1	WebSphere Business Integration Server Foundation for Windows V5.1
CD #1-3	WebSphere Business Integration Server Foundation for Linux/Intel, V5.1
CD #4-2	WebSphere Application Server V5.1 Archive Install for Linux
CD #5-2	Portal Server V5.1 Archive Install for Linux/UNIX
CD #5-3	Portal Server V5.1 Archive Install for Windows, AIX, Linux zSeries, Linux Intel
	Latest CD for IBM DB2 V8.2
CD #12-2	Lotus Domino Enterprise Server for Linux, V6.5.3
CD #12-6	Lotus Notes, Designer, Admin Clients for Windows, V6.5.3

## 5.1 Overview of WebSphere Portal installation on Linux

The WebSphere Portal V5.1 installation supports the following distributions of Linux:

- ▶ SUSE LINUX Enterprise Server (SLES) for Intel (x86) 8 2.4 Kernel with Service Pack 3
- ▶ SUSE LINUX Enterprise Server (SLES) for Intel (x86) 9
- ▶ SUSE LINUX Enterprise Server (SLES) for OS/390® 8 2.4 Kernel, 31-bit with Service Pack 3
- ▶ Red Hat Enterprise Linux Advanced Server 3.0 for Intel (x86), Update 1
- ▶ Red Hat Enterprise Linux Advanced Server 2.1 for Intel (x86), Update 3
- ▶ Red Hat Enterprise Linux Advanced Server 3.0 for iSeries and pSeries, Update 1
- ▶ Red Hat Enterprise Linux Advanced Server 3.0 for OS/390, Update 1

The sample scenario described in this chapter is more appropriate for a production environment, where you would have the Web server in tier 1, the WebSphere Application Server in tier 2, a robust LDAP directory in tier 3, and a database for WebSphere Portal authentication through the WebSphere Application Server in tier 4. The architecture of the sample scenario is shown in Figure 5-1 on page 178. If you prefer, you can install the LDAP and database servers on the same machine.

The sample scenario has been implemented on clean machines, having no previous versions of WebSphere Portal or its component products, such as WebSphere Application Server or a Web server.

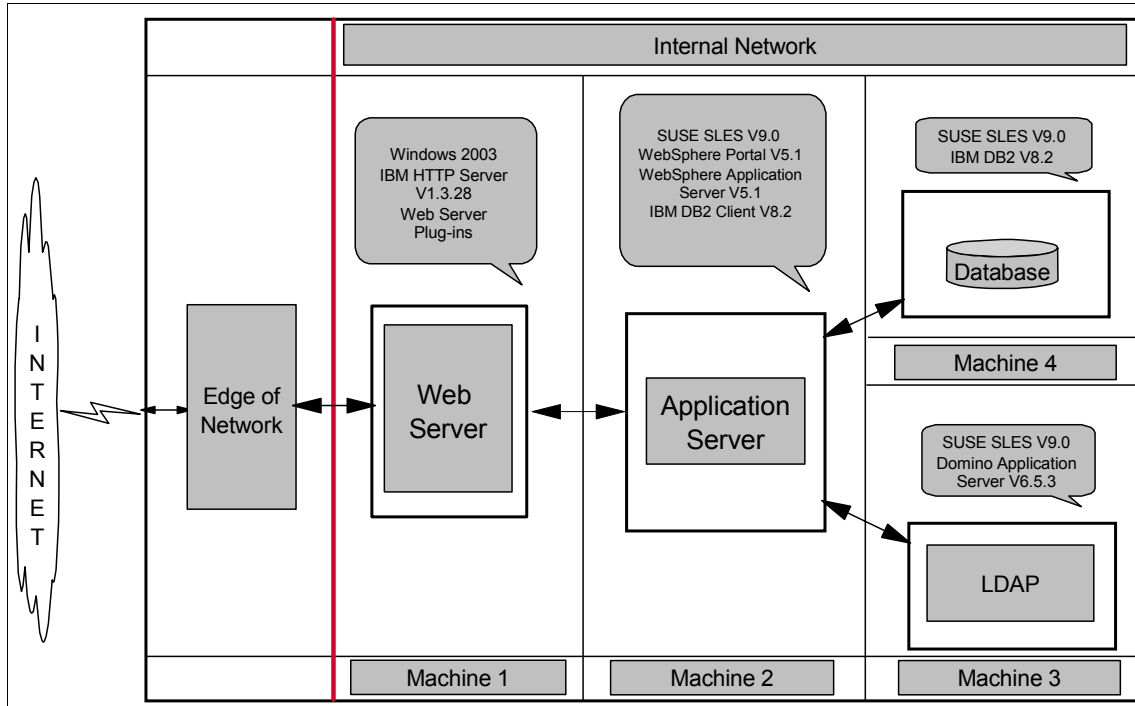


Figure 5-1 Architecture of the sample scenario for WebSphere Portal V5.1 on SLES V9.0

## 5.2 Preparing the machines for installation

Before beginning the installation, you should verify the following items:

- ▶ For information about the hardware requirements that should be fulfilled by the three machines and the software CDs required to implement this sample scenario, refer to the following *Information Center* and Table 5-1 on page 176:  
<http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/index.html>
- ▶ Any firewall products running on the machines have been disabled.
- ▶ Every machine has a static IP address.
- ▶ Each machine has a fully qualified host name; this is because after WebSphere Portal is configured to work with the Domino Directory, the WebSphere Application Server global security is enabled, and you must then type the fully qualified host name when accessing WebSphere Portal and the WebSphere Application Server administrative console. Table 5-2 on page 179 specifies the fully qualified host name of the three machines used in this sample scenario.



Table 5-2 Fully qualified host names of the machines

Machine	Fully qualified host name
1	bc1srv2.itso.ral.ibm.com
2	bc1srv3.itso.ral.ibm.com
3	bc1srv4.itso.ral.ibm.com
4	bc2srv1.itso.ral.ibm.com
5	ka6brlx.itso.ral.ibm.com

- ▶ Any anti-virus products running on the machines have been disabled.
- ▶ Network connectivity to the Internet is available.

## 5.3 Installing WebSphere Portal

This section describes the steps to perform the installation of WebSphere Portal V5.1 on machine 2. The installation program for WebSphere Portal V5.1 installs the following components under its full installation type:

- ▶ WebSphere Portal V5.1
- ▶ WebSphere Application Server V5.1
- ▶ Cloudscape V5.1.60.12

In this scenario, we are using a remote Web server. However, the IBM HTTP Server will not be installed here. After the installation, we verify the installation of each component.

To install WebSphere Portal V5.1, perform the following steps:

1. On machine 2, log in as the root user and start a terminal session.
2. Create the groups `mqm` and `mqbrkrs`. Create the user `mqm`. Add the user `mqm` and `root` to the groups `mqm` and `mqbrkrs`, as shown in Example 5-1 on page 180:
  - a. Create the group `mqm`:

```
groupadd mqm
```
  - b. Create the group `mqbrkrs`:

```
groupadd mqbrkrs
```
  - c. Create the user `mqm`, include it in the groups `mqm` and `mqbrkrs`, and create its home directory in `/home/mqm`:

```
useradd -G mqm,mqbrkrs -d /home/mqm mqm
```

d. Set mqm's password:

```
passwd mqm
```

e. Add root to the groups mqm and mqbrkrs:

```
usermod -G mqm,mqbrkrs root
```

*Example 5-1 Create groups and users*

---

```
groupadd mqm
groupadd mqbrkrs
useradd -G mqm,mqbrkrs -d /home/mqm mqm
usermod -G mqm,mqbrkrs root
```

---

3. Mount the Setup CD and start the WebSphere Portal installation wizard by running the following command:

```
#!/media/cdrom/install.sh
```

4. Select the language you would like to have for the installation and click **OK**, as shown in Figure 5-2. For our example, we selected **English**.



*Figure 5-2 Language for installation*

5. Click **Next** in the WebSphere Portal V5.1 Welcome window.

6. Read the license agreement, click **I accept the terms in the license agreement** to accept the WebSphere Portal V5.1 software license agreement, and click **Next**, as shown in Figure 5-3.

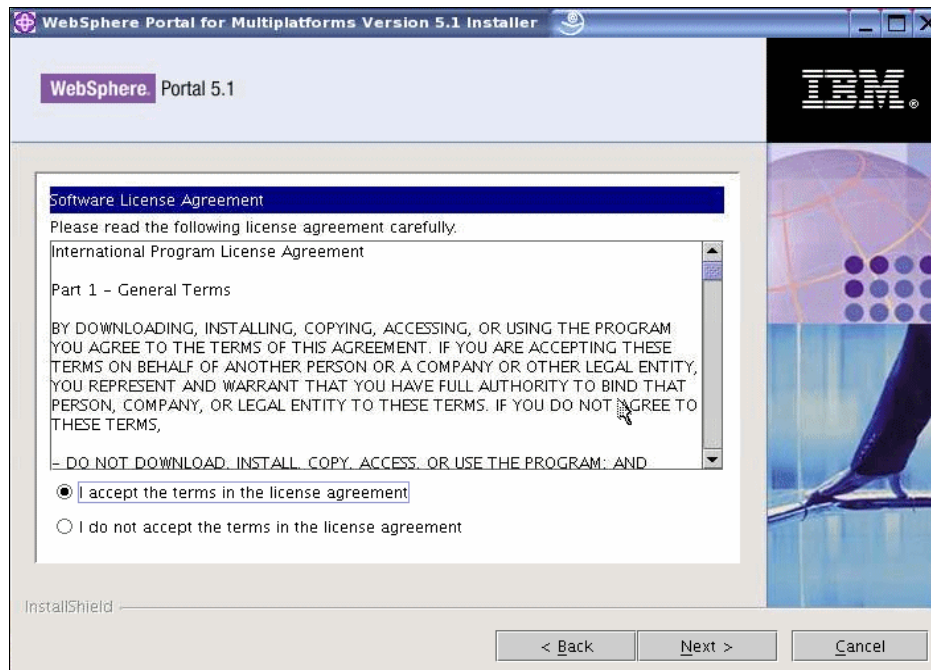


Figure 5-3 WebSphere Portal V5.1 License Agreement

7. For the installation type, WebSphere Portal V5.1 includes three different types of setup, as shown in Figure 5-4. Select **Full** and click **Next**.

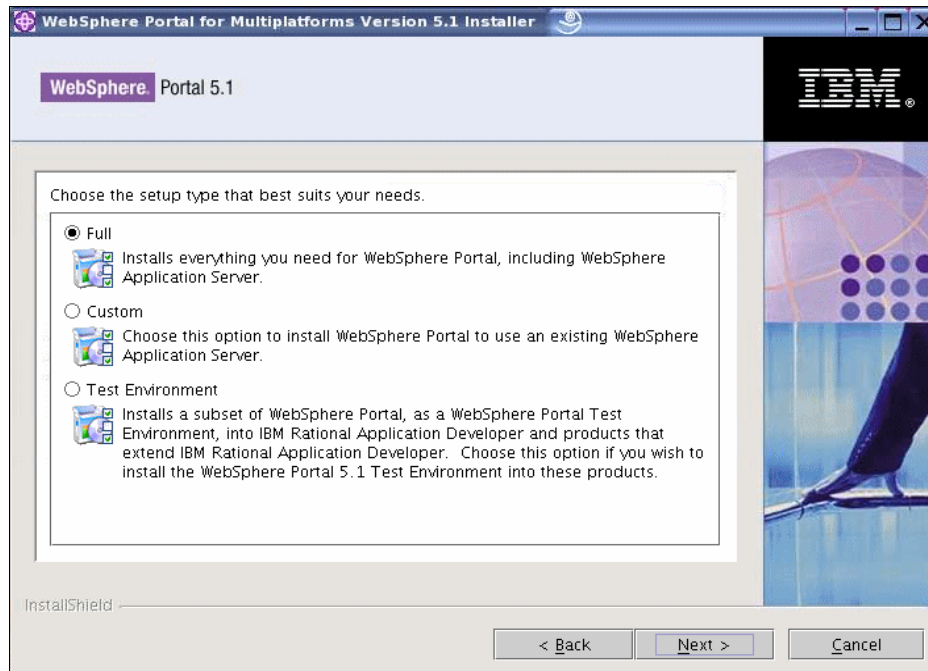


Figure 5-4 Installation type

8. The installer now checks for the required operating system and software prerequisites. Ignore the warning window shown in Figure 5-5 about the operating system and click **OK**.

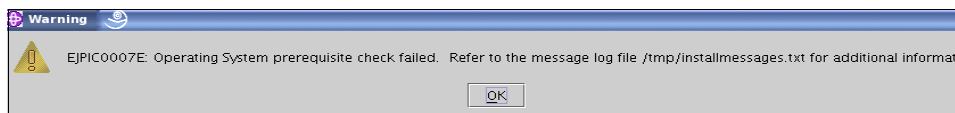


Figure 5-5 Operating System warning

9. For the WebSphere Application Server installation directory, select the default directory (see Figure 5-6) for the installation of WebSphere Application Server and click **Next**.

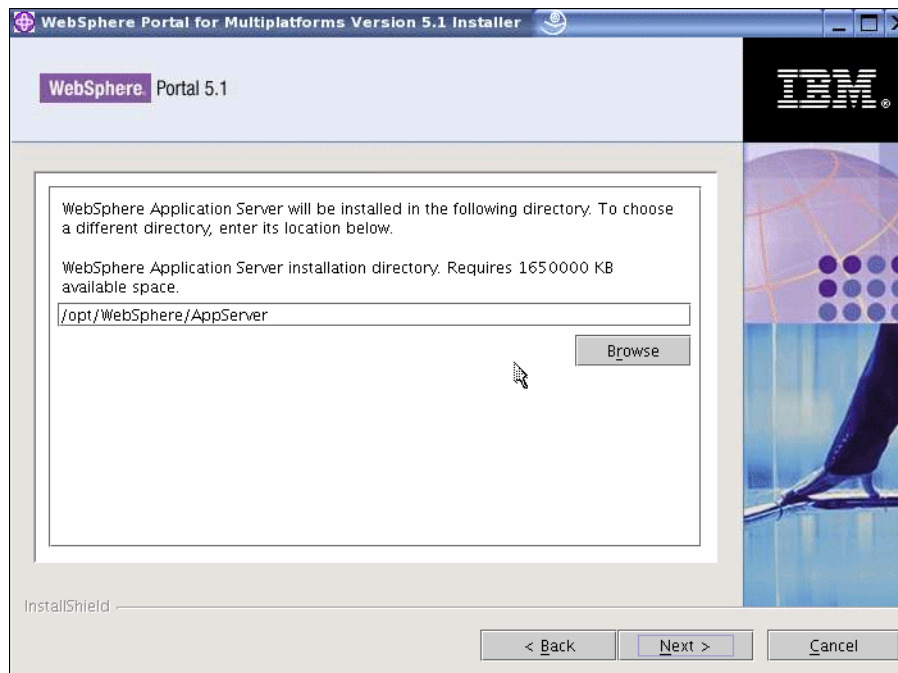


Figure 5-6 WebSphere Application Server installation directory

10. For the WebSphere Application Server Node name and hostname, enter the node name for the instance of WebSphere Application Server and the host name; here it is the fully qualified host name of machine 2. Click **Next**.

**Notes:**

- ▶ To avoid conflict with other instances of WebSphere Application Server in the network, it is best to have the node name as the host name of the machine on which WebSphere Application Server is being installed.
- ▶ Not entering the fully qualified host name might create problems if you would like to enable single sign-on (SSO) in the future.

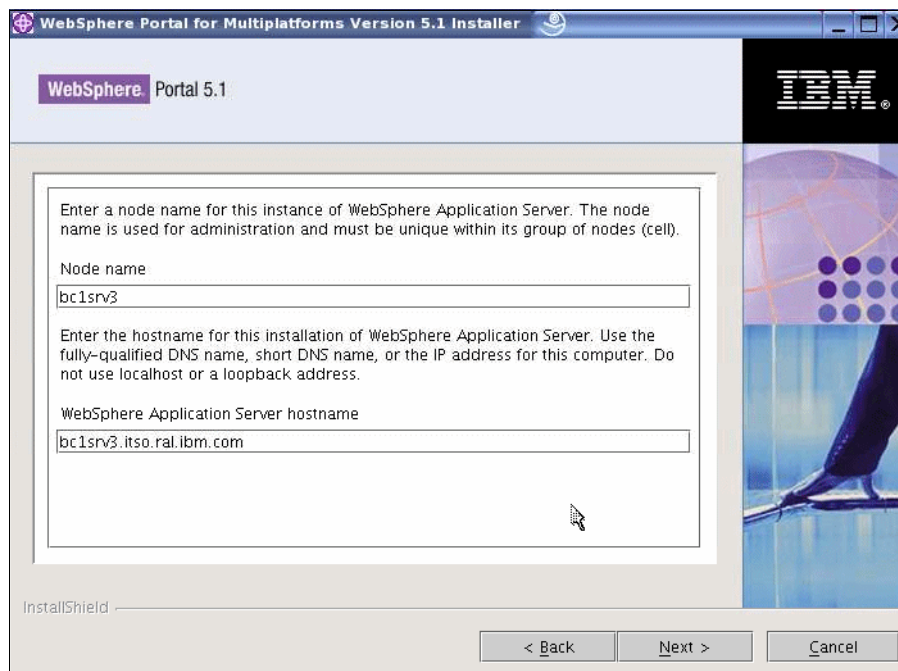


Figure 5-7 Node name and Hostname for WebSphere Application Server

11. For the WebSphere Portal installation directory, select the default directory, as shown in Figure 5-8. Click **Next**.

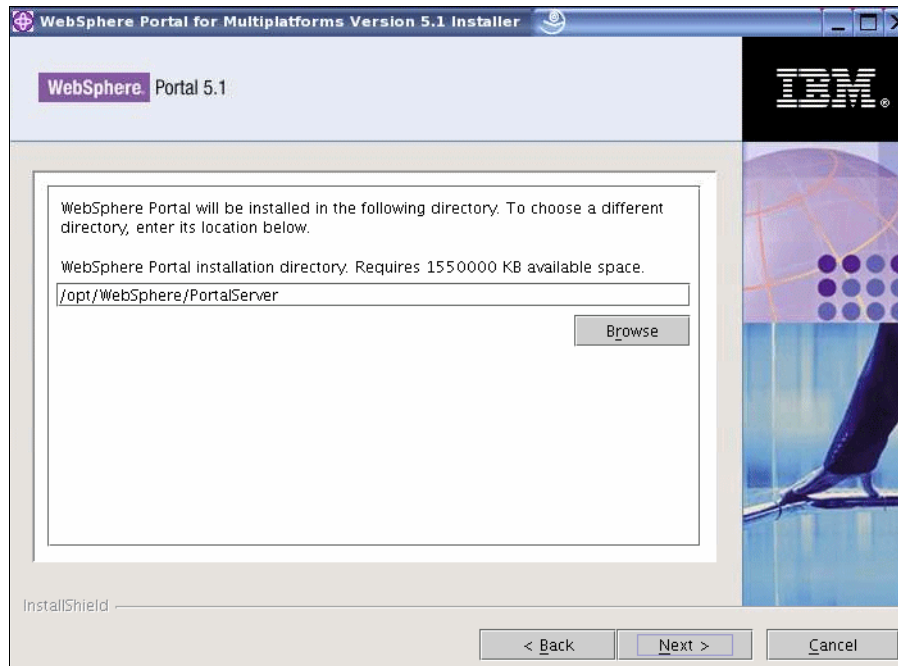


Figure 5-8 WebSphere Portal installation directory

12. For the WebSphere Portal administrator, enter the user name and password of the WebSphere Portal administrative user and click **Next**, as shown in Figure 5-9.

WebSphere Portal 5.1

Enter the WebSphere Portal administrative user and password. This user ID is used to access WebSphere Portal with administrator authority after installation. Note that this user ID is only used to log into WebSphere Portal and is not related to any user IDs used to access the operating system itself.

WebSphere Portal administrative user  
wpsadmin

WebSphere Portal administrative user password  
\*\*\*\*\*

Confirm password  
\*\*\*\*\*

< Back    Next >    Cancel

Figure 5-9 WebSphere Portal administrative user name and password



13. For the installation checklist, check the components (Figure 5-10) that will be installed and click **Next** to start the installation. You can click **Back** if you would like to make any changes.

**Important:** You will not be able to go back and make any changes to the installation after clicking **Next**.

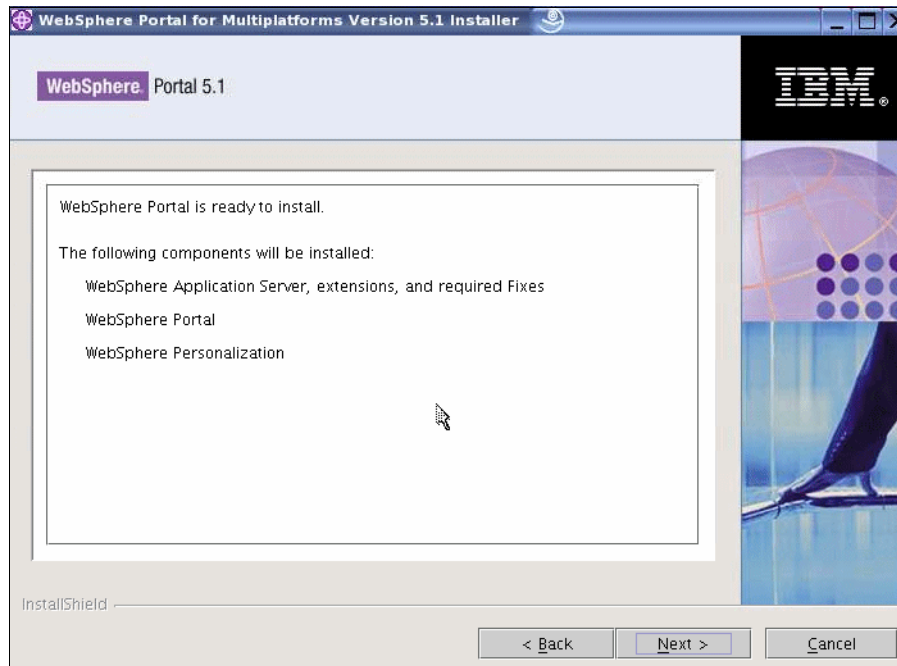


Figure 5-10 List of components selected for installation

14. Wait until the installation asks for another CD. Unmount the Setup CD and mount the CD #1-3. Click **Next** to start the WebSphere Application Server installation. Do the same with CD #4-2 to continue the installation.
15. After the installation completes, verify the installation of WebSphere Application Server with the following steps:
  - a. Open the WebSphere Application Server administrative console from a browser by entering the URL:  
`http://<hostname>:9090/admin`  
Where <hostname> is the fully qualified host name of machine 2, and 9090 is the port on which the WebSphere Application Server administrative server listens.

- b. Enter any user ID (for example, admin) and click **OK**. You will see a window similar to the one shown in Figure 5-11. This verifies the successful installation of WebSphere Application Server V5.1.

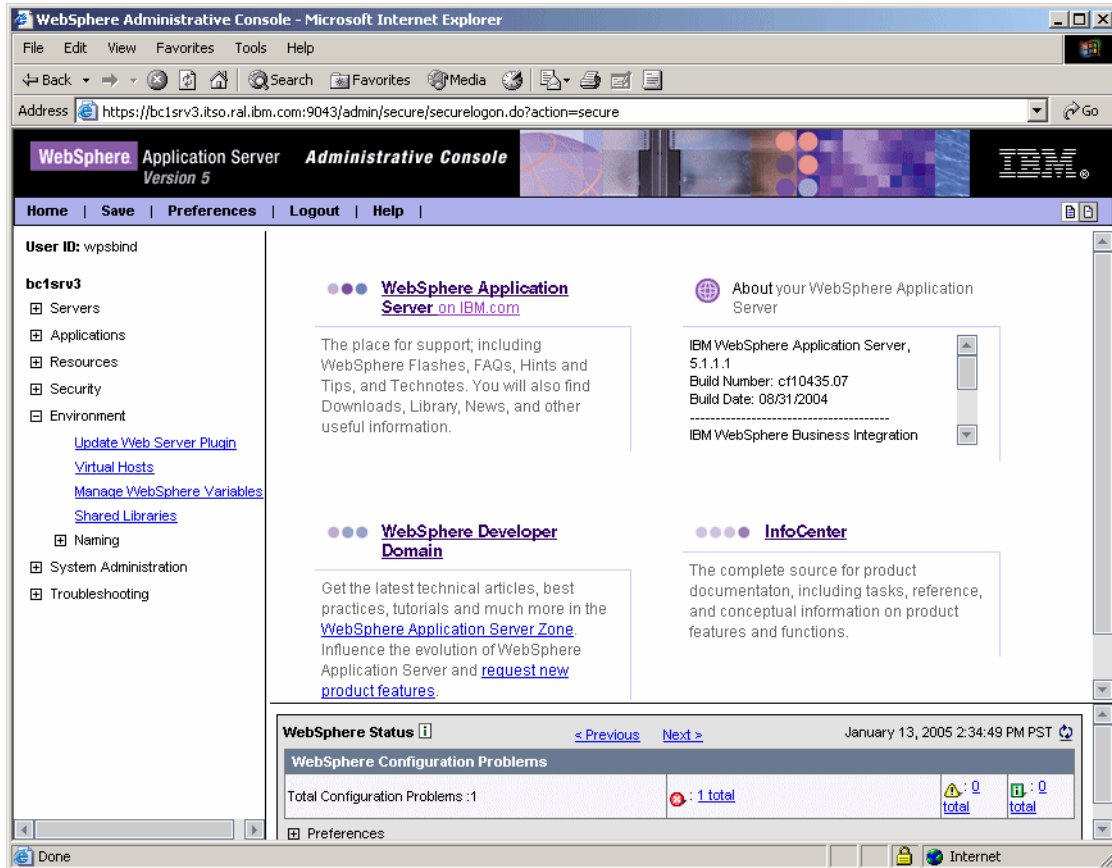


Figure 5-11 WebSphere Application Administrative Console

- c. You can double check the installation of WebSphere Application Server by accessing a Web application running on WebSphere Application Server. Enter the following URL in a browser:

http://<hostname>:9080/snoop

Where <hostname> is the fully qualified host name of machine 2, and 9080 is the port on which the Web applications running on WebSphere Application Server are presently listening.

16. After the WebSphere Application Server installation, unmount CD #4-2 and mount CD #5-2. Click **Next** to install WebSphere Portal. Do the same with CD #5-3 to continue the installation.

17. The final window tells you the result of the installation (successful or unsuccessful) and shows the list of components installed on the machine. Click **Finish** to stop and close the installation wizard.

18. Verify the installation of the WebSphere Portal with the following steps:

a. Access the following URL from a browser:

`http://<hostname>:9081/wps/porta1`

Where `<hostname>` is the fully qualified host name of machine 2, and 9081 is the port on which WebSphere Portal is presently listening.

b. Log in to the WebSphere Portal administrative window. Click **Log in** in the top right corner of the page and enter the user ID and password for the WebSphere Portal administrator. You created this user ID in step 12 on page 186. Click **Log in**. You will see a window similar to the one shown in Figure 5-12.

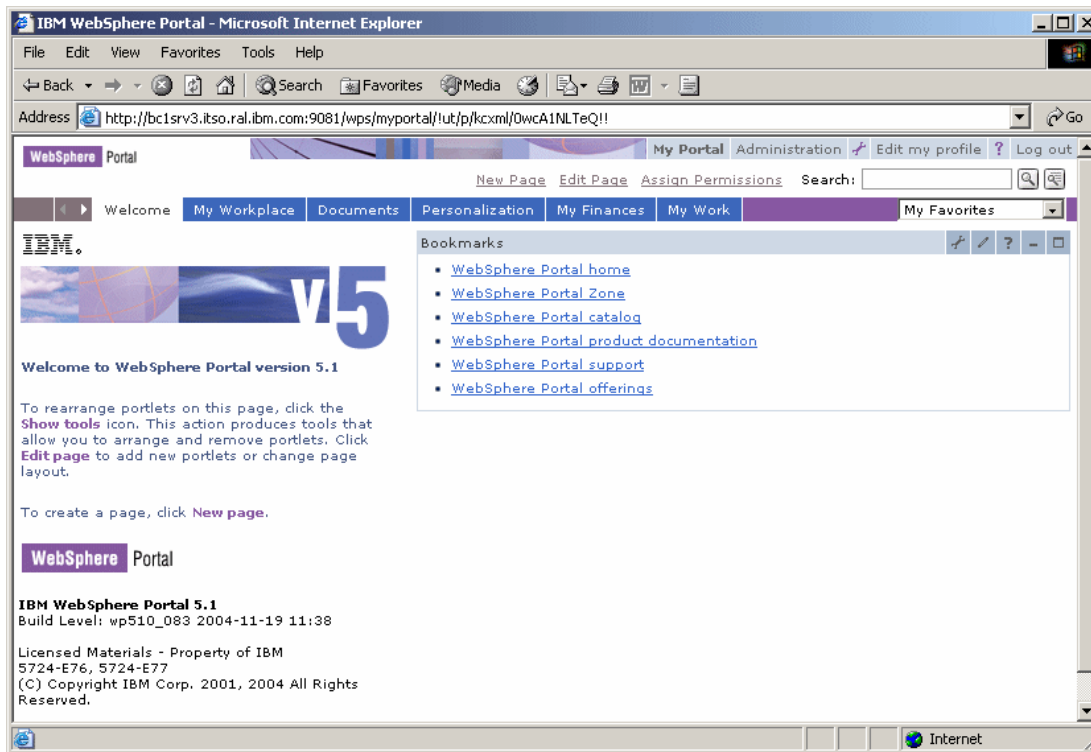


Figure 5-12 WebSphere Portal Welcome page for the Portal administrator

This completes the installation and verification of WebSphere Portal V5.1 on machine 2.

## 5.4 Installing IBM HTTP Server

This section describes the steps to perform the following tasks:

- ▶ Install IBM HTTP Server V1.3.28 on machine 1. This is done by using the WebSphere Application Server installation program in CD 1-1.
- ▶ Verify the installation of the IBM HTTP Server and the WebSphere Application Server plug-in.
- ▶ Configure WebSphere Portal to use the remote IBM HTTP Server as a Web server.

### 5.4.1 Installing IBM HTTP Server

To install the IBM HTTP Server, perform the following steps:

1. Insert CD #1-1 in machine 1 and start the installation wizard by running the file Install.exe from the directory <cd drive>/cd 1-1/was/win/WAS.
2. Click **Next** in the IBM HTTP Server Welcome window.
3. Click **I accept the terms in the license agreement** (Figure 5-13) to accept the IBM HTTP Server software license agreement and click **Next**.

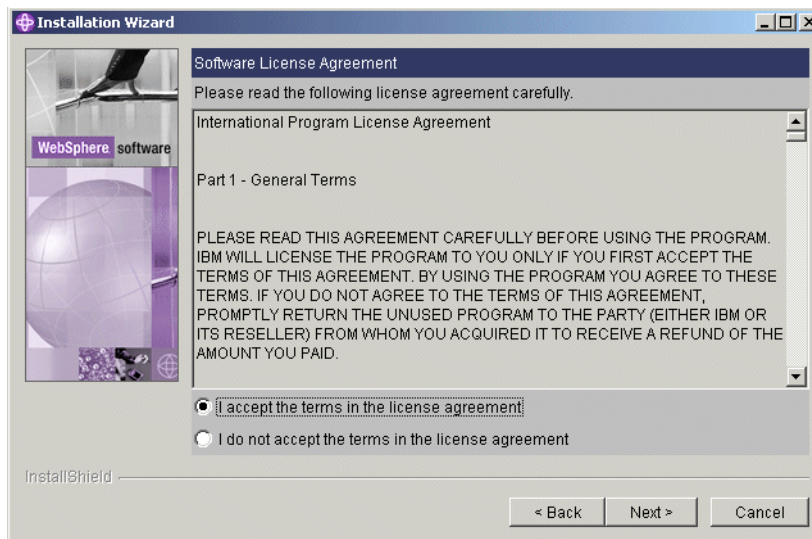


Figure 5-13 License Agreement for IBM HTTP Server

4. Select the **Custom** type to install only the IBM HTTP Server V1.3.28 and the plug-ins for the Web server, as shown in Figure 5-14. Click **Next**.

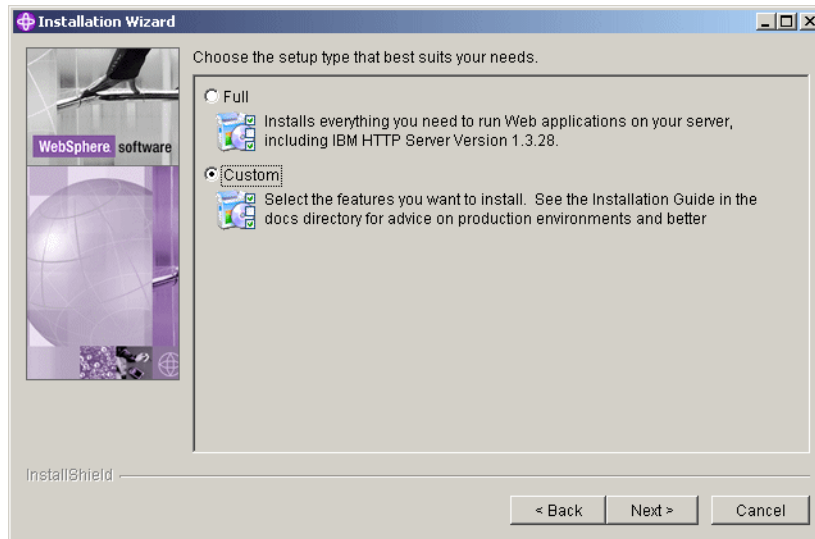


Figure 5-14 Installation type

5. Select the following features for installation (Figure 5-15):
- **IBM HTTP Server Version 1.3.28**
  - Web server plug-ins: **Plug-in for IBM HTTP Server v1.3**

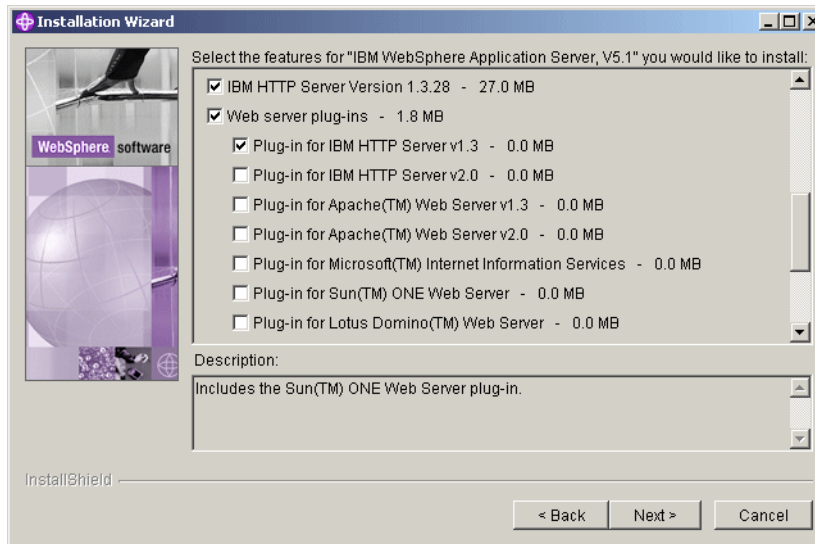


Figure 5-15 Components selected for installation

6. Enter the directory where you want to install the components or select the default (Figure 5-16) and click **Next**.

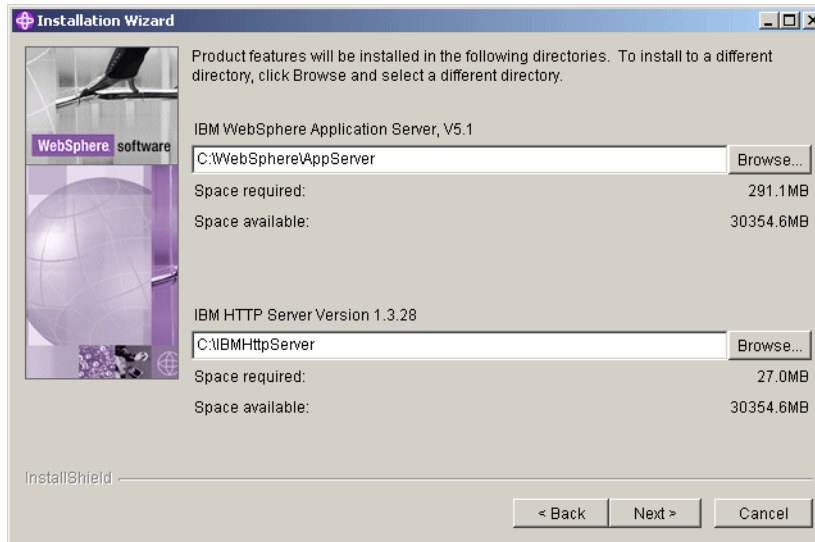


Figure 5-16 Installation directories

7. If you would want IBM HTTP Server to run as a service on your machine, select **Run IBM HTTP Server as a service**, enter the user ID and password of the IBM HTTP Server administrator, and click **Next**.



Figure 5-17 Run IBM HTTP Server as a service

**Note:** The window shown in Figure 5-18 opens only when the privileges required by the user have not been set before the installation started. Click **OK** if you get this window.

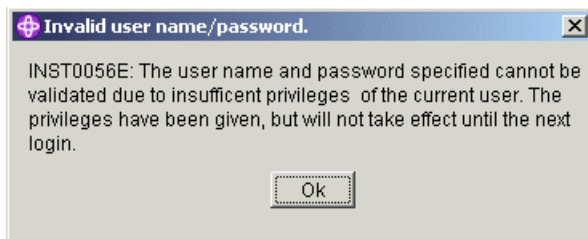


Figure 5-18 User rights set by the installation wizard

8. In the next window (Figure 5-19), verify the features being installed and click **Next**.

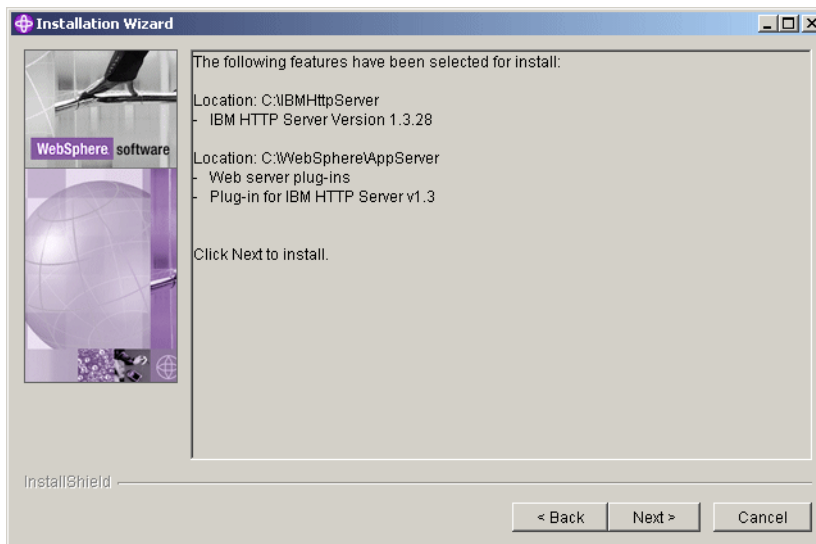


Figure 5-19 Components to be installed

9. After the installation, you can register the IBM HTTP Server by selecting the **Registration** option. Click **Next**.
10. In the next window, click **Finish** to stop and close the installation wizard.
11. Start IBM HTTP Server.



## 5.4.2 Verifying the installation

This section describes the steps to verify the installation of IBM HTTP Server and the WebSphere Application Server plug-in on machine 1.

### Verifying the installation of IBM HTTP Server

Complete the following steps to verify the IBM HTTP Server installation:

1. Open the Services window from Administrative Tools in Control Panel.
2. Check that IBM HTTP Server 1.3.28 is started. If not, start it.
3. Access the IBM HTTP Server 1.3.28 home page from a browser by entering the following URL:

`http://localhost`

You will see a page similar to the one shown in Figure 5-20.



Figure 5-20 IBM HTTP Server Welcome window

### Verifying the installation of WebSphere Application Server plug-in

To verify the installation of the WebSphere Application Server plug-in, check the Web server configuration; for example, if you install the IBM HTTP Server plug-in

on a machine running the Windows operating system, the plug-in installation updates the <ihs\_root>/conf/httpd.conf file, where <ihs\_root> is the root directory of the IBM HTTP Server installation, with the following lines:

```
LoadModule ibm_app_server_http_module
"C:\WebSphere\AppServer/bin/mod_ibm_app_server_http.dll"
WebSpherePluginConfig "C:\WebSphere\AppServer/config/cells/plugin-cfg.xml"
```

**Note:** If you have installed the IBM HTTP Server V2.0.47.1.1 instead of the V1.3.28.1, the httpd.conf file should be manually edited by replacing the above mentioned lines with the following lines:

```
LoadModule was_ap20_module
"C:\WebSphere\AppServer/bin/mod_was_ap20_http.dll"
WebSpherePluginConfig C:\WebSphere\AppServer/config/cells/plugin-cfg.xml"
```

### 5.4.3 Configuring WebSphere Portal with a remote IBM HTTP Server

This section describes the steps to configure WebSphere Portal V5.1 on machine 2 with IBM HTTP Server on machine 1.

#### ***On the WebSphere Portal V5.1 machine***

Complete the following steps:

1. Create a new default host alias:
  - a. Check the status of the WebSphere Application Server administrative server by using the following command from the <was\_root>/bin directory:

```
#!/serverStatus server1
```

If it is stopped, start it by using the following command:

```
./startServer server1
```
  - b. Open the WebSphere Application Server administrative console by entering the following URL in a browser:

```
http://<host_name>:9090/admin
```

Where <host\_name> is the fully qualified host name of the machine on which WebSphere Application Server was installed.
  - c. Log in to the administrative console, click **Environment** → **Virtual Hosts**, and then click **default\_host** in the list of Virtual Hosts.
  - d. Click **Host Aliases** under Additional Properties on the default\_host page.
  - e. Click **New** on the Host Aliases page.

- f. In the New page, under General Properties, as shown Figure 5-21, enter the following values:
- Host Name: The fully qualified host name of the machine where the HTTP server has been installed
  - Port: 80 or the port for which you would like to configure the HTTP server to accept client requests

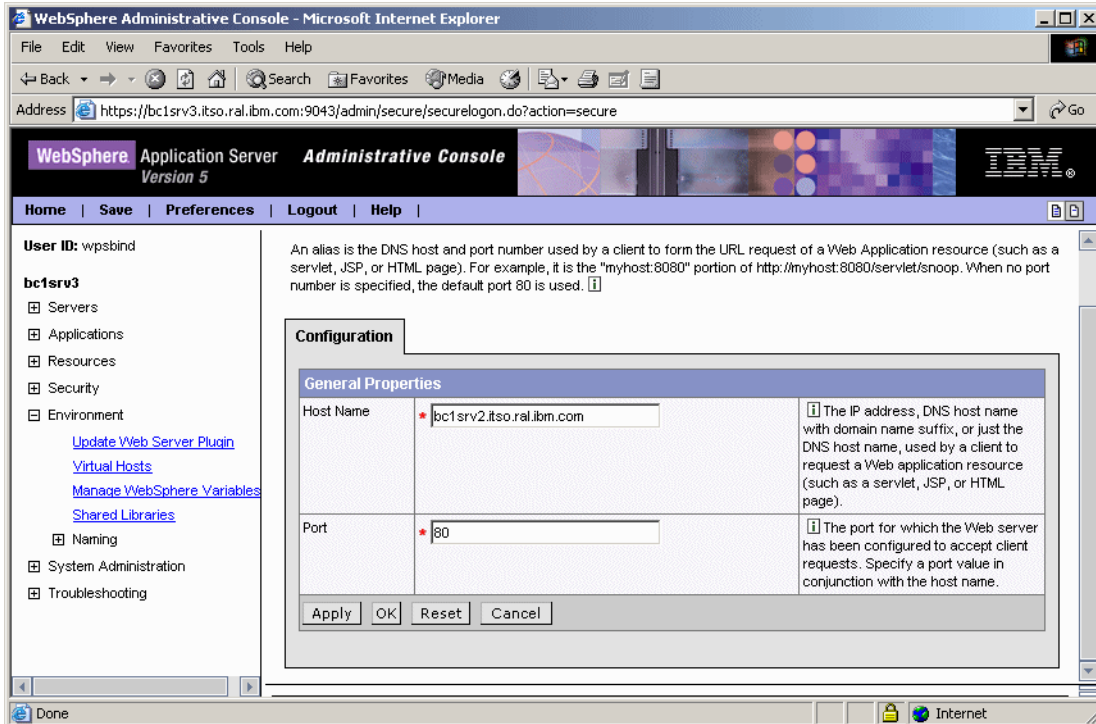


Figure 5-21 Adding the default host alias

- g. Click **OK** and then **Save** to save the changes to the configuration file.
2. Regenerate the Web server plug-in:
  - a. Update the Web server plug-in configuration by regenerating the plug-in for the Web server. Click **Environment** → **Update Web Server Plugin**.
  - b. Click **OK**.
  - c. Click **Logout** and then close the administrative console.

- d. Restart the WebSphere Application Server administration server by running the following command sequence from the <was\_root>/bin directory:

```
#!/stopServer server1
#!/startServer server1
```

- e. Check the status of WebSphere Portal by using the following command:

```
#!/serverStatus WebSphere_Portal
```

If it is stopped, start it by using the following command:

```
#!/startServer WebSphere_Portal
```

### ***On the IBM HTTP Server machine***

Complete the following steps:

1. Update the plug-in file, plugin-cfg.xml:
  - a. Copy the plug-in file from the directory <was\_root>/config/cells/ on the WebSphere Portal machine to the same directory in the HTTP server machine.
  - b. In the plug-in file, check the directory path for the logs and etc files.

For this scenario, because the Web server is on Windows and WebSphere Portal on Linux, the following changes have to be made:

```
/opt/WebSphere/AppServer/logs/ to <was_root>\AppServer\logs\
/opt/WebSphere/AppServer/etc/ to <was_root>\AppServer\etc\

```

**Note:** In any scenario where the Web server and WebSphere Portal are on machines with different operating systems, the above mentioned directory paths should be checked and edited to match the directory structure of the Web server's machine operating system.

2. Verify the plug-in configuration:
  - a. Restart the HTTP server.
  - b. Access the following URLs from a browser:

```
http://<hostname>/snoop
http://<hostname>/wps/portal
```

Where <hostname> is the fully qualified host name of the machine on which the Web server is installed.

**Note:** If the port entered in Figure 5-21 on page 197 is not 80, the port should be entered after the host name in the above URLs.

## 5.5 Installing IBM DB2 V8.2 for WebSphere Portal

By default, WebSphere Portal V5.1 uses Cloudscape, a built-in Java database installed automatically during the WebSphere Portal installation. Cloudscape is well-suited for basic portal environments, but it does not support a clustering environment or enabling of security in a database-only mode. Also, by default, WebSphere Portal uses the Cloudscape database as a custom user registry (CUR) for authentication under the database-only mode. There is always a gain in performance by moving to a database with greater scalability and capability.

In this scenario, we chose to use the latest version of IBM DB2 UDB Enterprise Server (V8.2) as the database for WebSphere Portal V5.1, because this is the supported DB2 version for SUSE LINUX Enterprise Server 9 (SLES9). This CD is not included in the WebSphere Portal V5.1 CDs list. For more information, see:

<http://www.ibm.com/db2/linux/validate>

The IBM DB2 UDB Enterprise Server will be installed on a remote machine, which would require us to install the IBM DB2 Administration Client on the WebSphere Portal machine so that WebSphere Portal can communicate with the IBM DB2 UDB Enterprise Server.

The process of implementing IBM DB2 V8.2 as the database for WebSphere Portal consists of the following steps:

- ▶ Installing IBM DB2 UDB Enterprise Server V8.2
- ▶ Installing of IBM DB2 Administration Client V8.2
- ▶ Migrating databases from Cloudscape to IBM DB2
- ▶ Configuring WebSphere Portal for IBM DB2
- ▶ Verifying that WebSphere Portal is using IBM DB2

### 5.5.1 Installing IBM DB2 UDB Enterprise Server V8.2

Complete the following instructions to install IBM DB2:

1. On machine 4, log in as the root user and start a terminal session.
2. Create the groups `dasadm1`, `db2grp1`, and `db2fgrp1`:

```
groupadd dasadm1
groupadd db2grp1
groupadd db2fgrp1
```

3. Mount the IBM DB2 V8.2 CD and start the installation wizard by running the following command from the `/media/cdrom` directory:

```
#!/db2setup
```

4. Click **Install Products** in the IBM DB2 Setup Launchpad.
5. Select **DB2 UDB Enterprise Server Edition** from the list of products available for installation, as shown in Figure 5-22, and click **Next**.

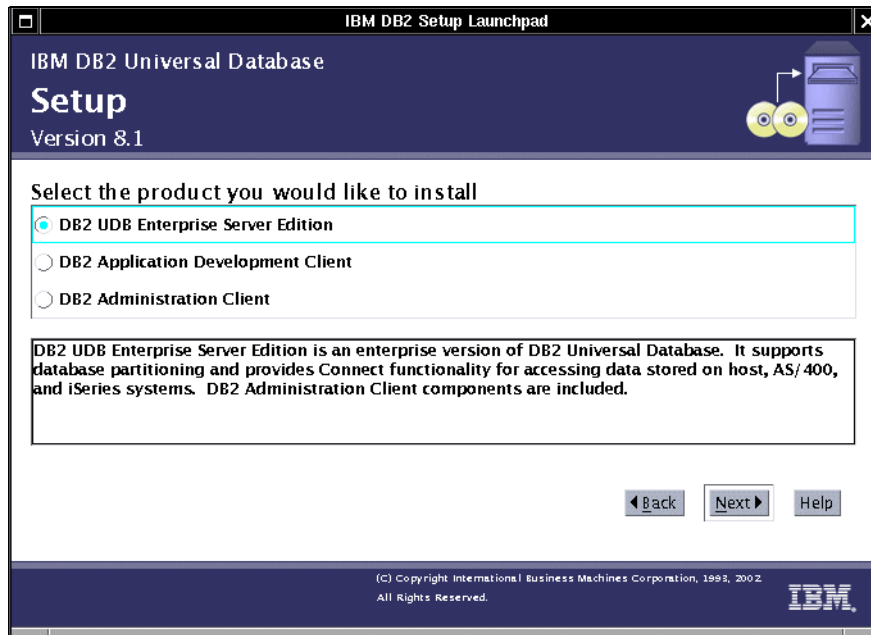


Figure 5-22 Choosing the product to be installed

6. Click **Next** in the DB2 Setup wizard welcome window.
7. Read the license agreement, select **Accept**, and click **Next**.
8. Select the **Typical** installation type and click **Next**.
9. Select **Install DB2 UDB Enterprise Server Edition on this computer** and click **Next**.
10. For the administrative user information, select **New user** to create a new user to administer the DB2 Administration Server. Retain the default values of:
  - User name: dasusr1
  - Group name: dasadm1
  - Home directory: /home/db2inst1Enter values for the Password and Confirm password fields and then click **Next**.
11. Select **Create a DB2 instance** to create a new DB2 instance and click **Next**.

**Note:** The name of the instance created here is the user name of the instance owner you create or provide under *Instance owner information*.

12. Select **Single-partition instance** and click **Next**.
13. For the instance owner information, select **New user** to create a new user to administer the instance created in step 10 on page 200. Retain the default values (Figure 5-23):
  - User name: db2inst1
  - Group name: db2grp1
  - Home directory: /home/db2inst1Enter values for the Password and Confirm password fields and then click **Next**.

**DB2 Setup wizard - DB2 UDB Enterprise Server Edition**

**Set user information for the DB2 instance owner**

Specify the instance-owning user information for the DB2 instance. DB2 will use this user to perform instance functions, and will store instance information in the user's home directory. The name of the instance will be the same as the user name. You can create a new user or use an existing one.

**New user**

User name: db2inst1

UID:   Use default UID

Group name: db2iadm1

CID:   Use default CID

Password:

Confirm password:

Home directory: /home/db2inst1

**Existing user**

User name:

For users of NIS or similar management systems:  
If the user information in your environment is managed remotely by NIS or a similar system, you must specify an existing user.

Figure 5-23 DB2 instance owner user information



14. For the fenced user information, select **New user** to create a new fenced user. Retain the default values shown in Figure 5-24. For example, we retained:

- User name: db2fenc1
- Group name: db2fgrp1
- Home directory: /home/db2fenc1

Enter values for the Password and Confirm password fields and then click **Next**.

The screenshot shows the 'DB2 Setup wizard - DB2 UDB Enterprise Server Edition' window. The left sidebar contains a list of steps from 1 to 13, with '9. Fenced user' selected. The main area is titled 'Set user information for the fenced user'. It contains a radio button for 'New user' which is selected. Below it are several input fields: 'User name' with 'db2fenc1', 'UID' (empty), 'Group name' with 'db2fgrp1', 'GID' (empty), 'Password' with '\*\*\*\*\*', 'Confirm password' with '\*\*\*\*\*', and 'Home directory' with '/home/db2fenc1'. There are two checked checkboxes: 'Use default UID' and 'Use default GID'. At the bottom, there is a 'User administration' box with the text 'Local users and groups will be created if necessary.' and a set of navigation buttons: 'Back', 'Next', 'Finish', 'Cancel', and 'Help'.

Figure 5-24 DB2 fenced user information

15. Click **Do not prepare the DB2 tools catalog on this computer** and click **Next**.

16. Enter the administration contact list information and click **Next**.



**Note:** Not selecting Enable Notification brings up a warning window. Ignore the warning and click **OK** to carry on with the installation.

17. Select **Defer this task until after installation is complete** and click **Next**.
18. Review the settings for the installation and click **Finish** to start the installation.
19. Wait for the installation to finish and then click the **Status report** tab to confirm that all the installed features have a status of Success. Click **Finish** to close the installation wizard.

## 5.5.2 Installing IBM DB2 Administration Client V8.2

This section describes the steps to install IBM DB2 Administration Client on machine 2. Complete the following steps:

1. Log in as the root user and start a terminal session.
2. Create the group db2grp1:  

```
groupadd db2grp1
```
3. Mount the IBM DB2 V8.2 CD and start the installation wizard by running the following command from the /media/cdrom directory:  

```
./db2setup
```
4. Click **Install Products**. In the next window, select **DB2 Administration Client**, and then click **Next**.
5. Click **Next** in the Welcome window.
6. Read the software license agreement, select **Accept**, and then click **Next**.
7. Select the **Typical** installation type and click **Next**.
8. Select **Create a DB2 instance** and click **Next**.
9. Retain the default values for DB2 instance owner, enter values for the Password and Confirm password fields, and click **Next**.
10. Review the settings for the installation and click **Finish** to start the installation.
11. Wait for the installation to finish and then click the **Status report** tab to confirm that all the installed features have a status of Success. Click **Finish** to close the installation wizard.

## 5.5.3 Creating remote databases

This section describes how to create the required databases for WebSphere Portal on a remote DB2 UDB Enterprise Server Edition machine. This example creates four databases, as shown in Table 5-3 on page 204.

Table 5-3 Databases and functions

Database	Function
WPS51	Used for WebSphere Portal and Member Manager (at a minimum) or to hold all data. Stores information about user customizations, such as pages, user profile, and login information.
JCR51	Used by Document Manager and Personalization components. Contains documents, Personalization rules, Personalization campaigns, and document library configuration information.
FDBK51	Used by Feedback components. Contains the information that is logged by your Web site for generating reports for analysis of site activity.
LM51	Used for LikeMinds data. Contains the recommendations to be displayed to users when their interactions with your Web site have been analyzed and predictions generated.

As you see in Table 5-3, WebSphere Portal and Member Manager information will be stored in the same database. You can create a different database for Member Manager. Or, you can simply create a single database to hold all the data required by Document Manager, Personalization, Feedback, and LikeMinds components. In this example, we separate all the information into different databases except for the Member Manager information.

To create the databases, log in as the DB2 instance owner and run the appropriate **db2** commands to create and update database configurations, as shown in Example 5-2.

*Example 5-2 Create and update database configurations*

```
#su - db2inst1
>db2 "create database wps51 using codeset UTF-8 territory us"
>db2 "update database configuration for wps51 using applheapsz 16384
app_ctl_heap_sz 8192"
>db2 "update database configuration for wps51 using stmtheap 60000"
>db2 "update database configuration for wps51 using locklist 400"
>db2 "update database configuration for wps51 using indexrec RESTART"
>db2 "update database configuration for wps51 using logfilsiz 1000"
>db2 "update database configuration for wps51 using logprimary 12"
>db2 "update database configuration for wps51 using logsecond 10"
>db2set DB2_RR_TO_RS=yes
>db2set DB2_EVALUNCOMMITTED=YES
>db2set DB2_INLIST_TO_NLJN=YES

>db2 "create database fdbk51 using codeset UTF-8 territory us collate using
identity"
>db2 "update database configuration for fdbk51 using applheapsz 5120"
```

```

>db2 "update database configuration for fdbk51 using logfilsiz 4096"
>db2 "update database configuration for fdbk51 using logprimary 4"
>db2 "update database configuration for fdbk51 using logsecond 25"

>db2 "create database lm51 using codeset UTF-8 territory us"

>db2 "create database jcr51 using codeset UTF-8 territory us"
>db2 "update database manager configuration using QUERY_HEAP_SZ 32768"
>db2 "update database manager configuration using UDF_MEM_SZ 7000"
>db2 "update database manager configuration using SHEAPTHRES 10000"
>db2 "update database manager configuration using MAXAGENTS 500"
>db2 "update database manager configuration using DFT_MON_TIMESTAMP OFF"
>db2 "update database configuration for jcr51 using LOCKTIMEOUT 30"
>db2 "update database configuration for jcr51 using LOCKLIST 1000"
>db2 "update database configuration for jcr51 using STMTHEAP 16384"
>db2 "update database configuration for jcr51 using AVG_APPLS 5"
>db2 "update database configuration for jcr51 using SORTHEAP 256"
>db2 "update database configuration for jcr51 using LOGPRIMARY 10"
>db2 "update database configuration for jcr51 using LOGFILSIZ 1000"
>db2 "update database configuration for jcr51 using LOGSECOND 20"
>db2 "update database configuration for jcr51 using LOGBUFSZ 32"
>db2 "update database configuration for jcr51 using MAXAPPLS 200"
>db2 "update database configuration for jcr51 using APPLHEAPSZ 4096"
>db2 "update database configuration for jcr51 using DFT_QUERYOPT 2"
>db2 "update database configuration for jcr51 using DBHEAP 2400"
>db2 "update database configuration for jcr51 using APP_CTL_HEAP_SZ 20000"
>db2 "connect to jcr51"
>db2 "create bufferpool ICMLSFREQBP4 SIZE 1000 PAGESIZE 4 K"
>db2 "create bufferpool ICMLSVOLATILEBP4 SIZE 8000 PAGESIZE 4 K"
>db2 "create bufferpool ICMLSMMAINBP32 SIZE 8000 PAGESIZE 32 K"
>db2 "create bufferpool CMBMAIN4 SIZE 1000 PAGESIZE 4 K"
>db2 "create bufferpool OBJECTPOOL SIZE 2000 PAGESIZE 32 K"
>db2 "create bufferpool OBJPARTSPOOL SIZE 200 PAGESIZE 32 K"
>db2 "create bufferpool SMSPPOOL SIZE 500 PAGESIZE 4 K"
>db2 "create bufferpool PARTSPOOL SIZE 100 PAGESIZE 32 K"
>db2 "create bufferpool BLOBPOOL SIZE 1000 PAGESIZE 32 K"
>db2 "create bufferpool REPLICAPPOOL SIZE 1000 PAGESIZE 32 K"
>db2 "create bufferpool TRACKINGPOOL SIZE 250 PAGESIZE 4 K"
>db2 "create bufferpool VALIDATEPOOL SIZE 500 PAGESIZE 32 K"
>db2 "create regular tablespace ICMLFQ32 PAGESIZE 32 K managed by system using
('ICMLFQ32') bufferpool ICMLSMMAINBP32"
>db2 "create regular tablespace ICMLNF32 PAGESIZE 32 K managed by system using
('ICMLNF32') bufferpool ICMLSMMAINBP32"
>db2 "create regular tablespace ICMVFQ04 PAGESIZE 4 K managed by system using
('ICMVQ04') bufferpool ICMLSVOLATILEBP4"
>db2 "create regular tablespace ICMSFQ04 PAGESIZE 4 K managed by system using
('ICMSFQ04') bufferpool ICMLSFREQBP4"
>db2 "create regular tablespace CMBINV04 PAGESIZE 4 K managed by system using
('CMBINV04') bufferpool CMBMAIN4"

```

```
>db2 "create system temporary tablespace ICMLSSYSTSPACE32 PAGESIZE 32 K managed
by system using ('icmlssystspace32') bufferpool ICMLSMAINBP32"
>db2 "create system temporary tablespace ICMLSSYSTSPACE4 PAGESIZE 4 K managed
by system using ('icmlssystspace4') bufferpool ICMLSVOLATILEBP4"
>db2 "create regular tablespace OBJECTS PAGESIZE 32 K managed by system using
('objects') bufferpool OBJECTPOOL"
>db2 "create regular tablespace OBJPARTS PAGESIZE 32 K managed by system using
('objparts') bufferpool OBJPARTSPOOL"
>db2 "create regular tablespace SMS PAGESIZE 4 K managed by system using
('sms') bufferpool SMSPOOL"
>db2 "create regular tablespace BLOBS PAGESIZE 32 K managed by system using
('blobs') bufferpool BLOBPOOL"
>db2 "create regular tablespace REPLICAS PAGESIZE 32 K managed by system using
('replicas') bufferpool REPLICAPool"
>db2 "create regular tablespace TRACKING PAGESIZE 4 K managed by system using
('tracking') bufferpool TRACKINGPOOL"
>db2 "create regular tablespace VALIDATEITM PAGESIZE 32 K managed by system
using ('validateitm') bufferpool VALIDATEPOOL"
>db2 disconnect jcr51
>db2 TERMINATE
```

---

## 5.5.4 Configuring the connection to remote databases

In order for WebSphere Portal to be able to connect to the databases, you need to perform the configurations provided in this section.

### Changes to perform on the DB2 server machine

Complete the following steps:

1. Edit the `/etc/services` file. Check if the DB2 service port numbers were included in this file, and if they were not, add them:

```
DB2_db2inst1 60000/tcp # DB2 connection service port
DB2_db2inst1_1 60001/tcp # DB2 interrupt service port
```

2. Save and close the file.
3. Log in as the DB2 instance owner and update the Service Name configuration (mandatory):

```
#su - db2inst1
>db2 UPDATE DBM CFG USING svcename DB2_db2inst1
```

Where `DB2_db2inst1` is the service name added into `services` file above.

4. Set the `DB2COMM` variable to use TCP/IP:

```
>db2set DB2COMM=TCPIP
```

## Changes to perform on the DB2 client machine

Complete the following steps:

1. Edit the `/etc/services` file and add the DB2 connection service port:

```
DB2_db2inst1 60000/tcp # DB2 connection service port
```

**Note:** You *must* use the same service name and port number on the DB2 server machine.

2. Save and close the file.
3. Set the `DB2COMM` variable to use TCP/IP:

```
#su - db2inst1
>db2set DB2COMM=TCPIP
```

4. Catalog the node name with the DB2 server IP address and service name:

```
#su - db2inst1
>db2 catalog tcpip node <node_name> remote <db2_srv_hn> server <svce_name>
```

Where `<node_name>` is the value you define for the DB2 server machine remote information (in our case, `WPSNODE`), `<db2_srv_hn>` is the fully qualified host name or IP address of the DB2 server machine, and `<svce_name>` is the value you specified in step 1, as shown Example 5-3.

### Example 5-3 Catalog node

---

```
>db2 catalog tcpip node WPSNODE remote bc1srv3.itso.ral.ibm.com server
DB2_db2inst1
```

---

5. Catalog the remote databases created on the DB2 server machine using the node name that was created in step 4:

```
#su - db2inst1
>db2 catalog database <wps_db_name as wps_db_name_alias> at node
<node_name>
>db2 catalog database <jcr_db_name as jcr_db_name_alias> at node
<node_name>
>db2 catalog database <fdbk_db_name as fdbk_db_name_alias> at node
<node_name>
>db2 catalog database <lm_db_name as lm_db_name_alias> at node <node_name>
```

Where `<wps_db_name>`, `<jcr_db_name>`, `<fdbk_db_name>`, and `<lm_db_name>` are the WebSphere Portal and WebSphere Content Publishing database names you used when you created them on the database server machine, and `<wps_db_name_alias>`, `<jcr_db_name_alias>`, `<fdbk_db_name_alias>`, and `<lm_db_name_alias>` are the values that you are defining for database names on the client machine. See Example 5-4 on page 208.

#### Example 5-4 Catalog database

---

```
>db2 catalog database WPS51 as WPS51N at node WPSNODE
>db2 catalog database JCR51 as JCR51N at node WPSNODE
>db2 catalog database FDBK51 as FDBK51N at node WPSNODE
>db2 catalog database LM51 as LM51N at node WPSNODE
```

---

**Note:** If you have created a database for Member Manager separate from WebSphere Portal, you will also have to catalog the Member Manager database.

#### 6. Test the connection to the databases:

```
#su - db2inst1
>db2 connect to <wps_db_name_alias> user <db2_user> using <db2_password>
>db2 connect to <jcr_db_name_alias> user <db2_user> using <db2_password>
>db2 connect to <fdbk_db_name_alias> user <db2_user> using <db2_password>
>db2 connect to <lm_db_name_alias> user <db2_user> using <db2_password>
```

Where <wps\_db\_name\_alias>, <jcr\_db\_name\_alias>, <fdbk\_db\_name\_alias>, and <lm\_db\_name\_alias> are the values you used in step 5 on page 207, <db2\_user> is the user name with rights to connect to this database, and <db2\_password> is the password for the user name you are defining. See Example 5-5.

#### Example 5-5 Connecting to the databases

---

```
>db2 connect to WPS51N user db2inst1 using password
>db2 connect to JCR51N user db2inst1 using password
>db2 connect to FDBK51N user db2inst1 using password
>db2 connect to LM51N user db2inst1 using password
```

---

### 5.5.5 Transferring data to the DB2 database

WebSphere Portal V5.1 uses Cloudscape as a database, so it does not require you to have DB2 UDB Enterprise Server, Oracle, Informix®, or SQL Server up and running at this time.

For a production architecture, we *strongly* recommend moving all data to a powerful database server such as DB2 UDB Enterprise Server Edition.

In WebSphere Portal V5.1, all configuration information is stored in the wpconfig.properties file. In order to have the database transferred, we need to change the appropriate values into this file and use the WPSconfig script to

execute the changes. Complete the following steps to move the data from Cloudscape to the DB2 UDB Enterprise Server database in machine 2:

1. Give the user root the privilege to run DB2 commands:
  - a. Edit the setupCmdLine.sh file in the <was\_root>/bin/ directory:

```
#cd /opt/WebSphere/AppServer/bin
#vi setupCmdLine.sh
```

(You can use vi or a graphic file editor.)
  - b. Add the following lines:

```
if [-f /home/db2inst1/sqllib/db2profile]; then
. /home/db2inst1/sqllib/db2profile;
fi
```
  - c. Save and close the file.
  - d. Do the same with the file .bash\_profile in the /root directory. If the file does not exist, create it.
  - e. Close all the shells and open a new one.
  - f. Verify that you can now perform **db2** commands by running **db21 eve1** at the command line.
2. Go to the <wp-root>/config directory and back up the wpconfig.properties file, where <wp-root> is the root directory for WebSphere Portal. For example, on Linux, the default install path is /opt/WebSphere/PortalServer.
3. Edit the WebSphere Portal configuration wpconfig.properties file and change the parameters, as shown in Table 5-4.

**Note:** For a detailed description of each property, refer to the section “Configuring WebSphere Portal for DB2” in *WebSphere Portal V5.1 Information Center*, available at:

<http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/index.html>

Table 5-4 DB2 configuration values for the wpconfig.properties file

Property	Value
DbSafeMode	false
DbType	db2
WpsDbName	wps51n
DbDriver	COM.ibm.db2.jdbc.app.DB2Driver
DbDriverDs	COM.ibm.db2.jdbc.DB2XADataSource

Property	Value
JdbcProvider	wpsdbJDBC
DbUrl	jdbc:db2:wps51n
DbUser	db2inst1
DbPassword	<type_db2inst1_password>
DbLibrary	/home/db2inst1/sql1lib/java/db2java.zip
WpsDsName	wpsdbDS
WpsXDbName	wps5TCP
WpsDbNode	wpsNode
JcrDbName	jcr51n
JcrDbUser	db2inst1
JcrDbPassword	<type_db2inst1_password>
JcrDbUrl	jdbc:db2:jcr51n
JcrXDbName	jcrdbTCP
JcrDbNode	wpsNode
JcrJdbcProvider	jcrdbJDBC
JcrDsName	JCRDS
JcrGeneratedDLLPath	\${WpsInstallLocation}/jcr/config/dynamic
JcrBinaryValueFileDir	\${WpsInstallLocation}/jcr/binaryValues
PznDbNode	wpsNode
FeedbackXDbName	fdbk5TCP
FeedbackDbName	fdbk51n
FeedbackDbUser	db2inst1
FeedbackDbPassword	<type_db2inst1_password>
FeedbackDbUrl	jdbc:db2:fdbk51n
LikemindsXDbName	1mdb5TCP



Property	Value
LikemindsDbName	lm51n
LikemindsDbUser	db2inst1
LikemindsDbPassword	<type_db2inst1_password>
LikemindsDbUrl	jdbc:db2:lm51n
WmmDsName	wmmDS
WmmAppName	wmmApp
WmmDbName	wps51n
WmmDbUser	db2inst1
WmmDbPassword	<type_db2inst1_password>
WmmDbUrl	jdbc:db2:wps51n

4. Save and close the wpconfig.properties file.

**Important:** For security reasons, we recommend that you leave each password field blank in the wpconfig.properties file. While running the following tasks, you can specify the password on the command line with the following syntax:

```
WPSconfig.sh <task_name> -D<password_property_key=password_value>
```

Where <task\_name> is the task that you will perform, and each password property should have one -D prefix and one key-value pair. In the following steps, we assume that all passwords are removed from the wpconfig.properties file.

5. You can test the database connections to Portal databases using the following commands:

```
#!/WPSconfig.sh validate-database-connection-wps \
-DDbPassword=<type_db2inst1_password>
#!/WPSconfig.sh validate-database-connection-jcr \
-DJcrDbPassword=<type_db2inst1_password>
#!/WPSconfig.sh validate-database-connection-feedback \
-DFeedbackDbPassword=<type_db2inst1_password>
#!/WPSconfig.sh validate-database-connection-likeminds \
-DLikemindsDbPassword=<type_db2inst1_password>
#!/WPSconfig.sh validate-database-connection-wmm \
-DWmmDbPassword=<type_db2inst1_password>
#!/WPSconfig.sh validate-database-driver
```

Wait for the BUILD SUCCESSFUL message. If you get a BUILD FAILED message, verify the wpconfig.properties file and validate again.

6. Perform the following command to transfer databases:

```
#!/WPSconfig.sh database-transfer \ -DDbPassword=<type_db2inst1_password> \
-DJcrDbPassword=<type_db2inst1_password> \
-DFeedbackDbPassword=<type_db2inst1_password> \
-DLikemindsDbPassword=<type_db2inst1_password> \
-DWmmDbPassword=<type_db2inst1_password>
```

This task will take several minutes to complete, and you will see a BUILD SUCCESSFUL message when it finishes. If you get a BUILD FAILED message, verify the wpconfig.properties file and repeat this step again.

7. Perform reorg check to improve performance:

```
#db2 connect to <db_name> user <user_name> using <password>
#db2 reorgchk update statistics on table all
#db2 terminate
#db2rbind <db_name> -l db2rbind.out -u <user_name> -p <password>
```

Where <db\_name> is your Portal database name, <user\_name> is the user you chose to be the owner of this database, and <password> is the DB2 user name password.

**Note:** You must perform these steps for each WebSphere Portal database, for example, WPS51N, JCR51N, FDBK51N, and LM51N.

8. Restart WebSphere Application Server, server1.
9. Open the WebSphere Application Server administrative console, and then perform the following steps:
  - a. Expand **Servers** and click **Application Servers**. Then, select **WebSphere\_Portal** from the list of Application Servers.
  - b. Select **Process Definition** from the list of Additional Properties.
  - c. Select **Java Virtual Machine** from the list of Additional Properties.
  - d. Add the value of DbLibrary in wpconfig.properties into the Classpath field. In this example, we add /home/db2inst1/sqllib/java/db2java.zip into the Classpath field. Click **Apply** and click **Save**.
  - e. Expand **Resources** from the left-side menu, and then click **JDBC Providers**. In this example, there are four JDBC providers:
    - feedbackJDBC
    - jcrdbJDBC
    - likemindsJDBC
    - wpsdbJDBC

- f. Select **wpsdbJDBC**, and then click **Data Sources** from Additional Properties. For each data source, click the **Test Connection** button to verify the database connections.
- g. Repeat the previous step for other JDBC providers.

10. Start WebSphere Portal.

11. Test the WebSphere Portal configuration by typing the following URL in a browser. You can log in as wpsadmin:

```
http://<wps_hostname>:9081/wps/portal
```

Where <wps\_hostname> is the fully qualified host name for WebSphere Portal, and <ihs\_hostname> is the fully qualified host name for the IBM HTTP Server machine.

In our example:

```
http://bc1srv3.itso.ra1.ibm.com:9081/wps/portal
```

**Important:** If you disabled port 9081 and enabled the remote HTTP port number, as in 6.4.4, “Disabling access to port 9081 (optional)” on page 277, you must enter the following URL:

```
http://<ihs_hostname>/wps/portal
```

In our example:

```
http://bc1srv2.itso.ra1.ibm.com/wps/portal
```

## 5.6 Installing Lotus Domino 6.5.3

At this stage of the implementation of the sample scenario, WebSphere Portal is using IBM DB2 V8.1 as the custom user registry (CUR) for authentication. However, it can be configured to use an LDAP directory to store user information and to authenticate users and do the authentication in database and LDAP mode.

This section describes the following topics:

- ▶ Installing Lotus Domino Enterprise Server 6.5.3
- ▶ Installing Domino Administrator
- ▶ Configuring the Domino server settings
- ▶ Configuring Domino Administrator
- ▶ Setting up Domino Directory
- ▶ Configuring WebSphere Portal for Domino Directory
- ▶ Verifying the LDAP configuration

## 5.6.1 Installing Lotus Domino Enterprise Server 6.5.3

In this section, you install Lotus Domino Enterprise Server. For more details, see *Lotus Domino 6 for Linux*, SG24-6835.

Complete the following steps:

1. On machine 3, log in as the root user and start a terminal session.
2. Create a user and a group for the Domino administration on Linux:

```
groupadd ldapadm
useradd -g ldapadm -d /local/notesdata ldapadmin
passwd ldapadmin (Enter a password for this user)
```

3. Mount CD #12-2 and start the text-based installation wizard by running the following command:

```
#./media/cdrom/linux/install
```

4. You will see a window similar to the one shown in Figure 5-25. Press Tab.

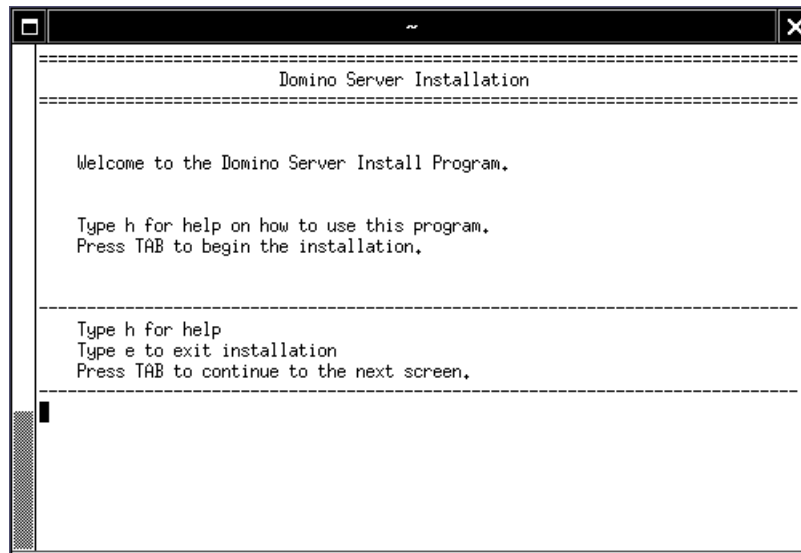


Figure 5-25 Welcome window for the installation of Lotus Domino Server

5. In the next window (Domino Server release notes), press Tab.
6. Press Tab again to see the License Agreement.
7. The Lotus Domino/Notes software agreement opens. Press Enter to go through the agreement until you see the window shown in Figure 5-26 on page 215. Press Tab.

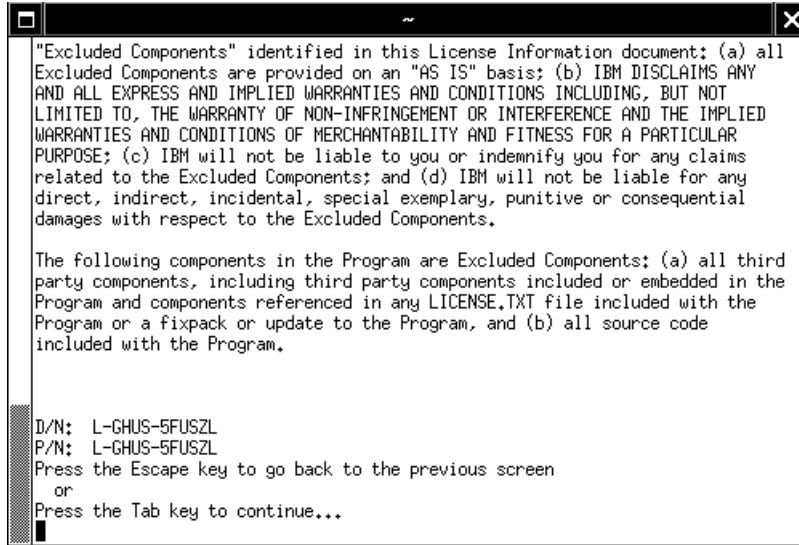


Figure 5-26 Lotus Domino/Notes software agreement

8. If the setting for the license agreement is not Yes, as shown in Figure 5-27, press the spacebar and then press Tab; otherwise, just press Tab.

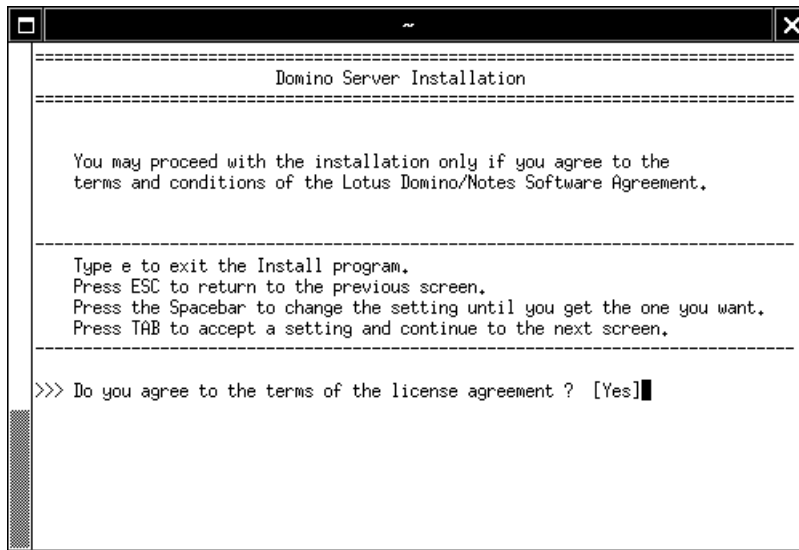


Figure 5-27 License Software Agreement

9. For the data directories, select the No option, pressing the spacebar, and then press Tab. See Figure 5-28 on page 216.

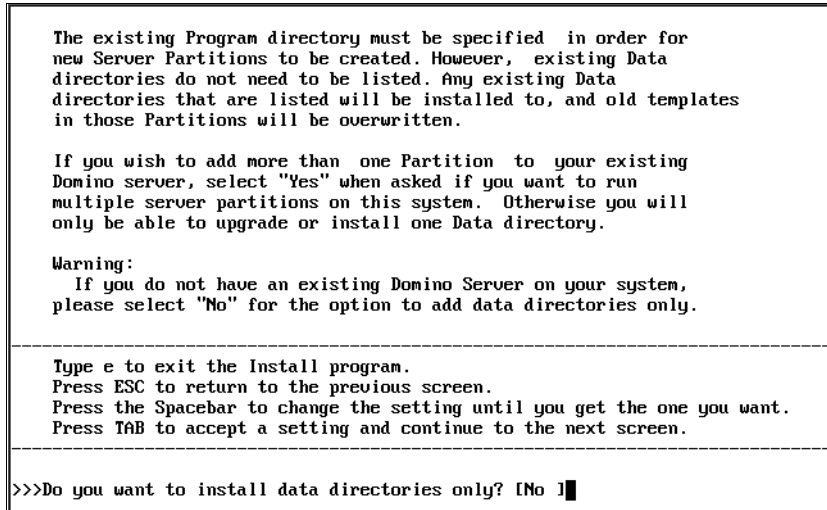


Figure 5-28 Data directories

- For the installation type, press the spacebar until you see Domino Enterprise Server as the setup type and then press Tab. See Figure 5-29.

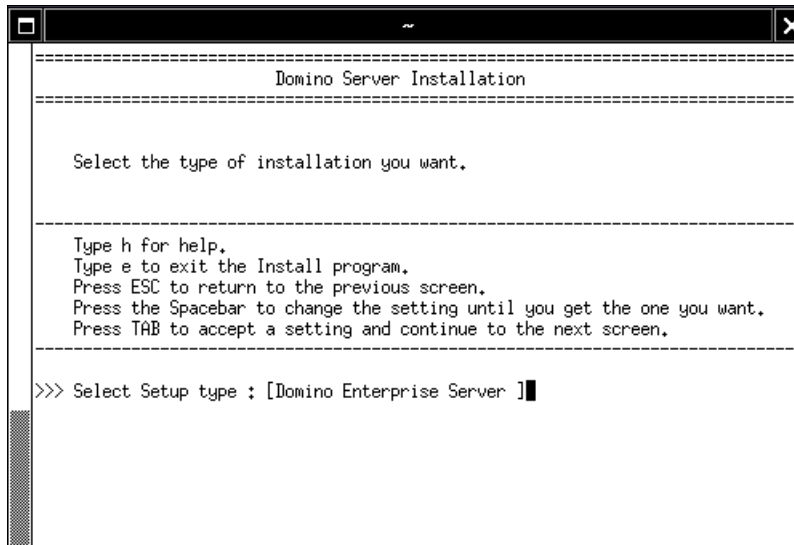


Figure 5-29 Installation type

- For the template files, select Yes and press Tab. See Figure 5-30 on page 217.

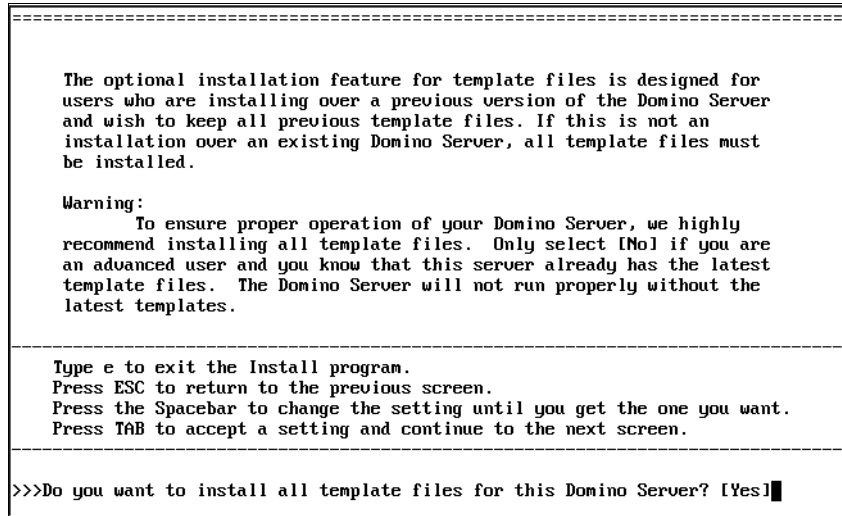


Figure 5-30 Template files

12. For the Application Service Provider (ASP) screen, select No and press Tab.  
See Figure 5-31.

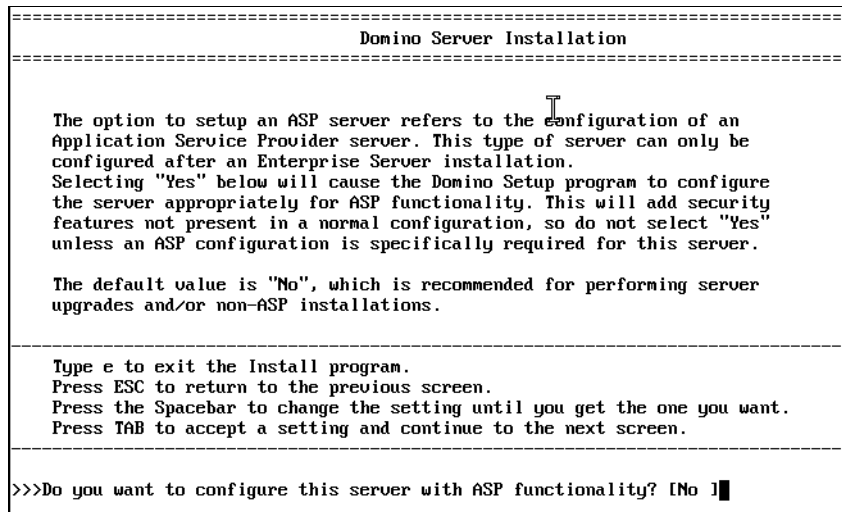


Figure 5-31 ASP information

**Important:** ASP support means Application Service Provider and has nothing to do with Active Server Pages.

13. For the Domino program files installation directory, press Tab to select the default settings for the Domino program files installation directory and continue; otherwise, press Enter to change the directory path. See Figure 5-32.

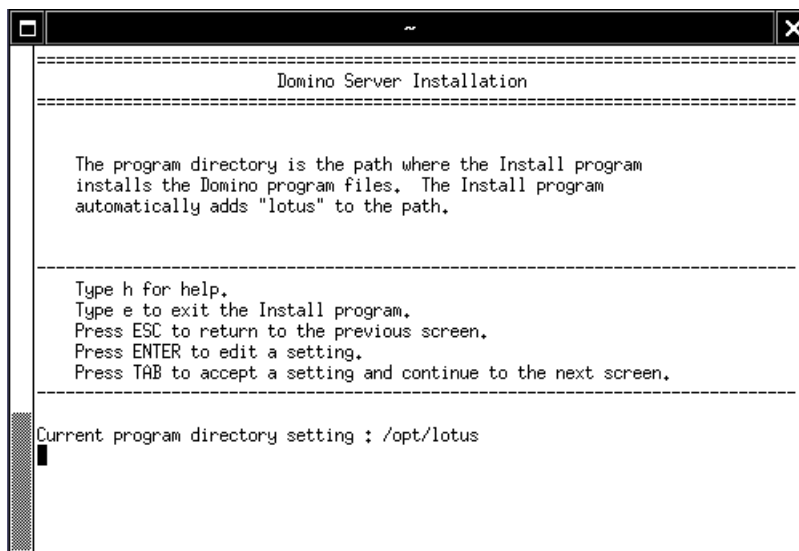


Figure 5-32 Domino Server Installation Directory

14. Press Tab in the next window.
15. The partitioning of Domino server can be performed on Linux, but we do not select this option now. Press the spacebar to state No in the settings and then press Tab. See Figure 5-33 on page 219.



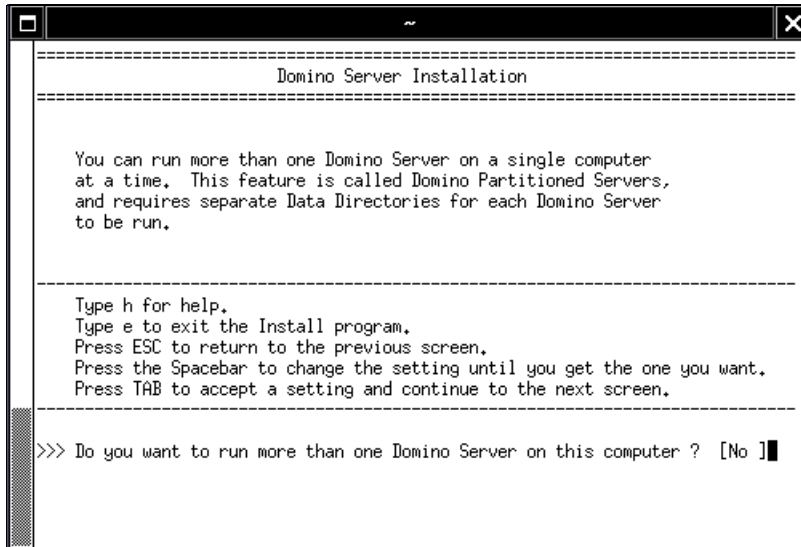


Figure 5-33 Domino Partitioned Servers

16. Press Tab to select the default settings for the Domino data files installation directory and continue; otherwise, press Enter to change the directory path. See Figure 5-34.

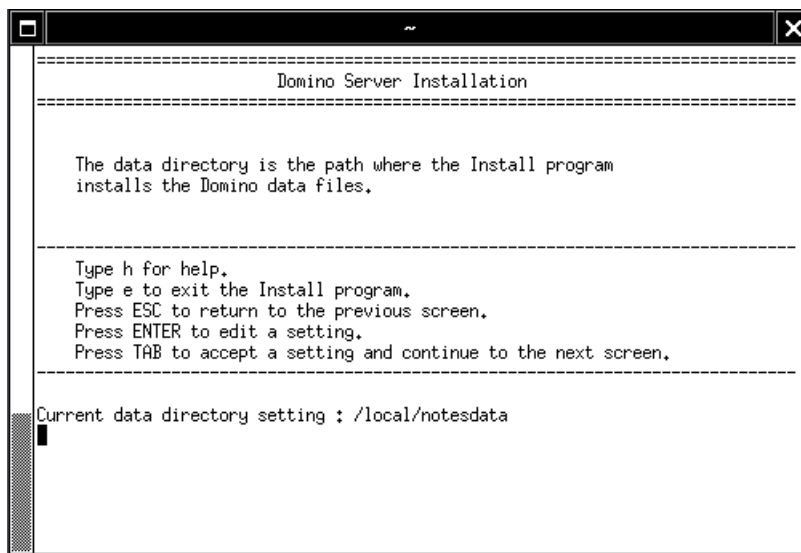


Figure 5-34 Domino data files installation directory

17. In the next window, press Enter to open the window shown in Figure 5-35. Enter the user name of the Domino Enterprise Server administrator and press Enter to return to the previous window. View the changes and press Tab.

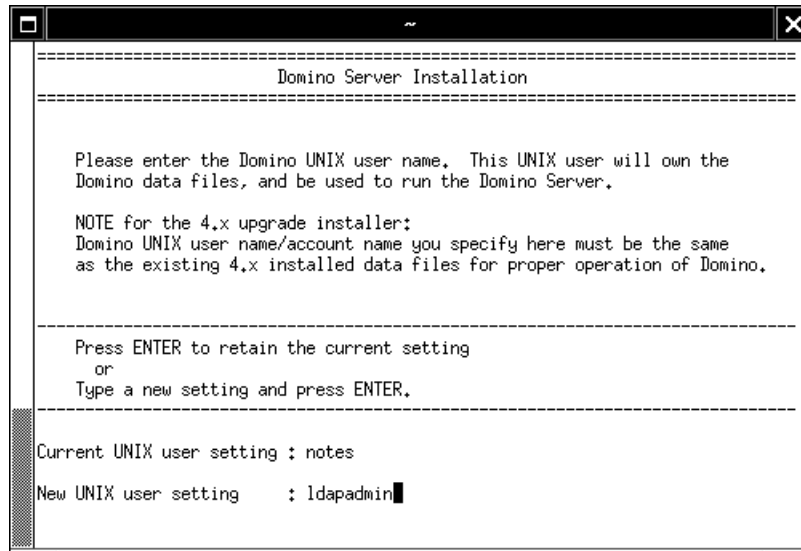


Figure 5-35 Changing the Domino Server administrator user name

18. In the next window, press Enter. You will see a window similar to the one shown in Figure 5-36 on page 221. Enter the name of the Domino Enterprise Server administrator group and press Enter to return to the previous window. Then, view the changes and press Tab.

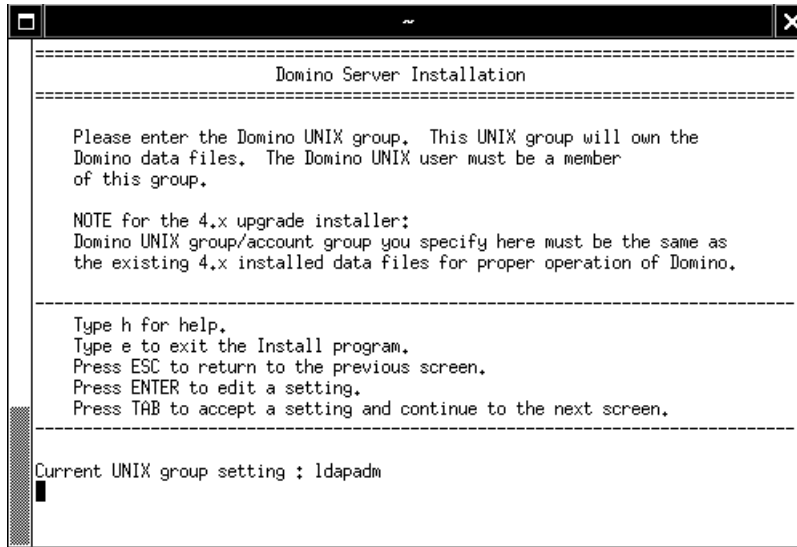


Figure 5-36 Changing the Domino Server administrator group name

19. Select Manual Server Setup and press Tab, as shown in Figure 5-37.

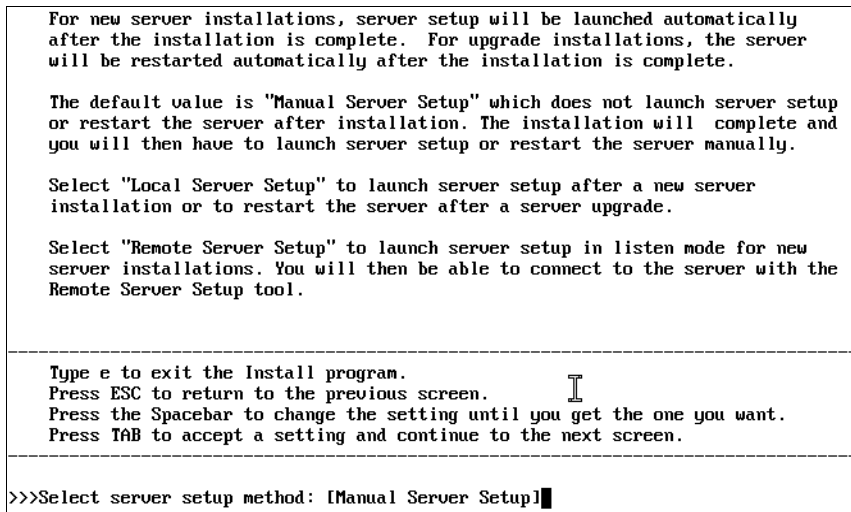


Figure 5-37 Server setup

20. Press Tab in the next window.

21. Check the settings for your installation and press Tab to start the installation. Your installation settings will be similar to those shown in Figure 5-38.

```
=====
 I
 Domino Server Installation
=====
Installation settings:

 Installation type : Domino Enterprise Server
 Install template files : Yes
 Server Setup Method : Manual Server Setup
 Configure to ASP Server: No

 Program directory : /opt/lotus
 Data directory : /local/notesdata
 UNIX user : ldapadmin
 UNIX group : ldapadm

Press the Escape key to re-configure the settings
or
Press the Tab key to perform the installation...
█
```

Figure 5-38 Domino Server Installation settings

22. After the installation completes, you will see a window similar to the one shown in Figure 5-39. This window provides you with the information about the installation settings and the status of the installation.

```

 ~
 Domino Server Installation

Installation settings:

 Installation type : Domino Enterprise Server
 Installing iNotes : iNotes is not supported for this platform: linux

 Program directory : /opt/lotus
 Data directory : /local/notesdata
 UNIX user : ldapadmin
 UNIX group : ldapadm

Validating...

Not checking patches for linux.

Installing Domino Server kits ...
The installation completed successfully.

Please be sure to login as the appropriate UNIX user
before running Domino - Do not run as root.
```

Figure 5-39 Successful completion of the installation

**Important:** For those familiar with Release 5 or earlier versions of Domino, do not type `http httpsetup` unless you do not have X-Windows installed. Domino 6 ships with a new Java installation program that can be run locally or remotely.

## 5.6.2 Installing Domino Administrator

Domino Administrator is required in order to administer Domino. In this instance, you will need to install it on a desktop, because the Windows Server 2003 is not a supported operating system. Complete the following steps:

1. Insert CD #12-6 (Lotus Notes, Designer, and Admin Clients for Windows) and start the **Setup.exe** program in the `lotusnotes\win\English` directory.
2. Click **Next** in the Welcome window. Read and accept the License Agreement and click **Next**.
3. Enter the Name and Company name. Click **Next**.
4. Browse to the folders where you want to install the Notes program files and data files or choose the default folders and click **Next**.
5. Select **Domino Administrator** and click **Next**. Make sure that you select the **Remote Server Setup** option. You will use this tool in 5.6.3, “Configuring the Domino server settings” on page 223.
6. Choose if you want it to be your default e-mail program and click **Install**.
7. Click **Finish** to complete the installation.

You have now installed Domino Administrator on the desktop.

## 5.6.3 Configuring the Domino server settings

Before configuring Domino Administrator you need to set up Domino server. Configure Domino server using the remote or local server setup. For more details, see *Lotus Domino 6 for Linux*, SG24-6835.

### Running the CheckOS tool

Complete the following steps:

1. On machine 3, log in as the root user and start a terminal session.
2. Change to the Lotus binaries directory:  

```
cd /opt/lotus/bin
```
3. Type `./checkos` to start the script.

**Note:** If you get an error or the script does not run, check to see if you are in the Lotus binaries directory. In addition, by issuing `ls`, you should be able to see the `checkos` file. If the file does not exist, the installation might not have completed.

## Setup

Perform the following steps:

1. Log out as root and log in as `ldapadmin`.
2. Open a terminal and verify if you are under the `/local/notesdata` directory.
3. Create the file `.bash_profile` in the `/local/notesdata` directory. Write the following line:

```
export PATH=$PATH:/opt/lotus/bin:./
```

**Important:** Linux is case-sensitive, and `PATH` must be uppercase.

4. Log out and log back in for the changes to take effect.
5. You can check that the `PATH` variable was set correctly by launching a shell and typing `echo $PATH` at the command prompt. To verify that you are using the Domino server executable, type `which server` and check the path.

## Remote setup

The new Java setup also allows for local or remote configuration. We recommend remote setup, because it gives you the ability to download the server and certifier ID files to your local workstation. Complete the following steps:

1. Log in as `ldapadmin`.
2. Make sure that the system `LANG` variable is set correctly for your language, that is, `LANG=en_US`, `LANG=de_DE@euro`. To set the system variable, type `LANG=en_US` or `LANG=de_DE`, for example, in the shell window, and press Enter.
3. Change to the Domino data directory (`/local/notesdata`) and start the Domino server with the `listen` option:

```
/opt/lotus/bin/server -listen
```

4. In the Domino Administrator machine, go to a command prompt, change to the Domino Administrator programs directory, and start the Java configurator (`serversetup.exe`), as shown in Figure 5-40 on page 225.

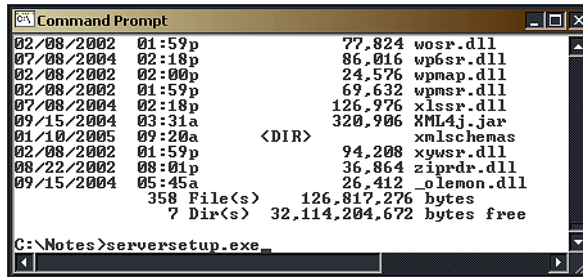


Figure 5-40 Starting the remote server setup

5. Enter either the server's name or IP address in the Remote Host Address field (Figure 5-41) and click **Ping**.



Figure 5-41 Connect To Remote Domino Server

6. If the remote server is set up correctly, and the network is functioning, you should see a message similar to the one shown in Figure 5-42. Click **OK**.

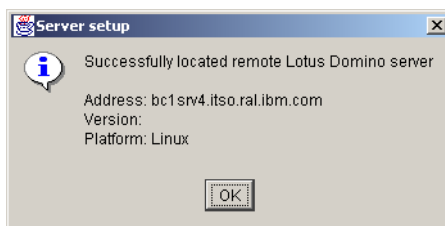


Figure 5-42 Successful ping

7. Now, click **Next** and you will see the window shown in Figure 5-43.

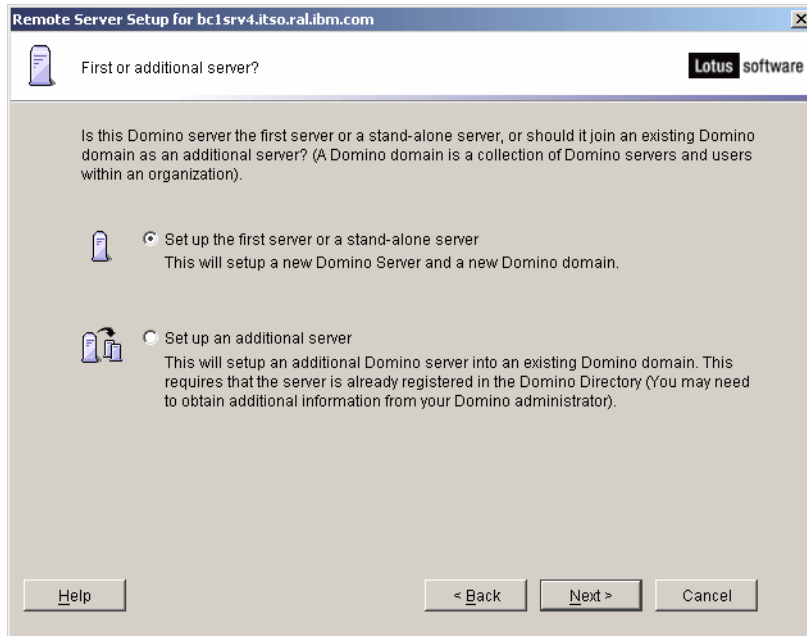


Figure 5-43 First or additional server

8. You are setting up the first server in what will be your new domain (the ITSO domain in our example). If you are setting up an additional server, you will be prompted to specify the location of your server ID and the hierarchical name of the additional server. Select your choice and click **Next**.



9. We have set the server name to be the same as the host name, as shown in Figure 5-44. If the common name matches the host name, the client will be able to locate it even if the server resides in a different domain from the user's home server. The title gives you an opportunity to provide a terse description of the server's main function or the organization to which it belongs. Click **Next** to continue with the installation.

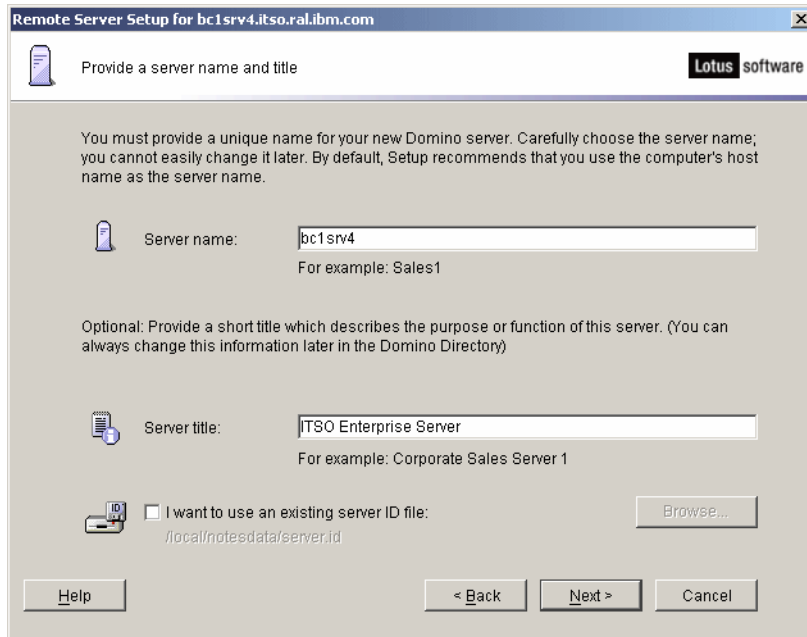


Figure 5-44 Server name and title

10. Set a meaningful Organization name, and make certain to enter a secure password for your Certifier ID, and then click **Next** to proceed. If you are rebuilding your Domino domain, you can select the **I want to use an existing certifier ID file** option to do so.

Remote Server Setup for bc1srv4.itso.ral.ibm.com

Choose your organization name Lotus software

The organization name is usually your company name. It becomes part of each server and user name. Do not choose a long organization name. For example, instead of Acme Corporation, use Acme.

Organization name: ITSO  
Minimum of 3 characters

This server's final name will be: bc1srv4/ITSO  
A typical user name will be: Jane Doe/ITSO

Organization Certifier password: \*\*\*\*\*  
Confirm password: \*\*\*\*\*  
Minimum of 5 characters

I want to use an existing certifier ID file:  
j:\local\notes\data\cert.id Browse...

To specify additional organization settings click Customize. Customize...

Help < Back Next > Cancel

Figure 5-45 Domino Organization name

11. For ease of administration and use, we made the Domino domain name the same as the organization name. See Figure 5-46. Type the name you would like to use and click **Next**.

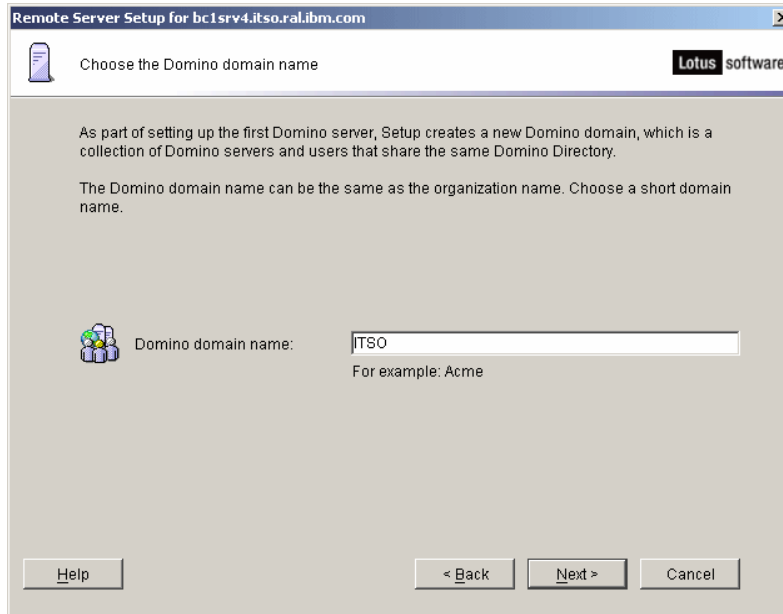


Figure 5-46 Domino domain name

12. Enter an Administrator name and password, and then click **Next**. See Figure 5-47.

**Important:** Do *not* select **Also save a local copy of the ID file** if you are running a remote installation because it will try to access the local file system on the server with which you do not have access. There is an option later in the remote setup to copy the ID files to your local workstations.

Remote Server Setup for bc1srv4.itso.ral.ibm.com

Specify an Administrator name and password

Lotus software

To create the Administrator's ID, you must provide the administrator's name and password. You can use the name of a specific person, or a last name only to create a generic Administrator ID that can be used by several people.

First name: Middle: Last name (or generic account name):

Administrator password: Confirm password:

Minimum of 5 characters

The Administrator ID file will be stored inside the server's Domino Directory.

Also save a local copy of the ID file:  
/local/notesdata/admin.id

I want to use an existing Administrator ID file:  
/local/notesdata/admin.id

Help < Back Next > Cancel

Figure 5-47 Domino Administrator name and password

13. Select all three options shown in Figure 5-48, and then click **Customize** to further refine your selections.

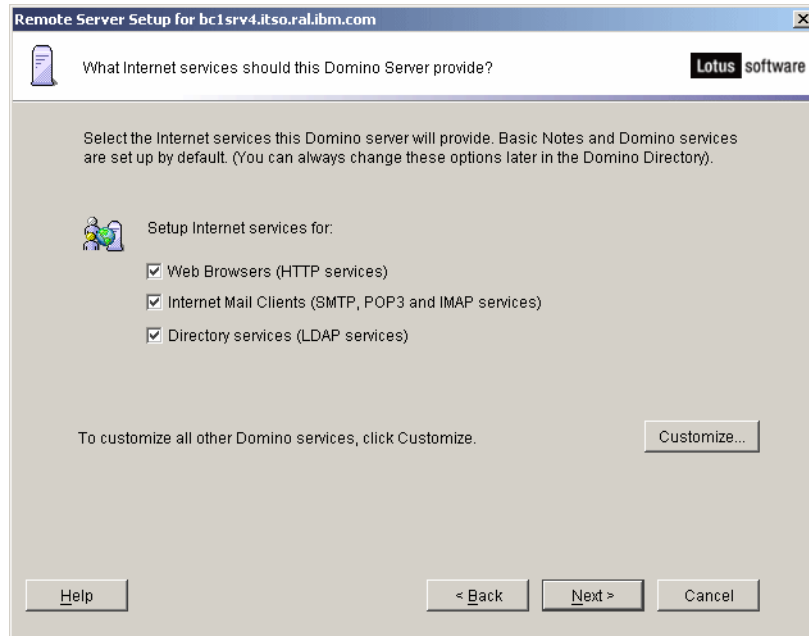


Figure 5-48 Domino services

14. For the advanced Domino services, as shown in Figure 5-49 on page 232, we selected **Calendar Connector**, **Schedule Manager**, and **Statistics** to provide the features needed for this server. We also selected **HTTP Server** for Web services; **IMAP Server** and **POP3 Server** for mail client access; **SMTP Server** for native mail delivery; **LDAP Server** to provide the Domino Directory to LDAP clients; and **Stats** for on demand statistics. See Figure 5-50 on page 232. You will need to consider which services are appropriate for the server you are setting up and select only those that you need. Click **OK**, and then click **Next**.

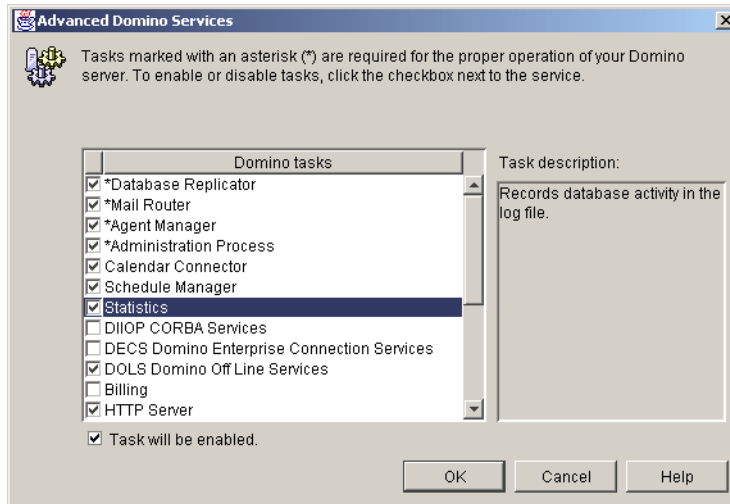


Figure 5-49 Advanced Domino Services: Part 1

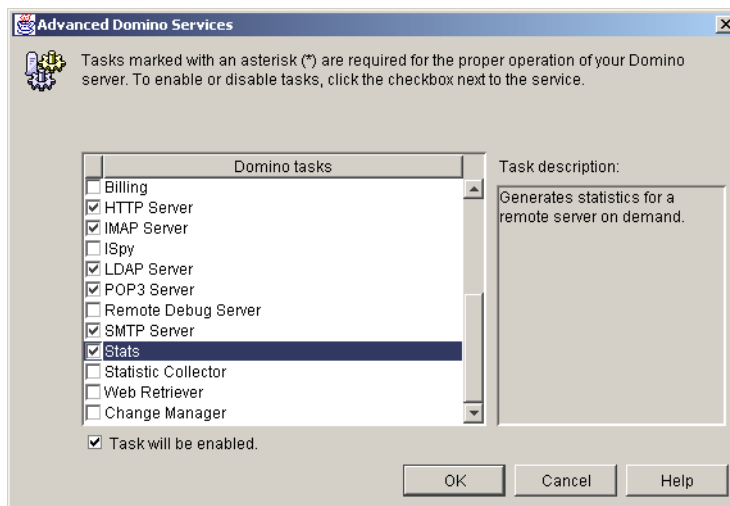


Figure 5-50 Advanced Domino Services: Part 2

15. In Figure 5-51, click **Customize** to enable encryption and to correct the detected network ports and host name. We selected **Encrypt** for the network traffic in order to guard against anyone sniffing the packets during transmission. See Figure 5-52. Click **OK**, and then click **Next**.

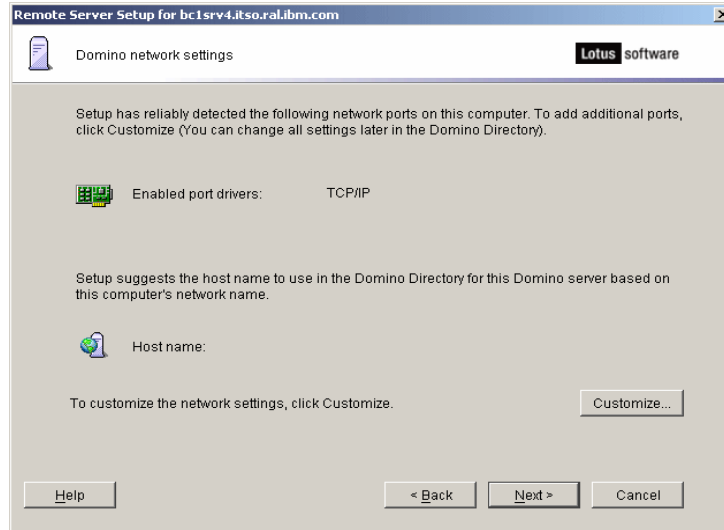


Figure 5-51 Network settings

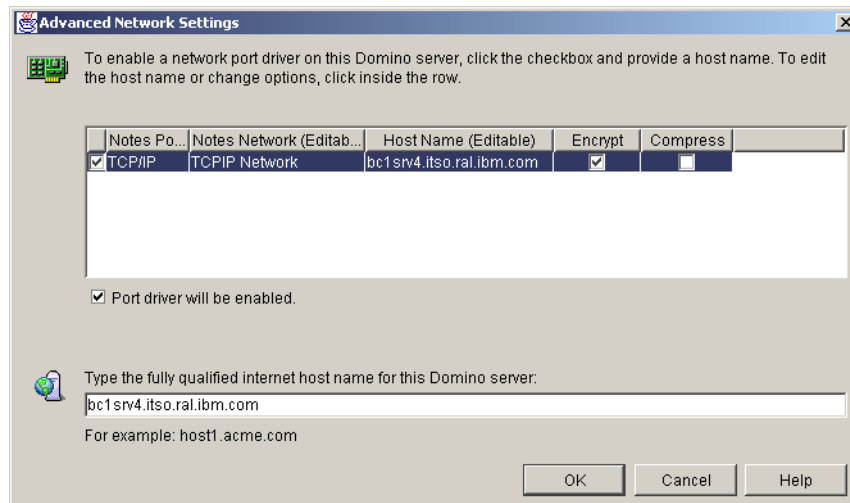


Figure 5-52 Advanced Network Settings

16. To increase security, ensure that the two security options shown in Figure 5-53 are selected (this is the default). Click **Next**.

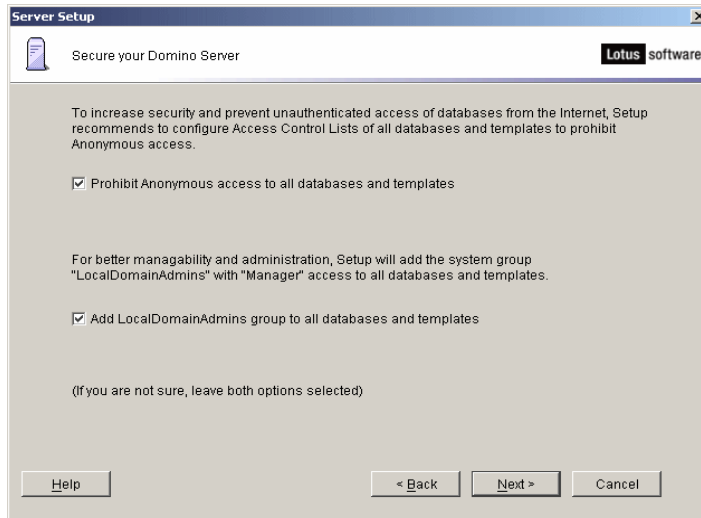


Figure 5-53 Domino security options

17. The remote setup allows the server and certifier ID files to be copied to the local workstation. In Figure 5-54, select **I want to make additional copies of the ID files** and click **Next**.

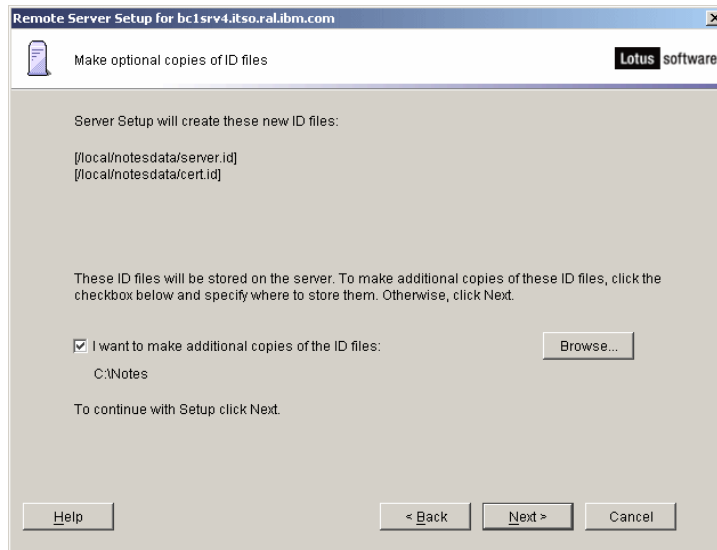


Figure 5-54 Additional copies of ID files



18. Now, click **Setup** to finish the process. After the installation completes, click **Yes** to stop the Domino server command in the listen mode.

## 5.6.4 Configuring Domino Administrator

To configure Domino Administrator, complete the following steps:

1. On machine 3, log in as root. Make sure that Linux does not have a mail server running by issuing `netstat -an | grep 25`. If yes, you should stop and then remove the service. See the following example:

```
netstat -an | grep 25 (verify if there is a service on port 25)
tcp 0 0 127.0.0.1:25 0.0.0.0:0 LISTEN
/etc/rc.d/rc5.d/S13postfix stop (stop the mail service)
rm -rf /etc/rc.d/rc5.d/S13postfix (remove the service from Linux startup)
```

2. Log out and log in as `ldapadmin`. Start the Domino server by entering the following command from the directory `/local/notesdata`:

```
/opt/lotus/bin/server
```

The server is started when you see a window similar to the one shown in Figure 5-55 on page 236.

**Note:** You can stop the Domino server by entering `exit` or `quit` and pressing Enter in the same console. If you close the window, the Domino server will not stop running. To access Domino again, type:

```
> su - ldapadmin
> /opt/lotus/bin/cconsole
Enter the full path of your ID file: user.id
Password: <password>
```

You need to copy the administrator ID (`user.id`) file from the Domino Administrator machine (`C:\Notes\Data`) to the Domino server machine (`/local/notesdata`).

```
ldaplinox:/local/notesdata # /opt/lotus/bin/server
Lotus Domino (r) Server, Release 5.0.12 , February 13, 2003
Copyright (c) 1985, 2003 IBM Corporation. All Rights Reserved.

Releasing unused storage in database log.nsf...
10/06/2003 02:29:12 PM Mail Router started for domain ITSORALEIGH
10/06/2003 02:29:12 PM Router; Internet SMTP host ldaplinox in domain
itso.ral.ibm.com
10/06/2003 02:29:17 PM Database Replicator started
10/06/2003 02:29:22 PM Index update process started
10/06/2003 02:29:27 PM Agent Manager started
10/06/2003 02:29:27 PM JVM: Java Virtual Machine initialized.
10/06/2003 02:29:27 PM AMgr; Executive '1' started
10/06/2003 02:29:32 PM ldaplinox/Itsoraleigh is the Administration Server of
the Domino Directory.
10/06/2003 02:29:32 PM Administration Process started
10/06/2003 02:29:37 PM Calendar Connector started
10/06/2003 02:29:42 PM Schedule Manager started
10/06/2003 02:29:42 PM SchedMgr; Validating Schedule Database
10/06/2003 02:29:42 PM SchedMgr; Done validating Schedule Database
10/06/2003 02:29:47 PM Event Monitor started
10/06/2003 02:29:52 PM Stats agent started
10/06/2003 02:29:57 PM JVM: Java Virtual Machine initialized.
10/06/2003 02:29:57 PM HTTP Web Server started
10/06/2003 02:30:02 PM DIIOP Server started on ldaplinox.itso.ral.ibm.com
10/06/2003 02:30:02 PM DIIOP port 63148 may not be available on this system,
will use port 60148 instead
10/06/2003 02:30:07 PM POP3 Server; Started
10/06/2003 02:30:12 PM LDAP Server; Started
10/06/2003 02:30:12 PM LDAP Server; Serving Directory
/local/notesdata/names.nsf in the Internet Domain
10/06/2003 02:30:12 PM LDAP Server; Maximum entries returned = Unlimited
10/06/2003 02:30:12 PM LDAP Server; Time limit for search = Unlimited seconds
10/06/2003 02:30:12 PM LDAP Server; Minimum characters needed for wild card =
1
10/06/2003 02:30:12 PM LDAP Server; WARNING: Authenticated Users do not need
SSL
10/06/2003 02:30:12 PM LDAP Server; Anonymous access allowed
10/06/2003 02:30:12 PM LDAP Schema; Started loading...
10/06/2003 02:30:15 PM LDAP Schema; Finished loading
10/06/2003 02:30:17 PM Maps Extractor started
10/06/2003 02:30:22 PM SHTP Server; Started
10/06/2003 02:30:22 PM Maps Extractor; Building Maps profile
10/06/2003 02:30:22 PM Maps Extractor; Maps profile built OK
10/06/2003 02:30:27 PM Database Server started
> █
```

Figure 5-55 Starting Domino Server for the first time

3. On the desktop machine, start the Domino Administrator. Click **Start** → **All Programs** → **Lotus Applications** → **Lotus Domino Administrator**.
4. Click **Next** in the Welcome window.

5. In the User Information window:
  - For Your Name, enter the Domino administrator name (ITSOAdmin in our example).
  - For Domino Server, enter the Domino server of your primary server. This name is a combination of the server name and the organization you create in those steps (bc1srv4/ITSO in our example).
  - Ensure that the **I want to connect to a Domino Server** option is selected.  
Click **Next**.
6. On the How do you want to connect to a Domino Server window, select **Set up a connection to a local area network**.
7. On the Domino Server Network information window, the server should be filled in. Select **TCP/IP** and enter the server's fully qualified host name (bc1srv4.itso.ra1.ibm.com in our example).
8. Depending on how you have it set up, it might pull the administrator ID off the server. If it does not, browse to the location of the administrator ID file.
9. Enter the password you chose for the administrator and click **OK**.
10. Clear the **Setup instant messaging** option on the Instant Messaging Setup window. Click **Next**.
11. Under Additional Services, leave all the options cleared. Click **Finish**.

The Domino Administrator interface opens.

## 5.6.5 Setting up Domino Directory

This section describes how to set up the Domino LDAP.

To add WebSphere Portal administrators to Domino Directory, you will need to create two users in your Domino Directory to work with WebSphere Portal. Complete the following steps:

1. Open Domino Administrator. Click **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Administrator**.
2. Go to the People view of the Domino Directory and click **Add Person**.
3. In the New Person form, enter the values shown in Table 5-5 on page 238 for the fields shown to create the Portal administrator user.

Table 5-5 Portal administrator user values

Field	Value
Last name	wpsadmin
User name	wpsadmin/ITSO wpsadmin
Short name/UserID	wpsadmin
Domain	itso.ral.ibm.com
Internet password	wpsadmin

4. Click **Save & Close** to save the entries for the user and return to the People view of Domino Directory.
5. Repeat steps 2 on page 237 through 4 to create the Application Server administrator user. Use the values shown in Table 5-6.

Table 5-6 Application Server administrator user values

Field	Value
Last name	wpsbind
User name	wpsbind/ITSO wpsbind
Short name/UserID	wpsbind
Domain	itso.ral.ibm.com
Internet password	wpsbind

6. In the end, you will have two users: wpsadmin and wpsbind.

**Important:** If you want to have the users that you create also be able to use the Mail portlet, you will need to create a mail database for them and specify it in the Person document in Domino Directory. Follow these steps:

1. Start Domino Administrator.
2. Click **File** → **Database** → **New**.

Make the database with the following options:

- Server: Primary server (bc1srv4/ITSO in our example)
- Title: user mail file
- File Name: mail\Auto Generated.nsf

Template information:

- Server: As above
  - Click **Show advanced Templates**.
  - Select **Domino Web Access (6) inotes6.ntf**.
3. When it opens, open the access control list (ACL) and give that specific user Editor access on this database.
  4. Close the mail file.
  5. Edit the Person document and enter the mail server and mail file name.
  6. Alter the ACL on the mail directory by using Domino Administrator to allow that user to have access to the directory.

7. Go to the Groups view and click **Add Group**.
8. In the New Group form, create a new group called wpsadmins. Select **Multi-purpose** for the Group type.
9. Add wpsbind and wpsadmin as members from the portal's address book. wpsbind will be used for LDAP bind authentication, too.
10. Click **Save & Close** to save the wpsadmins group.
11. Repeat these steps to create a group called wpscontentadministrators and wpsdocreviewers.

**Note:** Checkpoint for LDAP

To check LDAP, complete the following steps:

1. Open a browser.
2. Enter the following URL:  
`ldap://<fully_qualified_hostname>/cn=wpsbind,o=itso`  
For example: `ldap://bc1srv4.itso.ral.ibm.com/cn=wpsbind,o=itso`
3. You should see a window similar to the one shown in Figure 5-56.

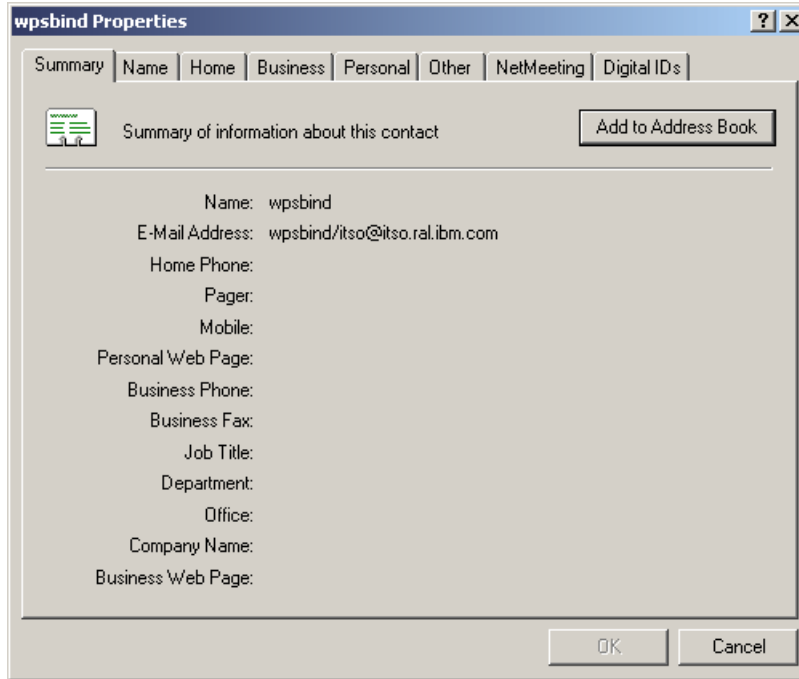


Figure 5-56 Checkpoint for LDAP

## 5.6.6 Updating the access control list of Domino Directory

To update the ACL, complete the following steps:

1. From Domino Administrator, open the server's Domino Directory. Click **File** → **Database** → **Access Control** to open names.nsf.
2. Click **Add**. Click the People icon, and select **wpsadmins**.
3. In the Basic panel, make sure that the Portal administrator group wpsadmins has either Author access or Editor access for all roles available by selecting **wpsadmins**, changing the access to **Manager**, and selecting the **Delete documents** option.
4. Assign the following Role types to the wpsadmins group:
  - GroupCreator
  - GroupModifier
  - UserCreator
  - UserModifier
5. Click **OK** to save the settings.

## 5.6.7 Specifying Domino LDAP configuration settings

In this section, we describe the Domino LDAP configuration settings.

### Adding the HTTP\_HostName attribute

To add the HTTP host name attribute, complete the following steps.

**Note:** You might not have to do this step depending on the configuration you choose for your Domino server. Every time we checked, it was already populated.

1. Verify if this attribute already exists. Click **File** → **Database** → **Open**. Select the Domino server (**bc1srv4/ITSO** in our example) and open the file **Domino LDAP Schema (schema.nsf)**. Select **All Schema Documents** → **LDAP Attribute Types** and search for HTTP\_HostName.
2. If it exists, skip this topic and go to “Completing the configuration” on page 242. If not, follow these steps.
3. Make sure that you have Manager access to the Schema database (schema.nsf).
4. Open the Schema database on any server in the domain that runs the LDAP service.
5. Select **All Schema Documents view**, and then click **New Document** → **Add Attribute Type**.
6. Complete the fields specified in Table 5-7 on the Basics tab.

Table 5-7 Values for the HTTP\_HostName attribute

Field	Action
LDAP name	Enter HTTP-HostName for the attribute.
OID	Enter the object identifier: 2.16.840.1.113678.2.2.2.2.461
Syntax name	Select <b>Directory String</b> .
Description	(Optional) Enter a description for the attribute.
Equality match	(Optional) Select a matching rule to apply when the equality operator is used to search for this attribute.
Ordering match	(Optional) Select a matching rule to apply when an ordering operator is used to search for this attribute.
Substrings match	(Optional) Select a matching rule to apply when a substring operator is used to search for this attribute.

Field	Action
Single valued	Choose one: <ul style="list-style-type: none"> <li>▶ Yes to allow more than one value for the attribute (default)</li> <li>▶ No to allow only one value</li> </ul>
Collective	Choose one: <ul style="list-style-type: none"> <li>▶ Yes to allow the values for this attribute to be shared</li> <li>▶ No to prevent values from being shared (default)</li> </ul>
No user modification	Choose one: <ul style="list-style-type: none"> <li>▶ Yes to prevent users from modifying the values</li> <li>▶ No to allow users to modify values (default)</li> </ul>

7. Click **Save & Close**. A draft document for the HTTP\_HostName attribute appears in the Draft Documents - Draft Attribute Types view.
8. Select the **HTTP\_HostName** draft documents, and click **Approve** → **Approve Selected Drafts**.

### Completing the configuration

To select the attributes for Domino LDAP, complete the following steps:

1. Use the Domino Administrator interface to open the Domino Directory, names.nsf, on the primary server (bc3srv5/itso in our example).
2. Navigate to the view **Configuration - Servers**.
3. Highlight **Configurations** and then open the Configuration Settings document. If a global configuration document does not exist, click **Add Configuration** to create a new configuration document and display Configuration Settings.
4. On the Basics tab, for the **Use these settings as the default settings for all servers** option, click **Yes**.

**Note:** You must select **Yes** to cause the LDAP tab to appear for use in the next step.

5. On the LDAP tab, click the button next to **Select Attribute Types** to open the LDAP Attribute Type Selection dialog box.
6. From the Object Classes drop-down list, select \*, and then click **Display Attributes**.
7. From the Selectable Attribute Types box, select the following fields, and then click **Add** to add them the Queriable Attribute Types box:
  - AltFullName
  - dominoCertificate



- givenName
  - FullName
  - HTTP\_HostName
  - Location
  - mail
  - MailAddress
  - MailDomain
  - MailFile
  - MailServer
  - member
  - NetAddresses
  - PublicKey
  - Sametime
  - sn
  - uid
  - userCertificate
8. Click **OK** to close the LDAP Attribute Type Selection dialog box and return to the Configuration Settings document.
  9. Ensure that the Anonymous users can query field displays the following attributes:
    - AltFullName
    - dominoCertificate
    - givenName
    - FullName
    - HTTP\_HostName
    - InternetAddress
    - Location
    - mail
    - MailAddress
    - MailDomain
    - MailFile
    - MailServer
    - member
    - NetAddresses
    - PublicKey
    - Sametime
    - sn
    - uid
    - userCertificate
  10. For the **Allow LDAP users write access** option, click **Yes**. This setting ensures that Portal users can use the self-care and self-registration features of WebSphere Portal.
  11. Keep all other default LDAP settings in Configuration Settings.

12. Click **Save & Close** to close Configuration Settings.

### **Additional Domino configuration**

To enable the database drop-down list, you must complete two tasks: enable the DIOP task and allow users the ability to run Java agents.

To enable the DIOP task to load automatically every time the Domino server starts, perform the following steps:

1. Open the notes.ini in the Domino program directory.
2. Locate the line `ServerTasks=` and add `diop` to the end of the line if it is not already there.
3. Save and close the file.

For more information about the DIOP task, refer to the *Lotus Domino Administrator Help*.

Next, perform the following steps to allow users the ability to run Java agents:

1. Start the Domino Console.
2. Open the address book from the primary server (bc1srv4/ITSO in our case).
3. Click the **Server** → **Servers** view.
4. Double-click the server document that you want to configure.
5. Make the following configuration changes to the server document:
  - a. On the Basics tab, make sure the Fully Qualified Internet Host Name field contains the fully qualified name that you entered in the browser to access this server.
  - b. Switch to the Ports tab. On the Notes Network Ports subtab, make sure the top line has the Port set to **TCPIP** and the Net Address set to the fully qualified name of the server. Make sure this port is set to **Enabled**.
  - c. Switch to the Internet Protocols tab. On the HTTP subtab, select **Yes** for the **Allow HTTP Clients To Browse Databases** option.
  - d. Switch to the Security tab. For troubleshooting and development purposes, set the following two fields to \* under the Programmability Restrictions section:
    - Run restricted LotusScript/Java agents
    - Run restricted Java/JavaScript/COM
    - Run unrestricted Java/JavaScript/COM

**Note:** You might want to restrict these fields to a subset of users. If you do this, note the following information:

- ▶ The Domino server to which you are connecting must be included with the full canonical name (for example, bc3srv5/itso). Next, add any users or groups that you want to receive a list of databases when placing a portlet in edit mode. You can also use an asterisk (\*) as a wild card.
- ▶ If you want to add the user wpsadmin, add the following information to the field: uid=wpsadmin/cn=users/o=ibm/c=us. To add all members in the /o=ibm/c=us organization, add the following value to the field: \*/o=ibm/c=us.

6. Click **Save & Close**.

### 5.6.8 Creating the Web SSO configuration (optional)

The Web single sign-on (SSO) configuration document is a domain-wide configuration document stored in the Domino Directory. You must create the Web SSO configuration document prior to enabling multiserver single sign-on. Complete the following steps:

1. Start Domino Administrator by clicking **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Server**.
2. Open Domino Directory.
3. Select **Server** → **All Server Documents**.
4. Select the server (primary server) and click **Web** → **Create Web SSO Configuration** (Figure 5-57 on page 246).

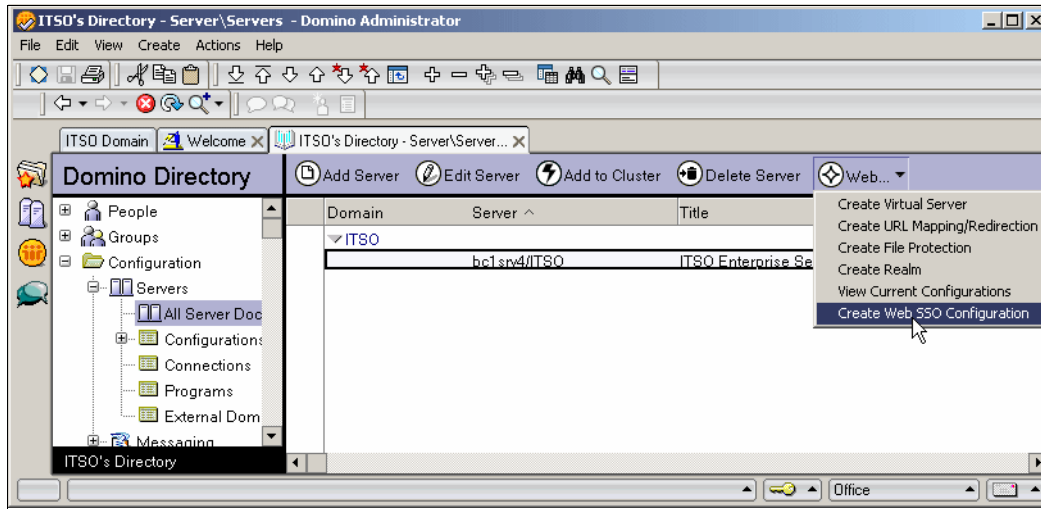


Figure 5-57 Create Web SSO Configuration

5. Enter the domain suffix for the token domain and select both servers in Domino Server Names field (Figure 5-58).

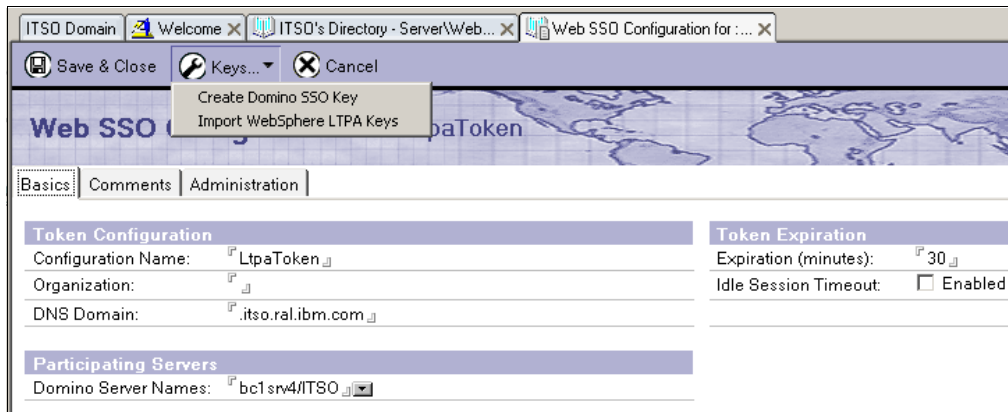


Figure 5-58 Create Web SSO key

6. From the Keys menu, select **Create Domino SSO Key**.
7. Click **OK**.
8. Click **Save & Close**.
9. Open the Server document (bc1srv4). Click **Configuration** → **Servers** → **All Servers Documents**.

10. Go to the Internet Protocol tab and then to the Domino Web Engine tab. In the Session Authentication field, select **Multiple Servers (SSO)**. In the Web SSO Configuration field, select **LTPA Token**.
11. Click **Save & Close**.
12. Close the Domino Administrator interface.
13. Restart the Domino server. To restart the server, issue the following command from the Domino Console:

```
restart server
```

**Note:** Checkpoint for Domino

You should be able to open the Domino home page using a browser by typing `http://<fully_qualified_domino_server>` in the URL. Port 80 is the default port number for Domino Web server. For example, in our lab configuration, the URL of the Domino home page is `http://bc1srv4.itso.ral.ibm.com`.

## 5.6.9 Configuring WebSphere Portal for Domino Directory

To edit the `wpconfig.properties` file and run the appropriate configuration tasks so that WebSphere Portal can work with the Domino LDAP server, complete the following steps:

1. In machine 2, locate the `<wp_root>/config/wpconfig.properties` file and create a backup copy.
2. Update the file property values under the WebSphere Application Server and Domino sections applicable to your environment using the values in Table 5-8 as a basis. For the purpose of the proof of concept, the fields shown in Table 5-8 were updated.

Table 5-8 Values used in the lab

Property	Value used
WasUserId	cn=wpsbind,o=ITS0
WasPassword	wpsbind
PortalAdminId	cn=wpsadmin,o=ITS0
PortalAdminIdShort	wpsadmin
PortalAdminPwd	wpsadmin
PortalAdminGroupId	cn=wpsadmins
PortalAdminGroupIdShort	wpsadmins

Property	Value used
WpsContentAdministrators	cn=wpscontentadministrators
WpsContentAdministratorsShort	wpscontentadministrators
WpsDocReviewer	cn=wpsdocreviewer
WpsDocReviewerShort	wpsdocreviewer
LTPAPassword	password
SSODomainName	itso.ral.ibm.com
LDAPHostName	bc1srv4.itso.ral.ibm.com
LDAPPort	389
LDAPAdminUID	cn=wpsbind,o=ITSO
LDAPAdminPwd	wpsbind
LDAPServerType	DOMINO502
LDAPBindID	cn=wpsbind,o=ITSO
LDAPBindPassword	wpsbind
WmmSystemId	cn=wpsbind,o=ITSO
WmmSystemIdPassword	wpsbind
LDAPSuffix	<blank>
LDAPUserPrefix	cn
LDAPUserSuffix	o=itso
LDAPGroupPrefix	cn
LDAPGroupSuffix	<blank>
LDAPUserObjectClass	inetOrgPerson
LDAPGroupObjectClass	groupOfNames
LDAPGroupMember	member
LDAPGroupFilter	(&(cn=%v)(objectclass=groupOfNames))

3. In machine 3, ensure that the Domino server is started:

```
ps -aux | grep server
```

If not, start the Domino server by typing (log in as ldapadmin):

```
cd /local/notesdata
/opt/lotus/bin/server
```

4. In machine 2, bring up a command prompt and change the current working directory to <was\_root>/bin.
5. Enter the following commands:

```
#!/startServer server1
#!/stopServer WebSphere_Portal
```
6. Change the current working directory to <wp\_root>/config.
7. Open a command prompt and navigate to wp\_root/config/wizard and execute the following command:

```
configwizard.sh.
```
8. Select **English** as the language.
9. Click **Next**.
10. Select **Enable LDAP security**, as shown in Figure 5-59. Click **Next**.

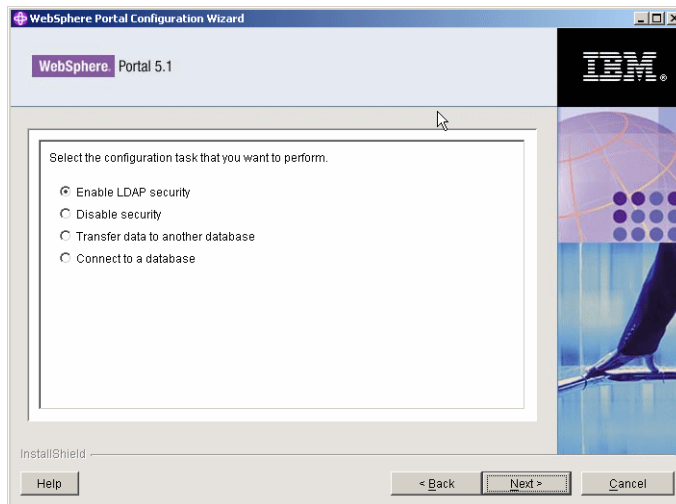


Figure 5-59 Enable LDAP security

11. Select **Lotus Domino Enterprise Server** and click **Next**.
12. Browse and select the **wpconfig.properties** file. Click **Next** and then step through the settings and validate the changes we made in the previous steps.

**Note:** In our setup, here we chose to enable security without realm support. Realms are used as part of the virtual portals. To enable realm support, you would need to use `validate-wmmur-ldap` and `enable-security-wmmur-ldap`.

13. Check the output for any error messages before proceeding with any additional tasks. Output is in `configtrace.log`, `configtrace1.log`, and `configwizard.log` in the `<wp_root>/log` directory.

**Important:** If the configuration task fails, verify the values in the `wpconfig.properties` file and check the output as specified in step 13. Before running the task again, be sure to stop the WebSphere Portal application server by entering the following command from the `<was_root>/bin` directory and specifying the WebSphere Application Server user ID and password (as defined by the `WasUserId` and `WasPassword` properties):

```
#!/stopServer WebSphere_Portal -user was_admin_userid -password was_admin_password
```

14. Stop the servers:

```
#!/stopServer WebSphere_Portal -user was_admin_userid -password was_admin_password
```

After this completes, also make sure that `server1` is stopped by issuing:

```
#!/stopServer server1 -user was_admin_userid -password was_admin_password
```

**Note:** After you have enabled security with your LDAP directory, you will need to provide the user ID and password required for security authentication on WebSphere Application Server when you perform certain administrative tasks with WebSphere Application Server.

In our configuration, the command is:

```
#!/stopServer WebSphere_Portal -user wpsbind -password wpsbind
```

15. Start both the servers by running the following commands in a command prompt from `<was_root>/bin`:

```
#!/startServer server1 -user was_admin_userid -password was_admin_password
```

After this completes, also make sure WebSphere Portal is started by issuing:

```
#!/startServer WebSphere_Portal -user was_admin_userid -password was_admin_password
```



## 5.6.10 Verifying the LDAP configuration

To verify that Domino Enterprise Server V6.5.3 for WebSphere Portal has been properly configured, complete the following steps:

1. Open WebSphere Portal and create a new user by clicking **Sign-up** in the upper-right corner.
2. Log in to WebSphere Portal as the user you just created.

If the login is successful, the configuration is successful, and your Domino Enterprise Server is working normally.

## 5.6.11 Configuring WebSphere Portal Web SSO (optional)

To configure WebSphere Portal Web SSO, perform the following steps:

1. Open the WebSphere administrative console:

`http://bc1srv3.itso.ra1.ibm.com:9090/admin`

**Note:** The SSO mechanism requires the use of a token. This token, referred to as a Lightweight Third Party Authentication (LTPA) token, contains data that uniquely identifies the user, such as the user ID and a digital signature used to authenticate the token by the application server.

If you have already configured SSO between Domino LDAP and WebSphere Application Server, use the same LTPA token that was created by WebSphere Application Server and imported by Domino LDAP.

2. Select **Security** → **Authentication Mechanisms** → **LTPA**.
3. Enter a name for the key file, for example, `/tmp/domwas.key`. The file will be saved in the WebSphere Portal server machine (Linux).

4. Click **Export Keys** (Figure 5-60).

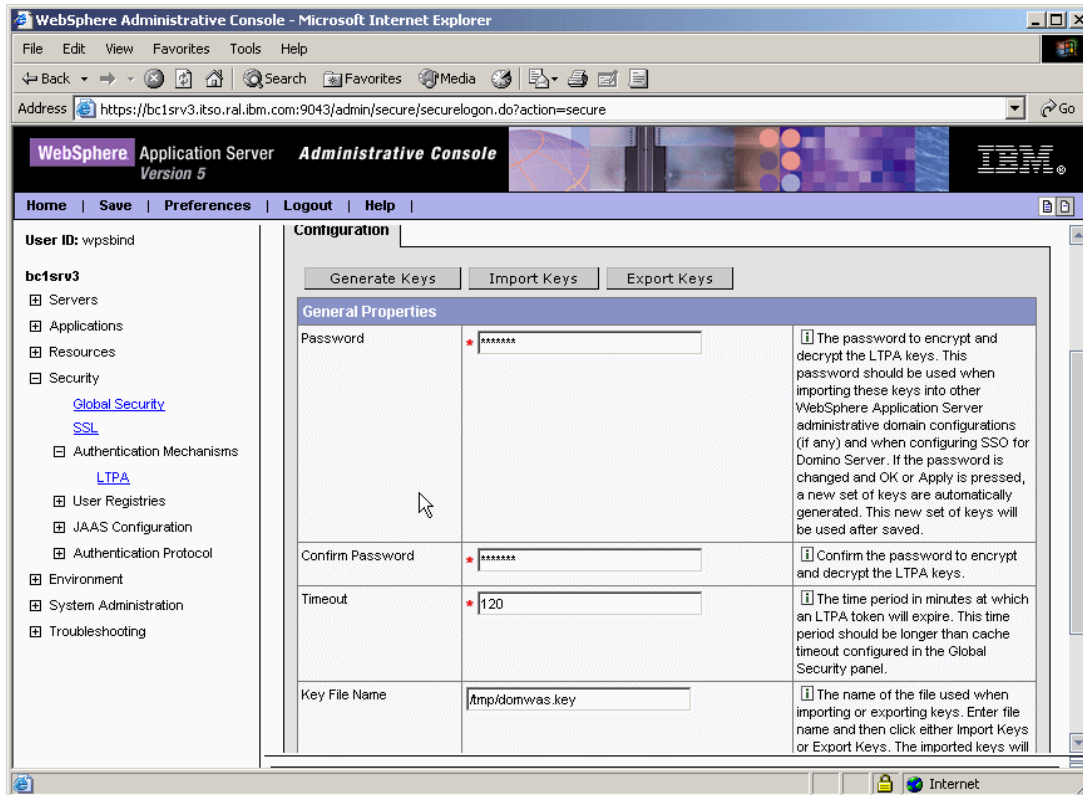


Figure 5-60 Export LTPA token from portal

5. Click **Save** (Figure 5-61). Click **Save** again to accept the modifications.

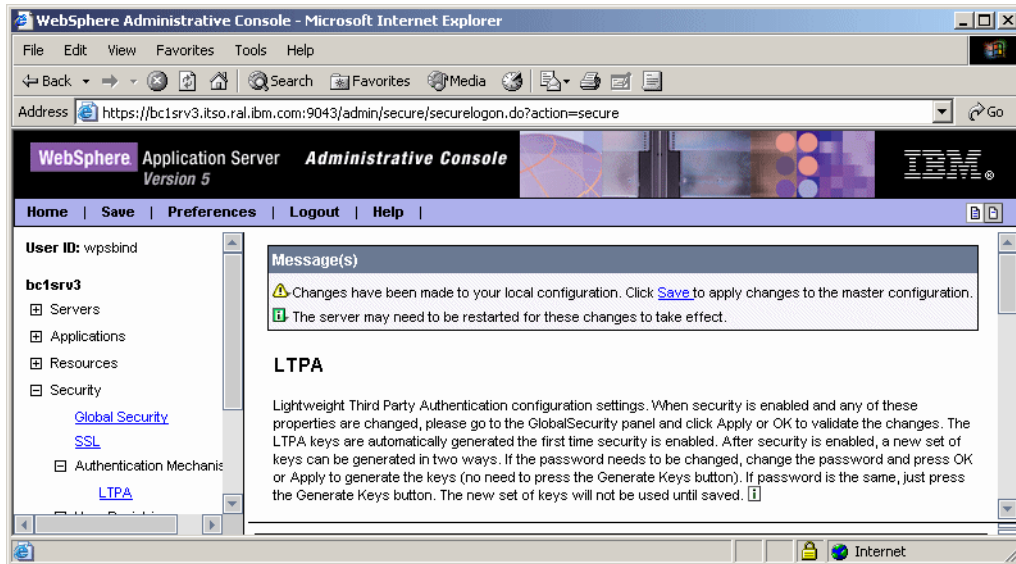


Figure 5-61 Click Save

6. Click **Logout**.
7. Stop both servers:  

```
#!/stopServer WebSphere_Portal -user was_admin_userid -password was_admin_password
```

After this completes, also make sure that server1 is stopped by issuing:

```
#!/stopServer server1 -user was_admin_userid -password was_admin_password
```
8. Bring up Domino Administrator.
9. Open the names.nsf database by clicking **File** → **Database** → **Open**.
10. Make sure that it is on the primary server (bc1srv4/ITSO in our example).
11. Click the **Configuration** tab.
12. Expand **Web**.
13. Click **Web Configuration**.
14. Expand \*- **Web SSO Configurations**-.
15. Open the Web SSO Configuration for the LTPA token (Figure 5-62 on page 254).

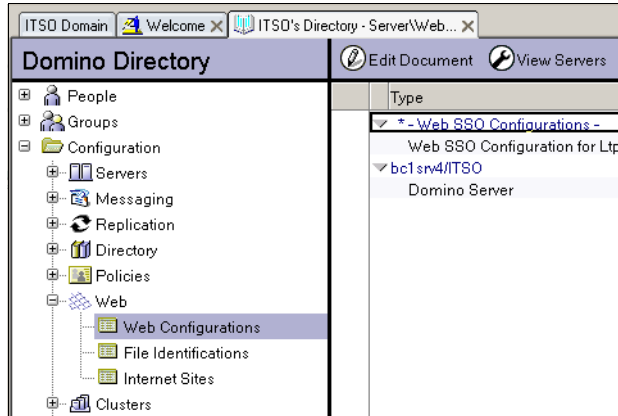


Figure 5-62 Import the LTPA token on the Domino server

16. Edit the document.

17. Click **Keys** → **Import WebSphere LTPA Keys** (Figure 5-63).

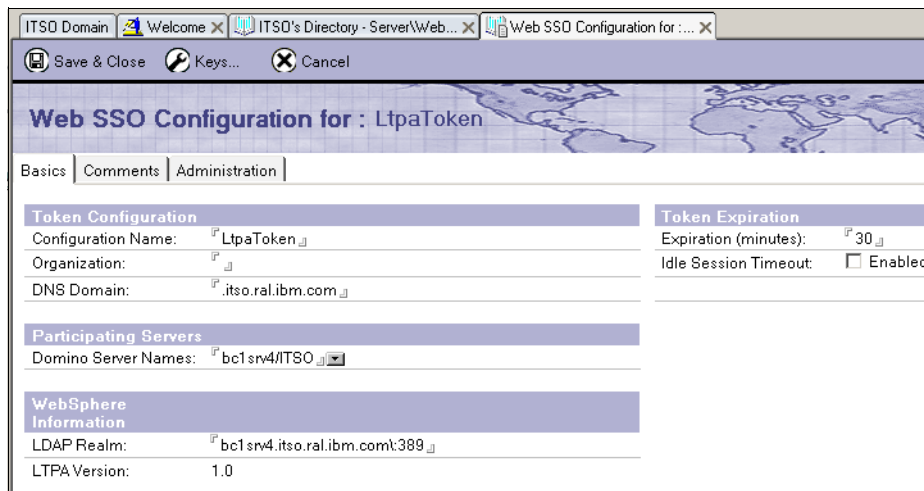


Figure 5-63 Import the LTPA key

18. Ignore the warning message that SSO configuration has already been initialized.

19. Click **OK**.

20. Copy the key file from the Linux server to the Windows desktop (where Domino Administrator was installed).

21. Enter the path of the key (Figure 5-64). For example, in the lab, the key was copied to C:\temp\domwas.key. Click **OK**.

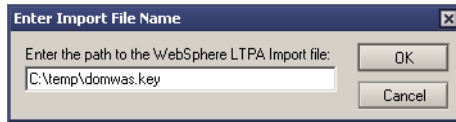


Figure 5-64 Path to the LTPA key

22. Type in the LTPA password, for example, password (Figure 5-65). Click **OK**.

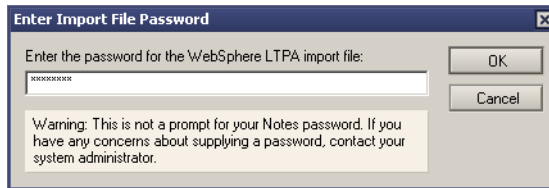


Figure 5-65 Enter the LTPA password

23. You will see the message Successfully imported WebSphere LTPA keys. Click **OK**.

24. Enter <server\_name>\:389 as the LDAP Realm (Figure 5-66). It is important to enter the slash and colon (\:) before the port number.

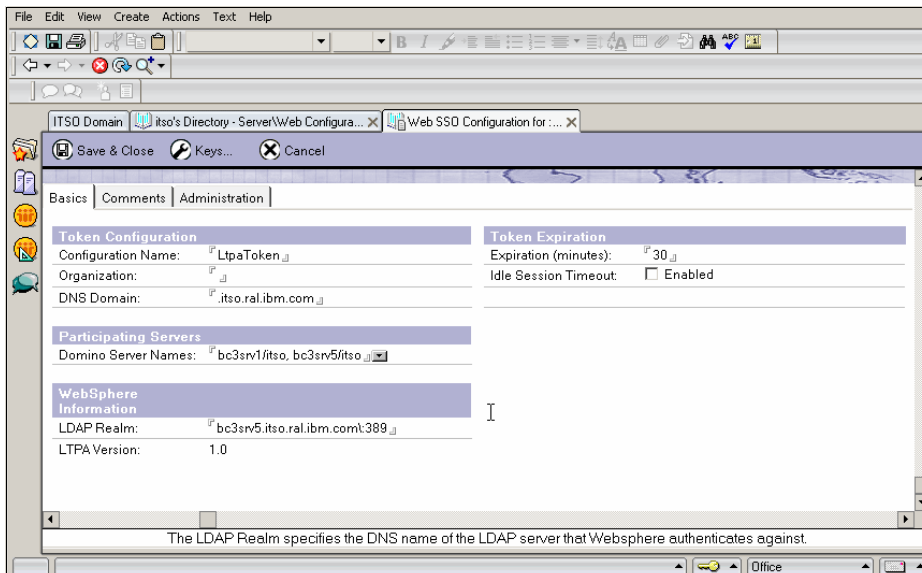


Figure 5-66 Finish importing the LTPA key

25. Click **Save & Close**.

26. Restart the Domino server.

27. Start the server by running the following commands in a command prompt from <was\_root>/bin:

```
#!/startServer server1 -user was_admin_userid -password was_admin_password
```

After this completes, start WebSphere Portal by issuing:

```
#!/startServer WebSphere_Portal -user was_admin_userid -password
was_admin_password
```

**Note:** Checkpoint for single sign-on

To check single sign-on, complete the following steps

1. Log in to the portal by entering the following URL:

```
http://<fully_qualified_server_name>:9081/wps/portal
```

In our example: <http://bc1srv3.itso.ral.ibm.com:9081/wps/portal>

2. Point the same browser to:

```
http://<domino_server>/names.nsf
```

In our example: <http://bc1srv4.itso.ral.ibm.com/names.nsf>

3. You should see the Domino address book without being challenged for an user name and password if single sign-on is working properly.



# WebSphere Portal: IBM AIX 5L V5.2 installation

This chapter describes the installation and configuration of IBM WebSphere Portal V5.1 for IBM AIX 5L Version 5.2 in a multi-tier environment.

This installation includes:

- ▶ Server one: IBM HTTP Server V1.3.28
- ▶ Server two:
  - WebSphere Application Server Enterprise V5.1.1.1
  - WebSphere Business Integration Server Foundation V5.1.1
  - WebSphere Portal V5.1
  - WebSphere Portal content publishing runtime
  - Cloudscape

Hardware supporting this server:

- IBM @server pSeries (RS/6000®) 44p Model 170:
  - One 450 MHz POWER3™-II processor
  - 2 GB RAM
  - Two 18 GB hard disk

- One SCSI CD-ROM drive
  - One 100 Mbps Ethernet
  - One GXT300P graphics adapter
- ▶ Server three: IBM DB2 Universal Database™ Enterprise Server Edition V8.1 with Fix Pack 6
  - ▶ Server four: IBM Tivoli Directory Server V5.2

This is an architecture more appropriate for a production environment, where you will need a more robust database and an LDAP directory for authentication.

Figure 6-1 shows an example of the architecture used in this book.

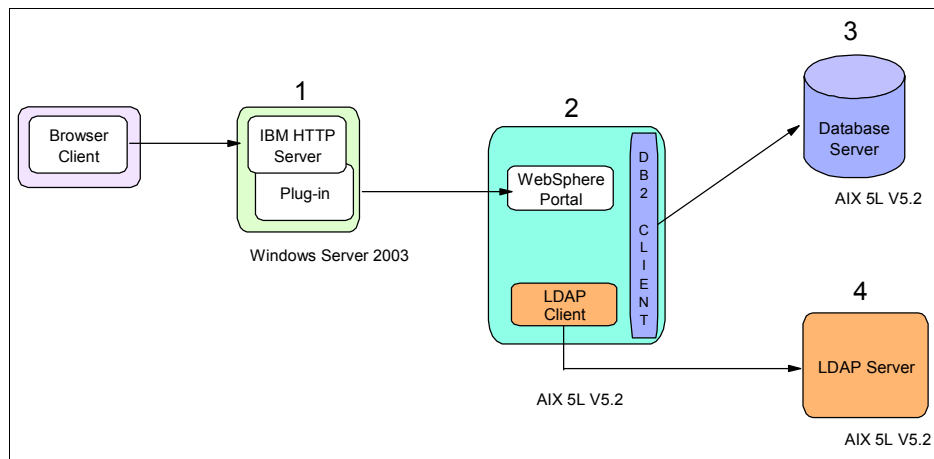


Figure 6-1 Installation topology of IBM AIX 5L in a multi-tier environment



For our lab installation, Table 6-1 specifies the CDs that are required for the installation of the WebSphere Portal components in this chapter.

*Table 6-1 Installation CDs*

<b>Disk</b>	<b>Description</b>
CD Setup	WebSphere Portal V5.1 - Portal Install (Setup), V5.1
CD #1-5	WebSphere Business Integration Server Foundation for AIX 5L V5.1
CD #4-3	WebSphere Application Server V5.1 Archive Install for AIX
CD #5-2	Portal Server V5.1 Archive Install for Linux/UNIX
CD #5-3	Portal Server V5.1 Archive Install for Windows, AIX, Solaris, HP-UX, Linux zSeries, Linux Intel, Linux PowerPC®
CD #8-3	IBM Tivoli Directory Server for AIX, V5.2
CD #9-4	DB2 UDB Enterprise Server Edition AIX -SBCS, V8.1
CD #9-12	DB2 UDB Enterprise Server Edition V8.1 Fix Pack 6 AIX - SBCS

## 6.1 Installing WebSphere Portal in a multi-tier environment

In WebSphere Portal V5.1, you have to install WebSphere Portal using Cloudscape. At this point, WebSphere Portal will not have security enabled. Later, you configure WebSphere Portal to use DB2 UDB Enterprise Server Edition and IBM Tivoli Directory Server as the LDAP. This is what you need to do:

1. Install a base WebSphere Portal environment; this includes:
  - a. WebSphere Application Server with required fixes
  - b. WebSphere Business Integration Server Foundation with required fixes
  - c. WebSphere Portal with Content Publishing and portlets
  - d. WebSphere Personalization
2. Install and configure IBM HTTP Server and WebSphere Application Server plug-in.
3. Install DB2 UDB Enterprise Server Edition and configure the databases.
4. Move the data from the Cloudscape database to DB2 UDB Enterprise Server Edition database.
5. Install LDAP and setting up users and groups.
6. Configure WebSphere Portal for LDAP.

## 6.2 Installing WebSphere Portal

This section describes the procedure for the WebSphere Portal installation on AIX.

**Important:** Avoid a potential port conflict between the administrative console and the AIX WebSM system management console. The AIX WebSM system management server listens on port 9090 by default.

Before starting the WebSphere Portal installation, verify that port 9090 is already in use by running the following command:

```
netstat -an |grep 9090
```

If you find an existing connection to this port, the WebSM process might be using it. We *strongly* recommend that you disable the service during the WebSphere Portal installation. To disable the WebSM server, issue the following command:

```
/usr/websm/bin/wmsserver -disable
```

If you want the WebSM server to coexist with WebSphere Application Server, you must change the Administrative port number when the installation of WebSphere Portal is completed. For more information, refer to the *WebSphere Application Server V5.1 Information Center*, available at:

<http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp>

It is assumed that you do not have WebSphere Application Server or a Web server, such as IBM HTTP Server, installed on this machine. The WebSphere Portal installation wizard will install and configure all the required components in order to have a base WebSphere Portal environment up and running.

**Important:** If you already have WebSphere Application Server installed, there are some steps you need to take before installing WebSphere Portal. Refer to the *WebSphere Portal V5.1 Information Center*, available at:

<http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/index.html>

Cloudscape will be used as a database repository until we move the data to a robust database server, such as IBM DB2 UDB Enterprise Server Edition.

To install WebSphere Portal, complete the following steps:

1. Check to see if you have met all the hardware and software requirements for WebSphere Portal. Refer to Chapter 2, “WebSphere Portal V5.1 planning and requirements” on page 25.
2. Insert the Setup disc and mount the CD-ROM file system. If you need more information about mounting a CD-ROM file system, refer to “Creating a CDROM file system” on page 377.

3. Run the installation script file by running the following command:  
`./install.sh`
4. Choose the language you want to use for the installation. Click **OK**.
5. Click **Next** on the Welcome window.
6. To continue, select **I accept the terms in the license agreement** and click **Next**.
7. Because it is assumed that you have not installed WebSphere Application Server, you should select the **Full** setup type, as shown in Figure 6-2. Click **Next**.

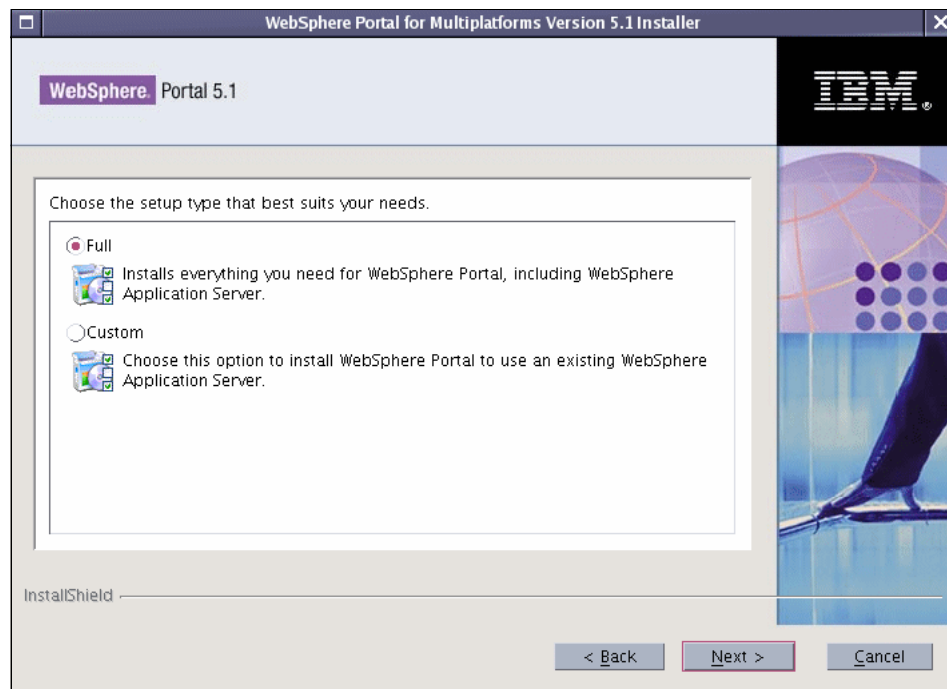


Figure 6-2 Select the Full installation type

8. Accept the default for the WebSphere Application Server directory or type in your own value (Figure 6-3). Click **Next**.

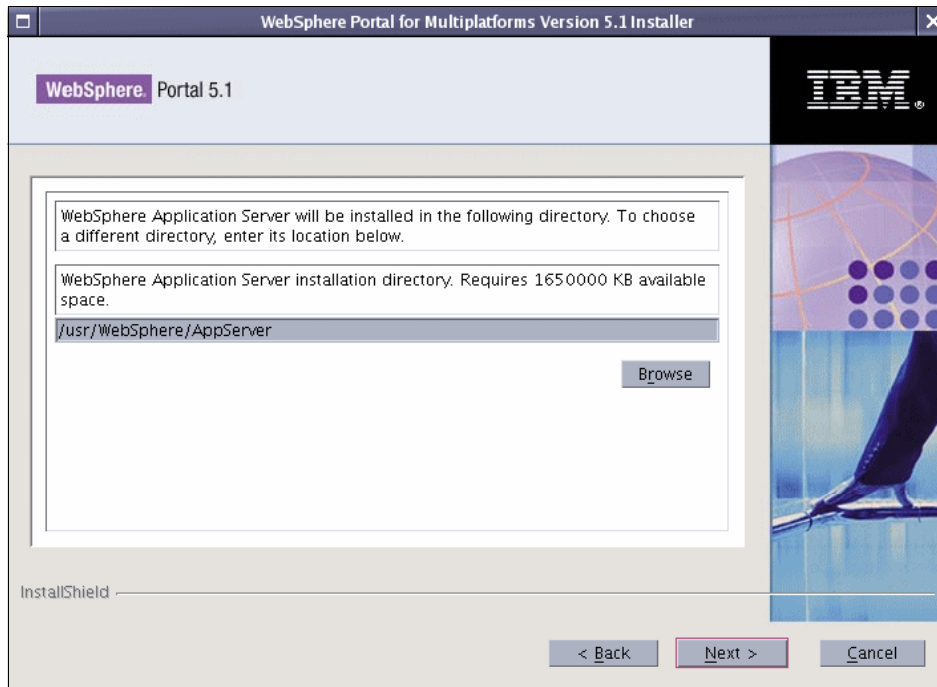
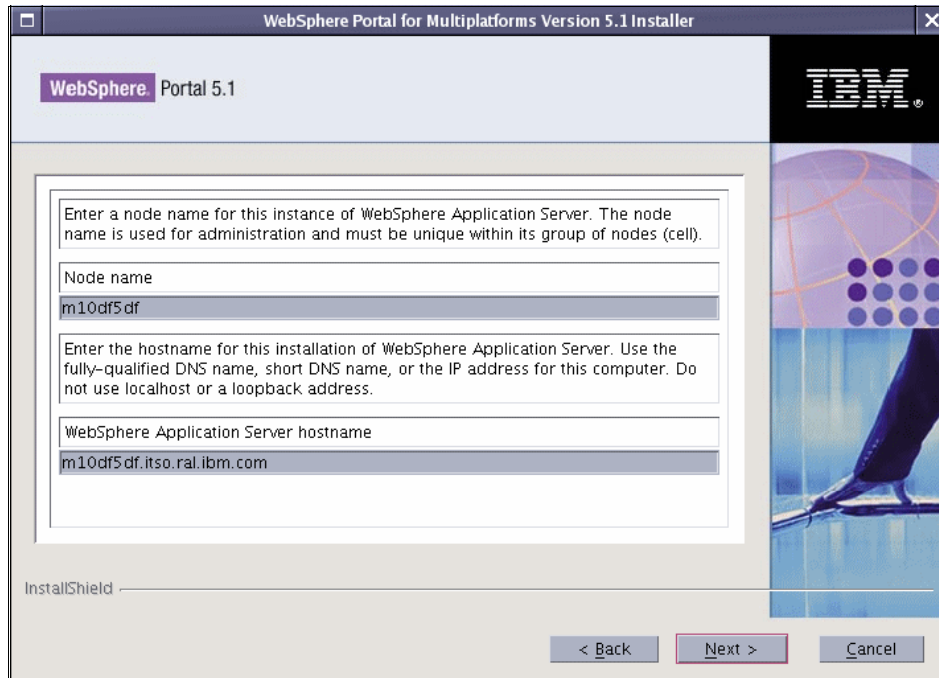


Figure 6-3 Enter a new installation directory or accept the default value

9. Type the node name and the fully qualified host name for the WebSphere Application Server, as shown in Figure 6-4 and click **Next**.

**Important:** When a host name is required, enter the fully qualified host name, that is, `hostname.domain.com`.



WebSphere Portal for Multiplatforms Version 5.1 Installer

WebSphere Portal 5.1

Enter a node name for this instance of WebSphere Application Server. The node name is used for administration and must be unique within its group of nodes (cell).

Node name  
m10df5df

Enter the hostname for this installation of WebSphere Application Server. Use the fully-qualified DNS name, short DNS name, or the IP address for this computer. Do not use localhost or a loopback address.

WebSphere Application Server hostname  
m10df5df.itso.ral.ibm.com

InstallShield

< Back   Next >   Cancel

Figure 6-4 Enter a node name and the fully qualified host name

10. Accept the default for the WebSphere Portal directory or type your own value (Figure 6-5) and click **Next**.

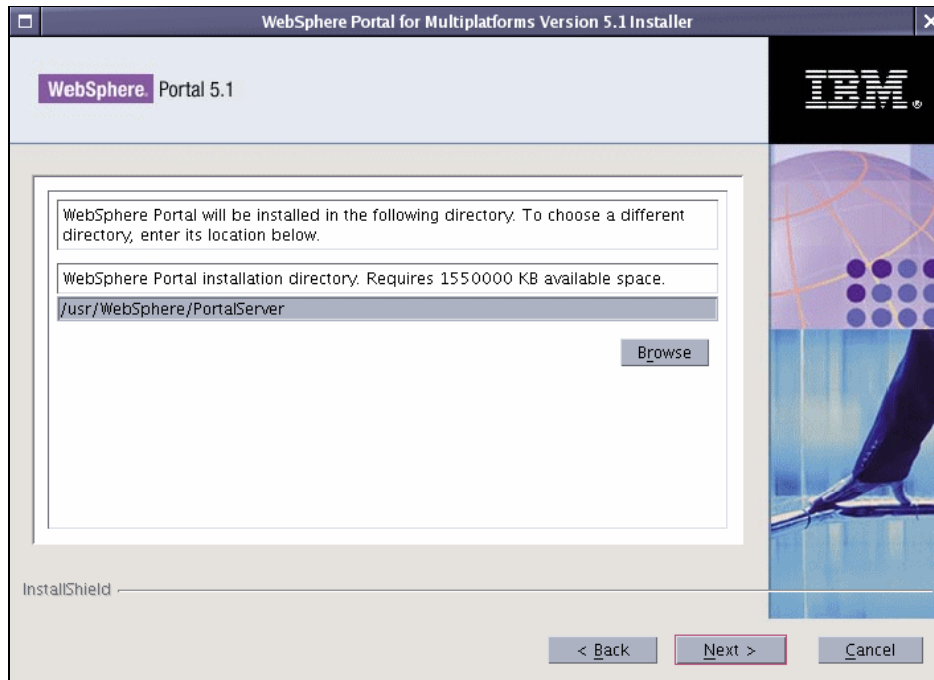


Figure 6-5 Enter a new installation directory or accept the default value

11. Enter `wpsadmin` for the Portal administrative user and the password; by default, the password value for this user is also `wpsadmin` (Figure 6-6). Click **Next**.

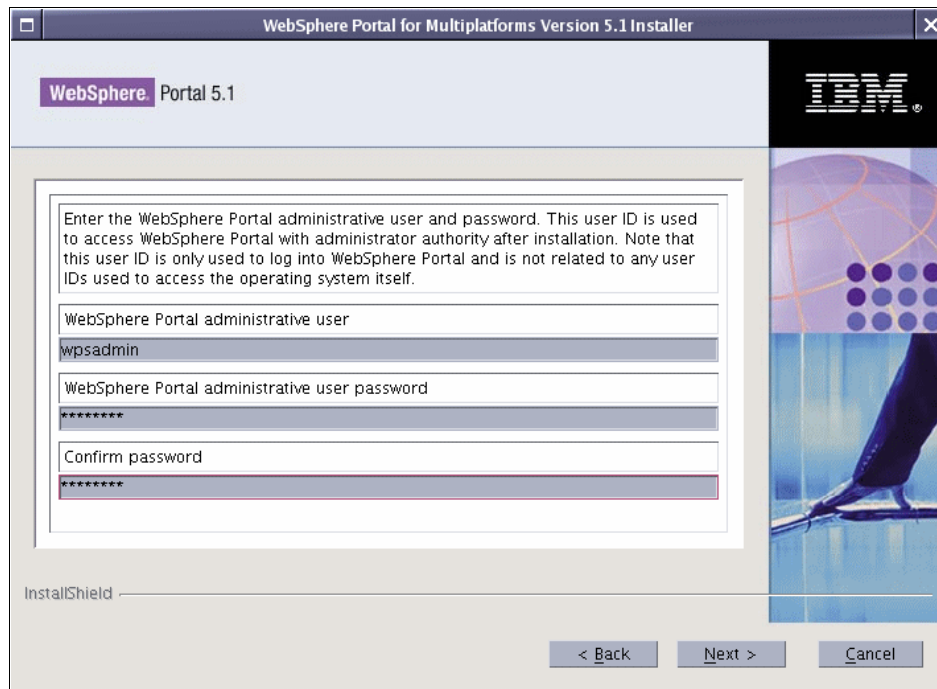


Figure 6-6 WebSphere Portal administrative user and password



12. Verify the components that will be installed (Figure 6-7) and click **Next**.

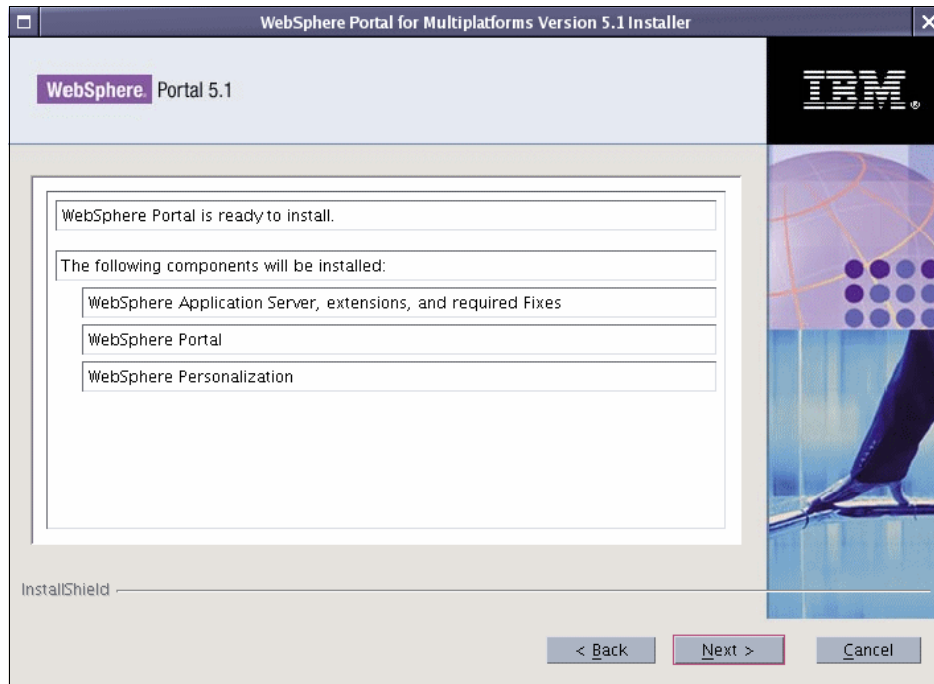


Figure 6-7 Components that will be installed

13. Later, you will be asked to insert the following discs to continue the installation:

- a. CD #1-5 (WebSphere Business Integration Server Foundation V5.1 for AIX)
- b. CD #4-3 (WebSphere Application Server V5.1 Archive Install for AIX)
- c. CD #5-2 (Portal Server V5.1 Archive Install for Linux/UNIX)
- d. CD #5-3 (Portal Server V5.1 Archive Install for Windows, AIX, Solaris, HP-UX, Linux zSeries, Linux Intel, Linux PowerPC)

**Tip:** Because the whole installation might take couple hours to complete, it is recommended that you copy the content of each disc to local machine for accelerating the installation. First, you need to create different directories, named cd<disc\_number>, and copy each disc content to its own directory. For example, the installation in this chapter will need these directories:

```
/tmp/cdSetup
/tmp/cd1-5
/tmp/cd4-3
/tmp/cd5-2
/tmp/cd5-3
```

Execute the install program under cdSetup path, and it will find the required source discs automatically.

14. Click **Finish** when you see the window shown in Figure 6-8.

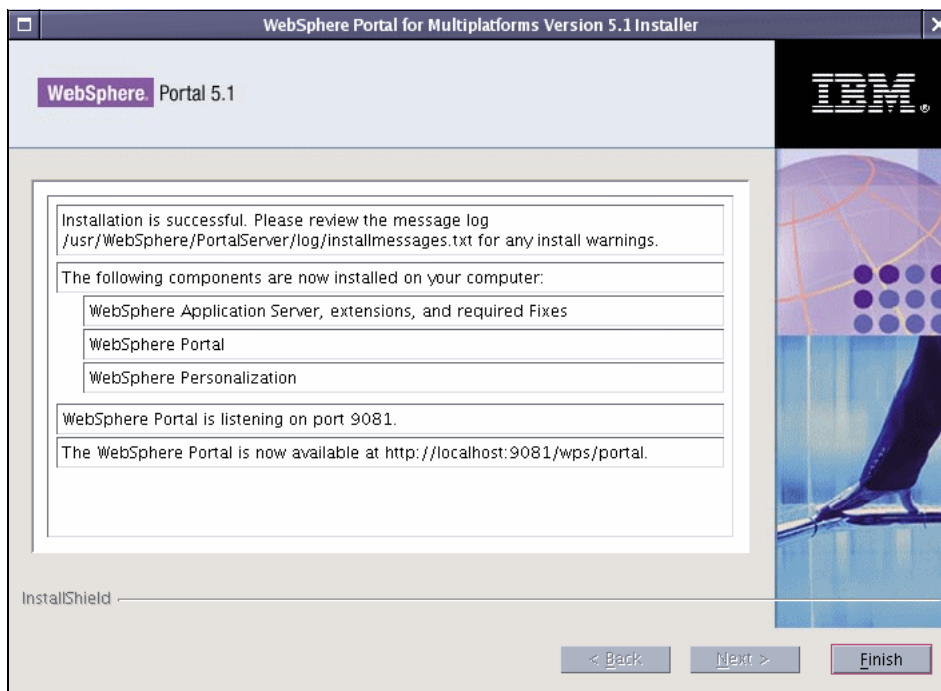


Figure 6-8 The installation is complete

15. Check to see if there is a error or warning message in the `/usr/WebSphere/PortalServer/log/installmessages.txt` file.

16. You can validate the installation by entering the following URL in a browser:

`http://<wps_hostname>:9081/wps/portal`

Where `<wps_hostname>` is the fully qualified host name for the WebSphere Portal machine.

You will see the WebSphere Portal Welcome page (Figure 6-9).

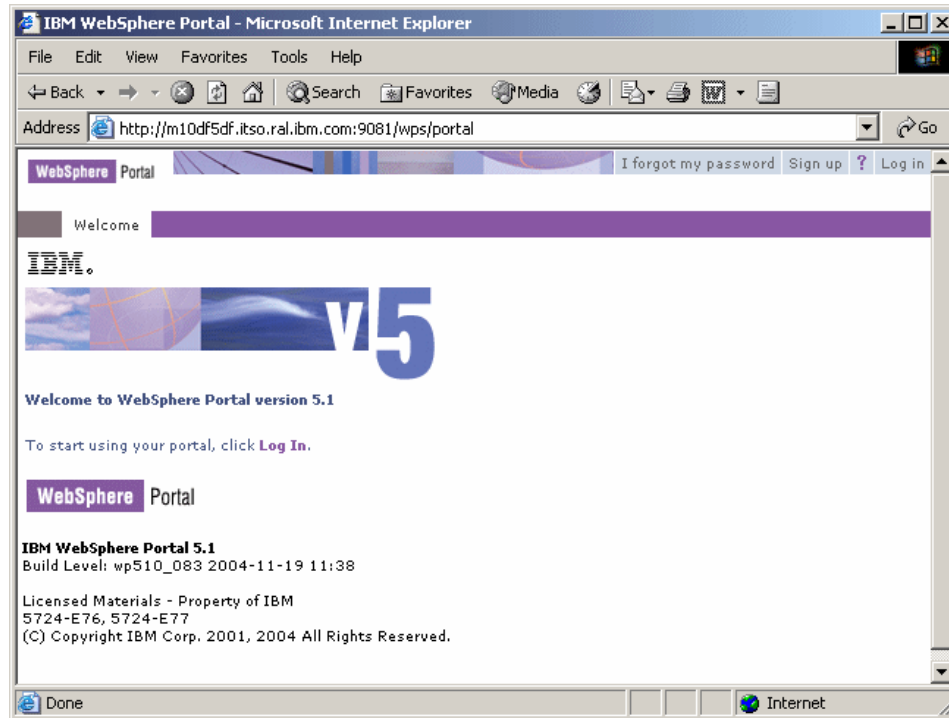


Figure 6-9 WebSphere Portal Welcome page

## 6.3 Installing a remote HTTP server

Installing the Web server on a separate machine can improve performance, security, and maintainability:

- ▶ **Performance:** The Web server and application server might require different machine sizes. The application server machine, for example, requires a more robust machine than the HTTP server.
- ▶ **Security:** You can create a secure demilitarized zone (DMZ) by putting a firewall between the Web server and the application server. This will protect your application from non-authorized access.

- **Maintainability:** The Web server can be reconfigured, replaced, or both without affecting the application server machine and vice versa.

In our scenario, we installed and configured IBM HTTP Server on a Microsoft Windows machine. This procedure can also be helpful for other platforms. Complete the following steps:

1. Insert the WebSphere Portal CD #1-1.
2. Run **Install.exe** from X:\win\WAS\ directory, where X is your CD-ROM drive.
3. When the installation wizard window opens, choose the language and click **OK**.
4. A Welcome window opens. Click **Next**.
5. On the Software License Agreement window, select **Accept** and click **Next**.
6. Select **Custom** on the Setup Type window. Click **Next**.
7. Select **IBM HTTP Server** and **Plug-in for IBM HTTP Server v1.3** for the Web server plug-ins *only*, as shown in Figure 6-10. Click **Next**.

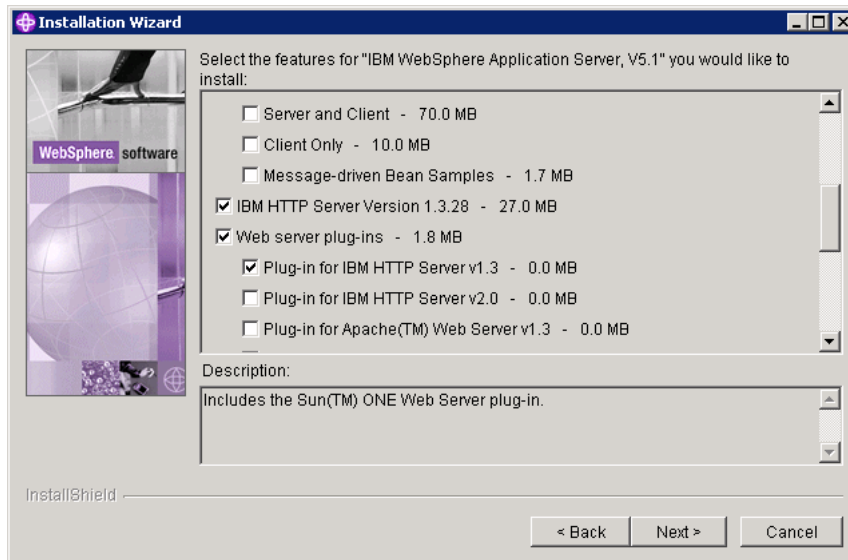


Figure 6-10 Selecting IBM HTTP Server components

8. Enter the path for the WebSphere Application Server plug-in and IBM HTTP Server or accept the defaults (see Figure 6-11). Click **Next**.

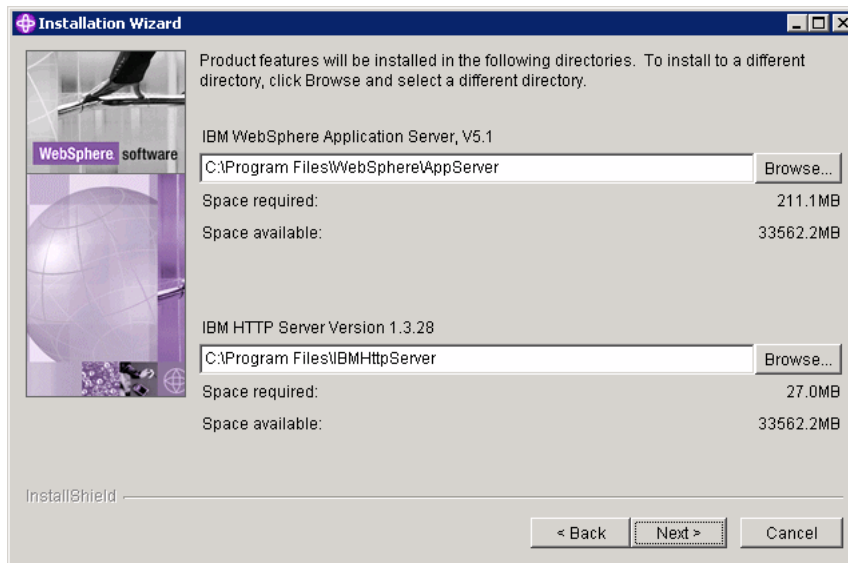


Figure 6-11 Enter the path for IBM HTTP Server and plug-in

9. Select the **Run IBM HTTP Server as a service** check box and type the user ID and password of the user account that will start the service. Click **Next**.

**Note:** If you chose to install IBM HTTP Server on Windows, you will probably get a warning window similar to the one shown in Figure 6-12. The installation will set the privileges for you, but you can also prevent this message by setting the required user rights *before* starting the installation.

You can assign or change user privileges by going to **Control Panel** → **Administrative Tools** → **Local Security Policy**. The HTTP user must have the following privileges:

- ▶ Act as part of the operating system
- ▶ Log on as a service



*Figure 6-12 The installation wizard will set the user rights for the user account*

10. Verify the components that will be installed. Click **Next**.

The installation process starts. Wait for this process to finish.

11. Select the Registration option if wanted. Click **Next**.

12. The installation has completed. Click **Finish**.

13. Reboot your machine.

14. Test that IBM HTTP Server is working properly by typing the following URL:

`http://localhost`

15. You will see the IBM HTTP Server Welcome page, as shown in Figure 6-13.



Figure 6-13 IBM HTTP Server Welcome page

## 6.4 Configuring the remote HTTP server

After installing WebSphere Portal and IBM HTTP Server, you must configure the plug-in configuration file located on the HTTP server machine.

In order to have WebSphere Application Server handle the requests that come from the remote HTTP server, follow the instructions in this section.

## 6.4.1 Configuring the plug-in

To verify that the plug-in was successfully installed on the remote Web server, complete the following steps:

1. Open the configuration file `<http_dir>/conf/httpd.conf`.

The following two lines must be present in the configuration file:

```
LoadModule ibm_app_server_http_module "C:\Program
Files\WebSphere\AppServer\bin\mod_ibm_app_server_http.dll"
WebSpherePluginConfig "C:\Program
Files\WebSphere\AppServer\config\cells\plugin-cfg.xml "
```

2. Start IBM HTTP Server.

## 6.4.2 Adding a new host alias

For testing purposes, you can work on WebSphere Portal without a Web server. This is possible because WebSphere Application Server has an embedded HTTP transport that takes care of that.

The default transport port for WebSphere Portal is 9081. As soon you install WebSphere Portal, you will be able to reach the WebSphere Portal Welcome page by entering the following URL:

```
http://<wps_hostname>:9081/wps/portal
```

The request is handled by the embedded HTTP server installed with WebSphere Application Server V5.1.

However, if you want your WebSphere Portal application to be accessible from the Internet, you have to configure WebSphere Portal to receive incoming requests from a Web server, generally listening on port 80. This can be done by adding the Web server fully qualified host name and the Web server port number to the virtual host that WebSphere Portal is using.

To add a new host alias to the default virtual host, complete the following steps:

1. Go to the WebSphere Portal machine and start WebSphere Application Server and WebSphere Portal:

```
#cd /usr/WebSphere/AppServer/bin
#./startServer.sh server1
#./startServer.sh WebSphere_Portal
```

2. Open the WebSphere Application Server administrative console by entering the following URL in a browser:

```
http://<wps_hostname>:9090/admin
```



Where <wps\_hostname> is the fully qualified host name of WebSphere Portal machine.

3. After logging in, expand **Environment** and select **Virtual Hosts**.
4. Click **default\_host**.
5. On the Additional Properties table, click the **Host Aliases** link.
6. Click **New** to add a host name and a port number.
7. Enter the fully qualified Host Name of the HTTP server machine and Port 80, as shown in Figure 6-14.

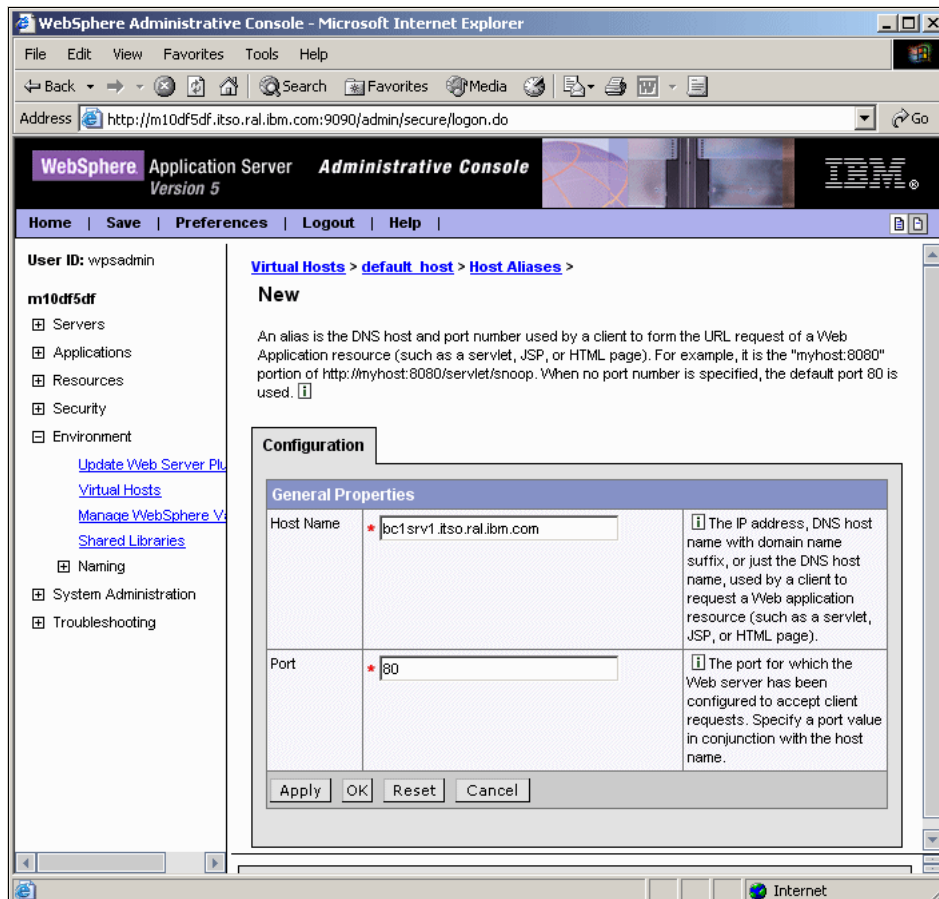


Figure 6-14 Add a new Host Alias

8. Click **OK**.
9. Click the **Save** link to save your configuration.

10. Click the **Save** button to save the changes to the master configuration.

### 6.4.3 Updating and copying the Web server plug-in configuration

The plug-in configuration file is an XML file located in each WebSphere Application Server machine. In a single machine installation, the Web server and WebSphere Application Server have access to the same plug-in file. However, for a remote Web server, you need to manually copy the plug-in file from the WebSphere Application Server machine to the HTTP server machine.

This section gives you instructions to update, copy, and correct the plug-in file.

To regenerate and copy the plug-in configuration file, complete the following steps:

1. Open the administrative console, expand **Environment**, and select **Update Web Server Plugin**.
2. Click **OK** to regenerate the plug-in configuration file.
3. Copy the `plug-in-cfg.xml` file from the machine where you installed WebSphere Portal to the Web server machine. This file is located in the `<was_root>/config/cells` directory.

**Important:** If your Web server is on Windows and WebSphere Portal on UNIX, as in this example, there is an extra step that you have to take before restarting the Web server.

On the Web server machine, open the `<was_root>/config/cells/plugin-cfg.xml` file and change *all* the lines that contain a UNIX formatted path to a Windows format. Otherwise, you will get an error when trying to start HTTP server service.

For example, change:

```
/usr/WebSphere/AppServer/logs/http_plugin.log
```

To:

```
X:\Program Files\WebSphere\AppServer\logs\http_plugin.log
```

4. Restart the IBM HTTP Server service.
5. Test whether the plug-in is functional by entering the following URLs in a browser:

```
http://<http_server_hostname>/snoop
http://<http_server_hostname>/wps/portal
```

This means that WebSphere Application Server is handling the requests that are coming from the remote HTTP server machine through the plug-in.

#### 6.4.4 Disabling access to port 9081 (optional)

As mentioned earlier, WebSphere Portal uses port 9081 by default. If you followed the steps in 6.4, “Configuring the remote HTTP server” on page 273, you already have the WebSphere Portal application receiving incoming requests from a remote Web server.

Therefore, you might want to disable access to port 9081. To disable access to port 9081, complete the following steps:

1. On the WebSphere Portal machine, make a backup of the file `/usr/WebSphere/PortalServer/config/wpconfig.properties` and open it.
2. Locate and change the following line:

```
WpsHostPort=9081
```

To:

```
WpsHostPort=80
```

3. Save the properties file.
4. This change will take effect after running the following command:  

```
#!/WPSconfig.sh httpserver-config
```
5. Open the WebSphere Application Server administrative console, expand **Environment** and select **Virtual Hosts**.
6. Click **default\_host**.
7. On the Additional Properties table, click the **Host Aliases** link.
8. Select the line that contains port 9081.
9. Click **Delete**.
10. Click **Save** at the top of the window.
11. Click the **Save** button to save to the master configuration.
12. Follow the steps in 6.4.3, “Updating and copying the Web server plug-in configuration” on page 276.
13. Restart server1.
14. Restart the WebSphere Portal application.

## 6.5 Installing and configuring DB2 UDB Enterprise Server Edition

This section describes the procedure of exporting the data from the Cloudscape database and importing it to a more powerful database server.

Separating the database server from the application server can improve performance and maintainability and provide high-availability:

- ▶ **Performance:** Keeping the database server in a different machine than the application server provides less competition for the machine resources and allows the appropriate tuning configuration for each product.
- ▶ **Maintainability:** Components can be reconfigured, replaced, or both without affecting the application server.
- ▶ **High-Availability:** This provides multiple database servers with common access to the application data, which reduces the chance of a single point of failure.

As previously described, we are running IBM DB2 UDB Enterprise Server Edition as the database server. These instructions will help you install and configure it. If you intend to use a database server other than DB2, refer to *WebSphere Portal V5.1 Information Center*.

### 6.5.1 Installing IBM DB2 UDB Enterprise Server

This section guides you through the installation of IBM DB2 UDB Enterprise Server Edition V8.1 on AIX 5L Version 5.2.

Refer to Chapter 2, “WebSphere Portal V5.1 planning and requirements” on page 25 for more information about what is supported on WebSphere Portal V5.1.

To start the DB2 UDB Enterprise Server Edition installation, complete the following steps:

1. Insert the CD #9-4 (DB2 UDB Enterprise Server Edition V8.1 for AIX - SBCS). Mount the /cdrom file system.
2. Run the DB2 setup program:

```
#cd /cdrom/ese.sbcs
#./db2setup
```

**Important:** Do *not* execute the db2\_install program unless you want to install DB2 manually. For more information about the manual installation, refer to *DB2 UDB V8 Information Center*, available at:

<http://publib.boulder.ibm.com/infocenter/db2help/index.jsp>

3. The IBM DB2 Setup window opens. Select **Install Products**.
4. Select **DB2 UDB Enterprise Server Edition**. Click **Next**.
5. The Welcome Setup wizard window opens. Click **Next**.
6. Select **Accept** if you agree to the license terms. Click **Next**.
7. Select **Typical** as the installation type (Figure 6-15). Click **Next**.

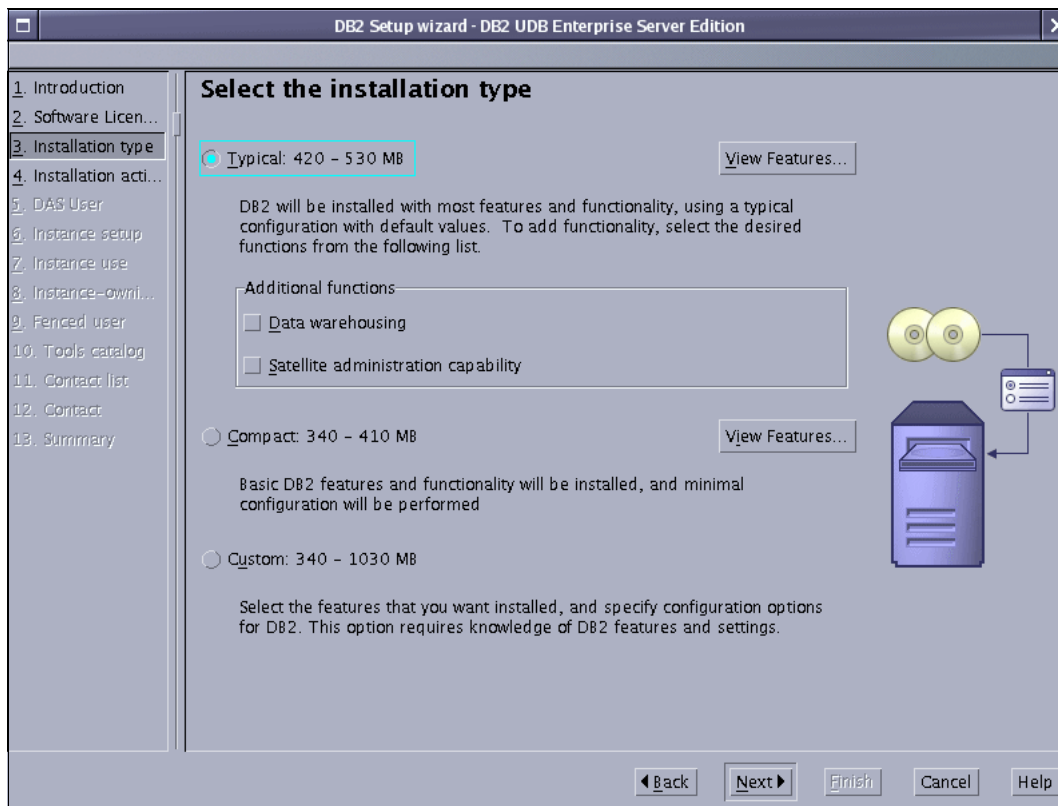


Figure 6-15 Select the installation type

**Note:** Table 6-2 lists the default users and groups that will be automatically created by DB2 UDB V8.1 Setup program. You can change these names or choose existing users and groups later during the installation if you want.

*Table 6-2 Default users and groups required by DB2*

User role	Default user name	Default group name
DB2 administration server user	dasusr1	dasadm1
DB2 fenced user	db2fenc1	db2fgrp1
DB2 instance owner	db2inst1	db2grp1

8. Select **Install DB2 UDB Enterprise Server Edition on this computer**. Click **Next**.
9. The installation wizard will create a user and a group that will run the DB2 Administration Server. You can use the same values or choose your own. Click **Next**.

10. Accept the default **Create a DB2 instance - 32 bit** (Figure 6-16). Click **Next**.

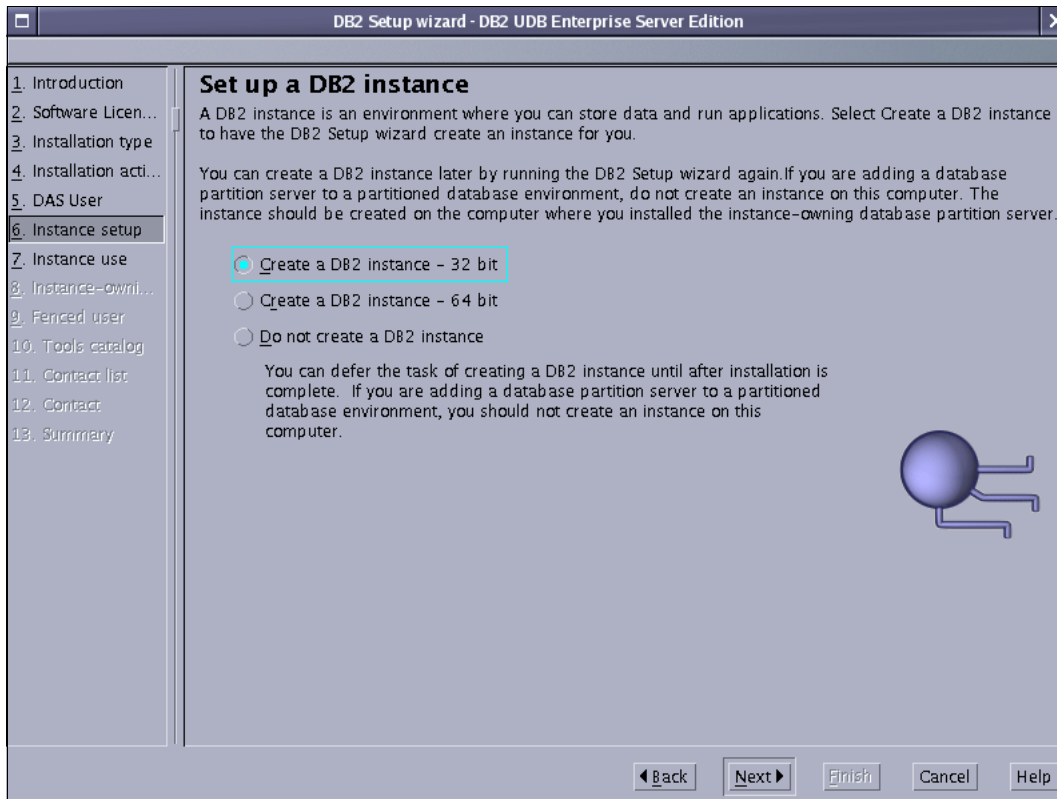


Figure 6-16 Creating the DB2 administrative user

11. Select **Single-partition instance**. Click **Next**.

12. The installation wizard will create a user and a group that will be the DB2 instance owner. Use the default values, as shown in Figure 6-17, or use your own values. Click **Next**.

**DB2 Setup wizard - DB2 UDB Enterprise Server Edition**

**Set user information for the DB2 instance owner**

Specify the instance-owning user information for the DB2 instance. DB2 will use this user to perform instance functions, and will store instance information in the user's home directory. The name of the instance will be the same as the user name. You can create a new user or use an existing one.

**New user**

User name:

UID:   Use default UID

Group name:

GID:   Use default GID

Password:

Confirm password:

Home directory:  ...

Existing user

User name:  ...

For users of NIS or similar management systems—  
If the user information in your environment is managed remotely by NIS or a similar system, you must specify an existing user.

◀ Back   Next ▶   Finish   Cancel   Help

Figure 6-17 Creating the DB2 instance owner

13. You can accept the default for the DB2 fenced user or enter the user name and group name you want. Type the password and click **Next**.
14. Select **Do not prepare the DB2 tools catalog on this computer**. Click **Next**.



15. Accept the default for the contact list information and enter the SMTP server name if you are using this feature. Click **Next**.

**Important:** For the purpose of this book, we do *not* enable the SMTP server notification, as shown in Figure 6-18. If the SMTP server field is not enabled, you will get a warning dialog box. Click **OK** to proceed.

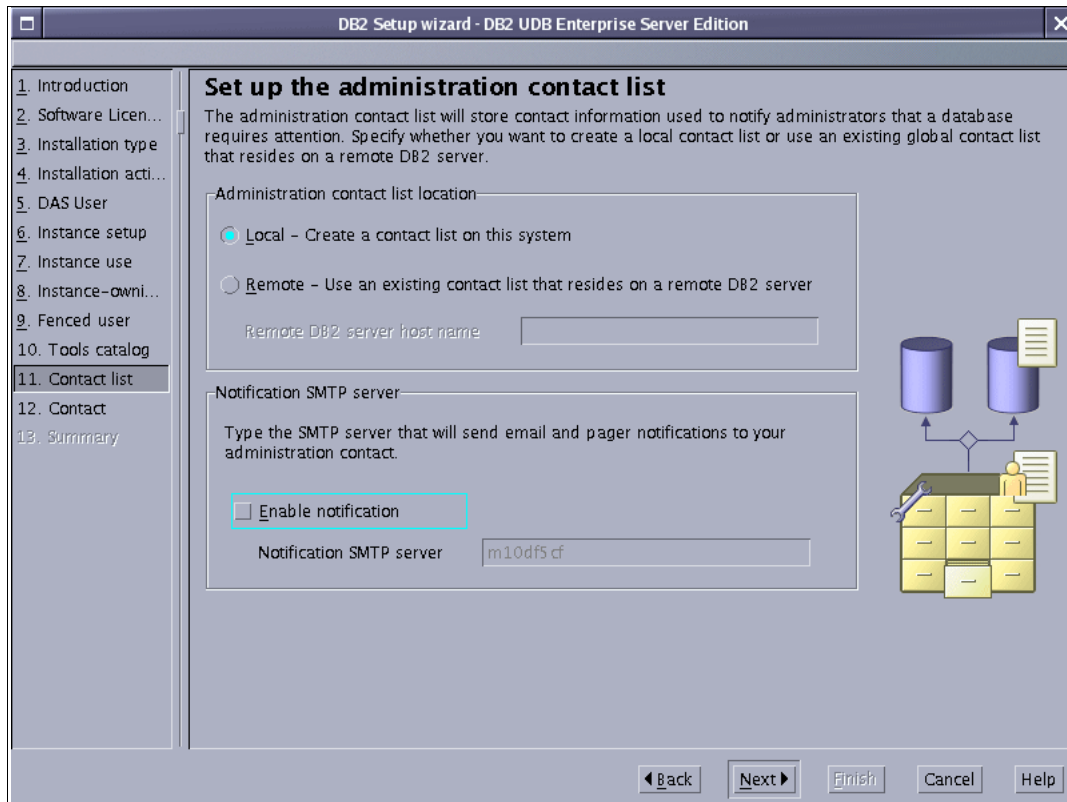


Figure 6-18 The administration contact list

16. Select the desired option for the health monitor notification. Click **Next**.
17. Verify the information displayed in the summary. Click **Finish** to complete the installation.
18. A window opens and displays the overall progress. Wait for this process to finish.

19. To confirm the success of the installation, a Status report window opens. Confirm that all tasks have a Success status (see Figure 6-19) and click **Finish**.

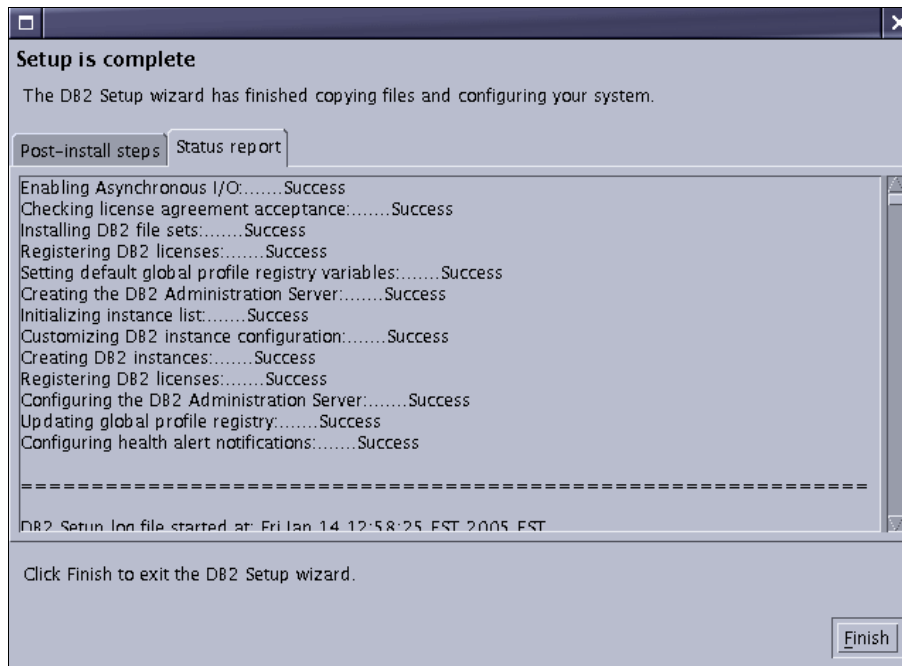


Figure 6-19 Status report window

## 6.5.2 Installing the IBM DB2 fix pack

WebSphere Portal V5.1 requires IBM DB2 Universal Database Enterprise Server Edition V8.1 Fix Pack 6. We recommend that you first read FixPackReadme.txt in the Fix Pack disc before you install DB2 Fix Pack 6.

**Note:** At this time, there are probably newer DB2 fix packs available. To avoid any unexpected problems, we strongly recommend that you install the latest DB2 fix pack instead of Fix Pack 6. To download the DB2 UDB V8 fix packs, visit the following site:

<http://www.ibm.com/software/data/db2/udb/support/downloadv8.html>

After installing DB2 UDB Enterprise Server Edition V8.1, to install IBM DB2 Fix Pack 6 on IBM DB2 UDB Enterprise Server, complete the following steps:

1. Stop the DB2 instance by running the following command:

```
#su - db2inst1
$db2 force applications all
$db2 terminate
$db2stop
$db2licd -end
$exit
```

2. Stop the DB2 Administration Server:

```
#su - dasusr1
$db2admin stop
$exit
```

3. On AIX, you should run the **slibclean** command to unload unused shared libraries from memory:

```
#su - root
#/usr/sbin/slibclean
```

4. Stop the DB2 Fault Monitor daemon and Fault Monitor Coordinator daemon:

```
#su - root
#cd /usr/opt/db2_08_01/bin
#./db2fmcu -d
#kill -9 <the pid of db2fmd>
```

5. Insert CD #9-12 (DB2 UDB Enterprise Server Edition V8.1 Fix Pack 6 for AIX - SBCS) and mount it on /cdrom.

**Important:** The DB2 UDB Enterprise Server Edition V8.1 Fix Pack 6 for AIX in the WebSphere Portal V5.1 package is an *Alternate FixPack* that allows multiple levels of DB2 to coexist in the same operating system. By default, the installation path of the Alternative FixPack in the AIX operating system:

```
/usr/opt/db2_08_FPn
```

Where n refers to the fix pack level.

Another kind of fix pack is called *Regular FixPack*, and it is always installed directly on top of the existing installation path:

```
/usr/opt/db2_08_01
```

For more information about the Regular FixPack and Alternate FixPack, refer to *DB2 UDB V8 Information Center*, available at:

<http://publib.boulder.ibm.com/infocenter/db2help/index.jsp>

All Regular FixPacks and Alternative FixPacks can be downloaded from *DB2 UDB V8 support site*:

<http://www.ibm.com/software/data/db2/udb/support/downloadv8.html>

6. Run `/cdrom/ese.mfp.sbcs/installAltFixPak` using the root user.  
When this completes, verify that all the filesets have a SUCCESS status.

7. Update the DB2 instances to use the new fix level:

- a. Log on as root.

- b. Run the following command to update DB2 instance:

```
<db2_fp_dir>/instance/db2iupdt <instance_name>
```

Where `<db2_fp_dir>` is your installation path of DB2 Fix Pack 6, and `<instance_name>` is your DB2 instance name.

For example:

```
/usr/opt/db2_08_FP6/instance/db2iupdt db2inst1
```

**Note:** If you have more than one DB2 instance, run this command for each instance.

8. Update the DB2 Administration Server instance:
  - a. Log on as root.

- b. Run the following command to update DAS instance:

```
<db2_fp_dir>/instance/dasupdt <das_instance_name>
```

Where <db2\_fp\_dir> is your installation path of DB2 Fix Pack 6, and <das\_instance\_name> is your DB2 Administration Server instance name.

For example:

```
/usr/opt/db2_08_FP6/instance/dasupdt dasusr1
```

9. Start the DB2 instance:

```
#su - db2inst1
$db2start
```

10. You must wait for the following success message:

```
SQL1063N DB2START processing was successful.
```

11. Enter the **db2level** command. It will give you the complete version of DB2. After the Fix Pack 1 installation, you will see the following output:

```
DB21085I Instance "db2inst1" uses "32" bits and DB2 code release
"SQL08016" with level identifier "02070106".
Informational tokens are "DB2 v8.1.1.56", "s040616", "U497635", and FixPak
"6".
Product is installed at "/usr/opt/db2_08_FP6".
```

### 6.5.3 Installing IBM DB2 Administration Client

This architecture requires you to install the DB2 Administration Client on the same machine where WebSphere Portal was installed.

This section describes how to install the IBM DB2 Administration Client installation.

**Important:** When creating the client instance, be sure that you are using the same name used in the server instance, for example, db2inst1.

Complete the following steps:

1. Create a user named db2inst1 and a group named db2grp1. Refer to Appendix C, "Creating users on AIX" on page 379.
2. Insert CD#9-4 (DB2 UDB Enterprise Server Edition V8.1 for AIX - SBCS) and mount it on /cdrom.
3. Go to the /cdrom/ese.sbc/ directory.
4. Run the command line installation script:

```
./db2_install
```

5. Enter `DB2.ADMCL` to install DB2 Administration Client. Wait for the process to finish.

6. Verify that the installation has a SUCCESS status.

7. Go to the `/usr/opt/db2_08_01/instance` directory.

8. Run the following command to create the DB2 instance:

```
./db2icrt -u db2inst1 db2inst1
```

9. Verify that the instance was created successfully by entering the following command:

```
#su - db2inst1
$db2level
```

### Installing Fix Pack 6 on DB2 Administration Client

The DB2 Administration Client must be at the same level as the DB2 UDB Enterprise Server machine. In this example, the version of DB2 UDB Enterprise Server Edition is V8.1 with Fix Pack 6. Therefore, you must install Fix Pack 6 on the client machine as well. Complete the following steps:

1. Stop all products that might be using the DB2 database.
2. Insert CD #9-12 (DB2 UDB Enterprise Server Edition V8.1 Fix Pack 6 for AIX - SBCS) and mount on it `/cdrom`.

3. Run `/cdrom/ese.mfp.sbc/install1AltFixPak` using the root user.

When this completes, verify that all the filesets have a SUCCESS status.

4. Update the DB2 client instance to use the new fix level:

a. Log on as root.

b. Run the following command to update the DB2 instance:

```
<db2_fp_dir>/instance/db2iupdt <instance_name>
```

Where `<db2_fp_dir>` is your installation path of DB2 Fix Pack 6, and `<instance_name>` is your DB2 instance name.

For example:

```
/usr/opt/db2_08_FP6/instance/db2iupdt db2inst1
```

5. You can check the DB2 instance by entering the `db2level` command. The following output came from a DB2 client on an AIX machine.

```
DB21085I Instance "db2inst1" uses "32" bits and DB2 code release
"SQL08016" with level identifier "02070106".
Informational tokens are "DB2 v8.1.1.58", "s040914", "U800265", and FixPak
"6".
Product is installed at "/usr/opt/db2_08_FP6".
```

## 6.5.4 Creating remote databases

This section describes how to create the required databases for WebSphere Portal on a remote DB2 UDB Enterprise Server machine. This example creates four databases, as shown in Table 6-3.

Table 6-3 Databases and functions

Database	Function
WPS51	Used for WebSphere Portal and Member Manager (at a minimum) or to hold all data. Stores information about user customizations, such as pages, the user profile, and login information.
JCR51	Used by Document Manager and Personalization components. Contains documents, Personalization rules, Personalization campaigns, and document library configuration information.
FDBK51	Used by Feedback components. Contains the information that is logged by your Web site for generating reports for analysis of site activity.
LM51	Used for LikeMinds data. Contains the recommendations to be displayed to users when their interactions with your Web site have been analyzed and predictions generated.

As you see in Table 6-3, WebSphere Portal and Member Manager information will be stored in the same database. You can create a different database for Member Manager. Or, you can simply create a single database to hold all the data required by the Document Manager, Personalization, Feedback, and LikeMinds components. In this example, we separate all the information into different databases except Member Manager information.

To create the databases, log in as the DB2 instance owner and run the appropriate **db2** commands to create and update the database configurations, as shown in Example 6-1.

Example 6-1 Create and update database configurations

```
#su - db2inst1
$db2 "create database wps51 using codeset UTF-8 territory us"
$db2 "update database configuration for wps51 using applheapsz 16384
app_ct1_heap_sz 8192"
$db2 "update database configuration for wps51 using stmtheap 60000"
$db2 "update database configuration for wps51 using locklist 400"
$db2 "update database configuration for wps51 using indexrec RESTART"
$db2 "update database configuration for wps51 using logfilsiz 1000"
$db2 "update database configuration for wps51 using logprimary 12"
$db2 "update database configuration for wps51 using logsecond 10"
$db2set DB2_RR_TO_RS=yes
$db2set DB2_EVALUNCOMMITTED=YES
```

```

$db2set DB2_INLIST_TO_NLJN=YES

$db2 "create database fdbk51 using codeset UTF-8 territory us collate using
identity"
$db2 "update database configuration for fdbk51 using applheapsz 5120"
$db2 "update database configuration for fdbk51 using logfilsiz 4096"
$db2 "update database configuration for fdbk51 using logprimary 4"
$db2 "update database configuration for fdbk51 using logsecond 25"

$db2 "create database lm51 using codeset UTF-8 territory us"

$db2 "create database jcr51 using codeset UTF-8 territory us"
$db2 "update database manager configuration using QUERY_HEAP_SZ 32768"
$db2 "update database manager configuration using UDF_MEM_SZ 7000"
$db2 "update database manager configuration using SHEAPTHRES 10000"
$db2 "update database manager configuration using MAXAGENTS 500"
$db2 "update database manager configuration using DFT_MON_TIMESTAMP OFF"
$db2 "update database configuration for jcr51 using LOCKTIMEOUT 30"
$db2 "update database configuration for jcr51 using LOCKLIST 1000"
$db2 "update database configuration for jcr51 using STMTHEAP 16384"
$db2 "update database configuration for jcr51 using AVG_APPLS 5"
$db2 "update database configuration for jcr51 using SORTHEAP 256"
$db2 "update database configuration for jcr51 using LOGPRIMARY 10"
$db2 "update database configuration for jcr51 using LOGFILSIZ 1000"
$db2 "update database configuration for jcr51 using LOGSECOND 20"
$db2 "update database configuration for jcr51 using LOGBUFSZ 32"
$db2 "update database configuration for jcr51 using MAXAPPLS 200"
$db2 "update database configuration for jcr51 using APPLHEAPSZ 4096"
$db2 "update database configuration for jcr51 using DFT_QUERYOPT 2"
$db2 "update database configuration for jcr51 using DBHEAP 2400"
$db2 "update database configuration for jcr51 using APP_CTL_HEAP_SZ 20000"
$db2 "connect to jcr51"
$db2 "create bufferpool ICMLSFREQBP4 SIZE 1000 PAGESIZE 4 K"
$db2 "create bufferpool ICMLSVOLATILEBP4 SIZE 8000 PAGESIZE 4 K"
$db2 "create bufferpool ICMLSMAINBP32 SIZE 8000 PAGESIZE 32 K"
$db2 "create bufferpool CMBMAIN4 SIZE 1000 PAGESIZE 4 K"
$db2 "create bufferpool OBJECTPOOL SIZE 2000 PAGESIZE 32 K"
$db2 "create bufferpool OBJPARTSPOOL SIZE 200 PAGESIZE 32 K"
$db2 "create bufferpool SMSPOOL SIZE 500 PAGESIZE 4 K"
$db2 "create bufferpool PARTSPOOL SIZE 100 PAGESIZE 32 K"
$db2 "create bufferpool BLOBPOOL SIZE 1000 PAGESIZE 32 K"
$db2 "create bufferpool REPLICAPool SIZE 1000 PAGESIZE 32 K"
$db2 "create bufferpool TRACKINGPOOL SIZE 250 PAGESIZE 4 K"
$db2 "create bufferpool VALIDATEPOOL SIZE 500 PAGESIZE 32 K"
$db2 "create regular tablespace ICMLFQ32 PAGESIZE 32 K managed by system using
('ICMLFQ32') bufferpool ICMLSMAINBP32"
$db2 "create regular tablespace ICMLNF32 PAGESIZE 32 K managed by system using
('ICMLNF32') bufferpool ICMLSMAINBP32"

```



```

$db2 "create regular tablespace ICMVFQ04 PAGESIZE 4 K managed by system using
('ICMVFQ04') bufferpool ICMLSVOLATILEBP4"
$db2 "create regular tablespace ICMSFQ04 PAGESIZE 4 K managed by system using
('ICMSFQ04') bufferpool ICMLSFREQBP4"
$db2 "create regular tablespace CMBINV04 PAGESIZE 4 K managed by system using
('CMBINV04') bufferpool CMBMAIN4"
$db2 "create system temporary tablespace ICMLSSYSTSPACE32 PAGESIZE 32 K managed
by system using ('icmlssystspace32') bufferpool ICMLSMAINBP32"
$db2 "create system temporary tablespace ICMLSSYSTSPACE4 PAGESIZE 4 K managed
by system using ('icmlssystspace4') bufferpool ICMLSVOLATILEBP4"
$db2 "create regular tablespace OBJECTS PAGESIZE 32 K managed by system using
('objects') bufferpool OBJECTPOOL"
$db2 "create regular tablespace OBJPARTS PAGESIZE 32 K managed by system using
('objparts') bufferpool OBJPARTSPOOL"
$db2 "create regular tablespace SMS PAGESIZE 4 K managed by system using
('sms') bufferpool SMSPOOL"
$db2 "create regular tablespace BLOBS PAGESIZE 32 K managed by system using
('blobs') bufferpool BLOBPOOL"
$db2 "create regular tablespace REPLICAS PAGESIZE 32 K managed by system using
('replicas') bufferpool REPLICAPool"
$db2 "create regular tablespace TRACKING PAGESIZE 4 K managed by system using
('tracking') bufferpool TRACKINGPOOL"
$db2 "create regular tablespace VALIDATEITM PAGESIZE 32 K managed by system
using ('validateitm') bufferpool VALIDATEPOOL"
$db2 disconnect jcr51
$db2 TERMINATE

```

---

## 6.5.5 Configuring the connection to remote databases

In order for WebSphere Portal to be able to connect to the databases, you need to perform the configurations provided in this section.

### Changes to perform on the DB2 server machine

Some of following steps might have been automatically configured by the DB2 UDB setup program if you executed the db2setup program. We recommend that you check these configuration values again.

Complete the following steps:

1. Edit the /etc/services file. Verify that the DB2 service port numbers were included in this file, and if they were not, add them:

```

DB2_db2inst1 60000/tcp # DB2 connection service port
DB2i_db2inst1 60001/tcp # DB2 interrupt service port

```

2. Save and close the file.

3. Log in as the DB2 instance owner and update the Service Name configuration:

```
#su - db2inst1
$db2 UPDATE DBM CFG USING svcename DB2_db2inst1
```

Where DB2\_db2inst1 is the service name added into services file above.

4. Set the DB2COMM variable to use TCP/IP:

```
$db2set DB2COMM=TCPIP
```

## Changes to perform on the DB2 client machine

Before you continue with the following steps, make sure that the DB2 instance on the server machine is running. Complete the following steps:

1. Edit the /etc/services file and add the DB2 connection service port:

```
DB2_db2inst1 60000/tcp # DB2 connection service port
```

**Note:** You *must* use the same service name and port number on the DB2 server machine.

2. Save and close the file.
3. Set the DB2COMM variable to use TCP/IP:

```
#su - db2inst1
$db2set DB2COMM=TCPIP
```

4. Catalog the node name with the DB2 server IP address and service name:

```
#su - db2inst1
$db2 catalog tcpip node <node_name> remote <db2_server_hostname> server
<service_name>
```

Where <node\_name> is the value you define for the DB2 server machine remote information, <db2\_server\_hostname> is the fully qualified host name *or* IP address of the DB2 server machine, and <service\_name> is the value you specified in step 1, as shown in Example 6-2.

### Example 6-2 Catalog node

---

```
$db2 catalog tcpip node WPSNODE remote db2.itso.ral.ibm.com server DB2_db2inst1
```

---

5. Catalog the remote databases created on the DB2 server machine using the node name that was created in step 4:

```
#su - db2inst1
$db2 catalog database <wps_db_name> as <wps_db_name_alias> at node
<node_name>
$db2 catalog database <jcr_db_name> as <jcr_db_name_alias> at node
<node_name>
```

```
$db2 catalog database <fdbk_db_name> as <fdbk_db_name_alias> at node
<node_name>
$db2 catalog database <lm_db_name> as <lm_db_name_alias> at node
<node_name>
```

Where <wps\_db\_name>, <jcr\_db\_name>, <fdbk\_db\_name>, and <lm\_db\_name> are the WebSphere Portal and WebSphere Portal content publishing database names you used when you created them on the database server machine, and <wps\_db\_name\_alias>, <jcr\_db\_name\_alias>, <fdbk\_db\_name\_alias>, and <lm\_db\_name\_alias> are the values that you are defining for database names on the client machine. See Example 6-3.

*Example 6-3 Catalog database*

---

```
$db2 catalog database WPS51 as WPS51N at node WPSNODE
$db2 catalog database JCR51 as JCR51N at node WPSNODE
$db2 catalog database FDBK51 as FDBK51N at node WPSNODE
$db2 catalog database LM51 as LM51N at node WPSNODE
```

---

**Note:** If you have created a database for Member Manager separate from WebSphere Portal, you will also have to catalog the Member Manager database.

6. Test the connection to the databases:

```
#su - db2inst1
$db2 connect to <wps_db_name_alias> user <db2_user> using <db2_password>
$db2 connect to <jcr_db_name_alias> user <db2_user> using <db2_password>
$db2 connect to <fdbk_db_name_alias> user <db2_user> using <db2_password>
$db2 connect to <lm_db_name_alias> user <db2_user> using <db2_password>
```

Where <wps\_db\_name\_alias>, <jcr\_db\_name\_alias>, <fdbk\_db\_name\_alias>, and <lm\_db\_name\_alias> are the values you used in step 5 on page 292, <db2\_user> is the user name with rights to connect to this database, and <db2\_password> is the password for the user name you are defining. See Example 6-4.

*Example 6-4 Connecting to the database*

---

```
$db2 connect to WPS51N user db2inst1 using password
$db2 connect to JCR51N user db2inst1 using password
$db2 connect to FDBK51N user db2inst1 using password
$db2 connect to LM51N user db2inst1 using password
```

---

## 6.5.6 Transferring data to the DB2 database

WebSphere Portal 5.1 uses Cloudscape as a database, so it does not require you to have DB2 UDB Enterprise Server, Oracle, Informix, or SQL Server up and running at this time.

For a production architecture, we *strongly* recommend moving all data to a powerful database server such as DB2 UDB Enterprise Server Edition.

In WebSphere Portal V5.1, all configuration information is stored in the `wpconfig.properties` file. In order to have the database transferred, we need to change the appropriate values into this file and use the `WPSconfig` script to execute the changes. To move the data from Cloudscape to DB2 UDB Enterprise Server database, complete the following steps:

1. Give the user `root` the privilege to run DB2 commands:
  - a. Open the `/usr/WebSphere/AppServer/bin/setupCmdLine.sh` file with an editor.
  - b. Add the following lines:

```
if [-f /home/db2inst1/sqllib/db2profile]; then
. /home/db2inst1/sqllib/db2profile;
fi
```
  - c. Save and close the file.
  - d. Load the `setupCmdLine.sh` file:

```
#. /usr/WebSphere/AppServer/bin/setupCmdLine.sh
```
  - e. Verify that you can now perform **db2** commands by running **db21 eve1** at the command line.
2. Go to the `<wp-root>/config` directory and back up the `wpconfig.properties` file, where `<wp-root>` is the root directory for WebSphere Portal. For example, on AIX, the default installation path is `/usr/WebSphere/PortalServer`.
3. Edit the WebSphere Portal configuration `wpconfig.properties` file and change the parameters, as shown in Table 6-4 on page 295.

**Note:** For a detailed description of each property, refer to the section of “Configuring WebSphere Portal for DB2” in *WebSphere Portal V5.1 Information Center*, available at:

<http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/index.html>

Table 6-4 DB2 configuration values for the `wpsconfig.properties` file

Property	Value
DbSafeMode	false
DbType	db2
WpsDbName	wps51n
DbDriver	COM.ibm.db2.jdbc.app.DB2Driver
DbDriverDs	COM.ibm.db2.jdbc.DB2XADataSource
JdbcProvider	wpsdbJDBC
DbUrl	jdbc:db2:wps51n
DbUser	db2inst1
DbPassword	<type_db2inst1_password>
DbLibrary	/home/db2inst1/sqllib/java/db2java.zip
WpsDsName	wpsdbDS
WpsXDbName	wps5TCP
WpsDbNode	wpsNode
JcrDbName	jcr51n
JcrDbUser	db2inst1
JcrDbPassword	<type_db2inst1_password>
JcrDbUrl	jdbc:db2:jcr51n
JcrXDbName	jcrdbTCP
JcrDbNode	wpsNode
JcrJdbcProvider	jcrdbJDBC
JcrDsName	JCRDS
JcrGeneratedDLLPath	\${WpsInstallLocation}/jcr/config/dynamic
JcrBinaryValueFileDir	\${WpsInstallLocation}/jcr/binaryValues
PznDbNode	wpsNode
FeedbackXDbName	fdbk5TCP

Property	Value
FeedbackDbName	fdbk51n
FeedbackDbUser	db2inst1
FeedbackDbPassword	<type_db2inst1_password>
FeedbackDbUrl	jdbc:db2:fdbk51n
LikemindsXDbName	1mdb5TCP
LikemindsDbName	1m51n
LikemindsDbUser	db2inst1
LikemindsDbPassword	<type_db2inst1_password>
LikemindsDbUrl	jdbc:db2:1m51n
WmmDsName	wmmDS
WmmAppName	wmmApp
WmmDbName	wps51n
WmmDbUser	db2inst1
WmmDbPassword	<type_db2inst1_password>
WmmDbUrl	jdbc:db2:wps51n

4. Save and close the wpconfig.properties file.

**Important:** For security reasons, we recommend that you leave each password field blank in the wpconfig.properties file. While running the following tasks, you can specify the password on the command line with the following syntax:

```
WPSconfig.sh <task_name> -D<password_property_key>=<password_value>
```

Where <task\_name> is the task that you will perform, and each password property should have one -D prefix and one key-value pair. In the following steps, we assume that all passwords are removed from the wpconfig.properties file.

5. You can test the database connections to Portal databases using the following commands:

```
#!/WPSconfig.sh validate-database-connection-wps \
-DDbPassword=<type_db2inst1_password\
#!/WPSconfig.sh validate-database-connection-jcr \
-DJcrDbPassword=<type_db2inst1_password\
#!/WPSconfig.sh validate-database-connection-feedback \
-DFeedbackDbPassword=<type_db2inst1_password\
#!/WPSconfig.sh validate-database-connection-likeminds \
-DLikemindsDbPassword=<type_db2inst1_password\
#!/WPSconfig.sh validate-database-connection-wmm \
-DWmmDbPassword=<type_db2inst1_password\
#!/WPSconfig.sh validate-database-driver
```

Wait for the BUILD SUCCESSFUL message. If you get BUILD FAILED message, verify the wpconfig.properties file and validate again.

6. Perform the following command to transfer databases:

```
#!/WPSconfig.sh database-transfer \
-DDbPassword=<type_db2inst1_password> \
-DJcrDbPassword=<type_db2inst1_password> \
-DFeedbackDbPassword=<type_db2inst1_password> \
-DLikemindsDbPassword=<type_db2inst1_password> \
-DWmmDbPassword=<type_db2inst1_password>
```

This task will take several minutes to complete, and you will see a BUILD SUCCESSFUL message when it finishes. If you get BUILD FAILED message, verify the wpconfig.properties file and repeat this step again.

7. Perform reorg check to improve performance:

```
#db2 connect to <db_name> user <db_user> using <db_password>
#db2 reorgchk update statistics on table all
#db2 terminate
#db2rbind <db_name> -l db2rbind.out -u <db_user> -p <db_password>
```

Where <db\_name> is your Portal database name, <db\_user> is the user you chose to be the owner of this database, and <db\_password> is the DB2 user name password.

**Note:** You must perform these steps for each WebSphere Portal database, for example, WPS51N, JCR51N, FDBK51N and LM51N.

8. Restart WebSphere Application Server, server1.
9. Open the WebSphere Application Server administrative console, and then perform the following steps:
  - a. Expand **Servers** and click **Application Servers**. Then, select **WebSphere\_Portal** from the list of Application Servers.

- b. Select **Process Definition** from the list of Additional Properties.
  - c. Select **Java Virtual Machine** from the list of Additional Properties.
  - d. Add the value of DbLibrary in wpconfig.properties into Classpath field. In this example, we add /home/db2inst1/sqllib/java/db2java.zip into the Classpath field.
  - e. Expand **Resources** from the left-side menu, and then click **JDBC Providers**. In this example, there will be four JDBC providers:
    - feedbackJDBC
    - jcrdbJDBC
    - likemindsJDBC
    - wpsdbJDBC
  - f. Select **wpsdbJDBC**, and then click **Data Sources** from Additional Properties. For each data source, click the **Test Connection** button to verify database connections.
  - g. Repeat the previous step for other JDBC providers.
10. Start WebSphere Portal.

11. Test the WebSphere Portal configuration by typing the following URL in a browser. You can log in as wpsadmin:

```
http://<wps_hostname>:9081/wps/myportal
```

**Important:** If you disabled port 9081 and enabled the remote HTTP port number as in 6.4.4, “Disabling access to port 9081 (optional)” on page 277, you must enter the following URL:

```
http://<http_server_hostname>/wps/myportal
```

Where <wps\_hostname> is the fully qualified host name for WebSphere Portal, and <http\_server\_hostname> is the fully qualified host name for the IBM HTTP Server machine.

## 6.6 Installing and configuring LDAP

A basic installation of WebSphere Portal will use Cloudscape as a custom user registry for authentication. We strongly recommend that you configure an LDAP server to be used as the user repository. The LDAP server will store all user information and provide user authentication to the WebSphere Portal application.

This section provides instructions to install and configure IBM Tivoli Directory Server V5.2 on AIX. We assume that you already have a DB2 UDB Enterprise Server Edition installed on this machine.



For detailed information, read the *IBM Tivoli Directory Server Installation and Configuration Guide*, SC32-1338, and *IBM Tivoli Directory Server Administration Guide*, SC32-1339. These guides can be found in the doc directory on the installation disc (CD #8-3).

## 6.6.1 Installing IBM Tivoli Directory Server

For hardware and software requirements, read the documentation provided by the *IBM Tivoli Directory Server Installation and Configuration Guide*, SC32-1338.

**Important:** IBM Tivoli Directory Server V5.2 requires AIX 5L V5.2 with a 64-bit kernel enabled; otherwise, you will not be able to install the LDAP server component later. To verify that AIX hardware is 64-bit, you can type:

```
bootinfo -y
```

To verify whether your AIX kernel is 64-bit, type:

```
bootinfo -K
```

If your hardware is 64-bit, but the kernel is only 32-bit, you have to follow these instructions to enable the 64-bit kernel:

1. Create symbolic links for the 64-bit kernel:

```
ln -sf /usr/lib/boot/unix_64 /unix
ln -sf /usr/lib/boot/unix_64 /usr/lib/boot/unix
```

2. Create a new boot image:

```
bosboot -ad /dev/iplddevice
```

3. Reboot your system:

```
shutdown -Fr
```

In an AIX environment, the product will be installed in the following directories:

- ▶ IBM Tivoli Directory Server: /usr/ldap
- ▶ IBM Global Security Tool Kit (GSKit): /usr/opt/ibm/gsksa and /usr/opt/ibm/gskta
- ▶ WebSphere Application Server Express V5.0.2: /usr/ldap/appsrv

To install IBM Tivoli Directory Server, complete the following steps:

1. Mount CD #8-3 on /cdrom and then go to the /cdrom/ismp directory.
2. Run the installation wizard file:

```
./setup
```

3. Select the desired language for the installation and then click **OK**.

4. The Welcome window opens. Click **Next**.
5. The installation wizard gives a warning about the presence of DB2 UDB Enterprise Server (Figure 6-20). Click **Next** to continue.

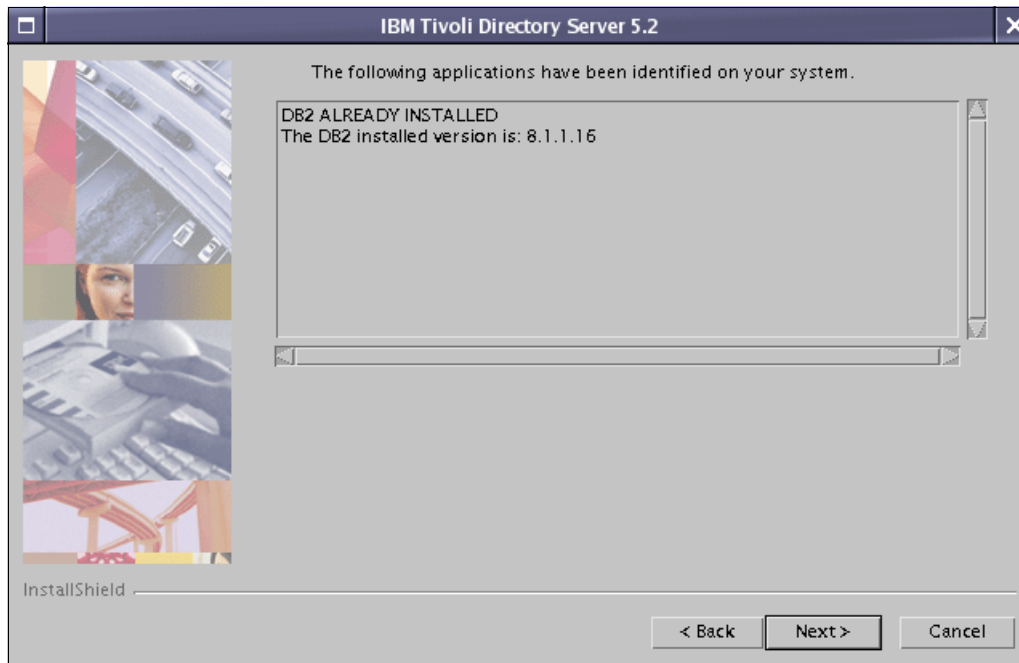


Figure 6-20 Warning about the presence of DB2 UDB Enterprise Server

6. Select the desired language in which you want IBM Tivoli Directory Server to be installed. Click **Next**.
7. Select the **Custom** installation type. Click **Next**.

8. Select the features you want to install. For this example, we installed everything but DB2 UDB Enterprise Server, as shown in Figure 6-21. You must install an embedded WebSphere Application Server - Express V5.0.2 for the Web Administration Tool. For more information about these features, refer to the IBM Tivoli Directory Server documentation.

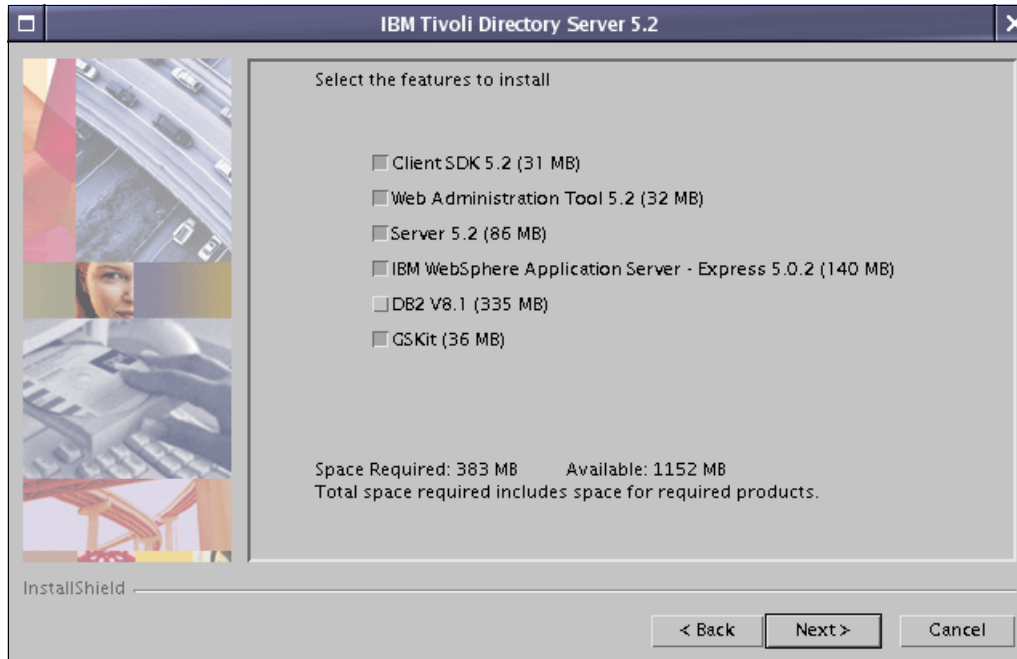


Figure 6-21 Available features for Tivoli Directory Server

9. Review your choices and then click **Next**.
10. Read the Client Readme information and click **Next**.
11. The Server Readme information opens. Click **Next** after reading it.
12. Click **Finish** to complete the installation. The IBM Tivoli Directory Server Configuration Tool will automatically be displayed.

Follow the steps in the next section to complete the installation.

## 6.6.2 Configuring the administrator DN

The administrator DN is required for LDAP management and WebSphere Portal configuration. To create an administrator DN, complete the following steps:

1. In the IBM Tivoli Directory Server Configuration Tool window, select **Administrator DN/password** from the left side.
2. On the right side, enter the Administrator DN name and its password, as shown in Figure 6-22.

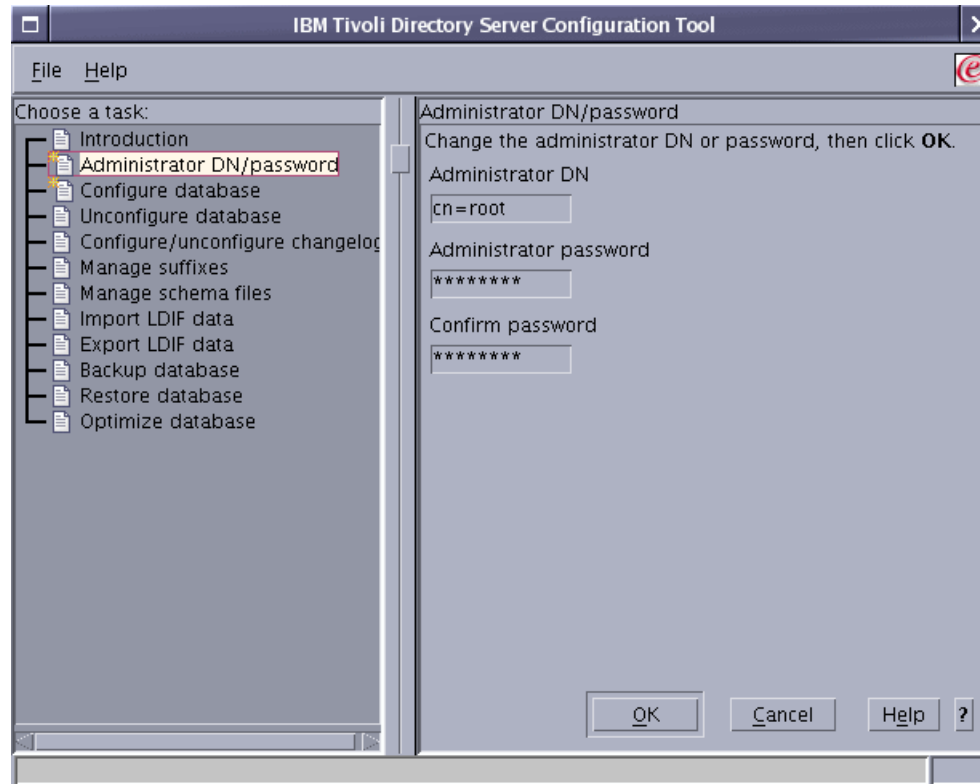


Figure 6-22 Configuring the Administrator DN name

3. Wait for the message Administrator DN and password successfully updated, as shown in Figure 6-23 on page 303. Click **OK**.



Figure 6-23 Administrator DN created

### 6.6.3 Configuring the LDAP database

You must now configure the LDAP database. In this example, we use an existing DB2 instance, named db2inst1. The Configuration Tool will create and configure the database.

Before configuring the database, you must be aware of the following requirements:

- ▶ Verify that the DB2COMM variable is *not* set. You can set the variable to a blank value, for example:

```
#su - db2inst1
$db2set DB2COMM=
```

- ▶ The root user *must* be a member of the DB2 user's primary group.

You can find more requirements for the DB2 user in the *IBM Tivoli Directory Server Installation and Configuration Guide*, SC32-1338.

To configure the LDAP database, complete the following steps:

1. If you closed the Configuration Tool, open it again by running the following command:

```
#!/usr/ldap/bin/ldapxcfg
```

2. Select **Configure database** from the left side of the window.

3. Select **Create a new database** (Figure 6-24). Click **Next**.

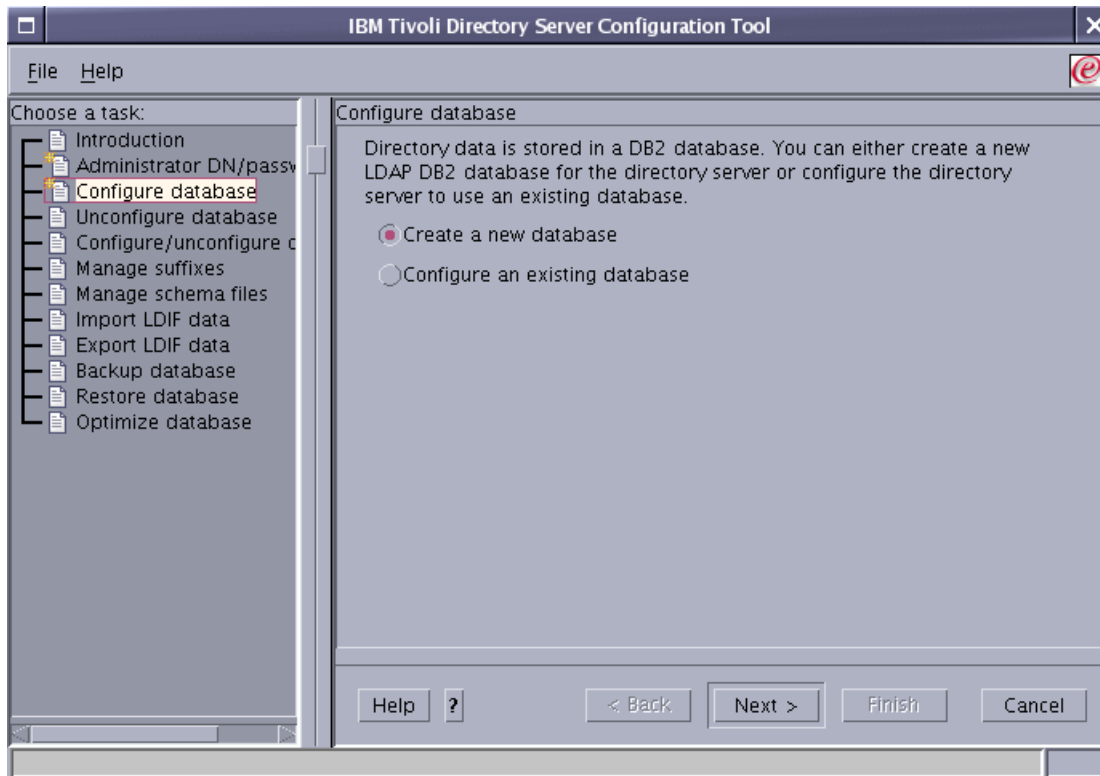


Figure 6-24 Create a new LDAP database

4. Enter the DB2 user name and password for the instance. In the example shown in Figure 6-25, we use an existing DB2 instance. If you would like to create a different instance, follow the steps in the *IBM Tivoli Directory Server Installation and Configuration Guide*, SC32-1338. Click **Next**.

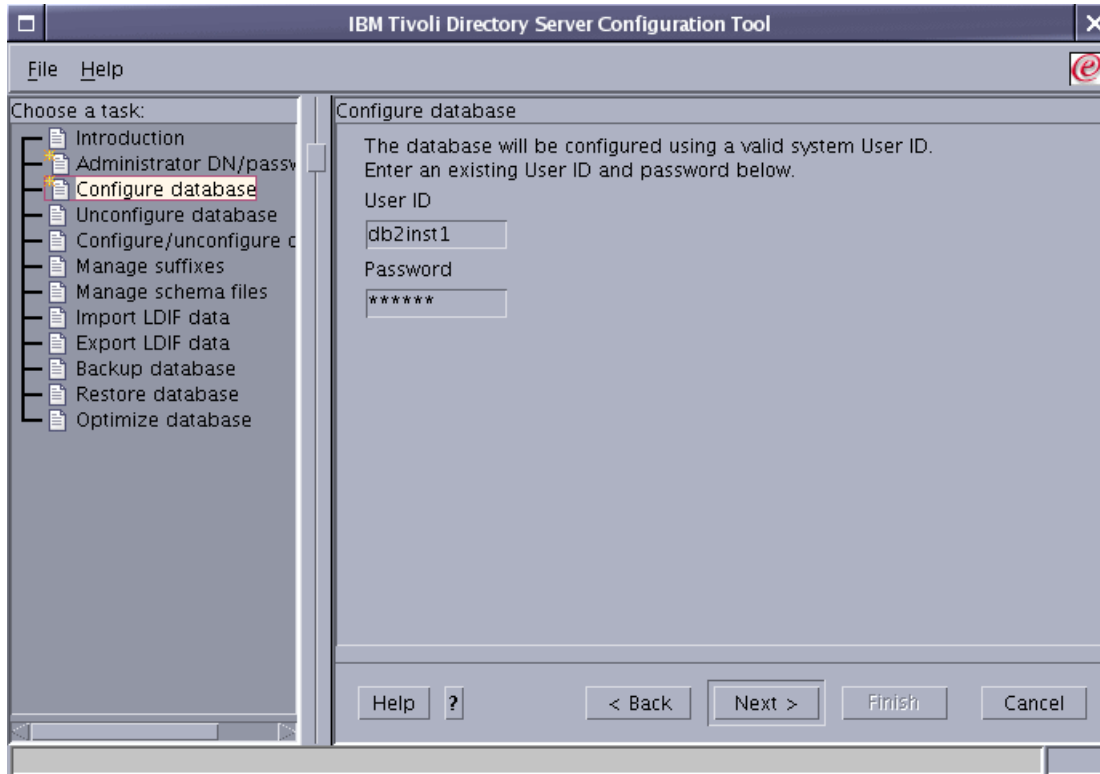


Figure 6-25 Enter the DB2 user ID and password

5. Enter the database name for the LDAP directory. LDAPDB2 is the default value, as shown in Figure 6-26. Click **Next**.

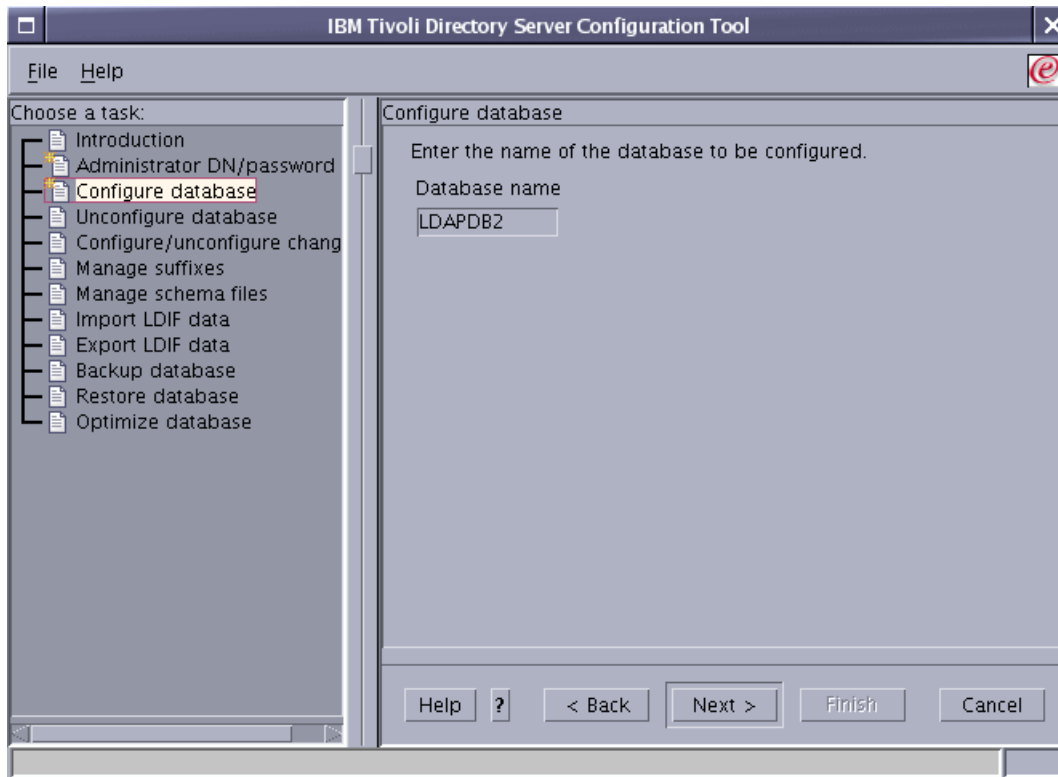


Figure 6-26 Enter the database name



6. Select **Create a universal DB2 database (UTF-8/UCS-2)**, as shown in Figure 6-27. Click **Next**.

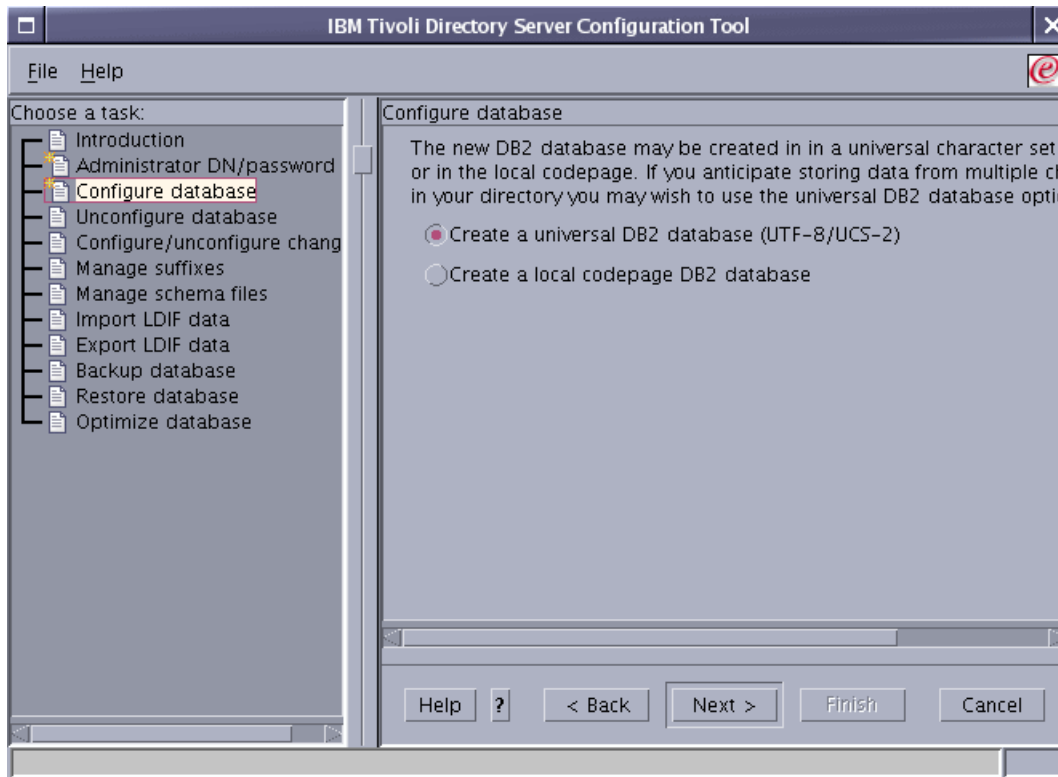


Figure 6-27 Select UTF-8 database

7. Enter the Database location, for example, /home/db2inst1, as shown in Figure 6-28. This is the location where the installation wizard will create the database. Click **Next**.

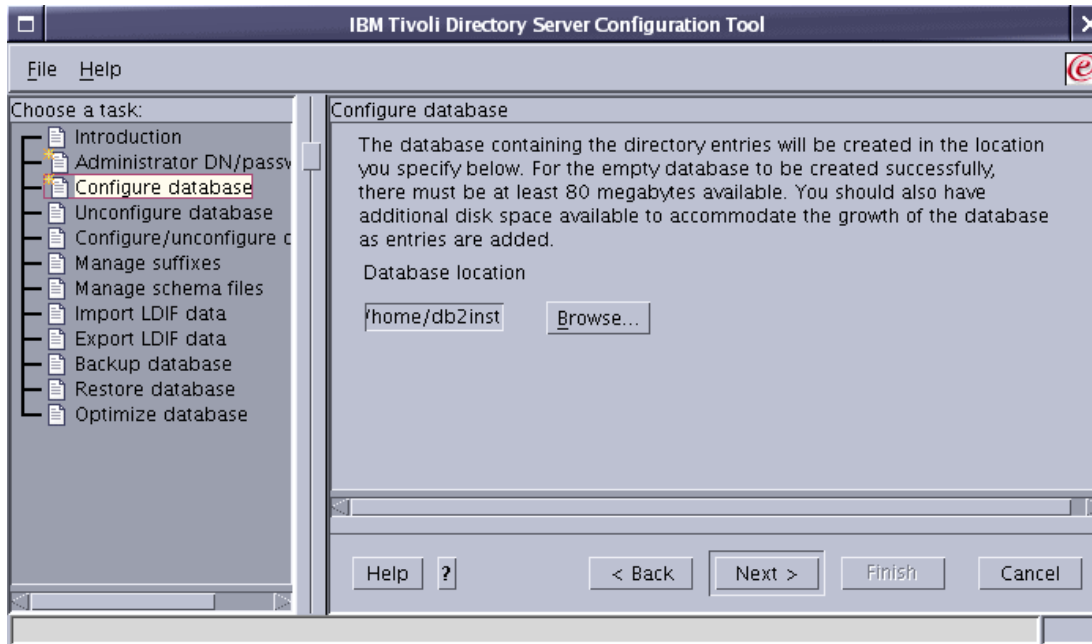


Figure 6-28 Enter the database location

8. If you are satisfied with the settings, click **Finish**.

9. Read the messages and verify that the database was created and configured successfully. You will see a window similar to the one shown in Figure 6-29.

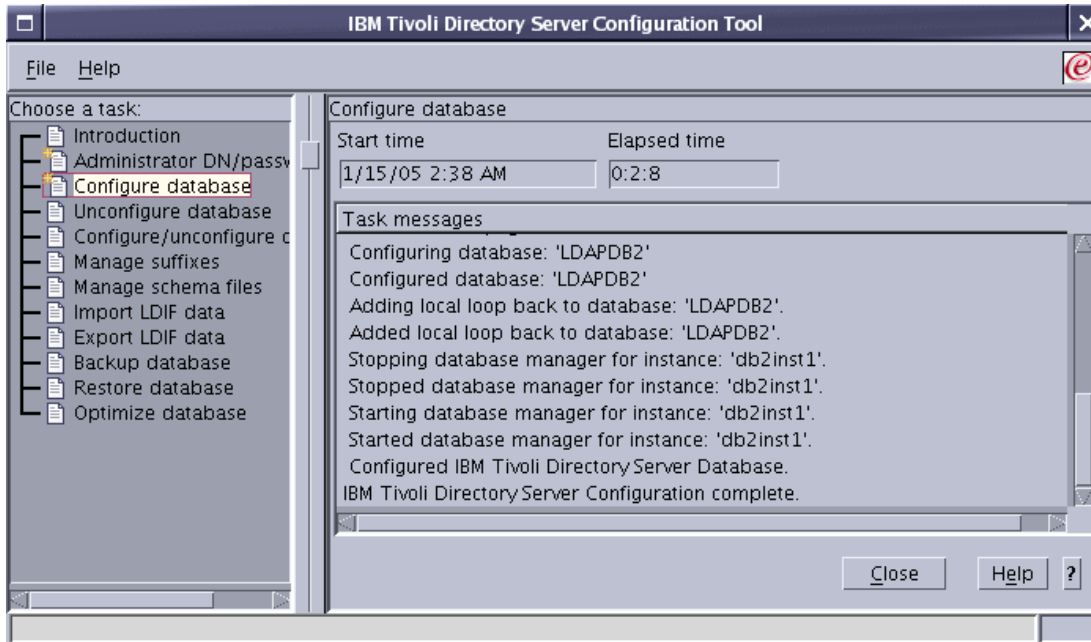


Figure 6-29 The database was created successfully

10. Start the LDAP server by running the following command on just one line:

```
#ibmdirctl -h <ldap_server_hostname> -D <admin_DN> -w <admin_DN_password> -p <ldap_admin_port_number> start
```

Where <ldap\_server\_hostname> is the fully qualified host name of your LDAP server, <admin\_DN> and <admin\_DN\_password> are the values you created in 6.6.2, “Configuring the administrator DN” on page 302, and <ldap\_admin\_port\_number> is the LDAP administration port number, which can be 3538 for non-SSL access or 3539 for SSL access. See Example 6-5.

*Example 6-5 Starting LDAP server*

```
#ibmdirctl -h m10df53f.itso.ibm.com -D cn=root -w abc123 -p 3538 start
```

11. Validate the LDAP configuration:

```
#ldapsearch -h <ldap_server_hostname> -s base objectclass=*
```

Where <ldap\_server\_hostname> is the fully qualified host name of your LDAP server.

## 6.6.4 Configuring the Web Administration Tool

This section explains how to configure the Web Administration Tool that is installed to administer IBM Tivoli Directory Server.

As soon you finish the installation and configuration of IBM Tivoli Directory Server, you must complete the following steps to be able to use the Web Administration Tool:

1. Start the Administrator daemon:

```
#ibmdiradm
```

2. Start the embedded version of WebSphere Application Server - Express:

```
#cd /usr/ldap/appsrv/bin
#./startServer.sh server1
```

3. Open the console by typing the following URL:

```
http://<ldap_server_hostname>:9080/IDSWebApp/IDSjsp/Login.jsp
```

4. Select **Console Admin** for the LDAP Hostname. Enter superadmin in the Username field and secret as the Password (Figure 6-30). Click **Login**.

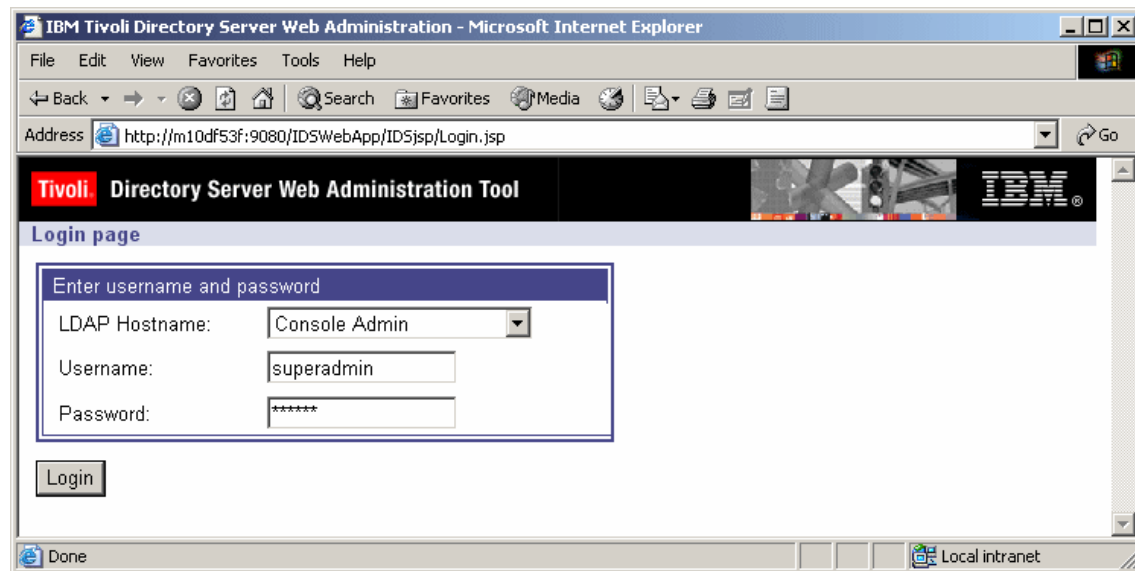


Figure 6-30 Console Admin login

The Web Administration Tool opens.

5. For security purposes, change the user name and password of the console administrator:
  - a. Expand **Console administration** on the left side of the window.
  - b. Select **Change console administrator login**.
  - c. Enter a new user name and secret as the password, as shown in Figure 6-31. Click **OK**.

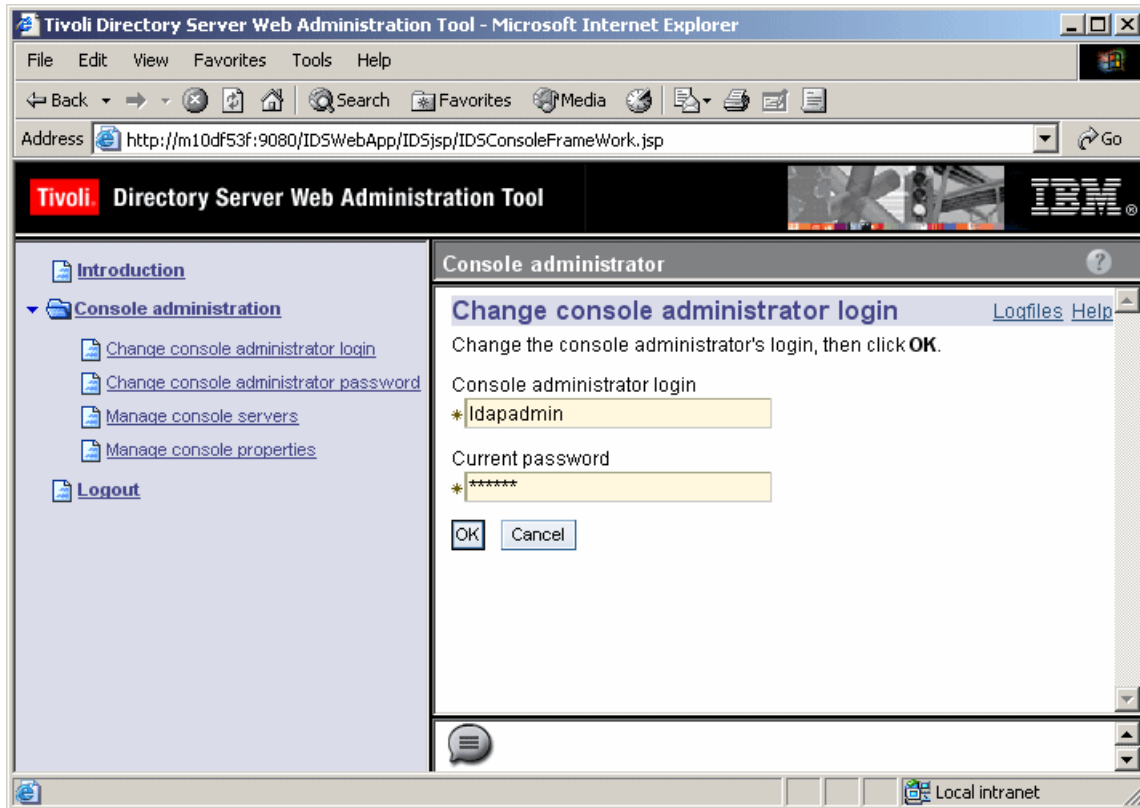


Figure 6-31 Changing the user name for Web Administration Tool

- d. Select **Change console administrator password**.

e. Enter the old password and type a new one (Figure 6-32).

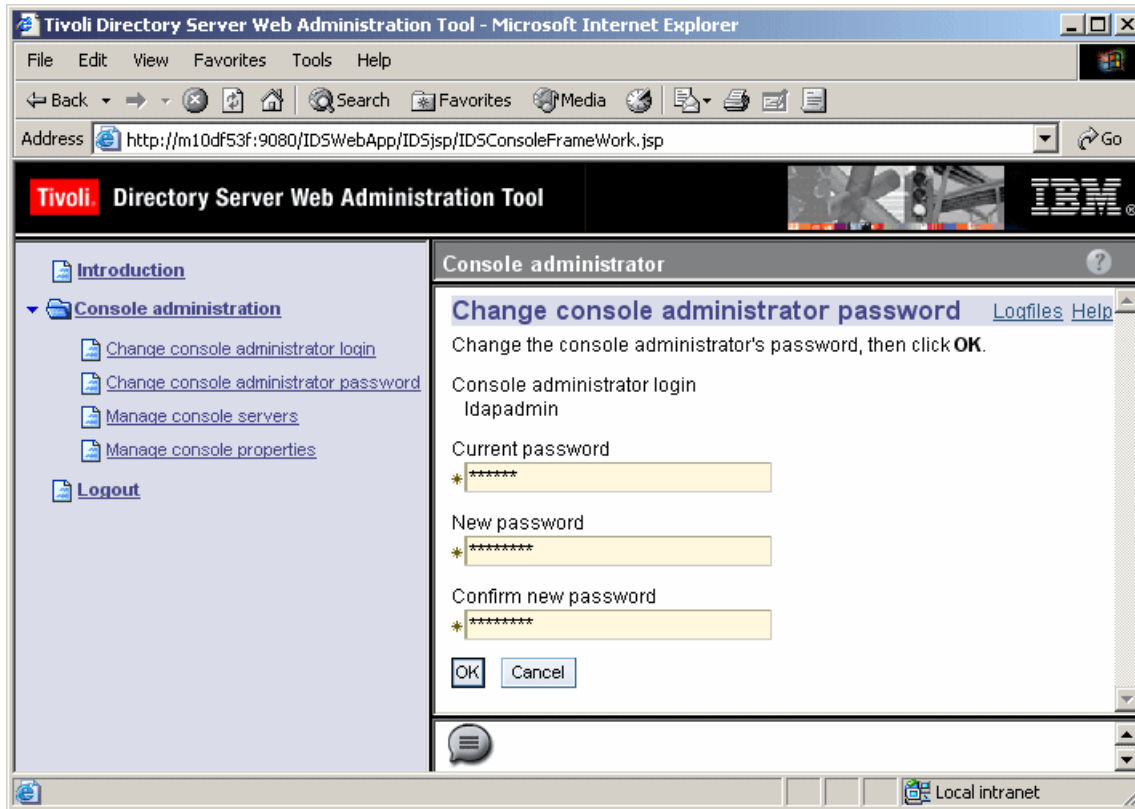


Figure 6-32 Changing the password for the Web Administration Tool user

## 6.6.5 Configuring the LDAP server for Web Administration Tool

This section provides the instructions to configure the LDAP server you want to administer using Web Administration Tool. Complete the following steps:

1. Open the Web Administration Tool.
2. Select **Manage console servers**.
3. Click **Add**.

4. Enter the fully qualified host name of the LDAP server and accept the default values for the LDAP port and Administration port number, as shown in Figure 6-33. Click **OK**.

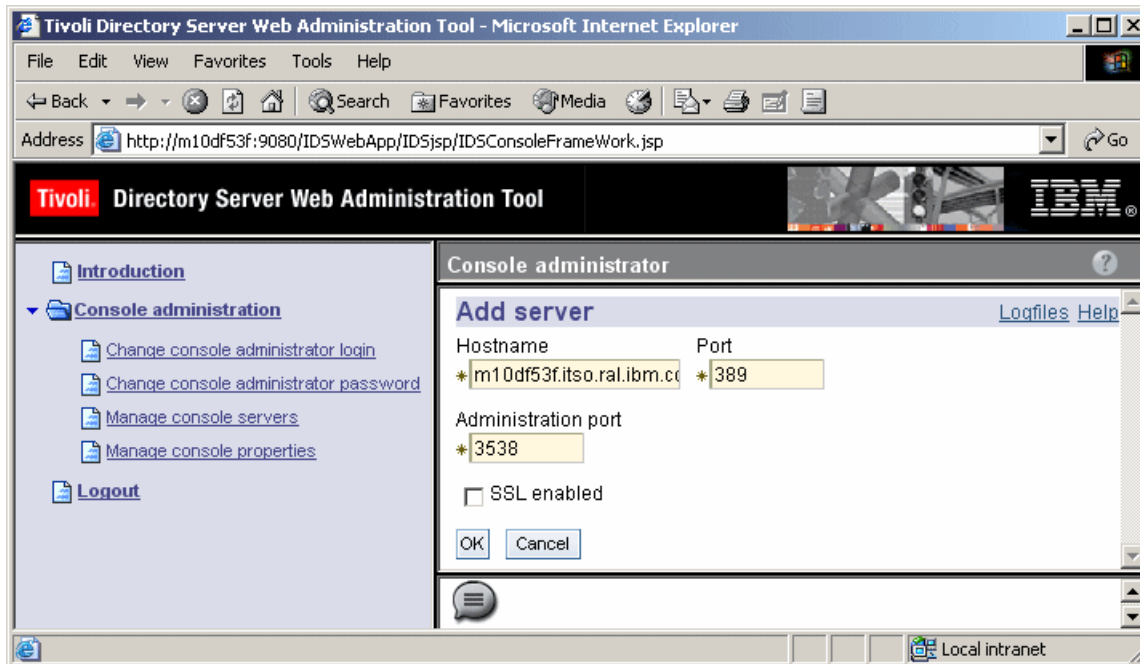


Figure 6-33 Adding the LDAP server host name

5. The server you just added is displayed in the list, as shown in Figure 6-34.

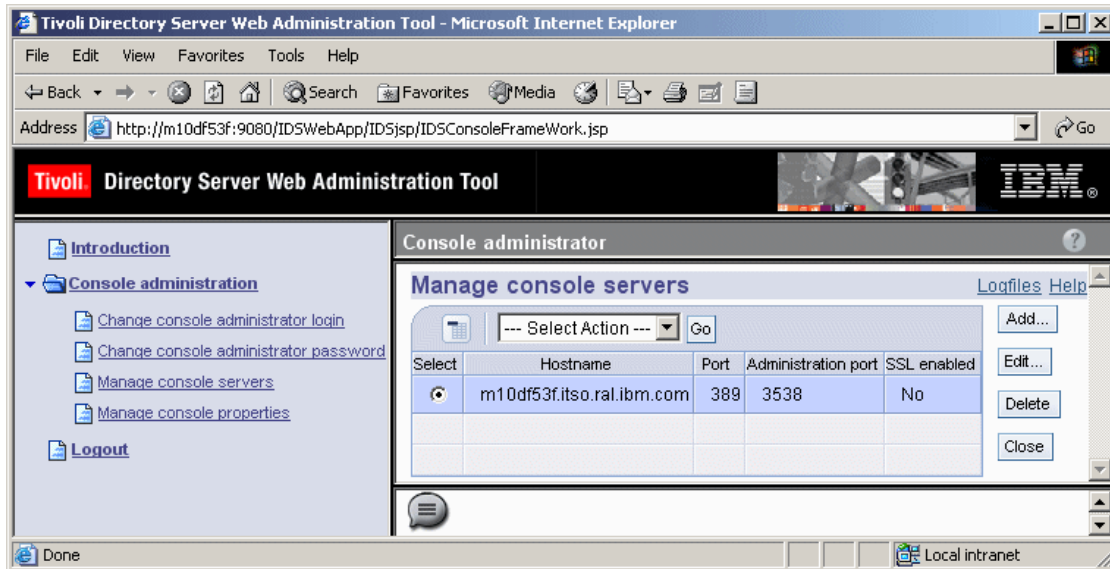


Figure 6-34 The LDAP host name appears in the list

6. Click **Logout**.

Now that you have added the LDAP server name, you will be able to administer the server using the Web Administration Tool. The previous procedure adds the LDAP server host name in the LDAP Hostname list on the Login page.



The login procedure for the LDAP server requires a different administrator name. You must use the administrator DN and its password, as shown in Figure 6-35.

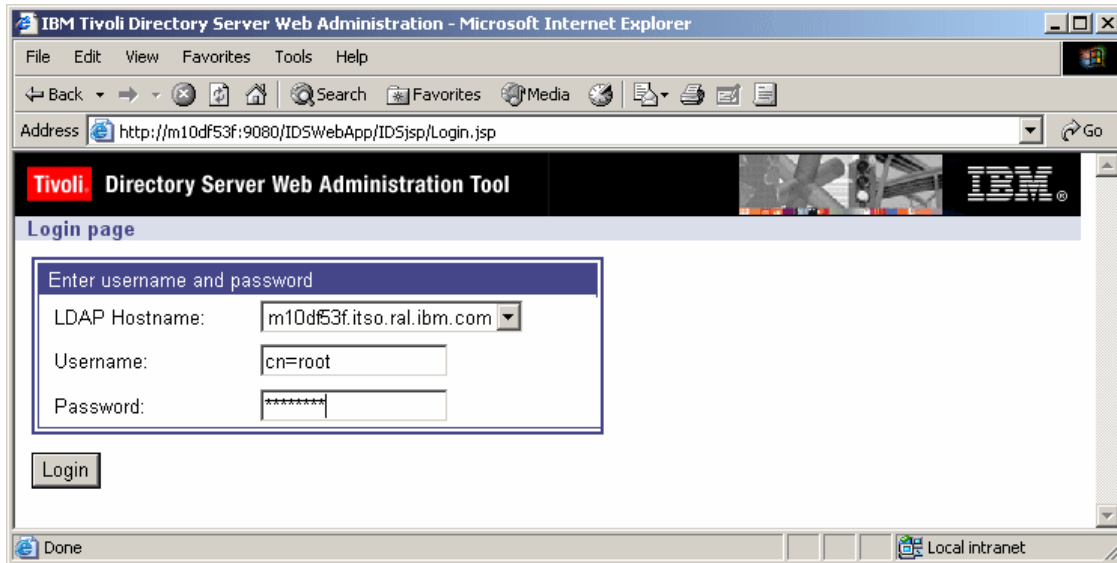


Figure 6-35 LDAP server login

## 6.6.6 Installing IBM Tivoli Directory Server V5.2 client

The architecture in use in this chapter requires you to install the LDAP client on the machine where WebSphere Portal was installed.

Complete the following steps:

1. Mount CD #8-3 on /cdrom.
2. Run the installation wizard file:  

```
/cdrom/ismp/setup
```
3. Select the desired language for the installation. Click **Next**.
4. Click **Next** on the Welcome window.
5. In this case, we already had DB2 UDB Enterprise Server Edition V8.1 installed. If you do not have DB2 UDB Enterprise Server installed on this machine, let the installation wizard install it for you. Click **Next**.
6. Select the language for Tivoli Directory Server. Click **Next**.
7. Select the **Custom** installation type. Click **Next**.
8. Select **Client SDK 5.2** and **GSKit only**, and clear all the other options. Click **Next**.

9. Click **Next** to start copying the files.
10. Read the Client Readme information and click **Next**.
11. Click **Finish**. The installation complete.

### 6.6.7 Preparing the LDAP server for WebSphere Portal

This section provides guidance for configuring the LDAP server to work with WebSphere Portal. We guide you through the following steps:

- ▶ Adding the suffix for WebSphere Portal
- ▶ Creating the required users and group
- ▶ Configuring the WebSphere Portal settings

#### Adding the suffix for WebSphere Portal

To add a new suffix into the LDAP structure, complete the following steps:

1. Open Web Administration Tool page.
2. Select the LDAP host name server from the LDAP Hostname list.
3. Enter the administrator DN name and password (Figure 6-35 on page 315). Click **Login**.
4. Expand **Server administration**.
5. Select **Manage server properties**.
6. Select **Suffixes** on the Manage server properties window.

7. Enter the Suffix DN value (Figure 6-36). Click **Add**.

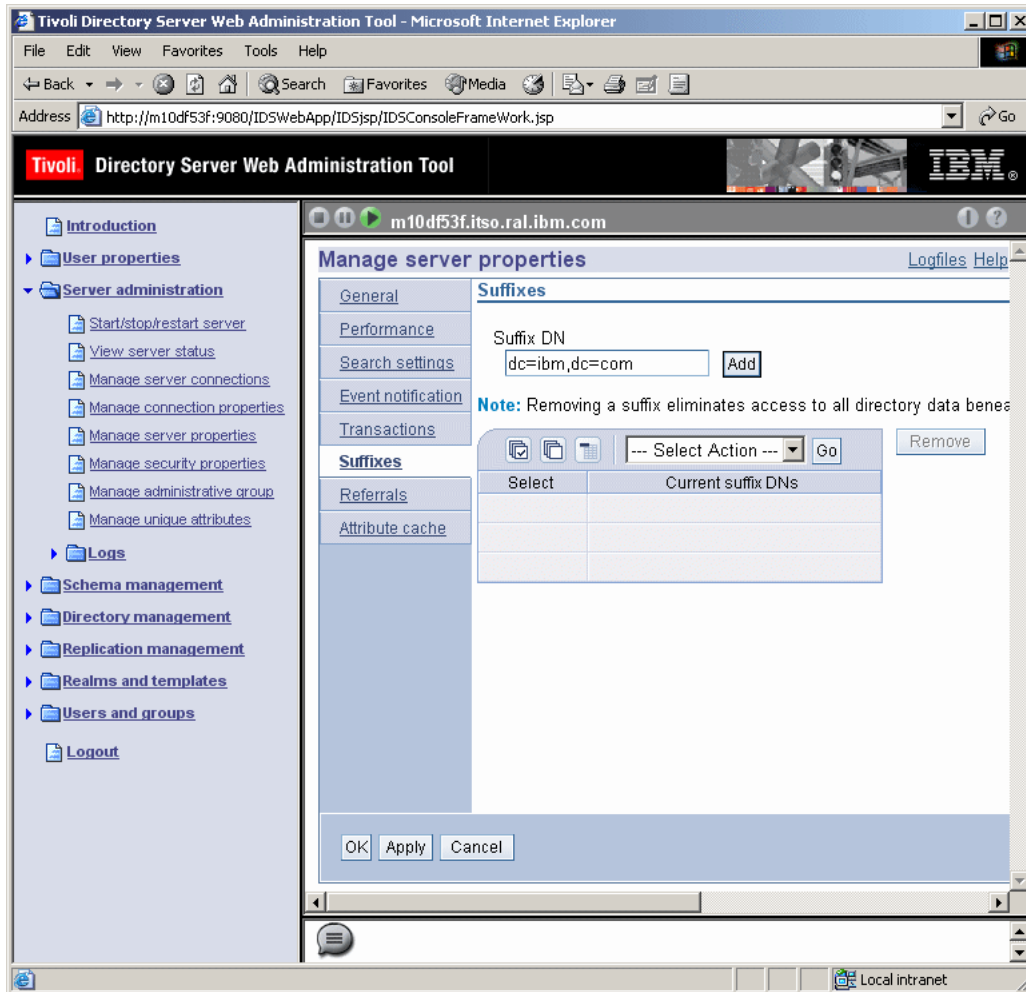


Figure 6-36 Adding the suffix

8. Click **OK** to save the changes.
9. Stop and start LDAP server:
  - a. Expand **Server administration**.
  - b. Select **Start/stop/restart server** from the left side of the Web Administration Tool window.
  - c. Click **Stop** and then **Start**. Look for the server started message on the bottom of the window.

## 6.6.8 Creating the required users and group

WebSphere Portal requires an administrator user, a bind user, and an administrator group. The PortalUsers.ldif file contains the required users and group for a basic WebSphere Portal environment. This file can be found on the Portal Setup CD.

To import the LDIF file into LDAP directory structure, complete the following steps:

1. Copy the PortalUsers.ldif file to your hard disk and edit it.
2. Replace all entries of `dc=yourco,dc=com` with the suffix you have created in “Adding the suffix for WebSphere Portal” on page 316. You might want to enter a different password for the `wpsadmin` and `wpsbind` users; it is easier than changing them later.
3. You *must* stop the LDAP server before importing the LDIF file.
4. Import the file by running the following command:

```
ldif2db -i <ldif_file_name>
```

Where `<ldif_file_name>` is the location and file name of the LDIF file. For example:

```
ldif2db -i /tmp/PortalUsers.ldif
```

The following message indicates that the LDIF file was successfully imported:

```
ldif2db: 6 entries have been successfully added out of 6 attempted.
```

5. Start the LDAP server.
6. Validate the LDIF import by executing the following **ldapsearch** command, in just one line. Replace all occurrences of `"dc=ibm,dc=com"` with your suffix:

```
ldapsearch -b "dc=ibm,dc=com" -h <ldap_server_hostname> -D
"uid=wpsbind,cn=users,dc=ibm,dc=com" -w <wpsbind_password>
"(&(uid=wpsadmin)(objectclass=inetOrgPerson))"
```

## 6.6.9 Configuring WebSphere Portal with the LDAP settings

This section provides instructions about how to configure the WebSphere Portal settings for an external LDAP directory.

To configure WebSphere Portal, complete the following steps:

1. Go to the `<wps-root>/config/` directory and create a backup of the `wpconfig.properties` configuration file.
2. Edit the original `wpconfig.properties` file.
3. Change the required properties values, as shown in Table 6-5 on page 319.

**Note:** For more information about the LDAP configuration in the `wpconfig.properties` file, refer to *WebSphere Portal V5.1 Information Center*, available at:

<http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/index.html>

Table 6-5 Changing the LDAP configuration in the `wpconfig.properties` file

Property	Value
WasUserId	uid=wpsbind,cn=users,dc=yourco,dc=com
WasPassword	<wpsbind_password>
WpsHostName	<wps_full_qualified_hostname>
PortalAdminId	uid=wpsadmin,cn=users,dc=ibm,dc=com
PortalAdminIdShort	wpsadmin
PortalAdminPwd	<wpsadmin_password>
PortalAdminGroupId	cn=wpsadmins,cn=groups,dc=ibm,dc=com
PortalAdminGroupIdShort	wpsadmins
LTPAPassword	<ltpa_password>
LTPATimeout	120
SSOEnable	true
SSODomainName	<Single Sign-on Domain> Example: .itso.ral.ibm.com
LDAPHostName	<The fully qualified LDAP host name>
LDAPPort	389
LDAPAdminUIId	<LDAP Administrator DN> Example: cn=root
LDAPAdminPwd	<LDAP Administrator DN password>
LDAPServerType	IBM_DIRECTORY_SERVER
LDAPBindID	uid=wpsbind,cn=users,dc=yourco,dc=com
LDAPBindPassword	<wpsbind_password>
LDAPSuffix	<Your LDAP suffix> Example: dc=ibm,dc=com

Property	Value
LDAPUserPrefix	uid
LDAPUserSuffix	cn=users
LDAPGroupPrefix	cn
LDAPGroupSuffix	cn=groups
LDAPUserObjectClass	inetOrgPerson
LDAPGroupObjectClass	groupOfUniqueNames
LDAPGroupMember	uniqueMember
LDAPsslEnable	false

4. Start server1.
5. Stop WebSphere\_Portal.
6. Test the connection to the LDAP server:

```
#cd /usr/WebSphere/PortalServer/config
#./WPSconfig.sh validate-ldap
```

Wait for the BUILD SUCCESSFUL message. If you get BUILD FAILED message, verify the wpconfig.properties file and repeat this step.

7. Execute the following task, according to your environment:
  - a. If security is *not* enabled, run the following command; otherwise, go to step b:

```
#./WPSconfig.sh enable-security-ldap
```
  - b. If security is already enabled, you must run the following command:

```
#./WPSconfig.sh secure-portal-ldap
```

**Note:** If you get errors during this process, verify the values in the wpconfig.properties file. You can find more details about the error in the <wps-root>/log/ConfigTrace.log file.

Before running this command again, stop WebSphere\_Portal. You might have to include the WebSphere administrator user and password to complete this task, for example:

```
stopServer.sh WebSphere_Portal -user wpsbind -password
<wpsbind_password>
```

8. Stop server1:

```
#cd /usr/WebSphere/AppServer/bin
#./stopServer.sh server1 -user wpsbind -password <wpsbind_password>
```

9. Start server1:

```
#./startServer.sh server1
```

10. Start WebSphere\_Portal:

```
#./startServer.sh WebSphere_Portal
```

## 6.7 Validating the overall configuration

This section will guide you through the validation of the database and LDAP configuration on WebSphere Portal.

As mentioned before in this chapter, by default, the WebSphere Portal uses Cloudscape as a database and also as a Custom User Registry for authentication.

We assume that you already have installed and configured the following items:

- ▶ Remote IBM HTTP Server
- ▶ Remote DB2 UDB Enterprise Server Edition
- ▶ Remote IBM Tivoli Directory Server (LDAP)
- ▶ Configured WebSphere Portal to use a remote Web server
- ▶ WebSphere Portal using the remote DB2 as a database and the remote IBM Tivoli Directory Server as an LDAP server

### 6.7.1 Validating the database configuration

You might want to verify that WebSphere Portal data is being written into the DB2 database. Complete the following steps:

1. Open the WebSphere Portal page by typing the following URL:

```
http://<http_server_hostname>/wps/myportal
```

Where <http\_server\_hostname> is your Web server's fully qualified host name, for example, bc1srv1.itso.ra1.ibm.com.

2. Log in as the WebSphere Portal administrator. In this example, we use wpsadmin (Figure 6-37). Click **Log in**.

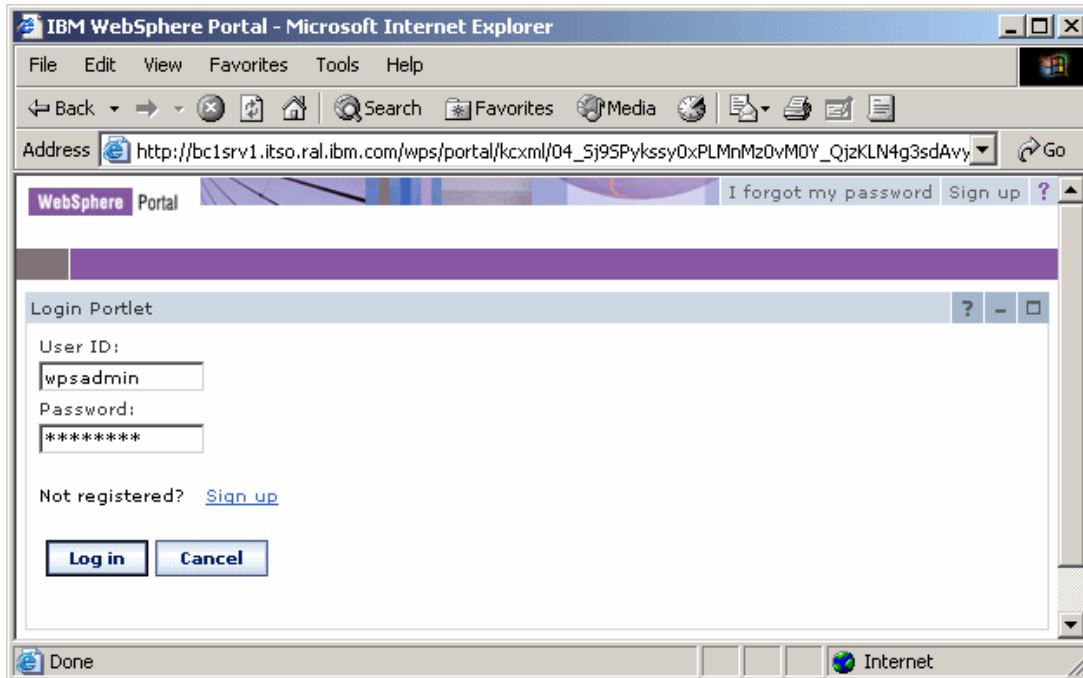


Figure 6-37 Log in as the WebSphere Portal administrator user

3. Click **Administration** on the top-right side of the window.
4. Click **Portal User Interface**, and then **Manage Pages**.



5. You will see a window similar to the one shown in Figure 6-38.

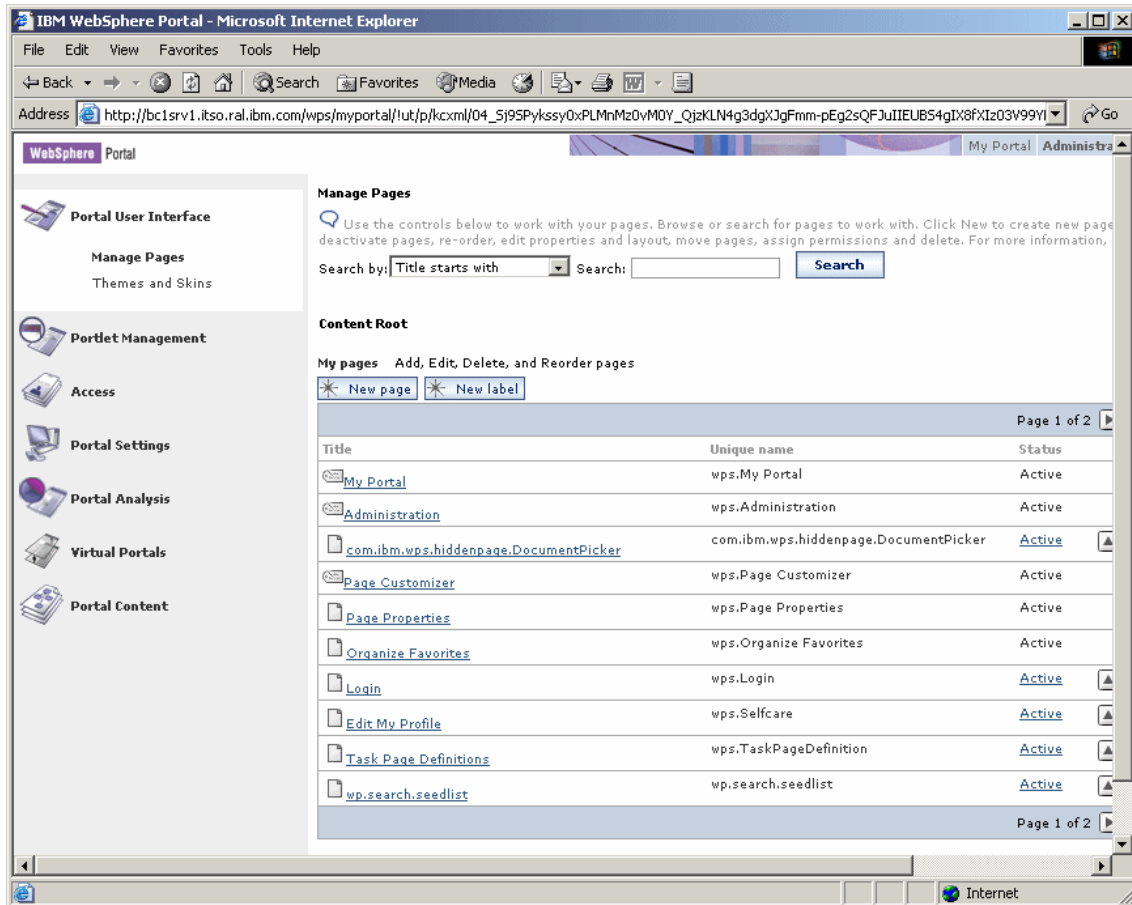


Figure 6-38 Manage Pages window

6. Click the **New Page** button.
7. Enter the Title of the page.
8. Select the desired Theme.
9. For the Type of Page option, choose the layout you want in this page by selecting one of the frames from the A content page with these properties area (Figure 6-39 on page 324). Click **OK**.

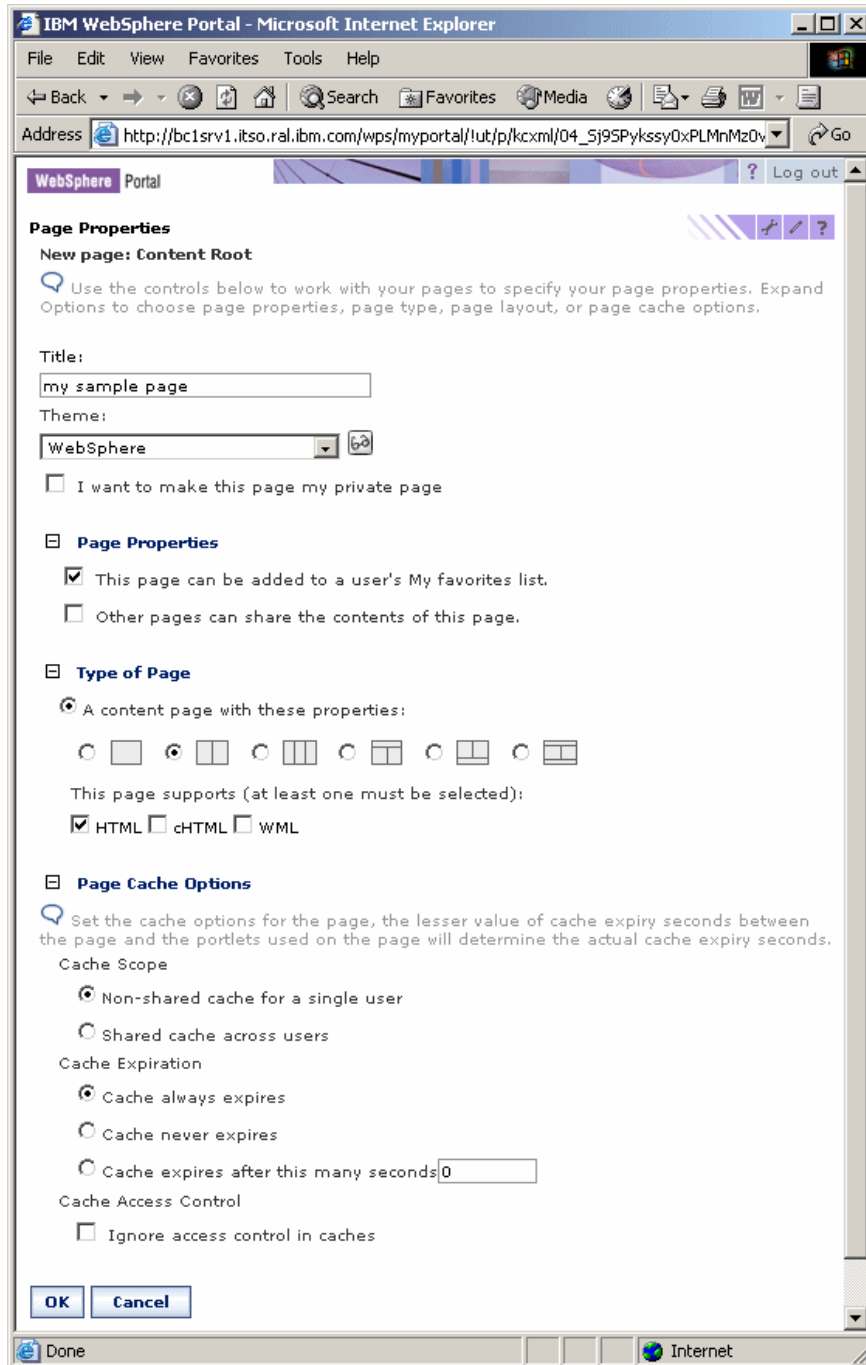


Figure 6-39 Page Properties window

10. Click **OK** when you see the message EJPAS0022W: <page\_title> page has been created successfully.

The Manage Page window opens. The page you just created appears in the list.

**Note:** You have created a blank page. You can continue and add portlets to this page, but for the purpose of this chapter, this is enough to validate the database configuration.

Now, you need to verify that the page you have created was stored into the WebSphere Portal database. Complete the following steps:

1. On the WebSphere Portal machine, open a terminal window.
2. Log in as the database owner user and start the DB2 command line:
3. Enter the following SQL statements. The result will show the information of the page you created earlier. See Example 6-6.

```
#su - db2inst1
$db2 connect to <db_name> user <db_user> using <db_password>
$db2 "select * from PAGE_INST_LOD where TITLE='<page_name>'"
```

*Example 6-6 Validating the DB2 configuration*

---

```
db2 connect to wps51n user db2inst1 using password
db2 "select * from PAGE_INST_LOD where TITLE='my sample page'"
```

---

The validation is successful if you get at least one entry in the PAGE\_INST\_LOD table.

## 6.7.2 Validating the LDAP configuration

This section will help you validate the LDAP configuration you completed in 6.6, “Installing and configuring LDAP” on page 298.

To create a new user using the WebSphere Portal Web page and verify that the user was added to IBM Tivoli Directory Server, complete the following steps:

1. Enter the following URL:

```
http://<wps_hostname>:9081/wps/portal
```

Where <wps\_hostname> is the fully qualified host name of the WebSphere Portal machine.

2. Click **Sign up** on the top-right side of the window.
3. Fill out the form with the required user information. Click **OK**.

4. You will see the Congratulation! Your enrollment was successful message. Click **Log in**.
5. Validate the successful enrollment by logging in to WebSphere Portal using the user name and password you just created.
6. After a successful login, verify that the user was added to the LDAP directory structure. In the WebSphere Portal machine, enter the following command:

```
ldapsearch -b "<your_suffix>" -h <ldap_server_hostname> -D
"uid=wpsbind,cn=users,dc=ibm,dc=com" -w "<wpsbind_password>"
"(&(uid=<new_user>)(objectclass=inetOrgPerson))"
```

Where `<your_suffix>` is the suffix you created in “Adding the suffix for WebSphere Portal” on page 316, `<ldap_server_hostname>` is the fully qualified host name for the LDAP server, `<wpsbind_password>` is the password of the wpsbind user, and `<new_user>` is the user ID name you created using the WebSphere Portal application. See Example 6-7. Type the command on just one line.

*Example 6-7 Validating LDAP configuration*

---

```
$ldapsearch -b "dc=ibm,dc=com" -h m10df53f.itso.ra1.ibm.com -D \
"uid=wpsbind,cn=users,dc=ibm,dc=com" -w "wpsbind" \
"(&(uid=david)(objectclass=inetOrgPerson))"
```

---



# WebSphere Portal: SUSE LINUX Enterprise Server 8 (SLES8) installation on zSeries

This chapter provides you with the complete instructions for installing IBM WebSphere Portal V5.1 middleware on IBM *@server* zSeries hardware running SUSE LINUX Enterprise Server 8 (SLES8), Service Pack 3.

During the installation of WebSphere Portal, we illustrate the installation of IBM WebSphere Business Integration Server Foundation and then WebSphere Portal V5.1.

## 7.1 Prerequisites

This section specifies the environmental configurations that you need to complete before beginning the installation of WebSphere Portal V5.1. We describe the SLES8 operating system requirements, IBM hardware requirements, IBM Middleware component space requirements, and WebSphere installation file requirements.

### 7.1.1 SLES8 operating system requirements

Table 7-1 displays the system requirements for SLES8.

Table 7-1 SLES8 system requirements

System requirements	Description
Memory	Minimum of 1 GB allocated to Linux guest
DASD	Minimum of three mini-disks
RPMs	Packages: <ul style="list-style-type: none"><li>▶ compat-2002.8.15-20</li><li>▶ unzip-5.50-57</li><li>▶ vnc-3.3.3r2-172</li><li>▶ pdksh-5.2.14-337</li></ul>

### 7.1.2 IBM hardware requirements

Table 7-2 specifies the supported operating systems for the IBM @server zSeries hardware.

Table 7-2 Operating systems

Linux distribution	Linux on zSeries
Red Hat Enterprise Linux Advanced Server 3.0 x390	
SUSE SLES8 s390	

### 7.1.3 IBM Middleware component space requirements

Table 7-3 on page 329 describes the space requirements for the IBM Middleware components addressed in this chapter.

Table 7-3 Middleware components

Component	/opt	/tmp
WebSphere Portal	1124 MB	50 MB
WebSphere Application Server	968 MB	700 MB
IBM HTTP Server	30 MB	N/A
Total	2424 MB	295 MB

## 7.1.4 WebSphere Portal installation CD requirements

For our example, Table 7-4 specifies the CDs that are required for the installation of the WebSphere Portal components in this chapter.

Table 7-4 Installation CDs

Disk	Description
Setup	WebSphere Portal V5.1 - Portal Install (Setup), V5.1
CD #1-11	WebSphere Business Integration Server Foundation for Linux/zSeries, V5.1
CD #1-12	WebSphere Business Integration Server Foundation for Linux/zSeries, V5.1
CD #1-20	WebSphere Business Integration Server Foundation - WebSphere Application Server V5.1 Fix Pack1 for Linux/zSeries
CD #2	Portal Server, V5.1
CD #3	Lotus Workplace Web Content Management™ and Personalization V2.1, V5.1

## 7.2 Installing WebSphere Portal V5.1

This section provides steps to install WebSphere Business Integration Server Foundation and WebSphere Portal. It describes the WebSphere Business Integration Server Foundation V5.1.1 software installation and WebSphere Business Integration Server Foundation V5.1.1 verification.

Follow these steps to install the WebSphere Business Integration Server Foundation V5.1.1 and WebSphere Portal V5.1 software and configure IBM Workplace Web Content Management.

**Note:** In the following procedure, we used downloaded files that represent the shrinkwrapped CDs necessary for this installation. The files were downloaded into the /opt/download directory. The CD numbers and descriptions are listed for your information in Table 7-5.

Table 7-5 Files and related CDs

File	CD	Description
C814EML.zip	Setup	WebSphere Portal V5.1- Portal install
C814RML.taz	1-11	WebSphere Business Integration Server Foundation for Linux/zSeries, V5.1
C814SML.taz	1-12	WebSphere Business Integration Server Foundation for Linux/zSeries, V5.1
C8150ML.taz	1-20	WebSphere Business Integration Server Foundation - WebSphere Application Server V5.1 Fix Pack1 for Linux/zSeries
C8152ML.zip	2	Portal Server, V5.1
C8153ML.zip	3	Lotus Workplace Web Content Management and Personalization V2.1, V5.1

Complete the following steps:

1. Prepare the installation environment and start the installation program by typing the following commands. Press Enter after each command.

```
#cd /opt/download
#unzip C814EML.zip
#tar xzvf C814RML.taz
#tar xzvf C814SML.taz
#tar xzvf C8150ML.taz
#unzip C8152ML.zip
#unzip C8153ML.zip
```

**Note:** After all the files are unpacked, run the following command:

```
#./install.sh &
```

2. The installation wizard begins and asks you to select a language. Select your preferred language. (In our example, we use the English language.) Click **OK**.



3. The Welcome to IBM WebSphere Portal for Multiplatforms, Version 5.1 Welcome window opens (Figure 7-1). Click **Next**.

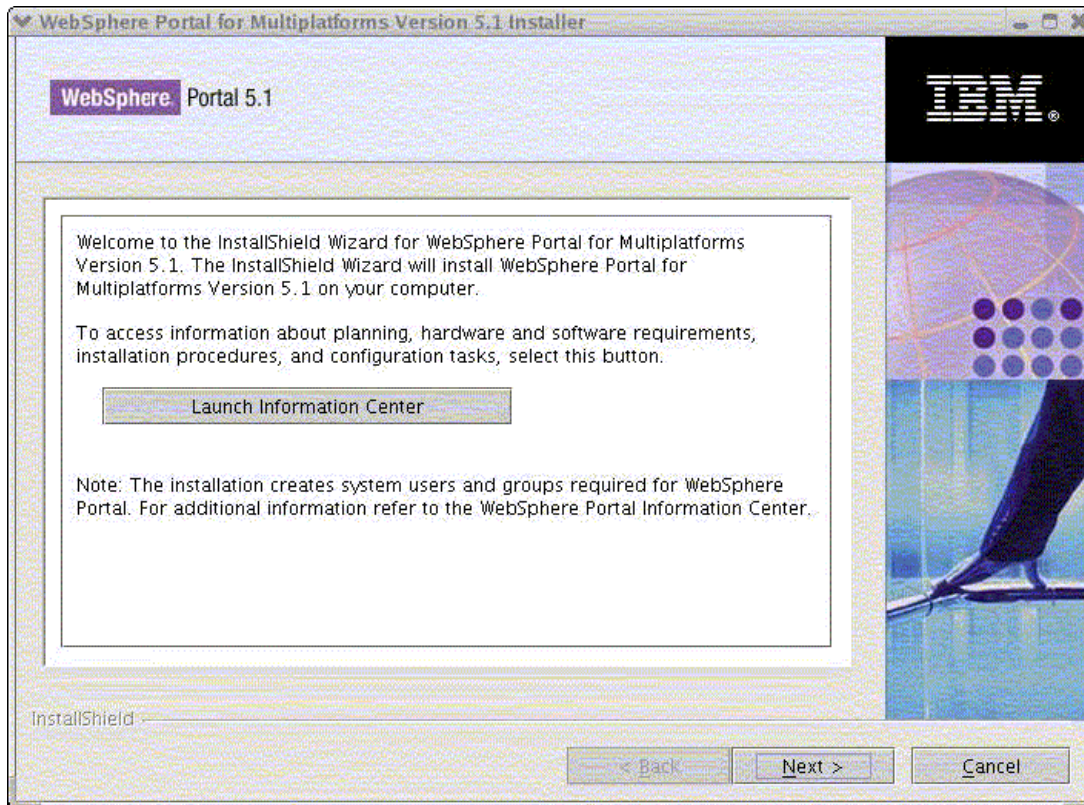


Figure 7-1 IBM WebSphere Portal installation wizard welcome window

4. The Software License Agreement panel opens. Select **I accept the terms in the license agreement**. Click **Next**.

5. Choose **Full** as the setup type (Figure 7-2). Click **Next**.

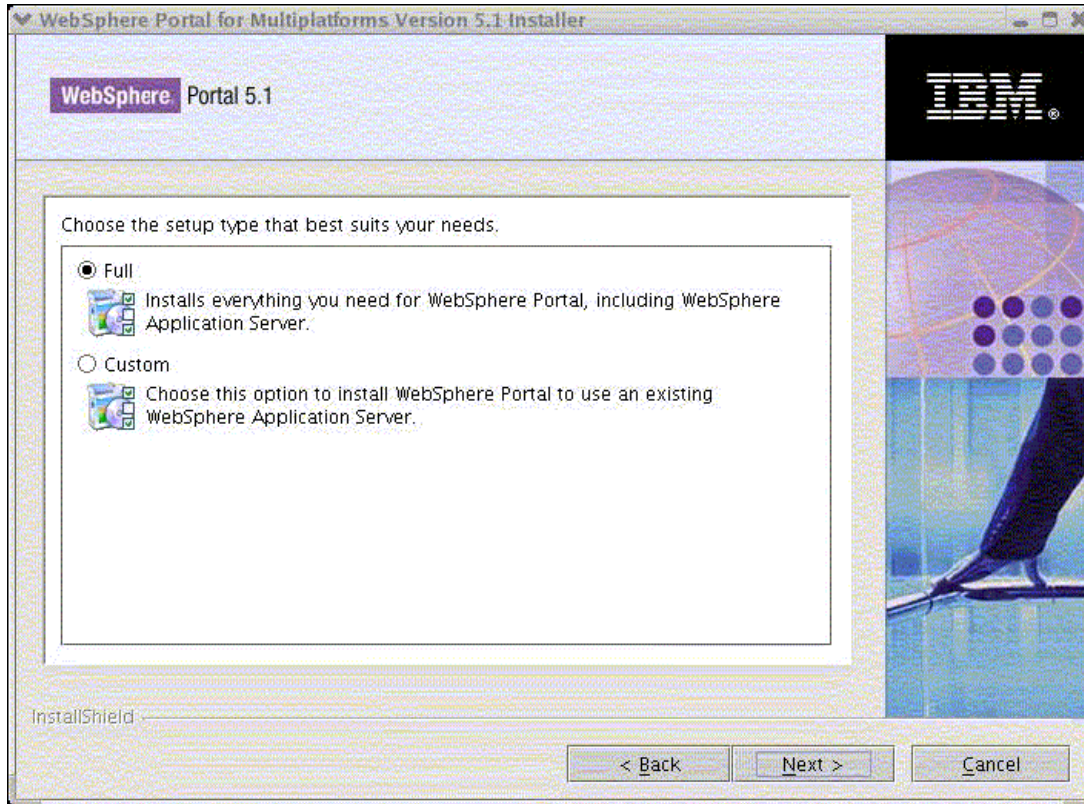


Figure 7-2 Setup type

6. For the installation directory, accept the default (Figure 7-3). Click **Next**.

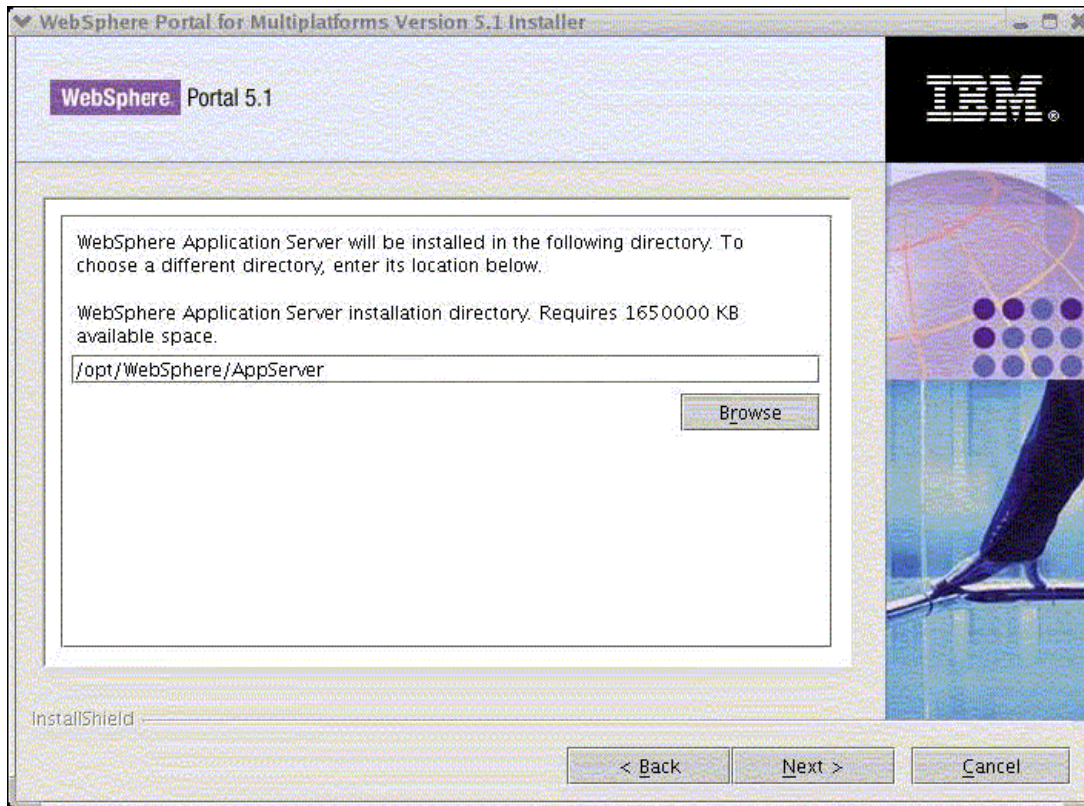


Figure 7-3 WebSphere Application Server installation directory



7. This window contains the Node name and WebSphere Application Server hostname (Figure 7-4). Click **Next**.

**Note:** Make sure the Node name and WebSphere Application Server hostname matches your machine host name.

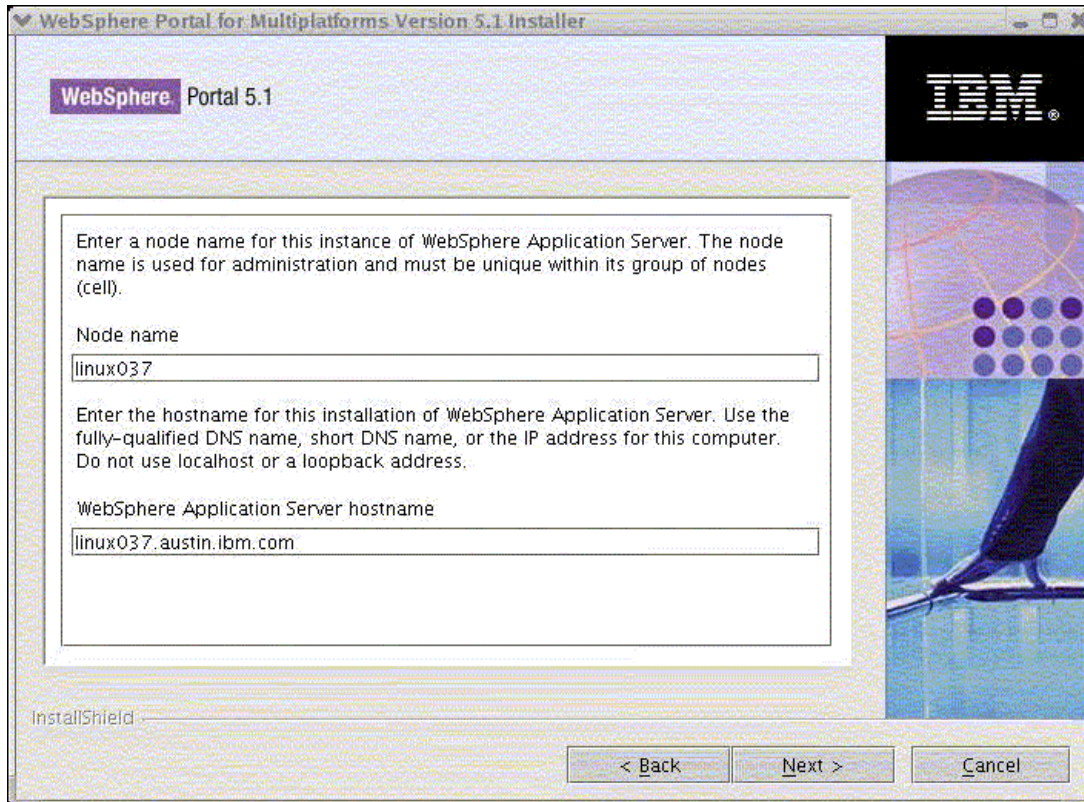


Figure 7-4 Node name and hostname

8. On the installation directory window, click **Next** (Figure 7-5).

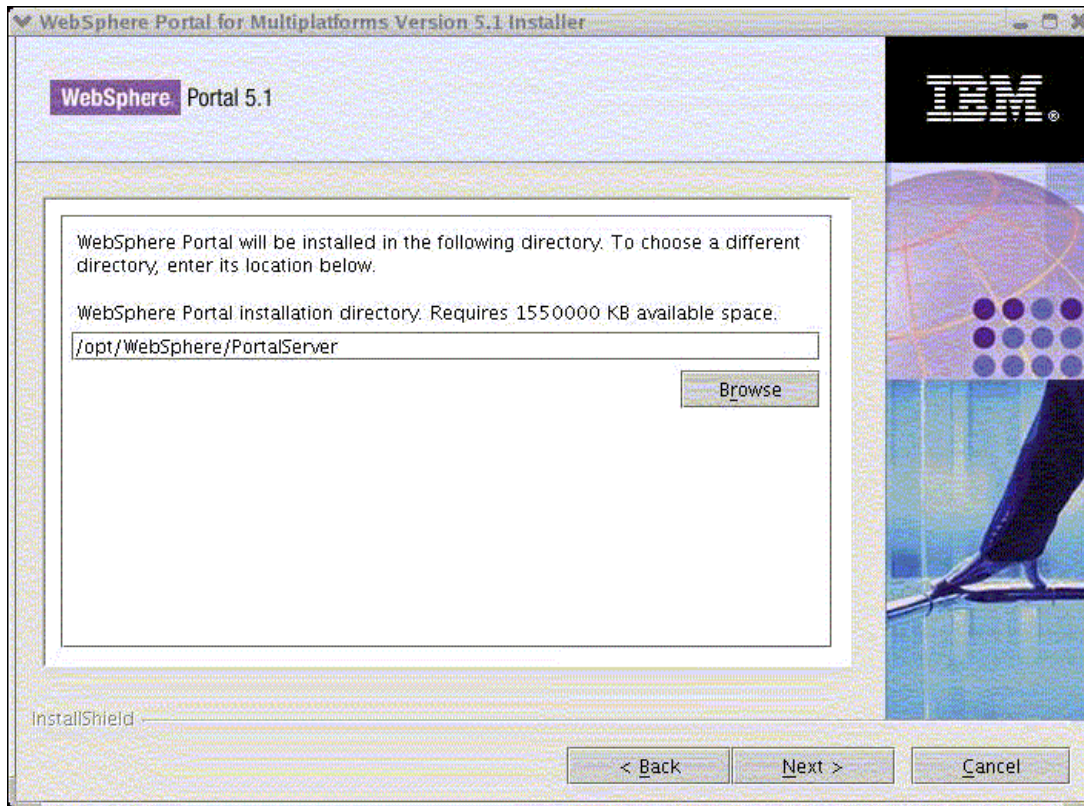


Figure 7-5 Installation directory

9. Enter WebSphere Portal Administrative user name and password (Figure 7-6). Click **Next**.

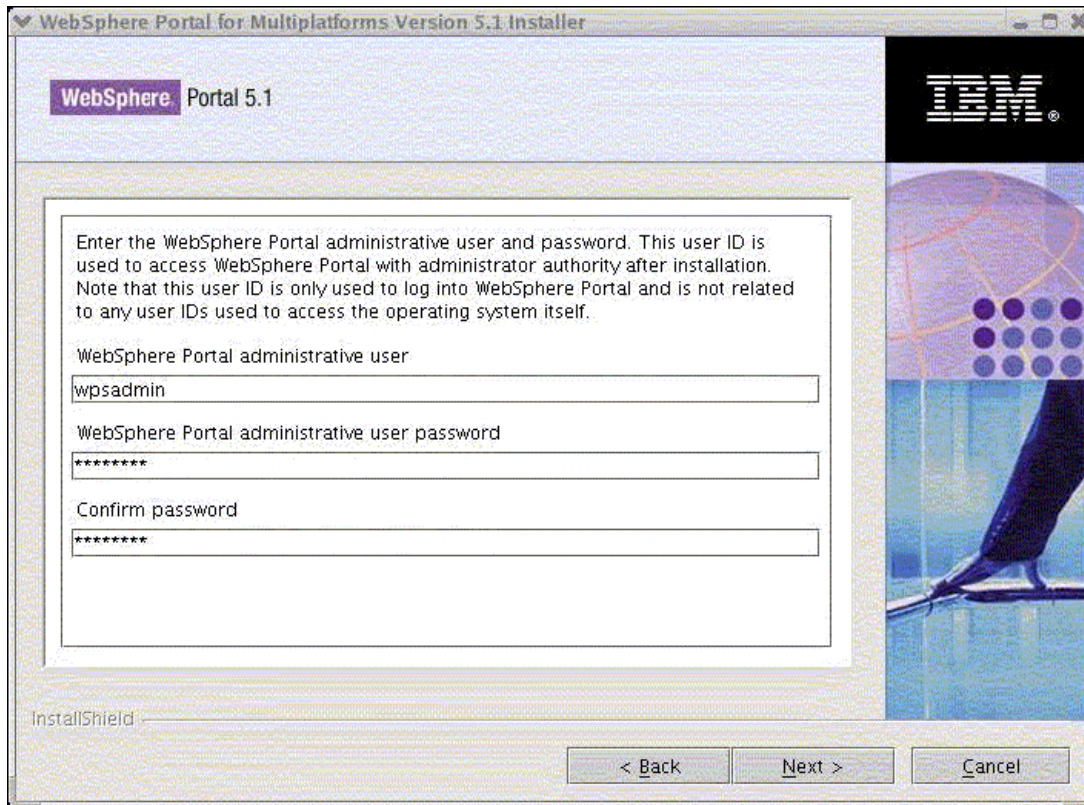


Figure 7-6 WebSphere Portal administrative name and password



10. Click **Next** (Figure 7-7). The Portal components will begin to install.

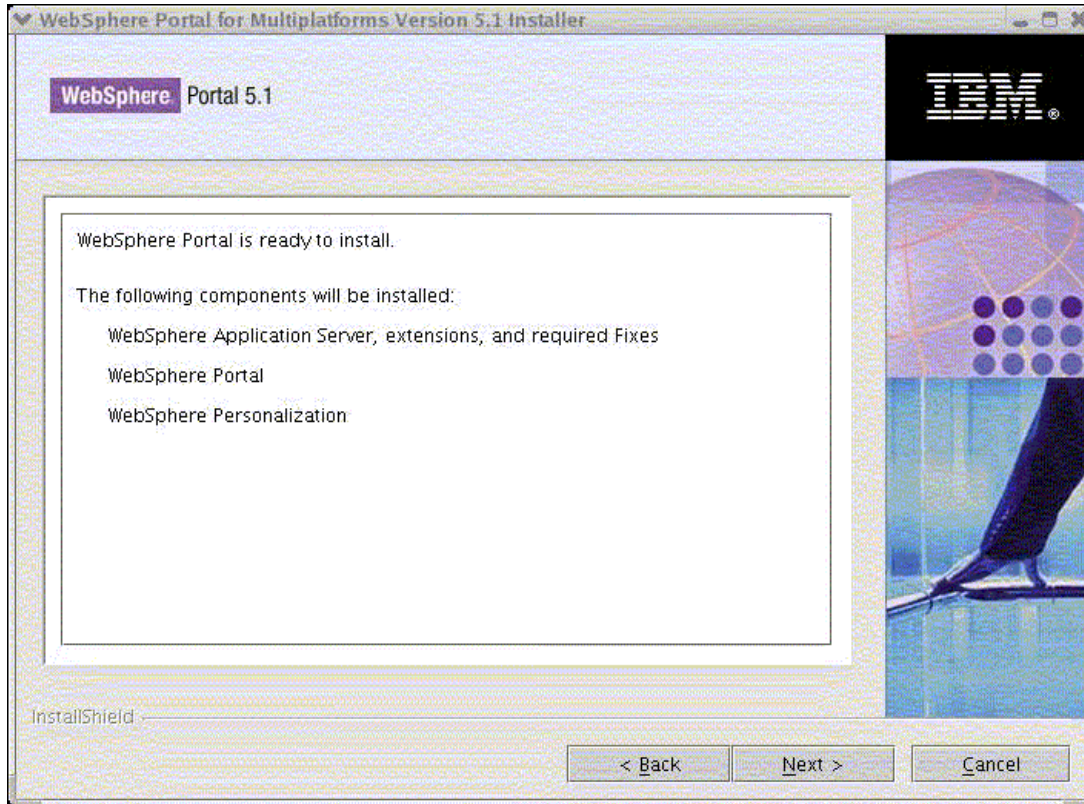


Figure 7-7 WebSphere Portal is ready to install

11. When the window shown in Figure 7-8 opens, clear the **Launch First Steps** option and click **Finish**.

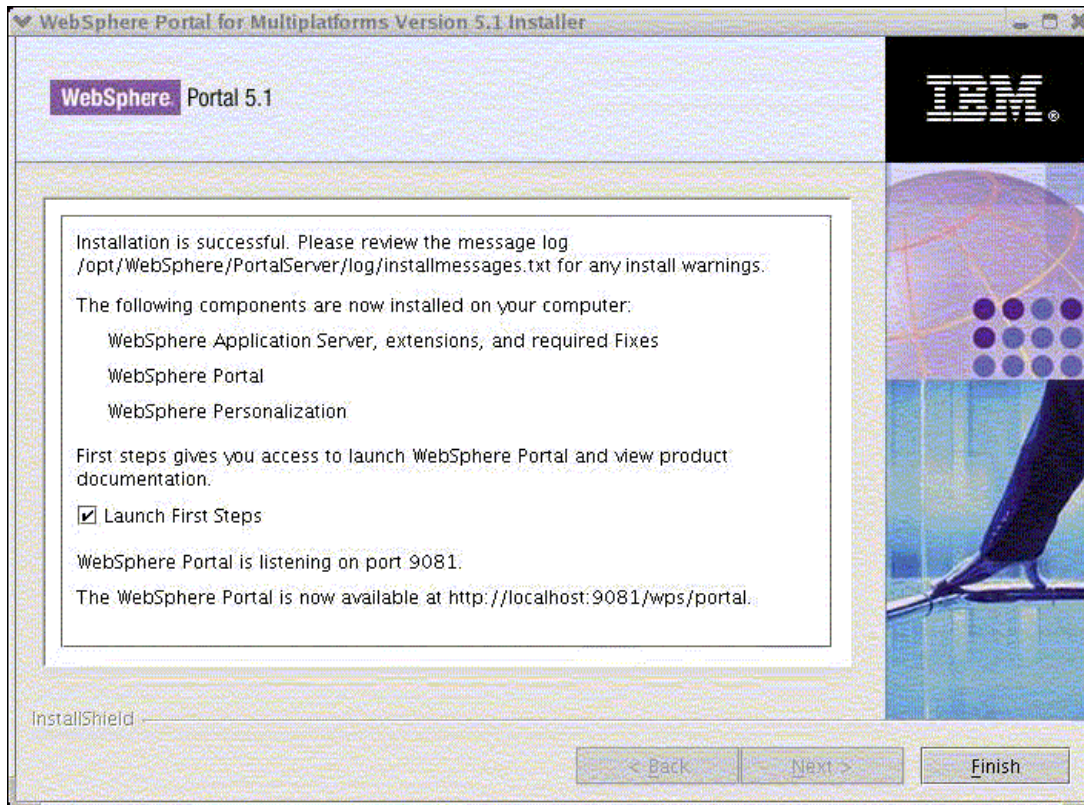


Figure 7-8 Installation successful

12. To access WebSphere Portal Welcome page, open a browser and enter the following URL:

`http://linux037.austin.ibm.com:9081/wps/portal`

The WebSphere Portal Welcome page opens.



13. Click the **Login** button on the top-right corner of the page (Figure 7-9).

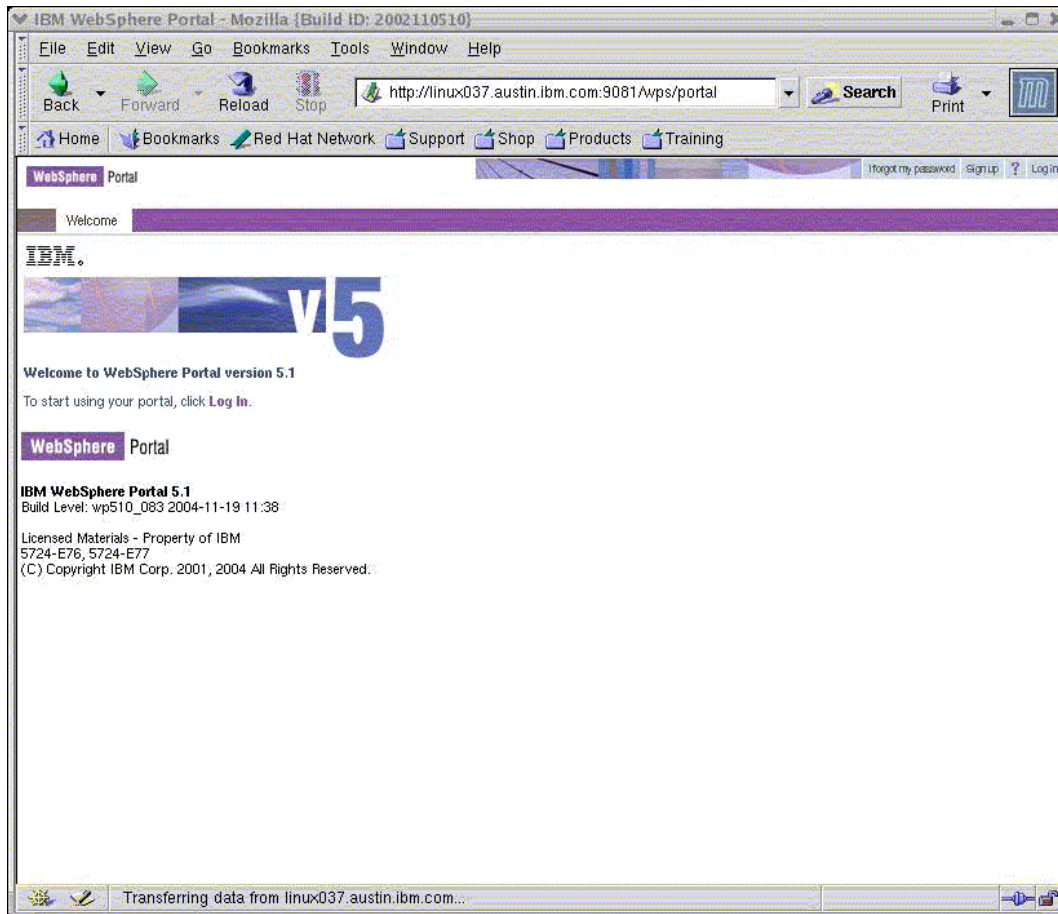


Figure 7-9 WebSphere Portal Welcome page

14. Enter wpsadmin for the User ID and wpsadmin for the Password to log in (Figure 7-10).

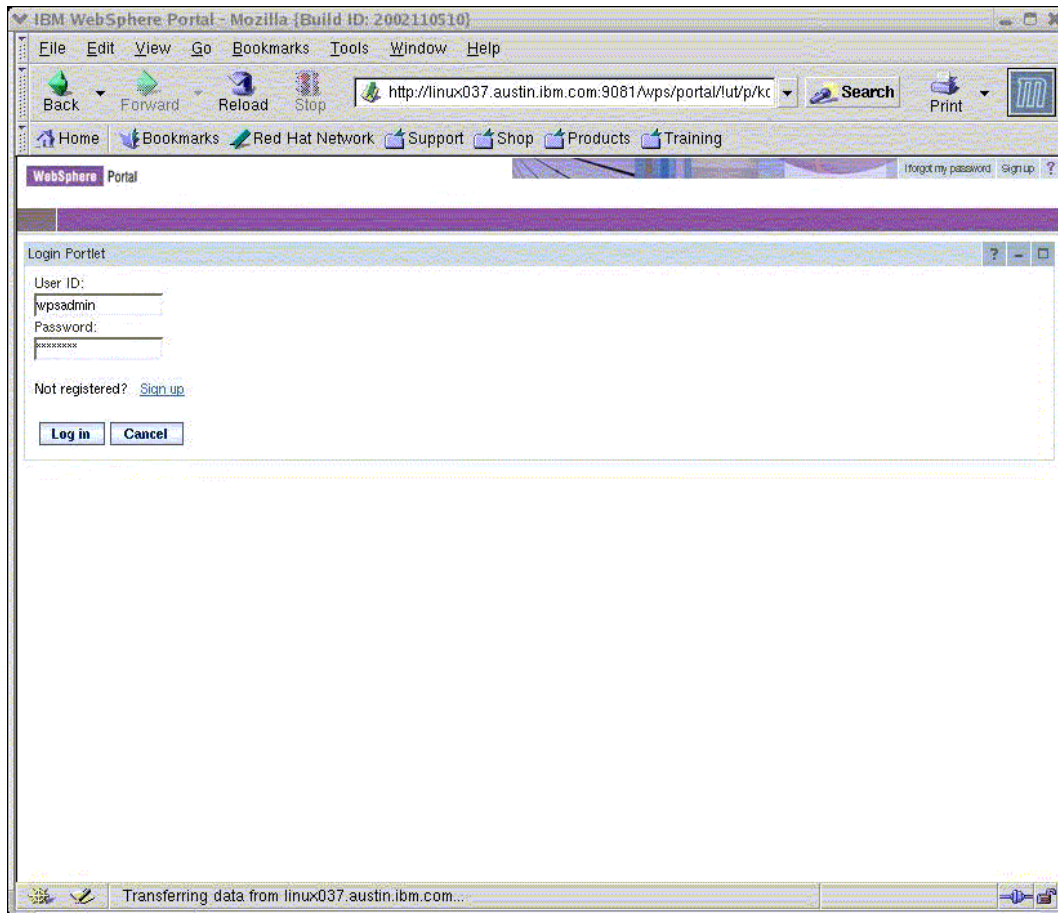


Figure 7-10 WebSphere Portal Login window

15. You should now be logged in to the WebSphere Portal V5.1 Administration page (Figure 7-11).

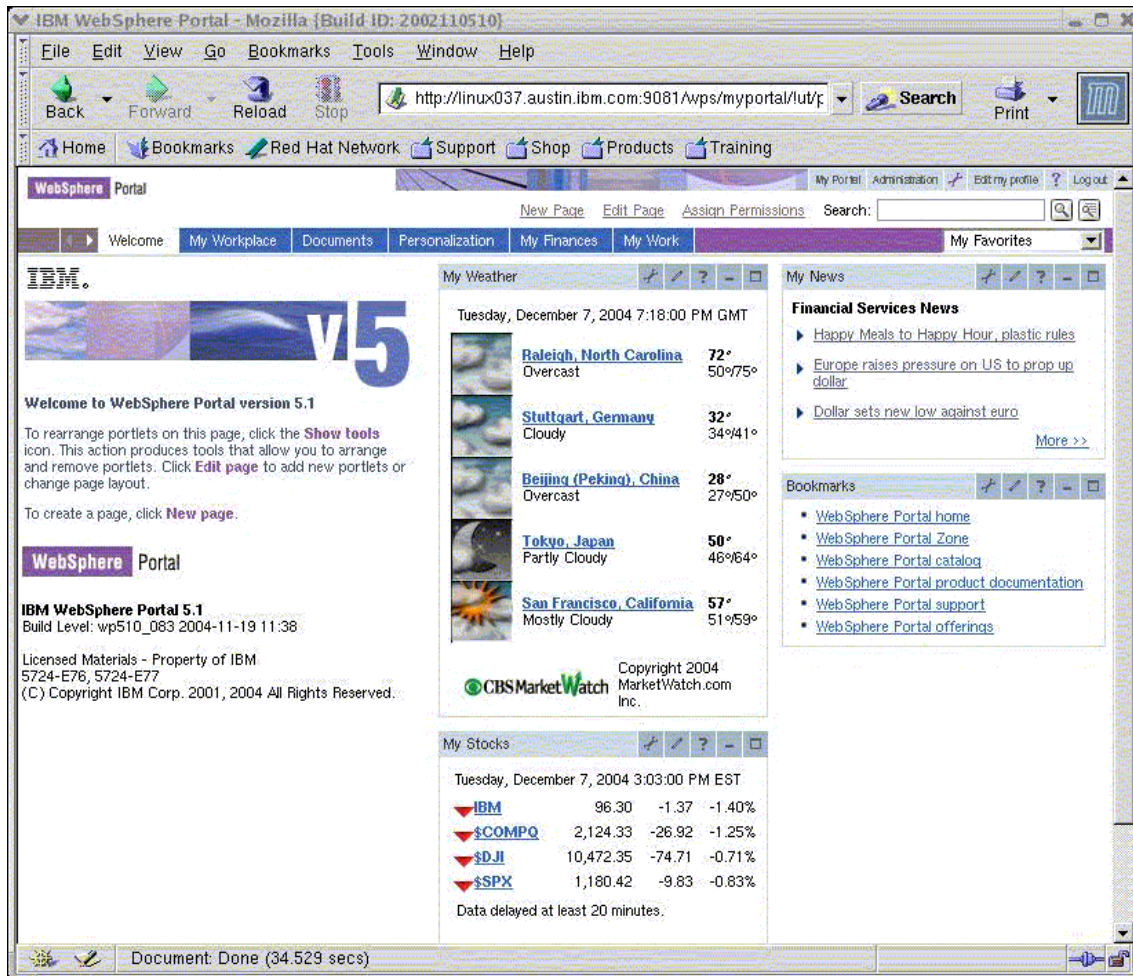


Figure 7-11 WebSphere Portal Administration page





# WebSphere Portal V5.0.2 to V5.1 migration

This chapter describes the steps to migrate from an existing IBM WebSphere Portal V5.0.2 environment to a new WebSphere Portal V5.1 environment.

We organize this chapter into the following topics:

- ▶ WebSphere Portal V5.1 migration overview
  - We discuss the migration to WebSphere Portal V5.1, supported migration paths, changes in WebSphere Portal V5.1, automated migration tasks, and manual migration steps. Figure 8-1 on page 344 shows a diagram simulating our migration.
- ▶ Migration process overview
  - We provide an overview of the five-step migration process.
- ▶ Prerequisites and preparing for the migration
  - We discuss the prerequisites to be completed before starting the migration process for both the WebSphere Portal V5.0.2 and WebSphere Portal V5.1 environments.
- ▶ Portal migration process
  - We perform the steps to migrate from WebSphere Portal V5.0.2 to WebSphere Portal V5.1.

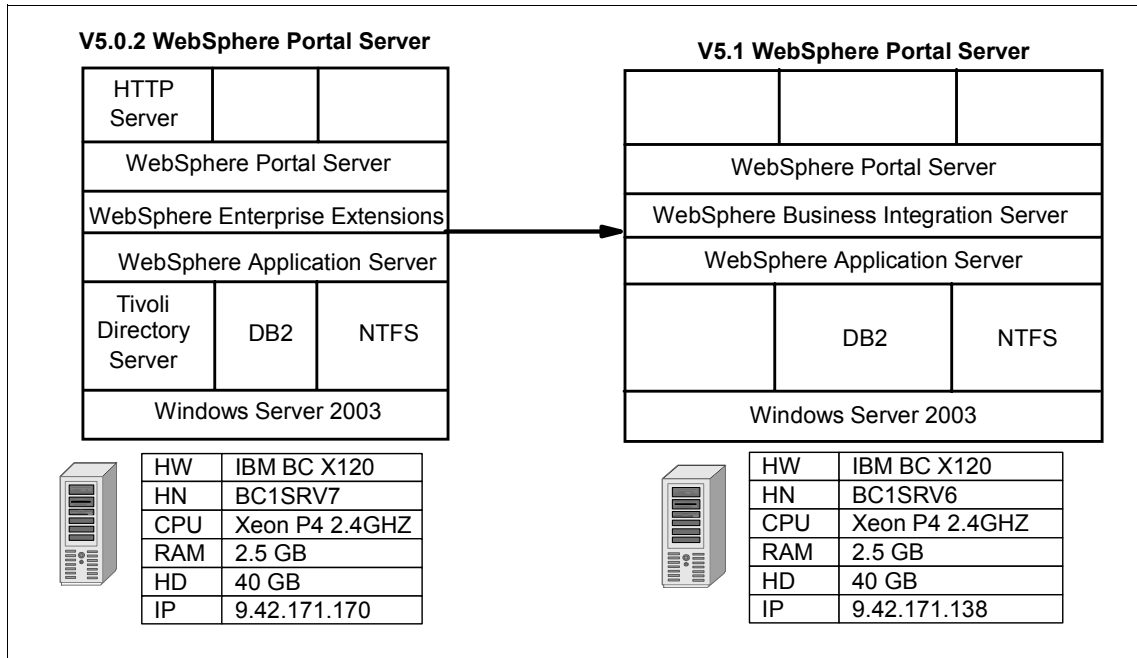


Figure 8-1 Architectural diagram for WebSphere Portal migration

## 8.1 WebSphere Portal V5.1 migration overview

In this section, we discuss WebSphere Portal V5.1 and some items you should understand about V5.1 prior to migrating to this platform:

- ▶ Supported migration paths and resources.

Some important points to consider while planning for the migration to WebSphere Portal V5.1 are:

- You can migrate to WebSphere Portal V5.1 only from WebSphere Portal Versions 4.1.6, 4.2.1, and 4.2.2, and any 5.0.x Version.
- Migration between WebSphere Portal environments running on different operating systems is not supported. For example, migrating from WebSphere Portal V5.0.x running on SUSE LINUX Enterprise Server (SLES) to WebSphere Portal V5.1 running on Windows 2000 is not possible.
- Migration across database servers is also not supported. For example, WebSphere Portal data cannot be migrated from Oracle to DB2 or vice versa.
- The migration of bookmarks or internal URLs is currently not supported and will be made available as a separate utility from the WebSphere Portal support site in the future.

- ▶ Migration in cluster environments.

To migrate from WebSphere Portal V5.0.x in a cluster environment, you need to perform the following steps:

- a. Install a stand-alone WebSphere Portal V5.1. This will serve as the new main node for WebSphere Portal V5.1 in a clustering environment.
  - b. Migrate the data from the WebSphere Portal V4.x or V5.0.x cluster main node to the WebSphere Portal V5.0 cluster main node.
  - c. Verify the successful migration to the WebSphere Portal V5.1 cluster main node.
  - d. Create new clone nodes from the WebSphere Portal V5.1 main node.
- ▶ Changes introduced in WebSphere Portal V5.1 affecting migration (there are many more changes in V5.1, but in this section, we only talk about changes affecting migration):
    - Portlet API changes, deprecations, and enhancements
    - Theme, skin, and taglib changes

## General recommendations for migration

When planning to migrate, you should take a moment to understand the scope of your migration and the specific tasks that might be required. Consider the following recommendations:

- ▶ Read through the migration documentation available with the Web-only version of the *Information Center* before starting any migration procedure, available at:  
<http://publib.boulder.ibm.com/infocenter/wp51help/index.jsp?topic=/com.ibm.wp.ent.doc/wpf/migrationv5.html>
- ▶ Develop a plan for migration: identify tasks, resources needed, testing methodology, and so on.
- ▶ Keep premigration customizations to a minimum.
- ▶ Test migration using a development machine.
- ▶ Use IBM Rational Application Developer for WebSphere Software Version 6.0 with portal tools to debug V5.0.x portlets on the V5.1 test environment.
- ▶ Thoroughly verify all aspects of your portal after migration, especially the access control.

## 8.2 Migration process overview

Prior to getting started, you should understand the typical migration process. Consider the following five-step migration process:

1. Install and configure WebSphere Portal V5.1.
2. Apply the migration fixes to the V5.0.x machine.
3. Complete some manual migration steps.
4. Run the migration tasks supplied with WebSphere Portal V5.1.
5. Migrate the small portion of access control information not covered by the migration tasks involving the manual steps.

**Note:** As you prepare and plan for the WebSphere Portal migration, you should consider the time and effort that will be required to perform this activity in your environment. Planning is key and enables you to address most questions or concerns before you start the migration process.



For more detailed information regarding the WebSphere Portal migration process, we recommend that you review the information in the *Information Center*, available at:

<http://publib.boulder.ibm.com/infocenter/wp51help/index.jsp?topic=/com.ibm.wp.ent.doc/wpf/migrationv5.html>

## 8.3 Prerequisites and preparing for the migration

This section discusses the prerequisites to address before starting the migration process:

- ▶ Install and configure of all components of WebSphere Portal V5.1, which includes:
  - Setting up and configuring WebSphere Portal for the database you plan to use.
  - Setting up and configuring WebSphere Portal for the LDAP server you plan to use.
  - Verifying the database and LDAP server configurations.
- ▶ An operational WebSphere Portal V5.0.2 environment.
- ▶ Migrate the LDAP database of the WebSphere Portal V5.0.2 system to the LDAP server of the WebSphere Portal V5.1 system. Perform the following steps to migrate the LDAP database.

On the WebSphere Portal V5.0.2 system, machine 1:

- a. Stop Tivoli Directory Server from the service console.
- b. Start the Tivoli Directory Server Configuration Tool.
- c. Click **Export LDIF Data**, enter a file name, and click **Export**.
- d. Wait for a success message and then click **Close**.
- e. Close the Tivoli Directory Server Configuration Tool.

You have successfully exported the LDAP database information on machine 1.

On the WebSphere Portal V5.1 system, machine 2:

- a. Stop Tivoli Directory Server from the service console.
- b. Start the Tivoli Directory Server Configuration Tool.
- c. Click **Import LDIF Data**, browse to the LDIF file copied from machine 1, and click **Import**.
- d. Wait for a success message and then click **Close**.

e. Close the Tivoli Directory Server Configuration Tool.

You have successfully migrated the database of Tivoli Directory Server V5.1 on machine 1 to the Tivoli Directory Server V5.2 on machine 2.

**Note:** You do not need to migrate the LDAP database if you are using the same LDAP server for both environments (as we did in our example to simplify things).

- ▶ Apply the migration interim fix to the WebSphere Portal V5.0.2 environment. Perform the following steps to apply the interim fix to your WebSphere Portal V5.0.2 system:

- a. Stop WebSphere Portal and server1 and open a command prompt.
- b. Copy the WP502\_MP\_Express\_patch.jar file from the wp51\_root/migration/efixes/ directory on the WebSphere Portal V5.1 server to the wp50\_root\update\fixes directory.
- c. Extract all the files from the JAR file into the wp50\_root\update\fixes directory.

**Note:** This JAR file is for WebSphere Portal V5.0.2. For other WebSphere Portal versions, see the *Information Center*.

- d. Extract the updated Portal Update Installer from the same location of the patch to the wp50\_root\update directory.
- e. In the command prompt, change to the wp50\_root\update directory.
- f. Install the fixes that came in the JAR file in the following order:
  - i. PQ82292
  - ii. PQ83022
  - iii. PQ89044
  - iv. PQ92163
  - v. PQ92090
  - vi. PQ92314
  - vii. PQ92583

To install the fixes, issue the following command:

```
updateportal.bat -fix -installDir "C:\WebSphere\PortalServer" -fixDir "C:\WebSphere\PortalServer\Update\Fixes" -install -fixJars <fixjarname>
```

**Note:** The <fixjarname> value will be replaced by PQ82292.jar on the first run and will then replace the PQ number each time until all fixes are installed.

- g. Restart WebSphere Portal.
- h. Verify that everything is working correctly.
- ▶ Make portlet applications available to the migration tasks for deployment.
 

Before making your custom portlets available for migration, you should update the portlet source code so that the portlets can work on WebSphere Portal V5.1. Refer to the section “Migrating custom portlet code in Manual migration steps” in the *WebSphere Portal V5.1 Information Center*. Most portlets that ran on V5.0 will run fine on V5.1. After you finish updating, there are two methods with which you can make the portlet applications available for migration:

  - Create WAR files of each portlet application you want to migrate and copy them to the <wp51\_root>/installableApps directory.
  - Edit the appsPath setting in the mig\_core.properties file, as discussed in the following Note box, and point to another directory where you have placed these files.

**Note:** The path entered as the value of the parameter appsPath should be accessible from the WebSphere Portal V5.1 system. In our example, we placed the files into installableApps, that way, all updated portlets for V5.1 will be picked up.

- ▶ Specify values in the properties files.
 

Providing values to the parameters in the property files enables you to invoke various migration tasks without supplying individual parameters on the command line. There are, in all, three property files for migration, two of which we describe here:

  - mig\_core.properties, where you specify the core migration properties. Column 2 in Table 8-1 indicates the values you need to enter for this sample scenario for the parameters in column 1. Column 3 provides a brief description of each parameter.

Table 8-1 Values for parameters in the mig\_core.properties file

Property	Value	Description
PrevWpsHostName	bc1srv7.itso.ral.ibm.com	Previous portal's host name.
PrevWpsPort	9081	The port you used to access the previous portal.

Property	Value	Description
PrefWpsContextRoot	wps	Previous portal's context root.
PrefWpsDefaultHome	portal	Previous portal's home.
PrevPortalAdminId	portaladmin	The administrator ID for the previous portal.
PrevPortalAdminPwd	portaladmin	The password for that administrator.
PrevWpsInstallLocation	Z:/WebSphere/PortalServer	If the other server is accessible, you can map a drive to it and do this.
pathUpgradedThemesSkins	c:/wpsupdate	Place where you have placed the updated themes and skins on the new server.

**Note:** The values in Table 8-1 are provided to help you document the parameters correctly based on our migration.

For more information regarding these parameters, see the Migration Task referenced in the WebSphere Portal V5.0.2 Information Center (click **Migrating** on the first page) at the following URL:

<http://publib.boulder.ibm.com/infocenter/wp51help/index.jsp>

- mig\_wmm.properties, when migrating from V5.0.x to V5.1 there is no need to update this file.
- ▶ Copy the wps.properties file from the <wp50\_root> directory of your WebSphere Portal V5.0.2 system to the <wp51\_root>/migration directory of the WebSphere Portal V5.1 system.
- ▶ Ensure that all groups in Tivoli Directory Server V5.1 on WebSphere Portal V5.0.2 have at least one member. Otherwise, some of the migration tasks will fail.

## Manual migration steps

There have been some significant changes to the API and to the navigation model used in WebSphere Portal V5.1. You must complete the following steps prior to running the migration tasks:

- ▶ Migrate your Struts portlets to the latest version. If you do not, they will not run correctly. See the following topic about updating your Struts portals:

[http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/wpf/mig\\_prep.html#update\\_struts](http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/wpf/mig_prep.html#update_struts)

- ▶ Migrate your themes and skins according to the following topic, because we could not cover the changes you might need to make in your scenario in this document:

[http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/wpf/mig\\_prep.html#update\\_themes\\_skins](http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/wpf/mig_prep.html#update_themes_skins)

**Note:** If you do not do the migration steps for your themes and do copy them to the `was_root\installedapps\<cell name>\wps.ear\wps.war\themes\html\` directory, it is likely that your page will not render, because the tag that causes the rendering of the page has changed.

## 8.4 Portal migration process

In this section, we continue with our example of migrating from WebSphere Portal V5.0.2 to WebSphere Portal V5.1.

Before running the migration tasks, complete the following steps:

1. On machine 1, make sure WebSphere Portal V5.0.2 is up and running.
2. On machine 2, make sure WebSphere Portal V5.1 is up and running.
3. On machine 2, open a command prompt and change to the migration directory (C:\WebSphere\PortalServer\migration).

**Note:** All migration tasks are run on the target server.

### 8.4.1 Migrating access controls on user groups

In this section, we migrate the access controls of the user groups. Complete the following steps:

1. From the command prompt, run the following command:

```
WpMigrate.bat migrate-user-groups-ac
```

Wait for the task to end; it should end with a `Build Successful` message.

2. Verify that the migration was a success by completing the following steps:
  - a. Log in to the WebSphere Portal V5.1 administrative interface.
  - b. Click **Access** → **Users and Group Permissions**. Under Users and User Groups, click **Users**.
  - c. From the Search on option box, select **givenName**, and in the Search for text box, enter the user name of a user with access controls on user groups in WebSphere Portal V5.0.2. Click **Search**.
  - d. Click the **Select Resource Type** icon next to the user name of the user you for which you just searched, and then under Resource Types, click **User Groups**.
  - e. You will see a window with a list of user groups. From the drop-down list, select **All available** and then click **Search**.

- f. You should see a window similar to the one shown in Figure 8-3 on page 354. Verify the permissions with the permissions the user has for the selected group on WebSphere Portal V5.0.2, as shown in Figure 8-2. For this scenario, the Manage permission and the Delegate permission equal an administrator role.

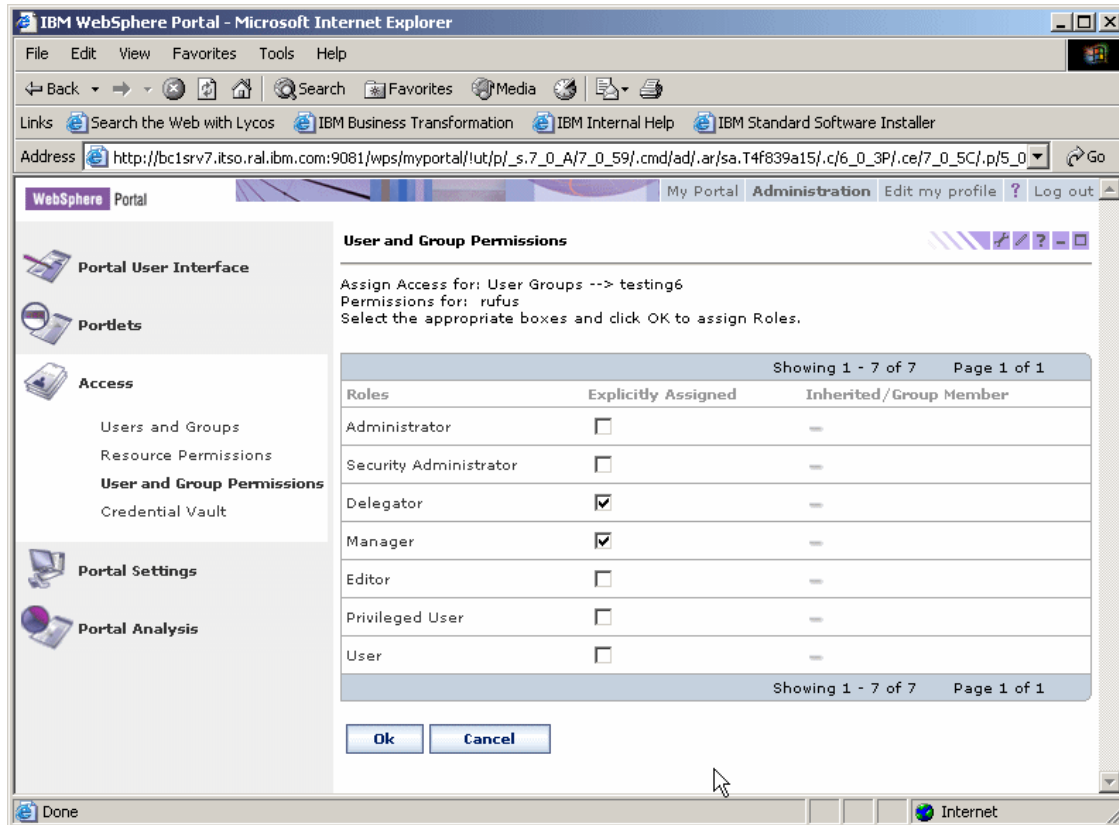


Figure 8-2 Permission-based access control on a group on WebSphere Portal V5.0.2

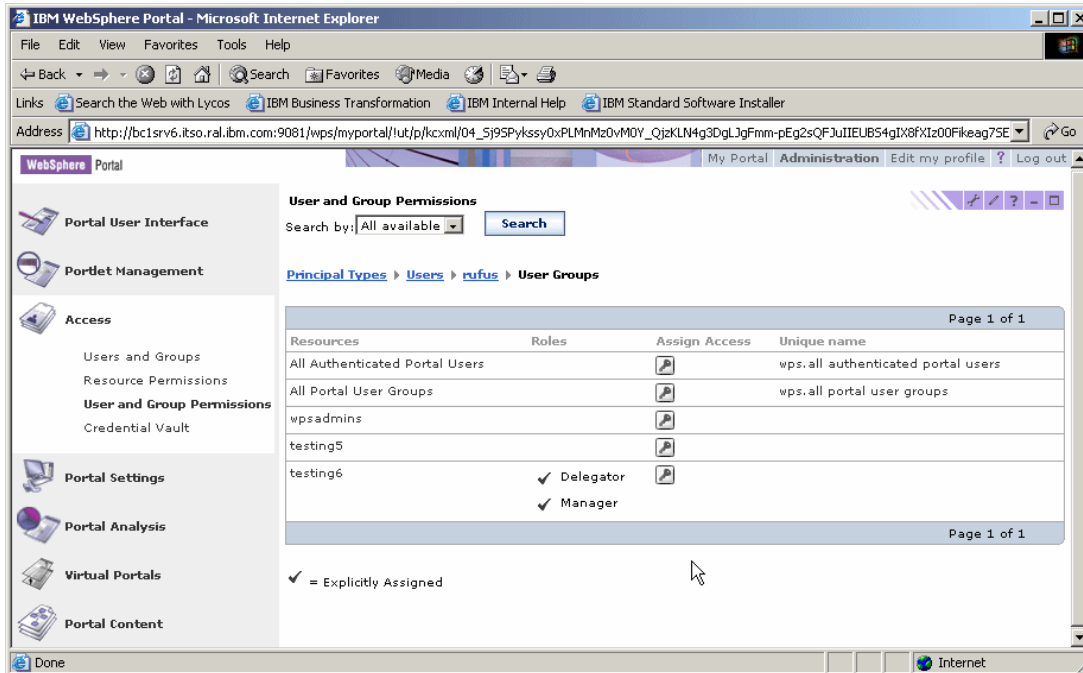


Figure 8-3 Role-based access control on a group on WebSphere Portal V5.1

- g. Perform the same type of verification for other users with access controls on user groups on WebSphere Portal V5.1.

## 8.4.2 Migrating virtual resources

To migrate the virtual resources from the V5.0.X system to the V5.1 system, from the command prompt, run the following command:

```
WpMigrate.bat migrate-virtual-resources
```

Wait for the task to end; it should end with a Build Successful message.

## 8.4.3 Migrating credential slots and segments

To migrate the credential slots and segments to the V5.1 system, complete the following steps:

1. From the command prompt, run the following command:

```
WpMigrate.bat migrate-credential-slots-segments
```

Wait for the task to end; it should end with a Build Successful message.



2. Verify that the migration was a success by completing the following steps:
  - a. Log in to the WebSphere Portal V5.1 administrative interface.
  - b. Click **Access** → **Credential Vault** and then click **Manage System Vault Slots**.
  - c. You should see a window similar to the one shown in Figure 8-5 on page 356. Verify the permissions with the permissions the user has for the selected group on WebSphere Portal V5.0.2, as shown in Figure 8-4.

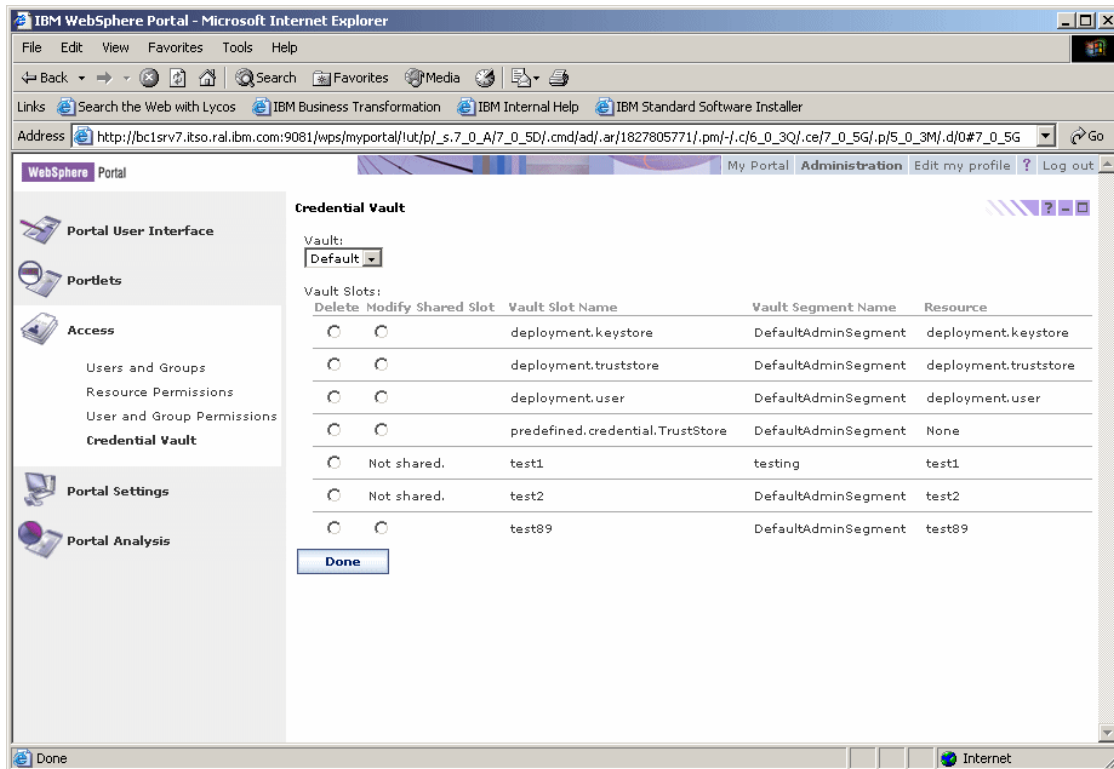


Figure 8-4 Credential Vault Slots in WebSphere Portal V5.0.2

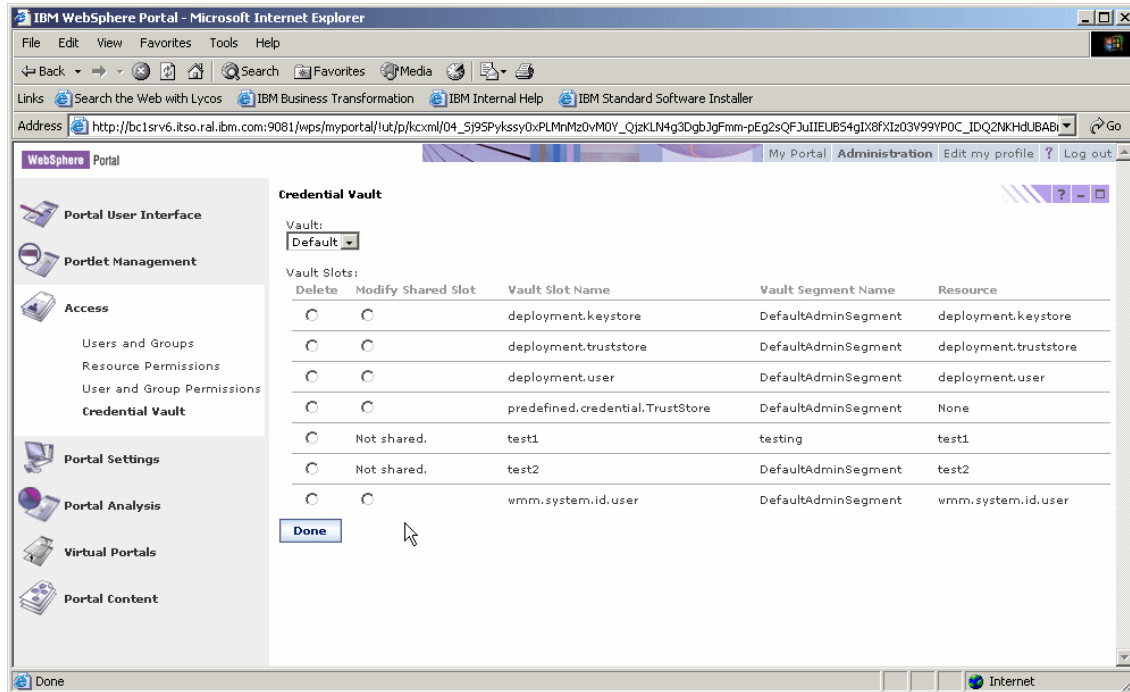


Figure 8-5 Credential Vault Slots in WebSphere Portal V5.1

## 8.4.4 Migrating pages, themes, skins, and applications

In this section, we perform the migration of the pages, labels, themes, skins, and portlet applications.

**Important:** Currently, there is an unhandled condition in the migration code. If your labels, pages, and portlets do not have unique names, they will be overlooked. Before proceeding with these steps, assign unique names to all the pages, portlets, and labels. A fix for this is planned to be released.

**Note:** In our environment, we created a label Jims test area with five pages beneath it (labelled efix list, puma, customer, test, and vault) with eight portlets placed on those various pages. Additionally, the theme required updating. See the *Information Center* for information about all the updates you must make for the theme. (In our example, we had a modified science theme, so we borrowed from that theme to do the update.)

Complete the following steps:

1. From the command prompt, run the following command:

```
WpMigrate.bat migrate-pages
```

Wait for a task to end; it should end with a `Build Successful` message.

2. Stop the WebSphere Portal V5.1 machine by issuing the following command from `was_root\bin`:

```
stopserver.bat WebSphere_Portal -user was_admin -password
was_admin_password
```

3. Copy the themes and skins to the correct location.
4. Start the server by issuing the following command from `was_root\bin`:

```
startserver.bat WebSphere_Portal
```
5. Verify that the migration was a success by completing the following steps:
  - a. Log in to the WebSphere Portal V5.1 administrative interface.
  - b. Click **Portlets** → **Manage Applications** on the left navigation pane.

- c. Verify that all the portlet applications listed as migrated are present under Web modules. For this scenario, the arrows (blue) in Figure 8-6 indicate the portlet applications migrated from WebSphere Portal V5.0.2 to WebSphere Portal V5.1; this is also indicated by the arrows (blue) in Figure 8-7 on page 359.

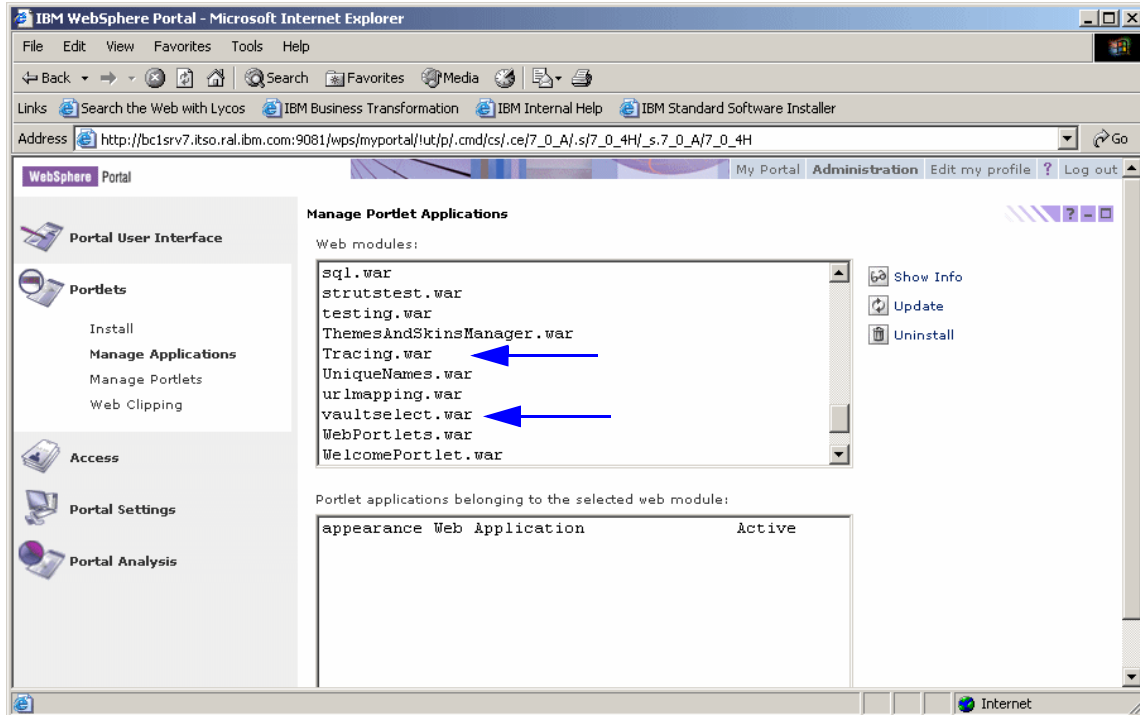


Figure 8-6 Portlet applications listed for migration from WebSphere Portal V5.0.2

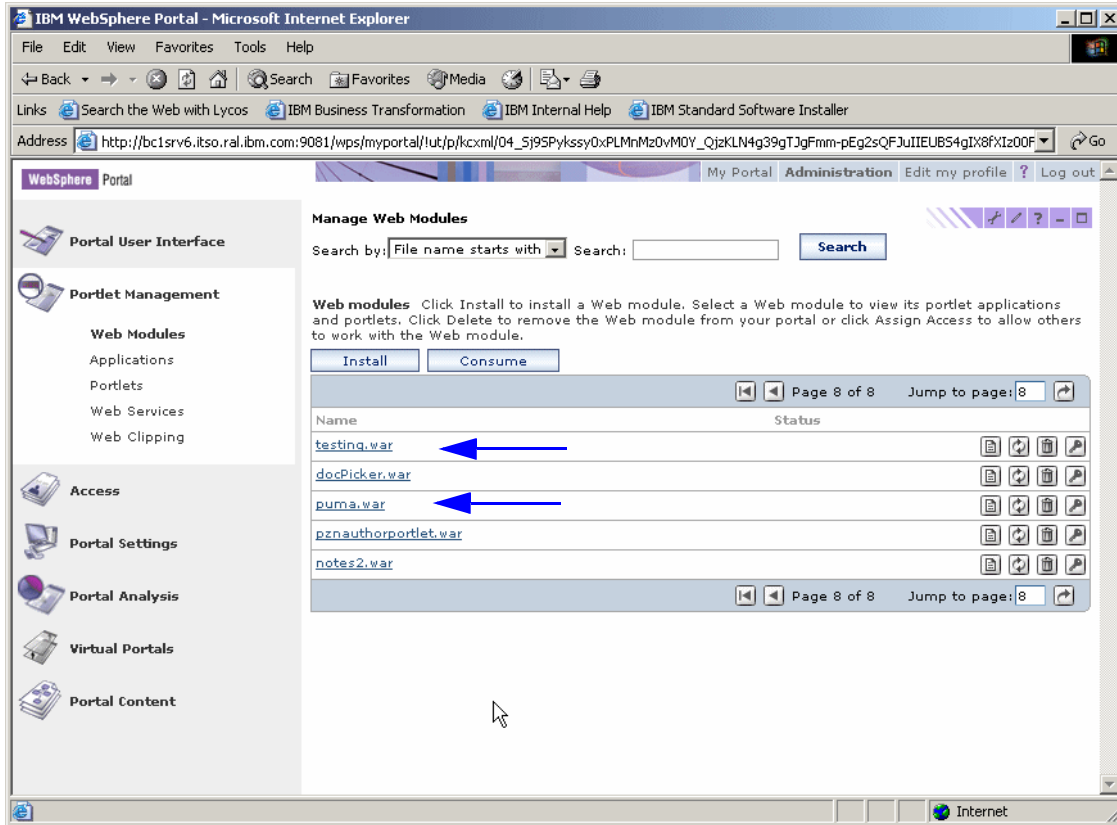


Figure 8-7 Portlet applications migrated to WebSphere Portal V5.1

- d. For each Web module migrated, verify that all portlet applications related to the Web module are also display in the Portlet Applications list. See Figure 8-6 on page 358 and Figure 8-7 for reference.

- e. Select each portlet application that was migrated and click **Modify parameters** to verify that the parameters that were set up for the portlet applications have also been migrated correctly. Verify this by looking at the InitialViewState parameter for the XmlAccess - Run File portlet from WebSphere Portal V5.0.2 to WebSphere Portal V5.1. Figure 8-8 shows how it looked in the WebSphere Portal V5.0.2 system, and Figure 8-9 on page 361 shows how it appears in WebSphere Portal V5.1.

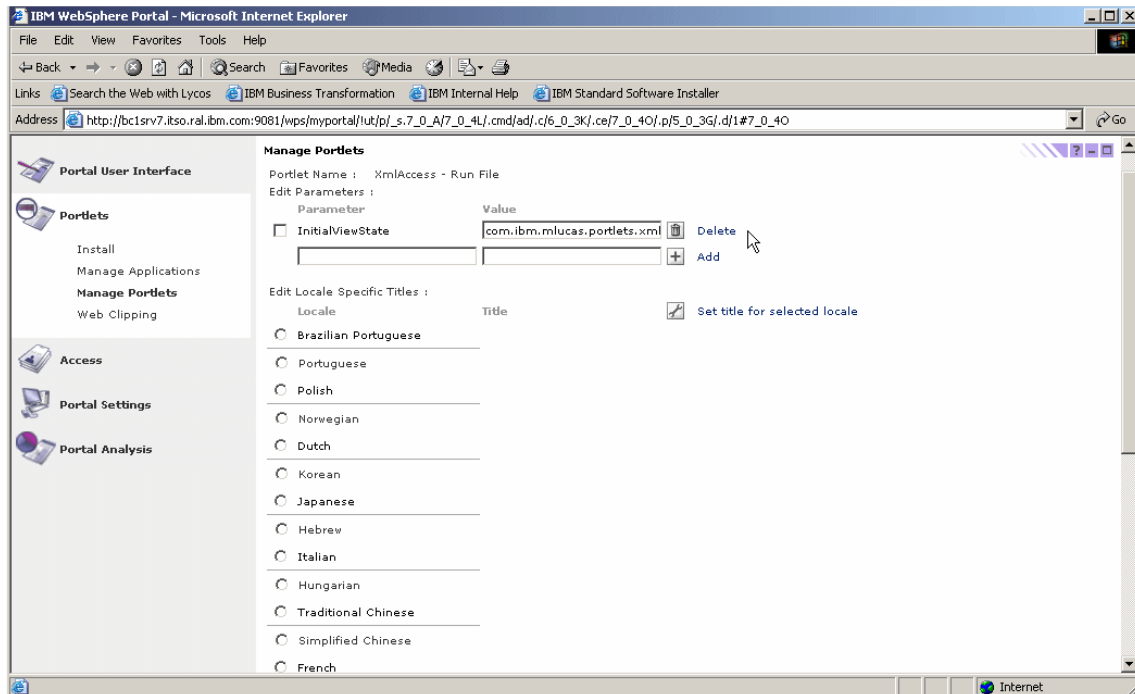


Figure 8-8 InitialViewState parameter for XMLAccess - Run File portlet on WebSphere Portal V5.0.2

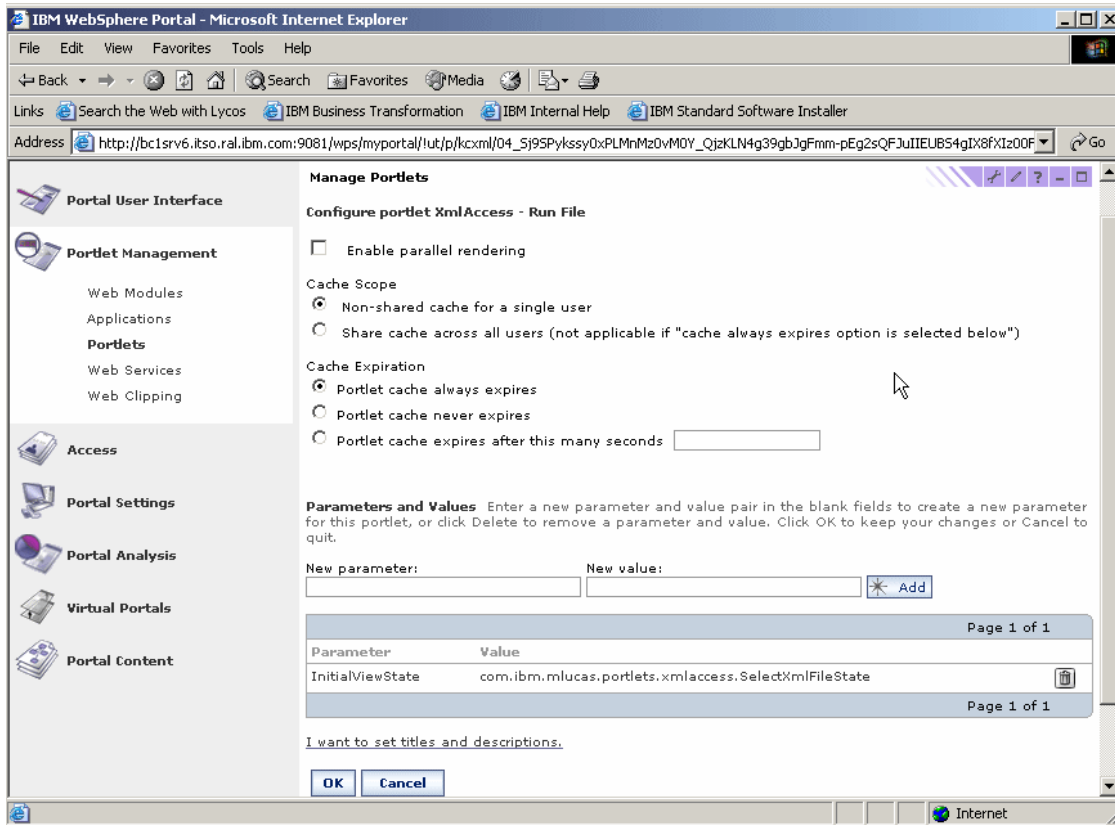


Figure 8-9 InitialViewState parameter for XMLAccess - Run File portlet on WebSphere Portal V5.1

- f. Verify also that all pages have been migrated along with the portlets and label. Log in to WebSphere Portal and verify that the same pages under Jims test area on the WebSphere Portal V5.0.2 system, as shown in Figure 8-10 on page 362, also exist under that label in the V5.1 system, as shown in Figure 8-11 on page 362.

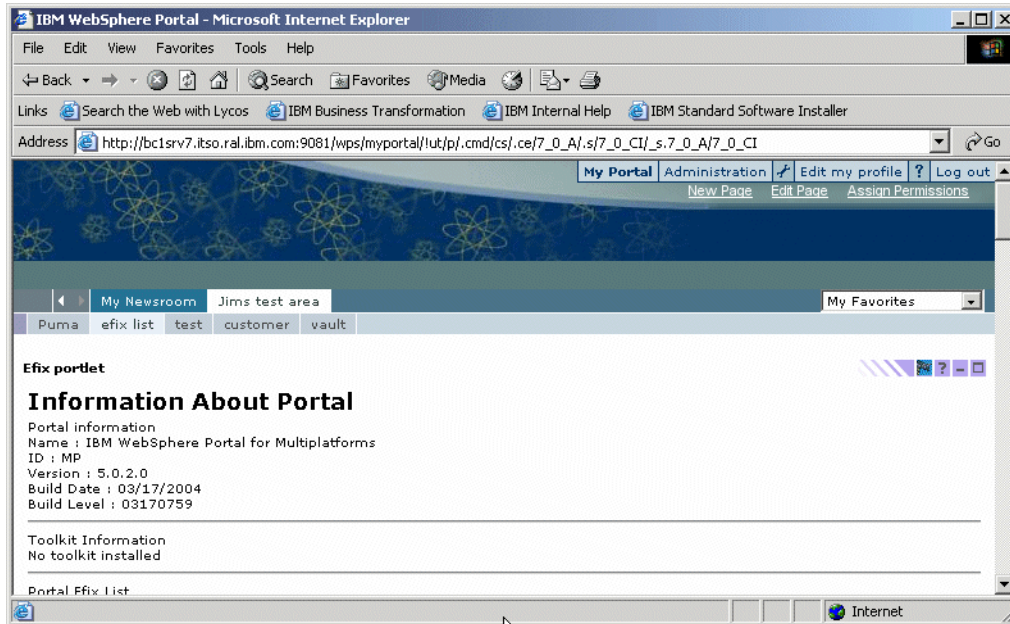


Figure 8-10 Pages as they appear in the V5.0.2 system

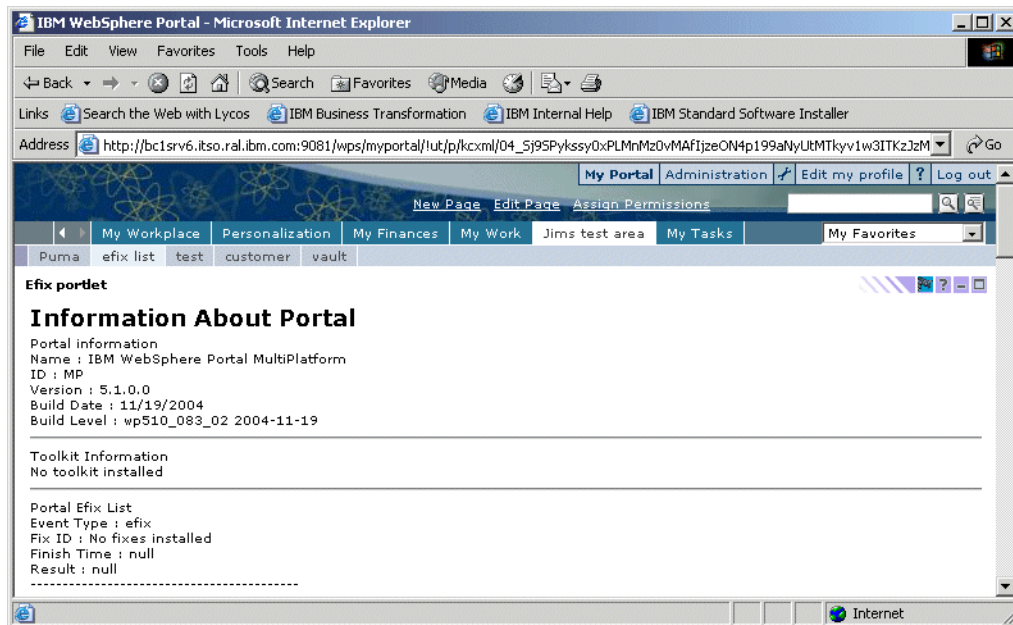


Figure 8-11 Pages as they appear in the V5.1 system



6. Verify the migration of the access control for the migrated portlet applications and portlets. In the administrative interface, click **Access** → **Resource Permissions**, and then under Resource Types, click **Portlet Applications**.

### 8.4.5 Migrating all the user customizations

To migrate all the user customizations, complete the following steps:

1. From the command prompt, run the following command:  
`WpMigrate.bat migrate-user-customizations`  
Wait for the task to end; it should end with a `Build Successful` message.
2. Verify that the migration was a success by completing the following steps:
  - a. Log in to the WebSphere Portal V5.1 with the credentials of a user who has customizations in WebSphere Portal V5.0.2.

- b. Browse to the migrated page in which the user has a customized portlet or portlets. For this scenario, go to the *efix list* page in the Jims test area page under My Portal. Verify that all the customizations from WebSphere Portal V5.0.2 are present in WebSphere Portal V5.1. For this scenario, Figure 8-12 and Figure 8-13 on page 365 indicate the migration of customizations on the *efix list* page from WebSphere Portal V5.0.2 to WebSphere Portal V5.1, respectively.

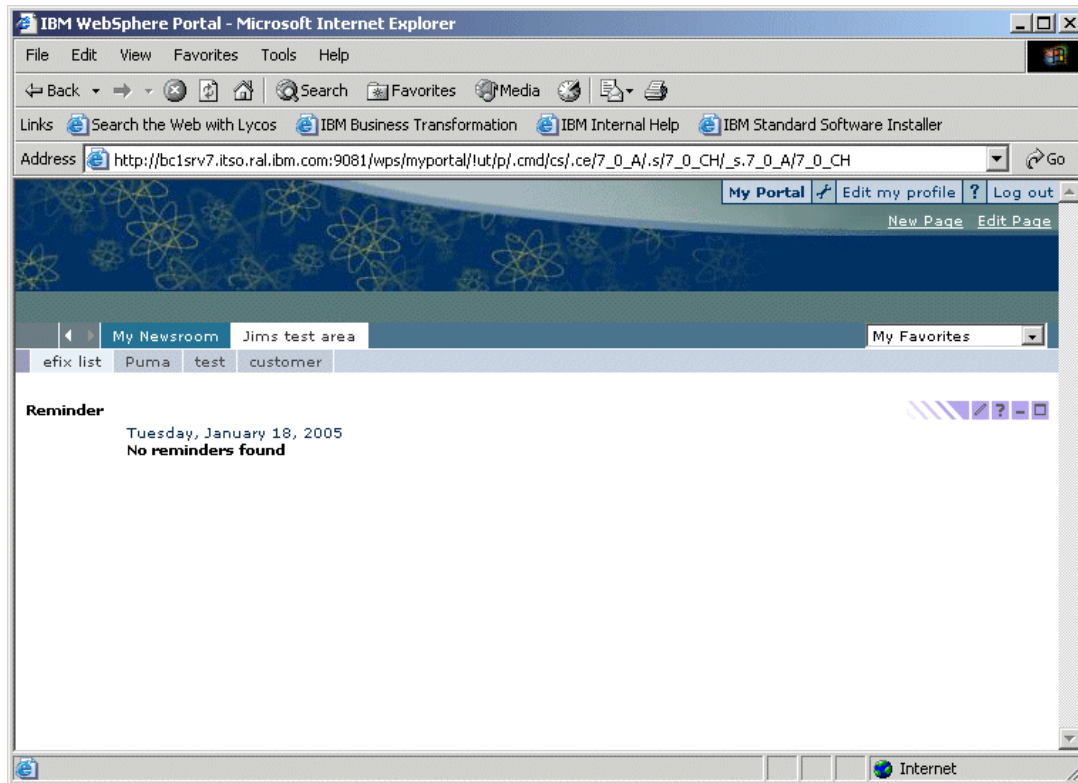


Figure 8-12 User customization for the *efix list* page in WebSphere Portal V5.0.2

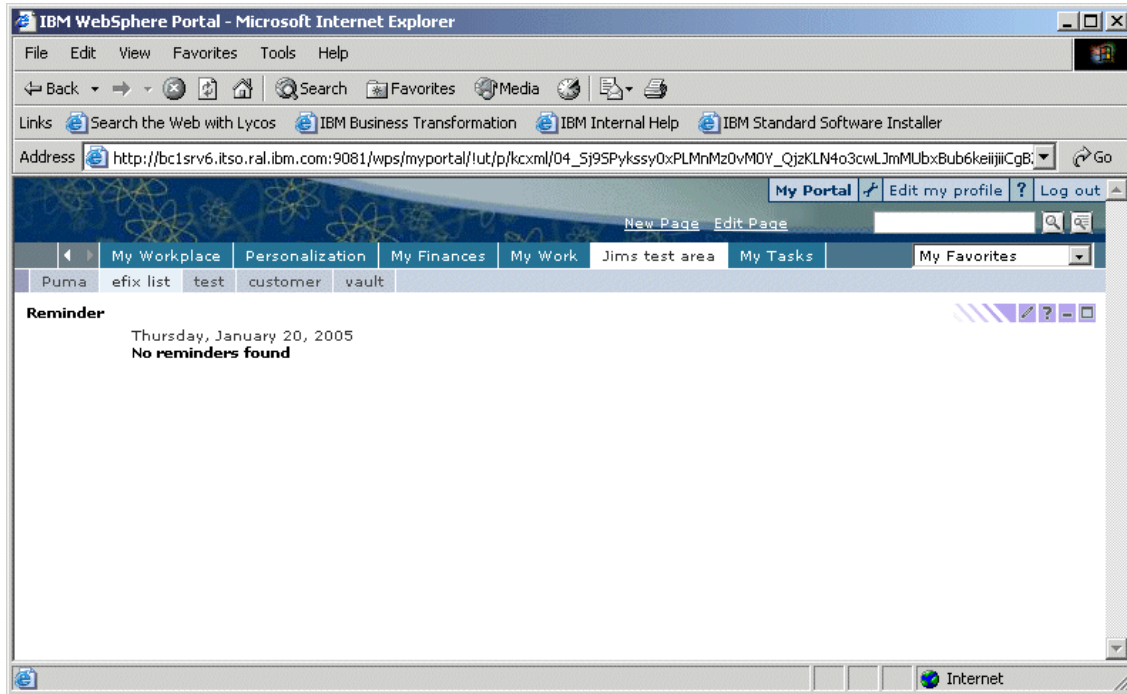


Figure 8-13 User customization for the efix list page in WebSphere Portal V5.1

- c. Perform the verification for other users with customizations on WebSphere Portal V5.0.2.

## 8.4.6 Migrating credential vault data

Migrating the credential vault data involves moving the data from two tables, VAULT\_DATA and VAULT\_RESOURCES, from the WebSphere Portal V5.0.2 database to the WebSphere Portal V5.1 database. Complete the following steps:

1. Perform the following steps on machine 1 to export these tables from the WebSphere Portal V5.0.2 database:
  - a. Start the DB2 command line processor by clicking **Start** → **All Programs** → **IBM DB2** → **Command Line Tools** → **Command Line Processor**.
  - b. Connect to the WebSphere Portal database:
 

```
connect to <wps50db> user <db2user> using <db2userpwd>
```

c. Run the following commands:

```
export to c:/temp/vault.data.wp5.ixf of ixf messages c:/temp/vault.data.
wp5.msgtxt select * from VAULT_DATA
export to c:/temp/vault.res.wp5.ixf of messages
c:/temp/vault.res.wp5.msgtxt select * from VAULT_RESOURCES
```

d. Disconnect from the WebSphere Portal database:

```
disconnect <wps50db>
```

Where <wps50db> is name of WebSphere Portal V5.0.2 database, <db2user> is the user ID of the database administrator, and <db2userpwd> is the password of this user ID.

2. Perform the following steps on machine 2 to import the data into the same tables of the WebSphere Portal V5.1 database:

a. Copy the vault.data.wp4.ixf and vault.res.wp4.ixf files from machine 1 to the same directory in machine 2.

b. Start the DB2 command line processor by clicking **Start** → **All Programs** → **IBM DB2** → **Command Line Tools** → **Command Line Processor**.

c. Connect to the WebSphere Portal database:

```
connect <wps51db> using <db2user> password <db2userpwd>
```

d. Run the following commands:

```
import from c:/temp/vault.data.wp5.ixf of ixf modified by
indexschema=<db2user> messages c:/temp/vault.data.wp51.msgtxt insert
into VAULT_DATA
import from c:/temp/vault.res.wp5.ixf of ixf modified by
indexschema=<db2user> messages c:/temp/vault.res.wp51.msgtxt insert into
VAULT_RESOURCES
```

e. Disconnect from the WebSphere Portal database:

```
disconnect <wps51db>
```

Where <wps51db> is name of WebSphere Portal V5.1 database, <db2user> is the user ID of the database administrator, and <db2userpwd> is the password of this user ID.

**Note:** The import into the VAULT\_RESOURCES table might generate some errors. If the error indicates that a row with the same resource name already exists, this is fine. This table only defines resource names for use in the vault. If they already exist, there is no need to redefine them, and this will not cause a problem in the subsequent import.

3. Verify that the migration was successful by completing the following steps:
  - a. Log in to the WebSphere Portal V5.1 administrative interface.
  - b. Click **Access** → **Credential Vault** on the left navigation pane.
  - c. Click **Manage system vault slots** and select the **Modify shared slot** option for Test89.
  - d. The value of the Shared userid field should be the one Test89 had in the WebSphere Portal V5.0.2 environment. You should see something similar to the window shown in Figure 8-14, and if you have a portlet that can query the vault slots, you will see something similar to the window shown in Figure 8-15 on page 368.

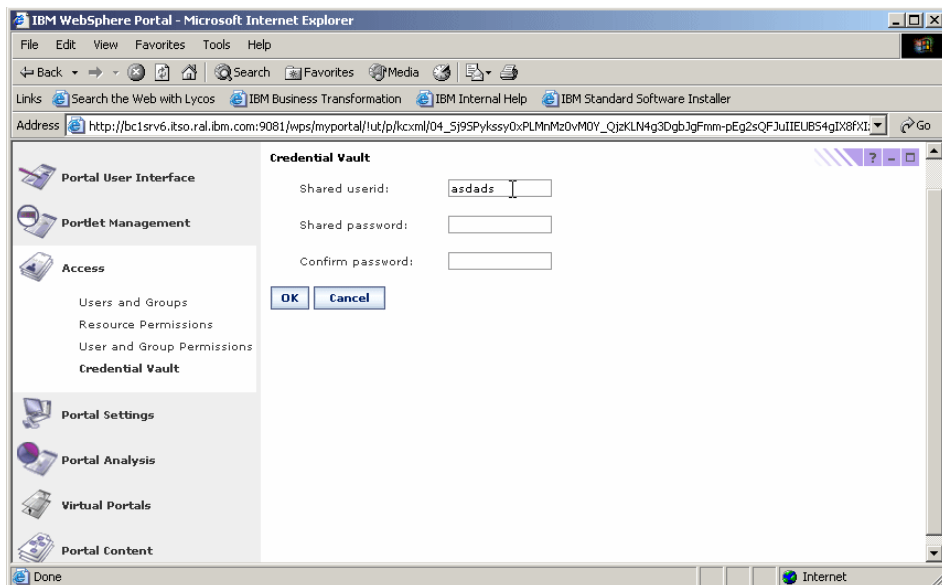


Figure 8-14 Verification of credential data migration

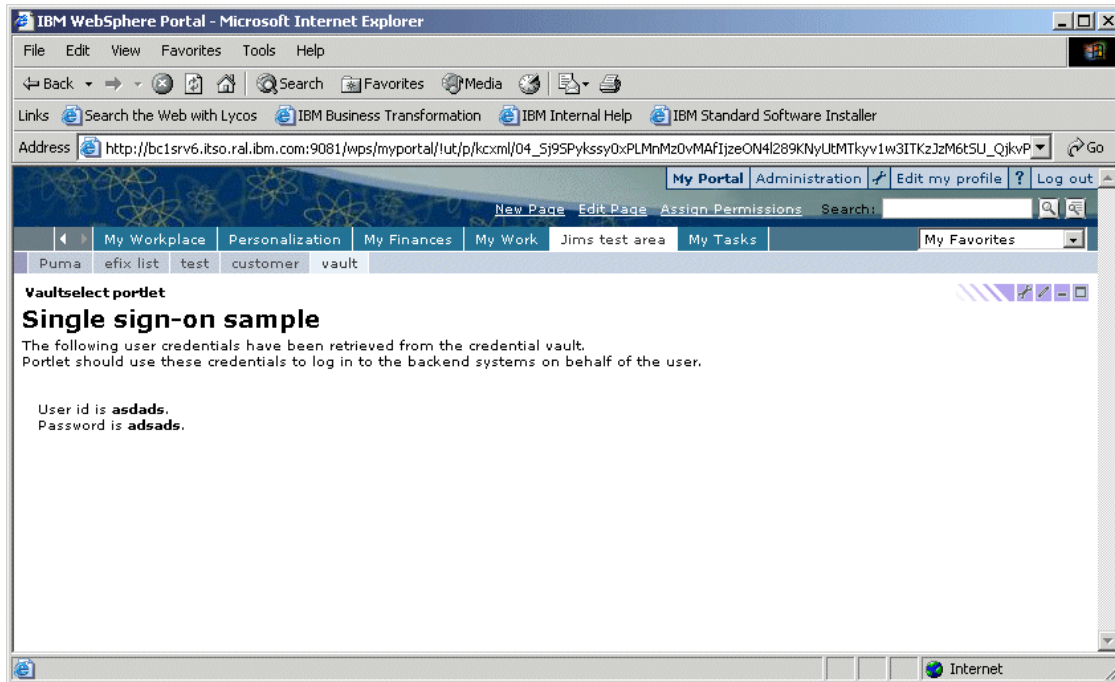
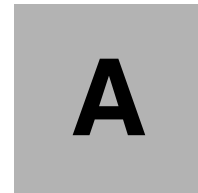


Figure 8-15 Portlet that can query the credential vaults shows that the data was migrated



# Identity management

This appendix provides an overview of Member Manager for IBM WebSphere Application Server, or simply WebSphere Member Manager, formerly known as WebSphere Member Services.

# WebSphere Member Manager

WebSphere Member Manager empowers WebSphere Portal with advanced capabilities to handle member data and profiles. A member of WebSphere Member Manager is one of the following types: a person, organization, organizational unit, or group. This is one of the key differentiators from WebSphere Portal.

Member Manager provides the following functions to the portal:

- ▶ A common profile management mechanism for WebSphere products to access and manage member profiles using attributes regardless of where and how the data of member profiles is stored. By default, WebSphere Portal uses seven attributes, namely, a unique identifier, a user password, a group, a first name, a last name, an e-mail address, and a preferred language.
- ▶ A set of services to act on and manage profiles, such as create, read, update, remove, search members, and manage groups in the profile repository.
- ▶ A hierarchical structuring of members.
- ▶ Database profile repository adapters to interact with the supported database profile repository.
- ▶ Lightweight Directory Access Protocol (LDAP) profile repository adapters to interact with the supported LDAP servers.
- ▶ Not all attributes can be stored in LDAP. A look-aside profile can be used for some those profiles, such as a composite attribute. WebSphere Member Manager provides a look-aside profile repository adapter to interact with a look-aside repository.
- ▶ A programmatic way to define new attributes and various member-related tasks in the profile repositories. Tasks can be performed programmatically by calling methods on the Member Manager API. The Member Manager API is contained in the following packages:
  - `com.ibm.websphere.wmm`, which contains the `MemberService` interface, the main interface of the Member Manager API. The methods in the `MemberService` interface enable you to perform member management operations.
  - `com.ibm.websphere.wmm.objects`, which contains enterprise bean home and remote interfaces for the stateless session bean used to implement the Member Manager API.
  - `com.ibm.websphere.wmm.datatype`, which contains interfaces and classes for parameters used by the methods of the Member Manager API.
  - `com.ibm.websphere.wmm.exception`, which contains classes for exceptions thrown by the Member Manager API.



- `com.ibm.websphere.wmm.adapter`, which contains class interfaces for developing profile repository adapters to connect profile repositories to Member Manager. The two adapters provided by Member Manager are developed according to the interfaces in this package.
- ▶ Tools and utilities, such as WebSphere Member Manager Attributes Loader, to assist developers to test, develop, and integrate WebSphere Member Manager.

## WebSphere Member Manager supported configuration

In general, information within a member profile for a person can be divided into the following three main categories:

- ▶ Profile information, such as name, title, address, e-mail, and demographical information
- ▶ Authentication information, such as a logon ID and password used for security and identification when logging on to a system
- ▶ Privilege information, such as roles for the person and the access control groups to which the member belongs

The information for a person may or may not be stored in the same storage location. For example, a client might have an existing LDAP profile repository whose schema cannot be changed to accommodate additional attributes required by an application. It could be for business or technical reasons that the new attributes cannot be accommodated. A look-aside repository can be used for the additional attributes and applications by using Member Manager, which will not be aware that two repositories are being used.

Another scenario is that the look-aside repository supports composite attributes that are typically not supported by LDAP profile repositories. For example, address is an example of a composite attribute. If a customer wants to use composite attributes, the customer can use the look-aside repository together with the LDAP profile repository, and the look-aside repository can supplement the capability of the LDAP repository.

Member Manager supports the following configurations:

- ▶ Profile repository: A repository where user profiles are stored. A profile repository can be either a database profile repository (such as `wmmDB`), an LDAP profile repository (such as `wmmLDAP`), or a *custom profile repository*. The custom repository can be of any nature, including a database or an LDAP server.

- ▶ Look-aside repository: A repository provided with Member Manager as a storage location for additional attributes that cannot be accommodated in the main profile repositories. For example, composite attributes are not supported in LDAP, and these types of attributes can be stored in the look-aside repository.

Member Manager can be configured in the following ways:

- ▶ Database repository only (Figure A-1)

The database repository is the only main repository. All profile data is stored in the WebSphere Member Manager database. By default, the base WebSphere Portal installation configures WebSphere Member Manager to use database repository only.

- ▶ LDAP Repository only (Figure A-1)

The LDAP repository is the only main repository. All profile data is stored on an LDAP server. Executing the **enable-security-ldap** command during the portal configuration tasks enables WebSphere Portal to work with an LDAP server.

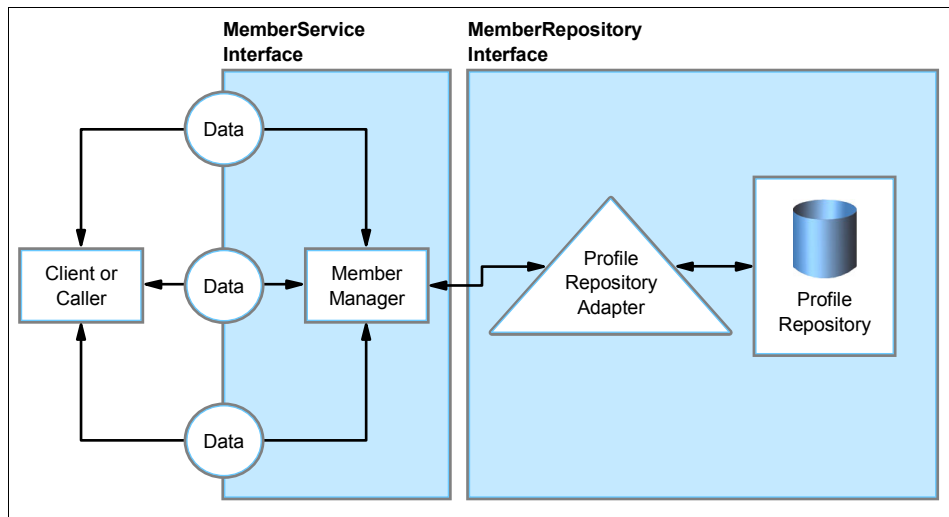


Figure A-1 Single profile repository

► LDAP repository plus look-aside repository (Figure A-2)

The LDAP repository is the main repository. It stores attributes specified in the WebSphere Member Manager LDAP Attributes XML file. The rest of the attributes are stored in the look-aside repository. The look-aside repository usually stores attributes that cannot be stored on the LDAP server, such as composite attributes. If all attributes you are using are supported by the LDAP server, there is no need to use the LDAP repository plus look-aside repository configuration. You can use the LDAP only configuration instead.

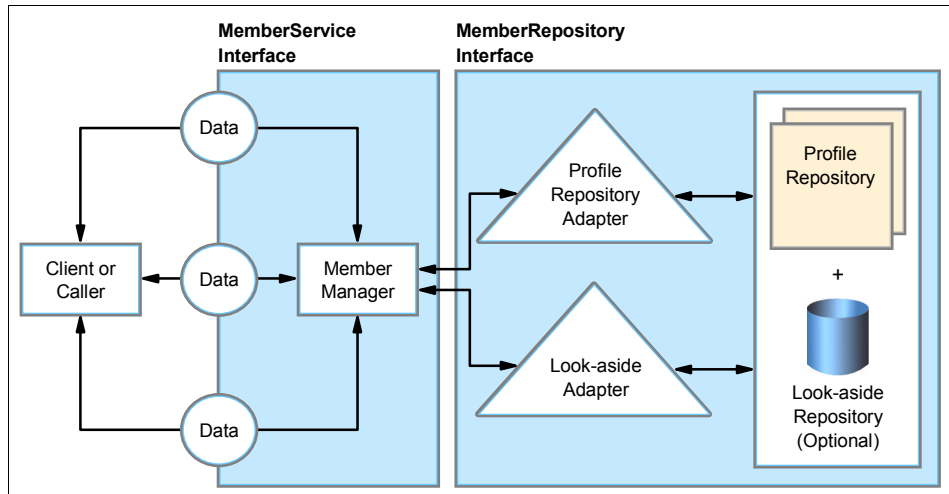


Figure A-2 A profile repository plus a look-aside repository

WebSphere Member Manager is installed and configured by the portal during the installation and configuration. The WebSphere Member Manager properties are supplied by the `wpsconfig.properties` file.





# B

## Preparing the AIX machine

Before installing WebSphere Portal V5.0 on AIX, you have to prepare the AIX machine with enough disk space. This appendix guides you through this process.

## Increasing the size of an existing file system

The WebSphere Portal installation requires 350 MB of free space on the /tmp file system. You might want to use the following calculation for increasing space on this specific file system and on any other you might need:

1. Find the new size value:

```
new_size=current_size + (required_space - free_space)
```

You can have the following values using the **df** command on AIX.

File system current size = 131072 bytes

File system free space = 126872 bytes

File system required space = 716800 bytes

New size = 721000 bytes

2. Increase the file system size:

```
#chfs -a size='<new_size>' /<file_system_mount_point>
```

For example:

```
#chfs -a size='721000' /tmp
```

## Creating a new file system

We recommend that you create a file system dedicated for the WebSphere Portal and WebSphere Application Server installation.

These instructions already include the required disk space for both products:

1. Type the following command:

```
#smitty fs
```

2. Select **Add/Change/Show/Delete File Systems**.
3. Select **Journalled File Systems**.
4. Select **Add a Journalled File System**.
5. Select **Add a Standard Journalled File System**.
6. Select the desired Volume Group.
7. Select **Megabytes** in the Unit Size field.
8. Enter the value 2200 for the Number of unit.
9. Enter /usr/WebSphere for the Mount Point value.
10. Select yes for the question Mount AUTOMATICALLY at system restart?.

11. Accept the defaults for the remaining fields and press Enter.
12. Press F10 to exit.
13. Mount the file system with the following command:

```
mount /usr/WebSphere
```

## Creating a CDROM file system

You can use the following instructions if you do not have a CDROM file system already created. Complete the following steps:

1. Type the following command:  

```
#smitty fs
```
2. Select **Add/Change/Show/Delete File Systems**.
3. Select **Add/Change/Show/Delete File Systems**.
4. Select **CDROM File Systems**.
5. Select **Add a CDROM File System**.
6. Press F4 to select the available CDROM Device Name.
7. Enter /cdrom in the Mount Point field.
8. Select no for the question Mount AUTOMATICALLY at system restart?.
9. Press Enter.
10. Press F10 to exit.
11. Mount the file system using the following command:  

```
mount /cdrom
```
12. To eject the CD, you need to unmount the file system:  

```
#umount /cdrom
```







## Creating users on AIX

This appendix provides instructions for creating users and groups on AIX.

Three users and groups are required to operate DB2. Table C-1 provides the user and group names used in the following instructions.

*Table C-1 Required users and groups*

Required user	User name	Group name
Instance Owner	db2inst1	db2iadm1
Fenced user	db2fenc1	db2fadm1
Administrator server	db2as	dasadm1

There are some limitations for the DB2 user and group names:

- ▶ User names on UNIX can contain 1 to 8 characters.
- ▶ Group and instance names can contain 1 to 8 characters.
- ▶ Names cannot be any of the following:
  - users
  - admins
  - guests
  - public

- local
- ▶ Names cannot begin with:
  - IBM
  - SQL
  - SYS
- ▶ Names cannot include accented characters.
- ▶ We recommend that you use lowercase for user and group names in UNIX.

## Creating DB2 groups

Create a group for the instance owner, one for the user that will execute UDFs or stored procedures, and one for the DB2 administrator user.

Log in as root and execute the following commands:

```
mkgroup db2iadm1
mkgroup db2fadm1
mkgroup dasadm1
```

## Creating DB2 users

Create a user that will belong to each group you have created previously.

Log in as root and execute the following commands:

```
mkuser pgrp=db2iadm1 groups=db2iadm1 home=/home/db2inst1 core=-1 data=491519
stack=32767 rss=-1 fsize=-1 db2inst1
mkuser pgrp=db2fadm1 groups=db2fadm1 home=/home/db2fenc1 db2fenc1
mkuser pgrp=dasadm1 groups=dasadm1 home=/home/db2as db2as
```

## Setting user passwords

Set an initial password for each user you have created.

Enter the following commands:

```
passwd db2inst1
passwd db2fenc1
passwd db2as
```

# Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

## IBM Redbooks

For information about ordering these publications, see “How to get IBM Redbooks” on page 383. Note that some of the documents referenced here may be available in softcopy only.

- ▶ *WebSphere Portal V5.0 Production Deployment and Operations Guide*, SG24-6391
- ▶ *IBM WebSphere Portal for Multiplatforms V5 Handbook*, SG24-6098
- ▶ *WebSphere Portal on z/OS*, SG24-6992
- ▶ *Patterns: Portal Search Custom Design*, SG24-6881
- ▶ *Develop and Deploy a Secure Portal Solution Using WebSphere Portal V5 and Tivoli Access Manager V5.1*, SG24-6325
- ▶ *Deploying a Secure Portal Solution on Linux Using WebSphere Portal V5.0.2 and Tivoli Access Manager V5.1*, REDP-9121
- ▶ *WebSphere Portal Collaboration Security Handbook*, SG24-6438
- ▶ *WebSphere Portal Server and DB2 Information Integrator: A Synergistic Solution*, SG24-6433
- ▶ *Document Management Using WebSphere Portal V5.0.2 and DB2 Content Manager V8.2*, SG24-6349
- ▶ *Portal Application Design and Development Guidelines*, REDP-3829
- ▶ *IBM WebSphere Portal V5 A Guide for Portlet Application Development*, SG24-6076
- ▶ *IBM WebSphere Application Server V5.1 System Management and Configuration, WebSphere Handbook Series*, SG24-6195
- ▶ *IBM WebSphere V5.1 Performance, Scalability, and High Availability, WebSphere Handbook Series*, SG24-6198
- ▶ *Lotus Domino 6 for Linux*, SG24-6835.

## Other publications

These publications are also relevant as further information sources:

- ▶ *IBM Tivoli Directory Server Installation and Configuration Guide*, SC32-1338
- ▶ *IBM Tivoli Directory Server Administration Guide*, SC32-1339
- ▶ IBM WebSphere Portal security solutions white paper, *Integrating WebSphere Portal software with your security infrastructure*, G325-2090, available at:  
[ftp://ftp.software.ibm.com/software/websphere/pdf/WS\\_Portal\\_Security\\_G325-2090-01.pdf](ftp://ftp.software.ibm.com/software/websphere/pdf/WS_Portal_Security_G325-2090-01.pdf)
- ▶ *Troubleshooting Pickers in Collaborative Portlets*, Technote 1157249
- ▶ *Troubleshooting Automatic Detection of your Mail File with the Different Collaborative Portlets*, Technote 1157029

## Online resources

These Web sites and URLs are also relevant as further information sources:

- ▶ *IBM WebSphere Portal for Multiplatforms Version 5.1 Information Center*  
<http://publib.boulder.ibm.com/pvc/wp/510/ent/en/InfoCenter/index.html>
- ▶ *Lotus Domino Administrator Help*  
<http://www.lotus.com/1dd/notesua.nsf/find/domino>
- ▶ *WebSphere Application Server V5.1 Information Center*  
<http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp>
- ▶ DB2 Universal Database version for SUSE LINUX Enterprise Server 9 (SLES9) validation  
<http://www.ibm.com/db2/linux/validate>
- ▶ DB2 UDB V8 fix packs  
<http://www.ibm.com/software/data/db2/udb/support/downloadv8.html>
- ▶ *DB2 V8 Information Center*  
<http://publib.boulder.ibm.com/infocenter/db2help/index.jsp>
- ▶ Fix packs and alternative fix packs DB2 UDB V8 support site  
<http://www.ibm.com/software/data/db2/udb/support/downloadv8.html>
- ▶ WebSphere Portal product documentation  
<http://www.ibm.com/developerworks/websphere/zones/portal/proddoc.html>

- ▶ WebSphere Portal Catalog  
<http://catalog.lotus.com/wps/portal/portal>
- ▶ WebSphere Portal zone for developers  
<http://www.ibm.com/websphere/developer/zones/portal>
- ▶ IBM WebSphere Portal Enable for Multiplatforms, Version 5.0 brochure  
[ftp://ftp.software.ibm.com/software/genservers/portal/Enable\\_G325-2112-01.pdf](ftp://ftp.software.ibm.com/software/genservers/portal/Enable_G325-2112-01.pdf)
- ▶ IBM Middleware Available on Linux  
<ftp://ftp.software.ibm.com/software/linux/IBMSoftwareOnLinux.pdf>
- ▶ Linux Integration Center Library  
<http://lic.austin.ibm.com/americas/library>

## How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

[ibm.com/redbooks](http://ibm.com/redbooks)

## Help from IBM

IBM Support and downloads

[ibm.com/support](http://ibm.com/support)

IBM Global Services

[ibm.com/services](http://ibm.com/services)



# Index

## A

- Access Manager 32
- accessibility support 30
- ACL 240
- Active Server Pages 217
- addNode 147
- addNode.bat 146
- administration enhancements 2
- administrative console 162
- administrator authority 45
- Administrator DN 302, 315
- AIX 4
- AIX kernel 299
- AIX WebSM system management server 261
- ANT scripts 2
- anti-virus product 179
- APPC support 57
- application server 32
- Application Server Network Deployment 32
- Application Service Provider (ASP) 217
- archive install 2, 4
- authentication 32
- Author access 82, 240
- authorization 32
- automated migration tasks 343

## B

- BPEAuthDataAliasEmb\_node\_server1 173
- Business Process Execution Language (BPEL) 6–7
- business process integration 1–2

## C

- Catalog node 292
- cell 133
- certifier recovery information warning 75
- CheckOS tool 223
- Checkpoint for Portal 49, 71
- clone nodes 345
- Cloudscape 2–3, 33, 53–54, 150, 175, 179, 199, 208, 257, 298
- CloudScapeLib 173

- cluster 134
- cluster environment 54
- cluster member nodes 162
- clustering 32
- cmInit.log 36
- codeset UTF-8 61
- collaboration 30
- Collaboration Center 29
- collaboration tools 6
- Collaborative Services Java archive file 98
- collective 83
- Commerce for e-commerce 33
- CommRes.jar 105
- configtrace.log 110
- configtrace1.log 110
- configuration wizard 2, 61
- ConfigWizard 149, 151
- content access service 23
- content management 30
- contentlib 173
- Crawler 9
- credential slots and segments 354
- Credential Vault data 365
- credential vault service 23
- CSEnvironment.properties 119
- custom portlets 349
- Custom User Registry 32, 71
- Custom User Registry (CUR) 71, 199, 213, 298

## D

- database repository 33
- database transfer performance 3
- DB2 54
- DB2 Administration Client 288
- DB2 Administration Server 280
- DB2 Command Line Processor (CLP) 365
- DB2 ConfigWizard DB transfer 61
- DB2 connection service port 207
- DB2 Content Manager Runtime Edition 62
- DB2 Enterprise Edition 55
- DB2 UDB Enterprise Server Edition V8.1 for AIX 278
- DB2 UDB Server 260

DbDriver 62, 209, 295  
DbDriverDs 62, 209, 295  
DbLibrary 62, 210, 295  
DbLibrary property 151  
DbPassword 62, 210, 295  
DbSafeMode 209, 295  
DbSafeMode property 152  
DbType 62, 209, 295  
DbUrl 62, 210, 295  
DbUser 62, 210, 295  
demilitarized zone (DMZ) 269  
demilitarized zone architecture 31  
deployment enhancements 2  
Deployment Manager 3, 131, 134, 164  
Deployment Manager cell 146, 170  
Deployment Manager SOAP connector-address 146  
DIOP task 85, 244  
directory server 34  
directory services 30, 33  
directory string 83  
dispatcher 131  
Document Management 15  
Document Manager 289  
Document Versioning 15  
Domino Administration Help 244  
Domino Administrator 74, 99, 132, 223  
Domino Directory 72  
Domino Directory Assistance 72  
Domino Enterprise Server 132  
Domino Enterprise Server V6.5.3 251  
Domino LDAP 242  
Domino server 72, 235  
Domino server names 246  
Domino Servlet Manager 96  
Domino Web Access (formerly iNotes) 119  
dynamic caching 162

## E

e-commerce 30  
Edge components 131  
Editor access 82, 240  
equality match 83, 241

## F

fbkDBAuth 173  
federated node 3  
feedback 289

FeedbackDbName 63, 210, 296  
FeedbackDbPassword 63, 210, 296  
FeedbackDbUrl 63, 210, 296  
FeedbackDbUser 63, 210, 296  
feedbackJDBC 212, 298  
FeedbackXDbName 210, 295  
file transfer services 134  
firewall 178, 269  
firewall applications 39  
fully-qualified host name 178

## G

global security 178  
Group names 54  
GroupCreator 82, 240  
GroupModifier 82, 240

## H

Health Monitor Notification 58  
horizontal scaling 156  
host alias list 165  
host integration 33  
Host-on-Demand 33  
HP-UX 4  
HTTP server host name 165  
HTTP servers 34  
HTTP tunneling 103  
HTTP\_HostName attribute 241

## I

IBM AIX 5L V5.2 257  
IBM Cloudscape 29  
IBM DB2 Client V8.2 175  
IBM DB2 UDB Enterprise Client 132, 150  
IBM DB2 UDB Enterprise Server 132  
IBM DB2 UDB Enterprise Server Edition 278  
IBM DB2 Universal Database 66  
IBM DB2 Universal Database Enterprise Server Edition V8.1 258, 284  
IBM DB2 V8.1.1.94 29  
IBM DB2 V8.2 176  
IBM eServer zSeries 327  
IBM HTTP Server 131, 175–176, 179, 257, 273  
IBM HTTP Server V1.3.28 190  
IBM Lotus Extended Search 11  
IBM Lotus Workplace Web Content Manager 61  
IBM Tivoli Directory Server 33, 299, 310



- IBM Tivoli Directory Server Configuration Tool 302
- IBM Tivoli Directory Server V5.2 258
- IBM Tivoli Directory Server V5.2 Client 315
- IBM Tivoli Directory Server V5.2 on AIX 298
- IBM WebSphere Edge Server 34
- IBM WebSphere Portal Server Cluster 132
- Identity Manager 32
- includeapps option 146
- includeapps parameter 146
- Informix 208
- Install Shield Multiplatform (ISMP) 3
- installation and configuration enhancements 2
- installation log files 35
- installmessages.txt 36
- installtraces1.txt 37
- installtraces2.txt 37
- installtraces3.txt 37
- instance names 54
- Instant Messaging and Web Conferencing 102–103
- internationalization 30
- IP address 207

## J

- Java agents 85, 244
- Java database 53
- Java servlet 96
- java.lang.OutOfMemoryError 171
- JavaUserClassesExt 98
- JcrBinaryValueFileDir 210, 295
- jcrdb.log 36
- jcrDBAuth 173
- jcrdbJDBC 212, 298
- JcrDbName 210, 295
- JcrDbNode 210, 295
- JcrDbPassword 210, 295
- JcrDbUnicode value 61
- JcrDbUrl 210, 295
- JcrDbUser 210, 295
- JcrDsName 210, 295
- JcrGeneratedDLLPath 210, 295
- JcrJdbcProvider 173, 210, 295
- JcrLib 173
- JcrXDbName 210, 295
- JdbcProvider 62, 173, 210, 295
- JNDI lookup 23
- JSR 168 portlets 23
- JSR 170 15

## L

- LCC.DominoDirectory.Enabled 118
- LCC.DominoDirectory.port 118
- LCC.DominoDirectory.Server 118
- LCC.DominoDirectory.SSL 118
- LCC.QuickPlace.Enabled 118
- LCC.QuickPlace.Port 118
- LCC.QuickPlace.Protocol 118
- LCC.QuickPlace.Server 118
- LCC.Sametime.Enabled 118
- LCC.Sametime.Port 118
- LCC.Sametime.Protocol 118
- LCC.Sametime.Server 118
- LDAP 2
- LDAP Bind authentication 80
- LDAP directory 71, 258
- LDAP hostname 314
- LDAP name 83, 241
- LDAP realm 255
- LDAP user registry 34
- LDAPAdminPwd 109, 248, 319
- LDAPAdminUld 109, 248, 319
- LDAPBindID 109, 248, 319
- LDAPBindPassword 109, 248, 319
- LDAPGroupFilter 109, 248
- LDAPGroupMember 109, 248, 320
- LDAPGroupObjectClass 109, 248, 320
- LDAPGroupPrefix 109, 248, 320
- LDAPGroupSuffix 109, 248, 320
- LDAPHostName 108, 248, 319
- LDAPPort 108, 248, 319
- ldapsearch command 318
- LDAPServerType 109, 248, 319
- LDAPsslEnable 320
- LDAPSuffix 109, 248, 319
- LDAPUserObjectClass 109, 248, 320
- LDAPUserPrefix 109, 248, 320
- LDAPUserSuffix 109, 248, 320
- LDIF import 318
- Lightweight Directory Access Protocol (LDAP) 71
- LikeMinds 62, 289
- LikemindsDbName 63, 211, 296
- LikemindsDbPassword 63, 211, 296
- LikemindsDbUrl 63, 211, 296
- LikemindsDbUser 63, 211, 296
- likemindsJDBC 212, 298
- LikemindsXDbName 210, 296
- Linux 4, 176
- ImDBAuth 173

- load balance 134
- LocalizeConfigMessages.log 37
- LocalizeConfigTrace.log 37
- LocalizeConfigtrace1.log 37
- LocalizeProgress.log 37
- LocalizeTrace.log 37
- log.txt 36
- Lotus Collaborative Components 72, 117
- Lotus Designer 223
- Lotus Discovery Server 117
- Lotus Domino 29, 33
- Lotus Domino Administrator R5 176
- Lotus Domino Application Server 6.5.3 175
- Lotus Domino Enterprise Server 149
- Lotus Domino V6.5.3 176
- Lotus Instant Messaging and Web Conference Release 6.3.1 30
- Lotus Notes 223
- Lotus QuickPlace 90
- Lotus Sametime 102
- Lotus Team Workplace 90, 98, 117
- Lotus Team Workplace Release 6.5.1 29
- LotusWorkplaceLib 173
- LTPAPassword 108, 248, 319
- LTPATimeout 319

## M

- manual migration 349
- master configuration repository 134
- maximum heap size 171
- Member Manager 62, 208, 289
- MemberRepository 71
- messaging queue service 32
- Microsoft Windows Server 2003 29, 142
- mig\_core.properties 349
- mig\_wmm.properties 350
- mig\_wpcp.properties 350
- migration paths 343
- mobile devices 30
- modular approach 32
- mq\_install.log 36

## N

- network connectivity 179
- Network Deployment 4, 133
- Network Deployment Information Center 147, 154
- node agent 134
- Notes Mail portlets 119

- Notes.ini 244
- Notes.ini file 91

## O

- object identifier 241
- OID 83, 241
- open architecture 32
- operations enhancements 2
- Oracle 208
- ordering match 83, 241

## P

- Parallel portlet 23
- pathUpgradedThemesSkins 350
- Pdmauthor 172
- PeopleOnline31.jar 105
- performance monitoring 134
- Personalization 2, 20, 289
- Portal administrator 45
- Portal administrator group 82
- Portal Cluster Search 13
- Portal Designer 23
- Portal Document Manager 2, 13, 15
- Portal EAR file 169
- Portal Installation Configuration Wizard 3
- Portal Installation Wizard 261
- Portal Scripting Interface 19
- Portal Server V5.1 Archive Install for Linux/UNIX 267
- Portal Server V5.1 Archive Install for Windows, AIX, Solaris 267
- Portal Site Development 23
- Portal Tools 23
- PortalAdminGroupId 108, 247, 319
- PortalAdminGroupIdShort 108, 247, 319
- PortalAdminId 108, 247, 319
- PortalAdminIdShort 108, 247, 319
- PortalAdminPwd 108, 247, 319
- PortalUsers.Idif 318
- portlet application 349
- portlet applications 5–6
- portletinstall.txt 36
- Post Install Configuration Wizard 4
- PrefWpsContextRoot 350
- PrefWpsDefaultHome 350
- Presence Awareness 15
- Presentation.war 172
- PrevPortalAdminId 350

PrevPortalAdminPwd 350  
PrevWpsHostName 349  
PrevWpsInstallLocation 350  
PrevWpsPort 349  
Process Choreographer 15  
production environment 3  
programming model enhancements 2  
properties file 3  
property files 3  
property values 3  
proxy 32  
PznDbNode 210, 295

## Q

QPServlet 98  
queriable attribute types 242

## R

Rational Application Developer V6.0 346  
Redbooks Web site 383  
    Contact us xiv  
register servers 75  
Release Manager 20  
remote HTTP server 269  
Remote Search Service 13  
removeNode script 170  
removeNode.bat 171  
replica LDAP servers 34  
reverse caching 18  
reverse proxy 131  
Reverse Proxy Security Server (RPSS) 34  
RichTextEditor.war 172

## S

Sametime Community 104  
Sametime Java Toolkit 105  
Schema database 82, 241  
Screaming Media portlets 53  
scripting syntax 19  
SDOMediatorsLib 173  
search 30  
Search Administration 19  
Search Administration Portlet Manage Search Col-  
lections 12  
Search Administration Portlet Pending Search Col-  
lection Items 12  
Search Administration Portlet Search and Browse

12  
Search Administration Portlet Seed List 12  
Search Administration Portlet Taxonomy Manager  
12  
Search Center 13  
Search Center Portlet for Search by Users 12  
search enhancements 2  
security 30  
security enhancements 2  
service choreography 6  
servlets.properties 98  
setupCmdLine.sh file 209  
single administrative domain 133  
single sign-on 30, 256  
single sign-on (SSO) 16  
single valued 83  
single-tier environment 29  
site analytics 30  
skin 169  
skins 5  
Solaris 4  
SpreadsheetBlox.war 172  
SQL Server 208  
SSODomainName 108, 248, 319  
SSOEnable 319  
startServer.log 141  
static IP address 178  
STComm.jar 105  
Struts Portlet Framework 23  
substrings match 83, 241  
SUSE LINUX Enterprise Server 8, SP 3 327  
SUSE LINUX Enterprise Server 9 (SLES9) 175  
syntax name 83, 241

## T

taxonomy 30  
Taxonomy Manager 19  
theme 169  
themes 5  
Tivoli 32  
Tivoli Access Manager 34, 103  
Tivoli Directory Server Configuration Tool 302, 347  
Tivoli Directory Server V5.2 299, 348  
Tivoli WebSEAL 33  
-trace parameter 146  
transfer\_db2.properties 211, 296

## U

URI 4  
URL generation service 23  
UserCreator 82, 240  
UserModifier 82, 240

## V

vertical cloning 54  
vertical scaling 156  
Virtual Portal 4–5, 110  
virtual portal 2, 30  
Virtual Portal administrators 6  
virtual portals 1  
virtual resources 354  
Visual Themes and Skins development 23

## W

WAS.PME.install.log 36  
WasPassword 108, 247, 319  
WasUserId 108, 247, 319  
WcmJdbcProvider 173  
WcmLib 173  
Web Administration Tool 301, 310, 312, 314  
Web Content Management 2, 21  
Web server plug-in 276  
Web server plug-ins 192  
Web SSO 245  
Web SSO Configuration 96, 113  
Web SSO configuration 87, 245  
WebSphere Administrative Console 251  
WebSphere Application Server 4, 34  
WebSphere Application Server - Express V5.0.2 301  
WebSphere Application Server Deployment Manager 3  
WebSphere Application Server Enterprise V5.1.1.1 257  
WebSphere Application Server for Network Deployment 135  
WebSphere Application Server Network Deployment 133, 156  
WebSphere Application Server Network Deployment V5.1 131  
WebSphere Application Server V5.1 175, 179  
WebSphere Application Server V5.1 Archive Install for AIX 267  
WebSphere Application Server V5.1.1.1 29  
WebSphere Business Integration Server Founda-

tion 29, 32, 47, 131–132, 137, 140, 145, 257, 260  
WebSphere Business Integration Server Foundation V5.1 for AIX 267  
WebSphere Business Integration Server Foundation V5.1.1 327  
WebSphere Business Integrator 7  
WebSphere LTPA keys 255  
WebSphere Member Manager 71  
WebSphere MQ 29, 33, 47  
WebSphere Personalization 260  
WebSphere Portal 45, 53, 175, 289, 349  
WebSphere Portal and WebSphere Business Integrator 7  
WebSphere Portal Archive Install 47  
WebSphere Portal content publishing 62  
WebSphere Portal content publishing runtime 257  
WebSphere Portal EAR file 169  
WebSphere Portal for Multiplatforms V5.1 29  
WebSphere Portal Search Portlets 11  
WebSphere Portal Taxonomy Manager portlet 12  
WebSphere Portal V5.0 2, 4  
WebSphere Portal V5.1 2, 29, 175, 179, 199, 257, 343  
WebSphere Portal V5.1 Information Center 319  
WebSphere Portal V5.1 InstallShield 35  
WebSphere Portal Web Content Manager 47  
WebSphere Process Choreographer 7  
Windows 4  
Windows 2000 175  
Windows 2000 Professional 176  
Windows Server 2003 223  
wmm user 81  
wmmApp 172  
WmmAppName 211, 296  
wmmDBAuth 173  
WmmDbName 63, 211, 296  
WmmDbPassword 63, 211, 296  
WmmDbUrl 63, 211, 296  
WmmDbUser 63, 211, 296  
WmmDsName 211, 296  
WmmSystemId 109, 248  
WmmSystemIdPassword 109, 248  
working image 2  
Workplace Server 73  
wp.wire.jar 150  
wpcconfig.properties 61, 67, 108, 152, 208, 318  
WpcpDbName 63  
WpcpDbPassword 63  
WpcpDbUrl 63

WpcpDbUser 63  
wpsinstalllog.txt 36  
wppmefp1.txt 36  
wps 172  
wps.ear 169  
wps\_orig.ear 169  
WPSconfig script 3, 208  
WPSConfig.bat 61  
WpsContentAdministrators 108, 248  
WpsContentAdministratorsShort 108, 248  
wpsDBAuth 173  
wpsdbJDBC 212, 298  
WpsDbName 209, 295  
wpsDbName 62  
WpsDbNode 210, 295  
WpsDocReviewer 108, 248  
WpsDocReviewerShort 108, 248  
WpsDsName 210, 295  
WpsHostName 319  
WpsHostName value 152  
wpsinstalllog.txt 36  
WPSlib 173  
WpsXDbName 210, 295  
wpwasfp1.txt 36  
wsadmin tool 19

## **X**

XMLAccess 19





# IBM WebSphere Portal for Multiplatforms V5.1 Handbook

(0.5" spine)  
0.475" <-> 0.875"  
250 <-> 459 pages









**Redbooks**

# IBM WebSphere Portal for Multiplatforms V5.1 Handbook

## **New features and enhancements**

## **WebSphere Portal V5.1 implementation demonstrated on multiple platforms**

## **Clustering and migration demonstrations included**

This IBM Redbook positions the new features and enhancements of IBM WebSphere Portal for Multiplatforms Version 5.1 and serves as a follow-up to the *IBM Redbook, IBM WebSphere Portal for Multiplatforms V5 Handbook*, SG24-6098.

This *IBM WebSphere Portal for Multiplatforms V5.1 Handbook* will help you to understand how to install, tailor, and configure WebSphere Portal V5.1 within the Microsoft Windows Server 2003, SUSE LINUX Enterprise Server 9 (SLES9), IBM AIX 5L, and Linux on zSeries/SUSE LINUX Enterprise Server 8 (SLES8) environments. We provide instructions to set up a clustered environment and also provide a demonstration of migrating from WebSphere Portal Version 5.0 to Version 5.1.

Although this book includes the steps for configuring WebSphere Portal V5.1 on the latest operating systems, we recommend that you refer to the *IBM Redbook IBM WebSphere Portal for Multiplatforms V5 Handbook* when you seek administrative and customization examples.

Other examples provided in this book include the implementation of IBM Lotus Domino Enterprise Server, Lotus Team Workplace, Lotus Collaborative Components, and IBM Tivoli Directory Server.

## **INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION**

## **BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE**

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

**For more information:**  
[ibm.com/redbooks](http://ibm.com/redbooks)