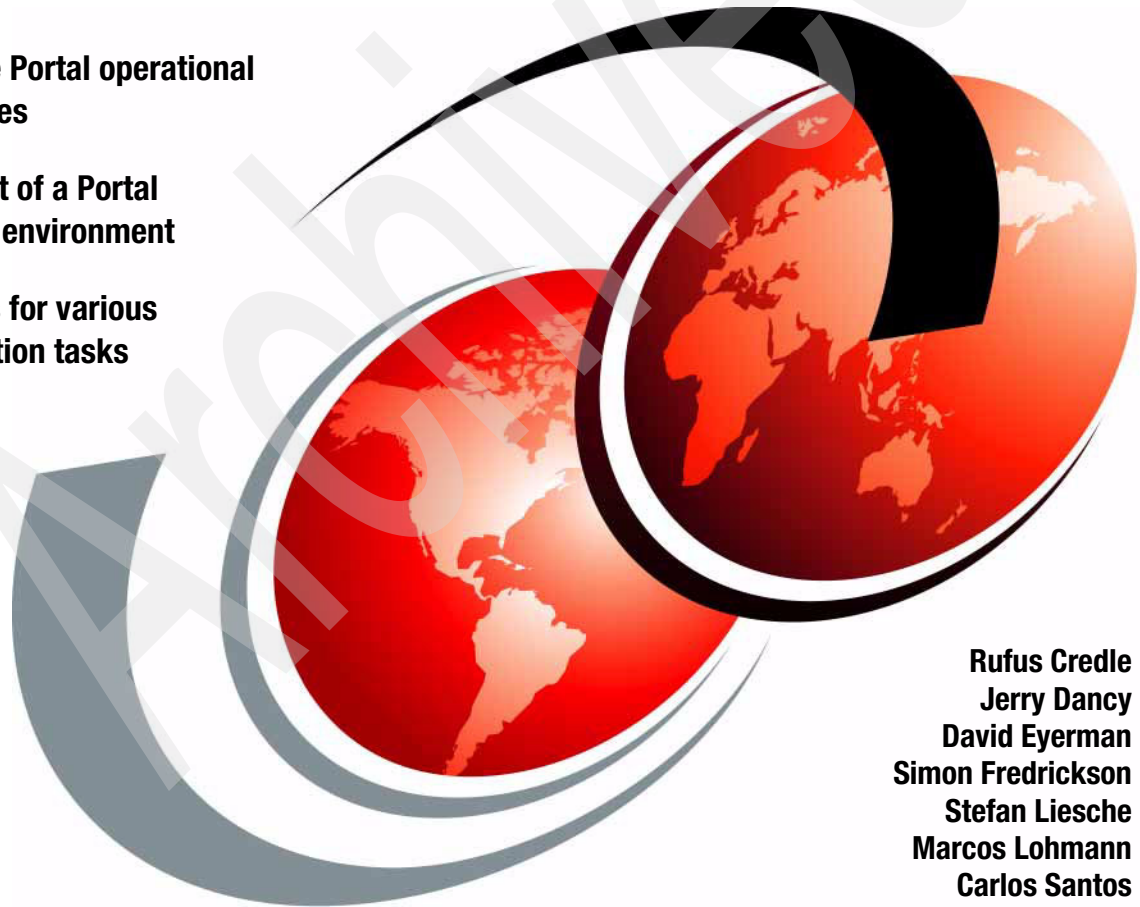


WebSphere Portal V5.0 Production Deployment and Operations Guide

WebSphere Portal operational
architectures

Deployment of a Portal
production environment

Procedures for various
administration tasks



Rufus Credle
Jerry Dancy
David Eyerman
Simon Fredrickson
Stefan Liesche
Marcos Lohmann
Carlos Santos



International Technical Support Organization

WebSphere Portal V5.0 Production Deployment and Operations Guide

January 2005

Archived

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

First Edition (January 2005)

This edition applies to IBM WebSphere Portal Extended for Multiplatforms Version 5.0.2.1.

© 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	xiii
Comments welcome	xiv
 Chapter 1. WebSphere Portal operational architecture	1
1.1 Term definitions	2
1.2 Deployment units	2
1.2.1 Dispatcher	3
1.2.2 Reverse caching proxy	3
1.2.3 HTTP server	4
1.2.4 WebSphere Portal	4
1.2.5 Forward caching proxy	4
1.2.6 Database server	4
1.2.7 Directory server	5
1.3 Building blocks of the Portal	5
1.3.1 A basic Portal installation	5
1.3.2 Configuring the Portal to fit into an established environment	6
1.4 Exploiting network capabilities	7
1.5 A collaborative Portal	9
1.6 Enhanced security Portal	10
1.6.1 Tivoli Access Manager	10
1.6.2 Netegrity SiteMinder	12
1.7 Portal clustering	13
1.7.1 The horizontal Portal cluster	14
1.7.2 The vertical Portal cluster	14
1.8 Decoupling from back-end systems	15
1.9 Example architectures in operation	16
1.9.1 The elaborated Portal cluster	16
1.9.2 The elaborated security Portal cluster	17
1.9.3 The Availability Gold Standard	18
 Chapter 2. Installing WebSphere Portal	21
2.1 Getting ready for the installation	22
2.1.1 Overview of production Portal architectures	23
2.2 Suggested roadmap	24

2.2.1 Planning phase	24
2.2.2 Installation phase	30
2.3 Portal documentation	63
Chapter 3. Security management	65
3.1 Password maintenance	66
3.1.1 Proxy authentication with Content Access Service	66
3.1.2 Changing the Portal database username and password	67
3.2 Credential Vault	69
3.2.1 How Credential Vault works	69
3.2.2 Using Credential Vault	70
3.3 Surfacing an application	71
3.4 Managing security	72
3.5 Integrating LDAP	73
3.5.1 Performance considerations	74
3.5.2 LDAP architecture and schema layout considerations	81
3.5.3 Using an LDAP server cluster	82
3.5.4 Using a single LDAP image	83
3.5.5 LDAP, WebSphere Portal, and the Q/A environment	83
3.5.6 LDAP administration	83
Chapter 4. Solution deployment	87
4.1 Understanding J2EE	88
4.2 Understanding a J2EE Portal	89
4.2.1 Portal structure	89
4.2.2 Elements of a Portal page	92
4.3 Portal configuration	93
4.3.1 Customizing the Portal	93
4.3.2 Installing the portlet	95
4.3.3 Updating the portlet	104
4.3.4 Portlet service	106
4.3.5 Installing theme and skin	107
Chapter 5. Moving from staging to production	111
5.1 The Portal staging process	112
5.2 Deployment and build process	112
5.2.1 Determining what to move	113
5.2.2 Using the XMLAccess tool for moving	114
5.2.3 Object IDs	117
5.2.4 The Custom Unique Names portlet	117
5.3 Transferring Portal artifacts using XMLAccess	118
5.3.1 Transfer process	118
5.3.2 Exporting a sample page using XMLAccess	119
5.3.3 Exporting and importing a new page	120

5.4 A step-by-step guide	121
5.4.1 Preparing the environment	121
5.5 Preparing the worksheet	124
5.5.1 Example worksheet.	124
5.6 Run activities	126
5.6.1 Verifying the prerequisites.	126
5.6.2 Using XMLAccess to export Portal artifacts	127
5.6.3 Bundling the supporting files.	129
5.6.4 Transferring the bundle	130
5.6.5 Distributing the supporting files to a single server.	131
5.6.6 Distributing the supporting files to a cluster	132
5.6.7 Updating the target configuration	135
5.7 Post transfer actions	137
5.7.1 Ensuring that the nodes are synchronized	137
5.7.2 Restarting the server.	137
5.7.3 Activating the portlets	137
5.7.4 Making any manual changes	138
5.8 How does customization and the transfer process work?	139
5.8.1 World clock scenario	139
5.9 Troubleshooting and best practices	142
5.9.1 Plan on a trial run	142
5.9.2 Problems importing pages	142
5.9.3 Activate portlets.	142
5.9.4 Synchronize the cluster.	142
5.9.5 Synchronize the nodes without security	143
Chapter 6. Production procedures and administration activities	145
6.1 Changing the host or domain name	146
6.1.1 Assumptions	147
6.1.2 Step-by-step procedures.	147
6.2 Changing database servers	149
6.2.1 Assumptions	150
6.2.2 Moving from a DB2 database to a DB2 database.	151
6.2.3 Moving from an Oracle database to an Oracle database	152
6.2.4 Moving from an SQLServer database to an SQLServer database	156
6.3 Changing LDAP servers	161
6.3.1 Assumptions	162
6.3.2 Step-by-step procedure.	163
6.4 Backup and recovery.	167
6.4.1 Overview of our approach to backup and recovery.	167
6.4.2 Our approach to backup	169
6.4.3 Our approach to recovery	170
6.4.4 Backup and recovery for Windows systems	171

6.5 Maintaining a healthy Portal environment	174
6.5.1 Scheduling regular backups	174
6.5.2 Reviewing log files	175
6.5.3 Applying fixes	176
6.5.4 Getting support	177
6.5.5 Using basic troubleshooting techniques	178
6.5.6 Using roadmaps	178
6.6 On Demand clustering solutions	178
6.6.1 Step-by-step of the On Demand procedure	181
6.7 Temporarily removing a clustered node to apply maintenance	188
6.7.1 Step-by-step procedure to temporarily remove a clustered node	188
6.8 Monitoring the Portal	193
Chapter 7. A high availability illustration	195
7.1 The sample cluster production environment	196
7.2 Before you begin the procedure	197
7.3 Assumptions	197
7.4 Initial production state	199
7.5 Remove Site B from cluster	200
7.6 Maintenance on Site B	204
7.7 Switch IP traffic from Site A to Site B	206
7.8 Maintenance on Site A	208
7.9 Switch IP traffic from Site B to Site A	211
7.10 Return to Initial Production state	214
Chapter 8. Performance tuning the environment	215
8.1 Understanding the environment	216
8.2 Application server tuning	216
8.2.1 Additional notes for an AIX environment	220
8.2.2 Application server cloning	220
8.3 Database server tuning	220
8.3.1 IBM DB2 Enterprise Edition Database parameter tuning	221
8.3.2 Oracle Enterprise Edition Database parameter tuning	222
8.3.3 Other database considerations	222
8.4 Directory server tuning	223
8.4.1 Web server tuning tips	224
8.4.2 Security filters	225
8.4.3 Dereferencing aliases	225
8.5 Operating system specific tuning parameters	226
8.6 Network tuning	227
8.6.1 Solaris networking	227
8.6.2 AIX networking	227
8.6.3 Windows networking	228

8.7 WebSphere Portal service properties	228
Appendix A. Operation tools	231
XMLAccess tool	231
Script to synchronize nodes	232
Script to delete portlets	234
Reference documentation	234
Appendix B. Portal installation worksheets and samples	235
Worksheets	236
Silent install sample	245
Verifying Portal installation log files	246
Appendix C. Changing the mode in WebSphere Portal	259
Setting read-only mode	260
Setting read or write mode	261
Appendix D. Switching database servers	265
Changing from a DB2 database to another DB2 database	266
Changing from an Oracle database to another Oracle database	267
Changing from an SQLServer database to another SQLServer database ..	269
Appendix E. Capacity planning	273
WebSphere Portal V5 or later database	273
Appendix F. A portal manager for WebSphere Portal	275
Wily Portal Manager for IBM WebSphere Portal	275
Appendix G. Additional material	277
Locating the Web material	277
Using the Web material	278
How to use the Web material	278
Abbreviations and acronyms	279
Related publications	281
IBM Redbooks	281
Online resources	281
How to get IBM Redbooks	285
Help from IBM	285
Index	287

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:

@server®

@server®

Redbooks (logo) ™

ibm.com®

xSeries®

AIX®

Cloudscape™

Domino®

DB2 Universal Database™

DB2®

IBM®

Lotus®

Redbooks™

Sametime®

Tivoli®

WebSphere®

Workplace™

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 contains best practices for deployment and operational support of WebSphere® Portal V5 in a production environment. It addresses the questions on how to initially deploy WebSphere Portal. After you have deployed WebSphere Portal, you can use the operational best practices described in this redbook for themes, skins, pages, and portlet updates in a 24/7 enterprise.

This redbook discusses the common notations for WebSphere Portal operational architecture and terminology. The architectures described in this redbook are examples used to present WebSphere Portal operation alternatives that allow you to combine, mix, and define your own Portal architecture.

Portal administrators can find in this redbook an installation roadmap that includes a suggested approach, best practices, links to required resources, and hints to perform a successful installation and configuration. When the staging environment has been set, this redbook also provides helpful instructions on moving Portal into production.

This redbook has been developed for the following audience: WebSphere Portal Implementors and Administrators, Software Engineers, Consulting IT Architects, IBM Business Partners, Domino® Administrators, and IBM WebSphere Portal Software Support teams.

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 (ITSO), Raleigh Center.



Rufus Credle is a Certified Consulting IT Specialist at the ITSO, Raleigh Center. In his role as project leader, he conducts residencies and develops Redbooks™ about network operating systems, ERP solutions, voice technology, high availability and clustering solutions, Web application servers, pervasive computing, and IBM and OEM e-business applications, all running IBM @server® xSeries® and IBM @server BladeCenter systems. Rufus' 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 BS degree in business management from Saint Augustine's College. Rufus has been employed at IBM for 24 years.



Jerry Dancy works as a Technical Lead for the WebSphere Portal Support Level 2 team. He has two years of experience in WebSphere Portal Support and previously worked as an Oracle DBA for four years. He holds a degree in Accounting and CIS from Appalachian State University. His areas of expertise include install, upgrade, configuration, and clustering of WebSphere Portal. He has written extensively on WebSphere Portal installation and configuration.



David Eyerman is a Senior Software Engineer in the IBM Silicon Valley Laboratory working in the WebSphere Portal Development team as one of the deployment and operations architects. His responsibilities are twofold. First, he assists customers and Business Partners with implementing Portal solutions using the currently available releases of WebSphere Portal. Secondly, he designs and develops components which would enhance the deployment, operation, and maintenance characteristics of Portal solutions. David has worked with the Portal team in IBM for over three years and is one of the original members of the group.



Simon Fredrickson is an IT Specialist with IBM Software Group Services in Melbourne, Australia. He has over seven years experience with IBM designing and deploying mission-critical applications using a wide range of Lotus®, WebSphere, and internet-based technologies. He started at IBM with Lotus, where he gained considerable experience in deploying Lotus technologies. He is a Lotus CLP. In recent years, he has been working closely with clients to help them deploy WebSphere Portal server and Foundation products, with a strong emphasis on Portal Clustering and the migrations and transfer of Portal environments.



Stefan Liesche is a Certified Consulting IT Architect in the IBM Development Laboratory in Boeblingen, Germany. He has 10 years of experience in the software development field. He holds a MS in computer science from the University of Hildesheim, Germany. He joined IBM in 1998 as part of the services group, where his speciality was designing large scale end-to-end e-business solutions for complex environments. Stefan has been working with WebSphere Portal for three years. He first worked on the construction of large scale portal solutions before joining the WebSphere Portal development architecture team as a deployment and operation architect. Currently, he is the Lead Architect of the WebSphere Portal Foundation layer where he focuses on the architecture of the core WebSphere Portal engine.



Marcos Lohmann is a System Analyst for an IBM Business Partner in Brazil - Silicnet BR Ltda. Marcos had previously worked as a Web Developer. He has over six years experience working with Web-based solutions and has worked with the WebSphere platform since March 2003. His areas of expertise include J2EE, .NET, Web Services, and Publishing Infra Structure for Multiplatforms. He has written extensively on solution deployment and security.



Carlos Santos is an IT Specialist with ITS Software Support in IBM Brazil. He has four years of experience in Java™ and Web applications. His areas of expertise include support for Java, WebSphere Application Server, and WebSphere Portal Server Multiplatforms. He is IBM Certified for WebSphere Application Server Advanced V4.0 Administration.

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

Tamikia Barrows, Jeanne Tucker, Diane O'Shea
ITSO, Raleigh Center

IBM WebSphere Portal Performance Team: Art Francis, Donald Wood, Laura Yen, Lorrie Tornek, Mark Alkins, Martin Presler-Marshall, Ruthie Lyle, Scott Snyder, Sharda Nandula, Susan Hanis, Terence Walker
IBM Research Triangle Park

Alex Lang, Joachim Loeffel, Keith Blake, Don Jones, Marshall Lamb
IBM Raleigh

Glenn Druce
IBM Australia

Patricia Witten
EnCode, Inc New Jersey

Stefan Hepper
IBM Germany

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 operational architecture

This chapter provides basic information for the WebSphere Portal operational architecture and terminology. It describes example architectures that you can use to present WebSphere Portal operation alternatives. You can combine, mix, and define your own Portal architecture based on these examples. After you review this chapter, you should have enough information to develop your own Portal architecture.

1.1 Term definitions

Some common terms and the graphical representation that this book uses are:

deployment unit A grouping of software components for placement onto nodes.



node A hardware platform at some point of abstraction, onto which you can place deployment units (components).



connection Connectivity between two or more nodes.



1.2 Deployment units

The cross-functional teams (the network team, data base administrators, back-end application administrators, collaboration specialist, and so on) that support the different technology in this figure must all work together for a successful implementation of the Portal.

The supported products of a full-scale WebSphere Portal environment that require the input of IT specialists or software engineers are:

- ▶ Dispatcher
- ▶ HTTP Server
- ▶ WebSphere Portal
 - Portal search
 - WebSphere Portal content publishing
- ▶ Directory server
- ▶ Database server
- ▶ Reverse caching proxy
- ▶ Forward caching proxy
- ▶ Reverse security proxy
- ▶ Security server
- ▶ Deployment Manager
- ▶ Tivoli® Intelligent Orchestrator

- ▶ Back-end systems
 - Domino
 - Host systems
 - Web applications
 - Sametime®
 - Web Services for remote portlet providers
 - Web Content Management Systems

For information about the current mapping of deployment units for supported product versions, go to the following Web address:

<http://www-106.ibm.com/developerworks/websphere/zones/portal/proddoc.html>

The following sections provide descriptions of the deployment units.

1.2.1 Dispatcher

A dispatcher is used to decouple groups of conceptual nodes within the infrastructure. Decoupling of conceptual node groups allows horizontal scaling of conceptual node groups that are independent of other conceptual node groups. At the same time, a dispatcher can compensate the failure of nodes within the load-balanced conceptual node group. To increase availability of the dispatcher, a standby system accompanies each dispatcher.

1.2.2 Reverse caching proxy

You use a reverse proxy within the Portal infrastructure to optimize the response times to user requests. A group of load-balanced reverse proxies handle requests that come from the network into the Portal infrastructure. Responses to requests for static resources are cached. (Here, *static resource* refers to data that stay unchanged for all users, regardless of the time slot. For example, if the content is static only for subseconds, but many users access it within this time slot, the resource is static.) The reverse proxy server distributes the cached responses later out of the cache directly by without using any other part of the Portal infrastructure. Thus, the proxy servers help decrease the load on the central Portal cluster infrastructure and reduce the cost for the more expensive Portal Server Cluster.

In WebSphere Portal V5.0 and later, reverse proxies can handle the following resources:

- ▶ Images
- ▶ JavaScript files
- ▶ Cascading style sheets (CSS)
- ▶ Static HTML pages (for example, help pages)
- ▶ Servlet responses (for example, maximizer servlet of B2E Portal)
- ▶ Anonymous pages

The Web server conceptual node sets HTTP caching directives in HTTP responses that are sent to the reverse proxies.

A request to a full Portal page is always followed by a sequence of requests (typically, an average of 20 to 30 requests) to static resources for the static components (mainly images) imbedded into the page.

1.2.3 HTTP server

You use the Web server to separate user access to the Portal infrastructure and the Portal servers conceptual nodes. In the case of WebSphere Portal downtimes (for example, during maintenance hours), you can continue to use Web servers to serve static page content to users and to enforce different authorization levels (for example, users and operating personnel).

1.2.4 WebSphere Portal

You use WebSphere Portal to create dynamic responses to user requests. The responses are personalized and usually present a combination of multiple input data. Therefore, the dynamic of the pages can be very high. WebSphere Portal is running inside an application server that allows multiple connections to other IT systems. The Portal server is the conceptual node on which authentication and authorization policies are applied and is the central conceptual node of the Portal infrastructure.

1.2.5 Forward caching proxy

You use a forward proxy within the Portal infrastructure to decouple the Portal conceptual node group from external systems delivering HTTP content. The forward proxy caches the content that the external systems deliver. Follow on requests to the same resource that come from the Portal server can then be handled more efficiently. These forward proxies are dedicated to the Portal and can be highly optimized for this task. The proxy servers do not handle data types other than HTTP responses. If you need to decouple systems that deliver data types other than HTTP content, you need to use other components.

1.2.6 Database server

The database is the data store component inside the Portal infrastructure. This database persists only with data directly being used for configurations within the Portal infrastructure. Content is contained within the server accessed through the data network. Because there is currently only a single database conceptual node inside the Portal infrastructure, all kinds of data are persisted to this data store.

The availability of the entire Portal infrastructure relies on the availability of the configuration data inside the database server conceptual node.

The set of persisted data can contain the following kinds of data:

- ▶ Configuration
- ▶ Customization and personalization
- ▶ User
- ▶ Application
- ▶ Authorization
- ▶ Session

1.2.7 Directory server

The directory server stores information (at a minimum, user ID, and password) about users working with or administering the Portal. Group information for the users can enrich the information. The user directory currently is not part of the Portal infrastructure and is seen as an external system.

1.3 Building blocks of the Portal

This section discusses the operational building blocks you use to achieve a successful installation of WebSphere Portal.

1.3.1 A basic Portal installation

A basic installation of WebSphere Portal is the easiest installation. It is a sufficient installation for you to begin exploring WebSphere Portal.

The common uses for a basic installation are:

- ▶ Quick testing of a Portal solution
- ▶ Demonstrating WebSphere Portal
- ▶ Showing a proof of concept
- ▶ Backing up and restoring easily

Figure 1-1 illustrates a single-system install of WebSphere Portal. In this scenario, you have several deployment units running on one node.

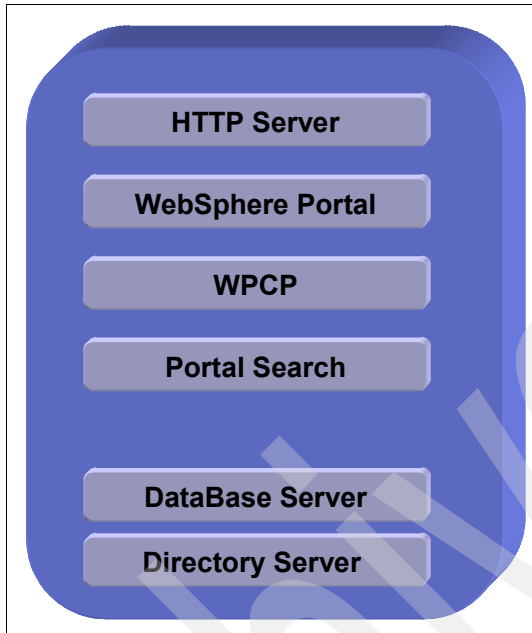


Figure 1-1 Basic Portal installation

Note: The figures that follow build upon the basic Portal installation depicted in Figure 1-1. Yellow boxes indicate an addition or changes to the basic installation.

1.3.2 Configuring the Portal to fit into an established environment

The standard installation for WebSphere Portal runs without a cluster. The common uses for a standard installation are:

- ▶ Adding security and separation of three tiers
- ▶ Using a real database and directory server
- ▶ Using a standard one machine production system by design
- ▶ Using for department or medium size businesses

Figure 1-2 on page 7 illustrates a three-tier architecture that run scripts to link with the HTTP server, database server, and directory server. Most companies have these technologies in place. Figure 1-2 on page 7 demonstrates how you can configure the Portal to fit into an established environment.

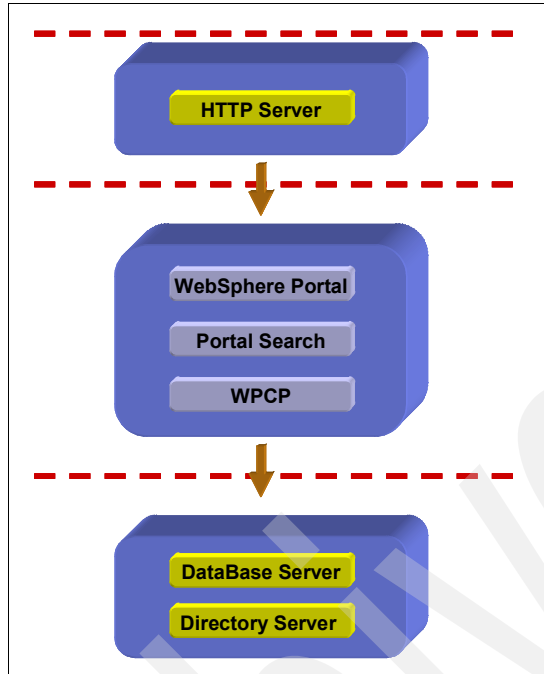


Figure 1-2 Standard Portal installation

This is still a simple configuration. However, it allows flexibility on placing nodes to exploit firewall security.

1.4 Exploiting network capabilities

Adding caching capabilities allows you to serve the following content from cache instead of from the WebSphere Portal:

- ▶ HTML pages
- ▶ Images
- ▶ Stylesheets
- ▶ JavaScript libraries
- ▶ Anonymous pages

You can locate the reverse caching proxy at any point between the Portal and the user. Your decision is influenced by:

- ▶ The bandwidth of the network to which a user request needs to pass in order to access the Portal.
- ▶ The percentage of user requests that pass a given segment.

All user requests pass the network which connects the Portal to the network. Locating the reverse caching proxy in this segment yields the highest user request hit rate. On the other hand, if your users are connected over low bandwidth, high latency affected networks (such as satellite links), you would achieve the highest benefit for user response time by locating the reverse caching proxy closer to the user. It is possible to combine multiple reverse caching proxies.

Figure 1-3 illustrates how you can locate the caching proxy that WebSphere Portal uses to improve content delivery times and portal system utilization.

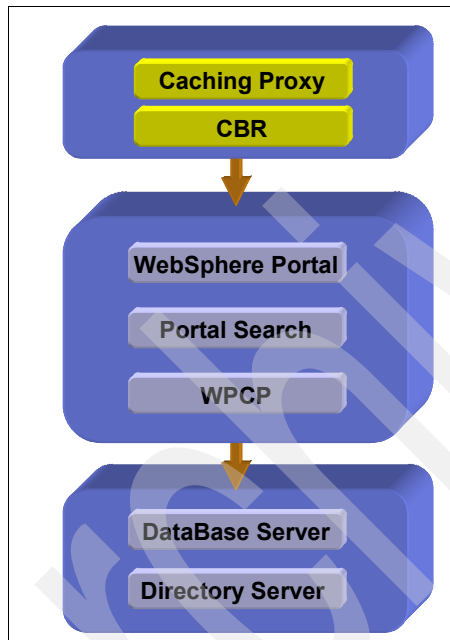


Figure 1-3 Adding the caching proxy deployment unit

This architecture comes available with WebSphere Edge Server and does not require additional hardware. For more information about caching proxy, visit the InfoCenter Web site:

<http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/index.html>

1.5 A collaborative Portal

This section discusses the components that allow you to go from a Portal Enable environment to a Portal Extend environment, the typical environment used in an internal Portal.

Figure 1-4 shows the products and components that are important for setting up a collaborative Portal.

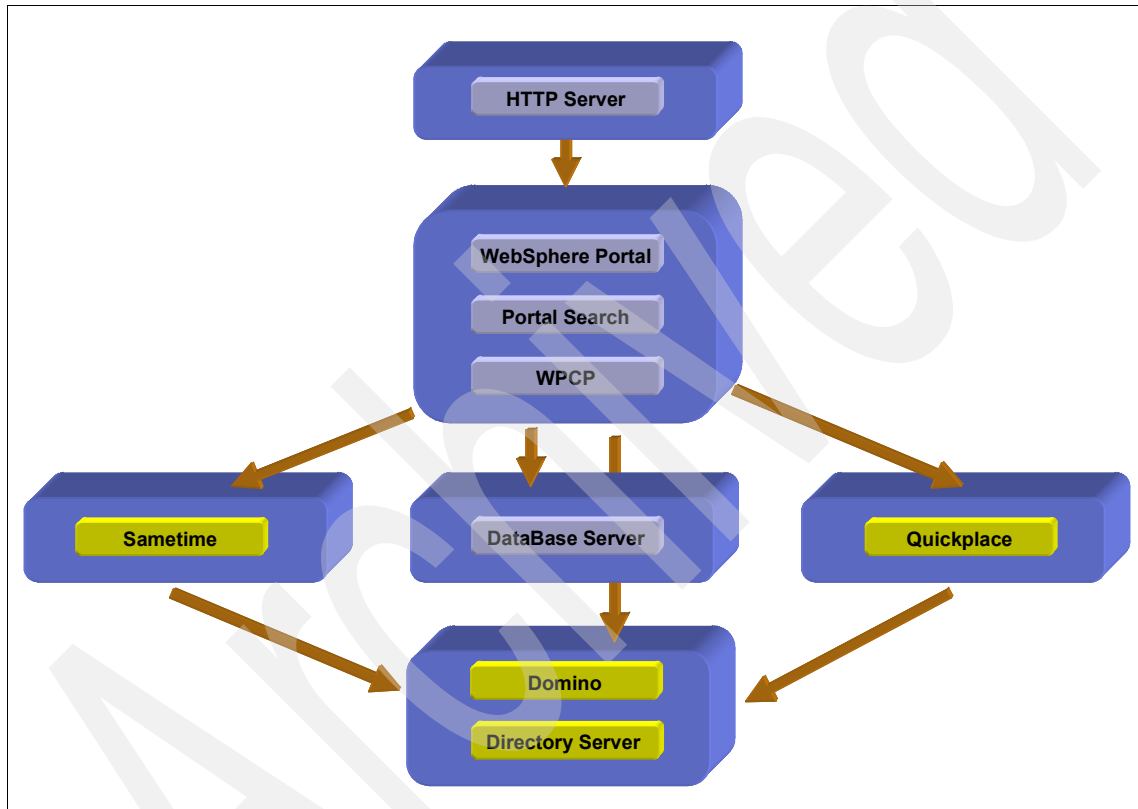


Figure 1-4 WebSphere Portal with a collaborative infrastructure

The existing nodes in this example are Sametime, Domino, and Quickplace. These extensions are used to incorporate the Portal into an existing collaboration environment.

1.6 Enhanced security Portal

This section discusses how to enhance the security structure for WebSphere Portal with Tivoli Access Manager or Netegrity SiteMinder in a non-clustered environment.

1.6.1 Tivoli Access Manager

In a WebSphere Portal environment, you need a secure Portal solution to address common security challenges such as:

authentication	Determining who is accessing the site.
authorization	Permitting or denying access to resources based on the policies and users or groups who access the resources.
single sign on	Logging on once for access to applications to which access has been granted.

IBM Tivoli Access Manager for e-business is an award winning, policy-based access control solution for e-business and enterprise applications. It provides a self-protecting environment by:

- ▶ Delivering a unified authentication and authorization for e-business initiatives as you secure a single enterprise or a federated environment
- ▶ Preventing unauthorized access by using a single security policy server to enforce security across multiple file types, application providers, devices, and protocols
- ▶ Maintaining password and user integrity using single sign on
- ▶ Discovering problems or potential problems using robust auditing and information-gathering tools

In Figure 1-5, WebSphere Portal and Tivoli Access Manager split security responsibilities by externalized security management (authentication, authorization, and credential store).

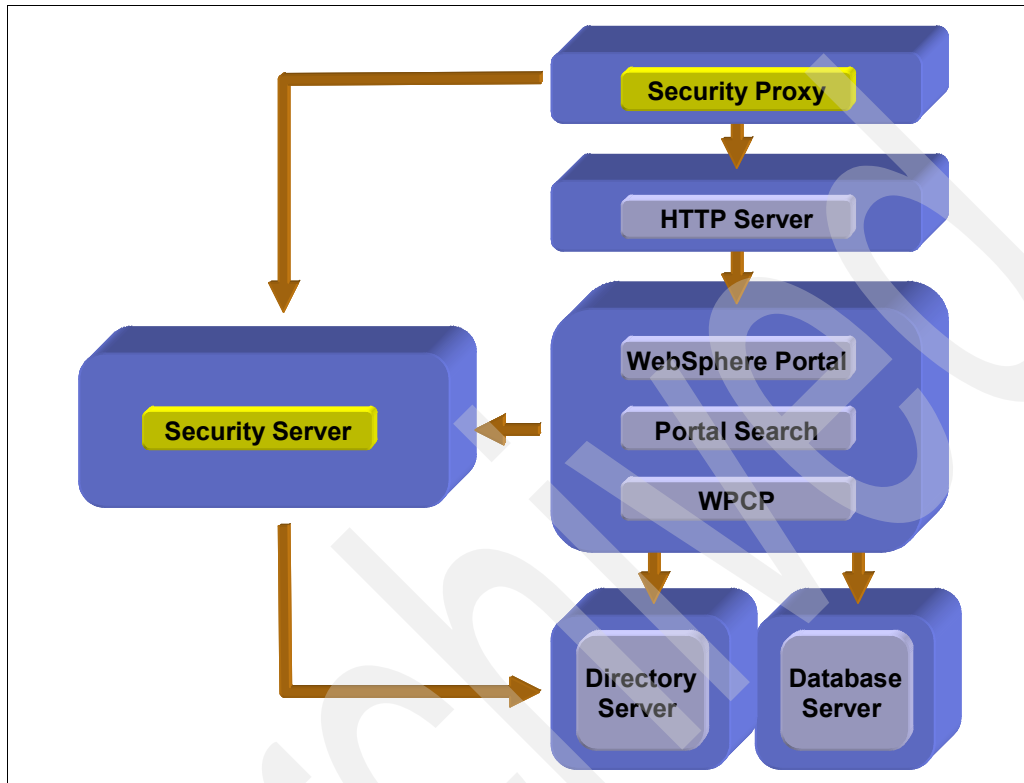


Figure 1-5 Tivoli Access Management security

For more information about implementing Tivoli Access Manager with WebSphere Portal, see *Develop and Deploy a Secure Portal Solution Using WebSphere Portal V5 and Tivoli Access Manager V5.1*, SG24-6325, available at the following Web address:

<http://www.redbooks.ibm.com/redbooks/pdfs/sg246325.pdf>

1.6.2 Netegrity SiteMinder

You can also use WebSphere Portal with Netegrity SiteMinder as an external security manager. SiteMinder enables you to administer and consistently enforce user access to Web applications by providing Single Sign On (SSO) to users.

Similar to Tivoli Access Manager, SiteMinder provides the following:

- ▶ Centralized, policy-based control of user authentication and authorization management
- ▶ SSO to an enterprises' Web applications
- ▶ Enterprise-class manageability
- ▶ Secure, standards-based federation security services
- ▶ Enterprise-class scalability and high availability
- ▶ Extensive support for heterogeneous IT environments
- ▶ Comprehensive audit and reporting services
- ▶ Comprehensive password management services
- ▶ Role-based access control

In Figure 1-6, WebSphere Portal and SiteMinder split security responsibilities by externalized security management (authentication and authorization).

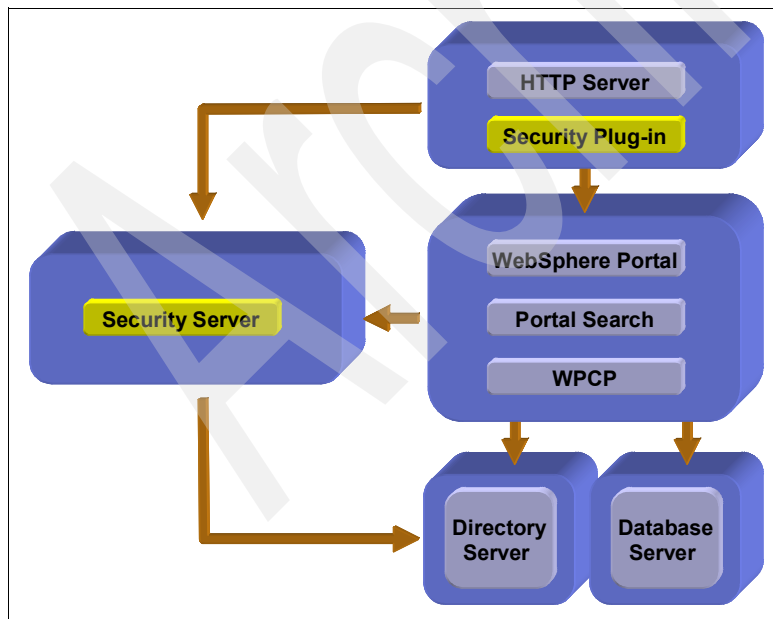


Figure 1-6 Netegrity SiteMinder security

1.7 Portal clustering

WebSphere Portal is integrated with and uses the WebSphere Application Server middleware. The middleware allows you to use multiple strategies for scaling and can be scaled vertically and horizontally. With both scaling concepts, the number of servers running the application is increased.

Vertical scaling refers to the concept of cloning an application onto a single node. You can use vertical scaling to fully use a node within the conceptual node group in the case where resource congestions or locking conditions prevent a single application instance to scale up to the nodes limit.

Horizontal scaling refers to the concept of increasing the number of nodes on which the application servers are running. You can use horizontal scaling in cases where all nodes within the cluster are fully used.

You can use vertical clustering to achieve better tolerance against malfunctioned applications that make the server process fail. In this case, other processes running on the same node are still able to serve other requests. However, the possibility of the same error causing other server processes to fail is high. Vertical cloning cannot accommodate for hardware failure.

You can use horizontal clustering to accommodate for software or hardware failures. If any conceptual node within the conceptual node group fails, other conceptual nodes within the conceptual node group can handle their workload.

With both vertical and horizontal clustering, take care to avoid data loss due to conceptual node failures. If data needs to be available even after conceptual node failures, this data needs to be persisted into a database or shared between multiple nodes in memory. This caution is in particular important for session data. Session data take over between conceptual nodes can only happen if the cluster is configured accordingly.

1.7.1 The horizontal Portal cluster

A horizontal Portal cluster provides fault-tolerance of Portal nodes as well as additional capacity. In this environment, scalability requires another machine to run the Deployment Manager.

Figure 1-7 illustrates the WebSphere Application Server clustering capabilities. You can have an arbitrary number of nodes. Figure 1-7 shows three WebSphere Portal nodes.

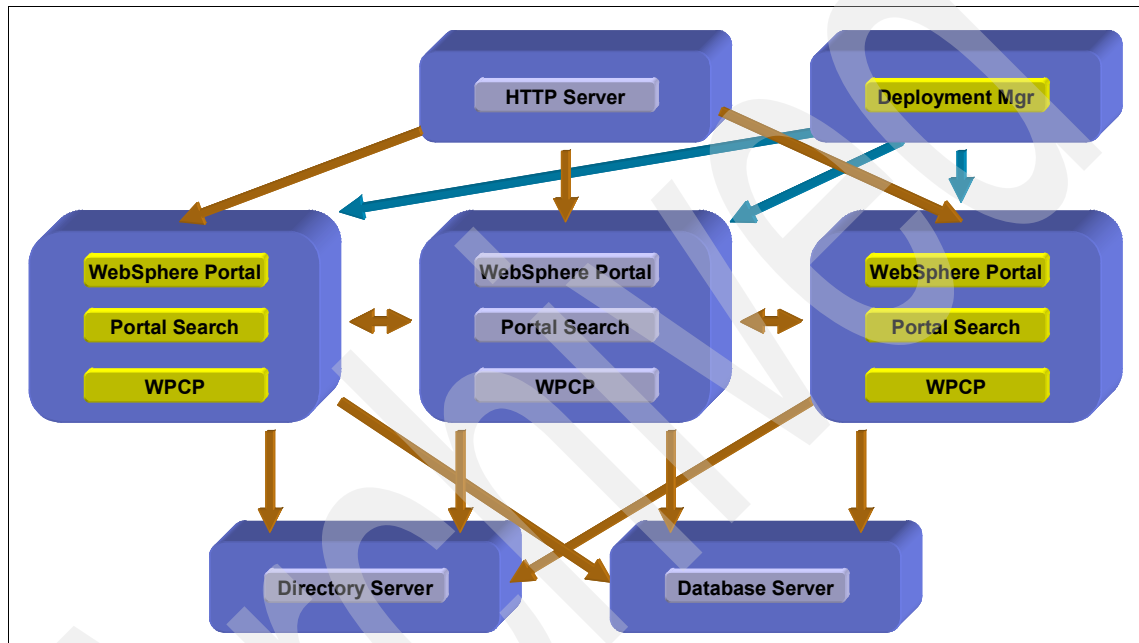


Figure 1-7 Horizontal Portal cluster

1.7.2 The vertical Portal cluster

A vertical Portal cluster provides additional scalability if you cannot drive your node CPU load on one server instance. This environment provides process failure tolerance.

Figure 1-8 illustrates the vertical Portal cluster using WebSphere Application Server clustering capabilities. This clustering approach does not provide additional hardware and capacity.

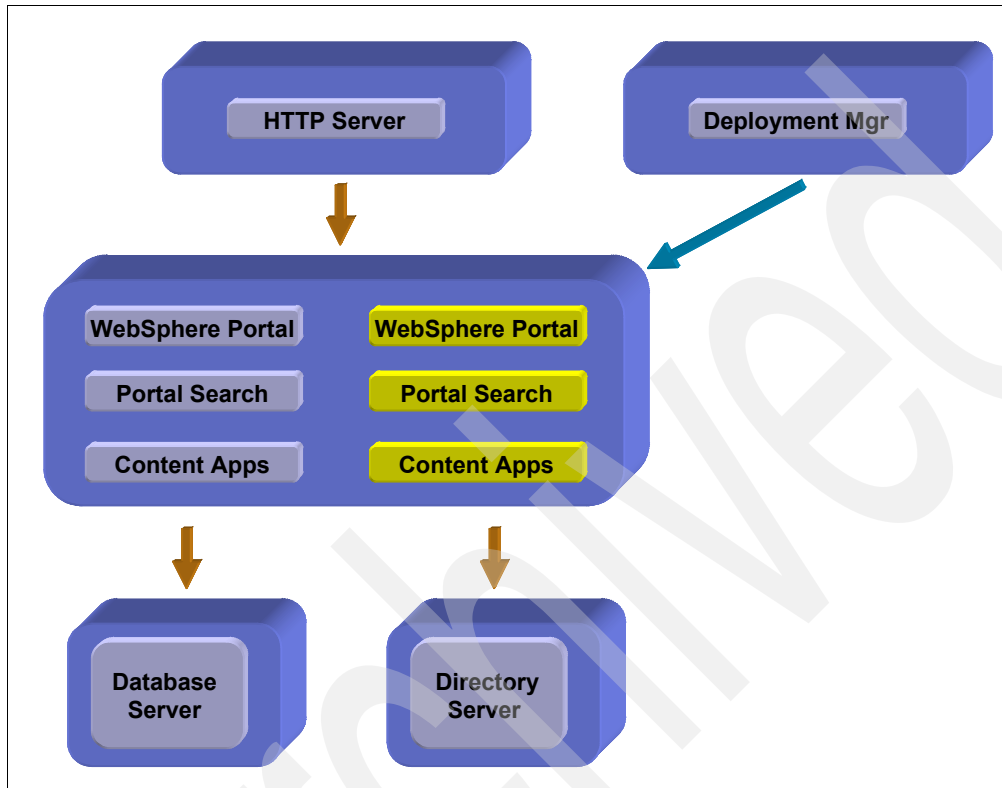


Figure 1-8 Vertical Portal cluster

1.8 Decoupling from back-end systems

You can decouple back-end systems by using forward caching proxies which reduce latency due to back-end access using a cacheable protocol. Forward caching proxies tie into an existing environment to optimize the application running over the network. In this environment, cache can use data sharing, thus reducing bottlenecks.

Note: Static content can be cacheable.

Figure 1-9 illustrates how the decoupling of back-end systems decreases the network latency and load on back-end systems.

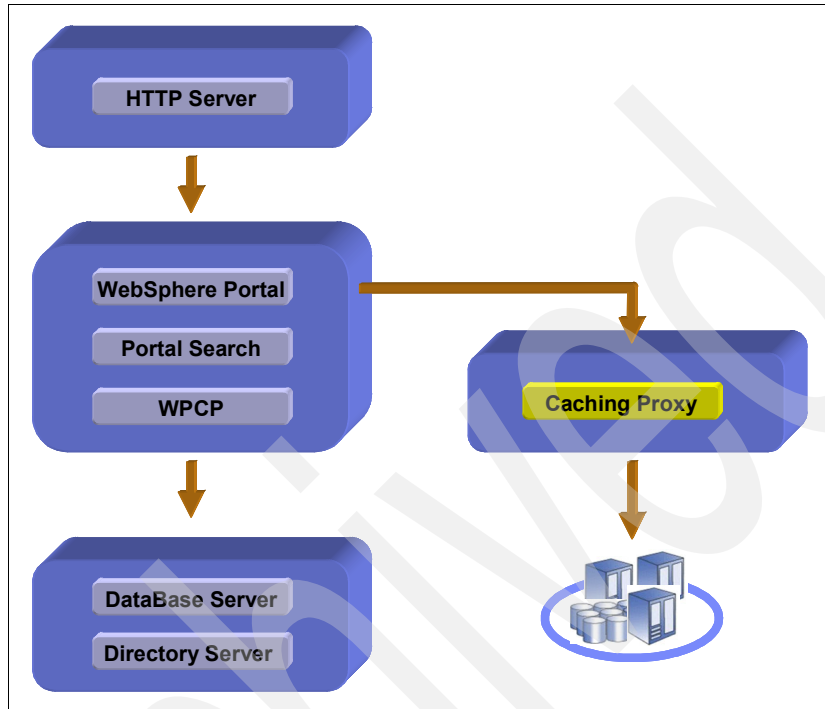


Figure 1-9 Decoupling from back-end systems

1.9 Example architectures in operation

This section contains examples of architectures that IBM Clients are using today.

1.9.1 The elaborated Portal cluster

The elaborated Portal cluster is a typical fault tolerant Portal cluster where caching is typically used. This solution avoids a single-point-of-failure with redundancy across the board. Each Portal is running in a different physical location (in this example, one in Raleigh and one in Charlotte). Only one directory server and database server is active at one time. Support 24x7 can also be used.

Figure 1-10 illustrates how this Portal architecture avoids a single-point-of-failure and makes use of caching.

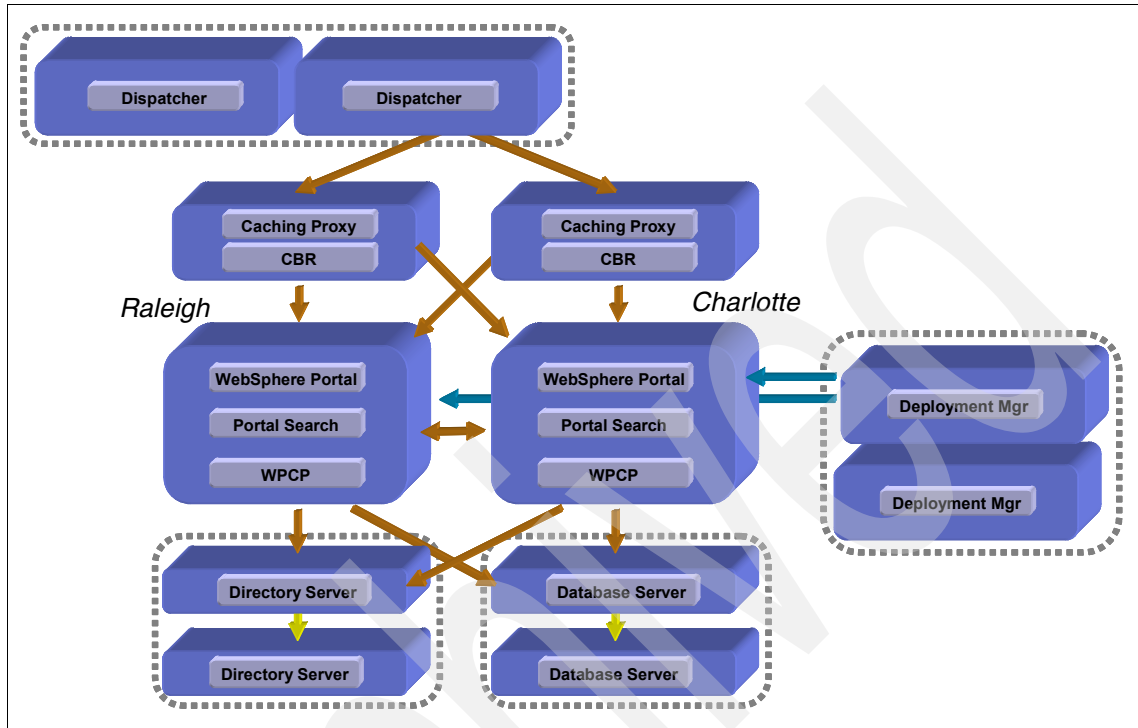


Figure 1-10 Elaborated Portal cluster

1.9.2 The elaborated security Portal cluster

In Figure 1-11 on page 18, the Portal cluster adds a security server (either Tivoli Access Manager or SiteMinder) providing 24x7 security operation. In addition, a Single Sign On environment can exist without having to logon more than once. This Portal architecture avoids a single-point-of-failure and makes use of caching and enhanced security. The location of security proxies allows for protection of cached content.

Note: Cacheable content can be protected by its own security manager.

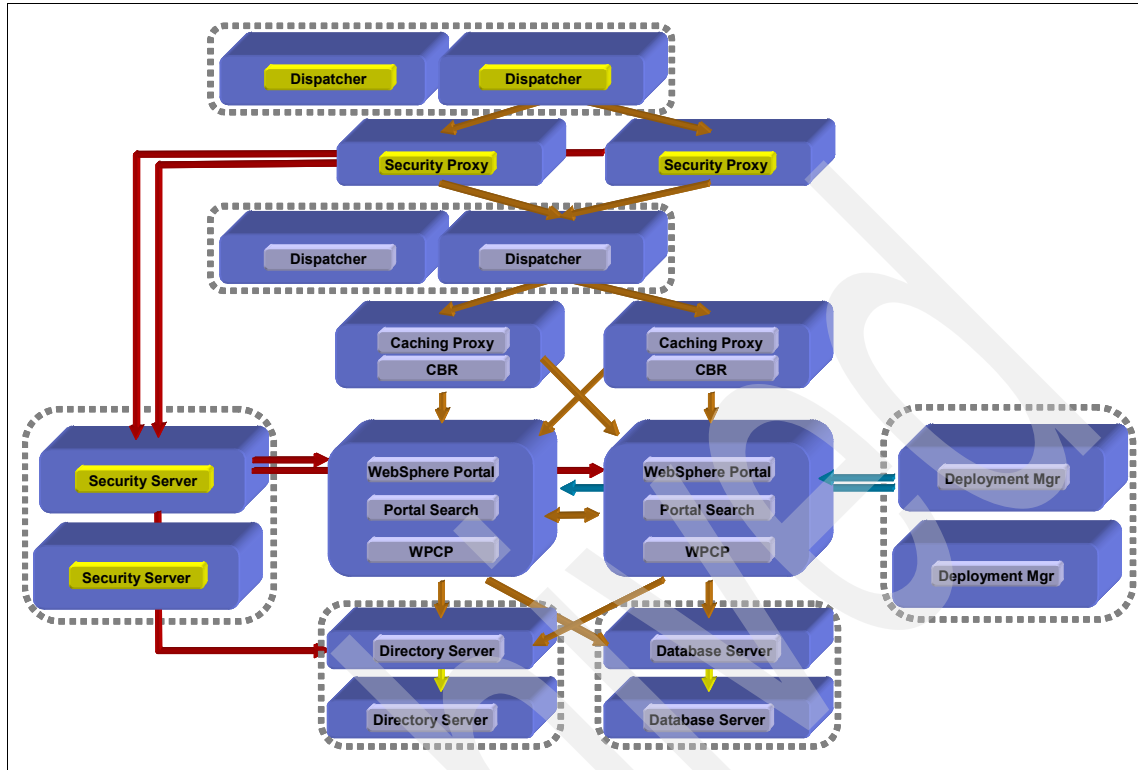


Figure 1-11 Elaborated security Portal cluster

1.9.3 The Availability Gold Standard

The Availability Gold Standard allows WebSphere Portal to run on two sets of clustered machines. This Portal architecture allows you to operate in a 24x7 environment while maintaining easy configuration and maintenance procedures. This is both an active and a passive configuration. The other side is used as a warm backup.

Continuous operation

The following statement speaks to the high availability of components operating in a 24x7 environment.

Glossary of Telecommunications Standard [1037C - 1997]

Operation in which certain components, such as nodes, facilities, circuits, or equipment, are in an operational state at all times. (188) Note: Continuous operation usually requires that there be fully redundant configuration, or at least a sufficient X out of Y degree of redundancy for compatible equipment, where X is the number of spare components and Y is the number of operational components.

In data transmission, operation in which the master station need not stop for a reply from a slave station after transmitting each message or transmission block.

WebSphere Portal is architecturally designed for continuous operation scenarios and additional fault tolerance.

Figure 1-12 illustrates two separate WebSphere Portal infrastructures. One is active, and the other one is in standby mode.

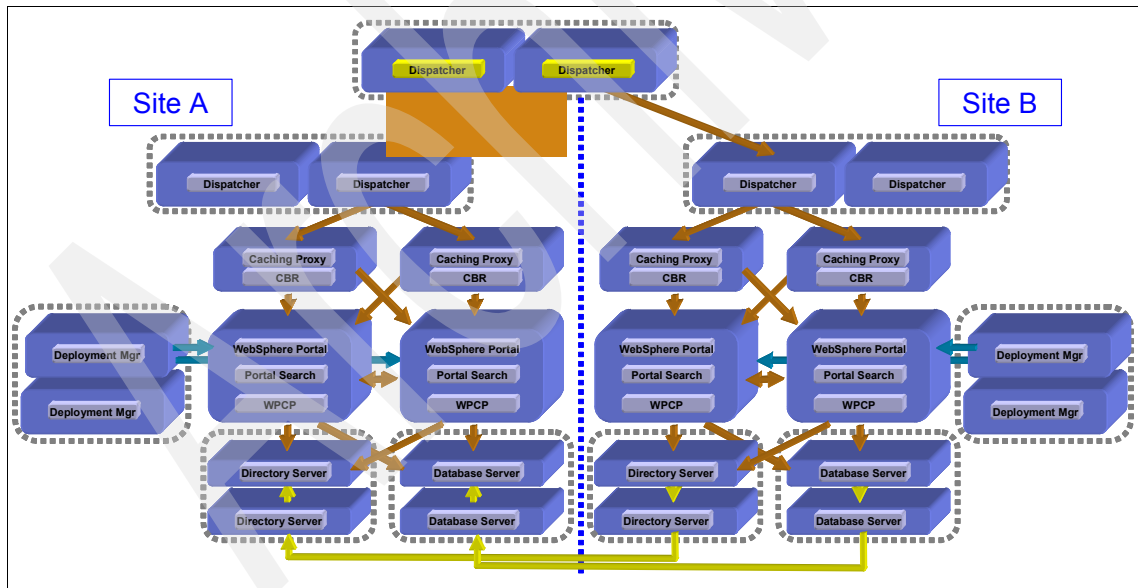


Figure 1-12 Availability Gold Standard architecture

Installing WebSphere Portal

This chapter discusses the planning, installation, and configuration activities that are required to deploy a WebSphere Portal production environment. It provides Portal administrators with a roadmap that includes a suggested approach, best practices, links to required resources, and hints to ensure a successful installation and configuration.

2.1 Getting ready for the installation

WebSphere Portal for Multiplatforms is not a single product. Instead, it is a software solution that contains multiple components. Depending on the architecture and topology, the installation task requires different skills and expertise. For example, installing a large Portal environment usually requires the efforts of the Portal server administrator as well as an IT architect, a database administrator (DBA), a security specialist, a Lightweight Directory Access Protocol (LDAP) specialist, and infrastructure (operating systems and networking) administrators. The Portal administrator must gather the required information and documentation for the installation and must also coordinate the team of experts when preparing to build production Portal environments.

A high-level overview of a roadmap for a production Portal server installation includes two phases:

Planning phase

1. Understanding the basic technology and components of the Portal
2. Specifying any requirements
3. Defining the topology and planning the capacity
4. Reviewing installation prerequisites and latest news
5. Planning for the integration of back-end servers
6. Compiling installation documents
7. Preparing for preinstallation activities

Installing phase

1. Setting up the infrastructure
2. Installing the basic configuration for WebSphere Portal
3. Installing the Network Deployment server
4. Installing Web servers and Load Balancer
5. Applying fixpacks and fixes
6. Installing the back-end servers
7. Creating and configuring the Portal clusters

Remember that deploying a Portal production environment is a complex task. It can require quite a bit of time to accomplish the suggested procedures contained in this book. Depending on the topology chosen, the capacity of the servers, and the availability of team members, you should be prepared to allocate, at a minimum, a few days to complete the whole process. Good preparation and a consistent approach will help the procedure move smoothly.

2.1.1 Overview of production Portal architectures

To accomplish the purposes of this book in reproducing the most common production Portal configurations, we chose to build three different environments as shown in Figure 2-1.

The first environment is the staging environment. This environment includes a single-node Portal server, an LDAP server, and a database server. Generally, large environments would split the staging arena into two separate areas: development servers and a user acceptance testing (UAT) server. This approach allows the development team to use rapid development tools along with all-in-one-box Portal servers. By separating the development boxes and the UAT server, you can keep the development tasks from affecting the acceptance test. Development performance issues are not within the scope of this book, so only the UAT server is considered in this architecture.

In addition to the staging environment, we also included two production environments representing the AIX® and Linux® platforms.

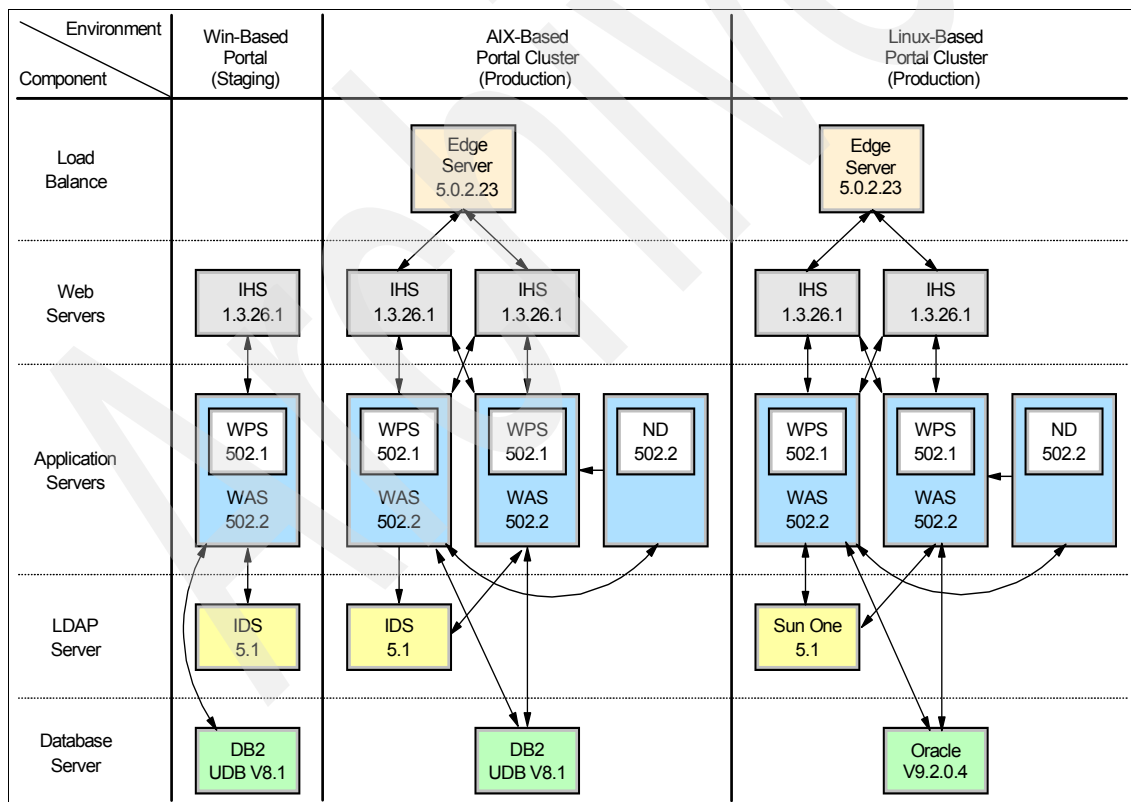


Figure 2-1 Staging and production environments

2.2 Suggested roadmap

Because of several different scenarios, platforms, and configurations, the effort to locate and review all the necessary information for a Portal install can be considerably challenging. The roadmap described in this section is intended to help Portal administrators to understand the installation activities performed in the development of this book. In addition, Portal administrators should review other documents and resources that are available. For information about other documents and resources available, see “Related publications” on page 281. In this book, the additional information is related to best practices and hints that apply only to production environments.

2.2.1 Planning phase

In environments that contain multiple servers, planning is the foundation step for stable, well behaved, and solid production servers. This section introduces a planning roadmap, along with several required resources that the Portal administrator should review prior to the planning phase. While planning the installation, the Portal administrator should assure compatibility and the support level for the entire environment, depending on feedback from other administrators. After completing the planning phase, the Portal administrator can launch the installation phase based on the documents produced during the planning phase, guarantying that the required installation information is available.

Step 1. Understanding the basic technology and components of the Portal

Understanding the Portal technology and components before you begin the planning and installation phases is critical. You should have a knowledge of key Portal concepts, such as single sign-on, security, directory services, content management, collaboration, search and taxonomy, support for mobile devices, accessibility support, and internationalization. If you are not familiar with Portal technology, review the following basic Portal documents:

- ▶ Guide to WebSphere Portal 5.0
http://www-106.ibm.com/developerworks/websphere/library/techarticles/0310_wendel/wendel.html
- ▶ *IBM WebSphere Portal for Multiplatforms V5 Handbook*, SG24-6098, Chapters 1 and 2
<http://www.redbooks.ibm.com/abstracts/sg246098.html>
- ▶ WebSphere Portal InfoCenter, Product Overview section
<http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/index.html>

Step 2. Specifying any requirements

Portals are a central point of access that encapsulate several components and functions. Before you begin the installation, you should conduct a thorough review with user representatives and IT architects to define functionality and performance objectives for the Portal.

Portal functions may include both WebSphere Portal functions and also external legacy systems. WebSphere Portal includes features such as Collaboration, Personalization, Extend Search, Click-to-Action, Translation, Single Sign On, Content management, and many others. For more information, see the resources listed in “Related publications” on page 281.

For the discussion in this book, the Portal functionality is based upon the built-in features of WebSphere Portal. This environment is the most common for the majority of Portal administrators when they first deploy Portals in production.

The logical design and software components for both the staging and production Portals include:

- ▶ Support for an external user registry running on database manager systems (for example, Oracle and DB2®)
- ▶ A user directory running on an LDAP-compliant component (for example, IDS and Sun ONE)
- ▶ WebSphere Portal Extend Edition V5.0.2.1
- ▶ Support for Load Balance component (Edge Server)
- ▶ Support for remote Web servers (IBM HTTP Server)
- ▶ Support for WebSphere Portal application clustering (WebSphere Application Server Network Deployment)

Step 3. Defining the topology and planning the capacity

Deploying a production Portal differs from other environments mainly because the deployment needs to happen as fast as possible in a highly controlled environment. Availability, stability, and performance are the main concerns for Portal administrators by the time a production Portal is designed. The business users of the Portal and the solution architect need to evaluate these concerns and to define clip levels. The criteria that you use for such definitions can vary according to the main objectives for your Portal environment.

A simple checklist on performance parameters that you need to consider when you define the specification are:

- ▶ The number of concurrent users
- ▶ The page views per second
- ▶ The average CPU usage per server
- ▶ Response time

Assuming that the Portal functionality and performance objectives are clearly understood, Portal administrators and IT architects should evaluate multiple scenarios and then design and document the final topology.

Defining the topology is a major step needed before you move from the planning phase to the installation phase. When you define the topology, you select the software components that you will use along with WebSphere Portal and how those components will be organized.

Review the following WebSphere Portal documentation before continuing:

- ▶ For installation matters, visit WebSphere Portal InfoCenter and see the Portal library page:

<http://www-106.ibm.com/developerworks/websphere/zones/portal/proddoc.html>

Look for the section *Version 5.0.x Information Centers* and choose the appropriate edition of WebSphere Portal. (See your CD package to assure which edition you should review.)

Note: This book uses WebSphere Portal Extend for Multiplatforms Version 5.0.2.1. For more information about the different editions and packages of WebSphere Portal, refer to the *Product Overview* section of the WebSphere Portal InfoCenter or the Guide to WebSphere Portal 5.0 document available at:

ftp://ftp.software.ibm.com/software/websphere/portal/pdf/Guide_to_WebSphere_PortalV5.pdf

- ▶ *IBM WebSphere Portal for Multiplatforms V5 Handbook*, Chapter 3

<http://publib-b.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/sg246098.html?Open>

For this book, we selected a topology that makes it possible to achieve a high level of performance and flexibility. We used a four-tier design that includes layers for load balancing, Web servers, application servers, Portal servers, and a database server. Clustering applies to the Web server, application server, and Portal server layers. Remote Web servers running WebSphere Application Server plug-ins perform the first level of load balancing. Another level of load balancing is implemented by a front-end Load Balance server (Edge Server). We

chose horizontal clustering because of its flexibility and performance. (See 1.7, “Portal clustering” on page 13 for more information.)

The output for this step is a set of documents that depicts the details for the logical and physical design of the Portal solution. Hardware capacity, software components, and network configuration should be included in this set of documents. For a sample topology and capacity Portal cluster for Linux, see Figure 2-2.

Databases and LDAP directories are most commonly managed by their own administrators. Thus, Portal administrators should communicate the Portal solution requirements in terms of database instances and directory configurations to these administrators. See Appendix B, “Portal installation worksheets and samples” on page 235 for sample forms and worksheets that you can use to clarify the workflow between the Portal and back-end server administrators.

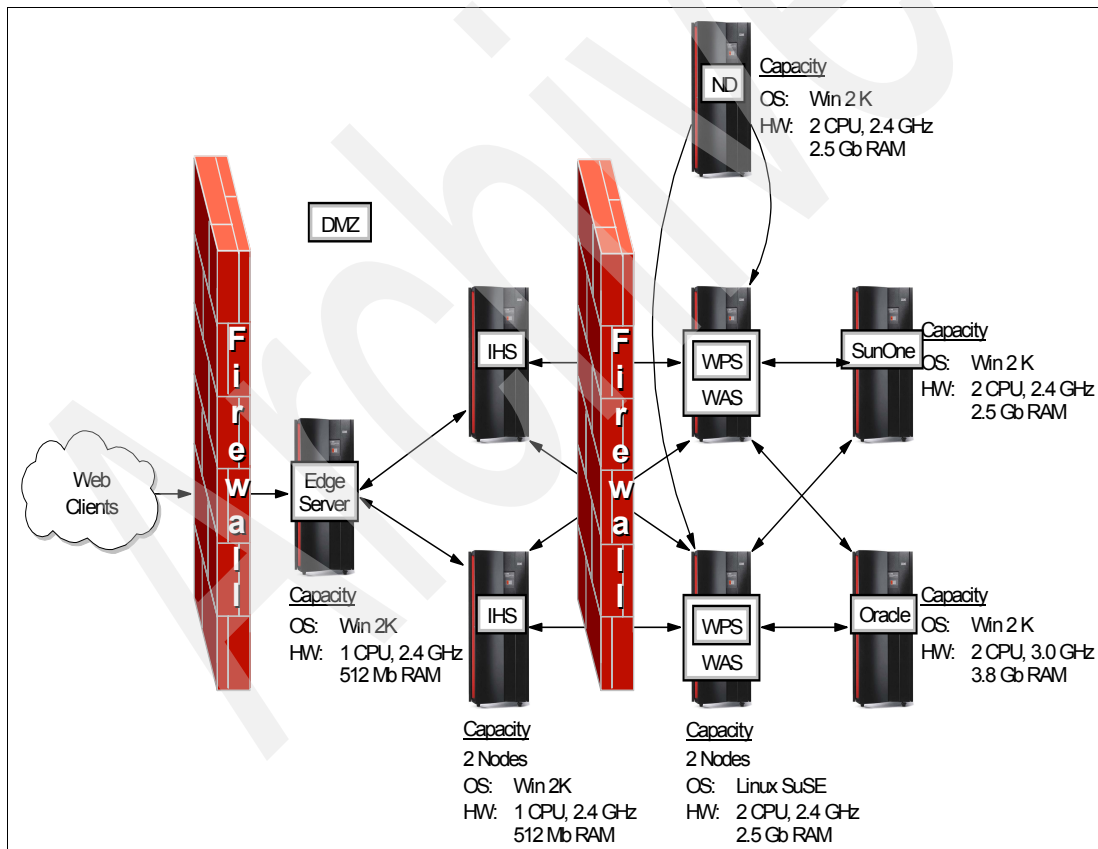


Figure 2-2 Portal cluster topology and capacity for a Linux system

Step 4. Reviewing installation prerequisites and latest news

After reviewing the logical and physical design, Portal administrators must ensure that all components included in the Portal solution are supported. In addition, check and verify any required upgrades to the software components. For a list of the latest supported hardware and software for WebSphere Portal, see:

http://publib.boulder.ibm.com/pvc/wp/5021/ent/en/InfoCenter/wpf/inst_req.html

You should also review the Release Notes for the WebSphere Portal edition that you are using in the Portal solution. For WebSphere Portal V5.0.2.1 Notes, see:

http://publib.boulder.ibm.com/pvc/wp/5021/ent/en/release_notes_ent.html

Step 5. Planning for the integration of back-end servers

To integrate WebSphere Portal with back-end servers, such as database and LDAP servers, the production Portal must have a database manager and an LDAP directory running outside the Portal server machine for performance reasons. Thus, you should create and tune a database and directory infrastructure on which the Portal application will rely.

To install a database and LDAP server on dedicated machines, you need to:

1. Install the database and LDAP server on dedicated machines if they are not currently installed or available.
2. Create and configure the Portal databases on the database server.
3. Install the database client code at the Portal machine and validate communication with the database server.
4. Add the Portal users and groups to the LDAP directory.
5. Establish and test communication between the Portal, database, and LDAP servers.
6. Run the Portal configuration tasks.

Some of these steps require specific skills, most commonly provided by the database and the LDAP administrators. Nevertheless, the Portal administrator still needs to specify and communicate Portal requirements to these administrators.

To help simplify the process, see Appendix B, “Portal installation worksheets and samples” on page 235. These worksheets are customized for database (DB2 and Oracle) and LDAP (IDS and Sun ONE) configurations. These forms are quick snapshots of the information that is described in the database and LDAP

installation sections of the WebSphere Portal InfoCenter. Review the database and LDAP installation sections in the following documentation before continuing:

<http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/index.html>

Each form is made of two sections. Update the first section by completing the parameters in the Value column. Then, communicate this information to the database and LDAP administrators. This installation worksheet contains the necessary data for the database and LDAP administrators to accomplish their infrastructure settings task. These administrators return the second form after the infrastructure settings task is complete. You need the data that the second form contains to perform the Portal configuration steps.

Step 6. Compiling installation documents

Before you install WebSphere Portal, be sure to collect all the required information, documents, and installation parameters from the worksheets available in Appendix B, “Portal installation worksheets and samples” on page 235. Completing the worksheets will help you anticipate any possible misconfiguration issues and avoid Portal installation failures.

Step 7. Preparing for preinstallation activities

It is necessary that you apply several fixes from different sources to accomplish the full WebSphere Portal V5.0.2.1 installation. Table 2-1 lists the fixes, patches, and maintenance packages that we used in the installation phase of this chapter.

Table 2-1 Fixes, patches, and maintenance packages

Sources	Available at
Windows® 2000 service packs	http://www.microsoft.com/windows2000/downloads/servicepacks/default.asp
AIX maintenance page	http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp
WebSphere Application Server support	http://www-306.ibm.com/software/webservers/support.html
WebSphere Portal Server support	http://www-306.ibm.com/software/genservers/portal/support/

2.2.2 Installation phase

This section outlines the installation process for both the staging and production servers. The complete process is divided into several steps and highlights the main issues, concerns, and validation procedures that you should be aware during the installation of each component in the Portal architecture.

Step 1. Setting up the infrastructure

This section explains how to set up the infrastructure.

Operating systems

In most organizations, the infrastructure is managed by the operational support team. Make sure that you give the infrastructure worksheet (see Table B-1 on page 236) to the administrator and that you place a request for the basic operating system and network setup.

Considering the operating system installation, there are two possible scenarios. You can use a server that is currently installed, or you can build the system from scratch and install a new instance of the operating system. With the first scenario, make sure that other installed products are compatible and will not cause port conflicts with WebSphere Portal. Ports already in the system may cause conflicts and failures during the installation process. Table 2-2 lists the main ports that WebSphere Application Server and WebSphere Portal use.

Table 2-2 Main WebSphere ports

Port	WebSphere Application Server	WebSphere Portal Server
HTTP Transport	9080	9081
HTTPS	9443	9444
HTTP Administrative Console	9090	9091
HTTP Administrative Console Secure	9043	9044
Internal JMS Server	5557	
JMS Server Queued Address	5558	
Bootstrap	2809	9810
SOAP Connector	8880	
DRS Client Address	7873	

You can identify those ports that are listed on the server by using the **netstat** command:

- ▶ On Windows servers
`netstat -an | find "LISTEN"`
- ▶ On Linux servers
`netstat -an | grep LISTEN | grep tcp`
- ▶ On AIX servers
`netstat -an | grep LISTEN`

With the second scenario, where you are installing a new instance of the operating system, make sure that you install the appropriate version of the operating system and patches. You should also install utilities that will be useful during the Portal installation, such as a tool that extracts files from zipped files, remote access tools, FTP servers, and so on.

In the staging server, we installed the following Windows 2003 Server Standard Edition components:

- ▶ Windows 2003 Server Standard
- ▶ A tool that extracts files from zipped files
- ▶ Support for terminal services client and remote desktop

We did not install patches in the staging server.

Note: For remote installation on Windows 2003 boxes, Windows 2003 automatically enables Terminal Services. However, you need to configure Remote Desktop before a terminal services client will connect to the server. To do so, right-click the My Computer icon and select **Properties**. Select the **Remote** tab and enable Remote Desktop by clicking **Allow users to connect remotely to this computer**.

In the Web servers, we installed the following Windows 2000 components:

- ▶ Windows 2000 Advanced Server
- ▶ Service Pack 4
- ▶ A tool that extracts files from zipped files

Verify your Windows version by right-clicking the My Computer icon and selecting the **General** tab in the System properties panel. You will see a window similar to Figure 2-3 on page 32.

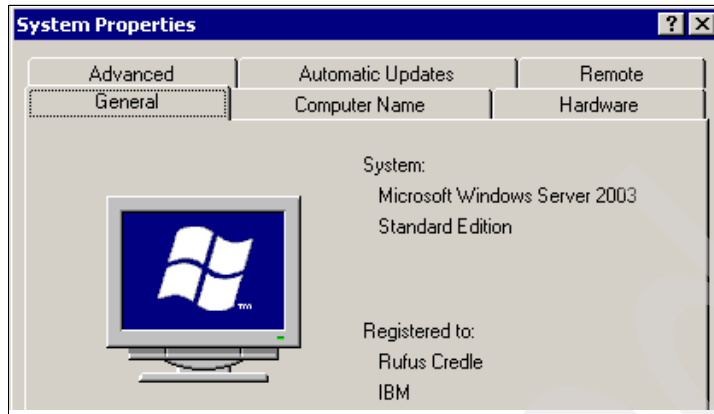


Figure 2-3 Verification of Windows 2003 version

In the production servers, we installed the following editions of AIX and Linux:

- For AIX
 - AIX V5.2.
 - Maintenance Level 02
 - APAR IY43952

You need to verify the AIX version and patches that are applied by running the commands shown in Figure 2-4.

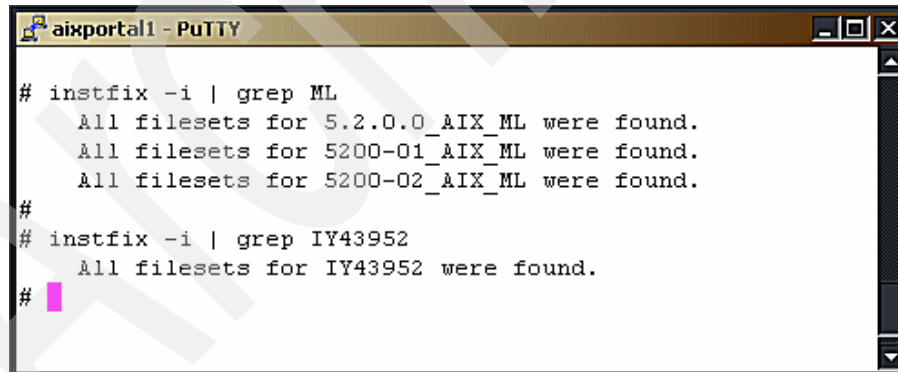
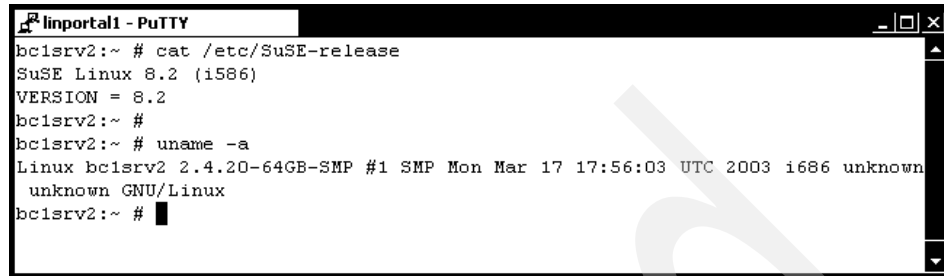


Figure 2-4 verification of AIX version and patches

- For Linux
 - SUSE SLES Linux for Intel® V8.2
 - No patches applied

You need to verify the Linux version and kernel release by running the commands shown in Figure 2-5.



```
linportal1 - PuTTY
bc1srv2:~ # cat /etc/SuSE-release
SuSE Linux 8.2 (i586)
VERSION = 8.2
bc1srv2:~ #
bc1srv2:~ # uname -a
Linux bc1srv2 2.4.20-64GB-SMP #1 SMP Mon Mar 17 17:56:03 UTC 2003 i686 unknown
GNU/Linux
bc1srv2:~ #
```

Figure 2-5 Verification of Linux version and kernel

Note: Before proceeding, assure that the system clock for each server is synchronized to the same hour and minute time stamp.

Administrator user

In Windows 2000 and 2003, you must grant the administrator user ID specific privileges before you run the Portal installer. Make sure that the administrator user ID is allowed to:

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

You can change user privileges by selecting **Control Panel → Administrative Tools → Local Security Policy → Security Settings → Local Policies → User Rights Assignment**.

Storage and file system

WebSphere Application Server and the WebSphere Portal server require a large amount of disk space. Thus, you need to allocate the necessary storage.

Review the prerequisites available from the WebSphere Portal InfoCenter for an updated list of the minimum storage requirements for the Portal server:

http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/wpf/inst_req.html

Windows servers administrators need only to verify the total available amount of disk storage and to assure that the minimum space requirements are satisfied. We encourage UNIX® administrators to create separate file systems for WebSphere Application Server and WebSphere Portal. Linux administrators should pay special attention to the size of the swapping partition, which must be at least as big as the physical memory of the server. Small swapping partitions

slow down the server so much that the Portal installer will fail during basic Portal setup.

Network setup

Network configuration is required to allow the Portal installer to run without failures. Each server included in the Portal solution is required to hold a static IP address, to have a fully qualified domain name, and to belong to the same domain as all other servers for single sign-on purposes.

Network setup validation is essential and is required before the Portal installer is run.

Verify the Windows 2000 and 2003 servers network configuration by selecting **Start → Settings → Network and Dial-Up Connections**. Right-click **Enabled connection**, and select **Properties**. Select **TCP/IP** and click **Properties**. You should get a window similar to Figure 2-6.

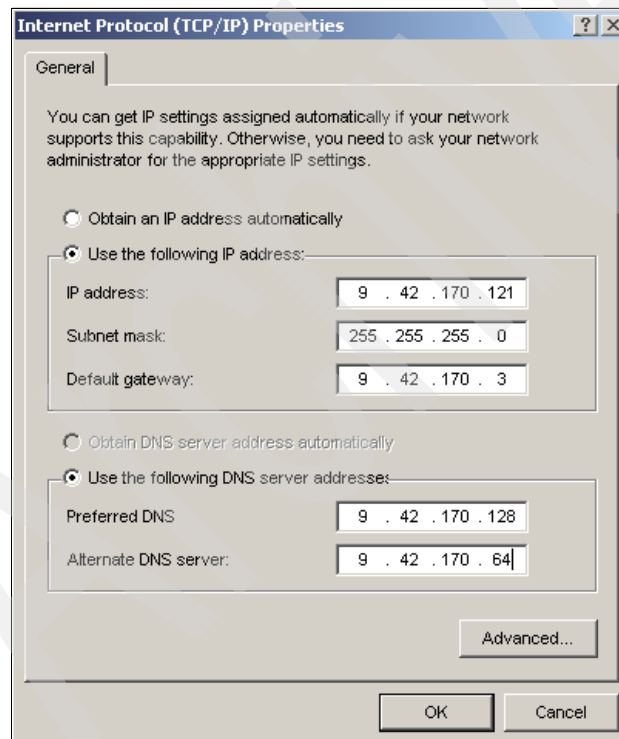


Figure 2-6 Verification of Windows 2000 network configuration, IP address

Also, you should verify that the domain name is correctly defined using the **ipconfig** command as shown in Example 2-1.

Example 2-1 Host name and domain validation in Windows 2000/2003

```
C:\Program Files\Administrator > ipconfig /all

Windows 2000 IP Configuration
Host Name . . . . . : devportal
Primary DNS Suffix . . . . . : redbook.ibm.com
```

Verify the AIX network configuration by running the following command:

```
# smitty tcpip
```

On the TCP/IP menus, select **Minimum Configuration** and **Startup**. Then, move the cursor to the main network interface and press Enter. You will see a window similar to Figure 2-7 that presents all network parameters.

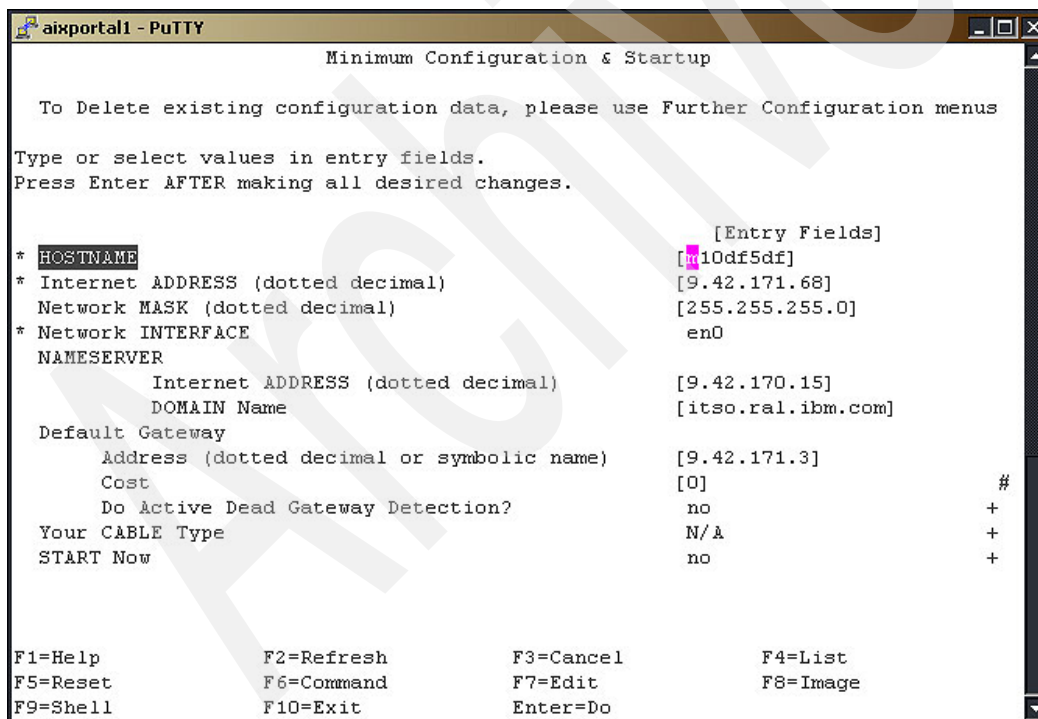
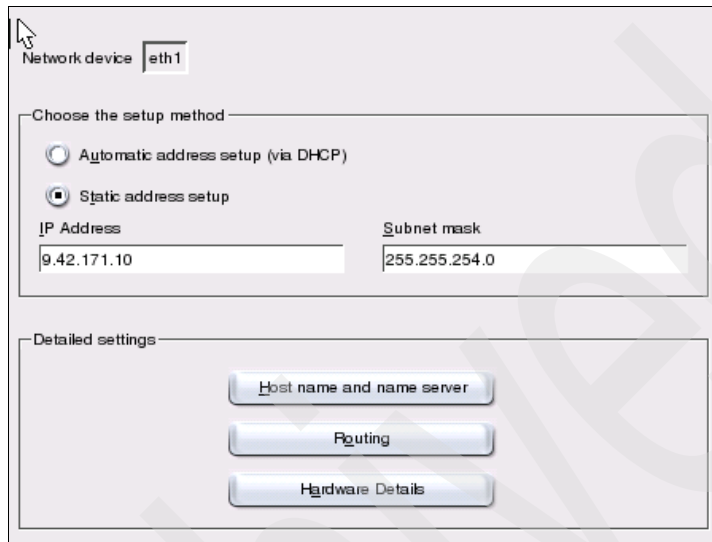


Figure 2-7 Verification of AIX network configuration

Verify the Linux network configuration by running the YaST Control Center utility. To do so, select **Yast2 Modules** → **Network Devices** → **Network card** → **Change**. On the list of available cards, select the current enabled interface and click **Edit**. A window similar to that shown in Figure 2-8 will appear.

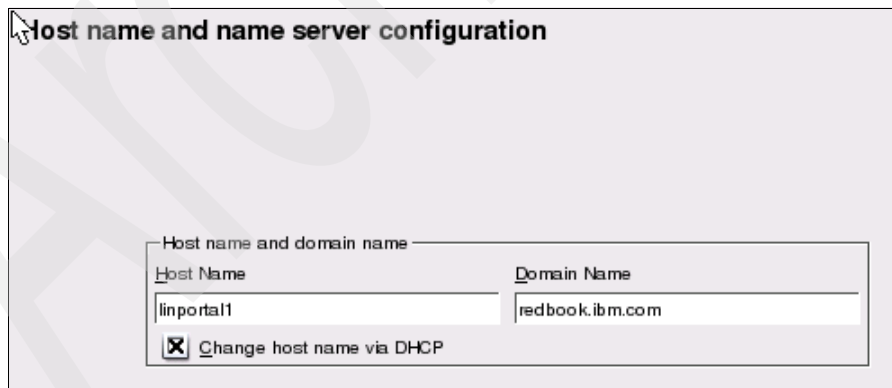


The screenshot shows the 'Network device' configuration window for the interface 'eth1'. It has a tabbed interface with the following sections:

- Choose the setup method:** Contains two radio buttons: 'Automatic address setup (via DHCP)' (unselected) and 'Static address setup' (selected).
- Static address setup fields:**
 - IP Address:** A text field containing '9.42.171.10'.
 - Subnet mask:** A text field containing '255.255.254.0'.
- Detailed settings:** A section containing three buttons: 'Host name and name server', 'Routing', and 'Hardware Details'.

Figure 2-8 Verification of Linux network configuration, IP address

In this window, select **Host name and name server** and verify the host and domain names, as shown in Figure 2-9.



The screenshot shows the 'Host name and name server configuration' window. It contains the following fields and options:

- Host name and domain name section:**
 - Host Name:** A text field containing 'linportal1'.
 - Domain Name:** A text field containing 'redbook.ibm.com'.
- Change host name via DHCP:** A checkbox that is checked (indicated by an 'X' in the box).

Figure 2-9 Verification of Linux network configuration, Host Name and Domain Name

Important: If you are using a firewall to restrict TCP/IP connections among the servers, then you must validate that the required communication ports between the Portal server and all other servers are active. The **telnet** command is the fastest way test these communication ports. If the firewall is configured correct, an error is not echoed back when you use the **telnet** command. Also, make sure that no firewall software is running on the Portal server during the Portal installation.

Step 2. Installing the basic configuration for WebSphere Portal

You can run the Portal installer in three different modes:

- ▶ Graphical User Interface (GUI) mode
- ▶ Text console mode
- ▶ Silent installation mode

A silent installation is suitable for production environments where you will install several instances of Portal server. Based on response files, you need to customize only a few parameters that change from server to server (for example, host name) before you launch the next run of the Portal installer.

Another advantage of a silent installation is that the installation facts are documented in text files that you can add to the server's documentation folder. You should load binary images of the Portal CDs into a disk drive that is shared by all the servers where the Portal installation will be run. A sample response file for Portal installation on Windows 2000 is available in Appendix B, "Portal installation worksheets and samples" on page 235.

Note: Support for Windows 2003 was introduced in WebSphere Portal V5.0.2. You should review the WebSphere Portal V5.0.2 installation readme file for installation instructions, because Windows 2003 installation is slightly different from other platforms.

http://publib.boulder.ibm.com/pvc/wp/502/ent/en/readme/install_win2003.html

Some versions of Java can report Windows 2003 incorrectly. For more information, see Technote 1173948:

http://www-1.ibm.com/support/docview.wss?rs=688&context=SSHRKX&q1=Windows+2003&uid=swg21173948&loc=en_US&cs=utf-8&lang=en

Before you run the installation procedure, make a backup copy of the vpd.properties file. In case you need to manually uninstall the Portal server (for example, due to a Portal installation failure), you can use the backup copy of this file instead of manually editing it to remove Portal server entries from the

installed software index. Table 2-3 lists the location of the vpd.properties file on Linux, AIX, and Windows operating systems.

Table 2-3 vpd.properties location by platform

Operating System	Location
Linux	/vpd.properties or /root/vpd.properties
AIX	/usr/lib/objrepos/vpd.properties
Windows	C:\WINNT\vpd.properties

Because of the small number of servers installed on the staging and production servers, we used the GUI mode for the Portal installation on these servers. We used the procedures in *IBM WebSphere Portal for Multiplatforms V5 Handbook* to accomplish the basic Portal configuration installation (see 2.3, “Portal documentation” on page 63).

After completing the basic installation, verify that no failures occurred by reviewing the installation log files. (See “Verifying Portal installation log files” on page 246 for a detailed description on reviewing these files.) For this book, we followed the instructions available in Chapters 5 and 6 in *IBM WebSphere Portal for Multiplatforms V5 Handbook*.

Step 3. Installing the Network Deployment server

To install WebSphere Network Deployment Server (Base), follow these steps:

1. Login to the server to be used as your Network Deployment server as an administrative user (for example, root).
2. Mount the WebSphere Application Server Network Deployment CD to /cdrom.
WebSphere Application Server ND is available in WebSphere Portal V5.0.2 CDs 1-10 (Linux) or 1-11 (AIX).
3. Run LaunchPad.sh from \cdrom\wasnd\linux\linuxi386 (Linux) or \cdrom\wasnd\aix\aix (AIX) and follow the instructions that appear.
4. Make sure that you select all features for installation.
5. Accept the default installation path for installation.
6. Accept the default settings for NodeName, HostName, and CellName. Be sure that HostName contains the fully qualified domain name of the server. If not, update it manually with the server's fully-qualified domain name.

7. When the installation finishes, check the installation log file named log.txt at /WebSphere/DeploymentManager/logs for errors or exceptions. Be sure that the following message appears in the log file:

INSTFIN: The WebSphere 5.0 install is complete

To install the WebSphere Application Server Network Deployment Enterprise components, follow these steps:

1. Mount the WebSphere Application Server Enterprise CD to /cdrom.
WebSphere Application Server Enterprise is available in WebSphere Portal V5.0.2 CDs 1-2 (Linux) or 1-3 (AIX).
2. Run LaunchPad.sh from \cdrom\was\linux (Linux) or \cdrom\was\aix (AIX) and follow the instructions that appear.
3. Make sure to select the Add option to the existing copy of WebSphere Application Server Network Deployment V5.0.
4. When the installation finishes, check the installation log file named WAS.PME.install.log at /WebSphere/DeploymentManager/logs for errors or exceptions. Be sure that the following message appears in the log file:

The InstallShield Wizard has successfully installed IBM WebSphere Application Server.

Step 4. Installing Web servers and Load Balancer

For production Portals, the integration of HTTP servers must handle the client HTTP requests. For details on the Portal configuration procedure for external remote Web servers, refer to the following:

http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/wpf/inst_ihs.html

Installing Web servers

Before you configure the Portal, install the Web servers by following these steps:

1. Login to the server intended for the Web HTTP services using the Administrator id. (This procedure assumes that IHS 1.3.26 is running on top of Windows 2000 SP4.)
2. Run install.exe from Portal cd1-1. See the directory \was\win\Was50.
3. Read the agreement and select the Language for the installation program. Then, click **Next** in the first panel.
4. Select **I accept the terms in the license agreement** and click **Next**
5. Select **Custom** for the setup type and click **Next**.
6. Disable all components and select **IBM HTTP Server 1.3.26**. Select **Yes, Web Server Plugins - IBM HTTP Server**.

7. Verify the installation path and click **Next** in the summary panel.
8. Wait until the installation finishes and click **Finish**.
9. Verify the installation by loading the IHS welcome page at:

`http://localhost`

Installing Load Balancer

The load balancing tool that we used in the production Portal server is WebSphere Edge Server V5.0 for Windows 2000. This product is included in WebSphere Portal Server V5.0.2 package. To install the load balancer, follow these steps:

1. Login to the server intended for the load balancing services using the Administrator id. (This procedure assumes that Edge Server V5.0 is running on top of Windows 2000 SP4.)
2. Run setup.bat from Portal cd1-21. See directory \wasedge\win.
3. Select the Language for the installation program and click **Next** in the first panel.
4. Select **Install** and click **Next** in the following window.
5. Read the agreement, select **I accept the terms in the license agreement**, and click **Yes**.
6. Select **Load Balancer and Documentation** from the components list and click **Next**.
7. Click **Finish** in the summary panel.
8. Wait until the installation finishes and click **Finish**. The server will reboot automatically.
9. Verify the installation by reviewing Windows services list and assuring that the new service IBM Dispatcher is registered and successfully started.

For further details on the installation procedures, refer to:

<http://www-306.ibm.com/software/webservers/appserv/doc/v50/ec/infocenter/edge/concepts.htm>

After the base code installation, you also need to configure the Dispatcher to enable the load balancing between the two installed Web servers. To configure the Dispatcher:

1. Start all the Web servers.
2. On the Network Dispatcher server, select **Start** → **Programs** → **IBM WebSphere** → **Edge Components** → **Load Balancer** → **Load Balancer**.
3. Expand Load Balancer.

4. Right-click **Dispatcher** and select **Start Configuration Wizard**.
5. Click **Next** on the welcome pages.
6. Click **Create Configuration**.
7. Select the item corresponding to your host from the drop-down list and click **Update Configuration & Continue**.
8. Enter the cluster host name (for example, lincluster.redbook.ibm.com@) and click **Update Configuration & Continue**.
9. Verify that the cluster host name was added and click **Next**.

Note: This is the host name of the fully-qualified domain name that will be used to access the Portal cluster.

10. Choose **Port 80** and click **Update Configuration & Continue**.
11. Verify that the port was added and click **Next**.
12. Click **Add server**.
13. Enter the first HTTP server name.
14. Repeat the process and add the second HTTP server.
15. Click **Update Configuration & Continue**.
16. Choose **Yes** and click **Update Configuration & Continue**.
17. Click **Next**.
18. Choose **Windows 2000** and click **View Loopback Instructions**.
19. Review the directions and click **Next**.
20. Click **Exit** and the cluster configuration is done.

You also need to create and configure the loopback adapter with the following properties in each Web server:

- ▶ Static IP Address
 - IP address = cluster IP address (for example, the IP address of the server running Edge Server V5.0)
 - SubNet Mask = 255.0.0.0
- ▶ DNS configuration
 - Preferred DNS server = local IP address
 - No gateway

You can verify the Edge Server settings by loading the welcome HTTP server from each Web server individually. Assure that only one Web server is started

and load a browser with the cluster HTTP page (for example, lincluster.redbook.ibm.com). You should also load the HTTP server home page.

Step 5. Applying fixpacks and fixes

Upgrading WebSphere Portal V5.0 to WebSphere Portal V5.0.2.1 requires the installation of a varied set of fixes for several WebSphere components, such as WebSphere Application Server Base, WebSphere Application Server PME, and Portal server. You need to apply fixpacks and fixes to all existing WebSphere Application Servers, Web servers, Network Deployment Server, and Portal servers.

To apply fixpacks and fixes, follow these steps:

1. Upgrade WebSphere Portal V5.0 to V5.0.2 by applying Portal Fixpack 2.

For detailed instructions, refer to the WebSphere Portal v5.0 Fix pack 2 readme at the following Web address:

http://www-1.ibm.com/support/docview.wss?rs=688&context=SSHRKX&q1=5.0.2&uid=swg27004658&loc=en_US&cs=utf-8&lang=en

Portal Fixpack 2 files and instructions are also available on the Fixpack CD that comes with the WebSphere Portal V5.0.2 CD bundle.

2. Upgrade WebSphere Portal to V5.0.2.1 by applying Portal cumulative fix 1.

For detailed instructions, refer to the WebSphere Portal V5.0.2 Cumulative fix 1 Readme at the following Web address:

http://www-1.ibm.com/support/docview.wss?rs=688&context=SSHRKX&q1=5.0.2.1&uid=swg27005009&loc=en_US&cs=utf-8&lang=en

By reviewing the installation instructions on the Web, you will see that you need to apply several minor steps and prerequisite fixes packages to WebSphere Application Server before the Portal fixes are installed and the final configuration tasks are applied to Portal server. To clarify this process, you should review carefully the installation instructions on the Web and the recommended approach and auxiliary technotes in the remainder of this section.

WebSphere Portal V5.0 basic configuration installs WebSphere Application Server V5.0.1 as the foundation software. Note that the Enterprise modules are also installed. Thus, you need to apply all WebSphere Application Server related fixpacks to both the main WebSphere Application Server component (also known as WebSphere Application Server Base) and to the Enterprise component (also known as WebSphere Application Server PME).

To verify which WebSphere Application Server components and versions are installed, you can use the VersionInfo tool. This tool resides in the bin directory of the WebSphere Application Server home installation. By running the tool

immediately after installing WebSphere Portal V5.0 basic configuration, you should obtain the output shown in Example 2-2.

Example 2-2 Verifying WebSphere Application Server Base and PME versions

```
C:\WebSphere\AppServer\bin>versionInfo
WVER0010I: Copyright (c) IBM Corporation 2002; All rights reserved.
WVER0011I: WebSphere Application Server Release 5.0
WVER0012I: VersionInfo reporter version 1.13, dated 3/15/03
```

IBM WebSphere Application Server Product Installation Status Report

Report at date and time 2004-08-19T17:32:57-04:00

Installation

Product Directory	C:\WebSphere\AppServer
Version Directory	\${product.dir}\properties\version
DTD Directory	\${version.dir}\dtd
Log Directory	\${version.dir}\log
Backup Directory	\${version.dir}\backup
TMP Directory	C:\DOCUME~1\santos\LOCALS~1\Temp

Installation Platform

Name	IBM WebSphere Application Server
Version	5.0

Technology List

BASE	installed
PME	installed

Installed Product

Name	IBM WebSphere Application Server
Version	5.0.1
ID	BASE
Build Level	ptf1M0314.04
Build Date	04/08/2003

Installed Product

Name IBM WebSphere Application Server Enterprise
Version 5.0.1
ID PME
Build Level ptf10316.01
Build Date 04/22/2003

End Installation Status Report

Upgrading Portal server to V5.0.2.1

We applied the following procedure on a Windows 2000 server to upgrade Portal server to V5.0.2.1. You can use these steps as a reference.

1. Download and install the WebSphere Application Server Update Installer from the following Web address:

<http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&uid=swg24001908>

To install the Update Installer tool, create a directory in the file system. Then, download the zipped file and extract the files to that directory. (Java 1.3.1 should be accessible.) Figure 2-10 shows the contents of the directory.

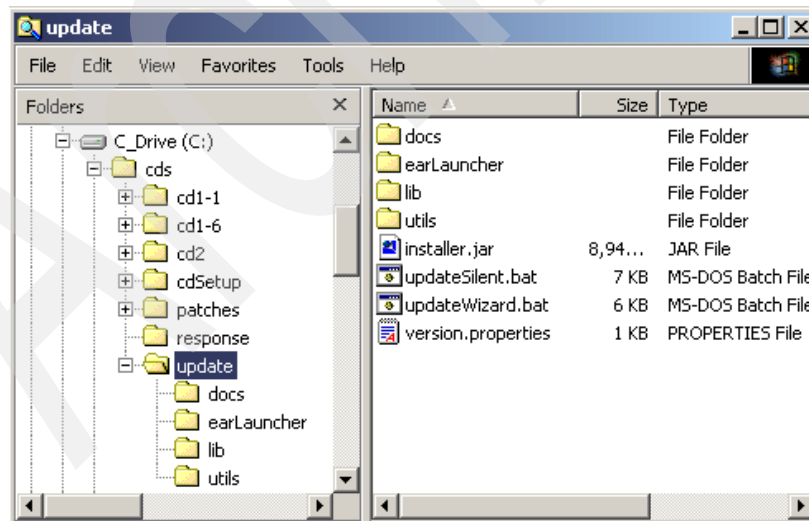


Figure 2-10 Update Installer extracted files

To configure the environment variables and launch the Update tools, run the WebSphere setup script. Example 2-3 shows the Windows example of this script.

Example 2-3 Windows example of setup script

```
C:\> C:\WebSphere\AppServer\bin\setupCmdLine
C:\> java -version
java version "1.3.1"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.3.1)
Classic VM (build 1.3.1, J2RE 1.3.1 IBM Windows 32 build cn131-20030618 (JIT
enabled: jitc))
```

2. Obtain the required WebSphere Application Server and Portal fixpacks and fixes.

WebSphere fixpacks and fixes do not require a specific directory in the WebSphere path installation for you to download the zipped file and extract the files. For single fixes updates, you can create an update directory under the WebSphere home directory. However, when handling multiples fixes and fixpacks, we recommend that you create a new directory structure. Then, extract the fixes into separate individual directories. Figure 2-11 shows the directory structure that we created for the fixes used in this procedure.

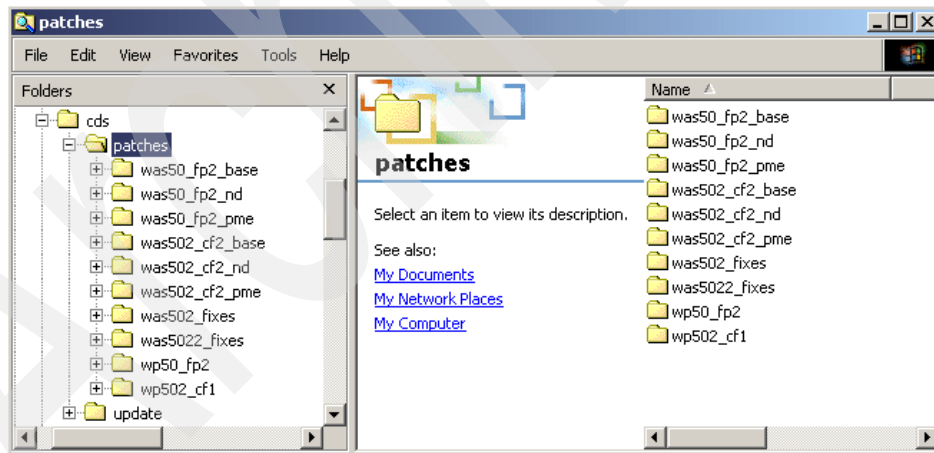


Figure 2-11 Fixpacks and fixes download directory structure

Table 2-4 on page 46 provides the links to the WebSphere Application Server download pages where the required fixpacks and fixes are available. The WebSphere Portal download pages are listed in the beginning of this section in “Step 5. Applying fixpacks and fixes” on page 42.

Table 2-4 WebSphere Application Server Base, PME, and Network Deployment fixpacks and fixes

Fixpacks and fixes	Download page and path
WebSphere Application Server V5.0 fp2 (Base/Network Deployment)	http://www-1.ibm.com/support/docview.wss?rs=180&tc=SSEQTP&uid=swg24005012 Download the zipped file and extract the contents to the c:\cds\patches\was50_fp2_base directory and to the c:\cds\patches\was50_fp2_nd directory.
WebSphere Application Server V5.0 fp2 (PME)	http://www-1.ibm.com/support/docview.wss?rs=823&context=SS4QY3&q1=fixpack&uid=swg24005055&loc=en_US&cs=utf-8&lang=en Download the zipped file and extract the contents to the c:\cds\patches\was50_fp2_pme directory.
WebSphere Application Server V5.0.2 fixes required by WebSphere Portal V5.0.2	http://www-1.ibm.com/support/docview.wss?rs=688&context=SSHRKX&q1=5.0.2&uid=swg24006343&loc=en_US&cs=utf-8&lang=en Download the zipped file and extract the contents to the c:\cds\patches\was502_fixes directory.
Note: These three fixpacks and fixes are also available on CDs 1-17 and 1-18 of the WebSphere Portal V5.0.2 bundle.	
WebSphere Application Server V5.0.2 cumulative fix 2 (Base/ND)	http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&q1=5.0.2+Cumulative+fix+2&uid=swg24005952&loc=en_US&cs=utf-8&lang=en Download the zipped file and extract the contents to the c:\cds\patches\was502_cf2_base directory and to the c:\cds\patches\was502_cf2_nd directory.
WebSphere Application Server V5.0.2 Cumulative fix 2 (PME)	http://www-1.ibm.com/support/docview.wss?rs=823&context=SS4QY3&uid=swg24005954 Download the zipped file and extract the contents to the c:\cds\patches\was502_cf2_pme directory.

Fixpacks and fixes	Download page and path
WebSphere Application Server V5.0.2.2 fixes required by WebSphere Portal V5.0.2.1	<p>Look for the WebSphere Portal V5.0.2.1 installation instructions to obtain the list of required fixes for WebSphere Application Server V5.0.2.2 at the following Web address:</p> <p>http://publib.boulder.ibm.com/pvc/wp/5021/ent/en/readme/install.html</p> <p>Download the fixes from the WebSphere Application Server support page:</p> <p>http://www-306.ibm.com/software/webservers/appserv/was/support/</p> <p>Download the zipped file and extract the contents to the c:\cds\patches\was5022_fixes directory.</p>
WebSphere Portal V5.0 Fix pack 2	<p>http://www-1.ibm.com/support/docview.wss?rs=688&context=SSHRKX&q1=5.0.2&uid=swg24006309&loc=en_US&cs=utf-8&lang=en</p> <p>Download the zipped file and extract the contents to the c:\cds\patches\wp50_fp2 directory.</p>
WebSphere Portal V5.0.2 Cumulative fix 1	<p>http://www-1.ibm.com/support/docview.wss?rs=688&context=SSHRKX&q1=5.0.2.1&uid=swg24006865&loc=en_US&cs=utf-8&lang=en</p> <p>Download the zipped file and extract the contents to the c:\cds\patches\wp502_cf1 directory.</p>
WebSphere Portal V5.0 - Portal Update Installer	<p>http://www-1.ibm.com/support/docview.wss?rs=688&context=SSHRKX&q1=PortalUpdateInstaller&uid=swg24005565&loc=en_US&cs=utf-8&lang=en</p> <p>Download the zipped file and extract the contents to the c:\cds\patches\wp502_cf1 directory.</p>

After downloading the zipped files and extracting all patch files, move to the directory where you installed the Update Installer tool:

```
C:\> cd \cds\update
C:\cds\update> \WebSphere\AppServer\bin\setupCmdLine
```

You should use the silent installation mode of the Update Installer tools (UpdateSilent.bat) to apply fixpacks and fixes. This tool is a simple command-line interface that you can use to install, uninstall, and list

WebSphere fixpacks and fixes. For more information about the syntax of UpdateSilent.bat, see:

ftp://ftp.software.ibm.com/software/websphere/appserv/support/tools/UpdateInstaller/readme_updateinstaller.html

3. Run the following commands to upgrade WebSphere Portal V5.0.0 to V5.0.2.
 - a. Upgrade WebSphere Application Server V5.0.1 to V5.0.2 by following these steps:
 - i. Review the WebSphere Application Server V5.0 installed fixes. Use the command listed in Example 2-4.

Example 2-4 Review installed fixes for WebSphere Application Server V5.0

```
C:\cds\update> updateSilent -fix -installDir C:\WebSphere\AppServer
```

```
Start of [ updatesilent ]
```

```
Verifying installer jar:  
[ installer.jar ]
```

```
222 File(s) copied  
Set encoding: console  
Copyright (c) IBM Corporation 2002; All rights reserved.  
WebSphere Application Server Version 5  
Jun 2, 2004  
Update Installer Version 5.0, Dated Jun 2, 2004
```

```
Fix update specified  
Target product directory: c:\WebSphere\AppServer  
Listing installed fixes:  
Fix name: PQ73644  
Fix name: PQ76567  
Fix name: WAS_CM_08-12-2003_5.0.2-5.0.1_cumulative_Fix  
Fix name: WAS_Dynacache_05-08-2003_5.0.1_cumulative_fix
```

```
End of [ updatesilent ]
```

- ii. Remove the WebSphere Application Server V5.0 currently installed fixes using the following command:

```
C:\cds\update> updateSilent -fix -installDir c:\WebSphere\AppServer  
-uninstall -fixes PQ73644 PQ76567  
WAS_CM_08-12-2003_5.0.2-5.0.1_cumulative_Fix  
WAS_Dynacache_05-08-2003_5.0.1_cumulative_fix
```

- iii. Verify that the fixes were successfully removed using the following command:

```
C:\cds\update> updateSilent -fix -installDir C:\WebSphere\AppServer
```

- iv. Install WebSphere Application Server Base V5.0 Fixpack 2 using the following command:

```
C:\cds\update> updateSilent -fixpack -installDir  
C:\WebSphere\AppServer -fixpackDir  
c:\cds\patches\was50_fp2_base\fixpacks -install -fixpackID  
was50_fp2_win -skipIHS -skipMQ
```

Note: This step can take several minutes to finish.

- v. Verify that Fixpack 2 (Base) was successfully installed using this command:

```
C:\cds\update> \WebSphere\AppServer\bin\versionInfo
```

The output of this command should list the following item:

Installed Product

```
-----  
Name           IBM WebSphere Application Server  
Version        5.0.2  
ID             BASE  
Build Level    ptf2M0325.01  
Build Date     06/23/2003
```

- vi. Install WebSphere Application Server PME V5.0 Fixpack 2 using the following commands:

```
C:\cds\update> updateSilent -fixpack -installDir  
C:\WebSphere\AppServer -fixpackDir  
c:\cds\patches\was50_fp2_pme\fixpacks -install -fixpackID  
was50_pme_fp2_win -skipIHS -skipMQ
```

- vii. Verify that Fixpack 2 (PME) was successfully installed using this command:

```
C:\cds\update> \WebSphere\AppServer\bin\versionInfo
```

The output of this command should list the following item:

Installed Product

```
-----  
Name           IBM WebSphere Application Server Enterprise  
Version        5.0.2  
ID             PME  
Build Level    ptf20327.03  
Build Date     07/10/2003
```

- viii. Install the WebSphere Application Server fixes that are required by WebSphere Portal V5.0.2 using the command listed in Example 2-5.

Example 2-5 Command to install the WebSphere Application Server fixes

```
C:\cds\update> updateSilent -fix -installDir "C:\WebSphere\AppServer" -fixDir
"C:\cds\patches\was502_fixes\efixes" -install -fixes PQ75469 PQ76567 PQ77008
PQ77142 PQ78166 PQ78370 PQ78382 PQ78882 PQ79083 PQ79193 PQ81020_5.0.2_Fix
PQ81248 WAS_Adapter_10-30-2003_5.0.2_cumulative_Fix
WAS_CM_08-12-2003_5.0.2-5.0.1_cumulative_Fix
WAS_Security_07-07-2003_5.0.2-5.0.1-5.0.0_JSSE_cumulative_Fix
WAS_Sessions_08-12-2003_5.0.2_cumulative_Fix
```

- ix. Verify the fixes were successfully installed using this command:

```
C:\cds\update> updateSilent -fix -installDir C:\WebSphere\AppServer
```

Tip: In the **Updatesilent** command, the **-fixes** parameter must be followed by a list of the fixes to be installed. The fix name can be identified by reviewing the contents of each fix .jar file. Look for the efixes subdirectory contained in each fix .jar file. The fixname to be used with Updatesilent is the *PQxxxxx* subdirectory located under the efixes directory.

The output of this command should list all 15 fixes installed during the previous step.

Note: Portal V5.0 Fixpack 2 installation instructions lists 16 WebSphere V5.0.2 fixes as pre-requisites. The cumulative plug-in fix is mandatory only when the Portal server is also hosting a Web server as well as the WebSphere plug-in.

- b. Install WebSphere Portal Fixpack 2 by running the following command:

```
C:\cds\update> cd \cds\patches\wp50_fp2
C:\cds\patches\wp50_fp2> updatePortal -fixpack -installDir
"C:\WebSphere\PortalServer" -fixpackDir "C:\cds\patches\wp50_fp2"
-install -fixpackID WP_PTF_502
```

Assure that no Java process is currently running and that the minimum required storage is available. For information about storage requirements, see:

[http://publib.boulder.ibm.com/pvc/wp/502/ent/en/readme/
install_win_unix.html](http://publib.boulder.ibm.com/pvc/wp/502/ent/en/readme/install_win_unix.html)

Note: This step can take several minutes to finish. Wait until a successful installation message appears.

- c. Run the WebSphere Portal V5.0.2 configuration task using this command:

```
C:\cds\patches\wp50_fp2> cd \WebSphere\PortalServer\config
C:\WebSphere\PortalServer\config> WPSconfig WP-PTF-502
-DPortalAdminPwd=itso
```

Note: This step can take several minutes to finish. Wait until the BUILD SUCCESSFUL message appears.

- d. Validate the WebSphere Portal V5.0.2 installation.

You can review the successful installation of WebSphere Portal V5.0.2 by loading the portal home page (for example, <http://ka0klfr.itso.ral.ibm.com:9081/wps/portal>).

- e. Stop the WebSphere Portal server and server1 application servers using the following commands:

```
C:\WebSphere\PortalServer\config> cd \WebSphere\AppServer\bin
C:\WebSphere\AppServer\bin> stopServer server1
C:\WebSphere\AppServer\bin> stopServer WebSphere_Portal
```

4. Run the following commands to upgrade WebSphere Portal V5.0.2 to V5.0.2.1:

- a. Upgrade WebSphere Application Server V5.0.2 to V5.0.2.2.

- i. Review the WebSphere Application Server V5.0.2 installed fixes. Use the command listed in Example 2-6.

Example 2-6 Review installed fixes for WebSphere Application Server V5.0.2

```
C:\cds\update> updateSilent -fix -installDir C:\WebSphere\AppServer
Start of [ updateSilent ]
```

```
Verifying installer jar:
[ installer.jar ]
```

```
Set encoding: console
Copyright (c) IBM Corporation 2002; All rights reserved.
WebSphere Application Server Version 5
Jun 2, 2004
Update Installer Version 5.0, Dated Jun 2, 2004
```

```
Fix update specified
Target product directory: c:\WebSphere\AppServer
Listing installed fixes:
```

Fix name: PQ75469
Fix name: PQ76567
Fix name: PQ77008
Fix name: PQ77142
Fix name: PQ78166
Fix name: PQ78370
Fix name: PQ78382
Fix name: PQ78882
Fix name: PQ79083
Fix name: PQ79193
Fix name: PQ81020_5.0.2_Fix
Fix name: PQ81248
Fix name: WAS_Adapter_10-30-2003_5.0.2_cumulative_Fix
Fix name: WAS_CM_08-12-2003_5.0.2-5.0.1_cumulative_Fix
Fix name: WAS_Security_07-07-2003_5.0.2-5.0.1-5.0.0_JSSE_cumulative_Fix
Fix name: WAS_Sessions_08-12-2003_5.0.2_cumulative_Fix

- ii. Remove the WebSphere Application Server V5.0.2 currently installed efices using the following command:

```
C:\cds\update> updateSilent -fix -installDir "C:\WebSphere\AppServer"  
-uninstall -fixes PQ75469 PQ76567 PQ77008 PQ77142 PQ78166 PQ78370  
PQ78382 PQ78882 PQ79083 PQ79193 PQ81020_5.0.2_Fix PQ81248  
WAS_Adapter_10-30-2003_5.0.2_cumulative_Fix  
WAS_CM_08-12-2003_5.0.2-5.0.1_cumulative_Fix  
WAS_Security_07-07-2003_5.0.2-5.0.1-5.0.0_JSSE_cumulative_Fix  
WAS_Sessions_08-12-2003_5.0.2_cumulative_Fix
```

- iii. Verify that the fixes were successfully removed using this command:

```
C:\cds\update> updateSilent -fix -installDir C:\WebSphere\AppServer
```

- iv. Install WebSphere Application Server Base V5.0.2 cumulative fix 2 using the following commands:

```
C:\cds\update> updateSilent -fixpack -installDir  
C:\WebSphere\AppServer -fixpackDir  
c:\cds\patches\was502_cf2_base\fixpacks -install -fixpackID  
was502_cf2_win -skipIHS -skipMQ
```

Note: This step can take several minutes to finish.

- v. Verify that Fixpack 2 (Base) was successfully installed using this command:

```
C:\cds\update> \WebSphere\AppServer\bin\versionInfo
```

The output of this command should list the following item:

Installed Product

```
-----  
Name           IBM WebSphere Application Server  
Version        5.0.2.2  
ID             BASE  
Build Level    cf20347.01  
Build Date     11/23/2003
```

- vi. Install WebSphere Application Server PME V5.0.2 cumulative fix 2 using the following commands:

```
C:\cds\update> updateSilent -fixpack -installDir  
C:\WebSphere\AppServer -fixpackDir  
C:\cds\patches\was502_cf2_pme\CumulativeFixes -install -fixpackID  
was502_pme_cf2_win -skipIHS -skipMQ
```

- vii. Verify that cumulative fix 2 (PME) was successfully installed using this command:

```
C:\cds\update> \WebSphere\AppServer\bin\versionInfo
```

The output of this command should list the following item:

Installed Product

```
-----  
Name           IBM WebSphere Application Server Enterprise  
Version        5.0.2.2  
ID             PME  
Build Level    cf20348.01  
Build Date     12/02/2003
```

- viii. Install the WebSphere Application Server efixes that are required by WebSphere Portal V5.0.2.1 using the commands listed in Example 2-7.

Example 2-7 Command to install the WebSphere Application Server efixes

```
C:\cds\update> updateSilent -fix -installDir "C:\WebSphere\AppServer" -fixDir  
"C:\cds\patches\was5022_fixes\efixes" -install -fixes PQ78370 PQ78882  
PQ81020_5.0.2_Fix PQ81248 PQ81416 WAS_Adapter_10-30-2003_5.0.2_cumulative_Fix  
WAS_CM_08-12-2003_5.0.2-5.0.1_cumulative_Fix  
WAS_Dynacache_01-30-2004_5.0.2_cumulative_fix  
WAS_Security_12-13-2003_5.0.2.3-5.0.2.2-5.0.2.1-5.0.2-5.0.1-5.0.0_JSSE_cumulati  
ve_Fix
```

ix. Verify that the fixes were successfully installed using this command.

```
C:\cds\update> updateSilent -fix -installDir C:\WebSphere\AppServer
```

The output of this command should list all nine fixes installed on the previous step.

b. Install WebSphere Portal cumulative fix 1 by running the following commands:

```
C:\cds\update> cd \cds\patches\wp502_cf1
C:\cds\patches\wp502_cf1> updatePortal -fixpack -installDir
"C:\WebSphere\PortalServer" -fixpackDir "C:\cds\patches\wp502_cf1"
-install -fixpackID WP_PTF_5021
```

Assure that no Java process is currently running and that the minimum required storage is available. For information about storage requirements, see:

<http://publib.boulder.ibm.com/pvc/wp/5021/ent/en/readme/install.html>

Note: This step can take several minutes to finish. Wait until a successful installation message appears.

c. Run the WebSphere Portal V5.0.2.1 configuration task using the following commands:

```
C:\cds\patches\wp502_cf1> cd \WebSphere\PortalServer\config
C:\WebSphere\PortalServer\config> WPSconfig WP-PTF-5021
-DPortalAdminPwd=itso
```

Note: This step can take several minutes to finish. Wait until the BUILD SUCCESSFUL message appears.

d. Validate the WebSphere Portal V5.0.2.1 installation.

You can review the successful installation of WebSphere Portal V5.0.2.1 by loading the Portal home page (for example, <http://ka0klfr.itso.ral.ibm.com:9081/wps/portal>).

e. Stop the WebSphere Portal server and server1 application servers using the following commands:

```
C:\WebSphere\PortalServer\config> cd \WebSphere\AppServer\bin
C:\WebSphere\AppServer\bin> stopServer server1
C:\WebSphere\AppServer\bin> stopServer WebSphere_Portal
```

The following auxiliary technotes explain several common issues regarding WebSphere Application Server Base, Programming Model Extensions, and Portal fixes:

- ▶ Technote 1145289, *Cumulative Fix Strategy for WebSphere Application Server V5.0 and V5.1*
http://www-1.ibm.com/support/docview.wss?rs=860&context=SW600&q1=fix+strategy&uid=swg21145289&loc=en_US&cs=utf-8&lang=en
- ▶ Technote 1162831, *Cumulative fix compatibility between Base and Network Deployment Editions, and Enterprise Edition*
http://www-1.ibm.com/support/docview.wss?rs=860&context=SW600&q1=fix+strategy&uid=swg21162831&loc=en_US&cs=utf-8&lang=en
- ▶ Technote 1173471, *Clarification on the WebSphere Portal version 5.0.2.1 installation*
http://www-1.ibm.com/support/docview.wss?rs=688&context=SSHRKX&q1=clarification&uid=swg21173471&loc=en_US&cs=utf-8&lang=en
- ▶ Technote 1140712, *Installing WebSphere Application Server V5.0 Enterprise Edition_FAQ*
<http://www-1.ibm.com/support/docview.wss?uid=swg21140712>

Fixpacks and fixes for WebSphere Network Deployment Server

To install fixpacks and fixes for WebSphere Network Deployment Server:

1. Download and install the WebSphere Application Server Update Installer from the following Web address:

<http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&uid=swg24001908>

To install the Update Installer tool, create a directory in the file system. Then, download the zipped file and extract the files to that directory. (Java 1.3.1 should be accessible.)

To configure the environment variables and launch the Update tools, run the WebSphere setup script.

2. Obtain the required WebSphere Application Server and Portal fixpacks and fixes.

See Table 2-4 on page 46 for the Web pages where you can download fixes. Download only the following fixes and use the same suggested download directory path names that appear in Table 2-4 on page 46:

- WebSphere Application Server V5.0 fp2 (Base/ND)
- WebSphere Application Server V5.0 fp2 (PME)
- WebSphere Application Server V5.0.2 cumulative fix 2 (Base/ND)
- WebSphere Application Server V5.0.2 cumulative fix 2 (PME)

WebSphere fixpacks and fixes do not require a specific directory in the WebSphere path installation for you to download the zipped file and extract the files. For single fixes updates, you can create an update directory under the WebSphere home directory. However, when handling multiples fixes and fixpacks, we recommend that you create a new directory structure. Then, extract the fixes into separate individual directories.

After you download the fixpacks and fixes, continue the installation of WebSphere Network Deployment Fixpack by following these steps:

1. Upgrade WebSphere Network Deployment V5.0 to V5.0.2.

a. Install Fixpack 2 by running the following commands:

```
C:\cds\update> updateSilent -fixpack -installDir
C:\WebSphere\DeploymentManager -fixpackDir
C:\cds\patches\was50_fp2_nd\fixpacks -install -fixpackID
was50_nd_fp2_win -skipIHS -skipMQ
```

Note: This step can take several minutes to finish.

b. Verify that Fixpack 2 (Network Deployment) was successfully installed by running the command in Example 2-8.

Example 2-8 Fixpack 2 commands

```
C:\cds\update> \WebSphere\DeploymentManager\bin\versionInfo
The output of this command should list the following item:
Installed Product
```

```
-----
Name          IBM WebSphere Application Server for Network Deployment
Version       5.0.2
ID            ND
```

c. Install WebSphere Network Deployment PME V5.0 Fixpack 2 using the following commands:

```
C:\cds\update> updateSilent -fixpack -installDir
C:\WebSphere\DeploymentManager -fixpackDir
C:\cds\patches\was50_fp2_pme\fixpacks -install -fixpackID
was50_pme_nd_fp2_win -skipIHS -skipMQ
```

- d. Verify that Fixpack 2 (PME) was successfully installed by running the command in Example 2-9:

Example 2-9 Successful installation command

```
C:\cds\update> \WebSphere\AppServer\bin\versionInfo
The output of this command should list the following item :
Installed Product
-----

Name          IBM WebSphere Application Server Enterprise
Version       5.0.2
ID            PME
```

2. Upgrade WebSphere Network Deployment V5.0.2 to V5.0.2.2.

- a. Install cumulative fix 2 using the following commands:

```
C:\cds\update> updateSilent -fixpack -installDir
C:\WebSphere\DeploymentManager -fixpackDir
C:\cds\patches\was502_cf2_nd\fixpacks -install -fixpackID
was50_nd_cf2_win -skipIHS -skipMQ
```

Note: This step can take several minutes to finish.

- b. Verify that cumulative fix2 (Network Deployment) was successfully installed by running the command in Example 2-10.

Example 2-10 Cumulative fix2 verification command

```
C:\cds\update> \WebSphere\DeploymentManager\bin\versionInfo
The output of this command should list the following item:
Installed Product
-----

Name          IBM WebSphere Application Server for Deployment Manager
Version       5.0.2.2
ID            ND
```

- c. Install WebSphere Application Server PME V5.0.2 cumulative fix using this command:

```
C:\cds\update> updateSilent -fixpack -installDir C:\WebSphere\AppServer
-fixpackDir c:\cds\patches\was502_cf2_pme\CumulativeFixes -install
-fixpackID was502_pme_nd_cf2_win -skipIHS -skipMQ
```

- d. Verify that cumulative fix 2 (PME) was successfully installed by running the command in Example 2-11.

Example 2-11

```
C:\cds\update> \WebSphere\DeploymentManager\bin\versionInfo
```

The output of this command should list the following item:

Installed Product

```
-----  
Name           IBM WebSphere Application Server Enterprise  
Version        5.0.2.2  
ID             PME
```

Fixpacks and fixes for Web servers

Web servers must also be upgraded to V5.0.2.2 level as well.

To install fixpacks and fixes for WebSphere Network Deployment Server:

1. Download and install the WebSphere Application Server Update Installer from the following Web address:

<http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&uid=swg24001908>

To install the Update Installer tool, create a directory in the file system. Then, download the zipped file and extract the files to that directory. (Java 1.3.1 should be accessible.)

To configure the environment variables and launch the Update tools, run the WebSphere setup script.

2. Obtain the required WebSphere Application Server and Portal fixpacks and fixes.

See Table 2-4 on page 46 for the Web pages where you can download fixes. Download only the following fixes and use the same suggested download directory path names that appear in Table 2-4 on page 46:

- WebSphere Application Server V5.0 fp2 (base)
- WebSphere Application Server V5.0.2 cumulative fix 2 (base)
- WebSphere Application Server V5.0.2.2 fixes required by WebSphere Portal V5.0.2.1
- efix, WebSphere Plug-in cumulative fix for V5.0.0, V5.0.1, and V5.0.2

WebSphere fixpacks and fixes do not require a specific directory in the WebSphere path installation for you to download the zipped file and extract the files. For single fixes updates, you can create an update directory under the WebSphere home directory. However, when handling multiples fixes and

fixpacks, we recommend that you create a new directory structure. Then, extract the fixes into separate individual directories.

3. Stop the HTTP Web server and HTTP administrative service.
4. Install Fixpack 2 using the following command:

```
C:\cds\update> updateSilent -fixpack -installDir C:\WebSphere\AppServer  
-fixpackDir c:\cds\patches\was50_fp2_base\fixpacks -install -fixpackID  
was50_fp2_win -skipMQ
```

Note: This step can take several minutes to finish.

5. Install cumulative fix 2 using the following command:

```
C:\cds\update> updateSilent -fixpack -installDir C:\WebSphere\AppServer  
-fixpackDir c:\cds\patches\was502_cf2_base\fixpacks -install -fixpackID  
was502_cf2_win -skipMQ
```

Note: This step can take several minutes to finish.

6. Install the plug-in cumulative efix by following these steps:
 - a. Make a backup copy of the WebSphere Application Server bin directory:
c:\WebSphere\AppServer\bin
 - b. Extract the efix zipped file to the WebSphere Application Server bin directory.
 - c. Restart Web server.
7. Verify that the installation was successful by reviewing the log file, c:\WebSphere\AppServer\logs\http_plugin.log. The following messages should appear in the log file:

```
Plug-ins loaded  
Bld Date: Feb 3 2004, 10:03:18
```

Note: The build date may vary depending on the version of the cumulative fix that you installed.

Step 6. Installing the back-end servers

Two kinds of back-end servers are most commonly used in production systems: database and LDAP servers. Because Cloudscape™ is not supported for production, you need to install a more robust database server. The options that we considered for this book were DB2 UDB Enterprise and Oracle Enterprise Server. For the LDAP service, we chose IBM Directory Server and Sun ONE Directory Server.

For details on the installation and integration procedure for the back-end servers, see the WebSphere Portal InfoCenter links listed in Table 2-5.

Table 2-5 WebSphere Portal InfoCenter links

Section	Link
Installing → Database	http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/wpf/intr_ldap.html
Installing → LDAP	http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/wpf/intr_db.html

Note: For cluster environments, the database configuration task is not the same for all Portal nodes. Review the following documents before you integrate the Portal nodes to the same database instance:

- ▶ *IBM WebSphere Portal for Multiplatforms V5 Handbook*, Chapter 7
<http://www.redbooks.ibm.com/abstracts/sg246098.html>
- ▶ *A step-by-step guide to configuring a WebSphere Portal V5 cluster, a Developer Domain* article
http://www-106.ibm.com/developerworks/websphere/library/techarticles/0401_1amb/1amb2.html

Verifying prerequisites

After the installation of the LDAP server, verify the LDAP service and the creation of Portal users by running an LDAP client tool such as `ldapsearch`. The expected output will be similar to the example in Example 2-12.

Example 2-12 Verification of LDAP service and Portal users creation

```
C:\Documents and Settings\Administrator>ldapsearch -h ldap.redbook.ibm.com -D
uid=wpsadmin,cn=users,ou=aixcluster,o=redbook -w itso -b
ou=aixcluster,o=redbook "uid=wpsadmin"
```

```
uid=wpsadmin,cn=users,ou=aixcluster,o=redbook
givenName=wps
uid=wpsadmin
objectclass=inetOrgPerson
objectclass=organizationalPerson
objectclass=person
objectclass=top
objectclass=ibm-appuuidaux
sn=admin
cn=wps admin
ibm-appuuid=694df9c0-e6fa-11d8-8441-829741125cb3
```

```
C:\Documents and Settings\Administrator>ldapsearch -h ldap.redbook.ibm.com -D
uid=wpsadmin,cn=users,ou=aixcluster,o=redbook -w itso -b
ou=aixcluster,o=redbook "cn=wpsadmins"
```

```
cn=wpsadmins,cn=groups,ou=aixcluster,o=redbook
objectclass=groupOfUniqueNames
objectclass=top
cn=wpsadmins
uniquemember=uid=wpsadmin,cn=users,ou=aixcluster,o=redbook
```

You can verify the database server infrastructure from the Portal server machine only if the DBA has installed a client tool. (A client tool is mandatory for DB2 but not for Oracle.)

You can review the DB2 server using the DB2 commands shown in Example 2-13:

Example 2-13 Verification of DB2 configuration

```
AIX Version 5
(C) Copyrights by IBM and by others 1982, 2002.
login: root
root's Password:
*****
*                                                                 *
*                                                                 *
* Welcome to AIX Version 5.2!                                   *
*                                                                 *
*                                                                 *
* Please see the README file in /usr/lpp/bos for information pertinent to *
* this release of the AIX Operating System.                     *
*                                                                 *
*                                                                 *
*****
Last unsuccessful login: Sat Aug 14 15:36:58 EDT 2004 on /dev/pts/7 from
freddolaptop.itso.ral.ibm.com
Last login: Wed Aug 18 11:12:07 EDT 2004 on /dev/pts/0 from
ka0klfr.itso.ral.ibm.com

# su - db2inst1
$ db2 list node directory

Node Directory

Number of entries in the directory = 1

Node 1 entry:
```

Node name	= PORTNODE
Comment	=
Directory entry type	= LOCAL
Protocol	= TCPIP
Hostname	= db.redbook.ibm.com
Service name	= db2c_DB2

\$ db2 list database directory

System Database Directory

Number of entries in the directory = 3

Database 1 entry:

Database alias	= WPCP50
Database name	= WCP502DB
Node name	= PORTNODE
Database release level	= a.00
Comment	=
Directory entry type	= Remote
Catalog database partition number	= -1

Database 2 entry:

Database alias	= FDBK50
Database name	= FDK502DB
Node name	= PORTNODE
Database release level	= a.00
Comment	=
Directory entry type	= Remote
Catalog database partition number	= -1

Database 3 entry:

Database alias	= WPS50
Database name	= WP502DB
Node name	= PORTNODE
Database release level	= a.00
Comment	=
Directory entry type	= Remote
Catalog database partition number	= -1

Step 7. Creating and configuring the Portal clusters

We used the following installation document for the Portal cluster configuration:

http://www-106.ibm.com/developerworks/websphere/library/techarticles/0401_lamb/lamb2.html

Important: After installation, during verification testing, we identified a multicast error. A fix for this error is available at:

<http://www-1.ibm.com/support/docview.wss?rs=688&uid=swg21167496>

You must apply this fix on top of WebSphere Application Server V5.0.2.2 in all Portal nodes.

2.3 Portal documentation

The following links to Portal documentation that might be useful for Portal administrators running a production Portal deployment:

- ▶ WebSphere Portal InfoCenter, main documentation page for WebSphere Portal V5
<http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/index.html>
- ▶ *IBM WebSphere Portal for Multiplatforms V5 Handbook*, portal installation redbook
<http://www.redbooks.ibm.com/abstracts/sg246098.html>
- ▶ *WebSphere Portal Guide*, overview guide of the WebSphere Portal solution
http://www-106.ibm.com/developerworks/websphere/library/techarticles/0310_wendel/wendel.html
- ▶ Portal V5.0.2.1 release notes
http://publib.boulder.ibm.com/pvc/wp/5021/ent/en/release_notes_ent.html
- ▶ Portal V5.0.2 cumulative fix 1
http://publib.boulder.ibm.com/pvc/wp/5021/ent/en/readme/readme_fp5021.html
- ▶ Portal V5.0.2 prerequisites
http://publib.boulder.ibm.com/pvc/wp/5021/ent/en/InfoCenter/wpf/inst_req.html
- ▶ Portal catalog
<http://www.ibm.com/software/genservers/portal/portlet/catalog>

► Developer domain - Portal articles

<http://www-106.ibm.com/developerworks/apps/ViewServlet.wss?viewType=Library&topic=0&count=10&keyword=Portal&prodfam=0&devDomain=wsdd&format=0&sortBy=Posted&start=1&showAll=true>

► Portal tutorial, Web-based course about Portal fundamentals

<http://www-106.ibm.com/developerworks/websphere/library/tutorials/d1/sw741>

► Portal administrative roadmap, Web links to WebSphere Portal InfoCenter sections, Developer Domain article, and WebSphere Portal handbook that are related to installation activities

<http://www-106.ibm.com/developerworks/apps/transform.wss?URL=/developerworks/websphere/zones/portal/roadmaps/portal-roadmaps.xml&xslURL=/developerworks/websphere/xsl/roadmaps.xsl&format=two-column&role=admin-mp#installation>



Security management

This chapter discusses the security items that you should consider and understand about WebSphere Portal.

3.1 Password maintenance

Password maintenance is an important issue regarding production Portal servers. Depending on the active features enabled on your Portal configuration, you might need to consider all the items below on your password revision schedule.

The following sections present an enumeration of credentials (either user-password pairs or electronic certificates) that you might use in your Portal instance as well as a general description and administration procedures for changing passwords and certificates.

3.1.1 Proxy authentication with Content Access Service

Content Access Service is part of the Portlet Service Registry. It is available to portlet developers to establish connections to external content beyond the network firewalls through a proxy server. This service is available for both authenticated and non-authenticated proxy servers. To enable the service, the Portal administrator must update the service configuration properties file and add a credential to the credential vault slot within the Default Vault Segment.

Enabling Content Access Service

You perform the following steps to enable Content Access Service:

1. Move to *WPS install directory\shared\app\config\services* and edit the properties file named *PortletServiceRegistryService.properties*.
2. Update the *proxy.http.** and *proxy.https.** properties with the IP address and port number of the proxy server. (Update https only if SSL support is enabled in the proxy server.)
3. Add *proxy.auth.** properties to the properties file as shown in Example 3-1.

Example 3-1 Updating PortletServiceRegistryService.properties

```
#
# the name of the http proxy host
#
com.ibm.wps.pe.pc.legacy.service.ContentAccessServiceImpl.proxy.http.host=9.42.170.155

#
# the name of the http proxy port
#
com.ibm.wps.pe.pc.legacy.service.ContentAccessServiceImpl.proxy.http.port=3128

com.ibm.wps.pe.pc.legacy.service.ContentAccessServiceImpl.proxy.https.host=9.42.170.155
com.ibm.wps.pe.pc.legacy.service.ContentAccessServiceImpl.proxy.https.port=3128
```

```
com.ibm.wps.pe.pc.legacy.service.ContentAccessServiceImpl.proxy.auth.enabled=true  
com.ibm.wps.pe.pc.legacy.service.ContentAccessServiceImpl.proxy.auth.credentialslot=predefined.  
credential.ContentAccessProxy
```

4. Add a new vault slot to DefaultAdminSegment vault.
Login to Portal with Portal administration user and select **Administration** → **Access** → **Credential Vault**.
5. Add a new vault slot that has the following properties:
 - Vault Slot Name: predefined.credential.ContentAccessProxy
 - Vault segment: DefaultAdminSegment
 - Vault Slot: shared
 - Shared Userid: The authentication user in the Proxy Server
 - Shared Password: The password for the authentication user in the Proxy Server
6. Restart the Portal server.

Note: WebClipping portlets do not use Content Access Service. You need to add authentication information to the portlet parameters in the appropriate section.

Updating the Proxy Server user ID and password

When a new user ID and password are required for the Proxy server, you also need to refresh the Portal credentials. To update the credentials for the authentication user, modify the vault slot to update the user ID and password fields. The Content Access Service is available after you restart the Portal server.

3.1.2 Changing the Portal database username and password

Quite often when deploying Portal as a proof of concept or as a limited production roll out, the user names and passwords chosen may not conform to existing security guidelines. If you have already deployed your Portal environment and your security or database specialists tell you that you need to change your database user name and passwords, you do not need re-install your Portal environment. Instead, follow these steps:

1. Have the database administrator (DBA) create new Portal database user and password and assign the appropriate permissions.
2. Make changes to username and password configuration via the Deployment Manager Administrative Console.

3. Change the entries in the wpconfig.properties file.

The procedure is basically the same for a cluster or a stand alone instance of WebSphere Portal. However, you make changes via the Deployment Manager instead of the WebSphere Application Server Administrative Console if you have deployed a Portal cluster.

Creating a new database user

First, get the DBA to create a new database user with the same rights as the existing Portal user. It is important that the new database user ID is an alias to all the tables that the original user owns, so that the new user can make changes to existing Portal data.

Also, remember to change your database settings on the machine where the Portal is running. Ensure that the database is cataloged locally using the new user ID and that you load the profile of the new database user.

Making changes via the Deployment Manager console

Before making any changes, be sure that you can list the tables of your Portal database via the DB2 command line interface to ensure that the changes have been made correctly. To do so, follow these steps:

1. Login to the Deployment Manager Administrative Console and click **Security** → **JAAS Configuration** → **J2C** → **Authentication Data**.
2. Change the user ID and password for wpsDBAuth to the new user name for the Portal.
3. For the WebSphere Member Manager and WebSphere Portal Content Publishing databases, change the user ID and password for wmmDbAuth, brbDBAuth, and brbDBAuth.
4. Save your changes and logout.

The wpconfig.properties file

Update the wpconfig.properties file with these new entries so that configuration tasks that run in the future will work.

To ensure that you have implemented all the changes correctly, restart the Deployment Manager and the Node Agents as well as the Portal cluster to confirm that the DB2 setting on each of the Portal clones is correct. When the cluster is running, check the logs to ensure that you can make changes to the Portal without generating errors.

3.2 Credential Vault

The Credential Vault is a repository where credentials are stored. Examples of credentials include certificates, private keys, user IDs, and passwords. WebSphere Portal provides a class called `CredentialVaultService` which portlets can use to store and retrieve credentials from the vault.

Many portlets need to access remote applications that require some form of user authentication. For accessing applications outside the Portal's realm, the Portal server provides a Credential Vault service that portlets can use to store the user ID and password for a user to login to an application. Portlets can use these on behalf of the user to access remote systems.

3.2.1 How Credential Vault works

Portlets obtain credentials by obtaining a `CredentialVaultPortletService` object and calling its `getCredential` method. With the returned credential, there are two options:

- ▶ Use passwords or keys from a passive credential, passing them in application-specific calls. Portlets that use passive credentials need to extract the secret out of the credential and do all the authentication communication with the back-end application.
- ▶ Call the `authenticate` method of an active credential. Active credential objects hide the credentials secret from the portlet, with no way to extract it out of the credential. Active credentials provide additional methods to perform the authentication.

3.2.2 Using Credential Vault

This section demonstrates the use of Credential Vault. You access Credential Vault from the WebSphere Portal Administration page as shown in Figure 3-1.

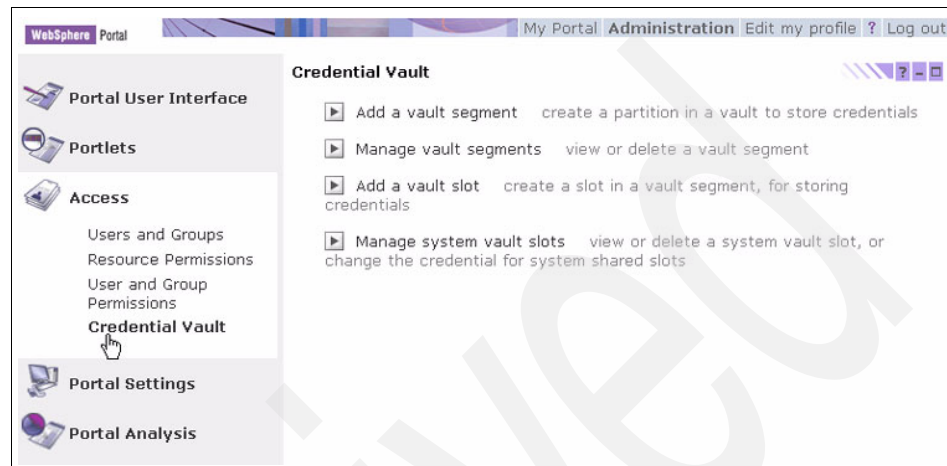


Figure 3-1 WebSphere Portal Administrative window, Credential Vault

Vault segment

The *vault segment* is a partition of a vault. There are two types of segments: user-managed and administrator-managed. Portal administrators can create administrator-managed segments using the Credential Vault tab on the Security page of the Portal Administration page. This tab is called the Credential Vault portlet. WebSphere Portal provides a user-managed segment in the default vault.

Vault slot

The *vault slot* is a part of a vault segment. It is represented using `CredentialSlotConfig` class. Portlets use vault slots to store and retrieve credentials. You can create a vault slot programmatically, in a user-managed segment. An administrator can also create a vault slot in an administrator-managed segment, using the Credential Vault portlet. The portlet can set and get credentials in vault slots created either way. The `CredentialSlotConfig` object contains configuration information about the slot (for example, the slot ID, segment object ID, and other attributes).

The Credential Vault that comes with WebSphere Portal defines four types of vault slots:

- ▶ Portlet private slot
- ▶ Shared slot
- ▶ Administrative slot
- ▶ System slot

You can find good examples of how to use vault slots within portlets at the following Web address:

http://www-106.ibm.com/developerworks/websphere/library/techarticles/0211_konduru/konduru.html

3.3 Surfacing an application

Surfacing an application is still an unsecure procedure once the surfaced application is accessible from outside the Portal.

Most of the time, you have to implement single sign-on with a surfaced application to prevent multiple logins for your users. You cannot make changes to the surfaced application because of security issues.

To surface an application, generally you use an IFrame portlet which calls the application into the Portal interface. Customizing an IFrame portlet for your application, you add the code shown in Example 3-2 to the portlet application to obtain the login data from a Credential Vault.

Example 3-2 Extracting the credentials from the private slot

```
private void getCredential(PortletRequest portletRequest,StringBuffer user ID,
    StringBuffer password) throws PortletServiceException {
    try{
        String slotId = (String) portletRequest.getData().getAttribute
            ("PrivateSlotSamplePortletSlotID");
        if(slotId==null)
            return ;
        UserPasswordPassiveCredential credential =(UserPasswordPassiveCredential)
            vaultService.getCredential
            (slotId, "UserPasswordPassive", new HashMap(), portletRequest);
        userid.append(credential.getUserId() );
        password.append( String.valueOf(credential.getPassword() ) );
    }
    catch(com.ibm.wps.portletservice.credentialvault.
        CredentialSecretNotSetException e){
        return ;
    }
}
```

To transfer this data to the login page of the surfaced application, use the JavaScript shown in Example 3-3 to map the Form and Fields of the target page and to submit the page.

Example 3-3 Mapping the target form in the login page

```
<script language="Java Script">
    myiframe.forms[0].login.value='<%=userID%>';
    myiframe.forms[0].password.value='<%=password%>';
    myiframe.forms[0].submit();
</script>
```

3.4 Managing security

WebSphere Portal provides several features to help administrators manage security within the Portal. Building on top of the WebSphere Application Server security framework, WebSphere Portal delivers multiple authentication mechanisms, such as Single Sign On support, Credential Vault, customized authorization and resource management, and security-related middleware APIs for portlet development. Such features are comprehensive and flexible enough to allow any Portal solution to handle corporate security requirements. Nevertheless, you can expand the built-in security infrastructure for WebSphere Portal and enlarge the scope to include a major enterprise scenario.

When the user requirements lead to an enterprise-wide security solution, integrating not only multiple Web applications but also legacy systems, then consider including an external authentication proxy in your Portal topology. External authentication products such as Tivoli Access Manager (TAM) add value in many aspects. Handling security in a centralized way not only guarantees that the security policy is uniform but also provides additional security services that save time and effort during portlet development. Scalability, accountability, and quality of protection are major issues that you should consider on a security integration solution. External security, the central point for security constraints, enforces the security standards and reduces the administrative effort.

Use the following questions to guide your evaluation of applying for external security infrastructure:

- ▶ Does your Portal provide clients with a unified Web experience by means of flexible single sign on to a number of Web applications?
- ▶ Does your Web applications share consistent and adequate security policies?
- ▶ Can the total cost of security management be clearly calculated for the overall enterprise Web applications scenario?

- ▶ Can your current Portal security settings support high-level customer growth?
- ▶ Can your current Portal security settings provide audit ability features and audit trails for all integrated Web applications?

If you answer a majority of these questions with no, consider a new evaluation on the security infrastructure.

The following resources are available to help you understand and evaluate the benefits and costs of integrating external security solutions to WebSphere Portal:

- ▶ *Integrating WebSphere Portal software with your security infrastructure*
ftp://ftp.software.ibm.com/software/websphere/pdf/WS_Portal_Security_G325-2090-01.pdf
- ▶ WebSphere Portal V5.0 InfoCenter
http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/wp/sec_ext_man.html
- ▶ *Develop and Deploy a Secure Portal Solution Using WebSphere Portal V5 and Tivoli Access Manager V5.1*, SG24-6325
<http://publib-b.boulder.ibm.com/abstracts/sg246325.html?Open>
- ▶ *WebSphere Portal with Tivoli Access Manager: Value Beyond Security*
<http://www-1.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100426>

3.5 Integrating LDAP

This section discusses approaches and considerations pertaining to implementing your Portal into an existing corporate LDAP. Security plays an important role in all WebSphere Portal production environments. Many customers use a central LDAP to manage security for multiple corporate enterprise systems. WebSphere Portal is designed so that you can configure directly into an existing LDAP. However, there are a few considerations that you should plan before integrating your Portal into an existing LDAP. You will need to work closely with the LDAP administrator to plan, design, and architect a solution.

3.5.1 Performance considerations

The items that effect LDAP performance are:

- ▶ The minimum number of LDAP calls made by WebSphere Portal is seven per login. Using nested groups significantly increases the number of calls made.

It is important to know how much overhead will be introduced into your LDAP system once it is integrated. Each login to the Portal will make seven LDAP calls. If the number of users that will access the Portal is large, then you should carefully consider the performance impact of the LDAP. Ideally, you should plan for and load test this set up in a staging environment that mirrors the production environment.

- ▶ LDAPSuffix property

The LDAPSuffix property in the wpconfig.properties file should be the least common dominator for where users and groups that access the Portal are located in the LDAP. This property defines to the Portal what leaf or leaves of the LDAP tree it should searched for users and groups. Of course, the broader the search, the slower the performance.

WebSphere Member Manager performance tips

This section discusses performance tips that apply to WebSphere Member Manager.

Note: To take full advantage of these performance tips if your WebSphere Portal level is lower than WebSphere Portal V5.0.2, you must have applied all the current WebSphere Member Manager fixes. Visit the WebSphere Portal Support site for the most current WebSphere Member Manager fixes:

<http://www-306.ibm.com/software/genservers/portal/support>

Using memberOfAttributeName to improve look up performance

Some LDAP servers support the memberOfAttributeName parameter (also called the groupMembership attribute). For all entries on the LDAP server, there is an attribute which stores the groups to which this entry belongs.

To improve performance for looking up group membership, activate this feature by editing the following parameter in the `wps.root/shared/app/wmm/wmm.xml` directory as shown in Example 3-4:

```
memberOfAttributeName=<The name of the memberOf attribute>"
```

Example 3-4 Editing the `memberOfAttributeName` parameter

```
<ldapRepository name="wmmLDAP"
  UUID="LDAP1"
  adapterClassName="com.ibm.ws.wmm.ldap.activedir.ActiveDirectoryAdapterImpl"
  supportDynamicAttributes="false"
  configurationFile="wmm/xml/wmmLDAPAttributes_AD.xml"
  wmmGenerateExtId="false"
  supportGetPersonByAccountName="true"
  profileRepositoryForGroups="LDAP1"
  supportTransactions="false"
  adminId="CN=db2admin,CN=Users,DC=andydomain,DC=torolab,DC=ibm,DC=com"
  adminPassword="xxxxxxx"
  ldapHost="andyserver.torolab.ibm.com"
  ldapPort="636"
  ldapTimeOut="6000"
  ldapAuthentication="SIMPLE"
  ldapType="0"
  memberOfAttributeName="memberOf"
  java.naming.security.protocol="ssl"
  groupCacheRefreshInterval="-1">
```

The following is a summary of the `memberOfAttributeName` parameters that LDAP servers support:

- ▶ Active Directory: `memberOf`
- ▶ Novell eDirectory: `groupMembership`
- ▶ IBM Directory Server: `ibm-allGroups`
- ▶ Sun ONE Directory Server: `nsroles`

Using `searchFilter` to improve search performance

By default, WebSphere Member Manager uses the object class to formulate the search filter when performing a search. For example, the following `wmm.xml` defines `objectClassesForRead` for *Person* as *user*. When searching for a

particular user, WebSphere Member Manager formulates the filter as (&(cn=*)(objectClass=user)).

```
<supportedLdapEntryType name="Person"
rdnAttrTypes="uid"
objectClassesForRead="user"
objectClassesForWrite="user"
searchBases="cn=groups,dc=yourco,dc=com" />
```

You can add the `searchFilter` parameter to define any filter you want for doing the search. For example, when searching for all users, the search filter becomes (&(cn=*)(objectCategory=Person)) as shown here:

```
<supportedLdapEntryType name="Person"
rdnAttrTypes="uid"
objectClassesForRead="user"
objectClassesForWrite="user"
searchBases="cn=users,dc=yourco,dc=com"
searchFilter="(ObjectCategory=Person)" />
```

You can apply the method to group and other member types, as shown here:

```
<supportedLdapEntryType name="Group"
rdnAttrTypes="cn"
objectClassesForRead="group"
objectClassesForWrite="group"
searchBases="cn=groups,dc=yourco,dc=com"
searchFilter="(ObjectCategory=Group)" />
```

For Active Directory server, use the `objectClass` and `objectCategory` parameters in the following scenarios:

- ▶ Note that `objectCategory` is indexed but `objectClass` is not. So, using `objectCategory` to do searching is faster than using `objectClass`.
- ▶ Users and computers share the same object class *user* (*computer* objectClass extends from *user* objectClass). Using the default filter, such as (&(cn=*)(objectClass=user)) returns both users and computers. To only return users, define a *userFilter* such as (&(cn=*)(objectCategory=Person)).

You can configure WebSphere Member Manager to search using `objectCategory` in `wmm.xml`, as shown here:

```
<supportedLdapEntryType name="Person"
rdnAttrTypes="uid"
objectClassesForRead="user"
objectClassesForWrite="user"
searchBases="cn=users,dc=yourco,dc=com"
searchFilter="(ObjectCategory=Person)" />
```

You can apply the method to group and other member types, as shown here:

```
<supportedLdapEntryType name="Group"
rdnAttrTypes="cn"
objectClassesForRead="group"
objectClassesForWrite="group"
searchBases="cn=groups,dc=yourco,dc=com"
searchFilter="(ObjectCategory=Group)"/>
```

Using searchBases to improve search performance

WebSphere Member Manager always searches under all nodes defined under the nodeMaps tag in the wmm.xml file to find users or groups. With the appropriate level of wmm.xml applied, you can define a smaller search base for a member type to improve search performance.

For example, if all of your groups are under a particular parent (such as cn=groups,dc=yourco,dc=com), you can define search bases for group by using the searchBases parameter as shown in the following:

```
<supportedLdapEntryType name="Group"
rdnAttrTypes="cn"
objectClassesForRead="groupOfNames"
objectClassesForWrite="groupOfNames"
searchBases="cn=groups,dc=yourco,dc=com"/>
```

With this parameter, when WebSphere Member Manager looks up groups, it only searches under cn=groups,dc=yourco,dc=com instead of dc=yourco,dc=com.

Multiple search bases are separated by semicolon (;), as in the following:

```
<supportedLdapEntryType name="Group"
rdnAttrTypes="cn"
objectClassesForRead="groupOfNames"
objectClassesForWrite="groupOfNames"
searchBases="cn=users1,dc=yourco,dc=com;cn=users2,dc=yourco,dc=com"/>
```

Using LDAP connection pool to improve performance

By default, WebSphere Member Manager creates one LDAP connection (JNDI dirContext). It reuses this connection for all LDAP operations. If you expect several users to be logging into the Portal concurrently, you can setup connection pooling to improve performance.

To enable connection pooling, you need to set `dirContextsMaxSize` to a value larger than 0. There are three parameters to control the connection:

- ▶ `dirContextsMaxSize`

The maximum number of live connections. If there is no available connection in the pool when a request is submitted, the request waits the number of milliseconds specified in the `dirContextTimeout` parameter. After this time has passed, if there are still no connections available and the current number of live connections is less than the `dirContextMazSize` parameter, a new connection is created. If the total number of live connections is equal to or larger than `dirContextMaxSize`, an exception is thrown.

The parameter is mandatory for enabling the pool. If this parameter is not specified or specified with a value less or equal to 0, the pool is disabled. In these cases, WMM will work like before (only reuse one connection).

- ▶ `dirContextsMinSize`

The minimum number of live connections. When the pool initializes, this is the number of connections that are created. The number of live connections changed between `dirContextsMinSize` and `dirContextTimeout` depends on the number of concurrent requests. The `dirContextsMinSize` must be larger than 0. The default value is 1. In most cases, it should not be larger than 10.

- ▶ `dirContextTimeout`

The number of milliseconds a request has to wait before throwing an exception if there is no available connections in the pool and the number of current connections reaches the `dirContextMaxSize`. A value of 0 means the waiting time is forever. The default value is 3000.

Increasing the groupCacheRefreshInterval

To improve performance in looking up group members, WebSphere Member Manager caches the names of all groups. The `groupCacheRefreshInterval` attribute is used for specifying how often the group cache should be refreshed (read all groups from LDAP server). If this attribute is not specified, the default value is 600 seconds. The unit of this attribute is seconds. It can have the following values:

- ▶ `groupCacheRefreshInterval="0"`

Group cache is always refreshed when there is a request for the group cache. This option has lowest performance; however, it ensures that the data in group cache is always the latest.

- ▶ `groupCacheRefreshInterval="-1"`

If the value is -1 or a negative number, the group cache is not refreshed until a group is created, renamed, or removed through WebSphere Member Manager.

This option has the highest performance. However, if you create, rename, or remove a group directly from LDAP server, the changes are not reflected in the group cache until you restart WebSphere Member Manager. If you create, rename, or remove the group through WebSphere Member Manager, the group cache is refreshed.

You can use this option for improved performance if there is no group update from the LDAP server side.

You should never specify a value of -1 when using a read-only LDAP.

- ▶ `groupCacheRefreshInterval="<any number of seconds>"`

If the value is a positive number, the group cache is refreshed if the number of seconds has passed and there is a request for the group cache. Note that the group cache is not refreshed if there is no request for the group cache, even if the time since last refresh has exceeded the specified seconds.

If you create, rename, or remove a group through WebSphere Member Manager, the group cache is refreshed. For example, if `groupCacheRefreshInterval=600`, then if you create a new group directly in the LDAP server, this new group may not be in the group cache for a maximum of 10 minutes.

Specific performance tips for Active Directory

Every entry on Active Directory has a built-in attribute called ObjectGUID. This attribute is automatically populated by Active Directory to uniquely identify each entry. You can configure WebSphere Member Manager to use the ObjectGUID attribute as External Id instead of using the `ibm-appUUID` that WebSphere Member Manager generates.

To do configure WebSphere Member Manager to use ObjectGUID, you need to:

- In wmm.xml, change wmmGenerateExtId="true" to wmmGenerateExtId="false" as shown in Example 3-5.

Example 3-5 Changing wmmGenerateExtId

```
<ldapRepository name="wmmLDAP"
  UUID="LDAP1"
  adapterClassName="com.ibm.ws.wmm.ldap.activedir.ActiveDirectoryAdapterImpl"
  supportDynamicAttributes="false"
  configurationFile="wmm/xml/wmmLDAPAttributes_AD.xml"
  wmmGenerateExtId="false"
  supportGetPersonByAccountName="true"
  profileRepositoryForGroups="LDAP1"
  supportTransactions="false"
  adminId="CN=wpsadmin,CN=users,DC=yourco,DC=com"
  adminPassword="xxxxxxx"
  ldapHost="andyserver.torolab.ibm.com"
  ldapPort="636"
  ldapTimeOut="6000"
  ldapAuthentication="SIMPLE"
  ldapType="0"
  memberOfAttributeName="memberOf"
  java.naming.security.protocol="ssl"
  groupCacheRefreshInterval="-1"
  dirContextsMaxSize="10"
  dirContextsMinSize="5"
  dirContextTimeout="1000">
```

- In wmm.xml, remove all occurrences of ";ibm-appUUID" as shown in Example 3-6.

Example 3-6 Removing ";ibm-appUUID"

```
<supportedLdapEntryTypes>
  <supportedLdapEntryType name="Person"
    rdnAttrTypes="cn"
    objectClassesForRead="user;ibm-appUUIDAux"
    objectClassesForWrite="user"
    searchBases="cn=users,dc=yourco,dc=com"
    searchFilter="(ObjectCategory=Person)"/>
  <supportedLdapEntryType name="Group"
    rdnAttrTypes="cn"
    objectClassesForRead="group"
    objectClassesForWrite="group;ibm-appUUIDAux"
    searchBases="cn=groups,dc=yourco,dc=com"
    searchFilter="(ObjectCategory=Group)"/>
  <supportedLdapEntryType name="Organization"
```

```

        rdnAttrTypes="o"
        objectClassesForRead="organization;ibm-appUIDAux"
        objectClassesForWrite="organization"/>
    <supportedLdapEntryType name="OrganizationalUnit"
        rdnAttrTypes="ou"
        objectClassesForRead="organizationalUnit;ibm-appUIDAux"
        objectClassesForWrite="organizationalUnit"/>
</supportedLdapEntryTypes>

```

- In `wmmLDAPServerAttributes.xml`, change the mapping of `extId` from `ibm-appUUID` to `objectGUID` as shown in Example 3-7.

Example 3-7 Changing

```

<attributeMap wmmAttributeName="extId"
    applicableMemberTypes="Person;Group;Organization;OrganizationalUnit"
    pluginAttributeName="objectGUID"
    dataType="String"
    pluginDataType="OctetString"
    multiValued="false"
    readOnly="true"/>

```

3.5.2 LDAP architecture and schema layout considerations

The following are LDAP architecture and schema layout considerations:

- By default, WebSphere Portal server assumes that your login name is the relative distinguished name of the LDAP entry. Commonly, customers want to use another attribute for the login ID. For example, customers may want to use an e-mail address as the login ID, which is stored under the LDAP's email attribute.

To change the login to use the email attribute, follow these steps:

- Ensure that the LDAP User Filter is set correctly by accessing the WebSphere Application Server AdminConsole and navigating to **Security** → **User Registries** → **LDAP** → **Advanced LDAP Settings**.

The setting should be similar to this example:

```
(&(email=%v)(objectclass=inetOrgPerson))
```

In this example, *email* is the LDAP attribute that will be matched with the login parameter, and *inetOrgPerson* is the LDAP object class of this user.

- Ensure that there is a attribute map tag for the email attribute in the `wmmLDAPServerAttributes.xml` file. To check this attribute, navigate to `wps_root/wmm`.

- c. Ensure that the PumaService.properties file is correct. Navigate to *wps_root/shared/app/config/services*. Open the file and change the following property:

```
user.fbadefault.filter=email
```

- d. Rerun the security task if required.

- ▶ When you assign IDs in the wpconfig.properties file to run the enable-security-ldap task, use separate IDs for the following properties:
 - WasUserid
 - PortalAdminId
 - LDAPAdminUid
 - LDAPBindID

Using separate IDs builds flexibility into your administration. For example, if WasUserid and LDAPBindID are the same value and if you need to change the WasUserid password for security reasons, then you would have to change the LDAPBindID password as well. You would have to make additional WebSphere Application Server configuration changes to account for the password change. Having separate IDs also allows only the necessary permissions to be given to each ID.

- ▶ Ensure that the Portal admin IDs (wpsadmin, wpsbind, wasadmin, wpsadmins) exist in the same sub-tree as the regular users and groups. If they do not, there are special considerations to get the Portal admin to work, and performance takes a hit.
- ▶ WebSphere Portal Server uses groups in the LDAP to manage access control lists. If you have the LDAP structured organizationally (cn=groups, ou=accounting, o=ibm and cn=groups, ou=sales, o=ibm), then it can become difficult to manage Portal access control lists. (It is technically possible, but not practical for manageability.) An alternative is to create a separate group somewhere in the LDAP that contains all the managers in the corporation. Then you can easily separate the access control lists on portlets and pages from the managers, users, and so on.

3.5.3 Using an LDAP server cluster

WebSphere Portal supports and recommends using an LDAP server cluster for distributing LDAP calls and for failover.

To use an LDAP server cluster, you must uncheck the Reuse Connection box in the Deployment Manager security settings. You can set the LDAPReuseConnection property to `false` in the wpconfig.properties file before running the enable-security-ldap task. Then, when you run the task to configure security, WebSphere Application Server is setup automatically to take advantage

of the LDAP server cluster. WebSphere Member Manager always rebinds to the LDAP, so you do not need to make configuration changes.

3.5.4 Using a single LDAP image

WebSphere Portal needs to be presented with a single LDAP image. If multiple LDAP images are involved, the CU can use a tool such as IDI to create a single image of the LDAP to present to WebSphere Portal.

3.5.5 LDAP, WebSphere Portal, and the Q/A environment

You should first configure the Portal to a Q/A replica of the production environment and then conduct load and stress testing. Then, follow the Switch LDAP procedure in the Portal administration chapter to reconfigure the Portal to the actual production LDAP.

3.5.6 LDAP administration

WebSphere Portal provides portlets that allow you to administer the LDAP from the Portal. However, we recommend that LDAP administration happen natively (for example, outside of Portal). Most companies choose to administer their LDAP natively using their specific LDAP administration tools. If you choose to administer the LDAP natively, you need to configure the Portal to a read-only LDAP. Follow the procedure below to configure Portal to a read-only LDAP:

Configuring WebSphere Portal for a read-only LDAP

If LDAP is not configured, perform these steps:

1. If you are running WebSphere Portal V5.0.0 or V5.0.2, install the interim fix PQ83389.
2. Change to the `wp_root/config/templates/wmm` directory.
3. Open the `wmm.xml` file for your LDAP type as shown in the following example:

```
wmm_LDAP.xml1.<YourLDAPType>.<NUMBER>.wmm
```

where:

`<YourLDAPType>` is the type of the LDAP, such as `IBM_DIRECTORY_SERVER`.
`<NUMBER>` specifies if a lookaside database is defined. Use 1 if a database is not defined or 3 if a database is defined.

4. Modify the following attributes in the `ldapRepository` tag section of the file:
 - Set `wmmGenerateExtId` to `false`
 - Add `ignoreReadOnlyUpdate` with `true` as the value

5. Open the wmmLDAPAttributes.xml file for your LDAP type.

wmmLDAPAttributes_<YourLDAPType>.xml

where:

<YourLDAPType> is the type of the LDAP, such as IBM_DIRECTORY_SERVER.

6. Set the readOnly attribute to true in every attributeMap tag.

```
<attributeMap wmmAttributeName="uid"
    ...
    readOnly="true"      <!-- Add the attribute if it is not already
defined -->
/>
```

7. Search for the definition of the extId attribute.

8. Modify the pluginAttributeName attribute to use a unique attribute in the LDAP directory.

```
<attributeMap wmmAttributeName="extId"
    ...
    pluginAttributeName="ibm-entryUuid"<!-- uniqueID within IBM
Directory Server -->
/>
```

9. Save the wmm.xml and wmmLDAPAttributes.xml files.

10. Choose the appropriate settings for your LDAP setup in the *wp_root/config/wpconfig.properties* file. For more information, see the WebSphere Portal InfoCenter.

11. Run the LDAP configuration task using the following command:

```
wp_root/config/wpsconfig.bat enable-security-ldap
```

Configuring WebSphere Portal for a read-only LDAP if the configuration fails

If you try to configure LDAP and receive the following error message, perform the following steps to complete the WebSphere Portal configuration for a read-only LDAP:

action-create-deployment-credentials:

```
[xmlaccess] <?xml version="1.0" encoding="UTF-8" ?>
```

```
[xmlaccess] <failure>
```

```
[xmlaccess] com.ibm.wps.command.xml.XmlCommandServlet$AuthorizationException:
```

XMLC0005E:

1. Perform steps 1 through 10 from “Configuring WebSphere Portal for a read-only LDAP” on page 83.

2. Run the configuration task using the following command:

```
wp_root/config/wpsconfig.bat init action-update-wmm-ldap
```

3. Stop and start WebSphere Portal.
4. Run the config task using the following command:
`wp_root/config/wpsconfig.bat action-create-deployment-credentials`

Archived

Solution deployment

This chapter describes specific points of the Java 2 Platform, Enterprise Edition (J2EE) platform which uses portlets for content and applications publishing. Portlets technology allows independent but integrated applications to be displayed on the same Web page, making it easier to navigate the page.

This chapter explains how to install and update portlets and how to customize the Portal look and feel.

4.1 Understanding J2EE

J2EE is a powerful set of standards for developing multi-tier enterprise applications. The J2EE platform simplifies enterprise applications by basing them on standardized, modular components, by providing a complete set of services to those components, and by handling many details of application behavior automatically, without complex programming.

WebSphere products are compliant with J2EE 1.3.

There are three types of modular components:

► Java Archive file (JAR)

A JAR file is a zipped file with a .jar extension. It contains a file system based in J2EE standards that organizes the code, libraries, descriptors, and other parts in folders named *containers*.

There are two types of JAR files:

- An EJB JAR file contains a deployment descriptor, the enterprise bean files, and related files.
- An Application Client JAR file contains a deployment descriptor, the class files for the application client, and related files.

► Web Archive file (WAR)

A WAR file is a standard JAR file with a .war extension. It contains a deployment descriptor, the Web component files, and related resources.

► Enterprise Archive file (EAR)

The EAR file contains a J2EE application with all of its modules. An EAR file is a standard JAR file with an .ear extension. It contains information about how to deploy your Web, client, and EJB modules and contains all their packages (WAR and JAR files).

For more information about the J2EE 1.3 specification, visit the following Web page:

<http://java.sun.com/j2ee/1.3/download.html#platformspec>

4.2 Understanding a J2EE Portal

A Portal on the J2EE platform is a Web-based module which covers the most important aspects of an enterprise system, such as collaboration, security, document management, personalization, and content publishing. The Portal allows you to publish custom applications in an homogeneous visual environment. Each module of the Portal is an independent Web application with a specific function.

The WPS.ear file is the Portal server package, but it is not the Portal server itself. The Portal server is a Web Application Container such as the WebSphere Application Server. It contains integrated functions, such as menus as well as look and feel.

The Portal commonly provides personalization, Single Sign On, and content aggregation from different sources. It also hosts the presentation layer of information systems. Aggregation means to integrate content from different sources within a Web page. A Portal may have sophisticated personalization features to provide customized content to users. Portal pages may have different sets of portlets that create different content for different users.

4.2.1 Portal structure

The Portal is composed of a hierarchical structure of nodes that can be represented in a parent-child relationship, starting from the content root of the Portal. A node is an addressable element in the Portal navigation tree that belongs to one of the following types:

- ▶ Pages

Pages display content in the form of portlets. Pages can contain child nodes, including other pages that provide content. A page can contain column containers, row containers, and portlets. Containers are columns or rows that you can use to arrange the layout of portlets or other containers on the page.

- ▶ Labels

Labels do not display any content but can contain other nodes. They primarily group nodes in the navigation.

- ▶ URLs

URLs can launch any URL-addressable resource, including external Web sites or pages within the Portal site.

Portlets

A portlet is a Web component that uses Java technology and that is managed by a portlet container. The portlet container processes requests and generates dynamic content. Portlets are used by portals as pluggable user interface components that provide a presentation layer to information systems.

The content a portlet generates is also called a **fragment**. A fragment is a piece of markup code, for example, Hypertext Markup Language (HTML), that adheres to certain rules and that can be aggregated with other fragments to form a complete document. The content of a portlet is normally aggregated with the content of other portlets to form the Portal page. A portlet container manages the life cycle of a portlet.

Web clients interact with portlets via a request and response paradigm implemented by the Portal. Normally, users interact with content that portlets produce. For example, users follow links or submit forms which results in the Portal receiving portlet actions. The Portal then forwards the portlet actions to the portlets which the user's interactions targeted.

The content generated by a portlet may vary from one user to another depending on the user configuration for the portlet.

Portlet container

A portlet container runs portlets and provides them with the required runtime environment. It contains portlets, manages their life cycle, and provides persistent storage for portlet preferences. A portlet container receives requests from the Portal to execute requests on the portlets hosted by it. A portlet container is not responsible for aggregating the content produced by the portlets. It is the responsibility of the Portal to handle the aggregation.

You can build a portal and a portlet container together as a single component of an application suite or as two separate components of a Portal application.

Portlet application

A portlet application is a Web application that contains portlets and a portlet deployment descriptor in addition to servlets, JavaServer Pages (JSPs), HTML pages, classes, and other resources that are normally found in a Web application. A bundled portlet application can run in multiple portlet containers implementations.

Besides the Web application-specific meta information, the portlet application must include descriptive meta information about the portlets that it contains.

Portlet directory structure

A portlet application follows the same directory hierarchy structure as Web applications. In addition, it must contain a deployment descriptor file called `/WEB-INF/portlet.xml`. Portlet classes, utility classes, and other resources accessed through the portlet application class loader must reside within the `/WEB-INF/classes` directory or within a JAR file in the `/WEB-INF/lib/` directory.

The following is a listing of the files that are included in a sample portlet application:

- ▶ `/images/myButton.gif`
- ▶ `/META-INF/MANIFEST.MF`
- ▶ `/WEB-INF/web.xml`
- ▶ `/WEB-INF/portlet.xml`
- ▶ `/WEB-INF/lib/myHelpers.jar`
- ▶ `/WEB-INF/classes/com/mycorp/servlets/MyServlet.class`
- ▶ `/WEB-INF/classes/com/mycorp/portlets/MyPortlet.class`
- ▶ `/WEB-INF/jsp/myHelp.jsp`

Portlet and Web application deployment descriptor

For Portlet Specification version 1.0, there is a clear distinction between Web resources, such as servlets, JSPs, static markup pages and so on, and portlets. This is because in Servlet Specification 2.3, the Web application deployment descriptor is not extensible. You must specify all Web resources that are not portlets in the `web.xml` deployment descriptor and all portlets and portlet-related settings in an additional file called `portlet.xml`. The format of this additional file is described in detail below.

Note: You can find the Portlet Specification 1.0 at the following Web address:

<http://www.jcp.org/aboutJava/communityprocess/review/jsr168>

You can find the Servlet Specifications 2.3 at the following Web address:

<http://www.jcp.org/aboutJava/communityprocess/final/jsr053>

Portlet deployment descriptor elements

The portlet deployment descriptor for all portlet containers must support the following types of configuration and deployment information:

- ▶ Portlet application definition
- ▶ Portlet definition

Uniqueness of deployment descriptor values

The scope of the portlet application definition must be unique in the following deployment descriptor values:

- ▶ portlet *portlet-name*
- ▶ custom-portlet-mode *portlet-mode*
- ▶ custom-window-state *window-state*
- ▶ user-attribute *name*

The scope of the portlet definition must be unique in the following deployment descriptor values:

- ▶ init-param *name*
- ▶ supports *mime-type*
- ▶ preference *name*
- ▶ security-role-ref *role-name*

4.2.2 Elements of a Portal page

Figure 4-1 illustrates the markup fragments that a portlet generates. A portal normally adds a title, control buttons, and other decorations to the markup fragment that the portlet generates. This new fragment is called a *portlet window*. Then, the Portal aggregates portlet windows into a complete document, the Portal page.

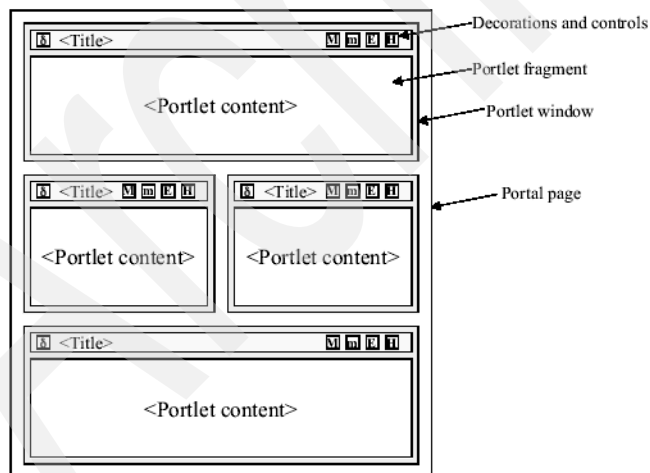


Figure 4-1 Elements of a Portal page

4.3 Portal configuration

This section describes the most typical activities on the WebSphere Portal configuration, such as Install Portlets, Change Theme and Skin, Create Pages, and related activities.

4.3.1 Customizing the Portal

This activity is one of the first activities to take place while implementing a Portal environment. This is because that is the part of the entire job that makes difference in a project presentation first impact.

The Manage Pages portlet allows you to perform the following tasks:

- ▶ Create, reorder, delete, and edit the properties of pages, labels, and URLs
- ▶ Reorder pages, labels, and URLs
- ▶ Assign access to pages, labels, and URLs

Details about these tasks are explained in the help for the Manage Pages portlet.

Opening Manage Pages

To open Manage Pages:

1. Log in to the Portal as an administrator.
2. Click **Administration** in the Portal toolbar.
3. In the navigation tree, click **Portal User Interface Manage Pages**. The nodes belonging to the currently selected node are displayed (Figure 4-2).

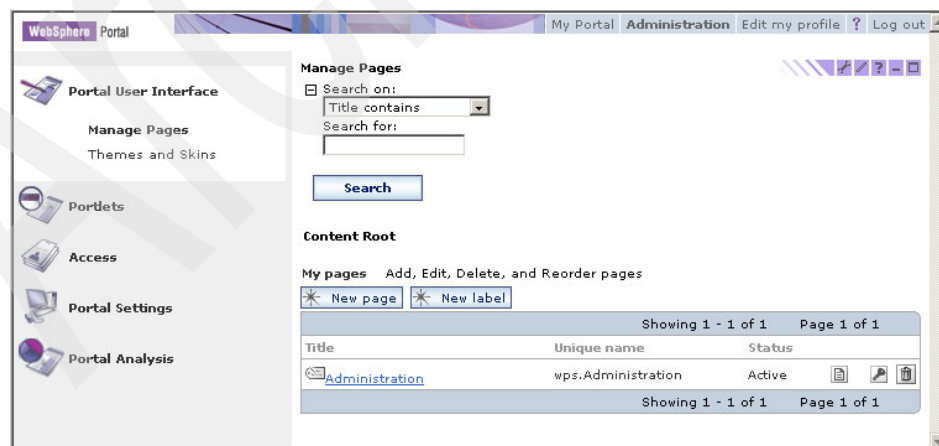


Figure 4-2 Manage Pages

4. Navigate to a node in the Portal hierarchy.

Manage Pages displays a table that shows the hierarchical structure of the Portal. The table displays a list of nodes that belong to the selected branch in the tree. The parent nodes are displayed above the list as a breadcrumb trail.

5. To view nodes at a higher level in the Portal structure, select a node from the breadcrumb trail above the table.

To view nodes at a lower level in the Portal structure, select a node from the Title column in the table.

Creating and deleting pages

Both administrators and users with appropriate access can create and delete pages. Users can only delete the pages they create.

If you are an administrator, follow these steps:

1. Open Manage Pages.
2. Navigate to the node under which you want to insert the new page.
3. Click **New Page**.

You can also create new labels and URLs.

If you are a user, follow these steps:

1. Navigate to the page in the Portal under which you want to insert the new page.
2. Click **New Page** in the toolbar.

Both of these tasks direct you to the Properties portlet for setting the page title and advanced options and to the Content portlet for editing the layout and content of the page. When you are finished, the new page is automatically activated. More detailed information is provided in the online help for each of these tasks.

Making one Portal appear as multiple Portals

You can make your single Portal installation appear as multiple Portals with different URLs. The different Portal representations show different pages with a different look and feel for different authenticated users, depending on their group membership. To configure your Portal to appear as multiple Portals, use the portlets for managing pages, layout and content, and users and groups as well as for working with themes and skins. These portlets allow you to assign specific content, layout, themes, and skins to pages and to give user groups permissions to view specific pages. Thus, you can create pages with completely different content and visual representation for view by various user groups. The user groups can even overlap.

4.3.2 Installing the portlet

This section describes two ways to deploy a portlet into a cluster environment. In both cases, you are not transferring from staging to production. You are instead installing directly to your Portal environment. Thus, we do not recommend this method if you are deploying to production. However, in most cases, this is a staging deployment procedure.

Installing a portlet from the Portal interface

Installing a portlet from the Portal interface is the easiest way to deploy an application. It is easiest but not the simplest. This activity involves more time changing from one interface to another than with the installation tasks themselves.

Note: If you are in a cluster environment, do not forget to synchronize the nodes after the install. Otherwise, you will not be able to start the Web-application in the cluster and make it available in all your Portal nodes.

Installing a portlet from the Portal interface involves four primary steps:

1. Installing the WAR file(s)
2. Synchronizing the nodes
3. Starting the Web application(s)
4. Activating the portlets

Installing the WAR file(s)

1. Log into the Portal as administrator (wpsadmin) and then go to the Administration page.
2. In the portlets session, click the Portlets menu in the left bar on the window to open the portlet.
3. In the sub-menu, select **Install**. The Install Portlets page will appear as shown in Figure 4-3 on page 96.

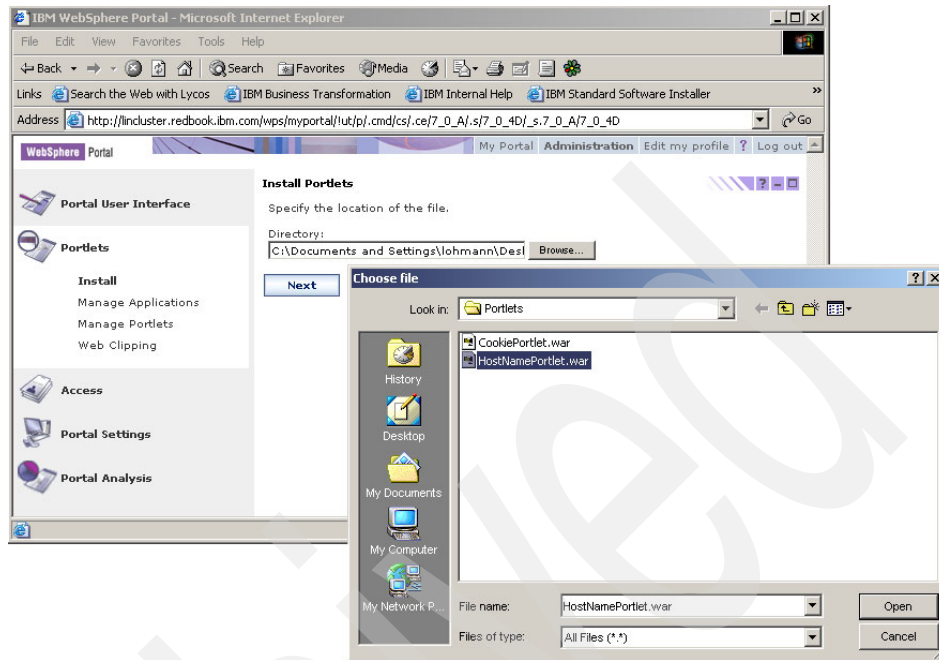


Figure 4-3 Portal interface installation

4. In the directory field, enter the path to the WAR file which contains the portlet. You can use the Browse button to navigate to the file and select it.
5. Click **Next** to start the install process.
Confirm the portlet information that is displayed. It is the description of the Concrete portlet as described in the deployment descriptor file (web.xml) and in the portlet specification (portlet.xml).
6. Click **Next** to confirm the installation.

Note: This process can take several minutes to complete, depending on the complexity of the portlet application being installed.

After completing the install, you will see the message shown in Figure 4-4 which indicates that the portlet was successfully installed.

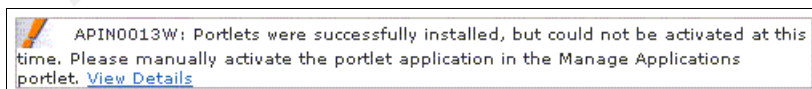


Figure 4-4 Install portlet message for clustered environments

Note: Even when the portlet installs successfully, you still need to start and activate the portlet manually because this Portal is in a cluster environment. Do not close the browser session. You will need it again later.

Synchronizing the nodes

Many times, the clusters are configured to automatically synchronize its nodes. However, if this is not the case, you need to synchronize all the nodes affected by this installation before starting the EAR file. We strongly recommend that you check to see if the nodes are synchronized. For more information about how to synchronize nodes in a cluster environment, see Example 4-4 “Synchronize Nodes - jacl script” on page 101.

Starting the Web application

To start the Web application:

1. Open the Deployment Manager Administrative Console and login as administrator (wasadmin).
2. Open the Applications menu in the left bar. The submenu shown in Figure 4-5 will appear.

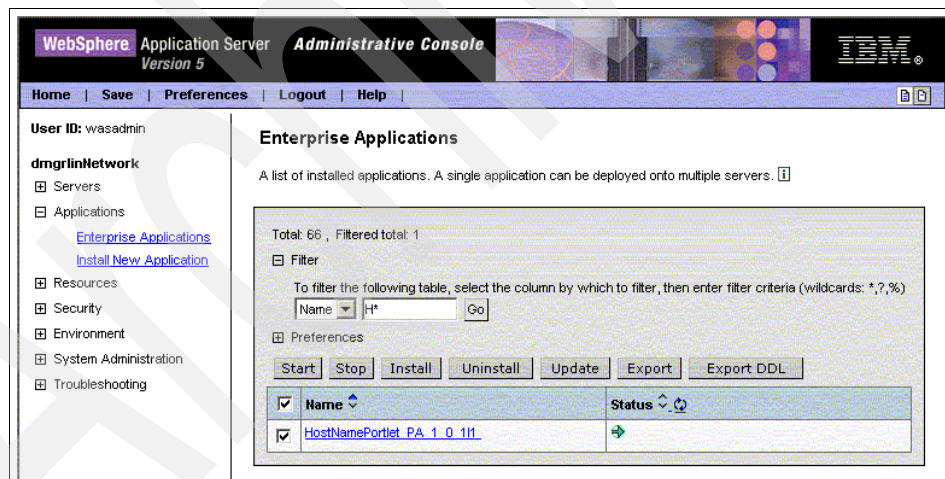


Figure 4-5 Start application

3. Select **Enterprise Applications** to open the management page.
4. Use the Filter field to facilitate the search for your Web application as indicated in Figure 4-5.
5. Check the check box of the application (or applications) that you want to start, and click **Start**.

Note: This task can take several minutes to complete depending on the complexity of the application and the number of nodes under your cluster.

- Wait for the filled green arrow which indicates that the application has started. Then, logout from the Administrative Console and go back to the Portal Administrative Page.

Activating the portlet

To activate the portlet that you installed, follow these steps:

- In the Portal Administrative page, select **Manage Applications** on the submenu of portlets. Two list boxes as shown in Figure 4-6 will appear.

For each WAR file listed in the first list box, the second list box shows all the portlets that belongs to this Web module.

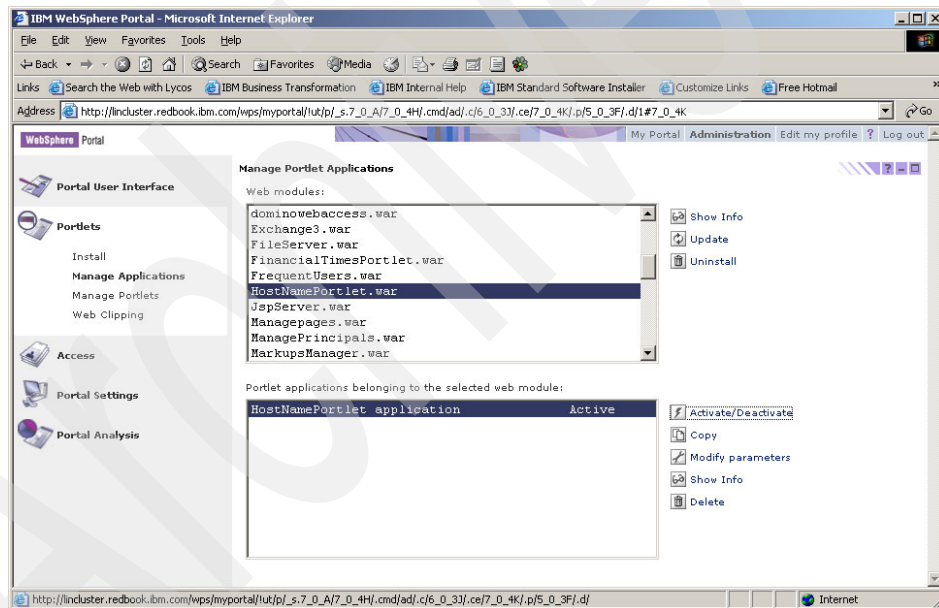


Figure 4-6 Activate portlet

- Select the WAR file that you just installed in the first list.
- Activate each portlet of the referenced Web module by selecting one at a time in the second list box and clicking **Activate/Deactivate**. This operation toggles the portlet status into active and inactive. Make sure that the portlets that you want to publish are set to Active.

Your portlet is ready to be added to a page.

Installing a portlet from the command line

This section explains how to use the command line to automate the deployment of one or more portlet applications using batch mode.

Note: This process requires experience with Extensible Markup Language (XML).

To automate the deployment of a portlet application, you use a tool called XMLAccess. XMLAccess is a Java-based tool that uses XML schemes to make changes to the Portal file system and database, making it possible to set several tasks required for the Portal management and maintenance. For more information about the XMLAccess tool, see 5.2.2, “Using the XMLAccess tool for moving” on page 114.

Example 4-1 describes an XML file that installs the World Clock portlet into the Portal.

Example 4-1 Example that installs the World Clock portlet

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<request xsi:noNamespaceSchemaLocation="PortalConfig_1.2.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" create-oids="true"
type="update" >
  <!-- Sample for deploying a portlet. -->
  <portal action="locate" >
    <!-- uid must match uid attribute of portlet-app in portlet.xml -->
    <web-app action="update" active="false"
uid="com.ibm.wps.portlets.worldclock" >
      <url>file:///server_root$/installableApps/worldclock.war</url>
      <!-- uid must match uid attribute of concrete-portlet-app in
portlet.xml -->
      <portlet-app action="update" active="false"
uid="com.ibm.wps.portlets.worldclock.1" >
        <!-- Name must match content of portlet-name subtag of
concrete-portlet in portlet.xml -->
        <portlet objectid="com.ibm.wps.portlets.worldclock"
action="update" active="false" name="World Clock" />
      </portlet-app>
    </web-app>
  </portal>
</request>
```

Note: The *active* attribute is set to false in all the tags to prevent warnings that are caused when you test the portlet's activation before synchronizing the nodes and starting the application. Also, the URL tag that contains a path for the WAR file must be the path for the WAR file that you want to install.

Example 4-1 “Example that installs the World Clock portlet” on page 99 installs just one portlet. However, it is possible to install more than one portlet at a time. To install multiple portlets simultaneously, replicate the web-app block that begins with web-app and ends with the </web-app> tags. Then, change the enclosed attributes that are related to the portlets that you want to install.

The XML file must be accessible in the Portal installation file system. We recommend that you create a folder in the Portal installation root named xmlscripts that will contain the XML files that you need for this process as shown in Example 4-2.

Example 4-2 Using XMLAccess to install portlet

```
[portal-root]/bin/xmlaccess.sh -user [wpsadmin] -pwd [password] -url  
http://wpshost.yourdomain.com/wps/config -in  
[portal-root]/xmlscripts/install_portlet.xml
```

Then, use the XMLAccess tool to run the installation task as shown in Example 4-3.

Example 4-3 Using XMLAccess to run the installation task

```
Licensed Materials - Property of IBM, 5724-E76, 5724-E77, (C) Copyright IBM  
Corp. 2001, 2003 - All Rights reserved. US Government Users Restricted Rights -  
Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM  
Corp.  
XMLA0006I: Connecting to URL http://lincluster.redbook.ibm.com/wps/config  
XMLA0002I: Reading input file /WebSphere/PortalServer/bin/install_portlet.xml  
XMLA0011I: Request was accepted.  
<?xml version="1.0" encoding="UTF-8"?>  
<!-- IBM WebSphere Portal/5.0.2.1 build 034 exported on Fri Aug 13 10:52:12 EDT  
2004 from bc1srv3/9.42.171.69 -->  
<!-- 1/3 [web-app uid=com.ibm.wps.portlets.worldclock] -->  
<!-- 2/3 [portlet-app uid=com.ibm.wps.portlets.worldclock.1] -->  
<!-- 3/3 [portlet com.ibm.wps.portlets.worldclock name=World Clock] -->  
<request type="update" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:noNamespaceSchemaLocation="PortalConfig_1.2.xsd">  
  <status element="all" result="ok"/>  
</request>
```

At this point, the Web application is installed in the Portal server. It is stopped and inactive.

To make the Web application available in all cluster members, you next need to synchronize the nodes in the cluster environment. You can use the wsadmin tool, a Java-based command prompt with a set of commands to administer all the WebSphere platforms.

For more information about the wsadmin tool, see the following Web address:

http://publib.boulder.ibm.com/infocenter/wasinfo/topic/com.ibm.websphere.base.doc/info/aes/ae/rxml_commandline.html

Example 4-4 demonstrates how to use the jac1 script to synchronize nodes. For more information about executing the jac1 script to synchronize all nodes in a clustered environment, see Example A-3 “sync_all_nodes.jac1” on page 232.

Example 4-4 Synchronize Nodes - jac1 script

```
[was-root]/bin/wsadmin.sh -f [was-root]/jac1script/sync_all_nodes.jac1 -user  
[wasadmin] -password [password]
```

After synchronization occurs, a message similar to that shown in Example 4-5 is displayed:

Example 4-5 WSAAdmin SyncNodes command return

Number of nodes to sync: 2

```
Start Synchronizing Node:  
WebSphere:platform=common,cell=dmgrlinNetwork,version=5.0,name=nodeSync,mbeanId  
entifier=nodeSync,type=NodeSync,node=linportal1,process=nodeagent  
Finished Synchronizing Node
```

```
Start Synchronizing Node:  
WebSphere:platform=common,cell=dmgrlinNetwork,version=5.0,name=nodeSync,mbeanId  
entifier=nodeSync,type=NodeSync,node=linportal2,process=nodeagent  
Finished Synchronizing Node
```

Finished Synchronizing all Nodes

You can now start and activate the application using the XMLAccess tool as shown in Example 4-6.

Note: Example 4-6 uses the same schema as Example 4-1, with the following changes:

- ▶ There is no URL tag `<url...></url>`.
- ▶ The **web-app** tag is set to `<web-app action="locate" ...>`.
- ▶ All **active** attributes are set to true.

Example 4-6 start_portlet.xml

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<request xsi:noNamespaceSchemaLocation="PortalConfig_1.2.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" create-oids="true"
type="update" >
  <!-- Sample for start a web-app. -->
  <portal action="locate" >
    <!-- uid must match uid attribute of portlet-app in portlet.xml -->
    <web-app action="locate" active="true"
uid="com.ibm.wps.portlets.worldclock" >
      <!-- uid must match uid attribute of concrete-portlet-app in
portlet.xml -->
      <portlet-app action="update" active="true"
uid="com.ibm.wps.portlets.worldclock.1" >
        <!-- Name must match content of portlet-name subtag of
concrete-portlet in portlet.xml -->
        <portlet objectid="com.ibm.wps.portlets.worldclock"
action="update" active="true" name="World Clock" />
      </portlet-app>
    </web-app>
  </portal>
</request>
```

We recommend that you save this file in the same file system as the other XML scripts so all the custom scripts remain together.

You can start and activate more than one application at a time (as shown in Example 4-1 “Example that installs the World Clock portlet” on page 99) by replicating the web-app block, changing the enclosed attributes related to the portlets that you want to start and activate.

Example 4-7 illustrates how to start the Enterprise Application and activate the portlet.

Example 4-7 Starting the Enterprise Application and activating the portlet

```
[portal-root]/bin/xmlaccess.sh -user [wpsadmin] -pwd [password] -url  
http://wpshost.yourdomain.com/wps/config -in  
[portal-root]/xmlscripts/start_portlet.xml
```

After synchronization occurs, a message similar to that shown in Example 4-8 is displayed:

Example 4-8 XMLAccess Start command return

```
Licensed Materials - Property of IBM, 5724-E76, 5724-E77, (C) Copyright IBM  
Corp. 2001, 2003 - All Rights reserved. US Government Users Restricted Rights -  
Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM  
Corp.  
XMLA0006I: Connecting to URL http://lincluster.redbook.ibm.com/wps/config  
XMLA0002I: Reading input file /WebSphere/PortalServer/bin/start_portlet.xml  
XMLA0011I: Request was accepted.  
<?xml version="1.0" encoding="UTF-8"?>  
<!-- IBM WebSphere Portal/5.0.2.1 build 034 exported on Fri Aug 13 18:39:35 EDT  
2004 from bc1srv2/9.42.171.10 -->  
<!-- 1/3 [web-app uid=com.ibm.wps.portlets.worldclock] -->  
<!-- 2/3 [portlet-app uid=com.ibm.wps.portlets.worldclock.1] -->  
<!-- 3/3 [portlet com.ibm.wps.portlets.worldclock name=World Clock] -->  
<request type="update" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:noNamespaceSchemaLocation="PortalConfig_1.2.xsd">  
  <status element="all" result="ok"/>  
</request>
```

Your portlet is ready to be added to a page.

Tip: Building both XML files (install_portlet.xml and start_portlet.xml) and placing all the codes in their correct file system, you can run the three commands shown in Example 4-2, Example 4-4, and Example 4-7 within the same script. To do so, create a file named deploy_portlets.sh and write the full command lines in it, one line for each command. Then, set permissions to run as a script.

4.3.3 Updating the portlet

Updating a portlet is one of the most frequent tasks in Portal administration and the reason for most of the services denial issues in production environments. This section describes how to update a portlet with the minimum risk of service denial.

Important: Portlet applications appear in the Enterprise Application list on the administrative console of WebSphere Application Server. However, you should never manage them from outside the Portal. Instead, manage them by using the WebSphere Portal administration portlets or the XML configuration interface of the Portal.

You recognize Web applications which comprise a portlet application by their administrative name, also called the display name. The display name is shown in the WebSphere Application Server Administrative console.

You can identify the name of such a portlet application by a Portal specific identifier suffix, such as `_PA_id`. You append this identifier to the portlet name, for example `Welcome_PA_1_04_uX2`. The name in turn is derived from the name of the WAR file when the portlet application was first installed. This administrative name never changes, even if you use a different filename to update the portlet application.

Updating a portlet from the Portal interface

To update a portlet from the Portal interface:

1. Log into the Portal as administrator (wpsadmin) and then go to the Administration page.
2. Select the **Portlets** menu in the left bar of the window to open the portlets session.
3. In the sub-menu, click **Manage Applications** to open the Manage Portlet Applications page as shown in Figure 4-7 on page 105.

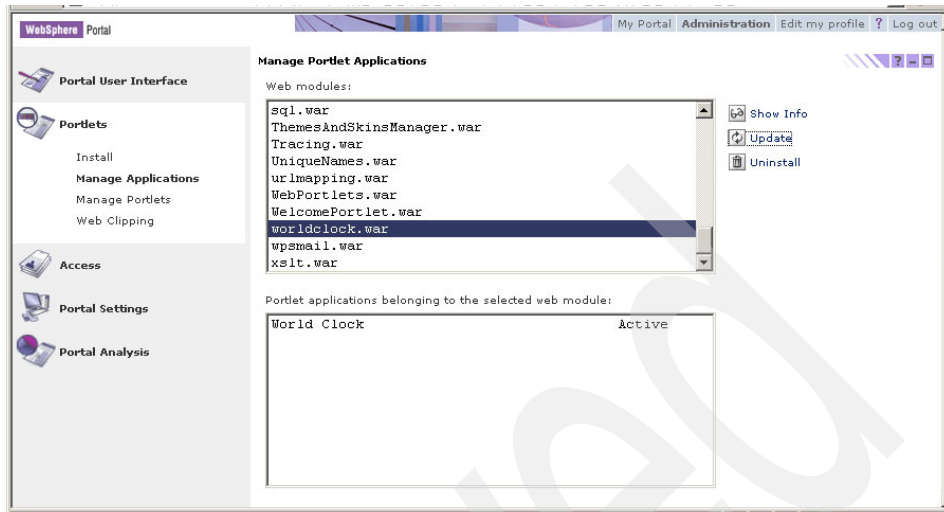


Figure 4-7 Update portlet from the Portal interface

4. Select the WAR file that you want to update from the first list box.
5. Click **Update**. You do not need to deactivate the Portlet Application to this task.
6. From this step, follow the procedure described in “Installing a portlet from the Portal interface” on page 95.

Updating a portlet from the command line

You update a portlet using the XMLAccess tool as described in “Installing a portlet from the command line” on page 99. We recommend that you keep backups of your custom EAR, WAR, and JAR files for further installations and recovery.

Note: Do not deploy portlets, themes, and skins directly to a production environment. We strongly recommend that you deploy to a staging environment before deploying to the production environment. See Chapter 5, “Moving from staging to production” on page 111 for information about how to deploy portlets to a staging environment.

4.3.4 Portlet service

To enable portlets to use pluggable services via dynamic discovery, the portlet Application Program Interface (API) provides the portlet service interface. A portlet service is accessed from the `PortletContext.getService()` method that looks up the appropriate factory for the service, creates the service, and returns it to the portlet. You can invoke a portlet service only from within a portlet.

You may implement various services from different vendors (for example, a Search Service, Location Service, or a Missileries). The following are services that are available with WebSphere Portal:

- ▶ `ContentAccessService`
- ▶ `CredentialVaultService`

Registering a portlet service

To register a portlet service:

1. Put the portlet service classes into a JAR file.
2. Place the JAR file in the `wp_root/shared/app` directory.
3. Add the JAR file to the application server's WebSphere Portal Server shared library. You can edit the library in the Administrative Console by selecting **Environment Shared Libraries WPSLib**.
4. Update the `PortletServiceRegistryService.properties` file in the `wp_root/shared/app/config/services` directory to register the new service:
 - Register the implementation as the corresponding service type.
 - Register the factory for the implementation.
5. Provide configuration parameters for the implementation as shown in the following example:

```
org.apache.jetspeed.portlet.service.default.factory =
    com.ibm.wps.pe.pc.legacy.service.PortletServiceDefaultFactory
...
my.portlet.service.HelloWorldService =
    my.portlet.service.impl.HelloWorldServiceImpl
my.portlet.service.impl.HelloWorldServiceImpl.factory =
    my.portlet.service.factory.HelloWorldServiceFactory
my.portlet.service.impl.HelloWorldServiceImpl.MY_MESSAGE = Hello World
(properties)!
...
```

4.3.5 Installing theme and skin

A Portal *theme* is a structure of JSPs and Cascading Style Sheets (CSS) that are based in a file system. The first step to creating a Portal theme is to understand its file system.

The WPS.ear is an Enterprise Application under the WebSphere Application Server. You can find it in the server file system as:

```
[was-root]/installedApps/wps.ear
```

In this file system, you find the themes and skins folders which have markups folders.

For each markup file system, there is an entire scope of JSPs, CSS, and images that are used for the basic Portal interface rendering (see Figure 4-8). In addition, there are some folders with the available regional and client settings for the basic rendering.

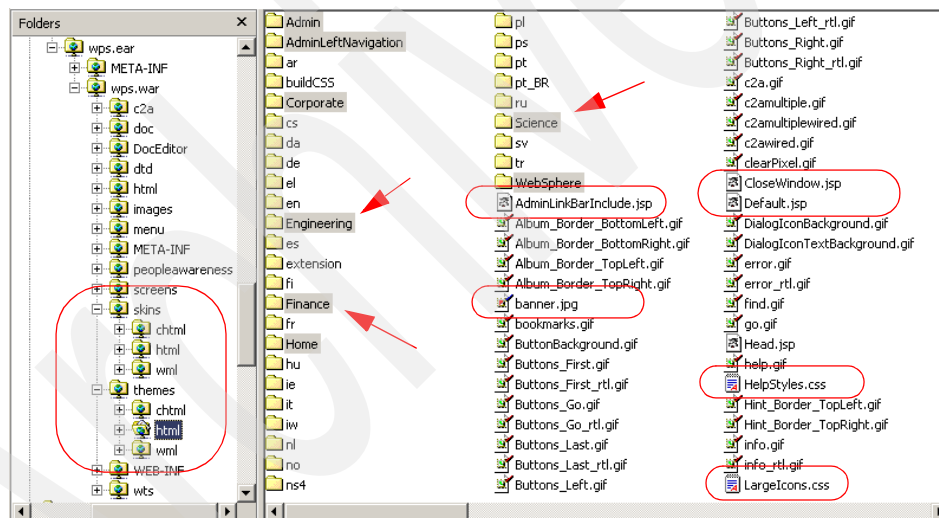


Figure 4-8 WPS.ear File System

There are distinguished folders in this file system that are themes themselves. For example, in Figure 4-9, there is the *Corporate* theme.

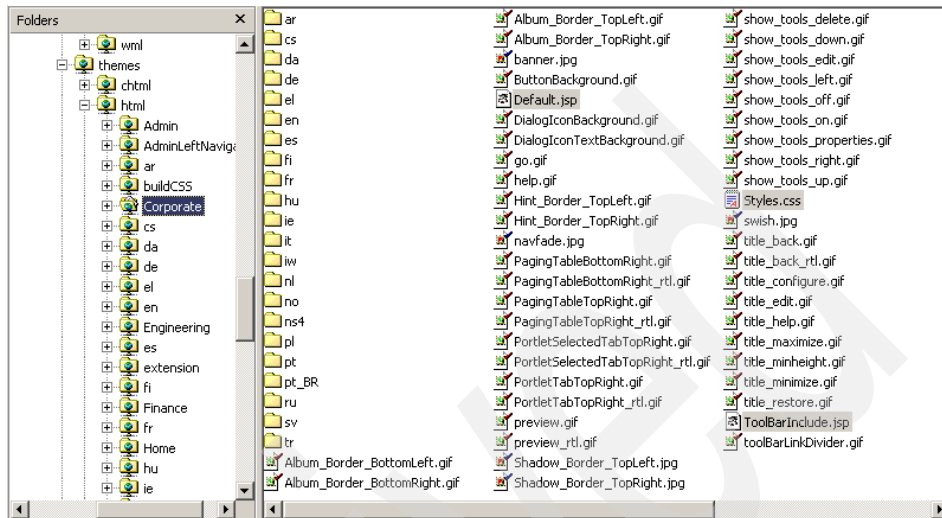


Figure 4-9 Theme file system

The themes have their own JSPs, CSS, and images as well their own regional settings.

Theme and skin deployment

In a cluster environment, you must export the Portal EAR file from the Deployment Manager, update the EAR file with the new theme and skin directories, and then import the Enterprise Application file back to the Deployment Manager cell. If you are on a stand-alone Portal server, use the application server in place of the Deployment Manager.

To deploy theme and skin, do the following:

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:


```
[UNIX]
#./wsadmin.sh -user <was_user> -password <password> $AdminApp export wps
/tmp/wps_orig.ear
[Windows]
wsadmin.bat -user <was_user> -password <password> $AdminApp export wps
c:\temp\wps_orig.ear
```

- c. Enter **quit** to exit the wsadmin command line.
A wps_orig.ear file is 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 you type the command on just one line.)


```
[UNIX]
#./EARExpander.sh -ear /tmp/wps_orig.ear -operationDir /tmp/wps_files/
-operation expand
[Windows]
EARExpander.bat -ear c:\temp\wps_orig.ear -operationDir
c:\temp\wps_files\ -operation expand
```
3. Copy the new theme and skin JSPs to the following locations:
 - a. Theme: *temp dir/wps_files/wps.war/themes/markup/*
 - b. Skin: *temp dir/wps_files/wps.war/skins/markup/*
4. Collapse the files back to an EAR file using the following command:


```
[UNIX]
#./EARExpander.sh -ear /tmp/wps.ear -operationDir /tmp/wps_files/
-operation collapse
[Windows]
EARExpander.bat -ear c:\temp\wps.ear -operationDir c:\temp\wps_files/
-operation collapse
```
5. Import the new wps.ear to the Deployment Manager:
 - a. Use wsadmin to import an EAR file:


```
[UNIX]
#./wsadmin.sh -user <was_user> -password <password>
wsadmin>$AdminApp install /tmp/wps.ear {-update -appname wps}
[Windows]
wsadmin.bat -user <was_user> -password <password>
wsadmin>$AdminApp install c:\tmp\wps.ear {-update -appname wps}
```

Wait for the message that the Application wps installed successfully.
 - b. Save the changes to the master configuration.
 - c. Quit the wsadmin using the following 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 `wpsadmin`:
`http://<hostname.com>/wps/myportal`
 - b. Click **Administration** and select **Portal User Interface**.
 - c. Select **Themes and Skins** view.
 - d. Click **Add new skin** button.
 - e. Enter the skin name and default locale title.
 - f. Enter the skin directory name. (The directory name must match the one that you created in step 3 on page 109.) Click **OK**.
 - g. Click **Add new theme** button.
 - 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 that you created in step 3 on page 109.)
 - j. Select the desired skins to use in this theme. Click **OK**.

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

Moving from staging to production

This chapter describes how to move Portal artifacts and configuration from one Portal environment to another. It describes the Portal development and build process and provides details on how to use the XMLAccess tool to transfer Portal artifacts between environments, based on lessons learned and our Lab research. This chapter also contains a step-by-step guide to moving from a staging to a production environment, including worksheets and a list of run activities as well as troubleshooting tips.

5.1 The Portal staging process

Figure 5-1 illustrates the staging process.

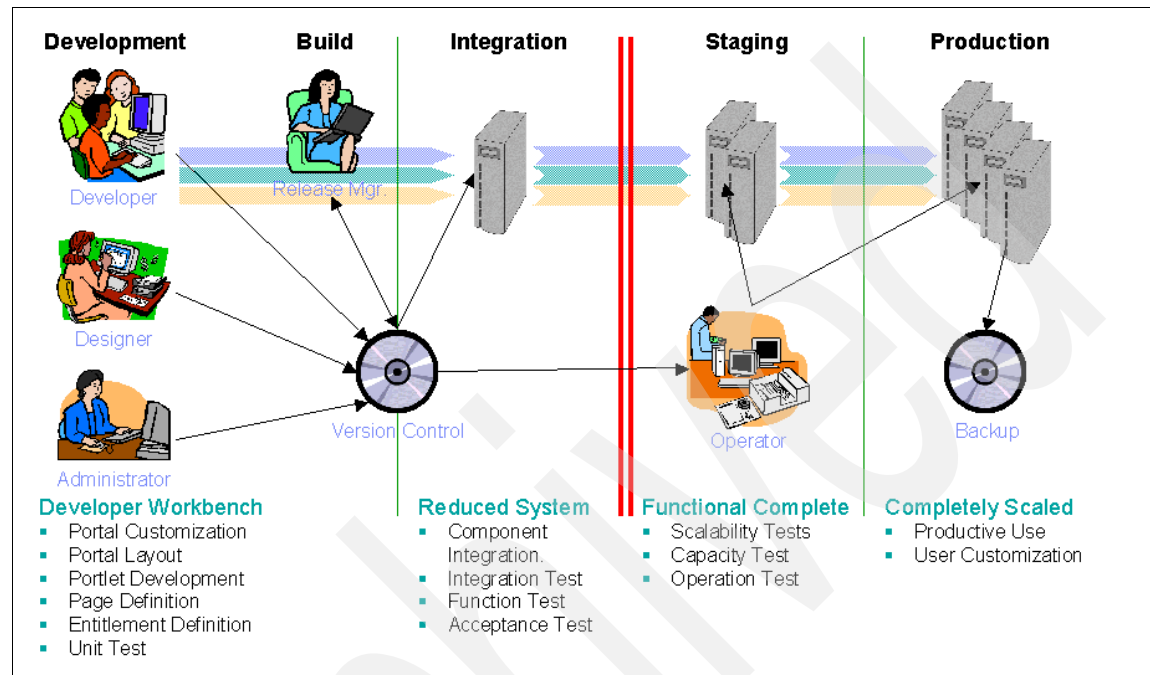


Figure 5-1 Portal staging process

The following sections discuss the elements of the staging process.

5.2 Deployment and build process

Here is an example of how you could implement a Portal build process across environments:

1. A developer implements portlets, servlets, Enterprise JavaBeans, and other J2EE artifacts using either WebSphere Studio or source code that is delivered into a version control system.
2. A designer creates themes, skins, HTML pages, portlet JSPs, and other design elements using any editor.
3. The results are delivered into a version control system.
4. An administrator creates the content tree (labels, URLs, and pages) using the Portal admin user interface of a development Portal.

5. The resulting content trees and portlet instances are exported using XMLAccess or a script and then delivered into a version control system.
6. The release manager assembles a consistent release in the version control system and creates the delivery. The release manager executes scripts (for example, ANT) to extract Java sources, design elements, and configurations from the version control system and then runs a build (compile and package).
7. The operator takes delivery and deploys it onto the staging and production systems. The operator executes ready made config tasks (for example, ANT), XMLAccess configurations, and wsadmin scripts) to deploy the delivery.

5.2.1 Determining what to move

What elements of the Portal you move depends on the type of release you have. If you have an incremental release, you:

- ▶ Add new resources to a release.
- ▶ Update resource attributes (only add properties to lists!).

If you have a differential release, you:

- ▶ Maintain all functionality of the incremental release.
- ▶ Delete existing resources.
- ▶ Update resource attributes (add or delete properties in lists!).

If you have data that has been configured by the user, you should configure the scope of the Portal for a single user.

Figure 5-2 on page 114 illustrates how incremental and differential releases of WebSphere Portal are applied during the Portal configuration life cycle.

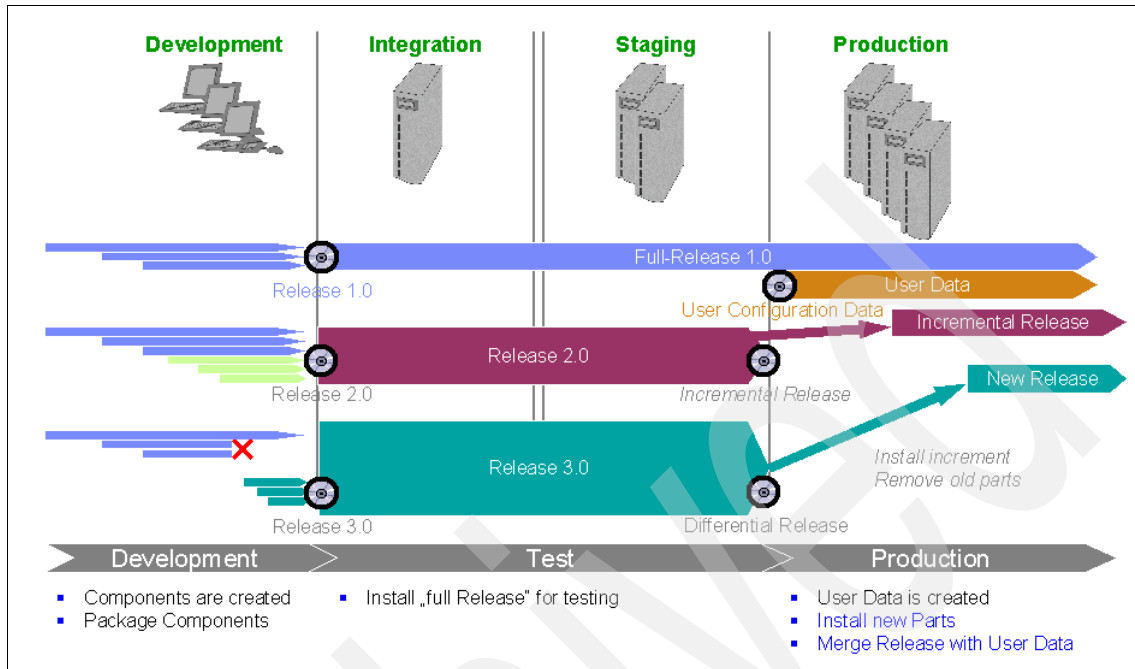


Figure 5-2 Portal configuration life cycle

5.2.2 Using the XMLAccess tool for moving

Although there is no automated method to move Portal applications from one environment to another, there are two options:

- ▶ Completely replace the old release with a new release. The drawbacks of this option is that any data that was customized by the user is lost. While this option works, we do not recommend it.
- ▶ Use the XMLAccess tool to load incremental or differential release as shown in Figure 5-3.

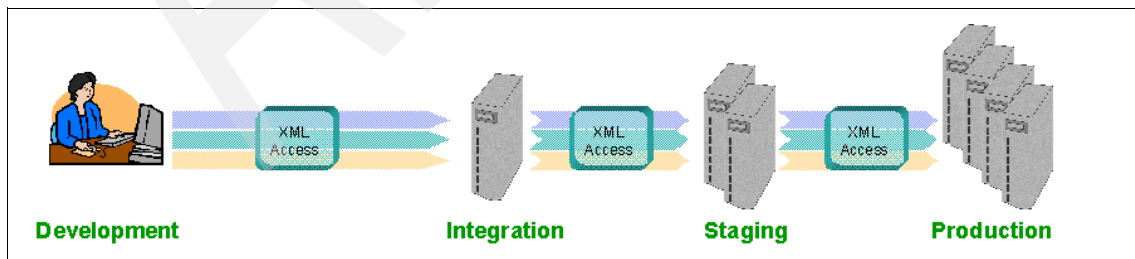


Figure 5-3 The XMLAccess tool

The XML configuration interface

The XML configuration interface is more commonly referred to as the XMLAccess tool, because `xmlaccess` is the command that is executed. The tool provides a batch processing interface for Portal configuration updates and allows you to export an entire Portal configuration or parts of a configuration. For example, you can process and export specific pages to an XML file. You can then re-create the exported configuration from a file on another Portal.

While XMLAccess is as simplified bulk transfer utility, there is no magic button that automatically moves all the components of your Portal to the next environment. The XMLAccess tool interface was developed in WebSphere Portal V2 to help customers move Portal artifacts from one machine to another.

The XMLAccess tool is best for the initial loading of Portal application and for doing incremental releases. However, it is increasingly being used as a command line Portal administration tool.

Why use XMLAccess

The major benefit of XMLAccess is its ability to update pages and portlets without losing user customization. If you perform your updates via XMLAccess, any user customization to a page or a portlet is retained because the object IDs are retained.

For example, your organization may have deployed a stock portlet that the user can customize to monitor certain stocks by adding just those stocks to the portlet. If you update this portlet, you do not want the user customization to be lost. The XMLAccess tool allows you to maintain the user's customization.

When exporting and importing via the XMLAccess tool, the object IDs of the portlet application are maintained. When a user customizes a portlet or a page, these customizations are stored in your back-end database. All these customizations are stored relative to the actual portlet application. The key that ties all of these customized versions of a portlet or page back to its parent is the object ID. For more information about the relationship between user customization and object IDs, see 5.8, “How does customization and the transfer process work?” on page 139.

How XMLAccess works

The XMLAccess command line client is a small separate program that connects to the server using an HTTP connection, which allows you to configure the Portal remotely. The XMLAccess command is located in the *wp root/bin* directory of the Portal server and is `xmlaccess.bat` (on Windows) or `xmlaccess.sh`.

The syntax for the command is as follows:

```
xmlaccess -user wpsadmin -pwd itso -in file.xml -out result.xml -url  
myhost:9082/wps/config
```

In the command line, use the following file names:

- ▶ **file.xml**: The name of a file containing the XML request (configuration export or update) that should be processed.
- ▶ **result.xml**: The name of the result file containing the XML output (configuration export). You can later use that file to re-import the exported configuration.
- ▶ **url**: The URL to access the Portal configuration servlet. This URL consists of the Portal host name, the base Uniform Resource Identifier for the Portal, as specified during installation (for example /wps), and the servlet extension /config.

You can use the XMLAccess tool to transfer a complete configuration, including:

- ▶ Pages
- ▶ Navigation
- ▶ Portlets
- ▶ Access Control List

Note: You need to transfer portlet .WAR files separately. Copy .WAR files to the \installableApps\ directory on the target server.

With the XMLAccess tool, you can also:

- ▶ Load the WebSphere Portal default portlets configuration during the initial install and transfer parts of Portal configuration.
- ▶ Create and modify existing Portal artifacts incremental releases.
- ▶ Delete Portal artifacts. However, you must manually add delete commands to the input file. Keep in mind, although the XMLAccess tool is a bulk transfer utility, the command does not know history. It only knows the Portal configuration at specific point in time.

For complete list of Portal artifacts that can be moved and for a complete list of commands, visit the InfoCenter Web site:

<http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/index.html>

5.2.3 Object IDs

All resources in the Portal (except for the Portal and the settings resources) have an object ID that uniquely identifies them in the Portal. The Portal generates Object IDs when resources are created. Object IDs are globally unique. Two object IDs that were automatically generated by different Portal installations can never be the same.

You can exchange resources between different Portal installations using XML exports and imports without worrying about possible object ID conflicts. Object IDs are represented by the `objectId` attribute in an XML export.

Object IDs are used to express references from one resource to another. For example, the following example references a portlet and puts it on a page using a symbolic object ID:

```
<portlet action="update" ... objectId="_3_609EVJDBI1S5CD0I_97 Welcome Portlet"
...>
...
<portletinstance action="update" ... portletref="_3_609EVJDBI1S5CD0I_97 Welcome
Portlet" ...>
```

Note: You cannot simply invent object IDs for new resources, because they must conform to a correct internal representation.

5.2.4 The Custom Unique Names portlet

A resource that has an object ID can optionally also have a unique name. You can use the unique name to identify the resource unambiguously. Unique names are useful if you need a symbolic way to identify certain resources.

In contrast to object IDs, it is possible to modify unique names of resources, which may be an advantage in certain situations. If you execute an XML import that assigns a unique name which is already used on the system, the execution fails. You can delete the unique name for a resource by setting it to the undefined value.

To set a unique name for a resource, use the Custom Unique Names portlet under Administration, Portal Settings.

Before you export with the XMLAccess tool, ensure that you have defined naming conventions for unique names to prevent name clashes.

5.3 Transferring Portal artifacts using XMLAccess

The process of moving Portal artifacts from one environment to another is a repeatable process that, once you complete it, you can effectively duplicate the process to transfer onto subsequent environments.

Note: The exception is a clustered environment where the export process remains the same but the import process requires extra steps.

You can transfer the following using the XMLAccess tool:

- ▶ Portal Web application configurations (portlet applications)
- ▶ Portal skin definitions
- ▶ Portal theme definitions
- ▶ Portal portlet configurations
- ▶ Portal site map (pages, labels, and links)
- ▶ Portal URL mappings

5.3.1 Transfer process

Transferring your Portal artifacts from one environment to another requires you to export your artifacts from the source environment and then transfer those artifacts to the target environment when you must import them.

The process involves the following steps:

1. Exporting the source configuration using XMLAccess commands.
2. Bundling the supporting files from the source Portal.
3. Transferring the bundled files to the target Portal.
4. Distributing the supporting files to the correct locations on the target Portal.
5. Updating the configuration of the target Portal using the XMLAccess tool.
6. Following up with post-transfer activities.

5.3.2 Exporting a sample page using XMLAccess

There are a number of sample scripts available from the WebSphere Portal InfoCenter. In the following example, we modified the sample file ExportPage.xml to export the Portal Welcome Page.

1. Copy and paste the following sample into a text editor and save it as ExportPage.xml.

```
<?xml version="1.0" encoding="UTF-8"?>
<request
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="PortalConfig_1.2.xsd"
  type="export">

  <portal action="locate">

    <!-- Export Select and Page-->

    <!-- This Sample will export the default welcome page based on it's
    custom unique name -->
    <!--content-node action="export" uniqueness="wps.My Portal.Welcome"
    " export-descendants="false"-->
    <content-node action="export" uniqueness="wps.My Portal.Welcome"/>

  </portal>
</request>
```

2. Check that the XML file is formatted correctly and that you have not copied over any unwanted characters by opening the file.
3. Run XMLAccess against this export script using the following command format:

```
[xmlaccess script] -user {PortalAdministrator} -pwd {PortalAdminPassword}
-url {portal config url} -in [xml input file] -out [out put file exported
xml]
```

In a Windows environment, the command line should look similar to the following:

```
c:\WebSphere\PortalServer\bin\xmlaccess.bat -user wpsadmin -pwd itso -url
http://devportal.redbook.ibm.com:9081/wps/config -in ExportWelcomePage.xml
-out ExportedWelcomePage.xml
```

In a UNIX environment, the command line should look similar to the following:

```
/WebSphere/PortalServer/bin/xmlaccess.bat -user wpsadmin -pwd itso -url
http://devportal.redbook.ibm.com:9081/wps/config -in ExportWelcomePage.xml
-out ExportedWelcomePage.xml
```

Regardless of whether the XML export works correctly, you will see an output file called ExportedWelcomePage.xml. If you open this file, the last line should

`display status element="all" result="ok" /`. If the export was unsuccessful, a error message appears to tell you what went wrong with the export.

5.3.3 Exporting and importing a new page

This section demonstrates very simply what is involved in moving a custom page from a staging to production environment.

Exporting

Using the same process describes in 5.3.2, “Exporting a sample page using XMLAccess” on page 119, you can export and then import a custom page from one Portal into another. In a staging or production environment, follow these steps:

1. Create a new blank page in your Portal.
2. Assign the blank page a unique name. You assign unique names to a Page via the Portal Administrative interface by selecting **Portal Settings** → **Custom Unique Names** and then selecting **Pages**. Find the page that you just created. Edit it and assign the page a meaningful custom unique name.

Important: Do not add any portlets to this page.

3. Create an XMLAccess input file following the instructions in 5.3.2, “Exporting a sample page using XMLAccess” on page 119. Give the page a unique name. You can copy the `ExportWelcomePage.xml` to `TestPage.xml`, and then change the `uniquename`.
4. Ensure that the `-out` parameter in the command line points to a new export file, for example `ExportedTestPage.xml`

Your command line may look something like this:

```
c:\WebSphere\PortalServer\bin\xmlaccess.bat -user wpsadmin -pwd itso -url
http://devportal.redbook.ibm.com:9081/wps/config -in ExportTestPage.xml
-out ExportedTestPage.xml
```

5. Run the export and ensure that you see the `status element="all" result="ok" /` message at the end of `ExportedTestPage.xml`.

Transferring

To transfer the file, copy (or FTP) the exported XML file (`ExportedTestPage.xml`) to the Production Portal Environment.

Importing

To import the file:

1. Prepare the XMLAccess import. The import is basically the same as the export except that you pass the exported output from the staging environment as the input for the production environment.

The XMLAccess input command line on UNIX may look like this:

```
/WebSphere/PortalServer/bin/xmlaccess.sh -user wpsadmin -pwd itso -url  
http://aixportal1.redbook.ibm.com:9081/wps/config -in ExportedTestPage.xml  
-out Results_ExportedTestPage.xml
```

2. Check the XML results by opening Results_ExportedTestPage.xml and check for the status element="all" result="ok"/ message. You may see warnings that the users and groups could not be retrieved from the Portal datastore if your LDAP environments are different between the staging and production environments.
3. Check that the page has been imported correctly by accessing the page in the Portal user interface via a Web browser.

5.4 A step-by-step guide

This section explains step-by-step how to move Portal artifacts from a staging to a production environment. It uses granular instructions so that you can follow the process whether you are moving all of the Portal artifacts or just updating some selected elements.

To follow these steps, we use worksheets and activity documents. When you move Portal artifacts, you should use the worksheets every time you transfer between environments.

5.4.1 Preparing the environment

Before your export or import Portal artifacts, we recommend that you prepare the transfer environment to reduce the chances of mistakes and to ensure that the Portal artifacts are exported to a easily identifiable location. Preparing the environment is not a compulsory step, but it is a best practice that we find works in a larger Portal deployment. Preparing the environment allows you to easily identify when artifacts were exported, so that you can revert back to the original files if needed.

Defining a naming standard

Ensure that you have defined a naming standard for the Portal artifacts as shown in Table 5-1.

Table 5-1 Example UniqueNames

	Default Install	HR	Accounting
Pages	wps.PageName	HR.pageName	Acc.pageName
Portlet applications	None	HR.portletName	Acc.portletName
Portlets	None	HR.Portlet	Acc.Portlet
URL mapping context	NA	HR.Url1	Acc.Url2
User groups	None	HR.GroupName	Acc.GroupName
Web modules	None	HR.AppName	Acc.AppName

You cannot assign unique names to skins, themes, and screens via the Portal Administration Interface. However, you can assign them using the XMLAccess tool. (For more information, see Chapter 4, “Solution deployment” on page 87.)

There is a sample file called DeployTheme.xml available online at the WebSphere Portal InfoCenter. Table 5-2 lists the unique names for skins, themes, and screens.

Table 5-2 Skins, themes, and screens UniqueNames

Skins	wps.skin.skinName	HR.skin.skinName	Acc.skin.skinName
Themes	wps.theme.themeName	HR.theme.themeName	Acc.theme.themeName
Screens	none	HR.screens01	Acc.screens01

Setting up a directory structure

You may want to export from the development or staging environments frequently. Unless you first set up the transfer environment correctly, you can easily lose an exported configuration or overwrite them.

To set up the environment correctly, create the directory structure shown in Figure 5-4 in the *wp root* directory.

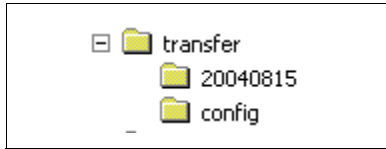


Figure 5-4 Subdirectories

You should create a transfer directory under *wp root* which will contain a config directory and a directory that represents the current date in *yyyymmdd* format.

The config directory contains XML files which list the actions to be performed in conjunction with the XMLAccess tool. The config directory also contains two scripts, one for exporting and one for importing.

The directory that represents the current date is where all the export scripts are run from on that date. All the exported XML files are written to this directory, allowing you to identify it easily in the future.

Setting up the XMLAccess script

The import and export scripts and batch files shown in the following example allow you to control how and where the exported XML files are written.

For Windows users:

```
c:\WebSphere\PortalServer\bin\xmlaccess.bat -user [Portal Admin User] -pwd
[Portal Admin User Password] -url [Source URL] -out exported%* -in
c:\WebSphere\PortalServer\transfer\config\%*
c:\WebSphere\PortalServer\bin\xmlaccess.bat -user wpsadmin -pwd itso -url
http://devportal.redbook.ibm.com:9081/wps/config -out exported_%* -in
c:\WebSphere\PortalServer\transfer\config\%*
qexport.sh (export for UNIX)
/WebSphere/PortalServer/bin/xmlaccess.sh -user [Portal Admin User] -pwd
[Portal Admin User Password] -url [Source URL] -out exported_$* -in
/WebSphere/PortalServer/transfer/config/$*
tail -n 3 exported_$*
```

For UNIX users:

```
/WebSphere/PortalServer/bin/xmlaccess.sh -user wpsadmin -pwd itso -url
http://devportal.redbook.ibm.com:9081/wps/config -out exported_$* -in
/WebSphere/PortalServer/transfer/config/$*
tail -n 3 exported_$*
```

The UNIX shell scripts also tails the resulting exported XML, so that you can determine if the XMLAccess tool was successful. Windows users need to open the file.

5.5 Preparing the worksheet

If you are performing the transfer from a staging to a production environment repeatedly, it is best to use worksheets and activity forms to fully document the process. These will allow administrators to delegate some of tasks.

5.5.1 Example worksheet

The example worksheet shown in Table 5-3 shows the values if you are transferring between a staging or development environment on Windows to a production environment on UNIX. This example illustrates the file structure in each environment.

Table 5-3 Example worksheet from Windows to UNIX

Description	Used by	Staging
Source server		portaldev.redbook.ibm.com
Transfer directory		C:\WebSphere\PortalServer\transfer
XML config location		C:\WebSphere\PortalServer\transfer\config
Shell scripts location		C:\WebSphere\PortalServer\transfer\config
Target directory		C:\WebSphere\PortalServer\transfer\ymmdd
Portal admin user		wpsadmin
Portal admin user password		itso
Source URL		portaldev.redbook.ibm.com:9081/wps/config
Skin source directory		C:\WebSphere\AppServer\installedApps\devportal\wps.ear\wps.war\skins\html
Theme source directory		C:\WebSphere\AppServer\installedApps\devportal\wps.ear\wps.war\themes\html
Screen source directory		C:\WebSphere\AppServer\installedApps\devportal\wps.ear\wps.war\screens\html

Description	Used by	Staging
Portlet source directory		C:\WebSphere\PortalServerdeployed\ *.war
Target server		portaltprod1.cmlconnect.org
Transfer directory		/WebSphere/PortalServer/transfer
Deployment Manager server		dmgrlin.redbook.ibm.com
Deployment Manager transfer directory		/DeploymentManager/transfer
XML config location		/WebSphere/PortalServer/transfer/config
Shell scripts location		/WebSphere/PortalServer/transfer/config
Source directory		/WebSphere/PortalServer/transfer/ yymmdd
Portal admin user		wpsadmin
Portal admin user password		itso
Target URL		linportal1.cmlconnect.org/wps/config
EAR operation server		dmgrlin.redbook.ibm.com
Portal admin user		wpsadmin
Portal admin user password		itso
EAR operation directory		/tmp/wps
Skin target directory		/tmp/wps_expanded/wps.war/skins/html
Theme target directory		/tmp/wps_expanded/wps.war/themes/html
Screen target directory		/tmp/wps_expanded/wps.war/screens/html

5.6 Run activities

This section detail the steps you need to perform to export a Portal configuration from one environment to the other. You should use a worksheet that is specific to your environment.

5.6.1 Verifying the prerequisites

There are a number of prerequisites that you need to meet before you move from one environment to the other. Use the following as a checklist to ensure that you are ready to begin:

- ▶ Complete a supporting worksheet. Environment information to support these activities is available in the Transfer Worksheet.
- ▶ Verify user access. The activities must be performed by an administrator. In a UNIX environment, ensure that you are using the same operating system as the user who owns the files.
- ▶ Run the XMLAccess commands as the Portal administrator. See the User Identities section of the Transfer Worksheet for more information.
- ▶ Confirm the supporting files and scripts.
- ▶ Verify that the XML config files are in the correct location as specified in the Setup section in the worksheet.
- ▶ Verify that the shell scripts are in the correct location as specified in the Setup section of the worksheet.
- ▶ Define all the unique names.

The instructions in the following sections detail how to export all elements of the Portal. If you need to refine the instructions for subsequent updates or if you need to import specific Portal artifacts, refer to the WebSphere Portal InfoCenter where there are a number of sample XMLAccess scripts provided for a various scenarios.

Table 5-4 includes the preliminary tasks you should perform.

Table 5-4 Prerequisites

Step	Instructions
Pre Req Check	Check the supporting files and scripts are in the locations specified in the worksheet. [XML Config Location] AdminPages.xml Pages.xml Portlets.xml Skins.xml Themes.xml [Shell Scripts Location] qexport.sh
Portal Admin User and Password	Update the qexport.sh in the scripts directory with the [Portal Admin User] [Portal Admin User Password] [Source URL]
Create a new bundle directory	Create a new bundle directory for this transfer. [Target Directory]

5.6.2 Using XMLAccess to export Portal artifacts

To export the Portal environment using the XMLAccess tool, follow these steps:

1. Create a new bundle directory for the transfer (the target directory). Then, from that directory, continue with the steps.
2. To export skins, run the following command:

```
qexport.sh Skins.xml
```

Substitute qexport.sh for qexport.bat if you are running in a Windows environment.

The result of this command should be:

```
<status element="all" result="ok"/> </request>
```

The results file, exported_Themes.xml, is written to the current directory.

3. To export themes, run the following command:

```
qexport.sh Themes.xml
```

Substitute qexport.sh for qexport.bat if you are running in a Windows environment.

The result of this command should be:

```
<status element="all" result="ok"/> </request>
```

The results file, `exported_Themes.xml`, is written to the current directory.

4. To export portlets, run the following command:

```
qexport.sh Portlets.xml
```

Substitute `qexport.sh` for `qexport.bat` if you are running in a Windows environment.

The result of this command should be:

```
<status element="all" result="ok"/> </request>
```

The results file, `exported_Portlets.xml`, is written to the current directory.

5. To export admin pages, run the following command:

```
qexport.sh AdminPages.xml
```

Substitute `qexport.sh` for `qexport.bat` if you are running in a Windows environment.

The result of this command should be:

```
<status element="all" result="ok"/> </request>
```

The results file, `exported_AdminPages.xml`, is written to the current directory.

6. To export pages, run the following command:

```
qexport.sh Pages.xml
```

Substitute `qexport.sh` for `qexport.bat` if you are running in a Windows environment.

The result of this command should be:

```
<status element="all" result="ok"/> </request>
```

The results file, `exported_Pages.xml`, is written to the current directory.

7. To export URLs, run the following command:

```
qexport.sh URLs.xml
```

Substitute `qexport.sh` for `qexport.bat` if you are running in a Windows environment.

The result of this command should be:

```
<status element="all" result="ok"/> </request>
```

The results file, `exported_URLs.xml`, is written to the current directory.

5.6.3 Bundling the supporting files

To bundle the supporting files in a single location outside of the Portal configuration, follow these steps:

1. Create the subdirectories from the target directory for each type of supporting file. For example, on UNIX:

- `mkdir skins`
- `mkdir themes`
- `mkdir screens`

On Windows:

- `md skins`
- `md themes`
- `md screens`

2. Copy the skin files from the skins source directory into the skins subdirectory. From the target directory, run the following commands for each skin to be transferred:

UNIX

```
cp -r [skin source directory] skins
```

Windows

```
xcopy /s [skin source directory] skins
```

3. Copy the theme files from the themes source directory into the themes subdirectory. From the target directory, run the following commands for each theme to be transferred:

UNIX

```
cp -r [theme source directory] themes
```

Windows

```
xcopy /s [skin source directory] themes
```

4. Copy the screen files from the screens source directory into the screens subdirectory. From the target directory, run the following command:

UNIX

```
cp [skins source directory] screens
```

Windows

```
xcopy [skins source directory] screens
```

5. Copy the installable portlet war files from the deployed portlets directory into the portlets subdirectory. From the target directory, run the following command:

UNIX

```
cp [portlet source directory] portlets
```

Windows

```
xcopy [portlet source directory] portlets
```

6. Bundle the target directory and all subdirectories into a single file for transfer to the target systems.

To do this in UNIX, run the following command from the target directory:

```
cd ..  
tar -cf yymmdd.tar Target Directory
```

This command creates a tar file at the same level as the target directory.

You can do the same thing in Windows with any file compression utility.

Whatever tool you use, it is important that you save the hierarchical directory structure. Save a the file yymmdd.zip at the same level as the target directory.

5.6.4 Transferring the bundle

To transfer the bundles to the target environment, follow these steps:

1. Create the target directory.
2. Create the following supporting files and scripts in the locations specified in the worksheet:

UNIX

```
qimport.sh
```

Windows

```
qimport.bat
```

3. Update the qimport.sh in the scripts directory with the Portal Admin User, Portal Admin User Password, and Target URL.
4. Copy the bundle.

FTP or otherwise transfer the tar file from the previous step to the transfer directory on the target server and, in the case of a cluster environment, the Deployment Manager Server.

5. Expand the bundle. Untar or extract the files as a subdirectory to the transfer directory, which creates a source directory.

UNIX

```
tar -xf yymdd.tar
```

Windows

Extract the files to the transfer directory. Be sure to save the directory hierarchy when you create a source directory.

5.6.5 Distributing the supporting files to a single server

To distribute the supporting files to their appropriate locations in the Portal installation, follow these steps.

Note: If you are deploying to a cluster, skip this section and go to 5.6.6, “Distributing the supporting files to a cluster” on page 132.

1. Copy the skin files from the skins source directory into the skins target directory.

2. From the source directory, run the following command.

UNIX

```
cp -r skins/* [skin target directory]
```

Windows

```
xcopy /s skins\* [skin target directory]
```

3. Copy the theme files from the themes source directory into the theme target directory.

4. From the source directory, run the following command.

UNIX

```
cp -r themes/* [theme target directory]
```

Windows

```
xcopy /s themes\* [theme target directory]
```

5. Copy the screen files from the screen source directory into the screen target directory.

6. From the source directory, run the following command.

UNIX

```
cp screens/* [screen target directory]
```

Windows

```
xcopy screens\* [screen target directory]
```

7. Copy the portlet .war install files from the portlets source directory into the portlet target directory.
8. From the source directory, run the following command.

UNIX

```
cp portlets/* [portlet target directory]
```

Windows

```
xcopy /s skins\* [portlet target directory]
```

5.6.6 Distributing the supporting files to a cluster

To distribute the supporting files to a clustered environment, follow these steps:

1. Export the WebSphere Portal EAR file from the Deployment Manager. The EAR file should be checked out into a temporary directory, such as C:\Temp on Windows 2000.
 - a. On the Deployment Manager node, DM01, change directories to the Deployment Manager's bin directory. For example, C:/WebSphere/DeploymentManager/bin.
 - b. Invoke the **wsadmin** command to export the file to a temporary directory (make sure all commands are entered on one line).

UNIX

```
./wsadmin.sh -user <admin_user_id> -password <admin_password> -c  
"$AdminApp export wps /tmp/wps.ear"
```

Windows

```
wsadmin.bat -user <admin_user_id> -password <admin_password> -c  
"$AdminApp export wps C:/temp/wps.ear"
```

- c. Create the /tmp/wps_expanded directory for UNIX or the C:\Temp\wps_expanded directory for Windows. Use the EARExpander

tool to expand the contents of the exported EAR file (make sure all commands are entered on one line).

UNIX

```
./EARExpander.sh -ear /tmp/wps.ear -operationDir /tmp/wps_expanded  
-operation expand
```

Windows

```
EARExpander.bat -ear C:\Temp\wps.ear -operationDir C:\Temp\wps_expanded  
-operation expand
```

2. Copy the skin files from the skins source directory into the skins target directory. From the source directory, run the following command.

UNIX

```
cp -r skins/* [skin target directory]
```

Windows

```
xcopy /s skins\* [skin target directory]
```

3. Copy the theme files from the themes source directory into the theme target directory. From the source directory, run the following command.

UNIX

```
cp -r themes/* [theme target directory]
```

Windows

```
xcopy /s themes\* [theme target directory]
```

4. Copy the screen files from the screen source directory into the screen target directory. From the source directory, run the following command.

UNIX

```
cp -r screens/* [skin target directory]
```

Windows

```
xcopy /s screens\* [skin target directory]
```

5. Place the updated themes and skins JSPs into the correct directory within the expanded EAR file.
6. Rebuild and update the WebSphere Portal EAR file in the Deployment Manager using the following steps:
 - a. Rename the old wps.ear file.

- b. Use the **EARExpander** command to collapse the EAR directory back into an EAR file:

UNIX

```
./EARExpander.sh -ear /tmp/wps.ear -operationDir /tmp/wps_expanded  
-operation collapse
```

Windows

```
EARExpander.bat -ear C:\Temp\wps.ear -operationDir C:\Temp\wps_expanded  
-operation collapse
```

- c. Use the **wsadmin** command to update the WebSphere Portal EAR file in the Deployment Manager. This action synchronizes the application across each node in the cluster.

UNIX

```
./wsadmin.sh -user <admin_user_id> -password <admin_password> -c  
"$AdminApp install /tmp/wps.ear {-update -appname wps}"
```

Windows

```
wsadmin.bat -user <admin_user_id> -password <admin_password> -c  
"$AdminApp install C:/Temp/wps.ear {-update -appname wps}"
```

Note: Updates to the configuration of a WebSphere Portal cluster must occur on the Deployment Manager and must be synchronized with the other nodes in the cluster. If updates are made to individual nodes in the cluster, the updates are lost when the master configuration on the Deployment Manager synchronizes with the nodes again.

Note: If you opened the wasadmin console, rather than using the command lines in these instructions, you need to save the revised configuration using the **\$AdminConfig save** command.

7. On the target node, copy the portlet .war install files from the portlet source directory into the portlet target directory. From the source directory, run the following command.

UNIX

```
cp portlets/* [portlet target directory]
```

Windows

```
xcopy /s skins\* [portlet target directory]
```

For additional considerations for deploying portlets in a cluster, see:

http://publib.boulder.ibm.com/pvc/wp/500/ent/en/InfoCenter/wpf/inst_cluster.html#deployport

5.6.7 Updating the target configuration

If you want to remove quickly all the existing Portlets from your target Portal, you can use the example script in Example A-4 “Delete_Portlets.xml script” on page 234. Keep in mind, however, that you need to import all the portlets from the staging environment successfully before you can access the target Portal again.

To update the configuration of the target Portal with the configurations that you exported from the source Portal via the XMLAccess tool, follow these steps from the source directory:

1. To import skins, run the following command:

```
qimport.sh exported_Skins.xml
```

Substitute qimport.sh for qimport.bat if you are running in a Windows environment.

The result of this command should be:

```
<status element="all" result="ok"/> </request>
```

The results file, result_exported_Skins.xml, is written to the current directory.

2. To import themes, run the following command:

```
qimport.sh exported_Themes.xml
```

Substitute qimport.sh for qimport.bat if you are running in a Windows environment.

The result of this command should be:

```
<status element="all" result="ok"/> </request>
```

The results file, result_exported_Themes.xml, is written to the current directory.

3. To import portlets, run the following command:

```
qimport.sh exported_Portlets.xml
```

Substitute qimport.sh for qimport.bat if you are running in a Windows environment.

The result of this command should be:

```
<status element="all" result="ok"/> </request>
```

The results file, result_exported_Portlets.xml, is written to the current directory.

4. To import admin pages, run the following command:

```
qimport.sh exported_AdminPages.xml
```

Substitute qimport.sh for qimport.bat if you are running in a Windows environment.

Note: You only need to perform this step once per environment or when you update the Admin Pages or portlets.

The result of this command should be:

```
<status element="all" result="ok"/> </request>
```

The results file, result_exported_AdminPages.xml, is written to the current directory.

5. To import pages, run the following command:

```
qimport.sh exported_Pages.xml
```

Substitute qimport.sh for qimport.bat if you are running in a Windows environment.

The result of this command should be:

```
<status element="all" result="ok"/> </request>
```

The results file, result_exported_Pages.xml, is written to the current directory.

6. To import URLs, run the following command:

```
qimport.sh exported_URLs.xml
```

Substitute qimport.sh for qimport.bat if you are running in a Windows environment.

The result of this command should be:

```
<status element="all" result="ok"/></request>
```

The results file, result_exported_URLs.xml, is written to the current directory.

5.7 Post transfer actions

This section details the tasks that you need to perform after you have successfully completed your last export.

5.7.1 Ensuring that the nodes are synchronized

In a clustered environment, ensure that you give the deployment manager sufficient time to synchronize with all nodes before you stop and restart the cluster. You can check the status via the user interface. However, monitoring the NodeAgent log on each node supplies detailed progress information. The NodeAgent SynchLog is located under the *was root/logs/nodeagent* directory. The log file is called SystemOut.log.

5.7.2 Restarting the server

If you have updated the following elements, then you need to restart the Portal for the changes to take effect:

- ▶ Skins
- ▶ Themes
- ▶ Screens

Skins, themes, and screens are added to the *wps.ear* file and are not re-initialized unless you restart the application. In a stand-alone environment, you need to stop and start the Portal server from the command line. In a clustered environment, you can stop and start the cluster from the Portal user interface, or you can issue a *RippleStart* from the user interface.

5.7.3 Activating the portlets

When you transfer and import portlets into a cluster, they are not automatically activated (see 4.3.2, “Installing the portlet” on page 95 for more detail).

In Appendix A, “Operation tools” on page 231 you can find a script that activates the portlets for you. If, however, you want to perform this task manually, follow these steps:

1. Synchronize the nodes via the Deployment Manager via the user interface or command line.
2. Start the Web application by activating the EAR file from the Deployment Manager.
3. Activate the portlets using the XMLAccess tool or the Portal user interface.

5.7.4 Making any manual changes

It is important to ensure that all the portlets in the production environment are configured for the production environment and not the staging environment. You need to make manual changes if you have transferred:

- ▶ Customized portlets
- ▶ Portal settings
- ▶ Collaborative portlets

Customized portlets

You can manually transfer customized portlets either a post transfer task or during the actual transfer. If you have any collaboration or ILWWCM portlets that are configured to point to servers in your development environment, these settings are still present in the portlets when they are transferred into the production environment via the XMLAccess tool.

You need to reconfigure the collaboration portlets via the Portal Administration interface to ensure that these portlets now point to the production environment. The same applies to Content Management portlets, ILWWCM portlets, and potentially any custom portlets that you have deployed.

If you would prefer to make these changes during the transfer process, you can edit the exported *_PortletName.xml* file and change references to the old environment.

Portal settings

You also need to transfer manually any changes made to global Portal settings. These may include:

- ▶ Any changes made to the *wpconfig.properties* file.
- ▶ Any changes that you have made to the Portal services configuration. The files that control the Portal services configuration are located in the *wps root/shared/app/config/services* file. Possible changes may include any changes made for Tivoli Access Manager and SiteMinder integration or caching.
- ▶ Company information within Portal. Changes here may include changing the banner text in your browser. These changes are located in the *war root/WEB-INF/classes/nls/engine.properties* file.

Collaborative components

When migrating Portal environments from the staging to the production environment, you need to reconfigure the collaborative components to ensure that the portlets are pointing the collaborative servers in the production

environment. The first time you transfer the collaborative portlets, test them to ensure that the production environment has been configured correctly for collaboration.

5.8 How does customization and the transfer process work?

This section illustrates why you should use XMLAccess to transfer a Portal. The most difficult step when transferring between environments is working out what gets stored where and what can I transfer. The following scenario illustrates what elements of the Portal environment you can export using the XMLAccess tool.

5.8.1 World clock scenario

We have the following two users who work in different time zones:

- ▶ Marcos Lohmann works in Brazil.
- ▶ Simon Fredrickson works in Australia.

Because the customization is not stored with the portlet, we need to export the world clock portlet using the sample shown in Example 5-1.

Example 5-1 Exporting the world clock portlet

```
<?xml version="1.0" encoding="UTF-8"?>
<request
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="PortalConfig_1.2.xsd"
  type="export">

  <portal action="locate">

    <!-- Export World Clock-->

    <!-- This Sample will export the World Clock based on it's default
unique name -->
    <web-app action="export" uniqueness="wps.WorldClock"/>

  </portal>
</request>
```

After you successfully export the portlet, examine the XML results. There is no reference to any of the users who have customized the portlet, because the customizations are stored with the page, not the portlet.

Now, export the page that contains this customized portlet. Because we added the world clock portlet to MyPortal page, the XML export configuration file looks like Example 5-2.

Example 5-2 The XML export configuration file

```
<?xml version="1.0" encoding="UTF-8"?>
<request
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="PortalConfig_1.2.xsd"
  type="export">

  <portal action="locate">

    <!-- Export Select My Portal Pages -->

    <!-- Start with the content Root page group -->
    <!-- Accounting Pages-->
    <content-node action="export" uniquename="wps.My Portal"
export-descendants="true"/>

  </portal>
</request>
```

The exported page shows where the customizations are stored. If you do a search for the username that customized the portlet, you see the settings for the customized portlet are stored at the end the output as part of the content node element.

For each customization of a portlet, there is *content node* element with its own set of attributes. Example 5-3 “Page customizations” on page 141 shows how the customized portlet is actually a derivative of the its parent, the world clock portlet.

Each customized portlet has its own object ID along with a reference to its parent and an object ID that represents it uniquely. However, there is not a separate WAR file deployed to the Portal server. This data is stored in the database. A new record is created for each customized portlet which maintains a reference in the database to its parent (in this scenario, t the object ID of the world clock). The XMLAccess tool’s ability to maintain object IDs is why you should use it to transfer between environments. If you maintain object IDs, then you maintain user customizations.

Example 5-3 is an extract of the page customizations for the two users from Brazil and Australia.

Example 5-3 Page customizations

Marcos Lohmann extract:

```
</content-node>
  <content-node action="update" active="true" allportletsallowed="true"
content-parentref="_6_082M600MBD0AH7I2_46 My Page" create-type="implicit"
derivation-parentref="_6_082M600MBD0AH7I2_46 My Page"
objectid="_6_082M600MBD0AH7I2_FM" skinref="undefined" themeref="undefined"
type="page">
  <access-control externalized="false"
owner="uid=mlohmnn,cn=users,ou=devportal,o=redbook" private="true"/>
  <component action="update" active="true" deletable="undefined"
maxsize="undefined" modifiable="undefined" movable="undefined"
objectid="_7_082M600MBD0AH7I2_P3" ordinal="undefined"
shadowref="_7_082M600MBD0AH7I2_P1" skinref="undefined" type="control"
width="undefined">
    <portletinstance action="update" handle=""
objectid="_5_082M600MBD0AH7I2_IR" portletref="_3_082M600MBD0AH7I2_50 World
Clock" shareref="_5_082M600MBD0AH7I2_IP">
      <parameter name="worldclock.localTimeZone" type="string"
update="set">P</parameter>
    </portletinstance>
  </component>
</content-node>
```

Simon Fredrickson extract

```
</content-node>
  <content-node action="update" active="true" allportletsallowed="true"
content-parentref="_6_082M600MBD0AH7I2_46 My Page" create-type="implicit"
derivation-parentref="_6_082M600MBD0AH7I2_46 My Page"
objectid="_6_082M600MBD0AH7I2_FL" skinref="undefined" themeref="undefined"
type="page">
  <access-control externalized="false"
owner="uid=sfredrickson,cn=users,ou=devportal,o=redbook" private="true"/>
  <component action="update" active="true" deletable="undefined"
maxsize="undefined" modifiable="undefined" movable="undefined"
objectid="_7_082M600MBD0AH7I2_P2" ordinal="undefined"
shadowref="_7_082M600MBD0AH7I2_P1" skinref="undefined" type="control"
width="undefined">
    <portletinstance action="update" handle=""
objectid="_5_082M600MBD0AH7I2_IQ" portletref="_3_082M600MBD0AH7I2_50 World
Clock" shareref="_5_082M600MBD0AH7I2_IP">
      <parameter name="worldclock.localTimeZone" type="string"
update="set">K1</parameter>
    </portletinstance>
  </component>
</content-node>
```

5.9 Troubleshooting and best practices

This section address some common issues, problems, and mistakes that can occur when using the XMLAccess tool to transfer between Portal environments.

5.9.1 Plan on a trial run

Start simple, and ensure that you can export and import individual Portal artifacts before doing a complete transfer of the staging environment to production. The exported XML files are not easy to read and interpret. Exporting and importing large amounts of data when testing can make it difficult to understand the output of the exports, which, in case of a failure, makes it even more difficult to determine why the imports failed.

5.9.2 Problems importing pages

Page imports fail if the portlets contained within them have not been imported correctly into the Portal. Sometimes, it is not clear exactly where the hierarchy the problem is. To help isolate the problem, import pages one layer at a time, or import separate branches one at a time. You also need to return to the staging environment and export just those pages or branches. Use the sample scripts in Appendix A, “Operation tools” on page 231 to export a page based on its unique name to ensure that you do not export all the pages under MyPortal.

5.9.3 Activate portlets

Ensure that the portlets are activated before you try to import pages. This is often overlooked in a clustered environment. Remember that there is a script to help with activating portlets provided in Appendix A, “Operation tools” on page 231.

5.9.4 Synchronize the cluster

Whenever you make changes to a cluster there is a risk that it may be come unsynchronized. If you are removing an EAR file to deploy screens, skins, and themes or deploying portlets and pages to a member of cluster so that it can be synchronized to all other nodes, you may find that you have to manually synchronize the cluster.

To synchronize the cluster, follow these steps:

1. Stop the cluster, node agents, and Deployment Manager from the System Administration panel of the Deployment Manager.

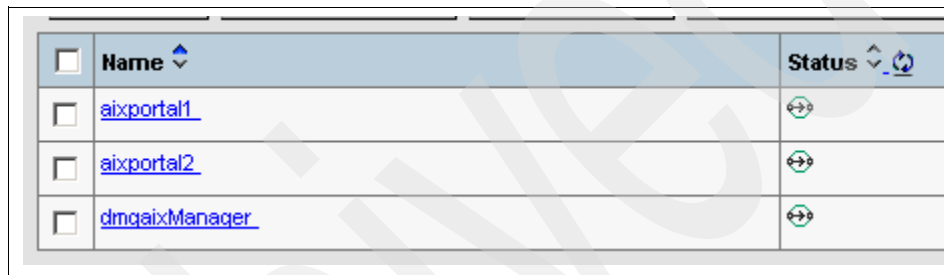
2. Manually synchronize the node agents with the Deployment Manager. From each of the nodes, go to the *was root/bin* directory and run the following:

```
syncNode dmgr_host [-username <uid>] [-password <pwd>]
```

In our environment the command looked like this:

```
./syncNode.sh dmgaix.redbook.ibm.com -username wasadmin -password itso
```

3. If the command is successful, start the node agents. If it is unsuccessful, synchronize the nodes without security (see 5.9.5, “Synchronize the nodes without security” on page 143).
4. Log into the Deployment Manager and ensure that all the nodes are synchronized as shown in Figure 5-5.



<input type="checkbox"/>	Name	Status
<input type="checkbox"/>	aixportal1	
<input type="checkbox"/>	aixportal2	
<input type="checkbox"/>	dmgaixManager	

Figure 5-5 Synchronized nodes

5. Start the Portal Cluster.

5.9.5 Synchronize the nodes without security

In the event that a manual synchronization of the node agents does not work, follow these steps to synchronize the Portal cluster without security. This process can eliminate any external security configuration influences that may affect a successful synchronization (for example, LDAP).

1. Log into the Deployment Manager Administration console.
2. Disable Global Security.

Click **Security** → **Global Security** and deselect the Enable Security radio button to disable Global Security.

3. Stop the cluster, node agents, and Deployment Manager from the System Administration panel of the Deployment Manager.
4. Manually synchronize node agents with the deployment manager. From each of the Nodes go to the *was root/bin* directory and run the following syncNode script:

```
syncNode dmgr_host [-username <uid>]
```

In our environment the command looked like this:

```
./syncNode.sh dmgaix.redbook.ibm.com
```

Note: There is no need to pass the username and password because you have disabled security via the Deployment Manager.

5. If successful, start the node agents.
6. Log into the Deployment Manager and ensure that all the nodes are synchronized.
7. Re-enable Global Security.

Click **Security** → **Global Security** and select the Enable Security radio button to enable Global Security.

Note: By default, this also enables Java 2 security. You do not want to enable Java 2 security. So, deselect the Java 2 security radio button to disable it.

8. Stop the node agents.
9. Stop Deployment Manager.
10. Manually synchronize the node agents with the Deployment Manager. From each of the nodes, go to the *was root/bin* directory and run the following syncNode script:

```
syncNode dmgr_host [-username <uid>] [-password <pwd>]
```

In our environment the command looked like this:

```
./syncNode.sh dmgaix.redbook.ibm.com -username wasadmin -password itso
```

11. If the script is successful, start the node agents.
12. Log into the Deployment Manager and ensure that all the nodes are synchronized.
13. Start the Portal Cluster.

This information is available from the WebSphere Portal InfoCenter at the following Web address:

<http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/wps/admxmlai.html>

Production procedures and administration activities

This chapter provides procedures to various administration tasks that may be required in a WebSphere Portal production environment. It describes possible approaches to solving WebSphere Portal issues that may arise in operational production environments.

6.1 Changing the host or domain name

This section describes the process for changing the domain name (or IP name) or host name of an operating WebSphere Portal V5.0 or later. You could use this procedure, for example, when a local network domain is reconfigured from `chicago.yourco.com` to `loop.chicago.yourco.com`. You can also use this procedure to reconfigure WebSphere Portal when you move a server from one location to another.

The WebSphere Application Server V5.0 configuration includes a `hostName` property in more than one configuration document. The value of the `hostName` property can be one of the following:

- ▶ A fully-qualified Domain Name System (DNS) host name string
- ▶ A short DNS host name string (the suggested value selected by a WebSphere Application Server V5.0 product install)
- ▶ Numeric IP address

There are advantages and disadvantages to any of the possible values. You should use a host name property value that best suites your needs.

The fully-qualified DNS host name has the advantage of being totally unambiguous and flexible. In this case, you can change the actual IP address for the host system without needing a WebSphere Application Server configuration change. This value for `hostName` is useful if you anticipate that you will change the IP address frequently, as is the case when you use Dynamic Host Configuration Protocol to assign IP addresses to host machines when they boot up. This value for `hostName` has the disadvantage of being dependent on the DNS. If DNS is not available, then connectivity is compromised.

The short host name is also dynamically resolvable. It has the advantage that you can redefine it in the local hosts file so that the system can run WebSphere even when disconnected from the network. If the short host name is resolved to `127.0.0.1` (local loopback) address in the hosts file for the system, then you can use WebSphere Application Server when disconnected from the network. This value for `hostName` also has the disadvantage of being dependent on DNS to work correctly when connected.

A numeric IP address has the advantage of not depending on DNS to function. The disadvantage is that it is a fixed address and must be altered in the WebSphere Application Server configuration files if the real system IP address is changed at any point.

The `hostName` property is given its value during product installation. You should take care during installation to select the `hostName` value that best suites the

situation in the WebSphere Application Server network environment. There is no feature in the browser-based admin console for WebSphere Application Server to modify the `hostName` property associated with a particular node. You can write a `wsadmin` script to modify the `hostName` property if necessary after installation.

You can use the following procedure to manually alter the `hostName` of a WebSphere Application Server or WebSphere Portal node. The procedure is valid for all versions of WebSphere Portal V5.0 or later.

The general approach to changing the host or domain name is:

- ▶ Update the network settings
- ▶ Stop the servers
- ▶ Update the Web server
- ▶ Update WebSphere Application Server
- ▶ Update WebSphere Portal

6.1.1 Assumptions

We made the following assumptions when writing this procedure:

- ▶ The domain name does not change on any back-end server that may be configured to WebSphere Portal, like an external database, LDAP, or Web server.
- ▶ The procedure does not cover how to change the host name of an external database, LDAP, or Web server.
- ▶ The user is familiar with WebSphere Application Server administration.

6.1.2 Step-by-step procedures

The following are the step-by-step procedures for changing host and domain names:

1. Update the host names in the operating system, DNS, and all other components in the infrastructure that are effected by this change.
2. Ensure that you have stopped all servers on the node. For example, stop the Web server, `server1`, and WebSphere Portal services.
3. Update the HTTP Server to handle the new host name correctly. Otherwise, the HTTP server will not accept requests with a different host name. While there are multiple ways to do this, the simplest way is to update the `ServerName` parameter in the `httpd.conf` file by following these steps:
 - a. Change to the `IBMHttpServer\conf\` subdirectory.
 - b. Make a backup copy of the `httpd.conf` file.

- c. Edit the file, and change the value of the `ServerName` to the new host name.

Note: Always perform `backupConfig` before making significant configuration changes.

4. In the `serverindex.xml` file for the node being modified, alter the value of the `hostName` property for the `ServerIndex` element in the file. Also, in the `serverindex.xml` file for the node being modified, alter the `host` property for every `EndPoint` in the file.
5. In each `server.xml` file on the node being modified, alter the `host` property everywhere it is used in the document.
6. Edit the `wsadmin.properties` file in the `properties` subdirectory under the installation root. Change the value of the `com.ibm.ws.scripting.host` property in that file to the new host address.
7. Edit the `orb.properties` file in the `java/jre/lib` subdirectory under the installation root. Change the value of the `com.ibm.CORBA.LocalHost` property in that file to the new host address.

Note: Always perform `backupConfig` before making significant configuration changes.

8. Execute the appropriate operating system command to change the name of the node directory (the subdirectory under `config/cells/cellname/nodes`) to the desired new node name.
9. Edit and alter the `node.xml` file in the node directory. Change the `name` property to the new node name value.
10. Edit and alter the `setupCmdLine` (.bat or .sh) file in the `bin` subdirectory. Change the `WAS_NODE` variable value to the new node name.
11. Edit the `security.xml` file in the cell directory. Change all occurrences of the old node name to the new one in that file. The node name should appear in the `security.xml` file as part of the `sslConfig` aliases defined in that file.
12. Edit the `deployment.xml` file under each installed application directory. Alter the `nodeName` property of the `deploymentTargets` element in that file to change the old node to the new node name.
13. Edit every `server.xml` file in server directories under this node. Change all occurrences of the old node name to the new node name. The node name in the `server.xml` file is usually part of an `sslConfig` alias (defined in the `security.xml` file previously edited).

14. Search all of the template files under the config/templates directory for any that contain the old node name value. Change all occurrences of the old node name in the config templates to the new name.
15. Drain down the messages on any Queues or Topics by running application code that processes all messages.
16. Run the **deletemq** utility to remove the message broker and queue managers that use the old node name.
17. Run **createmq** to recreate definitions using the new nodename.
18. Change the nodename on all the relevant Queue and Topic Connection Factories to the new nodename.
19. Change to the *PortalServer\shared\app\config\services* subdirectory.
20. Make a backup copy of the ConfigService.properties file.
21. Edit the ConfigService.properties file and remove the settings for:
 - host.name
 - host.port.http
 - host.port.https

This ensures that WebSphere Portal uses the host name in the incoming request to create response URLs which is needed where fully qualified URLs are required.

22. Start the Web server
23. Start Application Server server1.
 - a. Open a command prompt and change to the *was_root/bin* directory.
 - b. Enter the following command:

on UNIX:	./startServer.sh server1
on Windows:	startServer.bat server1
24. Start WebSphere Portal.
 - a. Open a command prompt and change to *was_root/bin* directory.
 - b. Enter the following command:

on UNIX:	./startServer.sh WebSphere_Portal
on Windows:	startServer.bat WebSphere_Portal

6.2 Changing database servers

During WebSphere Portal operations, there can be a number of reasons why you may need to port the external database server that the WebSphere Portal server is using to another database server. For example, you would need to change

database servers if you installed WebSphere Portal onto production boxes and then transferred the database from CloudScape to DB2 on Machine A. Machine A is the staging DB2 server. In this scenario, you might want to configure and build the production Portal while configured to the DB2 staging environment. Then, after you build the Portal production environment, you can port the DB2 database from the staging environment to the DB2 production environment on Machine B.

This section describes the process to change a working WebSphere Portal V5.0 server from the originally configured external database server to another database server on a different machine. This procedure work for both clustered and single node installations of WebSphere Portal.

The general approach to changing a database server is:

- ▶ Stop WebSphere Portal on the application server machine.
- ▶ Start the server1 application on the application server machine.
- ▶ Backup all WebSphere Portal databases.
- ▶ Restore the WebSphere Portal databases on the second database server.
- ▶ Reconfigure WebSphere Portal to use the databases on the second database server.
- ▶ Restart WebSphere Portal on the application server machine.

Note: Most likely, you will need assistance from an experienced DBA is to transfer Portal data from one database server to another.

6.2.1 Assumptions

We made the following assumptions when writing this procedure:

- ▶ The procedure only supports switching between homogenous database servers. Switching between unlike database servers is not supported.
- ▶ Two separate database servers are used in support of this procedure.
- ▶ Both database servers are loaded with the same version of the relational database software.
- ▶ The WebSphere Portal databases use the same names on both servers.
- ▶ The same user IDs and groups that are used to access the WebSphere Portal databases exist on both database servers and have the same database privileges.

- ▶ The WebSphere Portal databases are clones or exact copies, having been made by the native database, backup database, and restore database commands.
- ▶ Only off-line backups are employed.
- ▶ Availability of the Portal 24x7 is not required.

6.2.2 Moving from a DB2 database to a DB2 database

To switch from one DB2 database to another DB2 database, do the following:

1. The Database Client code on the WebSphere Portal server contains entries for the Database Server at Site A and the Database Server at Site B. These entries allow your client to move from one database site to another using the following commands:

```
db2 => catalog tcpip node SiteA remote SiteA.yourco.com server 50000 with
"Primary DB server"
db2 => catalog tcpip node SiteB remote SiteB.yourco.com server 50000 with
"Secondary DB server"
```

2. Catalog the WebSphere Portal databases that are on the Site A database server to the WebSphere Portal server using the following commands:

```
db2 => catalog database wps50 at node SiteA
db2 => catalog database wpcp50 at node SiteA
db2 => catalog database fdbk50 at node SiteA
```

3. To switch the between the database servers:

- a. Open a command prompt and navigate to the `was_root/bin` directory.
- b. Enter the following command:

```
on UNIX:      ./stopServer.sh WebSphere_Portal
on Windows:  stopServer.bat WebSphere_Portal
```

- c. Open a DB2 Universal Database™ Command Line window and uncatalog the WebSphere Portal databases at the WebSphere Portal server using the following commands:

```
db2 => uncatalog database wps50
db2 => uncatalog database wpcp50
db2 => uncatalog database fdbk50
```

4. At the primary database server, make a backup of the WebSphere Portal databases using the DB2 Universal Database backup database command.
5. Move the backup file to the second database server
6. Restore the WebSphere Portal databases using the DB2 Universal Database restore database command.

7. At the WebSphere Portal server, catalog the WebSphere Portal databases on the second database server using the following commands:

db2 => catalog database wps50 at node SiteB
db2 => catalog database wpcp50 at node SiteB
db2 => catalog database fdbk50 at node SiteB
8. Change to the *was_root/bin* directory, and enter the following commands:

on UNIX: **./startServer.sh WebSphere_Portal**
on Windows: **startServer.bat WebSphere_Portal**
9. Confirm the operation of WebSphere Portal with the databases on the new database server.

6.2.3 Moving from an Oracle database to an Oracle database

To switch from one Oracle database to another Oracle database, begin with these steps:

1. Open a command prompt and navigate to the *was_root/bin* directory.
2. Enter the following commands:

on UNIX: **./startServer.sh server1**
on Windows: **startServer.bat server1**

on UNIX: **./stopServer.sh WebSphere_Portal**
on Windows: **stopServer.bat WebSphere_Portal**
3. Backup all WebSphere Portal databases on the first database server using the export utility.
4. Move the .dmp file to the second database server.
5. Restore the WebSphere Portal databases on the second database server using the import utility.

Reconfiguring WebSphere Portal to use the databases on the second database server

To reconfigure WebSphere Portal to use the databases on the second database server, you first need to Access the WebSphere Application Server Administrative Console. Point your browser to `http://yourco.com:9090/admin`, where *yourco.com* is the name of the WebSphere Application Server node.

Then, in general for all data sources, follow these steps:

1. Navigate to the Custom Properties window under JDBC Providers.
2. Select the current host name in the URL parameter.
3. Change the Value parameter with the host name of the new database server.
4. Repeat these steps for all defined data sources.

The remainder of this section describes the procedure for specific data sources.

wps50DS data source

To reconfigure WebSphere Portal for the wps50DS data source:

1. Change the location of the wps50DS data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wps50JDBC** → **Data Sources** → **wps50DS** → **Custom Properties**.
2. Once at Custom Properties, click **URL** as shown in Figure 6-1.

<input type="checkbox"/>	URL	jdbc:oracle:thin:@oracle.yourco.com:1521:wps9i	This is a required prop indicating the databas Data Source will obtair as 'jdbc:oracle:thin:@loca
--------------------------	---------------------	--	--

Figure 6-1 URL value

3. Change the Oracle machine name in the Value text box as shown in Figure 6-2.

Value	<input type="text" value="jdbc:oracle:thin:@oracle.yourco.com"/>	<input type="checkbox"/> Value associated with this property in this property set.
-------	--	--

Figure 6-2 Edit URL value

4. Select **OK** to commit the change.

wmmDS data source

To reconfigure WebSphere Portal for the wmmDS data source:

1. Change the location of the wmmDS data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wps50JDBC** → **Data Sources** → **wmmDS** → **Custom Properties**.
2. Once at Custom Properties, click **URL** as shown in Figure 6-3.

<input type="checkbox"/>	URL	jdbc:oracle:thin:@oracle.yourco.com:1521:wps9i	This is a required prop indicating the database. Data Source will obtain as 'jdbc:oracle:thin:@loca
--------------------------	---------------------	--	---

Figure 6-3 URL value

3. Enter the host name of the new database server in the Value parameter as shown in Figure 6-4.

Value	<input type="text" value="jdbc:oracle:thin:@primary.yourco.co"/>	<input checked="" type="checkbox"/> Value associated with this property in this property set.
-------	--	---

Figure 6-4 Edit URL value

4. Select **OK** to commit the change.

feedbackDS data source

To reconfigure WebSphere Portal for the feedbackDS data source:

1. Change the location of the feedbackDS data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wps50JDBC** → **Data Sources (Version 4)** → **feedbackDS** → **Custom Properties**.
2. Once at Custom Properties select **URL** as shown in Figure 6-5.

<input type="checkbox"/>	Name ▾	Value ▾	Description ▾	Required ▾
<input type="checkbox"/>	URL	jdbc:oracle:thin:@oracle.yourco.com:1521:fdbk9i	This is the Oracle URL used for connecting to the database.	true

Figure 6-5 URL value

3. Enter the host name of the new database server in the Value parameter as shown in Figure 6-6.

Value	jdbc:oracle:thin:@oracle.yourco.com	Value associated with this property in this property set.
-------	-------------------------------------	---

Figure 6-6 Edit URL value

4. Select **OK** to commit the change.

persDS data source

To reconfigure WebSphere Portal for the persDS data source:

1. Change the location of the persDS data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wpcp50JDBC** → **Data Sources (Version 4)** → **persDS** → **Custom Properties**.
2. Once at Custom Properties, click **URL** as shown in Figure 6-7.

<input type="checkbox"/> URL	jdbc:oracle:thin:@oracle.yourco.com:1521:wp9i	This is a required prop indicating the databas Data Source will obtair as 'jdbc:oracle:thin:@loca
--	---	--

Figure 6-7 URL value

3. Enter the host name of the new database server in the Value parameter as shown in Figure 6-8.

Value	jdbc:oracle:thin:@primary.yourco.co	Value associated with this property in this property set.
-------	-------------------------------------	---

Figure 6-8 Edit URL value

4. Select **OK** to commit the change.

wcmDS Version 4 data source

To reconfigure WebSphere Portal for the wcmDS Version 4 data source:

1. Change the location of the wcmDS Version 4 data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wpcp50JDBC** → **Data Sources (Version 4)** → **wcmDS** → **Custom Properties**.

2. When you are at Custom Properties, click **URL** as shown in Figure 6-9.

<input type="checkbox"/> URL	<code>jdbc:oracle:thin:@oracle.yourco.com:1521:wp9i</code>	This is a required prop indicating the databas Data Source will obtair as <code>'jdbc:oracle:thin:@loca</code>
-------------------------------------	--	--

Figure 6-9 URL value

3. Enter the host name of the new database server in the Value parameter as shown in Figure 6-10.

Value	<code>jdbc:oracle:thin:@primary.yourco.co</code>	<input type="checkbox"/> Value associated with this property in this property set.
-------	--	---

Figure 6-10 Edit URL value

4. Select **OK** to commit the change.

Completing the change

To complete the switch to the second Oracle database server:

1. Save all changes.
2. Change to the `was_root/bin` directory, and enter the following command:
startServer WebSphere_Portal
3. Confirm the operation of WebSphere Portal with the databases on the new database server.

6.2.4 Moving from an SQLServer database to an SQLServer database

To switch from one SQLServer database to another SQLServer database:

1. Open a command prompt and change to the `was_root/bin` directory.
2. Enter the following commands:

on UNIX:	<code>./startServer.sh server1</code>
on Windows:	<code>startServer.bat server1</code>
on UNIX:	<code>./stopServer.sh WebSphere_Portal</code>
on Windows:	<code>stopServer.bat WebSphere_Portal</code>
3. Backup all WebSphere Portal databases on the first database server using the backup database command.

4. Move the backup file to the second database server.
5. Restore the WebSphere Portal databases on the second database server using the restore database command.

Reconfiguring WebSphere Portal to use the databases on the second database server

To reconfigure WebSphere Portal to use the databases on the second database server, you first need to Access the WebSphere Application Server Administrative console. Point your browser to `http://yourco.com:9090/admin`, where *yourco.com* is the name of the WebSphere Application Server node.

Then, in general for all data sources, follow these steps:

1. Navigate to the Custom Properties window under JDBC Providers.
2. Select the current host name in the `serverName` parameter.
3. Change the Value parameter with the host name of the new database server.
4. Repeat these steps for all defined data sources.

The remainder of this section describes the procedure for specific data sources.

wps50DS data source

To reconfigure WebSphere Portal for the wps50DS data source:

1. Change the location of the wps50DS data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wps50JDBC** → **Data Sources** → **wps50DS** → **Custom Properties**.
2. Once at Custom Properties, select the host name displayed in the value field of the `serverName` parameter as shown in Figure 6-11.

<input type="checkbox"/>	serverName	sqlserver1.yourco.com	This is a required property. The TCP/IP address of the SequeLink server in dotted format or host name format.	true
--------------------------	----------------------------	---------------------------------------	---	----------------------

Figure 6-11 *serverName* value

3. Enter the host name of the new database server in the Values parameter as shown in Figure 6-12.

Value	sqlserver2.yourco.com	<input type="checkbox"/> Value associated with this property in this property set.
-------	-----------------------	--

Figure 6-12 Edit serverName value

4. Select **OK** to commit the change.

wmmDS data source

To reconfigure WebSphere Portal for the wmmDS data source:

1. Change the location of the wmmDS data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wps50JDBC** → **Data Sources** → **wmmDS** → **Custom Properties**.
2. Once at Custom Properties, select the host name displayed in the value field of the serverName parameter as shown in Figure 6-13.

<input type="checkbox"/> serverName	sqlserver1.yourco.com	This is a required property. The TCP/IP address of the SequeLink server in dotted format or host name format.	true
---	---------------------------------------	---	----------------------

Figure 6-13 serverName value

3. Enter the host name of the new database server in the Values parameter as shown in Figure 6-14.

Value	sqlserver2.yourco.com	<input type="checkbox"/> Value associated with this property in this property set.
-------	-----------------------	--

Figure 6-14 Edit serverName value

4. Select **OK** to commit the change.

feedback5 data source

To reconfigure WebSphere Portal for the feedback5 data source:

1. Change the location of the feedback5 data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wpcp50JDBC** → **Data Sources** → **feedback5** → **Custom Properties**.

2. Once at Custom Properties, select the host name displayed in the value field of the serverName parameter as shown in Figure 6-15.

<input type="checkbox"/>	serverName	sqlserver1.yourco.com	This is a required property. The TCP/IP address of the SequeLink server in dotted format or host name format.	true
--------------------------	----------------------------	---------------------------------------	---	----------------------

Figure 6-15 serverName value

3. Enter the host name of the new database server in the Values parameter as shown in Figure 6-16.

Value	<input type="text" value="sqlserver2.yourco.com"/>	<input checked="" type="checkbox"/> Value associated with this property in this property set.
-------	--	---

Figure 6-16 Edit serverName value

4. Select **OK** to commit the change.

feedbackDS data source

To reconfigure WebSphere Portal for the feedbackDS data source:

1. Change the location of the feedbackDS data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wpcp50JDBC** → **Data Sources (Version 4)** → **feedbackDS** → **Custom Properties**.
2. When you are at Custom Properties, select the host name displayed in the value field of the serverName parameter as shown in Figure 6-17.

<input type="checkbox"/>	serverName	sqlserver1.yourco.com	This is a required property. The TCP/IP address of the SequeLink server in dotted format or host name format.	true
--------------------------	----------------------------	---------------------------------------	---	----------------------

Figure 6-17 serverName value

3. Enter the host name of the new database server in the Values parameter as shown in Figure 6-18 on page 160.

Value	sqlserver2.yourco.com	<input type="checkbox"/> Value associated with this property in this property set.
-------	-----------------------	--

Figure 6-18 Edit serverName value

4. Select **OK** to commit the change.

persDS data source

To reconfigure WebSphere Portal for the persDS data source:

1. Change the location of the persDS data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wpcp50JDBC** → **Data Sources (Version 4)** → **persDS** → **Custom Properties**.
2. Once at Custom Properties, select the host name displayed in the value field of the serverName parameter as shown in Figure 6-19.

<input type="checkbox"/> serverName	sqlserver1.yourco.com	This is a required property. The TCP/IP address of the SequeLink server in dotted format or host name format.	true
---	---------------------------------------	---	----------------------

Figure 6-19 serverName value

3. Enter the host name of the new database server in the Values parameter as shown in Figure 6-20.

Value	sqlserver2.yourco.com	<input type="checkbox"/> Value associated with this property in this property set.
-------	-----------------------	--

Figure 6-20 Edit serverName value

4. Select **OK** to commit the change.

wcmDS Version 4 data source

To reconfigure WebSphere Portal for the wcmDS Version 4 data source:

1. Change the location of the wcmDS Version 4 data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wpcp50JDBC** → **Data Sources (Version 4)** → **wcmDS** → **Custom Properties**.

- When you are at Custom Properties, select the host name displayed in the value field of the `serverName` parameter as shown in Figure 6-21.

<input type="checkbox"/>	serverName	sqlserver1.yourco.com	This is a required property. The TCP/IP address of the SequeLink server in dotted format or host name format.	true
--------------------------	----------------------------	---------------------------------------	---	----------------------

Figure 6-21 `serverName` value

- Enter the host name of the new database server in the Values parameter as shown in Figure 6-21.

Value	<input type="text" value="sqlserver2.yourco.com"/>	<input type="checkbox"/> Value associated with this property in this property set.
-------	--	--

Figure 6-22 Edit `serverName` value

- Select **OK** to commit the change.

Completing the change

To complete the switch to the second SQLServer database:

- Save all changes.
- Change to the `was_root/bin` directory, and enter the following commands:

on UNIX: `./startServer.sh WebSphere_Porta1`
 on Windows: `startServer.bat WebSphere_Porta1`
- Confirm the operation of WebSphere Portal with the databases on the new database server.

6.3 Changing LDAP servers

During WebSphere Portal operations, there can be a number of reasons why you may need to port the external LDAP server that the WebSphere Portal server is using to another LDAP server.

For example, you would need to change database servers if you installed WebSphere Portal onto production boxes and security has been configured to an IBM Directory Server on Machine A. Machine A is the staging IBM Directory Server server. In this scenario, you might want to configure and build the production Portal while configured to the IBM Directory Server staging

environment. Then, after you build the Portal production environment, you can port the IBM Directory Server LDAP from the staging environment to the IBM Directory Server production environment on Machine B.

This section describes the process to change a working WebSphere Portal V5.0 server from the originally configured LDAP database server to another LDAP server on a different machine. This procedure work for both clustered and single node installations of WebSphere Portal.

The general approach to changing an LDAP server is:

- ▶ Stop all servers, including Portal, server1, and, if clustered, dmgr and node agents.
- ▶ Make a file system backup of all nodes.
- ▶ Change the WebSphere Portal configuration.
- ▶ Start server1 or, if clustered, dmgr.
- ▶ Change the server1 or, if clustered, dmgr configuration.
- ▶ Restart server1 or, if clustered, dmgr.
- ▶ If clustered, manually synchronize each node.

Note: Most likely, you will need assistance from an experienced LDAP administrator to complete this process.

6.3.1 Assumptions

We made the following assumptions when writing this procedure:

- ▶ This procedure only supports switching between homogenous LDAP servers. Switching between unlike LDAP servers is not supported in this procedure.
- ▶ Two separate LDAP servers are used in support of this procedure.
- ▶ Both LDAP servers are loaded with the same version of the LDAP software.
- ▶ The following WebSphere Portal and WebSphere Application Server required users are set up with the same fully-qualified domain name, passwords, and permissions on both LDAP servers.
 - wpsadmin: Portal Admin user
 - wasadmin: WebSphere Application Server Admin user
 - wpsbind: LDAP bind user
 - cn=root: LDAP Admin user
- ▶ Only off-line backups are employed.
- ▶ Availability of the Portal 24x7 is not required.

6.3.2 Step-by-step procedure

For the purpose of illustration, this example includes an additional user in the new LDAP named switchldap to visually confirm that the Portal was configured to the new LDAP.

To switch from one LDAP server to another LDAP server, do the following:

1. Verify the list of users in the current LDAP using the Portal user interface by selecting **Portal** → **Administration** → **Access** → **Users and Groups**. Select all authenticated Portal users as shown in Figure 6-23.

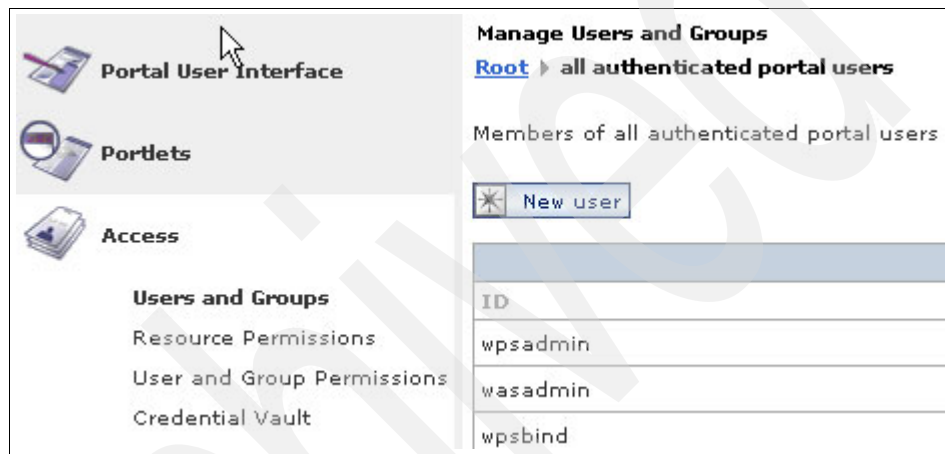


Figure 6-23 User list in original LDAP

2. Stop all servers and make a backup of the file system for all nodes.
 - Stop WebSphere Portal, or if clustered, stop the cluster through the Deployment Manager Administrative Console.
 - If clustered, stop node agents through the Deployment Manager Administrative Console.
 - Stop server1 or, if clustered the Deployment Manager, via the command line:

```
/was_root/bin/stopserver server1 -user <wasadmin> -password <wasadmin password>
```
 - Make file system backup of all nodes. See 6.4, “Backup and recovery” on page 167 for details about making a backup.
3. After backups are complete and the servers are stopped, open the `/wps_root/shared/app/wmm/wmm.xml` file and edit the following properties:
 - ldapHost
 - ldapPort

Additionally, in most cases the LDAP Admin ID and password are not the same value on the production LDAP server as on the staging LDAP server. If the LDAP Admin ID or password are different, edit the following properties as well:

- adminId
- adminPassword

To edit the adminPassword value, you must first encrypt the password using the wmm encryption tool. To do so, following these steps:

- From a command prompt, navigate to the *wp_root/config/work/wmm/bin* directory, where *wp_root* is the WebSphere Portal installation path.
- Encrypt the new password by entering the appropriate command, where *new_password* is the new password

on UNIX: `./wmm_encrypt.sh new_password`

on Windows: `wmm_encrypt.bat new_password`

The script returns a value for the ASCII encrypted string.

- Open the *wp_root/shared/app/wmm/wmm.xml* file with a text editor.
- Copy the value from the ASCII encrypted string and place it in the adminPassword field of the wmm.xml file.

Note: If the wmm.xml file is clustered, you need to edit it on each Portal node in the cluster as shown in the following example:

```
<ldapRepository name="wmmLDAP"
    UUID="LDAP1"

adapterClassName="com.ibm.ws.wmm.ldap.sunone.SunOneDirectoryAdapterImpl"
    supportDynamicAttributes="false"

configurationFile="/WebSphere/PortalServer/wmm/wmmLDAPServerAttributes.xml"
    wmmGenerateExtId="false"
    supportGetPersonByAccountName="true"
    profileRepositoryForGroups="LDAP1"
    supportTransactions="false"
    adminId="cn=Directory Manager"
    adminPassword="nCUIaY4HxqWpLbEQudsXA=="
    ldapHost="new_ldap.redbook.ibm.com"
    ldapPort="389"
    ldapTimeOut="6000"
    ldapAuthentication="SIMPLE"
    ldapType="0"
    groupCacheRefreshInterval="-1">
```

4. Configure the server1 Administrative Console or, if clustered, the Deployment Manager Administrative Console for the new LDAP server by following these steps:
 - a. Start server1 or, if clustered the Deployment Manager, via the command line.
 - b. Navigate to **Security** → **User Registries** → **LDAP**.
 - c. Edit the Host and Port fields as shown in Figure 6-24.

The screenshot shows a 'Configuration' window with a 'General Properties' tab. It contains a table with LDAP configuration fields and their descriptions.

General Properties		
Server User ID	* uid=wasadmin,ou=People,ou=linuxcl	i The user ID under which the server will execute (for security purposes).
Server User Password	* ****	i The password corresponding to the serverId.
Type	Custom	i The type of LDAP server being connected to.
Host	* new_server.redbook.ibm.com	i Specifies LDAP server host name.
Port	389	i Specifies LDAP server port.
Base Distinguished Name (DN)	ou=linuxcluster,p=redbook	i The base distinguished name of the directory service, indicating the starting point for LDAP searches of the directory service.
Bind Distinguished Name (DN)	uid=wpstbind,ou=People,ou=linuxclus	i The distinguished name for application server to use to bind to the directory service.

Figure 6-24 LDAP values

- d. Click **Apply**.
 - e. Click **Save**.
 - f. Click **Save** and make sure the Synchronize with Nodes check box is checked if clustered.
 - g. Click **Logout**.
5. Stop and Start server1 or, if clustered, the Deployment Manager from the command line.

Note: Steps 6 through 10 are only required in clustered environments:

6. Access the Administrative Console from a browser and login. This login is now using your new LDAP server settings.

7. Manually synchronize all Portal nodes by issuing the following command.

AIX

```
/<wsas_root>/bin >./syncNode.sh dmgrlin.redbook.ibm.com -username  
<wsas_admin_id> -password <password>
```

Windows

```
\<wsas_root>\bin>syncNode.bat dmgrlin.redbook.ibm.com -username  
<wsas_admin_id> -password <password>
```

This step is critical to clean the old LDAP server host name info from the node agent and Deployment Manager configuration. If you miss this step, you will see errors in the node agent SystemOut.log

8. After the manual synchronize is complete, start the node agents on each node from the command line.
9. After node agents have started, verify the Nodes are synchronized using the DM AdminConsole.
10. Use the Deployment Manager Administrative Console to verify that the node agents are running.
11. Start WebSphere Portal or, if clustered, use the Deployment Manager Administrative Console to start the cluster.
12. Verify the new list of users is in the current LDAP using the Portal user interface by selecting **Portal** → **Administration** → **Access** → **Users and Groups**. Select all authenticated Portal users as shown in Figure 6-25 on page 167.

Note: Notice the test user, switchldap, that was created in the new LDAP is now listed. This confirms that the Portal is configured to the new LDAP.

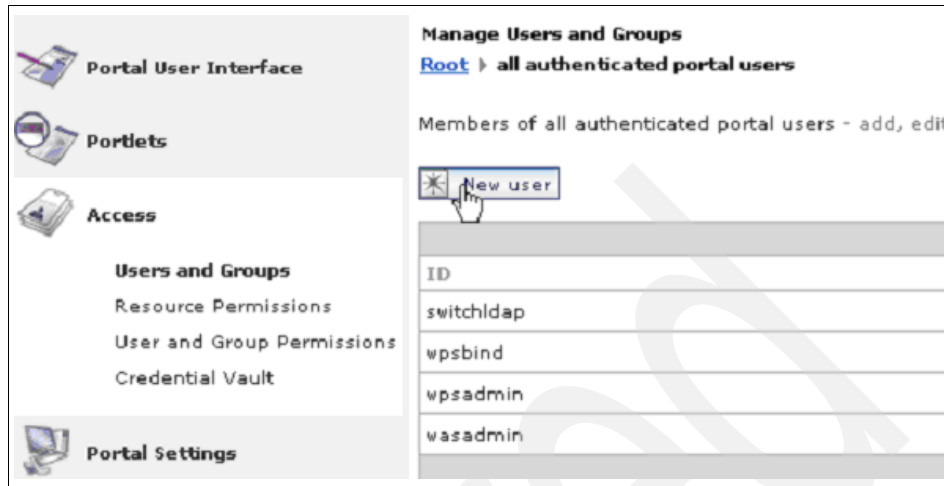


Figure 6-25 User list in new LDAP

13. To further check the new configuration, attempt to install a portlet.

6.4 Backup and recovery

A complete and thoroughly tested backup and recovery procedure is essential for any production environment. WebSphere Portal is no different. You should develop complete disaster recovery strategies and approaches and test those procedures in a testing environment. Once verified, you should implement these same procedures in the WebSphere Portal production environment.

This section does not detail a step-by-step process for backup and recovery. Rather, it provides insight into an approach for WebSphere Portal backup and recovery that you can implement into your existing disaster recovery procedures.

6.4.1 Overview of our approach to backup and recovery

The approach described in this section implements full system backups while maintaining 24x7 operations. The approach consists of stopping a percentage of the clustered nodes and then taking file system backups of the WebSphere Application Server and WebSphere Portal root directories while the Portal nodes and node agents are stopped. The remaining clustered nodes continue to operate and maintain the 24x7 operations.

After the backups are complete on the first group of Portal nodes, those nodes are brought back online in the cluster, another group of nodes are stopped, and the process is repeated. We recommend taking backups while the nodes are down to avoid incomplete backups because the server opens files while the backups are taking place.

Software tools may exist that allow complete backups to be made while files are open, but this section does not discuss these tools. If you wish to implement these types of tools, you can adjust the approach appropriately.

The general outline of the approach is:

- ▶ Stop a group of Portal nodes in the cluster.
- ▶ Take a file system backup of the stopped nodes.
- ▶ Start the nodes.
- ▶ Stop another group of nodes in the cluster.
- ▶ Take a file system backup of the stopped nodes.
- ▶ Start the nodes.
- ▶ Repeat this process until all nodes have been stopped and file system backups are taken of each node.
- ▶ Stop the Deployment Manager node.
- ▶ Take a file system backup of the Deployment Manager node.
- ▶ Take a database backup of all the databases associated with WebSphere Portal.
- ▶ Restart the Deployment Manager.

Important note about XMLAccess

XMLAccess does not play a part in our recommended backup and recovery approach. XMLAccess is not a tool that is designed for full backup and recovery purposes. XMLAccess is a tool designed for deploying Portal artifacts from one Portal environment to another Portal environment. For example, you can use XMLAccess to move Portal artifacts from your staging environment into your production environment once the Portal configuration has been thoroughly tested in the staging environment.

While XMLAccess does have features that can play a role in some backup and recovery situations, you should not rely on an XMLAccess export in a disaster recovery scenario. Thus, we have left XMLAccess out of the discussion for WebSphere Portal disaster recovery to avoid giving a false impression of the tool's capabilities.

For more information about XMLAccess and its features, see Chapter 4, “Solution deployment” on page 87 and Chapter 5, “Moving from staging to production” on page 111.

6.4.2 Our approach to backup

We recommend the following approach to backup:

1. Determine the time of day when the maintenance window takes place, preferably when the load on the cluster is the lowest.
2. Based on your environment, determine the fewest number of Portal nodes that are required to handle the load during this maintenance window.
3. Based on the length of your maintenance window and the minimum number of Portal nodes required to handle the load, determine the architecture of your backup procedure.

For example, if you have a maintenance window of two hours for a 10 node cluster, you will need a minimum of three Portal nodes up to meet the average load requirements for this time period. If you assume that you can backup the file systems in 30 minutes, you can then break the backup into two sections. Bring down five Portal nodes, take backups, and then bring them back online. Then, take down the other five nodes and take backups. This is the quickest approach in a 24x7 environment, because you have divided your backup process into two sections. However, if you have a nine node cluster and the load requires six nodes to be up, then you will have to divide it into three sections. Depending on the speed of your backup process, you might need to extend the maintenance window in this situation.

For this example, we divide the backups into two sections of five nodes each.

4. Stop the individual Portal application servers on nodes 1 through 5 using the Deployment Manager Administrative Console.
5. Stop the node agents for nodes 1 through 5 using the Deployment Manager Administrative Console.
6. Make sure no servers are running on nodes 1 through 5 by using the `serverStatus.sh/bat` command or by checking for running Java processes.
7. Take file system backups on each node, 1 through 5, of the WebSphere Application Server and WebSphere Portal root directories.
8. Start node agents through the command line on nodes 1 through 5 after file system backups are complete.
9. Synchronize the nodes through the Deployment Manager Administrative Console.

10. Start the individual Portal Application Servers on nodes 1 through 5 through the Deployment Manager Administrative Console.
11. Stop the individual Portal Application Servers on nodes 6 through 10 using the Deployment Manager Administrative Console.
12. Stop the node agents for nodes 6 through 10 using the Deployment Manager Administrative Console.
13. Make sure no servers are running on nodes 6 through 10 by using the **serverStatus.sh/bat** command or by checking for running Java processes.
14. Take file system backups on each node, 6 through 10, of the WebSphere Portal and WebSphere Application Server root directories.
15. Start node agents through the command line on nodes 6 through 10 after file system backups are complete.
16. Synchronize the nodes through the Deployment Manager Administrative Console.
17. Start the individual Portal Application Servers on nodes 6 through 10 through the Deployment Manager Administrative Console.
18. Stop the Deployment Manager server through the command line.
19. Take file system backups on the Deployment Manager node of the WebSphere Deployment Manager root directory.
20. Make online database backups of the WebSphere Portal databases using the backup tools associated with the database server used in your environment.
21. Once file system backups and database backups are complete, start the Deployment Manager server from the command line.

6.4.3 Our approach to recovery

Use backups made from the same day to restore the WebSphere Portal environment, follow these steps for recovery:

1. Delete the WebSphere Portal and WebSphere Application Server directories from each node. Also delete the WebSphere Deployment Manager directory from the Deployment Manager node.
2. Restore the WebSphere Portal and WebSphere Application Server directories on each node from their own backups. Also restore the WebSphere Deployment Manager directory on the Deployment Manager node.
3. Restore the Portal databases from the database backups.
4. Start the nodeagents on each Portal node.
5. Start the Deployment Manager server on the Deployment Manager node from the command line.

6. Synchronize the nodes via the Deployment Manager Administrative Console using the Full Synchronize option.
7. Start the cluster using the Deployment Manager Administrative Console.

Once again, these steps are not meant to provide a detailed step-by-step procedure but rather an approach to implementing a backup and recovery procedure for WebSphere Portal. You can automate many of these steps using scripts. Complete and reliable backups are critical. However, each backup plan is very specific to the environment. Thus, this general approach outlines the basic requirements for a full WebSphere Portal backup and recovery plan.

6.4.4 Backup and recovery for Windows systems

This section lists the that we suggest for backup and restore of WebSphere Portal V5 on Windows 2000/XP/2003.

Assumptions

Prior to executing the backup steps, we assume that WebSphere Portal V5.0 or later has been installed using the standard installation process. You can configure the Portal can to use an external Web server, a database server, or an LDAP server.

Important notes before you begin

Before you begin a back up or recovery process on Windows, note the following:

- ▶ WebSphere Portal does not have an undo or rollback facility.
- ▶ In the process of configuring WebSphere Portal, you might need to undo a configuration step.
- ▶ Without a rollback facility, the only way to back out a change is to uninstall WebSphere Portal, reinstall, and begin the configuration again. This process can take as much as two to three hours.
- ▶ The charts included in this section present an alternative method to recovering from a bad configuration step without having to uninstall and reinstalling. This alternative method can reduce the time for recovery from hours to minutes.
- ▶ The process creates a backup image that is restored on same machine where it is created and at same release level of WebSphere Portal.
 - Restoring to another machine not supported.
 - Switching between release levels is not supported.

Off-line backup process

To implement an off-line backup process:

1. Stop all WebSphere Application Server and WebSphere Portal services.
2. Stop the Web server if it is installed and running on the same machine.
3. Compress the \WebSphere\AppServer directory using compression software.
4. Compress the \WebSphere\PortalServer directory using compression software.
5. Compress the \IBMHTTPServer directory using compression software.
6. If an external database server is used, then backup the Portal databases using the native backup database commands.
If an external LDAP server is used, then back it up using the native backup commands.
7. Restart Web server, WebSphere Application Server, and WebSphere Portal.

Off-line recovery process

To implement an off-line recovery process:

1. Stop all WebSphere Application Server and WebSphere Portal services.
2. Stop the Web server if it is installed and running on the same machine.

Optional: Delete the \WebSphere\AppServer, \WebSphere\PortalServer, and \IBMHTTPServer directories.

3. Extract the WebSphere Application Server backup file to the \WebSphere\AppServer directory.
4. Extract the WebSphere Portal backup file \WebSphere\PortalServer directory.
5. Extract the Web server \IBMHTTPServer directory.
6. If an external database server is used, then restore the Portal databases using the native restore database commands.
If an external LDAP server is used, then restore it the native restore commands.
7. Restart Web server, WebSphere Application Server, and WebSphere Portal.

Notes

- ▶ The process assumes that the code is installed on the same system where the backup was taken. No restoring backups on different machines.
- ▶ This assumes WebSphere Application Server, WebSphere Portal, and IBM HTTP Server has been installed in the indicated directories. If not, then substitute your own.
- ▶ This assumes IBM HTTP Server is used. If not, then use what ever you have.
- ▶ The compression software can be PKZIP, WinZip, tar, or whatever you like.
- ▶ The AppServer and PortalSever subdirectories need to be compressed into separate files due to their size.
- ▶ The portal databases and LDAP servers can be and should be backed up in parallel with the AppServer and PortalServer subdirectories.
- ▶ The creation of the backups is I/O and CPU bound, but it takes about 30 to 40 minutes to complete.
- ▶ Restoration of the backups is I/O and CPU bound, but it takes about 20 minutes to complete.

This is all it takes to do an off-line backup and restore of WebSphere Portal V5.0 or later on Windows systems. We tested this procedure on Windows, Linux, and AIX systems, and it has worked every time.

Recommendation: Take backups after the initial install when WebSphere Portal is using Cloudscape and after you have configured WebSphere Portal to use the external database and LDAP servers.

Application of backup and recovery

We recommend the following for backup and recovery:

- ▶ Perform a backup after every major installation step. It will save time.
- ▶ If you cannot perform a back after every major installation step because of time or resource constraints, then backup after the initial install and before federating into cell if clustering.
 - A Cloudscape install is a backup of last resort.
 - Backup prior to federation, because most problems happen during federation.

- ▶ Make backup copies of the wpconfig.properties file. In fact, make multiple copies and keep them in multiple places.
 - It takes time to configure the file correctly. Once done, you do not want to do it again.
 - Make a copy after every major configuration (Database server, LDAP server, Web server, and so on).
 - If all else fails, you can restore from the Cloudscape based backup, replace the default wpconfig.properties file, and rerun the configuration tasks. The entire process is scriptable.

6.5 Maintaining a healthy Portal environment

Keeping the WebSphere Portal production environment as up-to-date and healthy as possible is the goal of every IT department. However, a production WebSphere Portal clustered environment can be complicated and can contain many different pieces of software. Thus, it can be a challenge to keep up with all the tasks necessary to maintain a production environment.

This section provides some approaches, information, and tools for the Portal administrator that can help maintain the WebSphere Portal environment.

6.5.1 Scheduling regular backups

An adequate and reliable backup strategy should be a part of every WebSphere Portal environment. Taking regular backups increases the health of the production environment by decreasing the amount of time required to fully recover the Portal environment on the event of a disaster.

The frequency that backups are taken varies based on the nature of the Portal environment. The more mature the Portal environment (meaning less updates to the Web applications or Portal configuration), the less frequent a full backup is needed. The more frequently you make changes to the Portal environment, then the more frequently you need full backups. When making the decision on the frequency of backups, consider how much time you are willing to spend redeploying from staging to production to recreate your Portal after recovering from the full backup.

We recommend full backups before you apply any big changes, such as maintenance, Web application updates, and so on, to the Portal environment.

For one approach to a complete WebSphere Portal backup and recovery strategy, see 6.4, “Backup and recovery” on page 167.

6.5.2 Reviewing log files

You should review and inspect log files regularly to catch issues quickly and to familiarize yourself with the logs and their layout. Some of the more common runtime logs and their typical locations are:

- ▶ Deployment Manager Logs
 - Located on the Deployment Manager node.
 - *dmgr_root/logs/dmgr*
 - SystemOut.log
 - SystemErr.log
 - You set trace from the Deployment Manager Administrative Console by selecting **Troubleshooting** → **Logs and Trace**. The default trace file location is *wsas_root/logs/servername/trace.log*. You can change the file location through the Deployment Manager.
- ▶ NodeAgent Logs
 - Located on each Portal node that has been federated into Deployment Manager control.
 - *wsas_root/logs/nodeagent*
 - SystemOut.log
 - SystemErr.log
 - You set trace from the Deployment Manager Administrative Console by selecting **Troubleshooting** → **Logs and Trace**. The default trace file location is *wsas_root/logs/servername/trace.log*. You can change the file location through the Deployment Manager Administrative Console.
- ▶ Portal log locations for first Portal node
 - Located on each Portal node
 - *wps_root/log*
 - SystemOut.log
 - SystemErr.log
 - *wps_timestamp.log*
- ▶ Portal log locations for each Portal node federated into Deployment Manager control after the initial Portal node (for example, Node2, Node3, and so on)
 - Located on each Portal node. (This is the default log location. You can change value by editing WebSphere Application Server variables through the Deployment Manager Administrative Console.)
 - *wsas_root/logs/servername*
 - SystemOut.log
 - SystemErr.log

- *wps_root/log*
 - *wps_timestamp.log*
- You can enable trace by editing the TraceString property in the log.properties file in the *wps_root/shared/app/config* directory. The trace writes to the *wps_timestamp.log* file
- ▶ WebSphere Application Server Logs
 - Located on each WebSphere Application Server node
 - *wsas_root/logs*
 - activity.log
 - serverStatus.log
 - wsadmin.traceout
 - addNode.log - for clusters
 - removeNode.log - for clusters
 - syncNode.log - for clusters
 - You can set trace through the Deployment Manager Administrative Console by selecting **Troubleshooting** → **Logs and Trace**. The default trace file location is *wsas_root/logs/servername/trace.log*. You can change the file location through the Deployment Manager Administrative Console.

Note: After federating a WebSphere Application Server node into Deployment Manager, control of the server1 is no longer used. Therefore, all WebSphere Application Server logging takes place through the Deployment Manager. However, as noted, the log locations may still exist on the individual WebSphere Application Server nodes.

You can find examples of the log files in Appendix G, “Additional material” on page 277.

6.5.3 Applying fixes

Fixes are released regularly for WebSphere Portal and published to the Web. To stay current with fixes that may affect your environment, it is best to create a My Support profile. You can customize a My Support profile to alert you automatically when new fixes are available. For instructions on how to customize your My Support profile, see:

<http://www-1.ibm.com/support/docview.wss?uid=swg21159292>

A common approach is to keep the applied fixes in the update directory on the node for ease of reapplication if necessary.

Most fixes can be applied while clustered. Refer to the readme file for the specific fix for any clustered specific considerations.

Always make sure you have the most current version of the Portal Update Installer. Search the WebSphere Portal Support Web for the most current version:

<http://www-306.ibm.com/software/genservers/portal/support/>

6.5.4 Getting support

When you encounter an issue with your Portal environment, you can contact WebSphere Portal Support for assistance with your troubleshooting. To speed up the resolution to your issue, do the following:

- ▶ Have access to FTP.

The easiest and quickest way to send logs to WebSphere Portal Support is to use FTP. Support has a FTP server set up to receive your files. To speed the resolution time, have FTP installed and configured so that you can send the log files. FTP is the preferred method. Sometimes the log files can be very large and many times email servers have a size limitation for attachments.

- ▶ Remote Access Services (RAS) Tool

WebSphere Portal Support provides a tool to make it easy for customers to send the log files to support. The RAS tool is a Java command that you can run from the command line. This tool automatically collects the logs that Support requires to begin looking into your issue. The tool not only collects the logs, but it also compresses the logs into one file.

After you decide you need to open a support ticket, run this tool and have the zipped file ready to send. When Support receives these logs, they begin an in depth investigation into the issue.

To collect logs and send them to Support, run the RASUtils.jar file to collect the log files. You can get the RASUtils.jar from the following link:

<http://www-1.ibm.com/support/docview.wss?uid=swg24005648>

The RASUtils.txt file contains the instructions on how to run the RASUtils.jar file. The results are a zipped file named WPRASCollect.zip. After you collect the log files, you are ready to open a support ticket with WebSphere Portal Support.

- ▶ How and when to contact support

For tips to make your support experience more efficient and to receive a more timely resolution to your issue, see:

<http://www-106.ibm.com/developerworks/websphere/zones/portal/portal10steps.html>

6.5.5 Using basic troubleshooting techniques

Troubleshooting in a WebSphere Portal environment can be very complicated. Sometimes following a structured method can be very helpful. Consider the following questions when you begin troubleshooting:

- ▶ When did it last work correctly? What has changed in the environment since that time?
- ▶ Can you isolate the problem? Can you reduce the number of variables that could be the cause of the problem?
- ▶ Can the problem be reproduced on demand?
- ▶ Have you checked the `wpconfig.properties` for mis-typed or incorrect values?

6.5.6 Using roadmaps

For details about the WebSphere Portal Roadmap and links that can be valuable for administering or troubleshooting the Portal, see:

<http://www-106.ibm.com/developerworks/websphere/zones/portal/roadmaps/>

6.6 On Demand clustering solutions

The concept of On Demand architecture and availability is a very powerful and cost effective alternative for doing business. WebSphere Portal can meet your On Demand needs and provide the appropriate resources where needed, at precisely the time needed.

The scenario in this section describes a procedure where a company running multiple WebSphere Portal clusters can add and remove Portal nodes, into and from clusters, as business requires. For example, the Accounting Cluster contains five Portal nodes and the Human Resources Cluster contains four Portal nodes. At the end of the year the Accounting cluster demands more capacity, while the Human Resources is under utilized during the same time period. The obvious solution is to move some capacity from the Human Resources cluster to the Accounting cluster.

This scenario describes how to remove nodes from an under-utilized cluster and add that capacity to the cluster that demands more resources, all while maintaining 24x7 operations on both clusters.

The general approach of this scenario is:

- ▶ Stop the cluster node on Cluster A.
- ▶ Remove the node from Cluster A.
- ▶ Edit the `wpconfig.properties` file on the removed node from Cluster A.
- ▶ Disable global security through the Deployment Manager Administrative Console on the removed node, if required.
- ▶ Run the `connect-database` task.
- ▶ Run the `enable-security-ldap` task, if required.
- ▶ Apply and required maintenance, if required.
- ▶ Run `addNode.sh` to add the node to Cluster B.
- ▶ Configure the node into Cluster B.

Details of the Scenario

In this scenario:

- ▶ Cluster A is configured to Oracle and SunOne LDAP.
- ▶ Cluster B is configured to DB2 and IBM Directory Server LDAP.
- ▶ Cluster A contains three Portal nodes as shown in Figure 6-26 on page 180.

[Server Cluster](#) > [linCluster](#) >

Cluster members

An application server that belongs to a group of servers called a cluster. 

Total: 3

 Filter

 Preferences

[New](#) [Delete](#) [Start](#) [Stop](#)



<input type="checkbox"/>	Member name 	Node 	Status  
<input type="checkbox"/>	WebSphere Portal	linportal1	
<input type="checkbox"/>	WebSphere Portal 2	linportal2	
<input type="checkbox"/>	WebSphere Portal 3	aixportal2	

Figure 6-26 Clustered nodes list from Cluster A


- Cluster B contains one Portal node as shown in Figure 6-27.


[Server Cluster](#) > [aixcluster](#) >

Cluster members

An application server that belongs to a group of servers called a cluster. 

Total: 1

 Filter

 Preferences

[New](#) [Delete](#) [Start](#) [Stop](#)






<input type="checkbox"/>	Member name 	Node 	Status  
<input type="checkbox"/>	WebSphere Portal1	aixportal1	

Figure 6-27 Clustered nodes list from Cluster B

6.6.1 Step-by-step of the On Demand procedure

The step-by-step instructions are as follows:

1. Stop the cluster member through the Deployment Manager Administrative Console on Cluster A by selecting **Servers** → **Clusters** → **cluster_name** → **Cluster Members**. Figure 6-28 will appear. Select the desired Cluster member and click **Stop**.

Server Cluster > linCluster >

Cluster members

An application server that belongs to a group of servers called a cluster. ⓘ

Total: 3

⊞ Filter

⊞ Preferences

New Delete Start Stop

<input type="checkbox"/>	Member name ▾	Node ▾	Status ▾ ↻
<input type="checkbox"/>	WebSphere_Portal	linportal1	➡
<input type="checkbox"/>	WebSphere_Portal_2	linportal2	➡
<input type="checkbox"/>	WebSphere_Portal_3	aixportal2	✖

Figure 6-28 Stop desired cluster member

2. After the cluster node is stopped, use the Deployment Manager Administrative Console to remove the cluster member by selecting **System Administration** → **Nodes**. Check the desired node and click **Remove Node** as shown in Figure 6-29 on page 182.

Nodes

A list of nodes in this cell. You can add new nodes into the cell by clicking on "Add Node" and specifying a remote Server instance. [i](#)

Total: 4

☐ Filter

☐ Preferences

<input type="checkbox"/>	Name	Status
<input checked="" type="checkbox"/>	aixportal2	
<input type="checkbox"/>	dmgrlinManager	
<input type="checkbox"/>	linportal1	
<input type="checkbox"/>	linportal2	

Figure 6-29 Select desired node to remove from cluster

- After selecting the node, you should be prompted for the WebSphere Application Server admin ID as shown in Figure 6-30.

[Nodes](#) >

Remove Node

Removing a node will cause the node to be immediately removed from the master configuration repository workspace until you login to the console again.

Click the OK button to remove the following nodes, or click the Cancel button to return to the prior page.

- [aixportal2](#)

User ID	<input type="text" value="wasadmin"/>	Because security is enabled, you must enter a user WebSphere instance to communicate with the deplo
Password	<input type="password" value="****"/>	The password for the user ID entered above

Figure 6-30 Supply ID and password for node removal

4. After the node is removed, you should see the message shown in Figure 6-31.

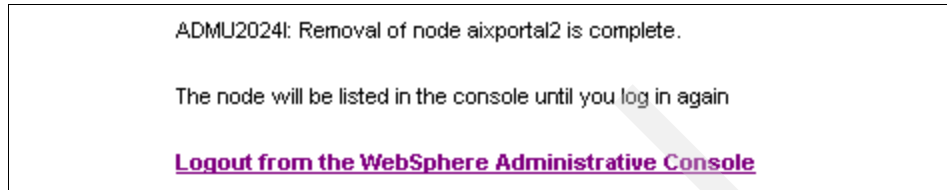


Figure 6-31 Successful node removal message

5. Log out and login to the Deployment Manager Administrative Console on Cluster A. Verify the cluster members by selecting **Servers** → **Clusters** → **cluster name** → **Cluster Members** as shown in Figure 6-32.



Figure 6-32 Clustered nodes list from Cluster A after removal

6. Run RippleStart on Cluster A by selecting **Servers** → **Clusters**. Select the Cluster, and click **RippleStart** as shown in Figure 6-33 on page 184.

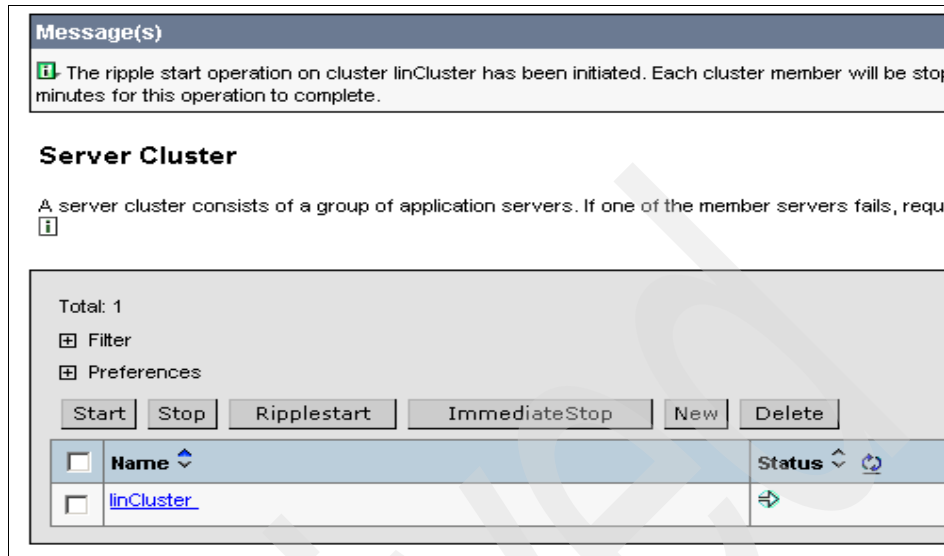


Figure 6-33 Run RippleStart of Cluster A

7. Regenerate plugin and move to Web server.
8. The cluster member just removed is now removed from the management of the Deployment Manager on Cluster A, but it is still configured to the production database and LDAP on Cluster A. Edit the wpconfig.properties file on the removed node to reflect the values for the production database and LDAP on Cluster B. Refer to the WebSphere Portal InfoCenter for the list of properties to edit for database and LDAP. Cross-reference those lists with a copy of a wpconfig.properties file from a node that is already in Cluster B. Also, ensure that the value of WpsHostName is the fully qualified name of the Portal machine and that the value of WpsHostPort is 9081.

Note: Make sure a Virtual Host Alias exists for port 9081. Click **Environment** → **Virtual Host Alias**. If 9081 does not exist, add it.

Also, when adding or removing nodes from a cluster, you should regenerate the Web server plugin and reconfigure the Web server after each node is added or removed.

If Cluster A and Cluster B are configured with the same LDAP settings then step 9 on page 185 and step 12 are not required.

9. Use the WebSphere Application Server server1 Administrative Console to manually disable security on the node just removed from Cluster A by following these steps:
 - a. Start server1 from the command line.
 - b. Render the WebSphere Application Server Administrative Console from a browser and login.
 - c. Click **Security** → **Global Security**. Deselect the Enabled box as shown in Figure 6-34.

Global Security

Specifies global security configuration for a managed domain. The following steps are required to turn from the left navigation panel and set the properties in that panel. 2) Enable security in this panel. [i](#)

Configuration

General Properties	
Enabled	<input type="checkbox"/>
Enforce Java 2 Security	<input type="checkbox"/>
Use Domain Qualified User IDs	<input type="checkbox"/>
Cache Timeout	* 600

Figure 6-34 Disable global security

- d. Click **Apply**.
- e. Save the changes and logout.
- f. Stop server1 from the command line.

Note: The remaining steps describe an approach that is basically identical to the normal addition of another WebSphere Portal node into a cluster. Refer to the WebSphere Portal InfoCenter for specific instructions.

10. Validate the settings in the wpconfig.properties file using the WPSconfig.sh/bat script as follows:

```
validate-ldap
validate-database-connection-wps
validate-database-connection-wpcp
validate-database-connection-wmm
```

11. Run the connect-database task to connect the Portal server to the production database for Cluster B using the WPSconfig.sh/bat script.
12. Use the WPSconfig.sh/bat script to run the enable-security-ldap task.
13. Apply or remove any maintenance (for example, fixpacks, fixes, and so on) that are required to bring the node to the same level of the nodes in Cluster B. You should apply fixes and fixpacks that require the node to be removed from the Deployment Manager at this time.

14. Run the addNode.sh script to federate the node into the Deployment Manager Administrative Console for Cluster B as follows.

```
Windows: <was_root>\bin\addNode.bat <deployment_manager_host>
<deployment_manager_port> -username <admin_user_id> -password
<admin_password>
UNIX: <was_root>/bin/addNode.sh <deployment_manager_host>
<deployment_manager_port> -username <admin_user_id> -password
<admin_password>
```

In this example:

- *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 and is required if security is enabled.
 - *admin_password* is the administrative user password. This parameter is optional and is required if security is enabled.
15. Add the node into Cluster B by selecting **Servers** → **Cluster** and clicking **New**. The window shown in Figure 6-35 on page 187 appears. Complete the fields in this window to establish the new cluster.

Create New Cluster Members

Create New Cluster Members

→ **Step 1 : Enter Basic Cluster Members Information**

Select the node where the new application server will reside.

Member name	WebSphere_Portal2
Select node	aixportal2 ▼
Weight	2
Http Ports	<input type="checkbox"/> Generate Unique Http Ports

Apply

Edit Delete

☐ **Application Servers**

Next Cancel

Figure 6-35 Add new cluster member to Cluster B

16. Configure the node for the cluster by first editing the `wpconfig.properties` file as follows:

- CellName: *dmgrNetwork cell name*
- ServerName: *node server name within cluster*

17. Edit the `DeploymentService.properties` file as follows:

- `wps.appserver.name`: *cluster name*

18. Regenerate plugin and move to Web server.

19. Run `RippleStart` on Cluster B.

20. Enable session persistence, if required.

6.7 Temporarily removing a clustered node to apply maintenance

In some cases, you might need to remove a Portal node temporarily from a cluster to apply or perform maintenance. Some WebSphere Portal and WebSphere Application Server fixes require that the node be removed from the cluster before applying the fix. Refer to the readme file for the specific fix to determine if you should remove the node.

Note: Many fixes support the application of the fix to each node while they remain clustered.

There may be other scenarios where temporarily removing a Portal node from the cluster is required. This section describes the steps that are required to temporarily remove a node from a cluster and then add the node back in a 24x7 environment.

Note: We recommend an adequate backup and recovery plan before performing major configuration changes.

6.7.1 Step-by-step procedure to temporarily remove a clustered node

To temporarily remove a clustered node:

1. Stop the cluster member from the Deployment Manager Administrative Console by selecting **Servers** → **Clusters** → **cluster_name** → **Cluster Members**. Select the desired Cluster and click **Stop** as shown in Figure 6-36 on page 189.

[Server Cluster](#) > [linCluster](#) >

Cluster members

An application server that belongs to a group of servers called a cluster. ⓘ

Total: 3

⊕ Filter

⊕ Preferences

New Delete Start Stop

<input type="checkbox"/> Member name	Node	Status
<input type="checkbox"/> WebSphere_Portal	linportal1	
<input type="checkbox"/> WebSphere_Portal_2	linportal2	
<input type="checkbox"/> WebSphere_Portal_3	aixportal2	

Figure 6-36 Stop desired cluster member

- After the cluster node is stopped, use the Deployment Manager Administrative Console to remove the cluster member by selecting **System Administration** → **Nodes**. Select the desired node and click **Remove Node** as shown in Figure 6-37.

Nodes

A list of nodes in this cell. You can add new nodes into the cell by clicking on "Add Node" and specifying a remote Server instance. ⓘ

Total: 4

⊕ Filter

⊕ Preferences

Add Node Remove Node Synchronize Full Resynchronize Stop

<input type="checkbox"/> Name	Status
<input checked="" type="checkbox"/> aixportal2	
<input type="checkbox"/> dmgrlinManager	
<input type="checkbox"/> linportal1	
<input type="checkbox"/> linportal2	

Figure 6-37 Select node to be removed

3. After clicking Remove Node, you should be prompted for the WebSphere Application Server admin ID as shown in Figure 6-38.

[Nodes](#) >

Remove Node

Removing a node will cause the node to be immediately removed from the master configuration repository workspace until you login to the console again.

Click the OK button to remove the following nodes, or click the Cancel button to return to the prior page.

- aixportal2

User ID	<input type="text" value="wasadmin"/>	Because security is enabled, you must enter a user WebSphere instance to communicate with the depla
Password	<input type="password" value="****"/>	The password for the user ID entered above

Figure 6-38 Supply ID and password from node removal

4. After the node is removed, you should the message as shown in Figure 6-39.

ADMU2024I: Removal of node aixportal2 is complete.

The node will be listed in the console until you log in again

[Logout from the WebSphere Administrative Console](#)

Figure 6-39 Node successfully removed message

5. Log out and login to the Deployment Manager Administrative Console. Verify the cluster members by selecting **Servers** → **Clusters** → **cluster_name** → **Cluster Members** as shown in Figure 6-40 on page 191.

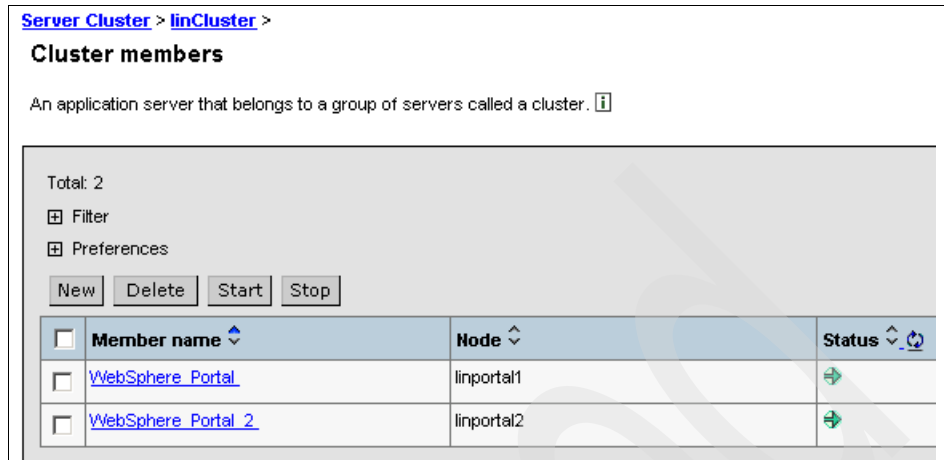


Figure 6-40 Clustered nodes list

- Run RippleStart by selecting **Servers** → **Clusters**. Check the Cluster and click **RippleStart** as shown in Figure 6-41.



Figure 6-41 Perform RippleStart

- The cluster member just removed is now removed from the management of the Deployment Manager, but it is still configured to the cluster's production database and LDAP.

8. Apply the maintenance required by following the specific instructions supplied with the fix.

In general, you should:

- Place the fix into the *wps_root/update/fixes* or *fixpacks* directory.
- Make sure you have the current Portal Update Installer.
- Stop the WebSphere Portal node using the Deployment Manager Administrative Console.
- Change the following properties in the *wpconfig.properties* file to contain the correct values for the Node as it exists outside the cluster:
 - *CellName*: *cell name* (default value is *machine_hostname*)
 - *ServerName*: *node server name* (default value is *WebSphere_Portal*)
- Run the Portal Update installer to apply the fix. The readme file for the fix includes the command syntax.

9. After applying the maintenance, run the *addNode.sh* script to federate the node back into the cluster's Deployment Manager Administrative Console as shown in the following example:

```
Windows: <was_root>\bin\addNode.bat <deployment_manager_host>
<deployment_manager_port> -username <admin_user_id> -password
<admin_password>
UNIX: <was_root>/bin/addNode.sh <deployment_manager_host>
<deployment_manager_port> -username <admin_user_id> -password
<admin_password>
```

In this example:

- *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 and is required if security is enabled.
- *admin_password* is the administrative user password. This parameter is optional and is required if security is enabled.

10. Add the node into the cluster by selecting **Servers** → **Cluster** and clicking **New**. The window shown in Figure 6-42 on page 193 appears. Complete the fields in this window to establish the new cluster.

Create New Cluster Members

Create New Cluster Members

→ **Step 1 : Enter Basic Cluster Members Information**

Select the node where the new application server will reside.

Member name	WebSphere_Portal2
Select node	aixportal2 ▼
Weight	2
Http Ports	<input type="checkbox"/> Generate Unique Http Ports

Apply

Edit Delete

☐ **Application Servers**

Next Cancel

Figure 6-42 Add node back into cluster.

11. Configure the node for the cluster by editing the wpconfig.properties file:
 - CellName: *dmgrNetwork cell name*
 - ServerName: *node server name within cluster*
12. Run RippleStart on the cluster.
13. Check to make sure the nodes are synchronized by selecting **System Administration** → **Nodes** from the Deployment Manager Administrative Console.

6.8 Monitoring the Portal

For information about monitoring Portal activity, see Appendix F, “A portal manager for WebSphere Portal” on page 275.

A high availability illustration

This chapter describes a procedure for performing minor maintenance on a clustered IBM WebSphere Portal V5.0 installation. The procedure described here is designed to permit installation of minor software fixes such as database fixpacks, WebSphere Application Server interim fixes, software point releases, and so on while maintaining 24x7 availability of the Portal.

This chapter does not cover upgrades to the directory server. See the appropriate documentation from the provider of the directory server product for instructions on installing software fixes. This process does involve a number of significant database operations. We recommended that you work closely with the DBA.

7.1 The sample cluster production environment

The procedure assumes a clustered WebSphere Application Server (hereafter called Application Server) and WebSphere Portal staging or production clustered environment similar to Figure 7-1. The procedure is designed to work with WebSphere Application Server V5.0.1, which was shipped with WebSphere Portal V5.0. While we developed the procedure for the second fixpack of WebSphere Portal V5.0.2, we tested this procedure with subsequent interim fixes and fixpacks. It works with all supported databases.

In Figure 7-1, DM01 is the Deployment Manager instance. WP01 and WP02 are WebSphere Portal instances running on Application Server.

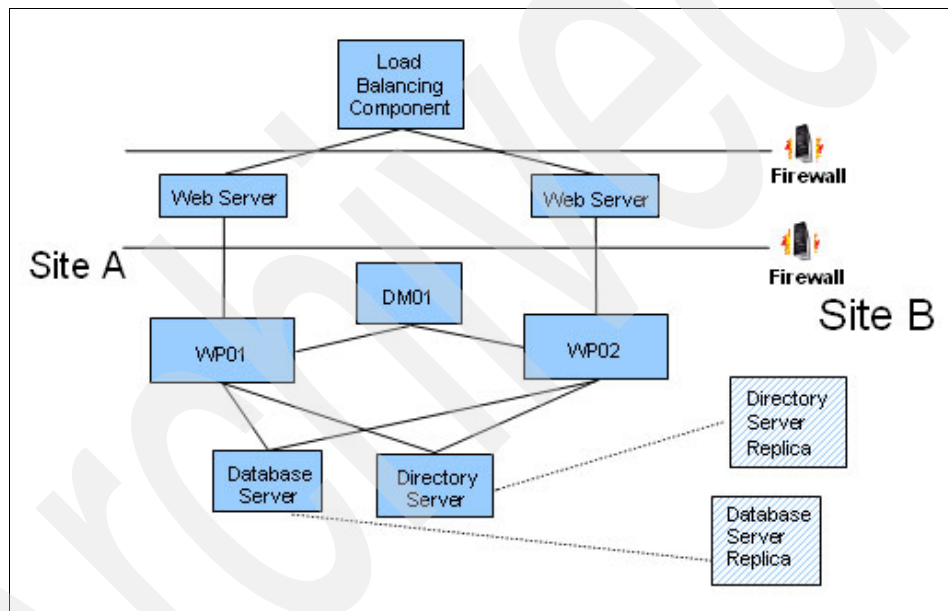


Figure 7-1 Sample cluster production environment

You could also follow this procedure with integration and test cluster topologies.

7.2 Before you begin the procedure

The task flow in this procedure is as follows:

1. Remove Site B from the cluster while Site A takes the full user load.
2. Upgrade Site B with the new interim fixes or fixpacks.
3. Route traffic to Site B while Site A is upgraded.
4. Merge the two sites back into the original cluster.

You see how to install fixpacks and interim fixes on the Web server, WebSphere Application Server, WebSphere Portal, and the database server. If you do not need to install any fixpacks or interim fixes on a particular server, you can skip the corresponding step.

The order and exact nature of the installation of the Web Server, WebSphere Application Server, and WebSphere Portal fixpacks can vary depending upon which versions of the various software products you are upgrading. Consult the installation instructions for the exact order in which any fixpacks should be installed.

Verify that your WebSphere environment contains the required hardware and software supported by the cumulative fix to be installed. The supported hardware and software requirements are available at:

<http://www.ibm.com/websphere/portal/library>

Make sure you have the required WebSphere Application Server interim fixes installed for the version of WebSphere Application Server you are running. You can download the latest WebSphere Application Server interim fixes from:

<http://www.ibm.com/websphere/support>

7.3 Assumptions

Before starting the procedure, ensure that:

- ▶ Site A is considered to be the primary site. The primary WebSphere Portal node is the first WebSphere Portal node that was added to the cell, typically through the use of the `-includeapps` parameter on the **addNode** command in WebSphere Application Server.
- ▶ Portal databases (wps50, wpcp50, and fdbk50) are replicated from Site A to Site B, using native database replication facilities or database backup and restore commands.
 - Database replication configuration is not covered in this procedure.
 - You decide the best way to implement this requirement.

- ▶ The Portal databases are not replicated from Site B to Site A. Only one way replication is in use.
- ▶ The WebSphere Portal database schemas do not change during this process.
- ▶ The team executing these commands has the cooperation and assistance of the DBA team.
- ▶ The directory server data is replicated between Site A and Site B using the facilities available in the respective directory server product.
 - Installation and configuration of the directory servers and their replication is not covered in this procedure.
 - You decide the best way to implement this requirement.
- ▶ During the maintenance procedure, the Portal databases are put into read-only mode.
 - Any edits on portlets or Portal pages are disallowed by the users of the Portal. The Portal administrator(s) can still edit portlets and Portal pages, but you risk losing any changes.
 - If a particular installation of WebSphere Portal does not allow the users to edit portlets or Portal pages, then you do not need to put the Portal into read-only mode.
 - The process for putting a Portal into read-only mode does not need to be completed if a particular installation of WebSphere Portal is willing to lose any edits completed by the end users while Site A is under going maintenance.
 - You decide the best way to implement this requirement.
- ▶ The IP sprayer directs all incoming traffic to either Site A or Site B.
- ▶ The HTTP servers route traffic within their sites only.
- ▶ Session persistence is enabled.

7.4 Initial production state

Initial production state is where this process begins and ends. Both WP01 and WP02 are running in production (Figure 7-2), using both the database server and the directory server. The database server at Site A is periodically replicated to a backup database server at Site B.

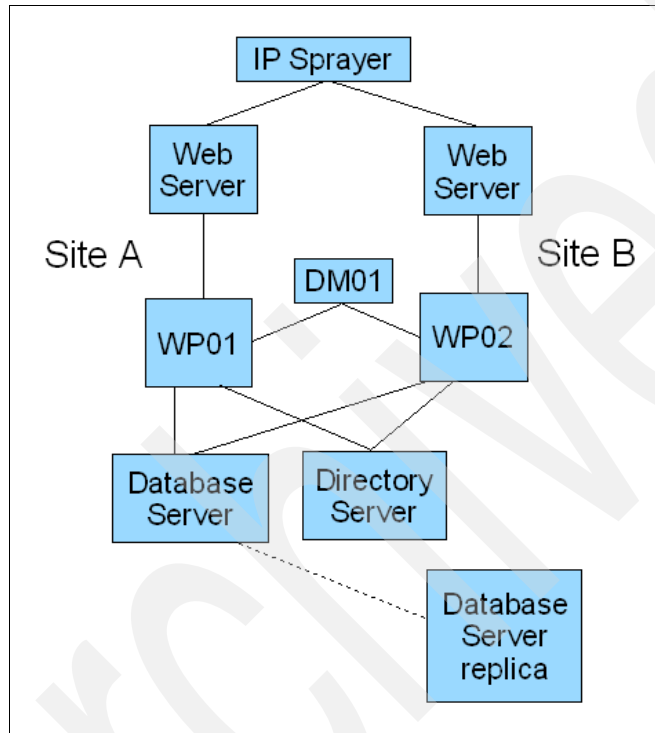


Figure 7-2 Operational production clustered environment

To begin the process, follow these steps:

1. Configure IP Sprayer to route IP traffic to both Site A and Site B.
2. Replicate the WebSphere Portal databases (wps50, wpcp50, and fdbk50) from Site A to Site B.
3. Site A is considered the primary site, because it was federated into the Deployment Manager using the `-includeapps` option.

7.5 Remove Site B from cluster

Configure the IP Sprayer to send IP traffic only to Site A (Figure 7-3). Remove Site B from the cluster and configure it to work with the Portal databases resident on the backup database server at Site B.

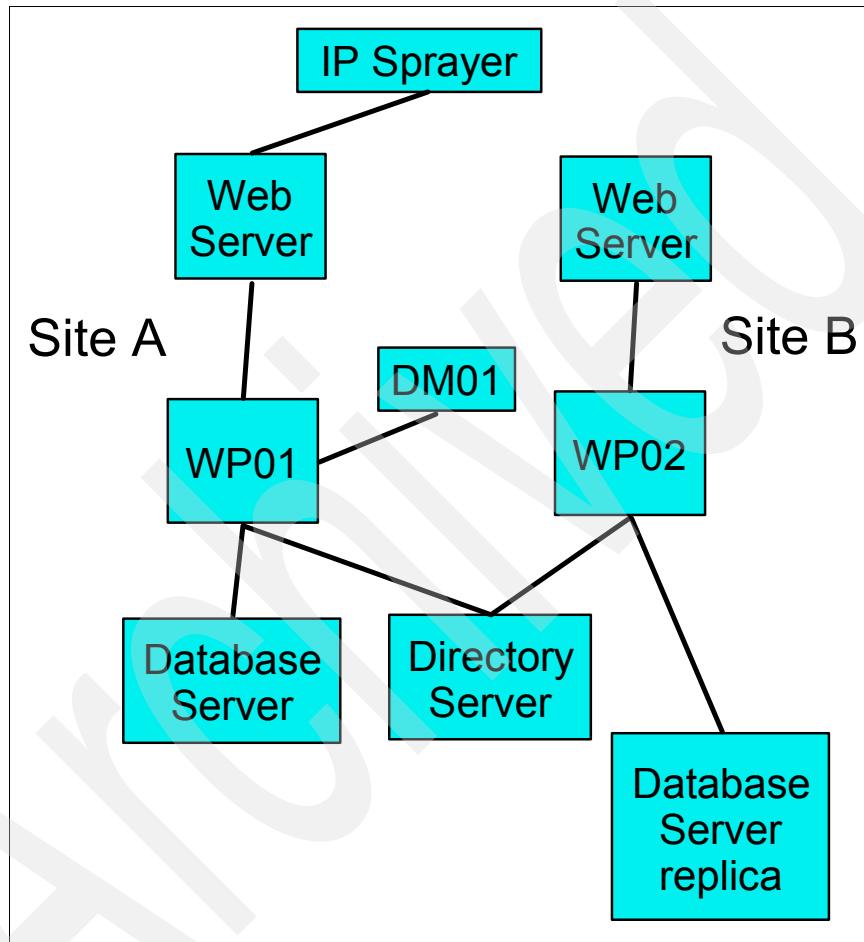


Figure 7-3 Site B removed and configured to work with Database Server replica

To continue the process:

1. Stop IP traffic from IP Sprayer to Site B. IP traffic should be routed to Site A.
2. Stop WebSphere Portal on Site B.
 - a. Open a command prompt and change to directory `was_root/bin`.
 - b. Enter the following commands:

on UNIX:	<code>./stopServer.sh WebSphere_Portal</code>
on Windows:	<code>stopServer.bat WebSphere_Portal</code>
3. Remove WebSphere Portal on Site B from cluster through Deployment Manager.
 - a. Check that the node agent server is running on Site B. List the active application servers using the following commands:

on UNIX:	<code>serverStatus.sh -all</code>
on Windows:	<code>serverStatus.bat -all</code>
 - b. If the node agent server is not running, start it. Open a command prompt and change to the `was_root/bin` directory and enter the following commands:

on UNIX:	<code>./stopServer.sh nodeagent</code>
on Windows:	<code>stopServer.bat nodeagent</code>
 - c. Follow the instructions under the subtopic *Removing a WebSphere Portal node from the cluster* in the *Uninstalling WebSphere Portal from a cluster* topic in the *Installing WebSphere Portal in a cluster environment* section of the WebSphere Portal InfoCenter:

<http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/index.html>

Note: Do not complete the steps listed in *Removing all Portal resource definitions from the cell*.

4. Regenerate Web server plug-in for Site A from the Deployment Manager Administration Console as shown Figure 7-4.

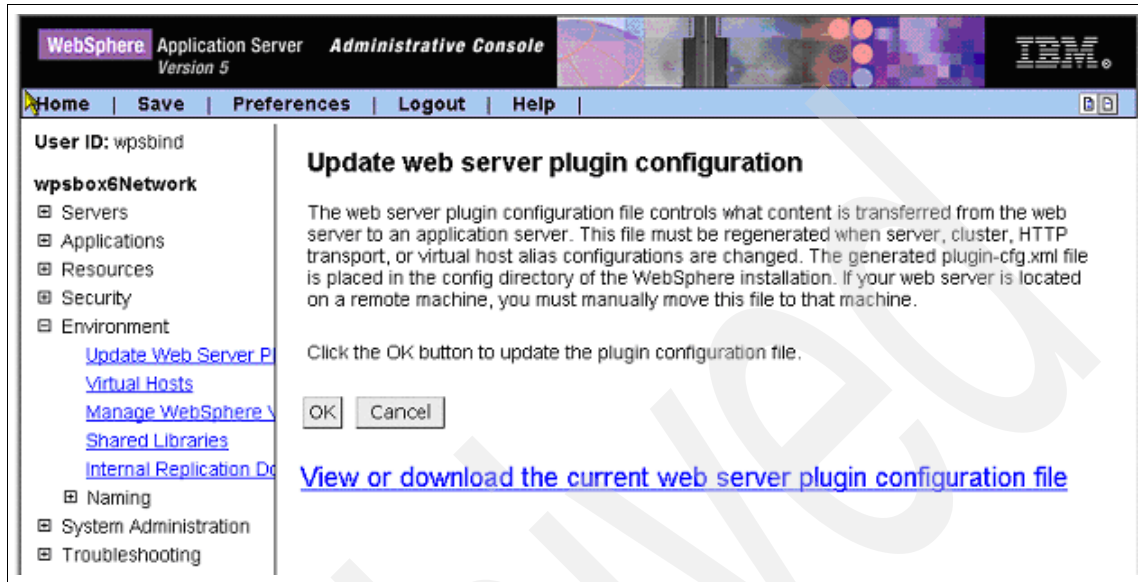


Figure 7-4 Regeneration of the plug-in file in Deployment Manager

- a. If necessary, edit the plug-in file to correct all subdirectories references.
- b. While all references to Site B should be removed from the file, check and make sure that they are not present.
- c. Copy plug-in file to Web Server at Site A.
5. Regenerate Web Sever plug-in for Site B from the WebSphere Application Server Administration Console on Site B.
 - a. If necessary, edit plug-in file to correct all subdirectories references.
 - b. Copy plug-in file to Web Server at Site B.
6. Stop database replication from Site A to Site B or take a backup of the Portal databases on the Site A database server and restore them on the database server on Site B.
7. Following the instructions in Appendix D, "Switching database servers" on page 265, switch the Portal server on Site B to access the database server at Site B.
8. At this point, you may wish to connect to one of the Portal databases such as WPS50 to verify the catalog changes.

9. Update the object ID for the Portal administrator user ID (for example, wpsadmin) in the wps50 database at Site B.
 10. Connect to the wps50 database using a command similar to the following:

```
connect to wps50x6 user <database userid> using <database password>
```
 11. Check the current object ID of the Portal administrator user ID (for example, wpsadmin) using a command similar to the following:

```
select oid, name from <database schema name>.user_desc
```
 12. The command in step 11 should produce output similar to the following:

OID	NAME
xxx	uid=wpsadmin,cn=users,dc=raleigh,dc=ibm,dc=com,cn=wpsadmins, cn=groups,dc=raleigh,dc=ibm,dc=com
 13. Update the Object ID of the Portal administrator user ID (for example, wpsadmin) using a command similar to the following:

```
update <database schema name>.user_desc set oid=10 where oid = xxx
```
- Note:** xxx is the Object ID from step 12.
14. Disconnect from the wps50 database.
 15. Start WebSphere Portal on Site B to test database connections and verify operation of Portal.

7.6 Maintenance on Site B

You install fixpacks and interim fixes on Site B as though it were a stand-alone installation as shown in Figure 7-5.

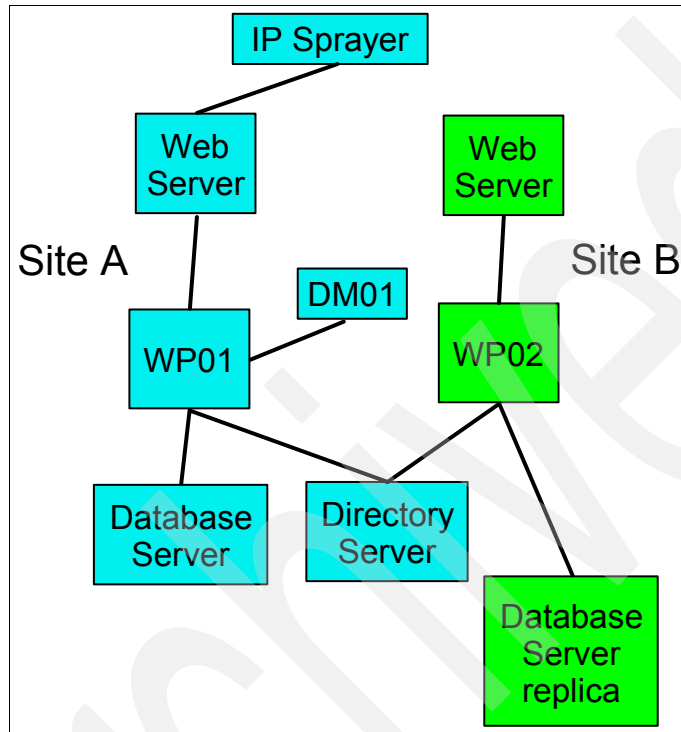


Figure 7-5 State of cluster while maintenance is performed on Site B

To continue the process:

1. Verify that your WebSphere environment contains the required hardware and software supported by the cumulative fix to be installed. The supported hardware and software requirements are available at:
<http://www.ibm.com/websphere/portal/library>
2. Make sure you have the required WebSphere Application Server interim fixes installed for the version of WebSphere Application Server that you are running. You can download the latest WebSphere Application Server interim fixes from the following Web address:
<http://www.ibm.com/websphere/support>

3. Download the fixpack and perform all the prerequisite steps listed in the instructions. WebSphere Portal fixpacks are available at:
http://www6.software.ibm.com/dl/websphere33/wps-h?S_PKG=d1wps50fp&S_TACT=&S_CMP=
4. Stop the Web Server on Site B.
5. Stop WebSphere Portal and server1 on Site B. Open a command prompt and change to the `was_root/bin` directory and enter the following commands:

on UNIX:	<code>./stopServer.sh WebSphere_Portal</code>
on UNIX:	<code>./stopServer.sh server1</code>
on Windows:	<code>stopServer.bat WebSphere_Portal</code>
on Windows:	<code>stopServer.sh server1</code>
6. Install the Web Server fixpack by following the instructions included with the Application Server fixpack. You can download Application Server fixpacks from the following Web address:
<http://www.ibm.com/websphere/support>
7. Install WebSphere Application Server fixpacks.
 - a. Install the WebSphere Application Server V5.0 Base fixpack, if applicable, on WP02 by following the instructions included with the WebSphere Application Server fixpack.
 - b. Install the WebSphere Application Server V5.0 Enterprise fixpack, if applicable, on WP02 by following the instructions included with the WebSphere Application Server fixpack.
 - c. Install any interim fixes, if applicable, on WP02 by following the installation instructions included with the WebSphere Application Server fixpacks.
 - d. The instructions included with the fixpack indicates what needs you need to install.
8. If desired, install any Database Server fixpacks by following the instructions included with the database fixpack.
9. Restart the Web Server.
10. Restart WebSphere Application Server. Open a command prompt and change to the `was_root/bin` directory and enter the following commands:

on UNIX:	<code>./stopServer.sh server1</code>
on Windows:	<code>stopServer.bat server1</code>
11. Test the WebSphere Application Server by accessing the snoop servlet (<http://your server name/snoop>) or by using your favorite test.

12. Install the WebSphere Portal fixpack on WP02 by following the stand-alone installation instructions included with the WebSphere Portal fixpack. WebSphere Portal fixpacks are available at:

http://www6.software.ibm.com/dl/websphere33/wps-h?S_PKG=d1wps50fp&S_TACT=&S_CMP=

13. Stop WebSphere Portal. Open a command prompt and change to the *was_root/bin* directory and enter the following commands:

on UNIX: `./stopServer.sh WebSphere_Portal`
on Windows: `stopServer.bat WebSphere_Portal`

14. Start WebSphere Portal. Open a command prompt and change to the *was_root/bin* directory and enter the following command:

on UNIX: `./startServer.sh WebSphere_Portal`
on Windows: `startServer.bat WebSphere_Portal`

15. Test the WebSphere Portal by logging in and accessing a number of pages.

7.7 Switch IP traffic from Site A to Site B

You have now upgraded Site B, and it is ready to take production IP traffic. To continue, you set the Portal on Site A to read-only mode and perform a final, one-time replication to move the latest changes to Site B. You start the Portal on

WP02 and configure the IP Sprayer to send IP traffic to Site B as shown in Figure 7-6.

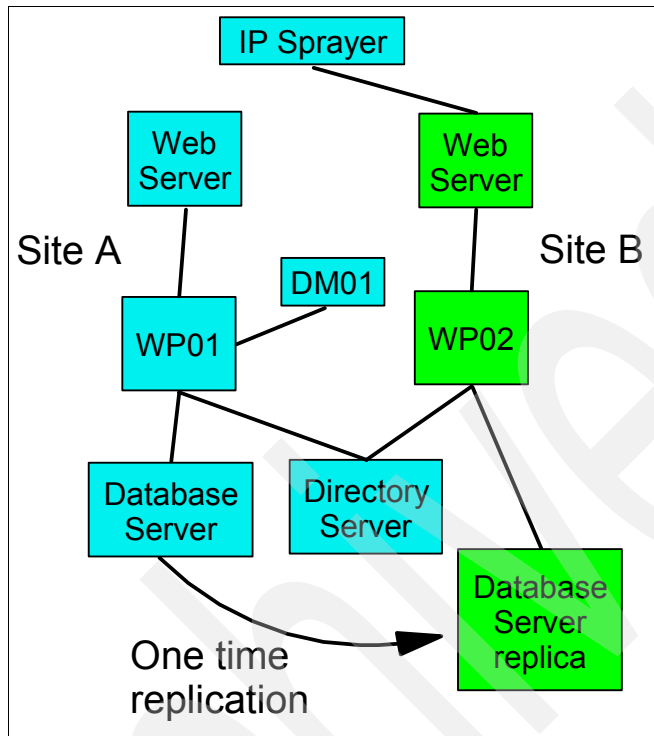


Figure 7-6 Site A down for maintenance while Site B takes the production IP traffic

To continue the process:

1. If WebSphere Portal on Site B is running, stop it now. Open a command prompt and change to the `was_root/bin` directory and enter the following commands:
on UNIX: `./stopServer.sh WebSphere_Portal`
on Windows: `stopServer.bat WebSphere_Portal`
2. Set WebSphere Portal on Site A to read-only mode using the XMLAccess command. See Appendix C, "Changing the mode in WebSphere Portal" on page 259 for instructions on how to perform this step.
3. Replicate once from Site A to Site B or backup, and restore the WebSphere Portal databases from Site A to Site B (see Appendix D, "Switching database servers" on page 265). This step also sets the Portal on Site B to read-only mode.

4. Start WebSphere Portal on Site B. Open a command prompt and change to the `was_root/bin` directory and enter the following commands:
on UNIX: `./startServer.sh WebSphere_Portal`
on Windows: `startServer.bat WebSphere_Portal`
5. Test the WebSphere Portal on Site B by logging in and accessing a number of pages.
6. Configure IP Sprayer to route IP traffic to Site B. All IP traffic should be routed to Site B at this time.

7.8 Maintenance on Site A

Next, you need to install fixpacks and interim fixes on Site A as though it was a cluster node as shown in Figure 7-7.

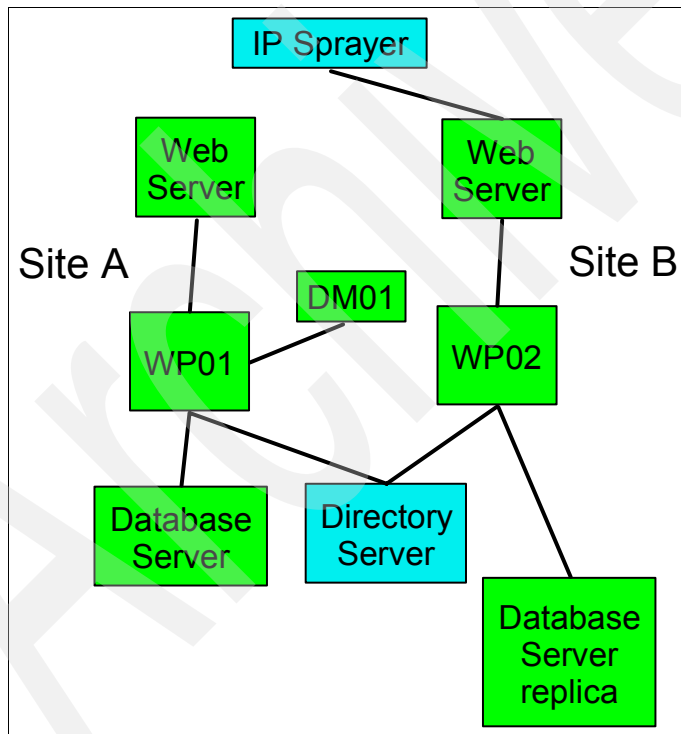


Figure 7-7 State of cluster while maintenance is performed on Site A

To continue the process:

1. Verify that your WebSphere environment contains the required hardware and software supported by the cumulative fix to be installed. The supported hardware and software requirements are available at:

<http://www.ibm.com/websphere/portal/library>

2. Make sure you have the required WebSphere Application Server interim fixes that are installed for the version of WebSphere Application Server that you are running. You can download the latest WebSphere Application Server interim fixes from the following Web address:

<http://www.ibm.com/websphere/support>

3. Download the fixpack and perform all prerequisite steps listed in the instructions. WebSphere Portal fixpacks are available at:

http://www6.software.ibm.com/dl/websphere33/wps-h?S_PKG=d1wps50fp&S_TACT=&S_CMP=

4. Set WebSphere Portal on Site A to edit mode using the XMLAccess command (see Appendix C, “Changing the mode in WebSphere Portal” on page 259).

5. Stop WebSphere Portal on Site A. Open a command prompt and change to the `was_root/bin` directory and enter the following commands:

on UNIX: **`./stopServer.sh WebSphere_Portal`**
on Windows: **`stopServer.bat WebSphere_Portal`**

6. Stop the Web Server on Site A.

7. Stop WebSphere Portal and server1 on Site A. Open a command prompt and change to the `was_root/bin` directory and enter the following commands:

on UNIX: **`./stopServer.sh WebSphere_Portal`**
on UNIX: **`./stopServer.sh server1`**
on Windows: **`stopServer.bat WebSphere_Portal`**
on Windows: **`stopServer.sh server1`**

8. Install the Web Server fixpack by following the instructions included with the WebSphere Application Server fixpack. WebSphere Application Server fixpacks can be downloaded from the following Web address:

<http://www.ibm.com/websphere/support>

9. Install WebSphere Deployment Manager fixpacks.

- a. Install the Deployment Manager fixpack on DM01 by following the instructions included with the WebSphere Application Server fixpack.
- b. Install the Deployment Manager EE fixpack, if applicable, on DM01 by following the instructions included with the WebSphere Application Server fixpack.

- c. The instructions included with the fixpack indicates what you need to install.
10. Install WebSphere Application Server fixpacks.
 - a. Install the WebSphere Application Server V5.0 Base fixpack, if applicable, on WP01 by following the instructions included with the WebSphere Application Server fixpack.
 - b. Install the WebSphere Application Server V5.0 Enterprise Edition fixpack, if applicable, on WP01 by following the instructions included with the WebSphere Application Server fixpack.
 - c. Install any interim fixes, if applicable, on WP01 by following the installation instructions included with the WebSphere Application Server fixpack.
 - d. The instructions included with the fixpack indicates what you need to install.
11. If desired, install Database server fixpack by following the instructions included with the database fixpack.
12. Restart the Web server.
13. Restart WebSphere Application Server. Open a command prompt and change to the *was_root/bin* directory and enter the following command:
on UNIX: **`./stopServer.sh server1`**
on Windows: **`stopServer.bat server1`**
14. Test the WebSphere Application Server by accessing the snoop servlet (http://your_server_name/snoop) or by using your favorite test.
15. Install the WebSphere Portal fixpack on WP02 by following the stand-alone installation instructions included with the WebSphere Portal fixpack. WebSphere Portal fixpacks are available at:
http://www6.software.ibm.com/d1/websphere33/wps-h?S_PKG=d1wps50fp&S_TACT=&S_CMP=
16. Stop WebSphere Portal. Open a command prompt and change to the *was_root/bin* directory and enter the following command:
on UNIX: **`./stopServer.sh WebSphere_Portal`**
on Windows: **`stopServer.bat WebSphere_Portal`**
17. Start WebSphere Portal. Open a command prompt and change to the *was_root/bin* directory and enter the following command:
on UNIX: **`./startServer.sh WebSphere_Portal`**
on Windows: **`startServer.bat WebSphere_Portal`**
18. Test the WebSphere Portal by logging in and accessing a number of pages.

7.9 Switch IP traffic from Site B to Site A

You have upgraded Site A, and it is ready to take production IP traffic. Now, you configure the IP Sprayer to send all IP traffic to Site A, and configure WP02 to use the database server at Site A. Finally, you refederate WP02 into the cluster with WP01 as show in Figure 7-8.

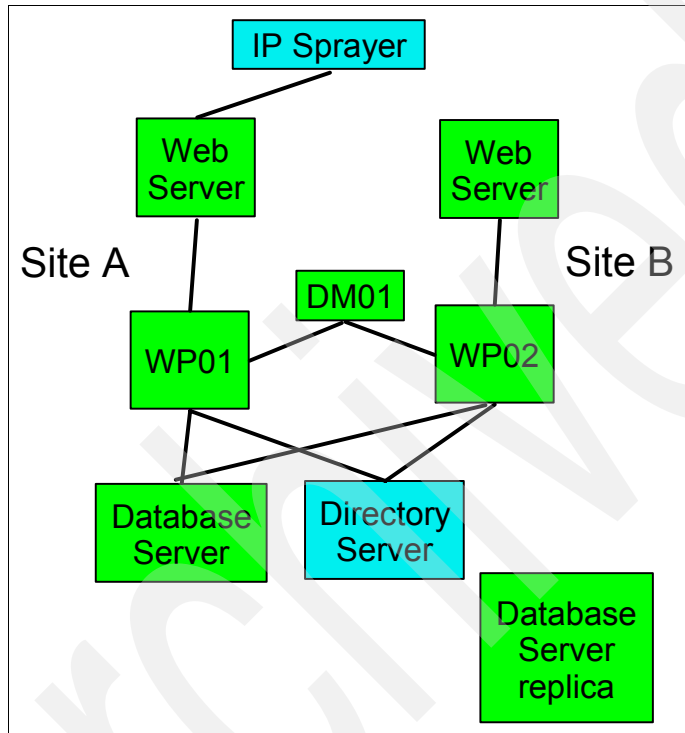


Figure 7-8 IP traffic configured to work with Database Server at Site A

To continue the process:

1. If not running, start WebSphere Portal on Site A. Open a command prompt and change to the `was_root/bin` directory and enter the following command:
on UNIX: `./startServer.sh WebSphere_Portal`
on Windows: `startServer.bat WebSphere_Portal`
2. Configure IP Sprayer to route IP traffic to Site A. All IP traffic should be routed to Site A at this time.
3. Set WebSphere Portal on Site A to edit mode using the XMLAccess command (see Appendix C, “Changing the mode in WebSphere Portal” on page 259).

4. Stop WebSphere Portal on Site B. Open a command prompt and change to the *was_root/bin* directory and enter the following commands:
on UNIX: `./stopServer.sh WebSphere_Portal`
on Windows: `stopServer.bat WebSphere_Portal`
5. Following the instructions in Appendix D, “Switching database servers” on page 265, switch the Portal server on Site B to access the Portal databases on the database server at Site A.
6. At this point, you may wish to connect to one of the Portal databases like WPS50 to verify the catalog changes.
7. Refederate WebSphere Portal at Site B back into the cluster through the use of the `addNode` command.

Add WebSphere Portal on site B to the Deployment Manager by entering the `addNode` command on one line of the server system to be added.

- on Windows:

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

- on UNIX:

```
<was_root>/bin/addNode.sh <deployment_manager_host>  
<deployment_manager_port> -username <admin_user_id> -password  
<admin_password>
```

In this example:

- *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 and is required if security is enabled.
- *admin_password* is the administrative user password. This parameter is optional and is required if security is enabled.

Note: Do *not* use the `-includeapps` option. If you do, the applications are not transferred because they are already in the master configuration of the Deployment Manager.

8. Regenerate Web server plug-in for both sites from the Deployment Manager Administration Console (see Figure 7-9).
 - a. If necessary, edit plug-in file to correct all subdirectories references.
 - b. To facilitate the correct routing of IP traffic from the Web server to WebSphere Portal within each site, remove all references in the plug-in file for the other site.
 - i. Remove all references for Site B in the plug-in file for Site A.
 - ii. Remove all references for Site A in the plug-in file for Site B.



Figure 7-9 Regeneration of the plug-in file in Deployment Manager

9. Copy plug-in file to Web server at Site A and at Site B. The file should be placed into the following directory:
 - on UNIX: `WAS_HOME/config/cells`
 - on Windows: `WAS_HOME\config\cells`
10. Rebuild cluster at the Deployment Manager.
 - a. Follow the instructions for WP02 under *Creating the cluster* in the *Installing WebSphere Portal in a cluster environment* section of the WebSphere Portal InfoCenter:

<http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/index.html>
 - b. Do not specify the `-includeapps` parameter.

7.10 Return to Initial Production state

At this point, you have completed maintenance on Site A and Site B. Now, you configure the IP Sprayer to send traffic to both Site A and Site B. The initial production state, steady state, is restored as shown in Figure 7-10.

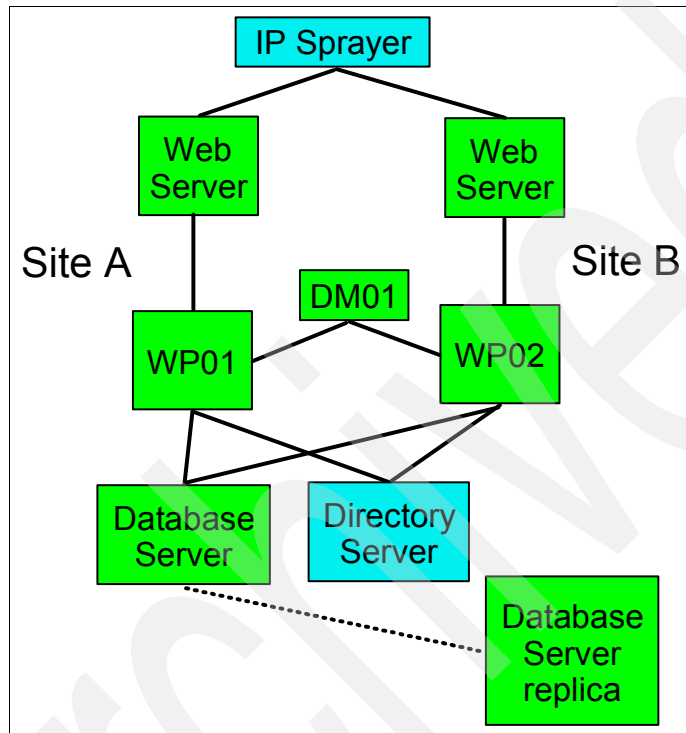


Figure 7-10 Upgraded operational production clustered environment

To complete the process:

1. Configure IP Sprayer to route IP traffic to Site A and Site B.
2. Restart database replication from database server at Site A to database server at Site B.

Performance tuning the environment

The IBM WebSphere Portal and Lotus Workplace™ Performance departments provided this chapter.

This chapter presents guidelines for parameter and application server tuning for IBM WebSphere Portal for Multiplatforms V5.0. Tuning is affected by many factors, including the workload scenario and the performance test environment. For tuning, we do not recommend that you use the same values that we used when testing our WebSphere Portal scenarios. These values may not be appropriate for your environment. However, knowing which of these parameters made the most performance impact in our testing might be useful information. When tuning individual systems, remember that it is important to begin with a baseline test and to monitor the performance statistics to see if you should change any parameters.

8.1 Understanding the environment

To provide functionality, WebSphere Portal V5.0 can make use of several additional servers. In our test environment, there was a database server and directory server in addition to the Portal server itself.

For maximum performance, the different back-end servers should reside on separate systems from the WebSphere Portal system. The primary benefit of having such a configuration is to avoid resource contention from multiple servers residing on a single server. Back-end servers sharing the WebSphere Portal application resources impacts the amount of throughput you can achieve.

Back-end servers for WebSphere Portal in our configuration were:

1. A remote database server for the WebSphere Portal database.
2. A remote database server for the session database when Workload Management was used.
3. A remote LDAP directory server.

8.2 Application server tuning

Because of its close relationship with the base WebSphere Application Server product, tuning the WebSphere Portal application server primarily involves tuning WebSphere Application Server.

This section does not cover every possible tuning parameter available for WebSphere Application Server. Instead, it presents our recommendations based on performance impacts that we experience in our testing environment. For more details on tuning WebSphere Application Server, see the Tuning Section of the InfoCenter at:

<http://www-3.ibm.com/software/webservers/appserv/was/library/>

Table 8-1 on page 217 presents our recommendations.

Table 8-1 Performance and tuning recommendations

Cross-platform tuning parameters		
High priority		
Parameter	Value	Description
Initial Heap Size Maximum Heap Size	1 GB or more	<p>Set the Java Virtual Machine heap size larger than 256 MB. For the best and most consistent throughput, set the starting minimum (ms) and maximum (mx) to the same size. We used 1 GB on Windows and 1.5 GB on AIX and Solaris</p> <p>Also, remember that the value for the Java Virtual Machine heap size is directly related to the amount of physical memory for the system. Never set the Java Virtual Machine heap size larger than the physical memory on the system.</p> <p>To set the parameter:</p> <ol style="list-style-type: none"> 1. Logon to WebSphere Administrative Console. 2. Click Servers → Application Servers → WebSphere Portal → Process Definition → Java Virtual Machine and set the following: <ul style="list-style-type: none"> – Initial Heap Size – Maximum Heap Size
Set Timeout	10 minutes	<p>The default value of Set Timeout is 30 minutes. Reducing this value to a lower number can help reduce memory consumption requirements, allowing a higher user load to be sustained for longer periods of time. Reducing the value too low can interfere with the user experience.</p> <p>To set the parameter:</p> <ol style="list-style-type: none"> 1. Logon to WebSphere Administrative Console. 2. Click Servers → Application Servers → WebSphere Portal → Web Container → Session Management → Session Timeout and change the Set Timeout parameter.
Lower priority		
Class Garbage Collection	-Xnoclassgc	<p>Using the -Xnoclassgc parameter allows for more class reuse, thus causing less garbage collections to occur.</p> <p>To set this parameter:</p> <ol style="list-style-type: none"> 1. Logon to WebSphere Portal Administrative Console. 2. Click Servers → Application Servers → WebSphere Portal → Process Definition → Java Virtual Machine → Generic JVM arguments and set - {add} -Xnoclassgc.

Cross-platform tuning parameters		
Servlet engine thread pool size	70	<p>In our testing, we used 70 for both the minimum and maximum settings for this parameter. Ideally, you set this value and then monitor the results using the Tivoli Performance Viewer. Increase this value if all the servlet threads are busy most of the time.</p> <p>To set this parameter:</p> <ol style="list-style-type: none"> 1. Logon to WebSphere Portal Administrative Console. 2. Click Servers → Application Servers → WebSphere Portal → Web Container → Thread Pool and set the following: <ul style="list-style-type: none"> – Minimum size threads – Maximum size threads
Data source connection pool size	25 or more	<p>Increase the connection pooling of the WebSphere Portal database. Based on our load, the maximum connection pools for the datasources were increased to 25 or higher.</p> <p>To set this parameter:</p> <ol style="list-style-type: none"> 1. Logon to WebSphere Portal Administrative Console. 2. Click Resources → JDBC Providers → wps50JDBC → Data Sources → wps50DS → Connection Pools and set the following: <ul style="list-style-type: none"> – Minimum connections – Maximum connections
Statement Cache Size	500	<p>You should increase the Statement Cache Size used by the wps50DS data source. We set this value to 500-1000. The statement cache can be monitored using the Tivoli Performance Viewer, to ensure that it is large enough.</p> <p>To set this parameter:</p> <ol style="list-style-type: none"> 1. Logon to WebSphere Portal Administrative Console. 2. Click Resources → JDBC Providers → wps50JDBC → Data Sources → wps50DS and set the Statement Cache Size parameter.

Cross-platform tuning parameters		
Tuning parameters specific to Solaris		
HotSpot option	-server	<p>The server mode offers higher throughput than client mode, at an expense of slightly longer startup times. We recommend using server mode for higher throughput.</p> <p>To set this parameter:</p> <ol style="list-style-type: none"> 1. Logon to WebSphere Portal Administrative Console. 2. Click Servers → Application Servers → WebSphere Portal → Process Definition → Java Virtual Machine → Generic JVM arguments and set {add} -server.
NewSize MaxNewSize	200 MB	<p>To help optimize Java garbage collection duration and frequency, we set the -XX:NewSize and -XX:MaxNewSize parameters to 200 MB.</p> <p>To set these parameters:</p> <ol style="list-style-type: none"> 1. Logon to WebSphere Portal Administrative Console. 2. Click Servers → Application Servers → WebSphere Portal → Process Definition → Java Virtual Machine → Generic JVM arguments and set the following: <ul style="list-style-type: none"> – {add} -XX:NewSize=200M – {add} -XX:MaxNewSize=200M
SurvivorRatio	12	<p>To help optimize Java garbage collection duration and frequency, we set the -XX:SurvivorRatio parameter to 12.</p> <p>To set this parameter:</p> <ol style="list-style-type: none"> 1. Logon to WebSphere Portal Administrative Console. 2. Click Servers → Application Servers → WebSphere Portal → Process Definition → Java Virtual Machine → Generic JVM arguments and set {add} -XX:SurvivorRatio=12.

8.2.1 Additional notes for an AIX environment

By default, the application server will not start on AIX with a heap size larger than 1 GB. To allow larger a JVM heap size, set the following environment variable:

```
LDR_CNTRL=MAXDATA=0xn0000000
```

In this variable, *n* is the number of segments you need. For a 2 GB heap size, set *n*=2, for 1792 MB, set *n*=3, and so on. Set it to 0 for WebSphere 1.3 or later to go to 2560 MB. For example, for a 1.5 GB heap size, set the following:

```
LDR_CNTRL=MAXDATA=0x40000000
```

This environment variable is available in AIX 4.3.3.10 and later. If you are using an earlier version, you must upgrade to get this support.

To set this parameter:

1. Logon to WebSphere Portal Administrative Console.
2. Click **Servers** → **Application Servers** → **WebSphere Portal** → **Process Definition** → **Environment Entries** → **New** and set:
 - name: LDR_CNTRL
 - value: MAXDATA=0x40000000

8.2.2 Application server cloning

For cloning, a general rule of thumb is not to blindly add clones onto the environment. The best way to add clones is to begin by performance testing with one instance of the application server and then measuring the throughput and system resource utilization. For configuring a vertical clone, if the CPU is utilized 85% or more, it is better not to add an additional clone. Thus, it is difficult to pinpoint the number of horizontal or vertical clones any one environment needs without doing extensive tests. Overall, workload management provides a huge impact in meeting overall performance objectives.

8.3 Database server tuning

In WebSphere Portal V5.0, several back-end database servers are required for core functionality. These servers include a database server for the application databases and a database server for the user registry. In our test lab, another database server that we rely on is a Lightweight Directory Access Protocol (LDAP) user repository.

8.3.1 IBM DB2 Enterprise Edition Database parameter tuning

For our testing, we used IBM DB2 Enterprise Edition V8.1 Fixpack 1 as our database server for the AIX and Windows platforms. Here are the specified parameters and values used in our environment for the WebSphere Portal database:

- ▶ db2 update db config for wps using applheapsz 1024
- ▶ db2 update db config for wps using app_ctl_heap_sz 1024
- ▶ db2 update db config for wps using maxappls 75
- ▶ db2 update db config for wps using locklist 1024
- ▶ db2 update db config for wps using buffpage 2500
- ▶ db2 update db config for wps using dbheap 4000
- ▶ db2 update db config for wps using sortheap 4000
- ▶ db2 update db config for wps using stmtheap 2048
- ▶ db2 update db config for wps using maxlocks 40
- ▶ db2 update db config for wps using num_iocleaners 7
- ▶ db2 update db config for wps using num_ioservers 7
- ▶ db2 update db config for wps using logsecond 10

Along with these database parameter changes, there are several other updates that are needed for the database:

- ▶ Reorganize the tables in the database periodically. When a row in a table is deleted, the space occupied by the row is not necessarily reclaimed until the table is reorganized. Perform the following command on each database:

```
db2 reorgchk update statistics on table all
```

This command scans the tables and index space to gather information of space and efficiency of indexes. This information is stored in the DB2 catalog. The SQL optimizer uses this information to select access paths to data. The utility then produces a report that recommends which tables should be reorganized. To reorganize any of the tables in the report, run the following command:

```
db2 reorg table <table-name>
```

- ▶ Ensure that the database server has an adequate number of disks. In our testing, we used from four to six drives. Also, if possible, due to constant logging from the databases, dedicate the database logs to a separate disk or disk from where the physical databases reside.
- ▶ Ensure that the MaxAppls parameter is greater than the total number of connections for both the datasource and the session manager for each WebSphere Portal application server clone. For example:

```
MaxAppls > ( total datasource connection + total session manager  
connections) * number of WP clones
```

- Use SMS tablespace type for DB2 temporary table spaces for systems which have nested queries. Otherwise, excessive time is spent in buffer writes on UPDATES and other SQL requests which require nested queries, as well as excessive disk use on the DB/2 server.

8.3.2 Oracle Enterprise Edition Database parameter tuning

For our Solaris testing, we used Oracle 9i as the database server for the WebSphere Portal Server database.

We applied the following on the Oracle database server:

- Analyzed database tables and indexes
 - Analyze index {index-name} compute statistics
 - Analyze table {table-name} compute statistics

Note: We executed these commands for each index and table in the database. Although we used the **analyze** command, Oracle recommends using **DBMS_STATS**. The **analyze** command will no longer be supported by Oracle.

3. Increased QUEUESIZE in the \$ORACLE_HOME/network/admin/listener.ora file to 40.
4. Set the following values with the **alter system** command:

```
alter system set processes=500 scope=spfile;
alter system set trace_enabled=false scope=spfile;
alter system set db_writer_processes=3 scope=spfile;
alter system set open_cursors=800 scope=spfile;
alter system set sessions=700 scope=spfile;
alter system set shared_pool_size=100663296 scope=spfile;
alter system set transactions=800 scope=spfile;
```

5. Set the following kernel settings in /etc/system:

```
set semsys:seminfo_semvms=32767
set semsys:seminfo_semmsl=1024
set semsys:seminfo_semopm=200
```

8.3.3 Other database considerations

WebSphere Portal uses several databases to maintain information about Portal visitors. Thus, the size of the database tables does not remain constant in a running Portal. For example, the first time a user visits the Portal, it adds an entry to one of the database tables. When places, pages, or access permissions are

created, additional table entries are created. This creation is done automatically on the user's behalf and is part of the normal Portal server processing.

However, the automatic creation of table entries can have an impact on performance. The performance of relational databases typically declines as tables grow unless the tables are periodically reorganized.

To ensure that the data in this paper reflects the performance of WebSphere Portal, and is not limited by database performance, we preloaded the databases before we ran the performance tests. We ran a LoadRunner script, which logged in and then logged out each user that was defined for the test environment. Then, we stopped the Portal application server and reorganized the database tables.

Any performance testing of WebSphere Portal which uses more than 1000 unique users should follow a similar procedure to populate database tables. Otherwise, you will see sub-optimal performance.

8.4 Directory server tuning

All of our tests used IBM Directory Server V5.1 running on AIX as the directory server. IBM Directory Server also uses a database as its storage mechanism. This database is typically located on the same system as the directory server. In the test environment, the IBM DB2 Enterprise Server served as the storage for user information. Table 8-2 lists the configuration changes that we made in our environment.

Table 8-2 Directory server tuning

Database Buffer Pool Sizes		
IBMDEFAULTBP	29 500	This buffer pool uses a 4 KB page size, so it uses 118 MB of memory
LDAPBP	1230	This buffer pool uses a 32 KB page size, so it uses 39 MB of memory.
IDS Parameters		
lbn-slapdACLCacheSize	150 000	All three of these values are in the file/usr/ldap/etc/ibmslapd.conf file. You must restart the LDAP server after changing these values.
lbn-slapdEntryCacheSize	150 000	
lbn-slapdFilterCacheSize	150 000	
lbn-slapdDbConnections	7	
lbn-slapdFilterCacheBypassLimit	5 000	

AIX Environment Variables		
MALLOCMULTIHEAP	4	All of these values are set in /etc/environment.
SPINLOOPTIME	650	
RDBM_CACHE_SIZE	128 000	

8.4.1 Web server tuning tips

Table 8-2 on page 223 lists the changes that we made to the IBM HTTP Server configuration file.

Table 8-3 Web server tuning

Setting	Value	Discussion
KeepAliveTimeout	5 (seconds)	We set this value to be less than the think time defined in our scripts, because we wanted to be conservative in our testing. Therefore, we assumed that each user will open new TCP connections for each page view. However, in a live environment, it can be helpful to increase the KeepAliveTimeout setting. A higher KeepAliveTimeout setting might increase contention for HTTP server processes. If you are running out of HTTP processes, decrease this value.
MaxClients (UNIX) or ThreadsPerChild (Windows)	300 or higher, depending on load	A value representing the maximum number of clients.
KeepAlive	on for UNIX off for Windows	We experienced problems with exhausting all the available sockets on Windows. So, we disabled the KeepAlive setting. Moving the HTTP server to a separate system would also help with this issue.
MaxKeepAliveRequests	0	This setting allows an unlimited number of requests on a single TCP connection.
MaxRequestsPerChild	250 000	A value representing the maximum number of requests.
StartServers	300	This setting makes a large pool of servers available at the beginning of the test.

Setting	Value	Discussion
access logging	Disabled	<p>We disabled this setting by commenting out the following configuration line in the HTTP Configuration file:</p> <pre>CustomLog /usr/HTTPServer/logs/access_log common</pre>

One option to relieve contention on the WebSphere Portal system is to install the Web server remotely from the Portal application server. In this environment, where both the Web server and the database servers are remote, the Portal server does not have to contend with these processes for system resources.

We also enabled the server-status module so that we could monitor the number of running and available Web server processes. This enables appropriate tuning of the MaxClients or ThreadsPerChild parameters.

8.4.2 Security filters

The default filter generated by the WebSphere Portal installation uses the most recommended filters for both IBM Directory Server and Lotus Domino Directory. If you are using a different LDAP directory or if you choose to modify the default filters for IBM Directory Server or Lotus Domino Directory, you should consider the possible performance impact when designing filters for your environment.

You should consider the following settings when designing your IDS or Domino Directory environment:

- ▶ Group Filter: (&(cn=%v)(objectclass=groupOfUniqueNames)))
- ▶ Group Member ID Map:
ibm-allGroups:member;ibm-allGroups:uniqueMember

To set these parameters:

1. Logon to WebSphere Administrative Console.
2. Select **Security** → **User Registries** → **LDAP** → **Advanced LDAP Settings** → **Group Member ID Map**.

8.4.3 Dereferencing aliases

If your LDAP directory is not configured with any aliases to objects (versus direct access to objects), it is beneficial to set a JNDI property to never dereference aliases. In the *was_root/properties/jndi.properties* file, where *was_root*

represents the WebSphere Application Server home, set the following parameter:

```
java.naming.ldap.derefAliases=never
```

If there is no `jndi.properties` file, create one that contains this parameter. In WebSphere Portal V5.0, this is now a default setting.

8.5 Operating system specific tuning parameters

This section discusses tuning parameters for different operating systems.

File Descriptors for UNIX systems

The File Descriptors parameter specifies the number of open files permitted. If this value is set too low, a memory allocation error occurs on AIX and a too many files open are logged to the `stderr` log file. Set this value higher than the default system value. For large SMP machines with clones, set the parameter to unlimited. The file descriptor variable must be set in the same window where you start the WebSphere administrative server.

To display the current value, use the `ulimit -a` command.

To change to a different value, use the `ulimit -n <new_value>` command.

Kernel parameters for Solaris platform

In our testing on Solaris, we updated the following operating system kernel parameters.

- ▶ `semsys:seminfo_semume`

This parameter limits the maximum semaphore undo entries per process. We set the value to 1024.

- ▶ `semsys:seminfo_semopm`

This parameter specifies the maximum number of System V semaphore operations per `semop(2)` call. We set this parameter to 16384.

You can add or update these parameters in the `/etc/system` file. It is a good practice to always backup the original copy of this file before you make any changes. You also need to reboot the system for the changes to take effect.

8.6 Network tuning

In any production environment, you should closely monitor the network to ensure that its performance is acceptable and consistent. Based on our private switched 100 MB Ethernet on a 1 GB backbone, we modified the network parameters listed in this section.

Note: You do not need to set all network parameters to these values. Just be aware that the network is also an entity in the performance environment as well as the bottleneck resolution process.

8.6.1 Solaris networking

For Solaris, use the **ndd** command to set the following TCP layer parameters:

```
/usr/sbin/ndd -set /dev/tcp tcp_time_wait_interval 60000
/usr/sbin/ndd -set /dev/tcp tcp_conn_req_max_q0 16192
/usr/sbin/ndd -set /dev/tcp tcp_conn_req_max_q 16192
/usr/sbin/ndd -set /dev/tcp tcp_rexmit_interval_initial 500
/usr/sbin/ndd -set /dev/tcp tcp_rexmit_interval_min 200
/usr/sbin/ndd -set /dev/tcp tcp_rexmit_interval_max 4000
/usr/sbin/ndd -set /dev/tcp tcp_ip_abort_interval 60000
/usr/sbin/ndd -set /dev/tcp tcp_keepalive_interval 90000
/usr/sbin/ndd -set /dev/tcp tcp_smallest_anon_port 1024
/usr/sbin/ndd -set /dev/tcp tcp_slow_start_initial 2
/usr/sbin/ndd -set /dev/tcp tcp_deferred_ack_interval 50
/usr/sbin/ndd -set /dev/tcp tcp_xmit_hiwat 65536
/usr/sbin/ndd -set /dev/tcp tcp_rcv_hiwat 65536
```

These changes take effect immediately and improve the network layer performance in high-volume environments. To make these changes permanent, add these statements to the `/etc/rc.2/S69inet` file.

8.6.2 AIX networking

For AIX, use the **no** command to set the following TCP layer parameters:

```
/usr/sbin/no -o tcp_sendspace=65536
/usr/sbin/no -o tcp_recvspace=65536
/usr/sbin/no -o udp_sendspace=65536
/usr/sbin/no -o udp_recvspace=65536
/usr/sbin/no -o somaxconn=10000
/usr/sbin/no -o tcp_nodelayack=1
```

These changes take effect immediately and improve the network layer performance in high volume environments. To make these changes permanent, add these statements to the `/etc/rc.net` file.

8.6.3 Windows networking

We set the following in the registry section of the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters` file:

```
MaxFreeTcbs = dword:0000ffff
MaxHashTableSize = dword:00004000
MaxUserPort = dword:0000fffe
TcpNumConnections = dword:00ffffffe
TcpTimedWaitDelay = dword:0000001e
TcpMaxConnectionRetransmission = dword:00000005
```

8.7 WebSphere Portal service properties

Table 8-4 lists several available WebSphere Portal parameters that you should modify according to the expected workload and dynamics of your environment.

All property files are located in the `wps_root/shared/app/config/services` directory.

Table 8-4 WebSphere Portal service properties

Parameter	Value that we used	Definition	Property File Name
public.expires	3600 (seconds)	Determines cache expiration time for the unauthenticated Portal page.	NavigatoService.properties
Persistent.session.option	0	Determines whether the user gets the option to resume their previous session. This function affects performance because WebSphere Portal Server must write the user's state to its database when the user logs out or the user's session timeouts.	ConfigService.properties

Parameter	Value that we used	Definition	Property File Name
default.interval bucket.*.interval	Default	Determines the interval (in seconds) to refresh one of the listed resource types from the database. If a bucket does not have an associated interval, the default will be used. If there are certain resource types that are not changed often, you may want to increase the interval for that resource type to reduce the amount of database reads.	RegistryService.properties
uri.requestid	False	Determines the support of URL addressability. To set URL addressability, set this property to <code>false</code> , which means IDs are not requested	ConfigService.properties
Access control cache lifetimes	3600 (seconds)	Applies to all of the access control caches in the CacheManagerService.properties file.	CacheManagerService.properties

Operation tools

This appendix describes the tools that we used with WebSphere Portal.

XMLAccess tool

Example A-1 contains the `install_portlet.xml` script that installs the XMLAccess tool.

Example: A-1 install_portlet.xml

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<request xsi:noNamespaceSchemaLocation="PortalConfig_1.2.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" create-oids="true"
type="update" >
  <!-- Sample for deploying a portlet. -->
  <portal action="locate" >
    <!-- uid must match uid attribute of portlet-app in portlet.xml -->
    <web-app action="update" active="false"
uid="com.ibm.wps.portlets.worldclock" >
      <url>file:///server_root$/installableApps/worldclock.war</url>
      <!-- uid must match uid attribute of concrete-portlet-app in
portlet.xml -->
      <portlet-app action="update" active="false"
uid="com.ibm.wps.portlets.worldclock.1" >
        <!-- Name must match content of portlet-name subtag of
concrete-portlet in portlet.xml -->
```

```

        <portlet objectid="com.ibm.wps.portlets.worldclock"
action="update" active="false" name="World Clock" />
    </portlet-app>
</web-app>
</portal>
</request>

```

Example A-2 contains the start_portlet.xml script that starts the XMLAccess tool.

Example: A-2 start_portlet.xml

```

<?xml version = '1.0' encoding = 'UTF-8'?>
<request xsi:noNamespaceSchemaLocation="PortalConfig_1.2.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" create-oids="true"
type="update" >
    <!-- Sample for start a web-app. -->
    <portal action="locate" >
        <!-- uid must match uid attribute of portlet-app in portlet.xml -->
        <web-app action="locate" active="true"
uid="com.ibm.wps.portlets.worldclock" >
            <!-- uid must match uid attribute of concrete-portlet-app in
portlet.xml -->
            <portlet-app action="update" active="true"
uid="com.ibm.wps.portlets.worldclock.1" >
                <!-- Name must match content of portlet-name subtag of
concrete-portlet in portlet.xml -->
                <portlet objectid="com.ibm.wps.portlets.worldclock"
action="update" active="true" name="World Clock" />
            </portlet-app>
        </web-app>
    </portal>
</request>

```

Script to synchronize nodes

Example A-3 contains the script that we used to synchronize nodes.

Example: A-3 sync_all_nodes.jacl

```

#
# Synchronizing all nodes within all the configured cells
#
# Mike Storzer, December 2003 for IBM Deutschland GmbH, Software Group
WebSphere Services Central EMEA Region
#

```

```

# The jacl script does not need any commandline input parameters, if performed
locally on a WAS installation
# with standard settings.
#
# The script may be called like:
# wsadmin -f sync_all_nodes.jacl
#
# Please adopt to this call, if you have configured security or DMGR is remote
or uses specific ports.
#
# This script results in the following output: (sample for a one-node
installation)
#
# Number of nodes to sync: 1
#
#      Start Synchronizing Node
#      Finished Synchronizing Node
#
# Finished Synchronizing all Nodes
#
#
# Disclaimer:
# This program may be used, executed, copied, modified and distributed without
royalty
# for the purpose of developing, using, marketing, or distribution.
#

# the following line determines the "NodeAgents".
set nodelist [$AdminControl queryNames type=NodeSync,*]

puts "Number of nodes to sync: [llength $nodelist]"

# now loop over the list of nodeagents and invoke the synchronization
foreach nodelistitem $nodelist {
    set syncitem [$AdminControl completeObjectName $nodelistitem]
    puts " "
    puts "Start Synchronizing Node: $nodelistitem"
    $AdminControl invoke $syncitem sync
    puts "Finished Synchronizing Node"
    puts " "
}
    puts "Finished Synchronizing all Nodes"
# End of script

```

Script to delete portlets

Example A-4 contains the script that we used to delete portlets.

Example: A-4 Delete_Portlets.xml script

```
<?xml version="1.0" encoding="UTF-8"?>
<request
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="PortalConfig_1.2.xsd"
  type="update">

  <portal action="locate">
    <!-- Delete ALL portlets from the portal -->
    <web-app objectid="*" action="delete" />
  </portal>
</request>
```

Reference documentation

The XML Configuration Interface section of the InfoCenter describes the following topic areas:

- ▶ About the XML configuration interface
- ▶ Changes in XML for WebSphere Portal V5.0.2
- ▶ Working with the XML configuration interface
- ▶ Moving from a test to production server using the XML configuration interface
- ▶ XML reference
- ▶ Troubleshooting the XML configuration interface
- ▶ XML messages
- ▶ Reference: Sample XML configuration files

For more information, visit the InfoCenter Web site:

<http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/index.html>



Portal installation worksheets and samples

This appendix contains the forms and worksheets you can use during the installation process. It also provides a sample response file for a silent installation.

Worksheets

Table B-1 Basic Portal installation worksheet

Installation step	Parameters	Value	Example/description
Operating system and network configuration	HostName		Network host name Example: Portal
	fully-qualified domain name		Full qualified domain name Example: Portal.redbook.ibm.com
	IP address		Static IP address Example: 9.42.171.139
	Subnet mask		Subnet mask Example: 255.255.255.0
	Default gateway		Default gateway IP address Example: 9.42.171.3
	DNS server		DNS servers addresses
	Ports in		List of ports Listened by the server Example: 9080, 9443, 9090, 9043, 5557, 5558, 2809, 8880, 7873, 9081, 9444, 9091, 9044
	Ports out		List of external ports connected by the server Example: Remote database port (5000, 1521), Remote LDAP (389)
	Administrator user ID		Admin user to be used for Portal installation Example: Administrator (Win), root (AIX/Linux)
	Administrator password		

Installation step	Parameters	Value	Example/description
Basic Portal installation	WebSphere Application Server installation directory		Directory path where WebSphere Application Server will be installed Example: C:\WebSphere\AppServer
	IBM HTTP Server installation directory		Directory path where IBM HTTP Server will be installed. Note: Skip this parameter if using Remote Web servers Example: C:\IBM\HttpServer
	System administrator ID		Example: Administrator
	System administrator password		
	Run WebSphere Application Server as a service (yes/no)		Note: Applies only to Windows
	Run IHS as a service (yes/no)		Note: Applies only to Windows
	Portal installation directory		Directory path where WebSphere Portal will be installed Example: C:\WebSphere\PortalServer
	WebSphere Portal administrator user		Example: wpsadmin
	WebSphere Portal administrator password		
	Note: Review the list of required CDs for basic Portal installation <ul style="list-style-type: none"> ▶ Windows 2000, cdSetup: CD1-1, CD1-6, CD2 ▶ Windows 2003, cdSetup: 2003, CD1-13, CD1-17, CD2 ▶ AIX, cdSetup: CD1-3, CD1-7, CD2 ▶ Linux for Intel, cdSetup: CD1-2, CD1-6, CD2 		

Table 8-5 DB2 Fact sheet (1 of 2)

WebSphere Portal databases configuration, DB2 UDB fact sheet		
DB server		
	Value	Example
DB2 UDB Version		DB2 UDB Enterprise V8.1 FP1
db2set variables	DB2_RR_TO_RS=yes DB2COMM=TCPIP	
Portal databases		
Instance Name		DB2
User Name		db2admin
Password		
User Privilege		sysadmin
Three databases are required for Portal		
WPS database		
Database name		wps50
Database alias		wps50tcp
DB config parameters	applheapsz 16384, app_ctl_heap_sz 8192, stmtheap 60000, locklist 400, indexrec RESTART, logfilsiz 1000, logprimary 12, logsecond 10	
WPCP database		
Database name		wpcp50
Database alias		wpcp50tcp
DB config parameters	applheapsz 4096, logfilsiz 4096, logprimary 4, logsecond 25	
Feedback database		
Database name		fdbk50
Database alias		fdbk50tcp
DB config parameters	applheapsz 4096, logfilsiz 4096, logprimary 4, logsecond 25	

WebSphere Portal databases configuration, DB2 UDB fact sheet		
DB2 client properties		
	Value	Example
Portal host where client is to be installed		portal.redbook.com
DB2 Version	DB2 client is required to be the same version as the DB2 server	
<p>Notes:</p> <ul style="list-style-type: none"> ▶ All databases must be created as UTF8 ▶ When creating objects the Portal code will use the users default tablespace ▶ For initial configuration each database needs 100Mb of space available ▶ For remote DB server, Portal requires the DB2 client software with aliases configured to the DB2 server databases <p>If necessary, access the links below for further instructions:</p> <ul style="list-style-type: none"> ▶ DB2 installation http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/wpf/inst_db2.html ▶ Databases creation and users http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/wpf/cr_rem_db2.html 		

Table B-2 DB2 Fact Sheet (2 of 2)

WebSphere Portal Databases configuration, DB2 UDB Fact Sheet			
DB2 Server			
Hostname			
Port			
Databases	Database Name	User	Password
WebSphere Portal Server			
WebSphere Portal Content Publishing			
Feedback			
DB2 client			
Installation Path for db2java.zip			

Table B-3 Oracle Fact Sheet (1 of 2)

WebSphere Portal Database configuration, Oracle Fact Sheet		
Oracle server		
	Value	Example
Oracle version		Oracle Enterprise Edition 9i Release 2 (9.2.0.1)
Portal databases A total of three databases and six users are required for Portal		
WebSphere Portal Server Database two users required		
Database Name		wps50
Users		wpsdbuser, wmmdbuser
User's Password		
WebSphere Portal Content Publishing database three users required (do not change the user names pznadmin and ejb)		
Database Name		wpcp50
Users	pznadmin, ejb	pznadmin, ejb, wcmdbadm
User's Password		
Feedback Database one user required (do not change the user name feedback)		
Database Name		fdbk50
Users	feedback	feedback
User's Password		
User permissions		
wpsbdusr	connect, resource	
wmmdbadm	connect, resource	
pznadmin	connect, resource	
ejb	connect, resource	
wcmdbusr	connect, resource, insert any table	
feedback	connect, resource	

WebSphere Portal Database configuration, Oracle Fact Sheet		
Permissions required for each user after configuration		
User	Permission	
pznadmin	alter,delete,insert,select,update to EJB.BRBeans_Rule alter,delete,insert,select,update to EJB.BRBeans_RuleFolder	
Oracle Client properties		
	Value	Example
Portal Host where client JDBC driver is to be installed		portal.redbook.com
Oracle version	Oracle JDBC code must be the same version/compatible as the Oracle server	
Note: <ul style="list-style-type: none">▶ All databases must be created as UTF8▶ When creating objects the Portal code will use the users default tablespace▶ For initial configuration each database needs 100Mb of space available▶ For remote DB server, Portal server requires the Oracle JDBC driver (classes12.zip) to be placed in the Portal server		
If necessary, access links below for further instructions:		
<ul style="list-style-type: none">▶ Oracle installation http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/wpf/plan_oracle.html▶ Oracle databases creation and users http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/wpf/cr_oracle_usrs.html		

Table B-4 Oracle Fact sheet (2 of 2)

WebSphere Portal Databases configuration - Oracle Fact Sheet			
Oracle Server			
Hostname			
Port			
Database	Database Name	Users	Passwords
WPS			
WPCP			
Feedback			
Oracle client			
Installation Path for classes12.zip			

Table B-5 IDS Fact Sheet (1 of 2)

WebSphere Portal Databases configuration - IDS Fact Sheet		
LDAP Server	Value	Example
LDAP Server Version		IBM Directory Server V5.1
Required LDAP Portal objects		
Base DN		dc=yourco,dc=com
user prefix		uid
user suffix		cn=users
group prefix		cn
group suffix		cn=groups
Portal admin DN		uid=wpsadmin,cn=users,dc=yourco,dc=com
Bind user DN		uid=wpsbind,cn=users,dc=yourco,dc=com
Portal admin group		cn=wpsadmins,cn=groups,dc=yourco,dc=com
<p>Note:</p> <ul style="list-style-type: none"> ▶ Portal users in the directory should support inetOrgPerson ▶ Sample LDIF file is available for import (see Portal Setup CD) <p>If necessary, access the link below for further instructions for the LDAP configuration:</p> <p>http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/wpf/cfg_ids.html</p>		

Table B-6 IDS Fact Sheet (2 of 2)

WebSphere Portal LDAP Configuration - IDS Fact Sheet	
LDAP Server	
Hostname	
LDAP Service Port	
LDAP Admin user ID	
LDAP admin password	
LDAP Bind user ID	
LDAP Bind password	

Table B-7 SunONE Fact Sheet (1 of 2)

WebSphere Portal Databases configuration - Sun ONE Fact Sheet		
LDAP Server	Value	Example
LDAP Server Version		Sun ONE Directory Server (formerly iPlanet) V5.1 FP2
Required LDAP Portal objects		
Base DN		o=yourco.com
user prefix		uid
user suffix		ou=people
group prefix		cn
group suffix		ou=groups
Portal admin DN		uid=wpsadmin,ou=people,ou=yourco.com
Bind user DN		uid=wpsbind,ou=people,ou=yourco.com
Portal admin group		cn=wpsadmins,ou=groups,o=yourco.com
<p>Note:</p> <ul style="list-style-type: none"> ▶ Portal users in the directory should support inetOrgPerson ▶ Sample LDIF file is available for import (see Portal Setup CD) <p>If necessary, access the link below for further instructions on the LDAP configuration:</p> <p>http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/wpf/images/iplanet.gif</p>		

Table B-8 Sun ONE Fact Sheet (2 of 2)

WebSphere Portal LDAP Configuration - Sun ONE Fact Sheet	
LDAP Server	
Hostname	
LDAP Service Port	
LDAP Admin user ID	
LDAP admin password	
LDAP Bind user ID	
LDAP Bind password	

Silent install sample

The Portal silent install requires that all binary images of the installation CDs are loaded and accessible to the installer. We advise that you load the images on a shared disk drive and distribute the images on separate directories. We also suggest that the names of the directories follow a pattern (for example, cd1-1, cd2, and so on).

Note: If you do not use a naming pattern, refer to technote 1144521 and download the fixed version of the response file. You can find the technote online at the following Web address:

http://www-1.ibm.com/support/docview.wss?rs=688&context=SSHRKX&q1=WpcpCDLoc.cdPath&uid=swg21144521&loc=en_US&cs=utf-8&lang=en

We used this sample response file to install the basic Portal configuration on a Windows 2000 server, including the Application Server, the Enterprise components, fixes, and also WebSphere Portal Content Publishing. We disabled the IBM HTTP Server installation (we set the `-W installIhs.choice` parameter to none). During the Portal installation, we launched WebSphere Application Server and WebSphere Application Server Enterprise installers in the background. Response files were automatically generated based on the parameters defined in the Portal response file. (For more information, see the `was5responsefile.txt`, `was5Pmeresponsefile.txt`, and `wpcp5responsefile.txt` files in the *Portal-install-Directory*\package directory.)

You can monitor the installation by tracking the log files that are created in the Windows temporary directory.

Verifying Portal installation log files

Table B-9 Verification of Portal silent installation

Installation Logs	Description
WebSphere Application Server Logs (Location = C:\WebSphere\AppServer\logs)	
log.txt	<p>WebSphere Application Server installation log.</p> <p>After a successful installation, this file is moved from the Windows temp directory to WebSphere Application Server logs directory . Assume that the following message exists in the end of the log file and that no exceptions have been thrown:</p> <p>INSTFIN: The WebSphere 5.0 install is complete.</p>
WAS.PME.install.log	<p>WebSphere Application Server Enterprise installation log.</p> <p>Assure that the following message exists in the end of the log file and that no exceptions have been thrown:</p> <p>The Summary Panel has the following message: The InstallShield Wizard has successfully installed IBM WebSphere Application Server Enterprise. Choose Finish to exit the wizard.</p>
PMEinstallsummary.log	<p>WebSphere Application Server Enterprise installation summary log.</p> <p>Assure that the following message exists in this file:</p> <p>Installation completed successfully.</p>
ivt.log	<p>Installation Verification Test is run just after WebSphere Application Server installation.</p> <p>Assure that the following message exists in this file:</p> <p>IVTL0080I: Installation Verification is complete</p>

Installation Logs	Description
WebSphere Portal Server Logs (Location = C:\Documents and Settings\Administrator\Local Settings\temp)	
wpsinstalllog.txt	WebSphere Portal installation wrap-up log. After a successful installation the last activity logged would be: Copying file from C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\installmessages.txt to C:\WebSphere\PortalServer\log\installmessages.txt
installmessages.txt	WebSphere Portal installation Summary log. Assure that the following message exists in the end of this file: EJPI0004I The installation has completed successfully.
wpsinstalllog.txt	WebSphere Portal installation log. After a successful installation the last activity logged would be : Logging: WebSphere Portal will listen on port 9081. The Portal welcome page is at http://localhost:9081/wps/portal .

Example: B-1 Portal Silent install response file

```
#####
#
#
# Response File for WebSphere Portal Version 5.0 Silent Installation
#
# Before you can begin the installation of WebSphere Portal you may want to
# first edit this response file with the values appropriate for your
# environment. Refer to the comments to learn how to use the response file and
# understand the various options. You must carefully complete or change the
# various values. If the values are not completed properly, the install may
# be unsuccessful.
#
# IMPORTANT: ALL VALUES MUST BE ENCLOSED IN DOUBLE QUOTES ( " " ).
#
# To use this response file with the installation, specify -options <file-name>
# as a command line argument to the install script, where <file-name> is the
# full path name of this response file.
#
#####
#
#####
#
#
# SILENT INSTALL CHOICE
#
# Description: Specify this parameter if you want to install WebSphere Portal
# silently. When installing silently, the installation program will not
# display
# any graphical interface panels or solicit input from the user. Note that if a
# required parameter is not specified in this response file, an error message
# will be displayed.
#
# If you want to use this response file but do not want to install silently,
# comment this parameter out.
#
#####
#
-silent

#####
#
#
# INSTALL WEBSPPHERE APPLICATION SERVER
#
# Description: Indicate whether you want to install a new instance of WebSphere
```

```

# Application Server or use an existing instance. If you want to use an
# existing instance of WebSphere Application Server that is not at the
supported
# level, you can choose to migrate the instance to the supported level.
#
# Values:
#
#   install - Installs a new instance of WebSphere Application Server.
#
#   use      - Use an existing instance of WebSphere Application Server.
#
#   migrate - Upgrade an existing WebSphere Application Server to the supported
#             level.
#
#####
#

-W installWas.choice="install"

#####
#
#
# WEBSHERE APPLICATION SERVER INSTALLATION LOCATION
#
# Description: Specify the directory where you want to install WebSphere
# Application Server. If you have WebSphere Application Server already
# installed specify the location where it is installed.
#
# Be sure to follow the convention for specifying path information on your
# platform. For example,
#
# Windows 2000: C:\WebSphere\AppServer
# AIX: /usr/WebSphere/AppServer
# Linux: /opt/WebSphere/AppServer
# Solaris: /opt/WebSphere/AppServer
#
#####
#

-W was.location="C:\WebSphere\AppServer"

#####
#
#
# INSTALL WEB SERVER (IBM HTTP SERVER)
#
# Description: Indicate whether you want to install a new Web server or use an
# existing Web server. If you choose to install a new Web server, the
# installation program will install IBM HTTP Server for you automatically.

```

```

#
# Note: This parameter is NOT required if you are using or upgrading an
existing
#       WebSphere Application Server.
#
# Values:
#
#   install - Install IBM HTTP Server
#
#   use      - Use an existing web server
#
#####

-W installIhs.choice="none"

#####
#
#
# IBM HTTP SERVER INSTALLATION LOCATION
#
# Description: Specify the directory where you want to install IBM HTTP Server.
# Application Server.
#
# This parameter is required if you chose to install IBM HTTP Server (specified
# a value of "install" for the installIhs.choice parameter). Otherwise, the
# parameter is not required.
#
# Be sure to follow the convention for specifying path information on your
# platform. For example,
#
# Windows 2000: C:\IBMHttpServer
# AIX: /usr/IBMHTTPServer
# Linux: /opt/IBMHTTPServer
# Solaris: /opt/IBMHTTPServer
#
#####

-W ihs.location="C:\IBMHttpServer"

#####
#
#
# HTTP SERVER TYPE
#
# Description: Specify the type of Web server that you want to use with
# WebSphere Portal.
#

```

```

# Values:
#
#   ihs      - IBM HTTP Server
#
#   apache   - Apache(TM) Web Server
#
#   iis      - Microsoft(TM) Internet Information Services
#
#   iplanet  - iPlanet(TM) Web Server
#
#   domino  - Lotus Domino(TM) Web Server
#
#####
#

-W httpServerType.choice="ihs"

#####
#
# LOTUS DOMINO(TM) WEB SERVER -- NOTES.JAR AND NAMES.NSF FILE LOCATIONS
#
# Description: Specify the file locations for the notes.jar and names.nsf
# files
# used by Lotus Domino Web Server. This parameter is required if you chose to
# use an existing Domino Web Server (specified a value of "domino" for the
# httpServerType.choice parameter).
#
#####
#

-W dominoPlugin.notes=""
-W dominoPlugin.names=""

#####
#
# WEB SERVER CONFIGURATION FILE LOCATIONS
#
# Description: Specify the full path location and file name for the Web
# server's
# configuration file, if you chose to use an existing Web server (specified a
# value of "use" for the installIhs.choice parameter). Each type of Web server
# (except Domino) has its own parameter for specifying the configuration file
# location. You can specify a path value for your Web server and leave the
# other
# Web server parameters empty or comment them out.
#
# Note: This parameter is NOT required if you chose to use a Domino Web server.

```

```

#
# Be sure to follow the convention for specifying path information on your
# platform. For example,
#
# Windows 2000: C:\IBMHttpServer\conf\http.conf
# AIX: /usr/IBMHTTPServer/???
# Linux: /opt/IBMHTTPServer/???
# Solaris: /opt/IBMHTTPServer/???
#
#####
#

#=====#
# IBM HTTP Server Configuration File Location #
#=====#

-W ihsPlugin.file=""

#=====#
# Apache(TM) Web Server Configuration File Location #
#=====#

-W apachePlugin.file=""

#=====#
# iPlanet(TM) Web Server Configuration File Location #
#=====#

-W iplanetPlugin.file=""

#####
#
#
# End of Web Server Configuration File Locations
#
#####
#
#
# WEBSphere APPLICATION SERVER NODE NAME
#
# Description: Specify the node within the WebSphere Application Server cell to
# which the WebSphere Portal application server will belong. This value must be
# unique among other node names in the same cell. Typically this value is the
# same as the host name for the computer.
#
# Note: You must replace the "DefaultNode" value with the node name that you

```

```

# want to use for your default node.
#
#####
#

-W node.name="ka0klfr"

#####
#
#
# WEBSphere APPLICATION SERVER HOST NAME
#
# Description: Specify the fully qualified host name or IP address of the
# computer running WebSphere Application Server. For example,
# "hostname.yourco.com".
#
#####
#

-W node.hostName="ka0klfr.itso.ral.ibm.com"

#####
#
#
# Begin Installing Services
#
#####
#

#####
#
#
# INSTALL THE IBM HTTP SERVER SERVICE (Windows 2000 only)
#
# Description: If you are installing IBM HTTP Server on a machine running
# Windows 2000, specify whether you want to install it as a service. Using
# Services, you can start and stop services, and configure startup and recovery
# actions.
#
# Note: If you are not installing IBM HTTP Server or are installing it on a
# system that is not running Windows 2000, you can ignore this parameter or
# comment it out.
#
# Values:
#
#   true   - Install IBM HTTP Server as service
#
#   false  - Do no install IBM HTTP Server as service
#

```

```
#####
#

-W wasService.ihs="false"

#####
#
#
# INSTALL THE WEBSHERE APPLICATION SERVER SERVICE (Windows 2000 only)
#
# Description: If you are installing WebSphere Application Server on a machine
# running Windows 2000, specify whether you want to install it as a service.
# Using Services, you can start and stop services, and configure startup and
# recovery actions.
#
# Note: If you are not installing WebSphere Application Server or are
# installing
# it on a system that is not running Windows 2000, you can ignore this
# parameter
# or comment it out.
#
# Values:
#
#   true   - Install WebSphere Application Server as service
#
#   false  - Do no install WebSphere Application Server as service
#
#####
#

-W wasService.was="true"

#####
#
#
# USER NAME AND PASSWORD FOR SERVICE INSTALLATION (Windows 2000 only)
#
# Description: If you chose to install either IBM HTTP Server or WebSphere
# Application Server as a service (specified a value of "true" for
# wasService.ihs and wasService.was parameters), you must also specify the
# user name and password that will be used to install the services. In order
# to install the service and have it run properly, the user you specify must
# have administrator authority and "Log on as a service" authority.
#
# Note: If you are not installing WebSphere Application Server or are
# installing
# it on a system that is not running Windows 2000, you can ignore these
# parameters or comment them out.
#
```

```

# Replace the placeholder values "YOUR_USER_NAME" and "YOUR_PASSWORD" with
# appropriate values for your system.
#
#####

-W wasService.user="Administrator"
-W wasService.password="its0ral"

#####
#
#
# WEBSphere PORTAL INSTALLATION LOCATION
#
# Description: Specify the directory where you want to install WebSphere
Portal.
#
# Be sure to follow the convention for specifying path information on your
# platform. For example,
#
# Windows 2000: C:\WebSphere\PortalServer
# AIX: /usr/WebSphere/PortalServer
# Linux: /opt/WebSphere/PortalServer
# Solaris: /opt/WebSphere/PortalServer
#
#####

-W portal.location="C:\WebSphere\PortalServer"

#####
#
#
# WEBSphere PORTAL ADMINISTRATIVE USER AND PASSWORD
#
# Enter the user ID and password for the Portal
# administrator
#
#####

-W portalAdmin.user="wpsadmin"
-W portalAdmin.password="itso"

#####
#
#
# SETUP CD LOCATION
#

```

```

# Description: Specify the directory path to the Setup CD.
# Although this can be to a CD-ROM drive, for unattended
# installation this location is more likely to be a directory where electronic
# product images are stored, such as on a network drive.
#
# Be sure to follow the convention for specifying path information on your
# platform.
#
#####
#

-W cdSetup.cdPath="C:\cds\cdSetup"

#####
#
#
# WEBSPPHERE APPLICATION SERVER CD LOCATION
#
# Description: Specify the directory path to the WebSphere Application Server
# installation images. Although this can be to a CD-ROM drive, for unattended
# installation this location is more likely to be a directory where electronic
# product images are stored, such as on a network drive.
#
# Be sure to follow the convention for specifying path information on your
# platform.
#
#####
#

-W userInputCDLoc2.cdPath="C:\cds\cd1-1"

#####
#
#
# WEBSPPHERE APPLICATION SERVER FIXPACK AND EFIXES CD LOCATION
#
# Description: Specify the directory path to the WebSphere Application Server
# Fixpack and eFixes installation images. Although this can be to a CD-ROM
# drive, for unattended installation this location is more likely to be a
# directory where electronic product images are stored, such as on a network
# drive.
#
# Be sure to follow the convention for specifying path information on your
# platform.
#
#####
#

-W wasfix1MediaLocation.cdPath="C:\cds\cd1-6"

```

```
#####
#
#
# WEBSphere PORTAL CD LOCATION
#
# Description: Specify the directory path to the WebSphere Portal installation
# images. Although this can be to a CD-ROM drive, for unattended installation
# this location is more likely to be a directory where electronic product
# images
# are stored, such as on a network drive.
#
# Be sure to follow the convention for specifying path information on your
# platform.
#
#####

-W WPSCDLoc.cdPath="C:\cds\cd2"

-W WpcpCDLoc.cdPath="$W(WPSCDLoc.cdPath)"

#####
#
#
# PORTAL BASIC CONFIGURATION OPTION
#
# Description: Specify whether you want to perform basic configuration of
# WebSphere Portal automatically when WebSphere Portal is installed. Although
# typically you will perform basic configuration automatically, there might be
# some situations where you want to install WebSphere Portal without performing
# configuration.
#
# Note that if you do not perform configuration during
# installation, you must perform the configuration steps manually. Required
# manual steps include deploying the WebSphere Portal enterprise application
# in WebSphere Application Server and creating WebSphere Portal datasources.
#
# Values:
#
#   yes - Basic configuration is performed automatically as part of the
#         WebSphere Portal installation. This is the default value and is
#         assumed if the basicConfig.choice parameter is not specified.
#
#   no  - Basic configuration is not performed during installation and must be
#         performed manually after installation.
#
#####
#
```

```
# -W basicConfig.choice="no"

#####
#
#
# The options above make this a custom install
#
#####
#

-W setupTypePanel.selectedSetupTypeId="custom"
```

Changing the mode in WebSphere Portal

The process described in this appendix disables edits on portlets or portal pages that were made by the users of the portal. The portal administrator(s) can still edit portlets and portal pages; however, we do not recommend it because changes might be lost.

If a particular installation of WebSphere Portal does not allow users to edit portlets or portal pages, then you do not have to put the portal into read-only mode.

You also do not need to complete this process if you can lose any edits completed by users while Site A is under going maintenance.

The commands in this process assume that the portal administrator(s) will use the XMLAccess tool to place the portal into read-only and read/write mode. You can also use the WebSphere Portal Administration Portlets. The portal administrator(s) decides the final method to use.

The examples shown in Example C-1 on page 260 and Example C-2 on page 262 are based on the sample UpdateAccesscontrol.xml file found in the Reference: Sample XML configuration files topic in the WebSphere Portal InfoCenter at:

<http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/index.html>

Setting read-only mode

To place the Portal in read-only mode, follow these steps:

1. Use the XMLAccess tool to export the page and portlet definitions in a given portal application.
2. Edit the .xml file to at least remove all Privileged User role permissions from the pages and portlets with that permission so defined. You should remove editor, manager, and all other role permissions if they are defined.
3. Never remove the manager role permission from the Portal Administration User ID (wpsadmin) or from the Portal Administration Group (wpsadmins).

Example C-1 shows an example .xml file.

Example: C-1 .xml file

```
<?xml version="1.0" encoding="UTF-8"?>
<request
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="PortalConfig_1.2.xsd"
  type="update"
  create-oids="true">

  <portal action="locate">

<!--Sample portlet entry
  <web-app action="locate" uid="1862436118">
    <portlet-app action="locate" uid="1910792017">
      <portlet action="update" active="true" name="YourCo News">
        <access-control>
          <role-block type="none"/>
          <role actionset="User" update="set">
            <mapping subjectid="anonymous portal user" subjecttype="user"
              update="set"/>
          </role>
          <role actionset="Administrator" update="set">
            <mapping subjectid="uid=wpsadmin,o=default organization"
              subjecttype="user" update="set"/>
            <mapping subjectid="cn=wpsadmins,o=default organization"
              subjecttype="user_group" update="set"/>
          </role>
          <role actionset="Privileged User" update="remove">
            <mapping subjectid="all authenticated portal users"
              subjecttype="user_group" update="remove"/>
          </role>
        </access-control>
      </portlet>
    </portlet-app>
```

```

</web-app>

<!--Sample page entry
  <content-node action="update" uniquename="wps.YourCo Portal.YourCo Area">
    <access-control>
      <role-block type="inheritance" actionset="Manager"/>
      <role actionset="Manager" update="set">
        <mapping subjectid="wpsadmin" subjecttype="USER" update="set"/>
      </role>
      <role actionset="User" update="set">
        <mapping subjectid="anonymous portal user" subjecttype="USER"
          update="set"/>
      </role>
      <role actionset="Privileged User" update="remove">
        <mapping subjectid="all authenticated portal users"
          subjecttype="user_group" update="remove"/>
      </role>
    </access-control>
  </content-node>

</portal>
</request>

```

4. Execute the file against the portal on Site A using the XMLAccess tool.

All customization and personalization permissions are now disabled. You can save this file for future use.

Setting read or write mode

To place the Portal in read or write mode, follow these steps:

1. Copy the file that you used to set the portal to read-only mode.
2. Edit the file to set Privileged User role permission on the pages and portlets where needed.
3. Set the editor, manager, and all other role permissions, if needed.

Example C-2 on page 262 shows an example .xml file.

```
<?xml version="1.0" encoding="UTF-8"?>
<request
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="PortalConfig_1.2.xsd"
  type="update"
  create-oids="true">

  <portal action="locate">

<!--Sample portlet entry
  <web-app action="locate" uid="1862436118">
    <portlet-app action="locate" uid="1910792017">
      <portlet action="update" active="true" name="YourCo News">
        <access-control>
          <role-block type="none"/>
          <role actionset="User" update="set">
            <mapping subjectid="anonymous portal user" subjecttype="user"
              update="set"/>
          </role>
          <role actionset="Administrator" update="set">
            <mapping subjectid="uid=wpsadmin,o=default organization"
              subjecttype="user" update="set"/>
            <mapping subjectid="cn=wpsadmins,o=default organization"
              subjecttype="user_group" update="set"/>
          </role>
          <role actionset="Privileged User" update="set">
            <mapping subjectid="all authenticated portal users"
              subjecttype="user_group" update="set"/>
          </role>
        </access-control>
      </portlet>
    </portlet-app>
  </web-app>

<!--Sample portlet entry
  <content-node action="update" uniqueness="wps.YourCo Portal.YourCo Area">
    <access-control>
      <!-- The manager role should not be inherited automatically from
        parents of this page. -->
      <role-block type="inheritance" actionset="Manager"/>
      <!-- The manager role is set explicitly on this page. -->
      <role actionset="Manager" update="set">
        <mapping subjectid="wpsadmin" subjecttype="USER" update="set"/>
      </role>
      <role actionset="User" update="set">
        <mapping subjectid="anonymous portal user" subjecttype="USER"
          update="set"/>
      </role>
    </access-control>
  </content-node>
</-->
</request>
```

```
        </role>
        <role actionset="Privileged User" update="set">
            <mapping subjectid="all authenticated portal users"
                subjecttype="user_group" update="set"/>
        </role>
    </access-control>
</content-node>

</portal>
</request>
```

4. Execute the file against the portal on Site A using the XMLAccess tool.

All customization and personalization permissions are now enabled. You can save this file for future use.

Switching database servers

This section describes the process to change a working WebSphere Portal V5.0 server from the originally configured external database server to another database server on a different machine. This procedure work for both clustered and single node installations of WebSphere Portal.

The general approach to changing a database server is:

- ▶ Stop WebSphere Portal on the application server machine.
- ▶ Start the server1 application on the application server machine.
- ▶ Backup all WebSphere Portal databases.
- ▶ Restore the WebSphere Portal databases on the second database server.
- ▶ Reconfigure WebSphere Portal to use the databases on the second database server.
- ▶ Restart WebSphere Portal on the application server machine.

Note: Most likely, you will need assistance from an experienced DBA is to transfer Portal data from one database server to another.

Changing from a DB2 database to another DB2 database

To switch from one DB2 database to another DB2 database, do the following:

1. The Database Client code on the WebSphere Portal server contains entries for the Database Server at Site A and the Database Server at Site B. These entries allow your client to move from one database site to another using the following commands:

```
db2 => catalog tcpip node SiteA remote SiteA.yourco.com server 50000 with  
"Primary DB server"
```

```
db2 => catalog tcpip node SiteB remote SiteB.yourco.com server 50000 with  
"Secondary DB server"
```

2. Catalog the WebSphere Portal databases that are on the Site A database server to the WebSphere Portal server using the following commands:

```
db2 => catalog database wps50 at node SiteA
```

```
db2 => catalog database wpcp50 at node SiteA
```

```
db2 => catalog database fdbk50 at node SiteA
```

3. To switch the between the database servers:

- a. Open a command prompt and navigate to the *was_root/bin* directory.

- b. Enter the following command:

```
on UNIX:          ./stopServer.sh WebSphere_Portal
```

```
on Windows:       stopServer.bat WebSphere_Portal
```

- c. Open a DB2 Universal Database Command Line window and uncatalog the WebSphere Portal databases at the WebSphere Portal server using the following commands:

```
db2 => uncatalog database wps50
```

```
db2 => uncatalog database wpcp50
```

```
db2 => uncatalog database fdbk50
```

4. At the primary database server, make a backup of the WebSphere Portal databases using the DB2 Universal Database backup database command.
5. Move the backup file to the second database server
6. Restore the WebSphere Portal databases using the DB2 Universal Database restore database command.
7. At the WebSphere Portal server, catalog the WebSphere Portal databases on the second database server using the following commands:

```
db2 => catalog database wps50 at node SiteB
```

```
db2 => catalog database wpcp50 at node SiteB
```

```
db2 => catalog database fdbk50 at node SiteB
```

8. Change to the *was_root/bin* directory, and enter the following commands:
on UNIX: `./startServer.sh WebSphere_Portal`
on Windows: `startServer.bat WebSphere_Portal`
9. Confirm the operation of WebSphere Portal with the databases on the new database server.

Changing from an Oracle database to another Oracle database

To switch from one Oracle database to another Oracle database, begin with these steps:

1. Open a command prompt and navigate to the *was_root/bin* directory.
2. Enter the following commands:
on UNIX: `./startServer.sh server1`
on Windows: `startServer.bat server1`

on UNIX: `./stopServer.sh WebSphere_Portal`
on Windows: `stopServer.bat WebSphere_Portal`
3. Backup all WebSphere Portal databases on the first database server using the export utility.
4. Move the .dmp file to the second database server.
5. Restore the WebSphere Portal databases on the second database server using the import utility.

Reconfiguring WebSphere Portal to use the databases on the second database server

To reconfigure WebSphere Portal to use the databases on the second database server, you first need to Access the WebSphere Application Server Administrative Console. Point your browser to `http://yourco.com:9090/admin`, where *yourco.com* is the name of the WebSphere Application Server node.

Then, in general for all data sources, follow these steps:

1. Navigate to the Custom Properties window under JDBC Providers.
2. Select the current hostname in the URL parameter.
3. Change the Value parameter with the hostname of the new database server.
4. Repeat these steps for all defined data sources.

The remainder of this section describes the procedure for specific data sources.

wps50DS data source

To reconfigure WebSphere Portal for the wps50DS data source:

1. Change the location of the wps50DS data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wps50JDBC** → **Data Sources** → **wps50DS** → **Custom Properties**.
2. Once at Custom Properties, click **URL**.
3. Change the Oracle machine name in the Value text.
4. Select **OK** to commit the change.

wmmDS data source

To reconfigure WebSphere Portal for the wmmDS data source:

1. Change the location of the wmmDS data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wps50JDBC** → **Data Sources** → **wmmDS** → **Custom Properties**.
2. Once at Custom Properties, click **URL**.
3. Enter the hostname of the new database server in the Value parameter.
4. Select **OK** to commit the change.

feedbackDS data source

To reconfigure WebSphere Portal for the feedbackDS data source:

1. Change the location of the feedbackDS data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wps50JDBC** → **Data Sources (Version 4)** → **feedbackDS** → **Custom Properties**.
2. Once at Custom Properties select **URL**.
3. Enter the hostname of the new database server in the Value parameter.
4. Select **OK** to commit the change.

persDS data source

To reconfigure WebSphere Portal for the persDS data source:

1. Change the location of the persDS data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wpcp50JDBC** → **Data Sources (Version 4)** → **persDS** → **Custom Properties**.
2. Once at Custom Properties, click **URL**.
3. Enter the hostname of the new database server in the Value parameter.

4. Select **OK** to commit the change.

wcmDS Version 4 data source

To reconfigure WebSphere Portal for the wcmDS Version 4 data source:

1. Change the location of the wcmDS Version 4 data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wpcp50JDBC** → **Data Sources (Version 4)** → **wcmDS** → **Custom Properties**.
2. Once at Custom Properties, click **URL**.
3. Enter the hostname of the new database server in the Value parameter.
4. Select **OK** to commit the change.

Completing the change

To complete the switch to the second Oracle database server:

1. Save all changes.
2. Change to the `was_root/bin` directory, and enter the following command:
`startServer WebSphere_Portal`
3. Confirm the operation of WebSphere Portal with the databases on the new database server.

Changing from an SQLServer database to another SQLServer database

To switch from one SQLServer database to another SQLServer database:

1. Open a command prompt and change to the `was_root/bin` directory.
2. Enter the following commands:

on UNIX:	<code>./startServer.sh server1</code>
on Windows:	<code>startServer.bat server1</code>
on UNIX:	<code>./stopServer.sh WebSphere_Portal</code>
on Windows:	<code>stopServer.bat WebSphere_Portal</code>
3. Backup all WebSphere Portal databases on the first database server using the backup database command.
4. Move the backup file to the second database server.
5. Restore the WebSphere Portal databases on the second database server using the restore database command.

Reconfiguring WebSphere Portal to use the databases on the second database server

To reconfigure WebSphere Portal to use the databases on the second database server, you first need to Access the WebSphere Application Server Administrative Console. Point your browser to `http://yourco.com:9090/admin`, where *yourco.com* is the name of the WebSphere Application Server node.

Then, in general for all data sources, follow these steps:

1. Navigate to the Custom Properties window under JDBC Providers.
2. Select the current hostname in the `serverName` parameter.
3. Change the Value parameter with the hostname of the new database server.
4. Repeat these steps for all defined data sources.

The remainder of this section describes the procedure for specific data sources.

wps50DS data source

To reconfigure WebSphere Portal for the wps50DS data source:

1. Change the location of the wps50DS data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wps50JDBC** → **Data Sources** → **wps50DS** → **Custom Properties**.
2. Once at Custom Properties, select the hostname displayed in the value field of the `serverName` parameter.
3. Enter the hostname of the new database server in the Values parameter.
4. Select **OK** to commit the change.

wmmDS data source

To reconfigure WebSphere Portal for the wmmDS data source:

1. Change the location of the wmmDS data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wps50JDBC** → **Data Sources** → **wmmDS** → **Custom Properties**.
2. Once at Custom Properties, select the hostname displayed in the value field of the `serverName` parameter.
3. Enter the hostname of the new database server in the Values parameter.
4. Select **OK** to commit the change.

feedback5 data source

To reconfigure WebSphere Portal for the feedback5 data source:

1. Change the location of the feedback5 data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wpcp50JDBC** → **Data Sources** → **feedback5** → **Custom Properties**.
2. Once at Custom Properties, select the hostname displayed in the value field of the serverName parameter.
3. Enter the hostname of the new database server in the Values parameter.
4. Select **OK** to commit the change.

feedbackDS data source

To reconfigure WebSphere Portal for the feedbackDS data source:

1. Change the location of the feedbackDS data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wpcp50JDBC** → **Data Sources (Version 4)** → **feedbackDS** → **Custom Properties**.
2. Once at Custom Properties, select the hostname displayed in the value field of the serverName parameter.
3. Enter the hostname of the new database server in the Values parameter.
4. Select **OK** to commit the change.

persDS data source

To reconfigure WebSphere Portal for the persDS data source:

1. Change the location of the persDS data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wpcp50JDBC** → **Data Sources (Version 4)** → **persDS** → **Custom Properties**.
2. Once at Custom Properties, select the hostname displayed in the value field of the serverName parameter.
3. Enter the hostname of the new database server in the Values parameter.
4. Select **OK** to commit the change.

wcmDS Version 4 data source

To reconfigure WebSphere Portal for the wcmDS Version 4 data source:

1. Change the location of the wcmDS Version 4 data source by going to Custom Properties. Then, starting at Resources, select **JDBC Providers** → **wpcp50JDBC** → **Data Sources (Version 4)** → **wcmDS** → **Custom Properties**.

2. Once at Custom Properties, select the hostname displayed in the value field of the `serverName` parameter.
3. Enter the hostname of the new database server in the Values parameter.
4. Select **OK** to commit the change.

Completing the change

To complete the switch to the second SQLServer database:

1. Save all changes.
2. Change to the `was_root/bin` directory, and enter the following commands:
on UNIX: `./startServer.sh WebSphere_Portal`
on Windows: `startServer.bat WebSphere_Portal`
3. Confirm the operation of WebSphere Portal with the databases on the new database server.

Capacity planning

This information was provided by IBM WebSphere Portal Support Team.

WebSphere Portal V5 or later database

The following are general sizing (seed) numbers for the WebSphere Portal V5 or later database (not an LDAP plus Look Aside Install, but rather an LDAP only install).

- ▶ Portal layout components:
 - 350 bytes per user
 - 5300 bytes per each Portal application
 - 5360 bytes per portlet
- ▶ General DB2 sizing factors:
 - 5 MB System Table Overhead, per database (potentially WebSphere Portal Server, feedback database (FDBK), and WebSphere Member Manager).
 - Database logs: Log size requirements are not directly tied to data sizes. You can even discard the logs. However, in production environments, they are usually retained for a specified amount of time.
 - A minimum amount of log space would be approximately 20 MB for a fairly static (few writes) Portal install, with a 100 000 user system.

- A maximum amount of log space could be 200 MB or more for a 100 000 user system.
- General DB2 software: 1 GB.

A portal manager for WebSphere Portal

The information in this appendix information is provided for your information.

Note: We did not use this product during the development on this book. However, the information is listed here to provide you with a solution for monitoring and managing your WebSphere Portal environments.

Wily Portal Manager for IBM WebSphere Portal

Monitoring and managing Portal applications in production presents some unique challenges. Unfortunately, when performance problems do occur, problem isolation can become an endless procedure of rebuilding and analyzing each and every portlet in its own test window without the ability to view internal Portal processes and their external interactions.

To solve this problem, Wily Technology leveraged its extensive experience helping customers deploy and manage their IBM WebSphere Portal solutions to create Wily Portal Manager.

Wily Portal Manager delivers 24x7 monitoring of the entire Portal framework during development, staging, QA, and live production. It also extends visibility

beyond the Portal framework, allowing the application manager to identify performance problems both within the Portal and in connections to critical back-end systems including databases, transaction servers, mainframe connections, and more.

Key benefits include:

- ▶ Real-time monitoring that accurately reveals internal Portal activity in the production environment.
- ▶ Comprehensive monitoring of the Portal environment including Portal workflow, individual portlets and connections to back-end systems.
- ▶ Out-of-the-box reporting system for quick and easy analysis of historical performance data.
- ▶ Easy-to-use dashboards that summarize overall Portal health and quickly indicate problem areas within the workflow.
- ▶ Explorer tree views that allow you to precisely isolate problems in individual portlets.
- ▶ Automated threshold alarms that proactively notify you of Portal performance issues before they impact users.
- ▶ Open-standard architecture that easily extends performance monitoring beyond the Portal framework.

For more information about the Wily Portal Manager for WebSphere Portal, visit the following Web site:

http://www.wilytech.com/solutions/products/PortalManager_IBM.html

Additional material

This redbook refers to additional material that you can download from the Internet as described below.

Locating the Web material

The Web material associated with this redbook is available in softcopy on the Internet from the IBM Redbooks Web server. Point your Web browser to:

<ftp://www.redbooks.ibm.com/redbooks/SG246391>

Alternatively, you can go to the IBM Redbooks Web site at:

ibm.com/redbooks

Select **Additional materials** and open the directory that corresponds with the redbook form number, SG246391.

Using the Web material

The additional Web material that accompanies this redbook includes the following files:

<i>File name</i>	<i>Description</i>
SystemOut.log_wpsnode_startup	SystemOut.log_wpsnode_startup file
removeNode.log	removeNode.log file
syncNode.log	syncNode.log file
SystemOut.log_dmgr_startup	SystemOut.log_dmgr_startup file
SystemOut.log_nodeagent_startup	SystemOut.log_nodeagent_startup file
addNode.log	addNode.log

How to use the Web material

Create a subdirectory (folder) on your workstation, and extract the contents of the Web material zipped file into this folder.

Abbreviations and acronyms

B2E	business to employee	WAS	WebSphere Application Server
DBA	database administrator	WASC	WebSphere Application Server Clustering
DHCP	Dynamic Host Configuration Protocol	WCMS	Web content management systems
DMGR	Deployment Manager	WML	Wireless Markup Language
DNS	Domain Name Server	WMM	WebSphere Member Manager
EAR	Enterprise Archive	WP	WebSphere Portal
EJB	Enterprise JavaBeans	WPCP	WebSphere Portal content publishing
FQDN	fully qualified domain name	WPS	WebSphere Portal server
HTML	Hypertext Markup Language	WSRP	Web Services for Remote Portlet
IBM	International Business Machines Corporation	XHTML	Extensible Hypertext Markup Language
IHS	IBM HTTP Server		
ILWWCM	IBM Lotus Workplace Web Content Management		
ITSO	International Technical Support Organization		
JAR	Java Archive		
JMS	Java Message Service		
JVM	Java Virtual Machine		
LDAP	Lightweight Directory Access Protocol		
LTPA	Lightweight Third Party Authentication		
PME	Programming Model Extensions		
RBAC	role-based access control		
SSO	single sign-on		
TAM	Tivoli Access Manager		
UAT	user acceptance testing		
UI	user interface		
URI	Uniform Resource Identifier		
VCS	version control system		
WAR	Web Archive		

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 285. Note that some of the documents referenced here may be available in softcopy only.

- ▶ *Develop and Deploy a Secure Portal Solution Using WebSphere Portal V5 and Tivoli Access Manager V5.1*, SG24-6325
- ▶ *WebSphere Scalability: WLM and Clustering Using WebSphere Application Server Advanced Edition*, SG24-6153
- ▶ *IBM WebSphere Portal for Multiplatforms V5 Handbook*, SG24-6098
- ▶ *Develop and Deploy a Secure Portal Solution Using WebSphere Portal V5 and Tivoli Access Manager V5*, SG24-6325

Online resources

These Web sites and URLs are also relevant as further information sources:

- ▶ WebSphere Portal InfoCenter, section Product Overview
<http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/index.html>
- ▶ WebSphere Portal Documentation Library
<http://www-106.ibm.com/developerworks/websphere/zones/portal/proddoc.html>
- ▶ Oracle Corporation, Oracle Technology Network
<http://otn.oracle.com/pls/tahiti/tahiti.initora>
- ▶ WebSphere Server Best Practices
http://www.ibm.com/software/webserver/appserv/ws_bestpractices.pdf
- ▶ *Develop and Deploy a Secure Portal Solution Using WebSphere Portal V5 and Tivoli Access Manager V5.1*, SG24-6325-00
<http://www.redbooks.ibm.com/redbooks/pdfs/sg246325.pdf/>

- ▶ Guide to WebSphere Portal 5.0
http://www-106.ibm.com/developerworks/websphere/library/techarticles/0310_wendel/wendel.html
- ▶ *IBM WebSphere Portal for Multiplatforms V5 Handbook*, SG24-6098
<http://www.redbooks.ibm.com/abstracts/sg246098.html>
- ▶ WebSphere Portal for Multiplatforms Version 5.0.2 Cumulative Fix 1 (5.0.2.1)
http://publib.boulder.ibm.com/pvc/wp/5021/ent/en/InfoCenter/wpf/inst_req.html
- ▶ WebSphere Portal for Multiplatforms Version 5.0.2.1 Release Notes
http://publib.boulder.ibm.com/pvc/wp/5021/ent/en/release_notes_ent.html
- ▶ Windows 2000 service packs
<http://www.microsoft.com/windows2000/downloads/servicepacks/default.asp>
- ▶ AIX maintenance page
<http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp>
- ▶ WebSphere Application Server support
<http://www-306.ibm.com/software/webservers/support.html>
- ▶ WebSphere Portal Server support
<http://www-306.ibm.com/software/genservers/portal/support/>
- ▶ WPS50 Install on Windows 2003
http://www-1.ibm.com/support/docview.wss?rs=688&context=SSHRKX&q1=Windows+2003&uid=swg21173948&loc=en_US&cs=utf-8&lang=en
- ▶ Configuring the Web server
http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/wpf/inst_ihs.html
- ▶ Concepts, Planning, and Installation for Edge Components
<http://www-306.ibm.com/software/webservers/appserv/doc/v50/ec/infocenter/edge/concepts.htm>
- ▶ UpdateInstaller for WebSphere Application Server V5.0 releases
<http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&uid=swg24001908>
- ▶ WebSphere Application Server 5.0 fp2 (Base/ND)
<http://www-1.ibm.com/support/docview.wss?rs=180&tc=SSEQTP&uid=swg24005012>
 download and unzip to c:\cds\patches\was50_fp2_base

- ▶ WebSphere Application Server 5.0 fp2 (PME)
http://www-1.ibm.com/support/docview.wss?rs=823&context=SS4QY3&q1=fixpack&uid=swg24005055&loc=en_US&cs=utf-8&lang=en
- ▶ WebSphere Application Server 5.0.2 fixes required by WebSphere Portal V5.0.2
http://www-1.ibm.com/support/docview.wss?rs=688&context=SSHRKX&q1=5.0.2&uid=swg24006343&loc=en_US&cs=utf-8&lang=en
- ▶ WebSphere Application Server 5.0.2 cumulative fix 2 (Base/ND)
http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&q1=5.0.2+Cumulative+fix+2&uid=swg24005952&loc=en_US&cs=utf-8&lang=en
- ▶ IBM WebSphere Application Server - Readme for the update installer application for Version 5.0.2
ftp://ftp.software.ibm.com/software/websphere/appserv/support/tools/UpdateInstaller/readme_updateinstaller.html
- ▶ Installing WebSphere Portal V5.0.2 on V5.0 platforms (Windows 2000 and UNIX)
http://publib.boulder.ibm.com/pvc/wp/502/ent/en/readme/install_win_unix.html
- ▶ Cumulative Fix Strategy for WebSphere Application Server V5.0 and V5.1 releases
http://www-1.ibm.com/support/docview.wss?rs=860&context=SW600&q1=fix+strategy&uid=swg21145289&loc=en_US&cs=utf-8&lang=en
- ▶ Technote 1162831, Cumulative fix compatibility between Base and Network Deployment Editions, and Enterprise Edition
http://www-1.ibm.com/support/docview.wss?rs=860&context=SW600&q1=fix+strategy&uid=swg21162831&loc=en_US&cs=utf-8&lang=en
- ▶ Technote 1173471, Clarification on the WebSphere Portal version 5.0.2.1 installation
http://www-1.ibm.com/support/docview.wss?rs=688&context=SSHRKX&q1=clarification&uid=swg21173471&loc=en_US&cs=utf-8&lang=en
- ▶ Technote 1140712, Installing WebSphere Application Server V5.0 Enterprise Edition_FAQ
<http://www-1.ibm.com/support/docview.wss?uid=swg21140712>
- ▶ LDAP
http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/wpf/intr_ldap.html
- ▶ Cloudscape database
http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/wpf/intr_db.html

- ▶ A step-by-step guide to configuring a WebSphere Portal V5 cluster
http://www-106.ibm.com/developerworks/websphere/library/techarticles/0401_1amb/1amb2.html
- ▶ Portal V5.0.2 prerequisites
http://publib.boulder.ibm.com/pvc/wp/5021/ent/en/InfoCenter/wpf/inst_req.html
- ▶ Portal catalog
<http://www.ibm.com/software/genservers/portal/portlet/catalog>
- ▶ Developer domain, Portal articles
<http://www-106.ibm.com/developerworks/apps/ViewServlet.wss?viewType=Library&topic=0&count=10&keyword=Portal&prodfam=0&devDomain=wsdd&format=0&sortBy=Posted&start=1&showAll=true>
- ▶ Portal tutorial- Web based course about Portal fundamentals
<http://www-106.ibm.com/developerworks/websphere/library/tutorials/d1/sw741>
- ▶ Portal administrative roadmap
<http://www-106.ibm.com/developerworks/apps/transform.wss?URL=/developerworks/websphere/zones/portal/roadmaps/portal-roadmaps.xml&xslURL=/developerworks/websphere/xsl/roadmaps.xsl&format=two-column&role=admin-mp#installation>
- ▶ Using Credential Vault to Provide Single Sign-on for Portlets
http://www-106.ibm.com/developerworks/websphere/library/techarticles/0211_konduru/konduru.html
- ▶ WebSphere Portal Version 5.0 with your security infrastructure
ftp://ftp.software.ibm.com/software/websphere/pdf/WS_Portal_Security_G325-2090-01.pdf
- ▶ *Develop and Deploy a Secure Portal Solution Using WebSphere Portal V5 and Tivoli Access Manager V5.1*, SG24-6325,
<http://publib-b.boulder.ibm.com/abstracts/sg246325.html?Open>
- ▶ Tech Doc, WebSphere Portal with Tivoli Access Manager: Value Beyond Security
<http://www-1.ibm.com/support/techdocs/atmastr.nsf/WebIndex/WP100426>
- ▶ WebSphere Portal Support
<http://www-306.ibm.com/software/genservers/portal/support/>
- ▶ J2EE 1.3 Downloads
<http://java.sun.com/j2ee/1.3/download.html#platformspec>
- ▶ Portlet Specification 1.0
<http://www.jcp.org/aboutJava/communityprocess/review/jsr168>

- ▶ Servlet Specification 2.3
<http://www.jcp.org/aboutJava/communityprocess/final/jsr053>
- ▶ About the XML configuration interface
<http://publib.boulder.ibm.com/pvc/wp/502/ent/en/InfoCenter/wps/adxmlabt.html>
- ▶ WSadmin tool
http://publib.boulder.ibm.com/infocenter/wasinfo/topic/com.ibm.websphere.base.doc/info/aes/ae/rxml_commandline.html
- ▶ Installing WebSphere Portal in a cluster environment
http://publib.boulder.ibm.com/pvc/wp/500/ent/en/InfoCenter/wpf/inst_cluster.html#deploythemes
- ▶ For more information about the Wiley Portal Manager for IBM WebSphere Portal, visit the following Web site:
http://www.wilytech.com/solutions/products/PortalManager_IBM.html

How to get IBM Redbooks

You can search for, view, or download IBM Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy IBM Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Archived

Index

Symbols

.ear extension 88
.war extension 88
.xml file samples 260, 262

A

access control list 116
accessibility support 24
active configuration 18
Active Directory 75–76, 79
adminId 164
administrator user ID 33, 203, 236
adminPassword 164
aggregation 89
AIX
 database server 221
 environment 220
 maintenance page 29
 network configuration 35
 networking 227
 version for production server 32
 vpd.properties file 38
AIX environment variables
 MALLOCMULTIHEAP 224
 RDBM_CACHE_SIZE 224
 SPINLOOPTIME 224
anonymous pages 3, 7
ANT 113
Application Client JAR file 88
application data 5
application providers 10
application server 4, 108, 150, 265
application server cloning 220
application server tuning 216
architecture building blocks 5
audit and reporting services 12
authentication 66–67, 69, 72
authorization data 5
Availability Gold Standard 18

B

back-end application administrator 2

back-end servers 28, 59, 220

back-end systems 3, 16

backup

 applying 173

 offline 172

 our approach 169

 procedure 167

 scheduling 174

 strategy 174

batch files 123

batch mode 99

batch processing interface 115

C

cachable protocol 15

cache 3, 15

Caching Proxy 8

capacity planning 25

cascading style sheets (CSS) 3, 107

child nodes 89

class garbage collection 217

clip levels 25

cloning an application 13

cloning, application server 220

cloning, horizontal 220

cloning, vertical 220

CloudScape 59, 150, 173

cluster 60, 95, 97, 100, 108, 179

cluster topologies 196

cluster, creating 63

cluster, deploying a portlet

 portlet

 deployment 95

cluster, elaborated 16

cluster, elaborated security 17

cluster, horizontal 14

cluster, LDAP server 82

cluster, Linux 27

cluster, vertical 13–14

collaboration 24

collaboration specialist 2

collaborative Portal 9

conceptual node 3, 13

- concurrent users 26
- configuration
 - active and passive 18
 - data 5
 - failure 84
- containers 88
- Content Access Service 66
- content management 24
- Content Management portlets 138
- content node element 140
- content trees 113
- ContentAccessService 106
- continuous operation 19
- CPU usage per server, average 26
- credential store 11
- Credential Vault 69, 71–72
 - administrative slot 71
 - CredentialSlotConfig class 70
 - CredentialVaultPortletService object 69
 - CredentialVaultService 106
 - portlet 70
 - portlet private slot 71
 - shared slot 71
 - system slot 71
- cross-functional teams 2
- cumulative fix2 for Network Deployment 57
- customization data 5

D

- data
 - application 5
 - authorization 5
 - configuration 5
 - customization 5
 - personalization 5
 - session 5
 - user 5
- data source connection pool size 218
- data store component 4
- data types 4
- database administrator (DBA) 2, 22, 61, 67, 150, 195, 265
- database manager 28
- database performance 223
- database server 2, 4, 23, 59, 149, 174
- database server tuning 220
- DB2 25, 61, 150–151, 266
- DB2 UDB command line 151, 266

- DB2 UDB Enterprise 59
- dedicated servers 28
- Default Vault Segment 66
- Delete_Portlets.xml 234
- deployment descriptor values 92
- Deployment Manager
 - activating portlets 137
 - Administrative Console 67–68, 97
 - checking nodes 193
 - host name 186, 192, 212
 - logs 175
 - rebuilding cluster 213
 - removing cluster member 181, 189
 - security settings 82
 - server 125
 - setting trace 175–176
 - SOAP connector address 186, 192, 212
 - stopping cluster member 181, 188
 - transfer directory 125
- DeployTheme.xml 122
- development server 23
- directory hierarchy structure 91
- directory server 2, 5
- directory server tuning 223
- directory services 24
- directory structure 45, 123
- Dispatcher 40
- dispatcher 2
- DNS configuration 41
- DNS hostname string 146
- DNS server 236
- Domain Name System (DNS) 146
- Domino 3, 9, 225
- Dynamic Host Configuration Protocol 146

E

- EAR file 88, 105
- EAR operation directory 125
- EAR operation server 125
- Edge Server 25–26
- efixes directory 50
- elaborated cluster 16
- elaborated security cluster 17
- electronic certificates 66
- Enterprise Archive file. See EAR file.
- Enterprise JavaBeans 112
- environment variables
 - MALLOCMULTIHEAP 224

- RDBM_CACHE_SIZE 224
- SPINLOOPTIME 224
- example worksheet 124
- expertise 22
- export
 - custom 120
 - sample page 119
 - scripts 123
- exporting via the XMLAccess tool 115
- ExportWelcomePage.xml 120
- Extensible Markup Language. See XML.

F

- federation security services 12
- feedback5 data source 158, 271
- feedbackDS data source 154, 159, 268, 271
- file descriptor variable 226
- file.xml 116
- firewall security 7
- fixes 29, 42, 55, 58
- fixpacks 42, 58, 197
- forward proxy 2, 4
- fragment 90
- FTP 177
- fully-qualified domain name 38
- fully-qualified domain name hostname 41

G

- getCredential method 69
- Graphical User Interface mode (GUI) for Web-Sphere Portal 37
- groupCacheRefreshInterval 78

H

- heterogeneous IT environments 12
- hierarchical structure of nodes 89
- homogenous database servers 150
- horizontal cloning 13
- horizontal cluster 14, 27
- horizontal scaling 13
- host systems 3
- HostName parameter 236
- hostname property value 146
- hostname, fully-qualified domain name 41
- HTML pages 7, 112
- HTTP
 - caching directives 4

- connection 115
- content 4
- HTTP Server 2, 25
- Hypertext Markup Language (HTML) 90, 112

I

IBM

- Directory Server 59, 75, 161, 225
- Dispatcher 40
- Redbooks Web site 285
- IBMDEFAULTBP parameter 223
- IDS 25, 28
- IDS parameters
 - lbm-slapdACLCacheSize 223
 - lbm-slapdDbConnections 223
 - lbm-slapdEntryCacheSize 223
 - lbm-slapdFilterCacheBypassLimit 223
 - lbm-slapdFilterCacheSize 223
- IFrame portlet 71
- ILWWCM portlets 138
- images 3, 7
- import
 - custom page 120
 - via the XMLAccess tool 115
- InfoCenter Web site 8, 24, 26, 29, 33, 60
- information systems 89
- infrastructure worksheet 30
- init-param 92
- install_portlet.xml 231
- installation
 - compiling documents 29
 - log file 39
 - planning 22
 - prerequisites 28
 - process 30
 - worksheet 29
- installation, silent 37
- IT architect 22

J

- J2EE 88
- J2EE 1.3 specification 88
- J2EE artifacts 112
- jacl script 101
- JAR file 88, 105
 - Application Client 88
 - EJB 88
- Java

- Enterprise JavaBeans 112
- JavaScript example 72
- JavaScript files 3
- JavaScript libraries 7
- JavaServer Pages (JSPs) 90–91
- process 50
- Technote 1173948 37
- Virtual Machine heap size 217
- Java 2 Platform, Enterprise Edition. See J2EE.
- Java Archive file. See JAR file.
- JDBC Providers 153, 157, 267, 270
- JNDI DirContext 77
- jndi.properties 226

L

- label 89, 112
- latency 15
- LDAP
 - administration 83
 - architecture 81
 - calls 74
 - compliant component 25
 - connection pool 77
 - directory 28
 - integration 73
 - LDAPBP parameter 223
 - ldapHost property 163
 - ldapPort property 163
 - LDAPSuffix property 74
 - schema layout 81
 - server 23, 59, 161, 174, 223
 - server, cluster 82
 - specialist 22
- Lightweight Directory Access Protocol. See LDAP.
- Linux 32
 - network configuration 36
 - vpd.properties file 38
- Linux cluster 27
- Load Balance server, front-end 26
- Load Balancer 22, 25, 39–40
- LoadRunner script 223
- local loopback 146
- Local Security Policy 33
- log files 38–39, 137, 175, 177, 226, 245–246
- Lotus Domino 3, 9, 225
- Lotus Workplace Performance 215

M

- maintenance 195
- maintenance packages 29
- Manage Pages 94
- Manage Pages portlet 93
- Manage Portlet Applications 104
- MaxClients 225
- middleware 13
- mobile devices 24
- multicast error 63

N

- navigation 116
- Netegrity SiteMinder 10, 12
- netstat command 31
- network
 - AIX configuration 35
 - firewall 66
 - layer performance 227
 - Linux configuration 36
 - setup 30
 - team 2
 - tuning 227
- Network Deployment server 22, 38
- node 89
- node agents 68
- NodeAgent 137
- NodeAgent logs 175
- nodeMaps tag 77
- Novell eDirectory 75
- nternationalization 24
- numeric IP address 146

O

- object ID 115, 117, 203
- objectCategory 76
- ObjectGUID attribute 79
- off-line backup 151, 162, 172–173
- off-line recovery 172
- operating system 30
- operational architecture 1
- operational building blocks 5
- Oracle 25, 59, 61, 152, 222, 267

P

- page views per second 26
- pages 89, 116

- parameters
 - dirContextsMaxSize 78
 - dirContextsMinSize 78
 - dirContextTimeout 78
 - HostName 236
 - IBMDEFAULTBP 223
 - lbm-slapdACLCacheSize 223
 - lbm-slapdDbConnections 223
 - lbm-slapdEntryCacheSize 223
 - lbm-slapdFilterCacheBypassLimit 223
 - lbm-slapdFilterCacheSize 223
 - LDAPBP 223
 - MaxFreeTcbs 228
 - MaxHashTableSize 228
 - MaxUserPort 228
 - TcpMaxConnectionRetransmission 228
 - TcpNumConnections 228
 - TcpTimedWaitDela 228
 - Xnoclassgc 217
- passive configuration 18
- passive credential 69
- password maintenance 66
- password management services 12
- password revision schedule 66
- patches 29
- performance 215
- performance parameters 26
- persDS data source 155, 160, 268, 271
- persisted data 5
- personalization data 5
- PKZIP 173
- pluggable user interface components 90
- plug-in file 202
- plug-ins 26
- portlet
 - activating 137
 - application 71, 90
 - application definition 91
 - classes 91
 - configurations 118
 - container 90
 - Content Management 138
 - Credential Vault 70
 - Custom Unique Names 117
 - definition 90–91
 - Delete_Portlets.xml 234
 - descriptor values
 - custom-portlet-mode 92
 - custom-window-state 92
 - portlet-name 92
 - user-attribute 92
 - IFrame 71
 - ILWWCM 138
 - install_portlet.xml 103
 - instances 113
 - JSPs 112
 - life cycle 90
 - Manage Pages 93
 - Manage Portlet Applications 104
 - portlet.xml 91
 - PortletContext.getService() method 106
 - service classes 106
 - source directory 125
 - start_portlet.xml 103
 - technology 87
 - WebClipping 67
 - World Clock 99
 - XMLAccess tool 116
- Portlet Service Registry 66
- ports
 - Bootstrap 30
 - DRS Client Address 30
 - HTTP Admin Console 30
 - HTTP Admin Console Secure 30
 - HTTP Transport 30
 - HTTPS 30
 - JMS Server Queued 30
 - JMS Server, internal 30
 - SOAP Connector 30
- production
 - database 184
 - environment 37, 105, 150, 162
 - server 32
 - system 113
- Programming Model Extensions technotes 55
- proxy authentication 66
- proxy server 3, 66

Q

- Q/A environment 83
- Quickplace 9

R

- RASUtils.jar 177
- RASUtils.txt 177
- recovery 167, 170, 173
- recovery, off-line 172

- Redbooks Web site
 - Contact us xiv
- relational database 150
- release manager 113
- Remote Access Services (RAS) Tool 177
- remote desktop 31
- remote portlet providers, Web services 3
- response time 26
- result.xml 116
- reverse caching proxy 2
- reverse proxy 3
- reverse proxy server 3
- reverse security proxy 2
- RippleStart 137, 183, 187, 191, 193
- roadmap 24
- role-based access control 12
- row containers 89

S

- Sametime 3, 9
- samples 235
- scaling, horizontal 13
- scaling, vertical 13
- screen source directory 124
- search 24
- searchBases 77
- security
 - Deployment Manager 82
 - filters 225
 - firewall 7
 - framework 72
 - guidelines 67
 - management 65, 72
 - server 2
 - specialist 22
 - WebSphere Portal 24
 - WebSphere Portal structure 10
- server tuning
 - settings
 - access logging 225
 - KeepAlive 224
 - KeepAliveTimeout 224
 - MaxClients 224
 - MaxKeepAliveRequests 224
 - MaxRequestsPerChild 224
 - StartServers 224
 - ThreadsPerChild 224
- serverName parameter 158, 270

- servlet 3, 112
- servlet engine thread pool size 218
- session data 5, 13
- Set Timeout parameter 217
- shell scripts 126
- shell scripts location 124–125
- single security policy server 10
- single sign on 10
- Single Sign On support 72
- single sign-on 10, 24, 34, 71
- single-node Portal server 23
- SiteMinder 17, 138
- skills 22
- skin source directory 124
- skins 105, 112
- software point releases 195
- Solaris 219, 226–227
- source code 112
- source directory 125
- source server 124
- source URL 124
- SQLServer 156, 269
- staging 23, 113, 150, 161
- standby mode 19
- start_portlet.xml 232
- static
 - components 4
 - content 15
 - HTML pages 3
 - IP address 34
 - markup pages 91
 - page 4
 - resource 3–4
- stylesheets 7
- Sun ONE 25, 28, 59, 75
- support 177
- surfacing an application 71
- SUSE SLES Linux 32
- switching database servers 265
- sync_all_nodes.jacl 232
- SynchLog 137
- SystemOut.log 137

T

- tar command 173
- target directory 124
- target server 125
- target URL 125

- taxonomy 24
- TCP/IP 34
- Technote 1140712 55
- Technote 1145289 55
- Technote 1162831 55
- Technote 1173471 55
- term definition 2
- terminal services client 31
- text console mode for WebSphere Portal 37
- theme source directory 124
- themes 105, 112
- ThreadsPerChild 225
- three tier architecture 6
- Tivoli Access Manager 10, 17, 72, 138
- Tivoli Intelligent Orchestrator 2
- Tivoli Performance Viewer 218
- topology definition 25–26
- TraceString property 176
- transfer directory 123–125
- transfer process 118
- tuning parameter 216

U

- Uniform Resource Identifier 116
- UniqueNames 122
- UNIX 33, 124, 126, 149, 156, 161, 164, 226
- UNIX shell scripts 124
- Update Installer 177, 192
- UpdateInstaller tool 44, 55, 58
- Updatesilent command 50
- URL-addressable resource 89
- user acceptance testing (UAT) 23
- user data 5
- User Rights Assignment 33
- user-password pairs 66

V

- value column 29
- vault segment 70
- vault slot 70–71
- verification testing 63
- version control system 112
- vertical clone 220
- vertical cluster 13–14
- vertical scaling 13
- vpd.properties 37

W

- WAR file 88, 96, 105, 140
- wcmDS Version 4 data source 155, 160, 269, 271
- Web Application Container 89
- Web applications 3
- Web Archive file. See WAR file.
- Web component 90
- Web Content Management Systems 3
- Web server 4, 22, 25, 31, 39, 174
- Web server tuning 224
- Web Services for remote portlet providers 3
- WebClipping portlets 67
- WebSphere
 - cumulative fix2 for Network Deployment 57
 - Network Deployment 38
 - parameters
 - dirContextsMaxSize 78
 - dirContextsMinSize 78
 - dirContextTimeout 78
 - ports
 - Bootstrap 30
 - DRS Client Address 30
 - HTTP Admin Console 30
 - HTTP Admin Console Secure 30
 - HTTP Transport 30
 - HTTPS 30
 - JMS Server Queued Address 30
 - JMS Server, internal 30
 - SOAP Connector 30
- WebSphere Application Server
 - Administrative Console 68, 153, 157, 267, 270
 - clustering 14
 - fixpacks 210
 - interim fixes 204
 - logs 176
 - main ports 30
 - Network Deployment 25, 39
 - Portal server 89
 - server tuning 216
 - support 29
 - technotes 55
- WebSphere Edge Server 40
- WebSphere Member Manager 68, 76–80, 83, 273
 - fixes 74
 - groupMembership attribute 74
 - MemberOf attribute 74
 - performance tips 74
- WebSphere Portal
 - admin user 124

- admin user password 124
- administration 70
- Administration Interface 122
- Administration page 70
- administrator 22
- artifacts 111, 115, 118
- back-end server 216
- backup and recovery 167
- basic installation 5
- changing database servers 149
- changing LDAP servers 161
- Click-to-Action 25
- clusters 178
- Collaboration 25
- connection, definition of 2
- Content management 25
- content publishing 2, 68
- credentials 67
- CredentialVaultService 106
- database considerations 222
- databases 197
- deployment 63
- Deployment Manager 2
- deployment unit, definition of 2
- deployment units 3
- documentation 63
- Enable environment 9
- Extend environment 9
- Extend Search 25
- fixes 55
- Graphical User Interface mode (GUI) 37
- InfoCenter Web site 8, 24, 26, 29, 33, 60
- installer 34
- log 175
- maintenance 174, 188, 195
- Multiplatforms Version 5.0.2.1 26
- navigation tree 89
- node, definition of 2
- operational architecture 1
- Personalization 25
- Portal page 92
- portlet configurations 118
- release notes 28
- roadmap 24
- samples 235
- search 2
- security 24
- security guidelines 67
- security management 65, 72
- security structure 10
- Server 30, 273
- Server Cluster 3
- Server support 29
- silent installation mode 37
- Single Sign On 25
- site map 118
- skin definitions 118
- standard installation without a cluster 6
- support 177
- text console mode 37
- theme 107
- theme definitions 118
- topology 72
- Translation 25
- Update Installer 177, 192
- URL mappings 118
- Web application configurations 118
- Wily Portal Manager 275
- WebSphere Studio 112
- Windows 171
 - database server 221
 - networking 228
 - vpd.properties file 38
 - Windows 2000 service packs 29
 - Windows 2003 Server Standard Edition 31
- Windows 2000 44
- Windows systems
 - backup and recovery 171
- WinZip 173
- wmmDS data source 154, 158, 268, 270
- workload management 220
- worksheet 29, 235
- World Clock portlet 99
- wpconfig.properties 68, 184
- WPRASCollect.zip 177
- WPS.ear 89, 107
- wps50DS data source 153, 157, 268, 270
- wpsadmin 95
- WpsHostName 184
- WpsHostPort 184
- wsadmin script 113, 147

X

- XML 99–100, 103–104
- XML config location 124–125
- XML configuration interface. See XMLAccess tool.
- XML sample files 260, 262

XML schemes 99
XML scripts 102
XMLAccess tool 99–100, 102–103, 105, 114–119,
123, 127, 135, 137, 139, 168–169, 231
xmlaccess.bat 115
xmlaccess.sh 115
-Xnoclassgc parameter 217

Y

YasT Control Center utility 36



WebSphere Portal V5.0 Production Deployment and Operations Guide

(0.5" spine)
0.475" <-> 0.875"
250 <-> 459 pages



Redbooks

WebSphere Portal V5.0 Production Deployment and Operations Guide

WebSphere Portal operational architectures

Deployment of a Portal production environment

Procedures for various administration tasks

This IBM Redbook contains best practices for deployment and operational support of WebSphere Portal V5 in a production environment. It addresses the questions on how to initially deploy WebSphere Portal. After you have deployed WebSphere Portal, you can use the operational best practices described in this redbook for themes, skins, pages, and portlet updates in a 24/7 enterprise.

This redbook discusses the common notations for WebSphere Portal operational architecture and terminology. The architectures described in this redbook are examples used to present WebSphere Portal operation alternatives that allow you to combine, mix, and define your own Portal architecture.

Portal administrators can find in this redbook an installation roadmap that includes a suggested approach, best practices, links to required resources, and hints to perform a successful installation and configuration. When the staging environment has been set, this redbook also provides helpful instructions on moving the Portal into production.

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