A step-by-step guide to configuring a WebSphere Portal v6.0.1.0 cluster using WebSphere Application Server v6.0.2.17 and WebSphere Process Server v6.0.2.1

Table of contents

About the example environment.....4
Install Deployment Manager (DMGR) ……...6
Install WAS v6.0.2.9
Install WPS v6.0.1.1
Create DMGR profile
Upgrade WAS v6.0.2.9 to v6.0.2.17 and WPS v6.0.1.1 to v6.0.2.1
Install WPSv6.0.1 on on future cluster node, Node1……13
Install WAS v6.0.2.9
Install WPS v6.0.1.1
Create Custom profile
Upgrade WAS v6.0.2.9 to v6.0.2.17 and WPS v6.0.1.1 to v6.0.2.1
Prepare the DMGR and Node1 for the Portal install
Install WPv6.0.0.0 on the managed node, Node1
Re-enable auto-sync between DMGR and Node1
Upgrade WPv6.0.0.0 to WP v6.0.1
Migrate portal node1 database to DB2v 8.2.14 database ……..34
Create a cell level data source
Configure Portal to use a remote IBM HTTP Server v6.0……49
Install IBM HTTP Server on DMGR machine
Install plug in on DMGR
Configure IBM HTTP server on DMGR
Create the cluster of primary node ……..53
Install WPSv6.0.1 on on future cluster node, Node2 ……..54
Install WAS v6.0.2.9
Install WPS v6.0.1.1
Create a Custom profile
Upgrade WAS v6.0.2.9 to v6.0.2.17 and WPS v6.0.1.1 to v6.0.2.1
Install WPv6.0.0.0 on the managed node, Node2
Add node2 to the cluster
Upgrade WPv6.0.0.0 to WP v6.0.1
Configure Portal Node 1, Portal Node 2 and the DMGR for LDAP security with Realm Support ……..76

This guide describes a comprehensive procedure for installing, configuring, and building an IBM® WebSphere® Portal V6.0.1.0 cluster using:

IBM WebSphere Application Server 6.0.2.17
IBM WebSphere Process Server 6.0.2.1
Windows® 2003 Server
DB2 v8.2.14
IBM Tivoli Directory Server v5.2
IBM HTTP Server 6.0

To perform the tasks described here you need basic WebSphere Portal and WebSphere Application Server knowledge and administration skills. Some steps might require the assistance of another system administrator, such as the database administrator or LDAP administrator.

Introduction

Building and configuring a cluster can be a very complex task. You can build portal clusters in various ways. This article provides a best practice approach for building a cluster environment using WebSphere Portal. This example produces a two-node horizontal cluster, as shown in Figure 1. Your environment might require special considerations, but you should still follow this step-by-step approach as an overall guide.

Although this guide is specifically written for WP v6.0.1.0 and WAS v6.0.2.17 and WPS v6.0.2.1 versions, the same approach will apply to any WP v6.0.x version and any WAS 6.0.x/WPS 6.0.x version as well.

The guide will also use the following acronyms:
WP – WebSphere Portal
WPS – WebSphere Process Server
WAS – WebSphere Application Server

About the example environment

This guide shows you how to configure a cluster consisting of:

- Two WebSphere Portal V6.0.1.0 nodes, called PNode and SNode
- A database server, in this case, DB2 v8.2.14, which contains the WebSphere Portal, WebSphere Member Manager, and WebSphere Portal content publishing databases
- A single Web server, IBM HTTP Server V6.0.0.0
- The LDAP server, in this case IBM Tivloi Directory Server V5.2
- The Deployment Manager, which is installed from the Application Server V6.0.2.9 Network Deployment package.

In this example scenario, PNode and SNode are Windows Server 2003 with Service pack 2 systems, and the backend data storage is DB2. The Data item represents various databases, which are set up by WebSphere Portal:

- wpsdm: portal Release database
- commdb: portal community database
- custdb: portal customization database
- jcrdb: portal JCR database
- wmmdb: portal member manager database

Introductory Note: Through out this document we will use the following short names for the installation and configuration of portal, application and process server:

wp_server_root: Root directory for WebSphere Portal
was_server_root: Profile directory for WebSphere Application Server
was_profile_root: Profile directory for application Server
was_config_root: Configuration files directory of Application Server
wp_config_root: Configuration files directory of Portal Server

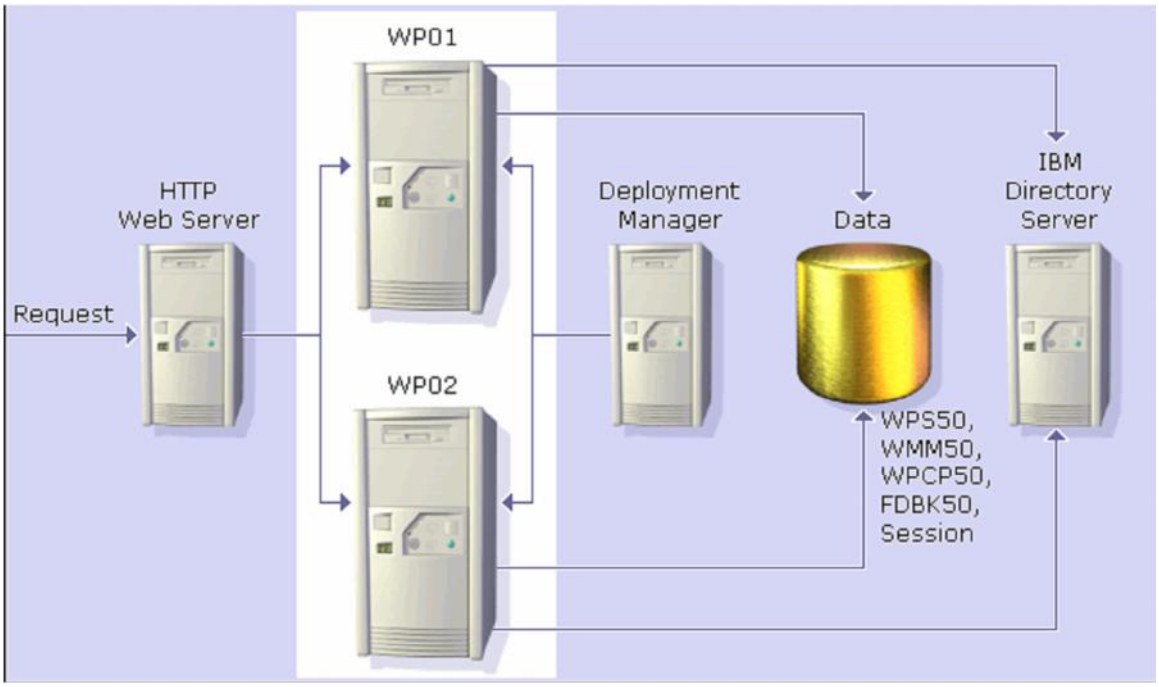


Figure-1 Target portal cluster

Additional Introductory Note: This guide also introduces the WebSphere Process Server. This adds on component to WAS allows Portal to take advantage of the SOA architecture. Portal can be installed and clustered without WebSphere Process Server, but then you would loose the SOA features.
WebSphere Process Server is installed and configured by default when using the Portal Typical install path. However, one very important limitation exists with WebSphere Process Server. WebSphere Process Server does NOT allow a WebSphere Process Server profile to be federated if a Portal server already exists on the node. This limitation basically makes a node that has been installed by the Portal installer using the Typical install path to be UNCLUSTERABLE. So to work around this we MUST install WebSphere Application Server and WebSphereProcess Server separately by using their native installers and then federate the empty profile and then install Portal onto the already existing, federated profile.
This will be mentioned all through the installation sections of this guide.

Install and upgrade WAS 6.0.2.9/WPS 6.0.1.1 Deployment Manager

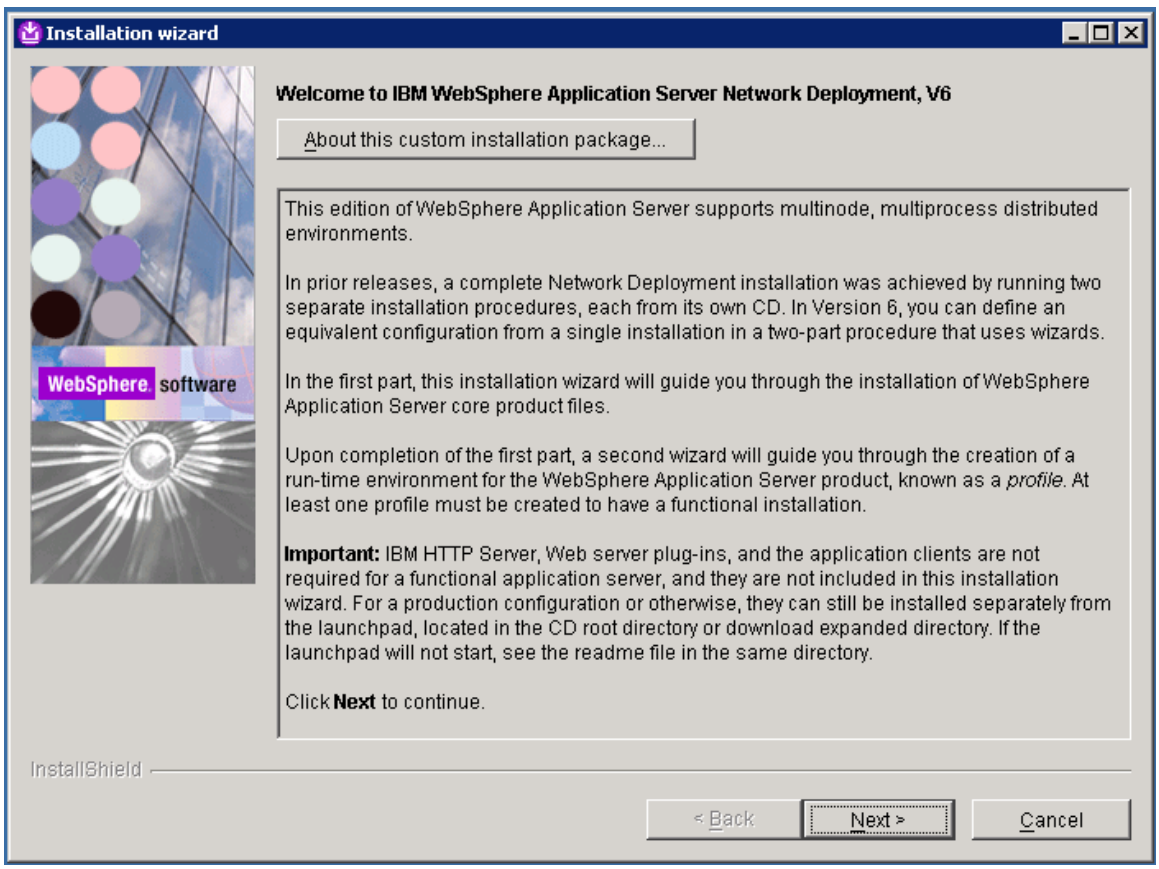
Important: This guide explicitly defines the required approach to build a WebSphere Portal cluster which has been installed on WebSphere Process Server (WPS).
To do this you must install Portal into an already federated WAS/WPS profile. Because of this requirement, we MUST install WAS/WPS from their native installers and federate the node BEFORE using the Portal installer to install Portal.

Install WAS v6.0.2.9

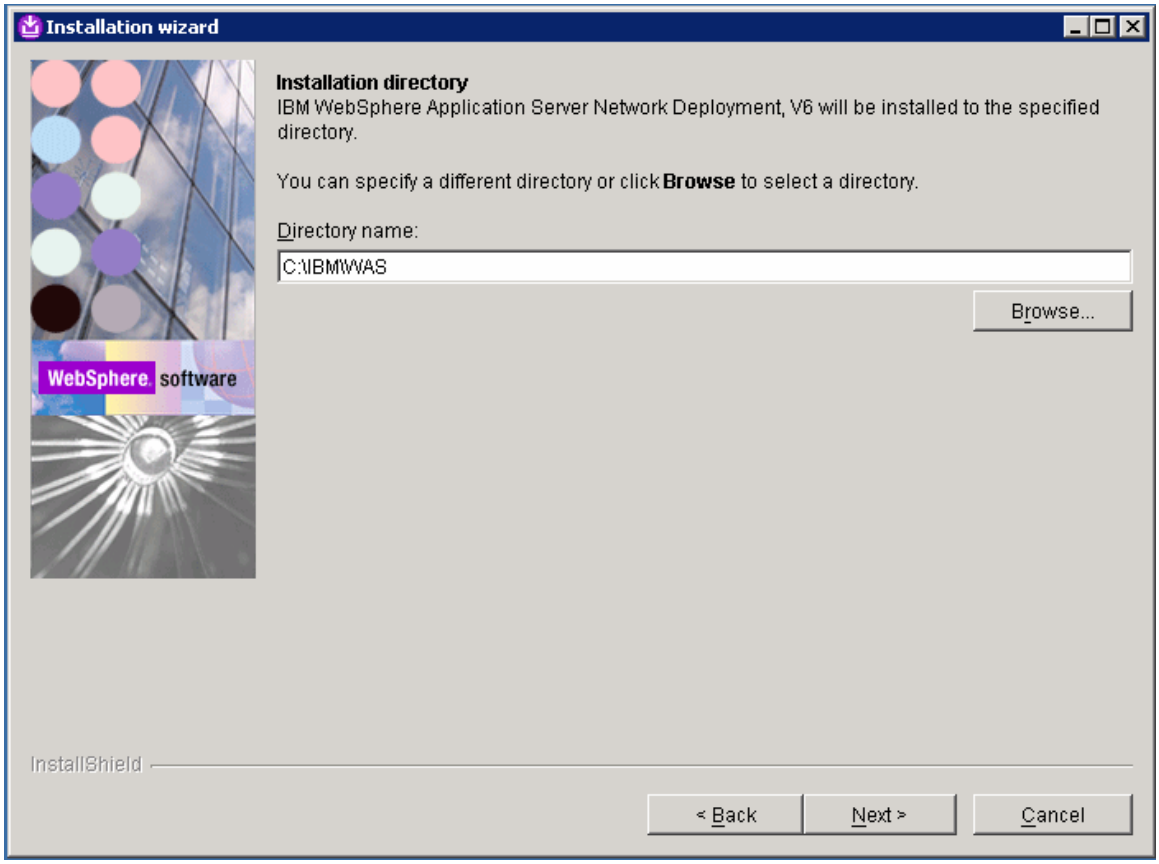
Install the DMGR by following the procedure below:

1. Install WSAS DMGR by running the installer from:
   <cd_root>/W-1/windows/ia32/ifpackage/WAS/install.exe

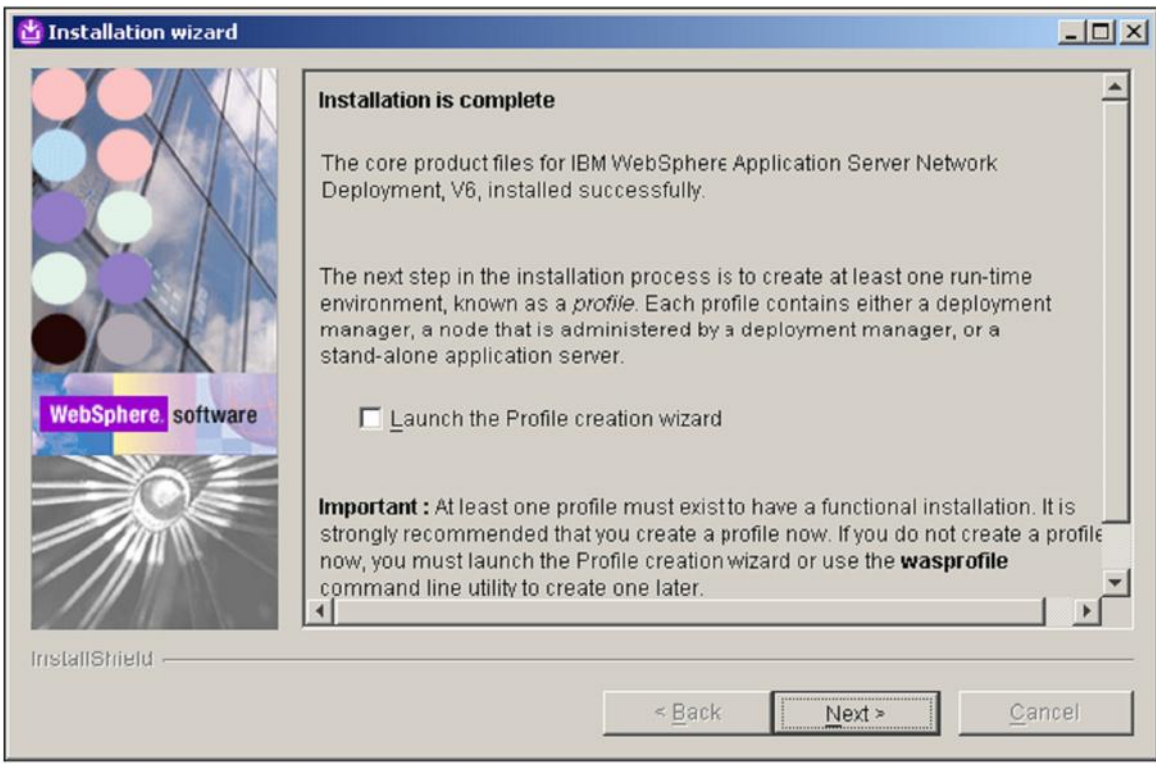
Note: Make sure the installer screen is titled "**Welcome to WebSphere Application Server Network Deployment, V6**". This title means that you can use this installer to install either, DMGR or WAS profiles. If the title is "WebSphere Application Server Version 6.0", you are using an installer that only has the ability to install WAS profiles and not DMGR profiles:



2. If installing on Windows, when asked for the install location, please shorten the default path. There is a path name limitation in Windows. Windows cannot handle path names longer than 256 characters.



3. You should be prompted during the install (with a panel near the end) if you would like to create a profile….at this time please choose NOT to create a profile by making sure the "Launch the Profile creation wizard" checkbox remains UNCHECKED. We will create a WPS profile at the end of the WPS install.

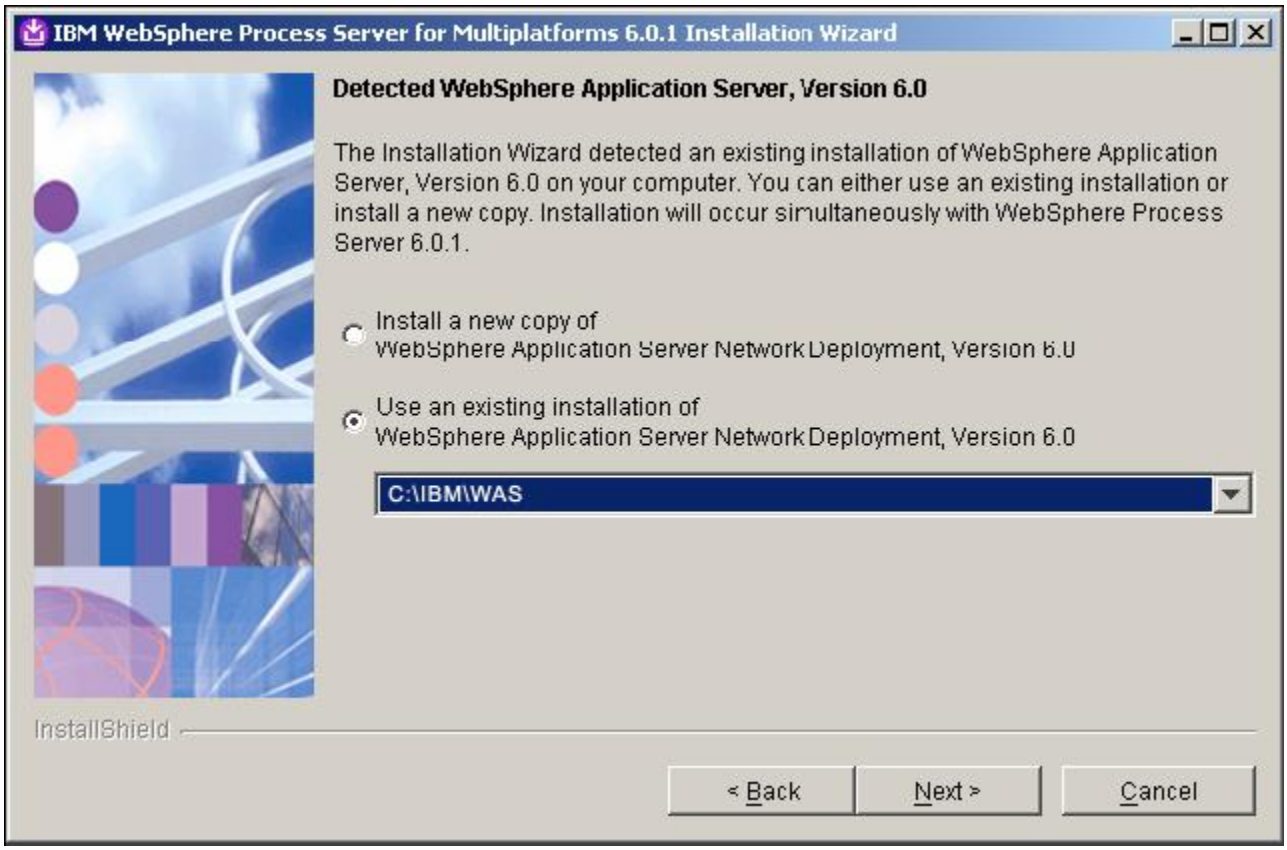


Install WPS v6.0.1.1

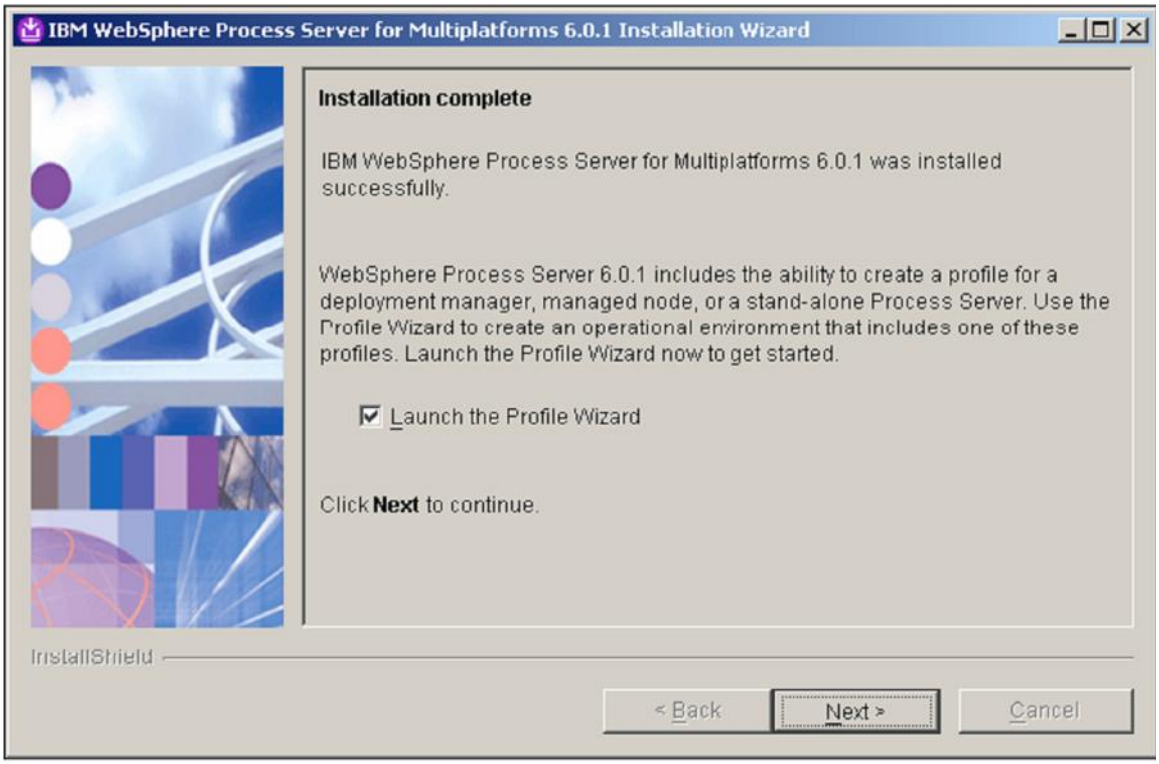
1. Install WPS 6.0.1.1 by running the installer from:
<cd_root>/W-2/windows/ia32/WBI/install.bat

Note: Please ensure you use the **install.bat** file and NOT the install.exe to install WPS.

2. Ensure you use the existing WAS you just installed.

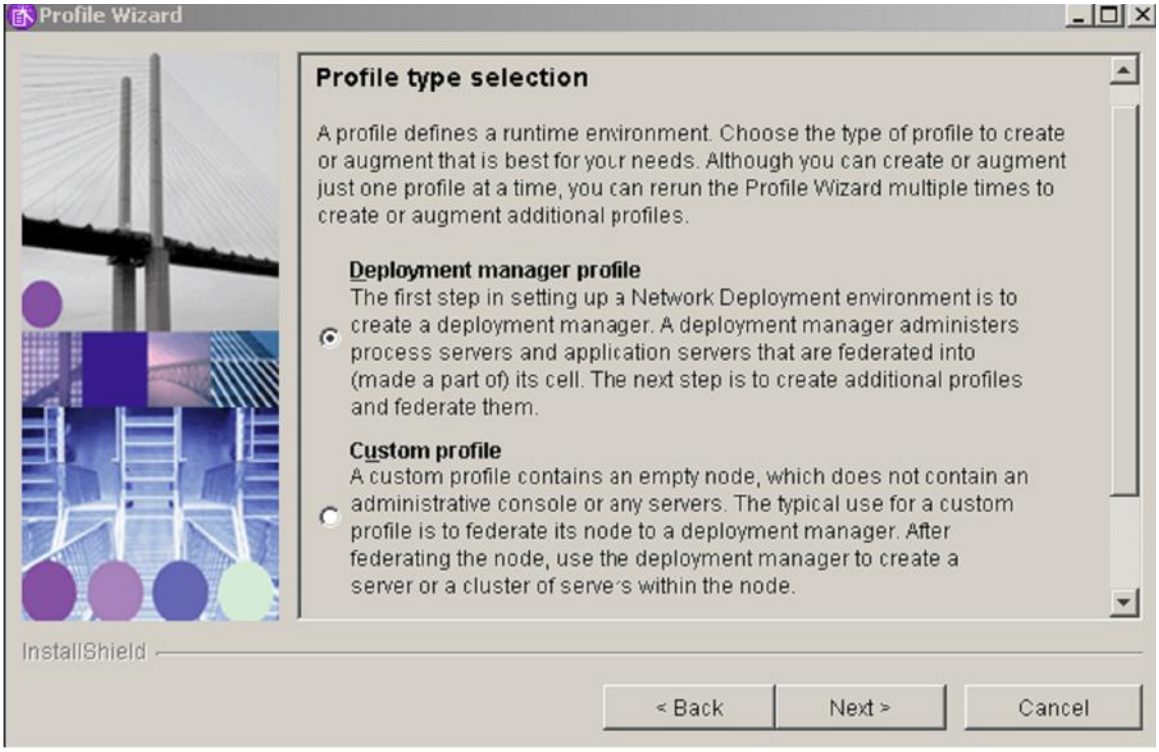


3. You should be prompted during the install (with panel near the end) if you would like to create a profile. At this time we will create a WPS DMGR profile. Please ensure the "Launch the Profile Wizard" checkbox is CHECKED and click Next to launch the WPS profile creation wizard.



Note: If you have to launch the WPS profile creation wizard manually, please ensure you launch the WPS profile creation wizard and NOT the WAS profile creation wizard. The WPS profile creation wizard script is located at:
<was_root>/bin/ProfileCreator_wbi/pcatWindows.exe

4. After the profile creation wizard is launched, ensure the “Deployment manager profile” radio button is selected on the “Profile type selection” panel and click “Next”:

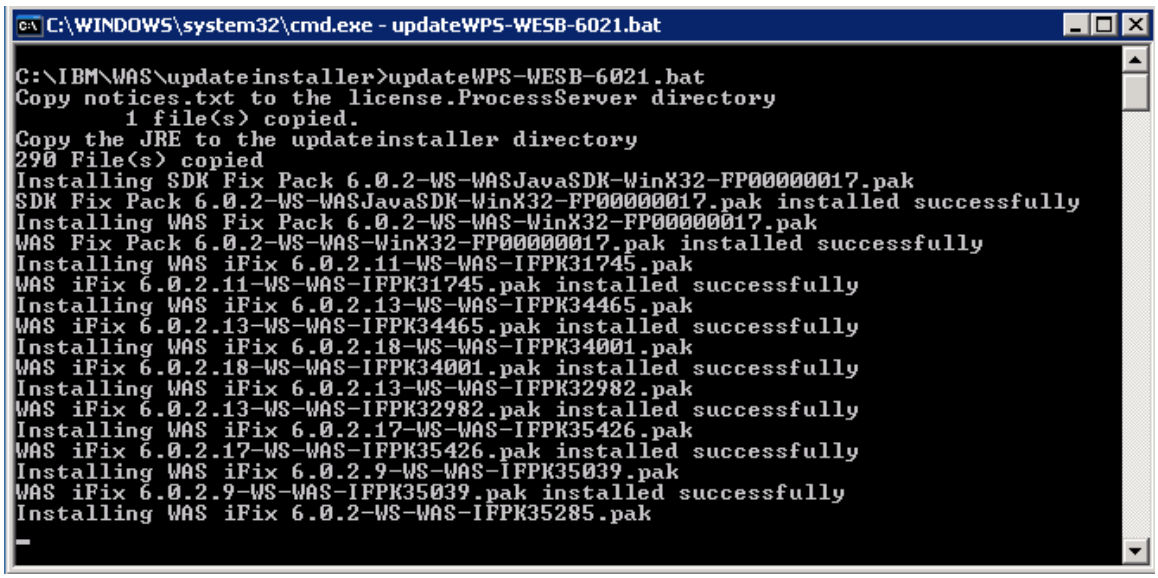


Upgrade WAS from version 6.0.2.9 to version 6.0.2.17 and WPS from 6.0.1.1 to version 6.0.2.1

1. After the DMGR profile is created, then upgrade WAS v 6.0.2.9 to version 6.0.2.17 and WPS v6.0.1.1 to version 6.0.2.1.WebSphere Process Server Version 6.0 Refresh Pack 2 for Windows platforms **6.0-WS-WPS-ESB-WinX32-RP0000002.zip**, upgrades WAS to v6.0.217 and WPS to v6.0.2.1. You can download it at:
http://www-1.ibm.com/support/docview.wss?rs=2307&uid=swg24014373

2. Create a directory updateinstaller under <was_root> and extract the package at <was_root>/updateinstaller.

3. Open the command prompt and change directory to <was_root>/updateinstaller, then run the batch file **updateWPS-WESB-6021.bat**.



Note: If during installation any errors occur, then correct those errors, uninstall the fixpack or fixes installed by the batch file and rerun the batch files again.

4. Verify the version of WAS and WPS by running the batch file v**ersionInfo.bat** in command prompt, it's located at *<was_root>\bin* directory.

5. Verify the operation of the DMGR by starting the server and rendering it through a browser, example:
http://dmgr:9060/admin

Note: The default port for the WAS AdminConsole has changed to 9060 in WAS 6.x.

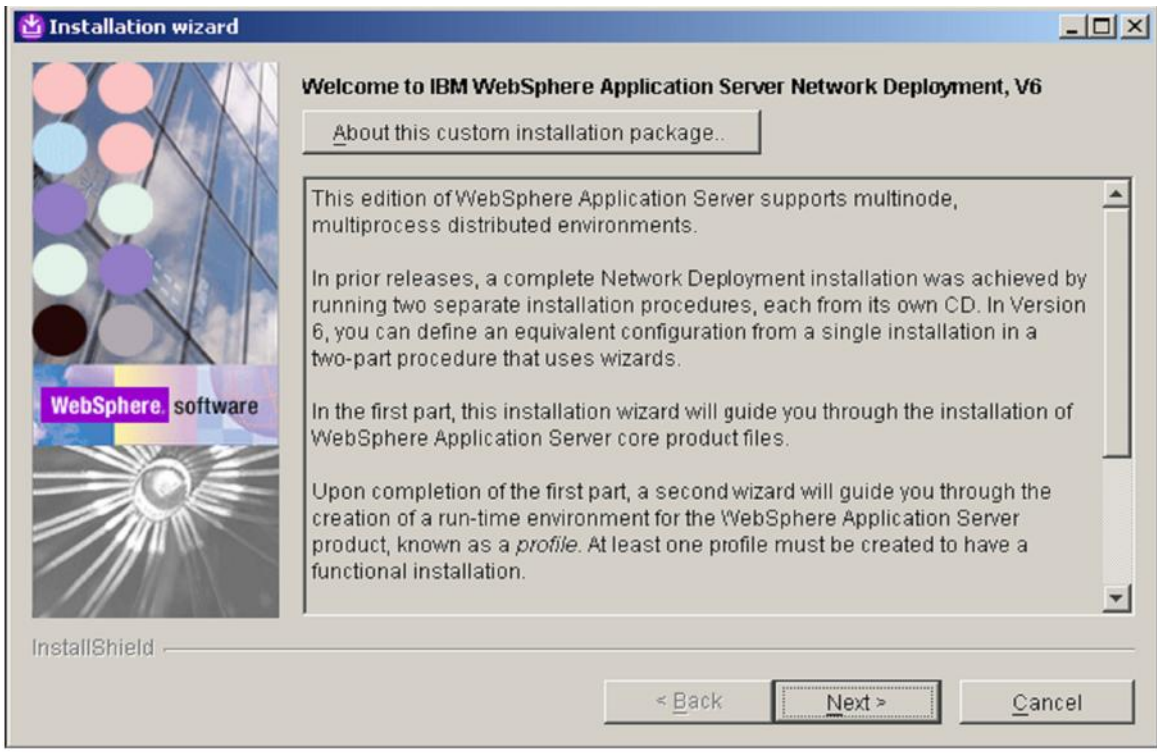
Install WAS 6.0.2.9/WPS 6.0.0.0 on future cluster node, PNode

Important: This guide explicitly defines the required approach to build a Portal cluster which has been installed on WebSphere Process Server. To do this you must install Portal into an already federated WAS/WPS profile. Because of this requirement, we MUST install WAS/WPS from their native installers and federate the node BEFORE using the Portal installer to install Portal.

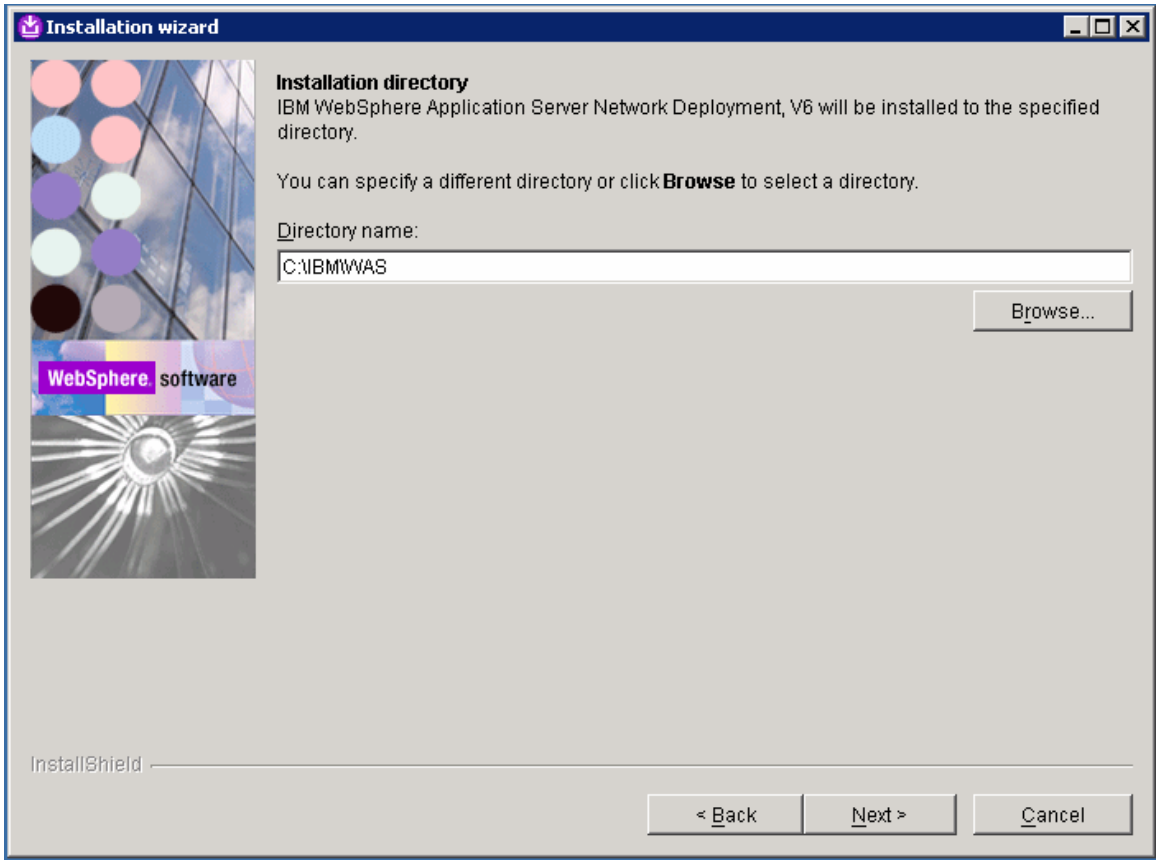
Install WAS v6.0.2.9

1. Install WAS on Node1 by running the installer from:
   <cd_root>/W-1/windows/ia32/ifpackage/WAS/install.exe

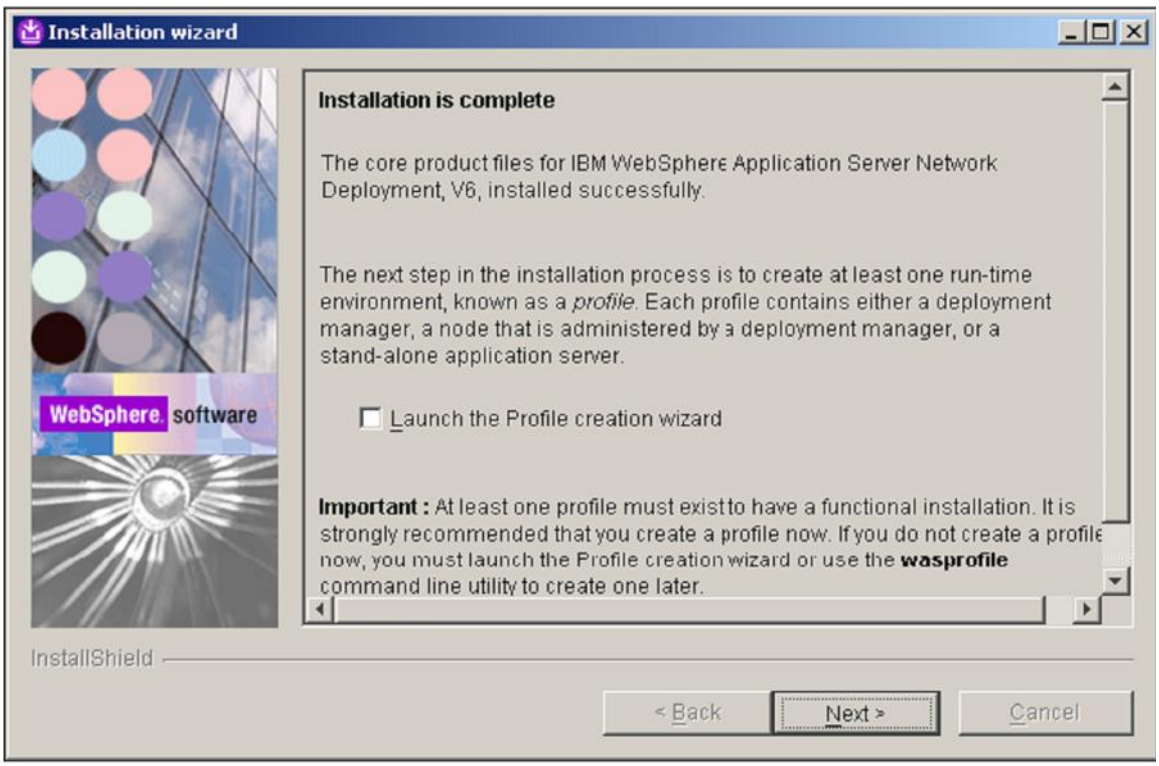
Note: Make sure the installer screen is titled "**Welcome to IBM WebSphere Application Server Network Deployment, V6**". This title means that you can use this installer to install either, DMGR or WSAS profiles. If the title is "WebSphere Application Server Version 6.0", you are using an installer that only has the ability to install WAS profiles and not DMGR profiles:



2. If installing on Windows, when asked for the install location, please shorten the default path. There is a path name limitation in Windows. Windows cannot handle path names longer than 256 characters.



3. You should be prompted during the install (with a panel near the end) if you would like to create a profile….at this time please choose NOT to create a profile by making sure the "Launch the Profile creation wizard" checkbox remains UNCHECKED. We will create a WPS profile at the end of the WPS install.

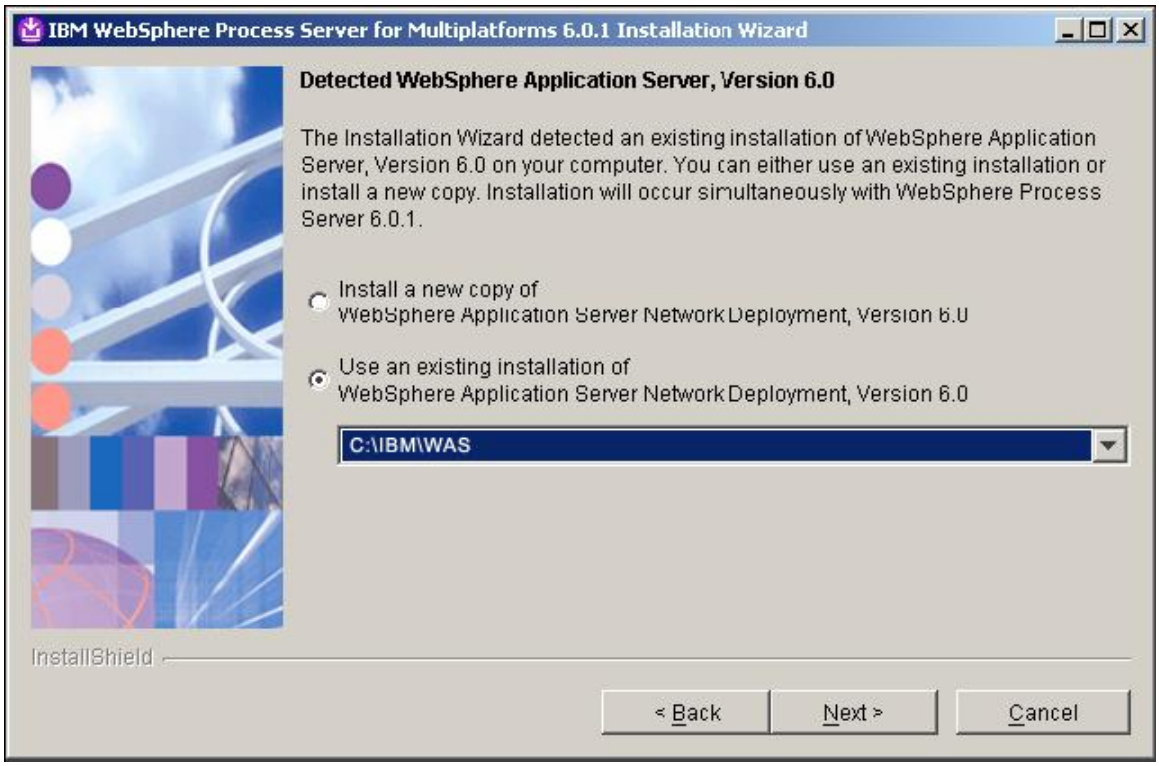


Install WPS v6.0.1.1

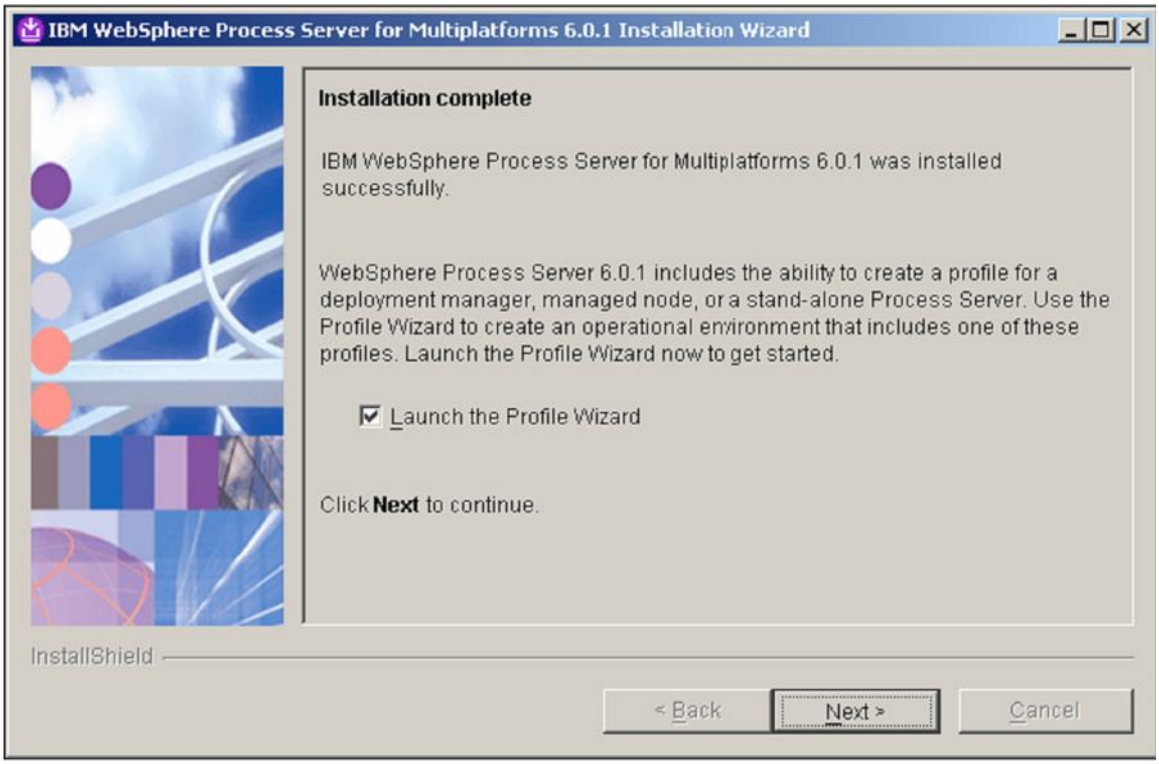
1. Install WPS 6.0.1.1 by running the installer from:
<cd_root>/W-2/windows/ia32/WBI/install.bat

Note: Please ensure you use the **install.bat** file and NOT the install.exe to install WPS.

2. Ensure you use the existing WAS you just installed:

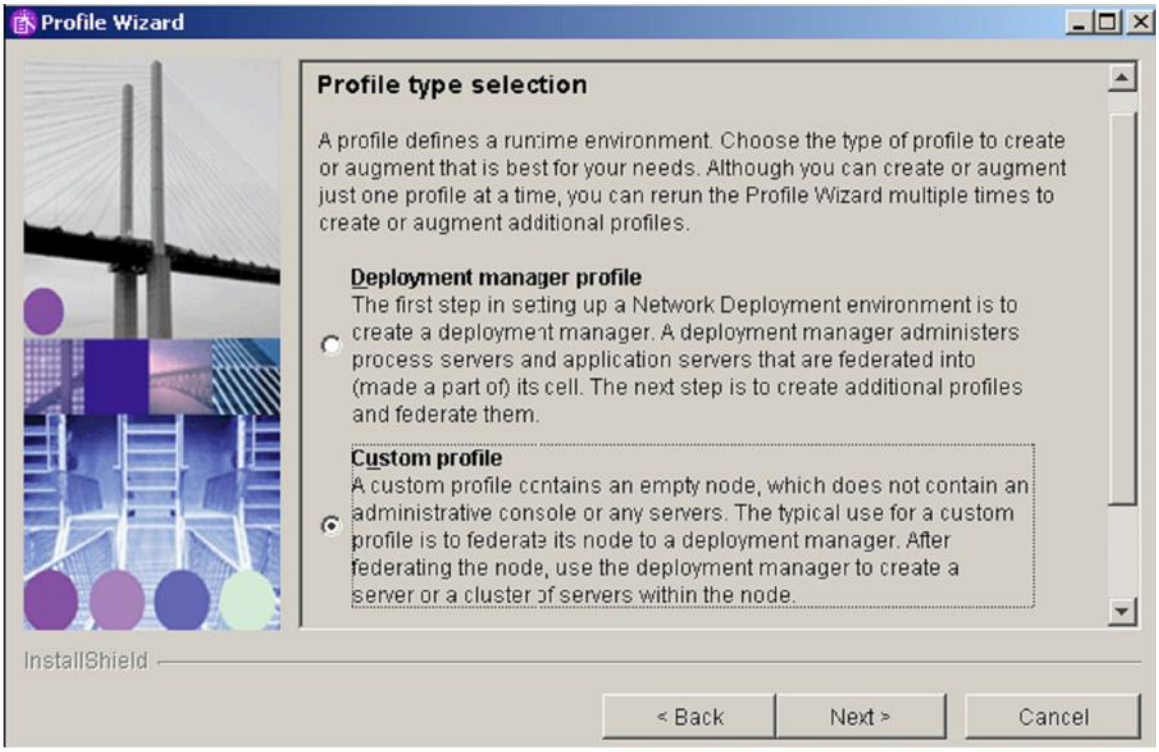


3. You should be prompted during the install (with a panel near the end) if you would like to create a profile. At this time we will create a WPS Custom profile. Please ensure the "Launch the Profile Wizard" checkbox is CHECKED and click Next to launch the WPS profile creation wizard.

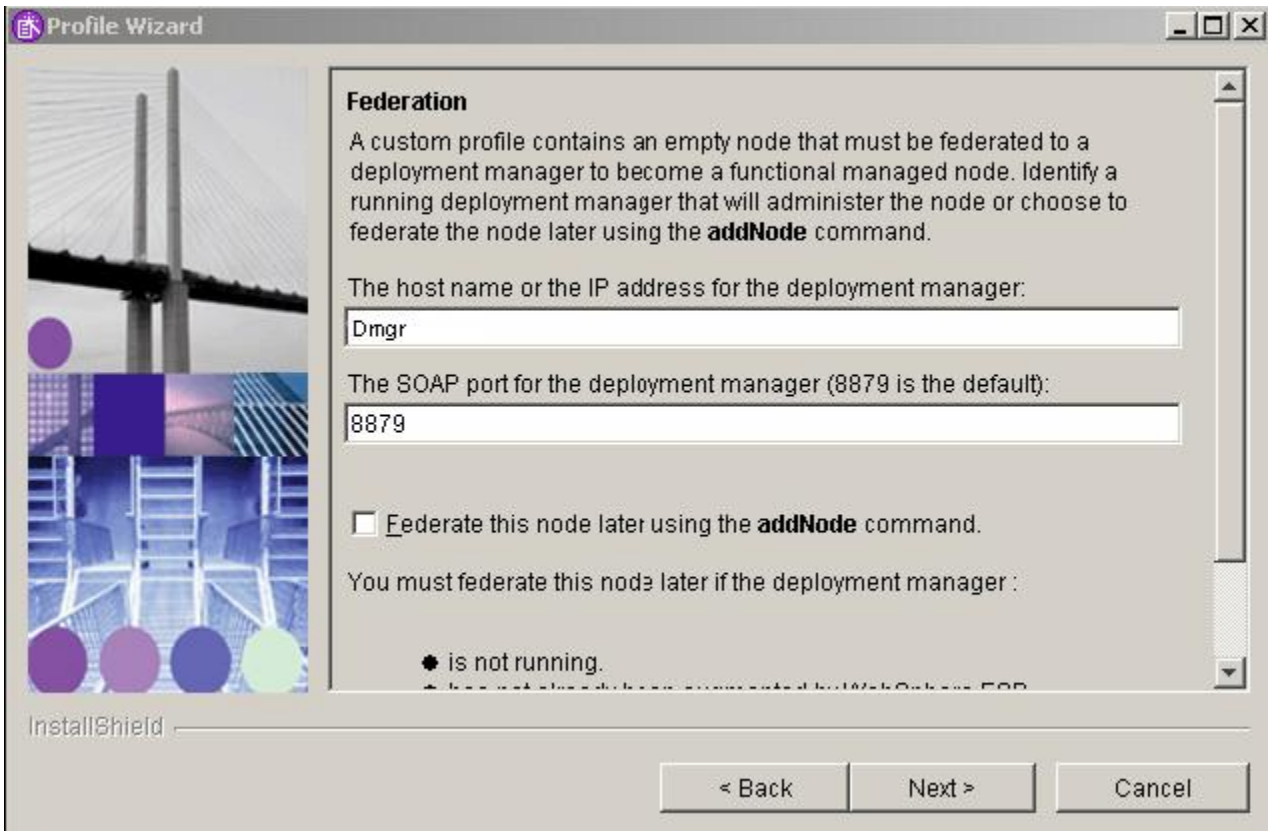


Note: If you have to launch the WPS profile creation wizard manually, please ensure you launch the WPS profile creation wizard and NOT the WSAS profile creation wizard. The WPS profile creation wizard script is located at:
<was_root>/bin/**ProfileCreator_wbi**/pcatWindows.exe

4. After the profile creation wizard is launched, ensure the “Custom profile” radio button is selected on the “Profile type selection” panel and click “Next”:



5. Next you will decide if you would like to have the profile creation wizard to automatically federate the Custom profile after creation. Please allow the profile creation wizard to federate the Custom profile. To do this, please ensure the “Federate this node later using the addNode command” checkbox remains UNCHECKED.
Also, please ensure that the clocks are synchronized to within 5 minutes of each other on Node1 machine and the DMGR machine. If the clocks are not within 5 minutes, the addNode process will fail.



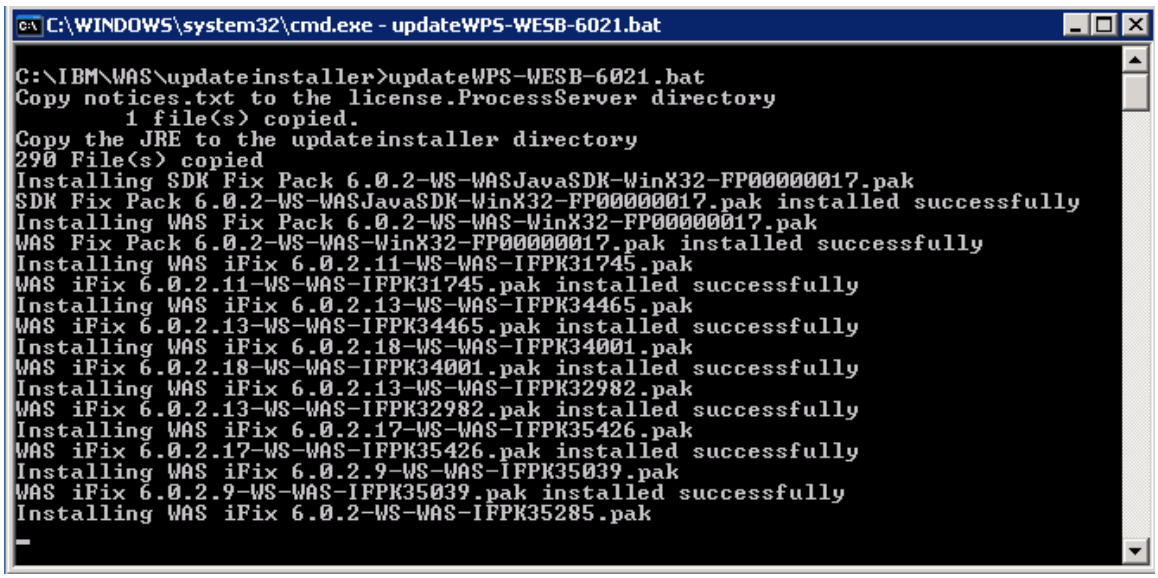
Upgrade WAS v6.0.2.9 to v6.0.2.17 and WPS v6.0.1.1 to v6.0.2.1

Upgrade WAS from version 6.0.2.9 to version 6.0.2.17 and WPS from 6.0.1.1 to version 6.0.2.1

1. After the DMGR profile is created, then upgrade WAS v 6.0.2.9 to version 6.0.2.17 and WPS v6.0.1.1 to version 6.0.2.1.WebSphere Process Server Version 6.0 Refresh Pack 2 for Windows platforms **6.0-WS-WPS-ESB-WinX32-RP0000002.zip**, upgrades WAS to v6.0.217 and WPS to v6.0.2.1. You can download it at:
http://www-1.ibm.com/support/docview.wss?rs=2307&uid=swg24014373

2. Create a directory updateinstaller under <was_root> and extract the package at <was_root>/updateinstaller.

3. Open the command prompt and change directory to <was_root>/updateinstaller, then run the batch file **updateWPS-WESB-6021.bat**.



Note: If during installation any errors occur, then correct those errors, uninstall the fixpack or fixes installed by the batch file and rerun the batch files again.

4. Verify the version of WAS and WPS by running the batch file v**ersionInfo.bat** in command prompt, it's located at *<was_root>\bin* directory.

5. Verify the operation of the DMGR by starting the server and rendering it through a browser, example:
http://dmgr:9060/admin

Note: The default port for the WAS AdminConsole has changed to 9060 in WAS 6.x.

Prepare the DMGR and Node1 for the Portal install

1. Update the Deployment Manager machine with required WMM JAR files. These files are located on the Setup CD provided as part of the installation package for WebSphere Portal.
Copy the following files from the <cd_root>/W-Setup/dmgr_wmmjars directory on the Setup
CD to the /<was_server_root>/lib directory on the deployment manager machine:
* wmm.jar
* wmm.ejb.jar
* wp.wire.jar

Important: If this will be the first Portal node you will install into the cell, proceed to the next step and continue with the primary node installation. If you have already federated other managed nodes into the cell, you must also copy these JAR files to the /<wsas_root>/lib directory on each of those managed nodes, regardless of whether you intend to install WebSphere Portal on the nodes.

2. Change the time-out request for the Simple Object Access Protocol (SOAP) client for the DMGR and the Node 1. The default, in seconds, is 180.
On the DMGR machine locate the <dmgr_profile_root>/properties/ directory and edit the soap.client.props file. Change the line to
com.ibm.SOAP.requestTimeout=6000
On the WSAS Node1 machine locate the <wsas_profile_root>/properties/ directory and edit the soap.client.props file. Change the line to
com.ibm.SOAP.requestTimeout=6000

3. Ensure the nodeagent is running on Node1 so the following changes are synchronized to the node. Login to the DMGR AdminConsole and change the timeout values for the deployment manager by navigating to:
System Administration>Deployment Manager>Web container transport chains

4. Increase the timeout values for each entry listed in the Web container transport chains section by clicking on each entry. After clicking on an entry, complete the following steps to increase the timeout values:

a) Click HTTP Inbound Channel.
b) Change the Read timeout value to 180.
c) Change the Write timeout value to 180.
d) Save your configuration changes and synchronize with the node

5. Change the timeout request period for the Java Management Extensions (JMX) connector.

a) Log in to the administrative console for the deployment manager
b) Click System administration > Deployment Manager > Administration Services > JMX connectors > SOAPConnector > Custom Properties.
c) Select the requestTimeout property, and increase the value from 600 to 6000.

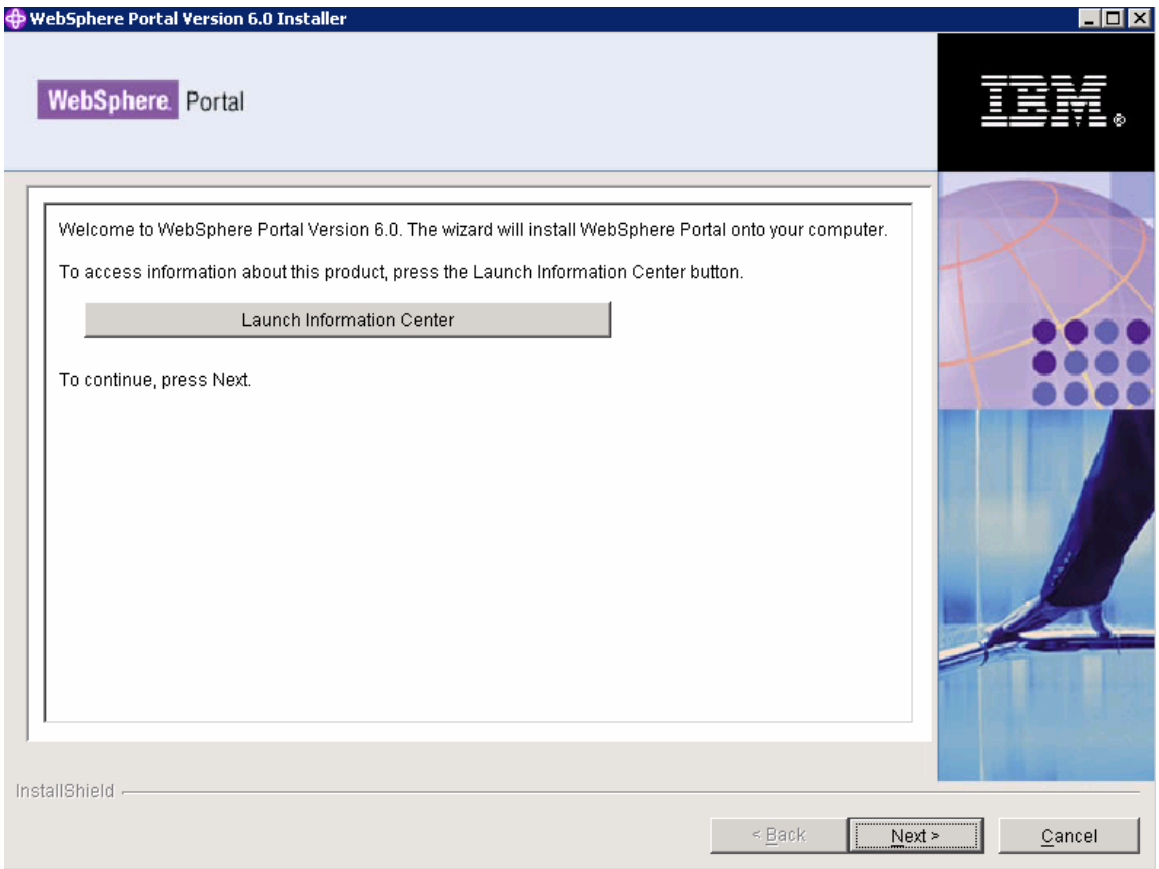
d) Save your configuration changes and synchronize with the node

6. Disable automatic synchronization between this node and the deployment manager.
a) Log in to the administrative console for the deployment manager.
b) Click System Administration > Node Agents >nodeagent name for desired node> File synchronization service.
c) Ensure that the Automatic Synchronization check box is NOT checked.
d) Save your changes and synchronize with the node.

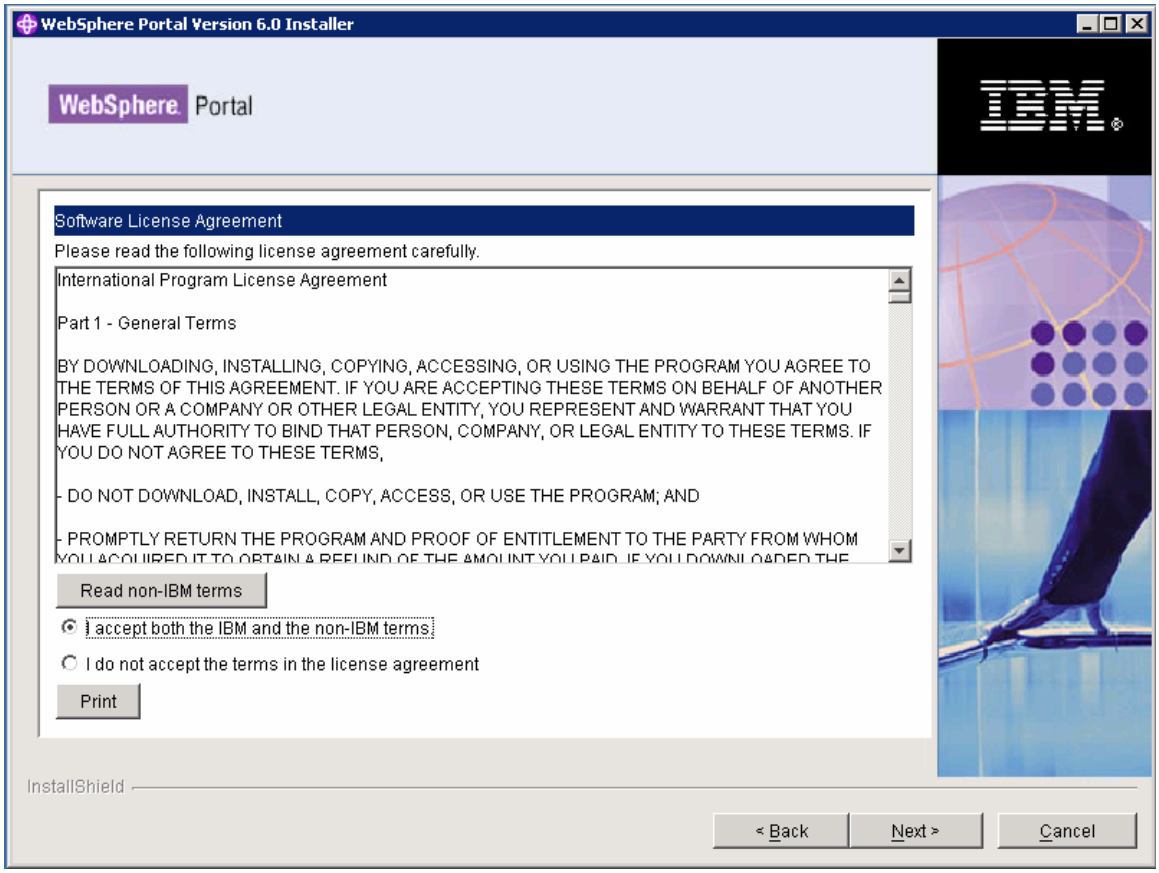
7. Restart the DMGR and the nodeagent

Install Portal onto the managed node, Node1

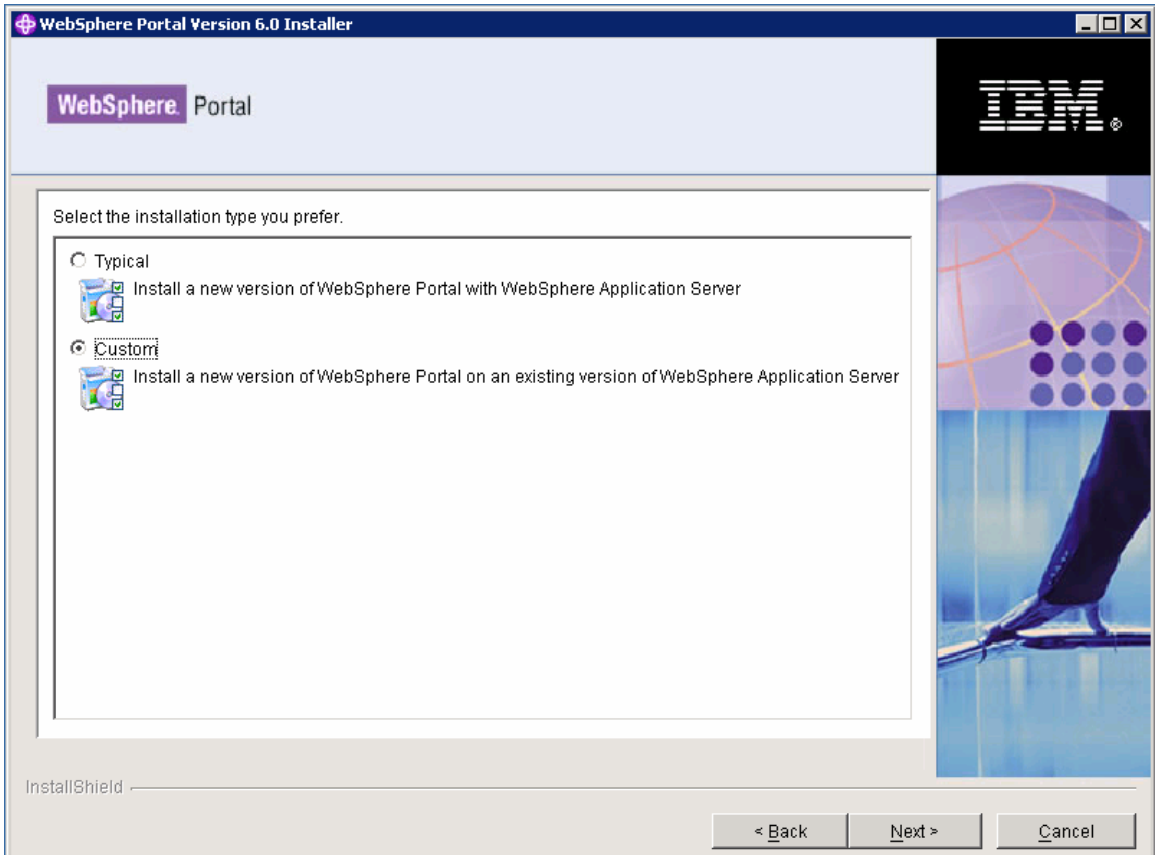
1. Start the Portal installer from <cd_root>/W-Setup/install.bat



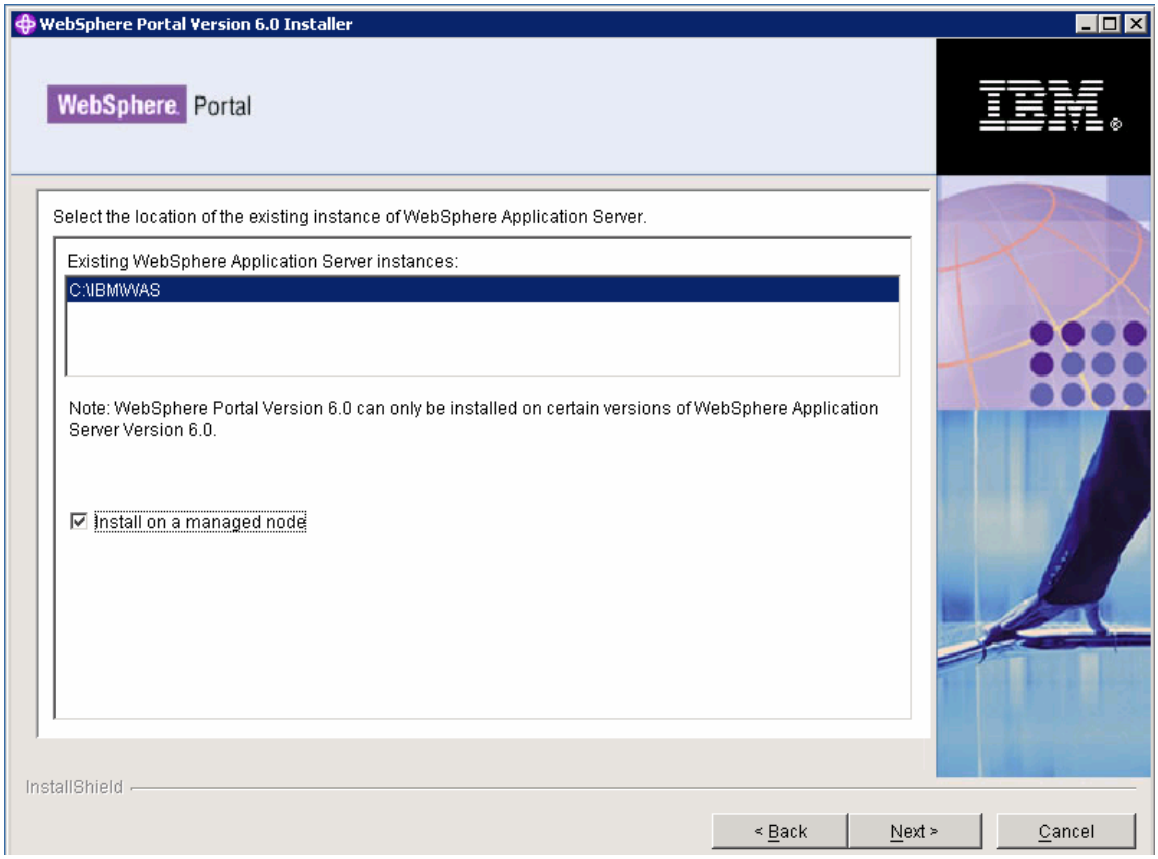
2. Accept the license agreement



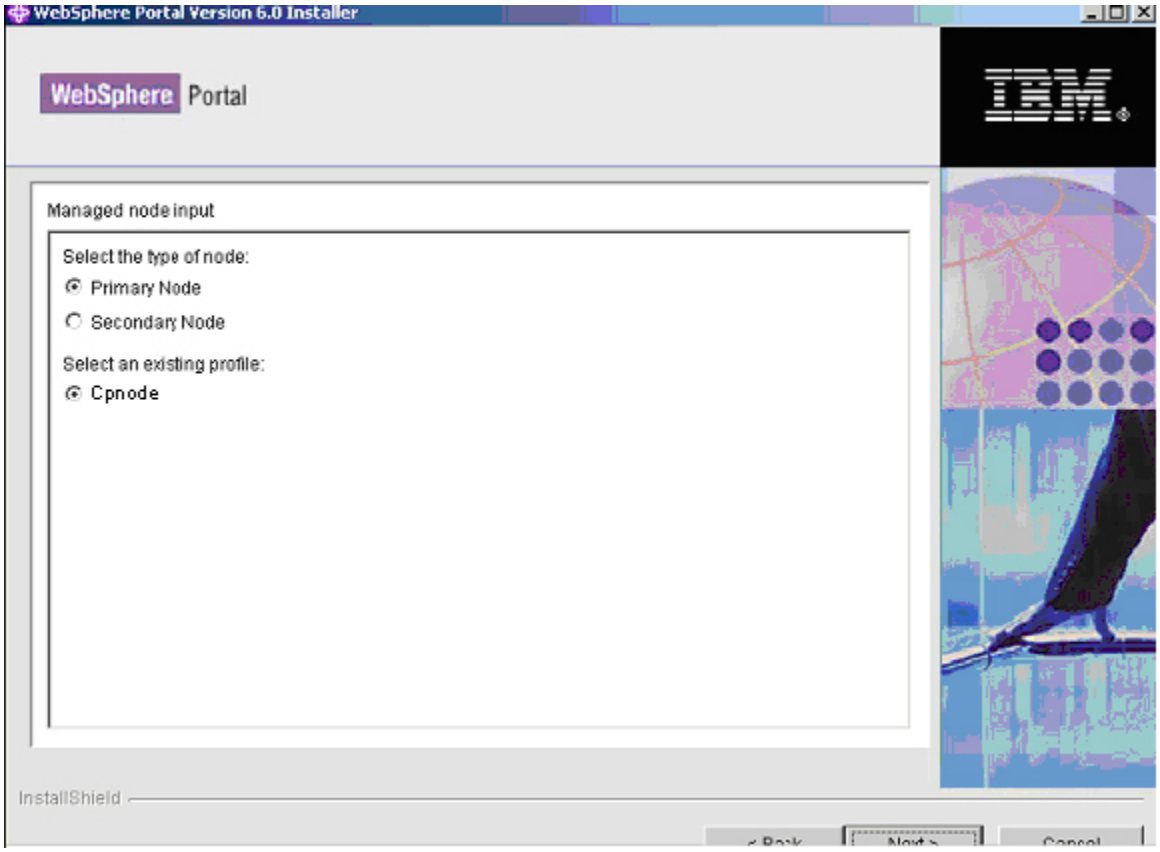
3. Select Custom installation type:



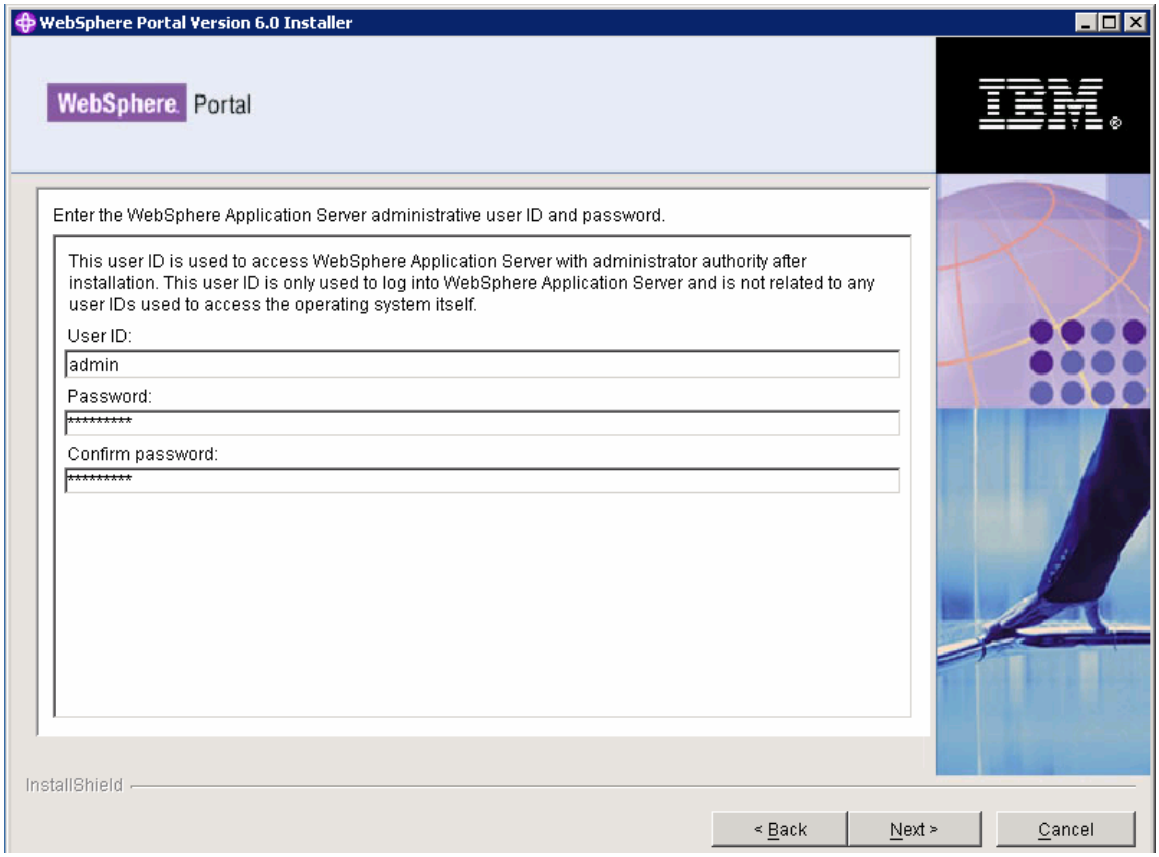
4. Select the existing WebSphere Application Server install location and check “Install on a managed node” checkbox next



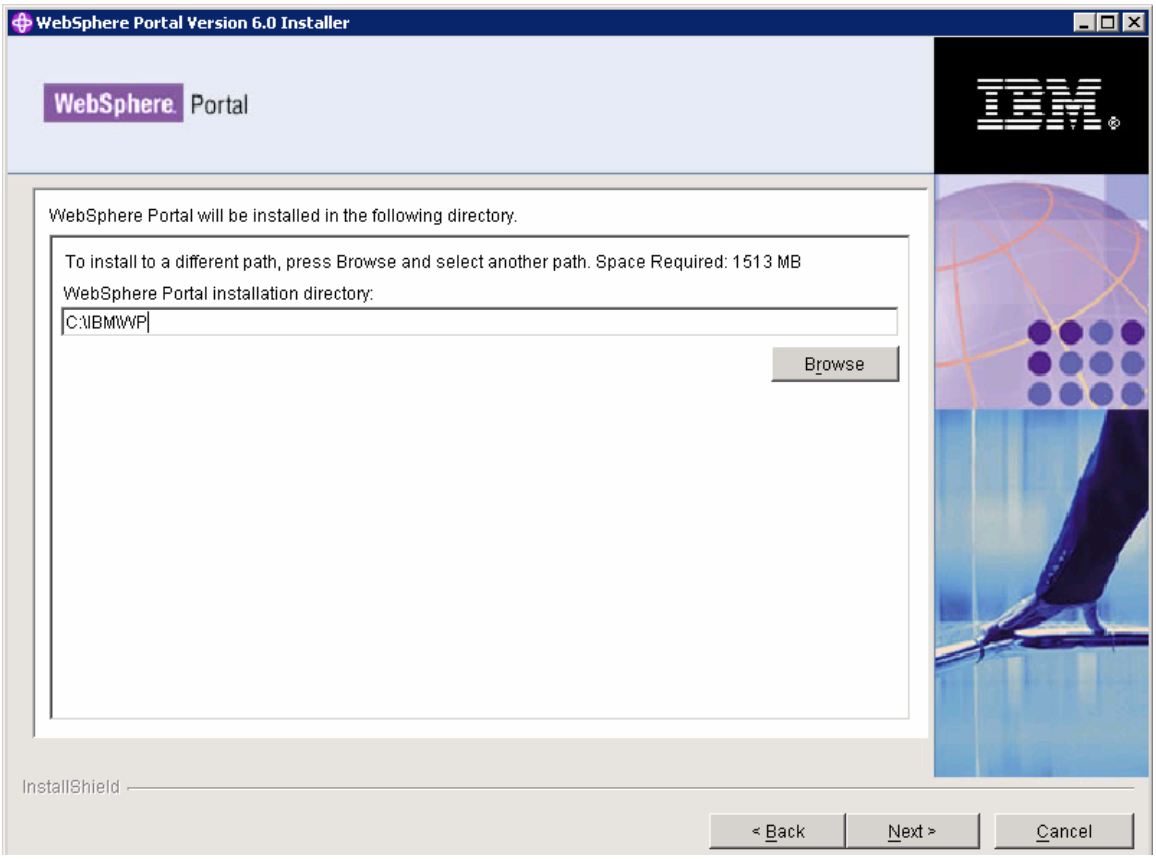
5. Select Primary Node as type of node and select the desired profile that you wish to install Portal onto



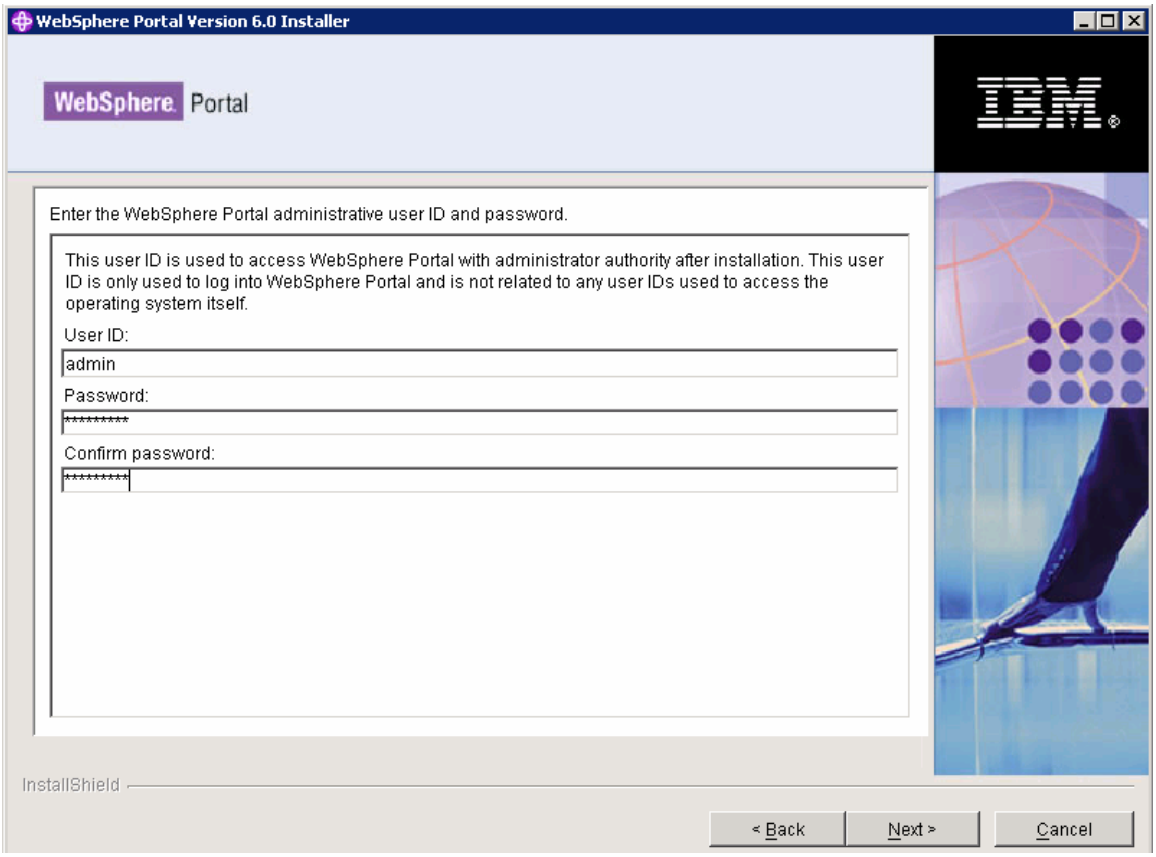
6. Define a WAS administrator User ID and Password. This is a new panel in the Portal installer because with Portal v6 the install will enable security by default to the WMM database.



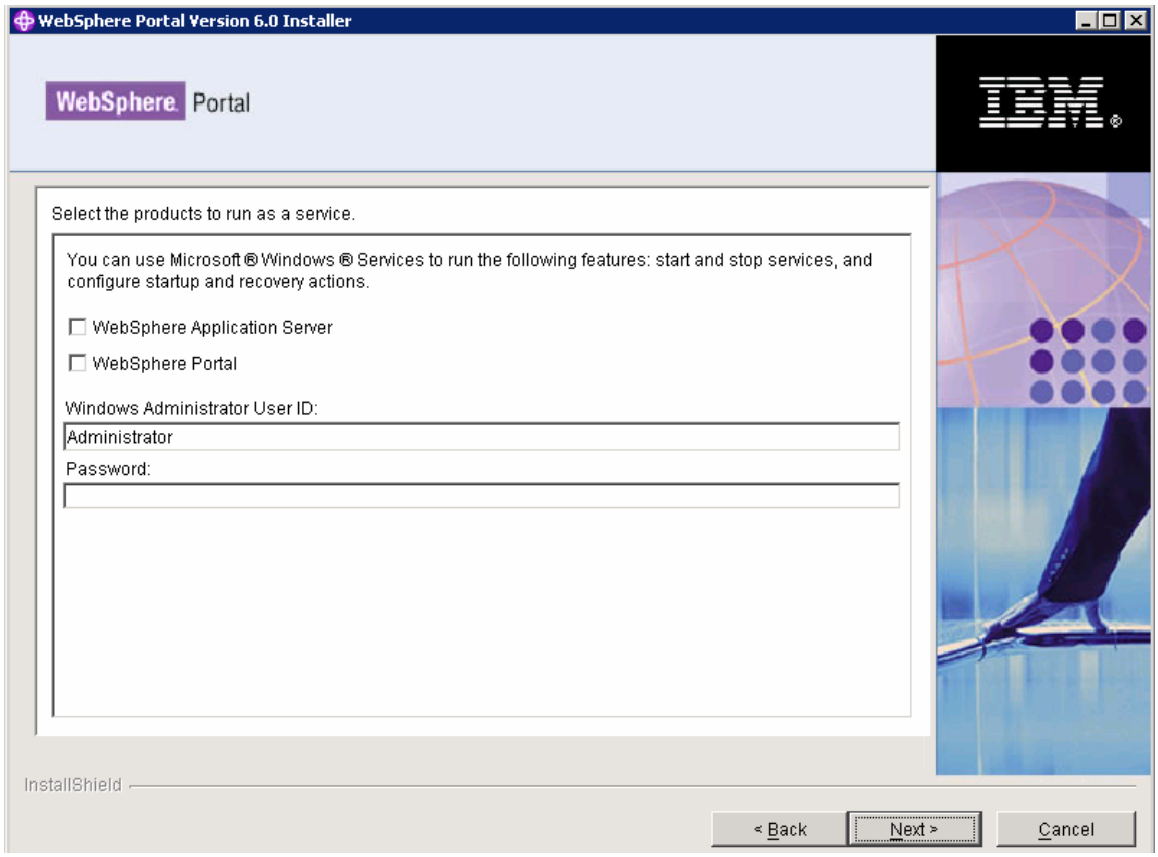
7. Define the desired location for Portal to be installed



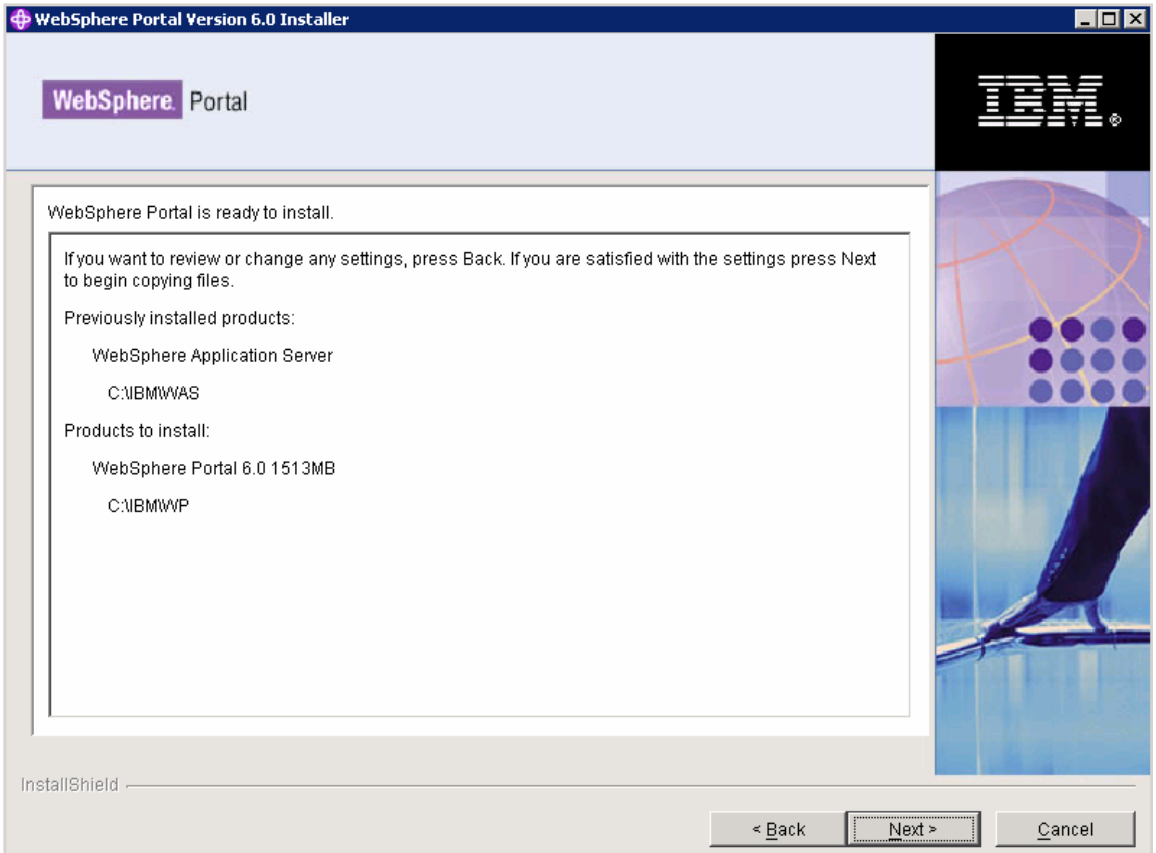
8. Define the Portal administrator User ID and password



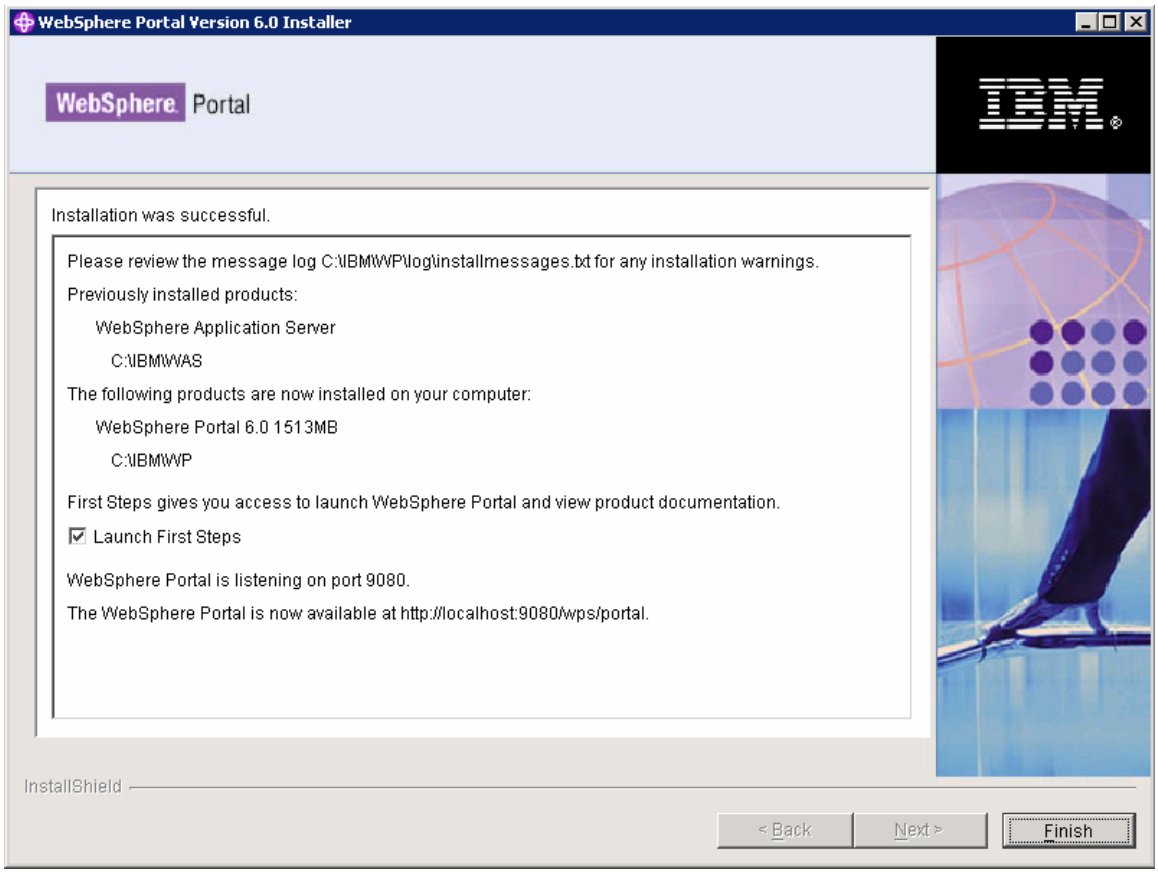
9. Decide whether you want WAS and Portal to run as a service. In this guide we choose NOT to run either as a Windows service.



10. Review Summary panel and click Next to begin the install



11. Verify that portal install successfully and click Finish.



Re-enable auto-sync

1. Log in to the administrative console for the Deployment Manager.

2. Click System Administration > Node Agents > *node_name* > File Synchronization Service.

3. Select the Automatic Synchronization check box.

4. Save your changes and synchronize with the node.

5. Restart the node agent.

6. Verify the Portal install by accessing it thru a browser. By default Portal is installed onto port 9080:
http//<hostname>:9080/wps/portal

Upgrade WP v6.0.0.0 to WP v6.0.1

1. Download the WebSphere Portal v6 refresh pack 1 **6.0.1-WP-Multi-RP001.zip** and portal update installer **PortalUpdateInstaller.zip** at: http://www-1.ibm.com/support/docview.wss?rs=688&context=SSHRKX&dc%C3%9400&uid=swg24015257&loc=en_US&cs=UTF-8&lang=en&rss=ct688websphere

2. Create a directory updateinstaller at <wps_root> and extract the **PortalUpdateInstaller.zip** at <wps_root>/updateinstaller.

3. Extract 6.0.1-WP-Multi-RP001.zip at /portal_server_root/updateinstaller/fixpack/.

4. Open the command prompt and change the directory to /app_server_root/bin/, run the setupCmdLine.bat file to setup the environment.

5. Change the directory to /portal_server_root/updateinstaller/ and run the following command to install the fixpack:

   Updateportal.bat –installDir \portal_server_root –fixpack –install –fixpackDir portal_server_root\updateinstaller\fixpacks\ -fixpackID WP_PTF_601

Migrate portal node1 database to DB2v 8.2.14 database

IBM WebSphere Portal stores configuration, access control, such as user identities, credentials, and permissions for accessing portal resources, and user data in a database. By default, WebSphere Portal installs and uses a Cloudscape database.
The Cloudscape database that is not intended for use in a production environment or for authoring Web content. It should only be used for testing or proof of concept purposes. Cloudscape does not support vertical cloning, clustered environments, or enabling security in a database-only mode. That's why we will configure the portal to use DB2 database, as it's better able to handle large amounts of data and can be tuned for performance.

For improved performance DB2 database software must be installed on a separate machine. In a remote database environment, there are two connection types. Either WebSphere Portal connects to the DB2 server system using a local DB2 Connect installation (JDBC type 2 connection) or connects directly to the DB2 server (JDBC type 4 connection).

In this documents will be using JDBC type 2 connection. For that WebSphere Portal and a DB2 Connect are installed on the same machine and DB2 server is installed on a separate machine (the remote machine).

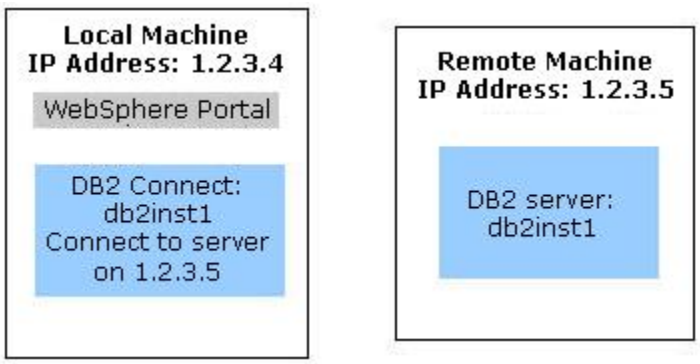


Figure 2. Remote Database Environment (JDBC type 2 connection)

1. Log in with a user ID that has administrative authority.

2. Click Start > Programs > Administrative Tools > Computer Management > Local Users and Groups and set following policies:
   Be defined locally
   Belong to the local Administrator group

3. Click Start > Programs > Administrative Tools > Local Security Policy. Next, click Local Policies > User Rights Assignment and set following policies:

Act as part of the operating system
Have permissions to create a token object
Have permissions to adjust memory quotas for a process
Have permissions to replace a process level token

4. Install a supported version of DB2 server by following the instructions that are provided with the DB2 documentation.

5. Install the client software, DB2 Connect, on the same machine as WebSphere Portal and WebSphere Application Server. Installing DB2 Connect enables the WebSphere Portal to use the required JDBC drivers. You must also ensure that the DB2 Connect installation is the same name as the server profile name. Refer to the DB2information center for more information:
http://www.ibm.com/software/data/pubs/

6. The following pre-requested fix packs must be installed on DB2 client and server machines before database transfer.

a. For DB2 v8.1 Fix Pack 14 must be downloaded and installed.
b. For DB2 v9.1 Fix Pack 1 must be downloaded and installed.
c. Fix Pack can be downloaded from the link:
http://www-1.ibm.com/support/docview.wss?rs=71&uid=swg27007053

7. Locate the following file:
db2home/sqllib/db2cli.ini

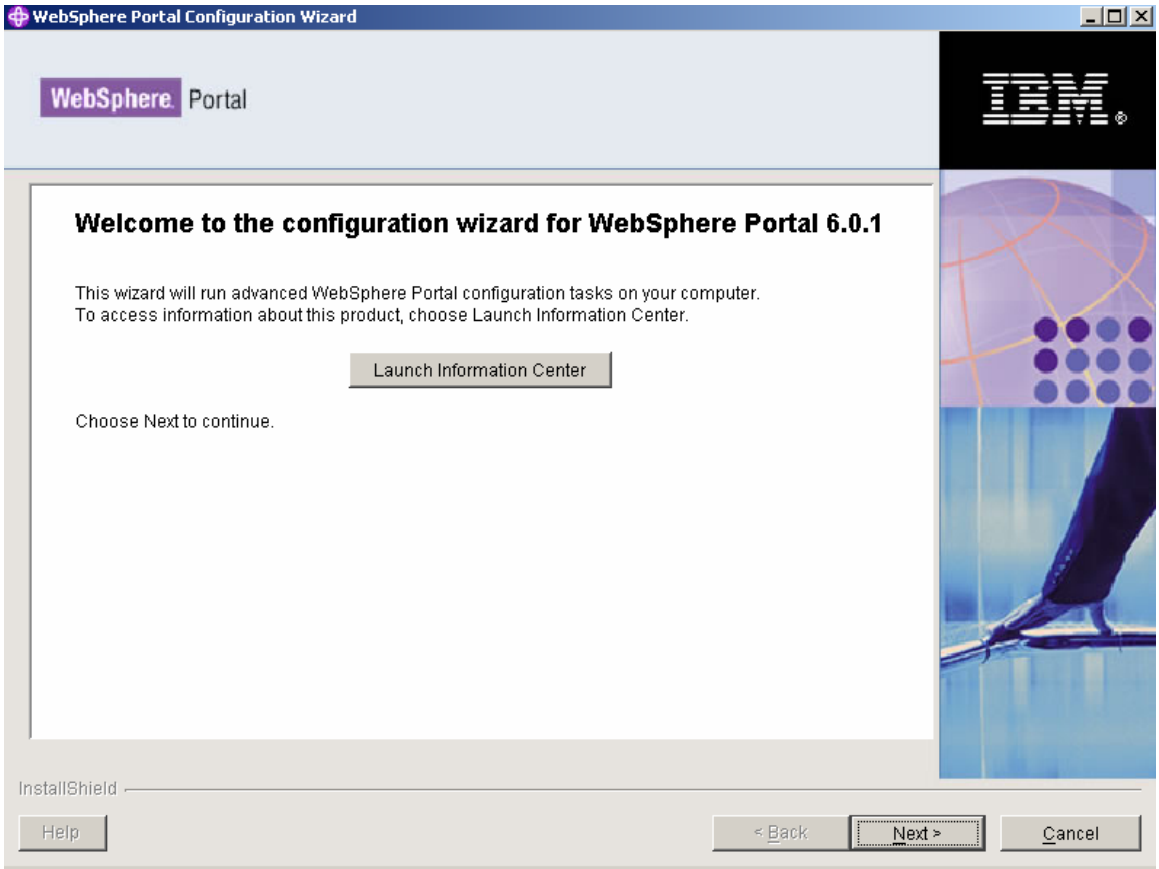
8. Edit the file by adding the following to the end of the file:

[COMMON]
DYNAMIC=1
ReturnAliases=0

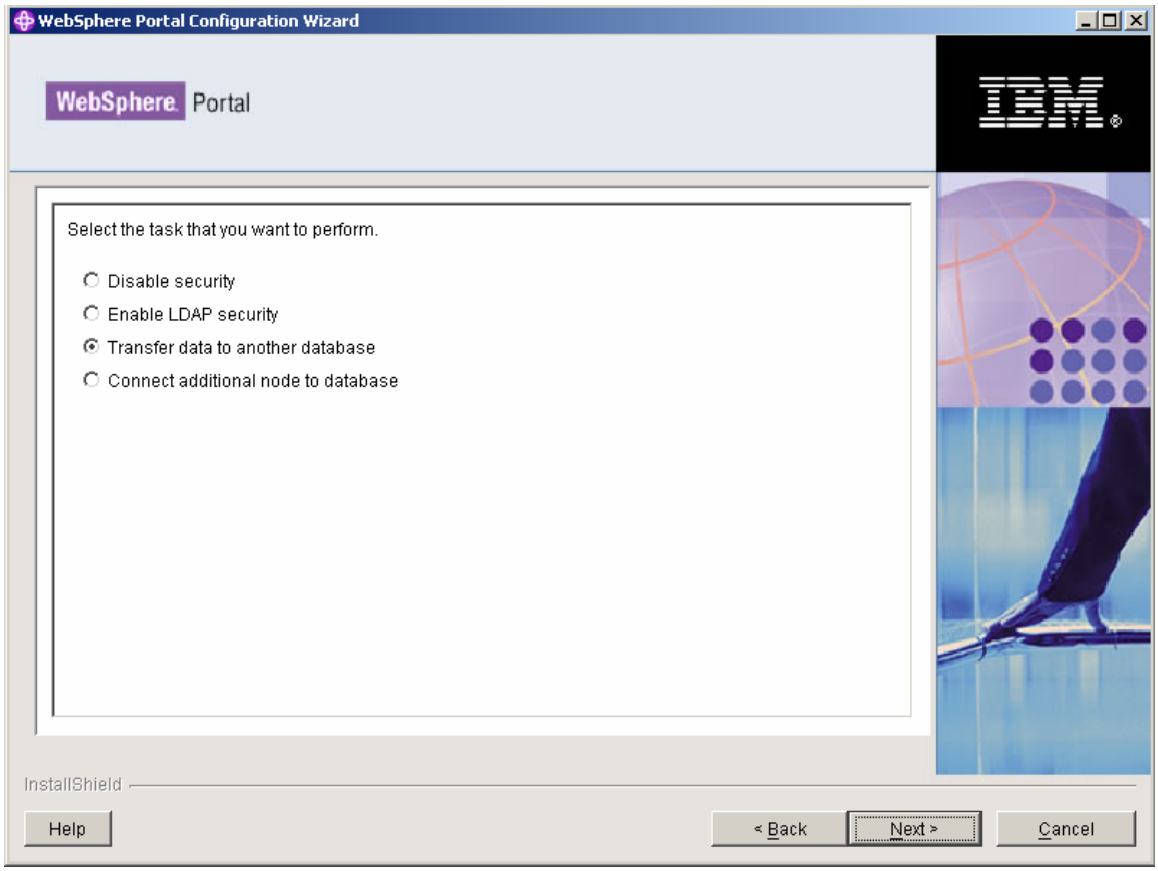
Note: An empty line is required after the ReturnAliases=0 at the end of the file.

9. Start the ConfigWizard from <wp_root>/config/wizard/configwizard.bat.

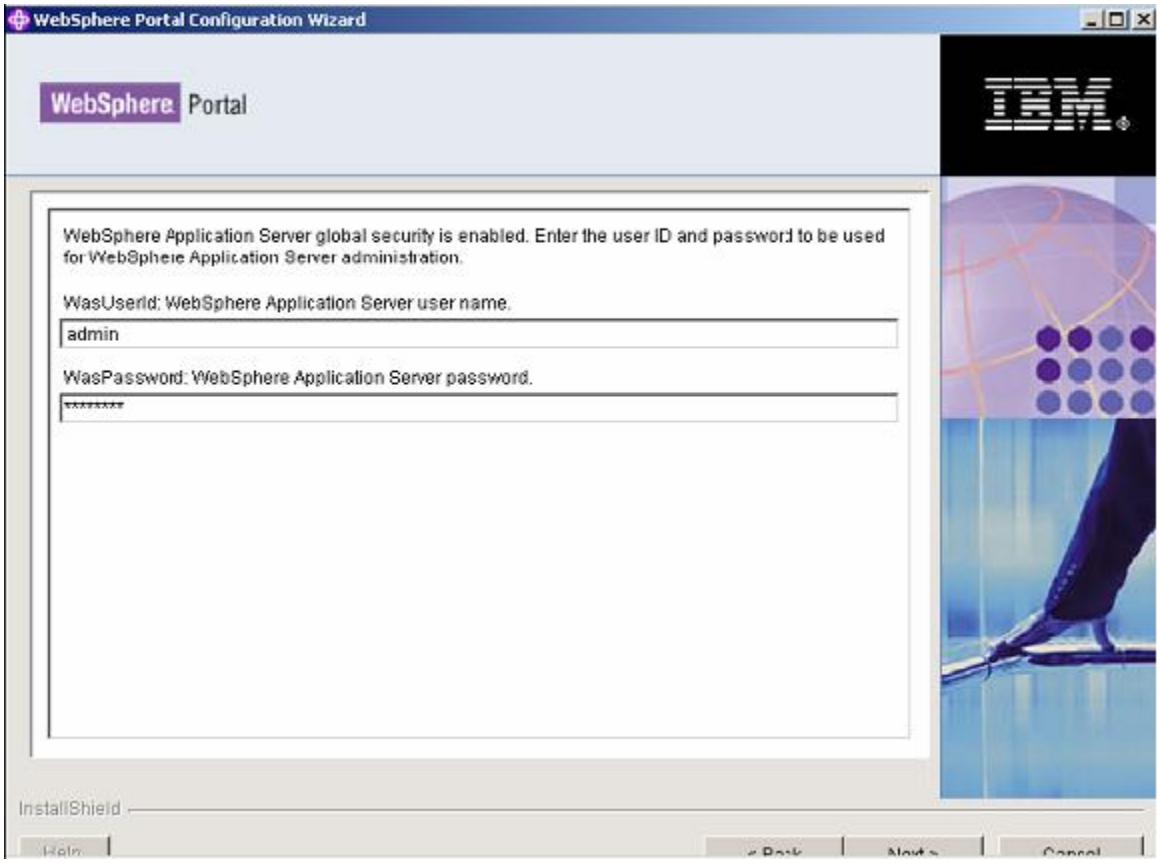
10. Click **Next** on the Welcome Screen.



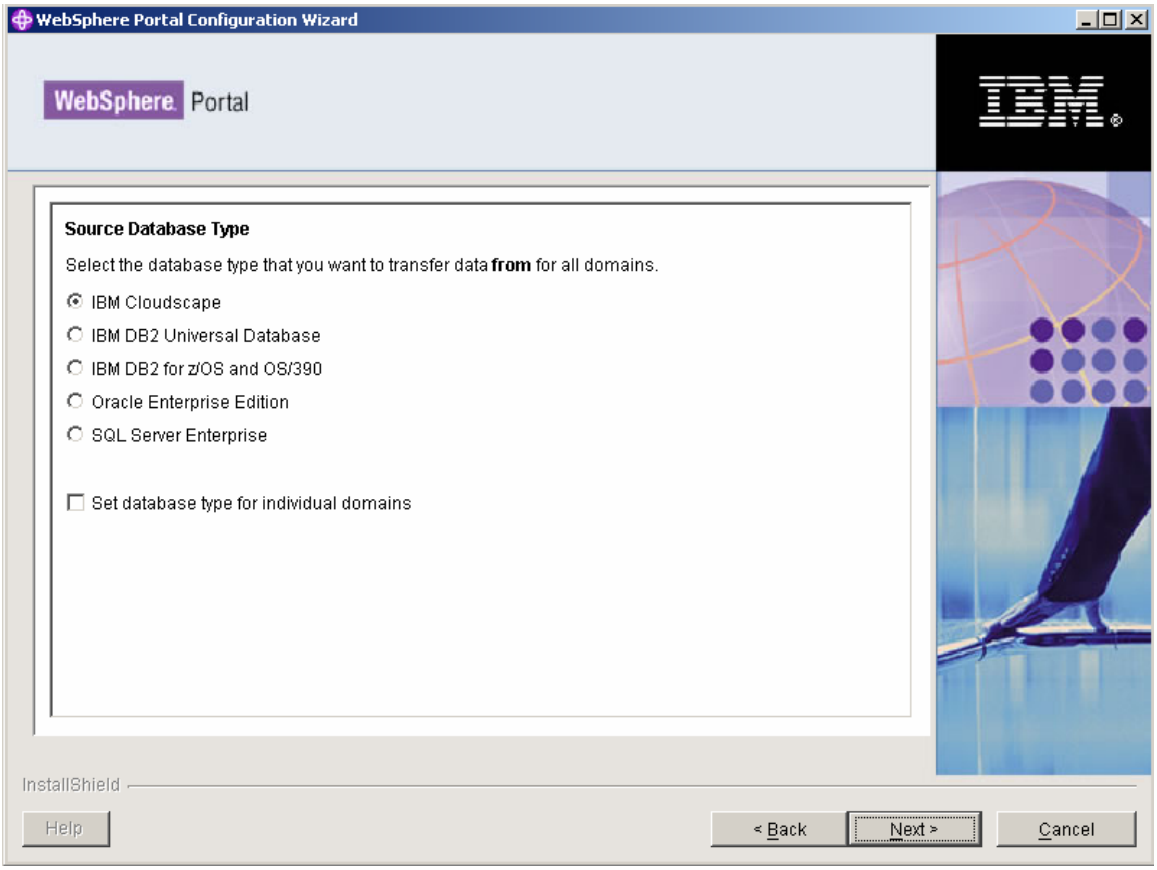
11. Select **Transfer data to another database**, and click Next button.



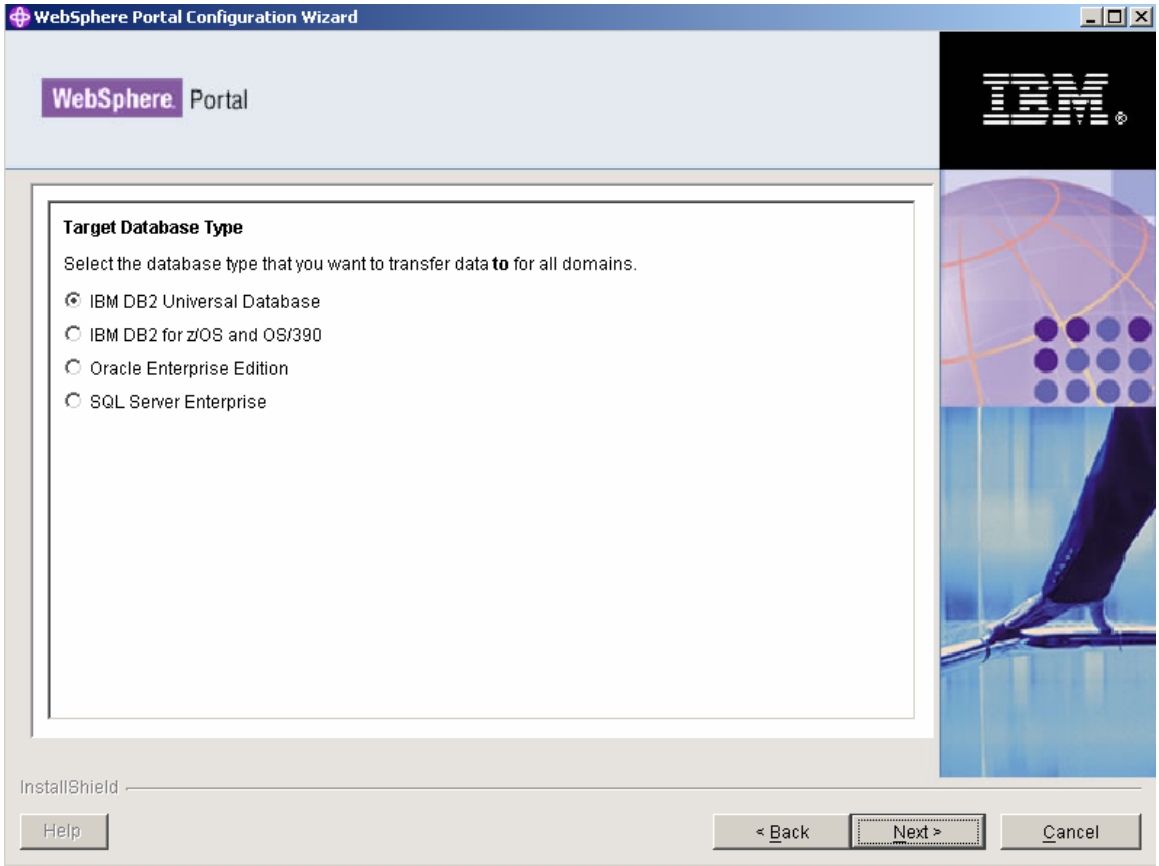
12. Provide the WSAS Admin User and password and click Next button.



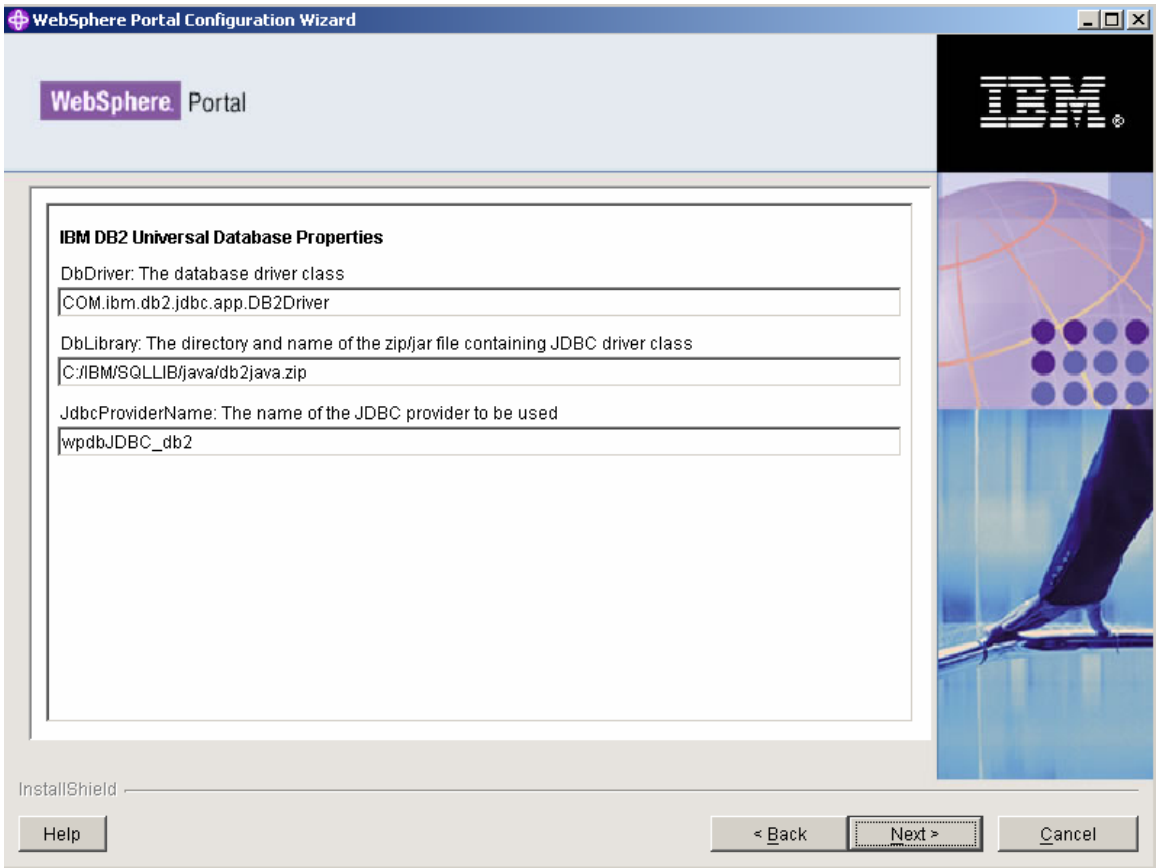
13. Select the IBM Cloudscape as Source Database Type and click Next button.



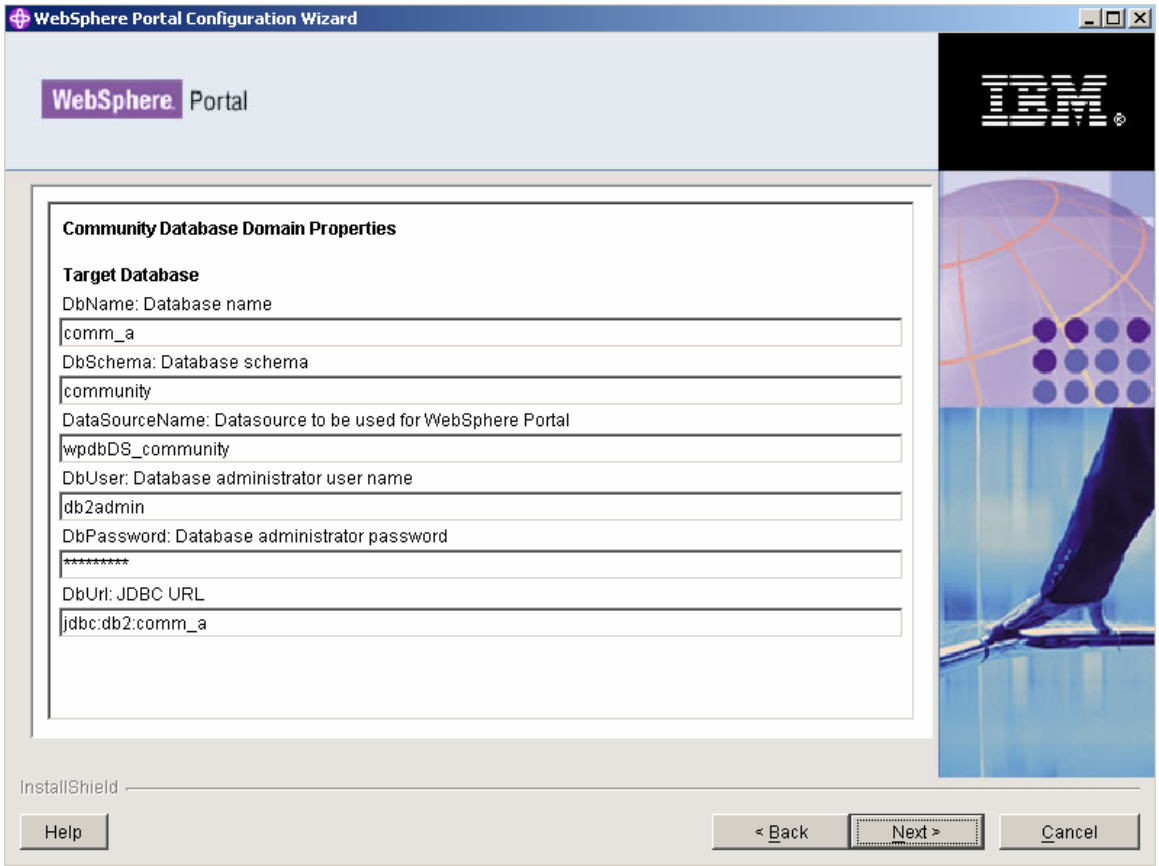
14. Select the DB2 Universal Database as Target Database Type and click Next button.



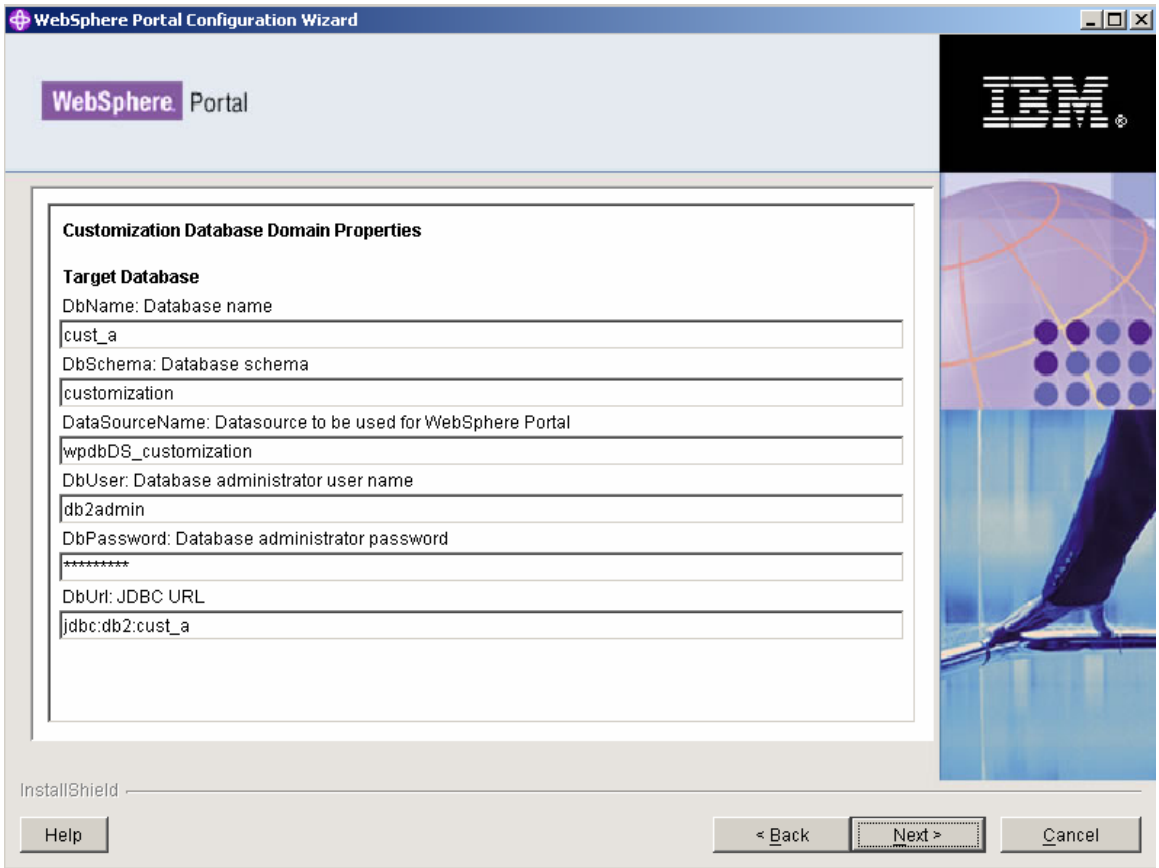
15. Fill the fields as appropriate for your environment and click Next button.



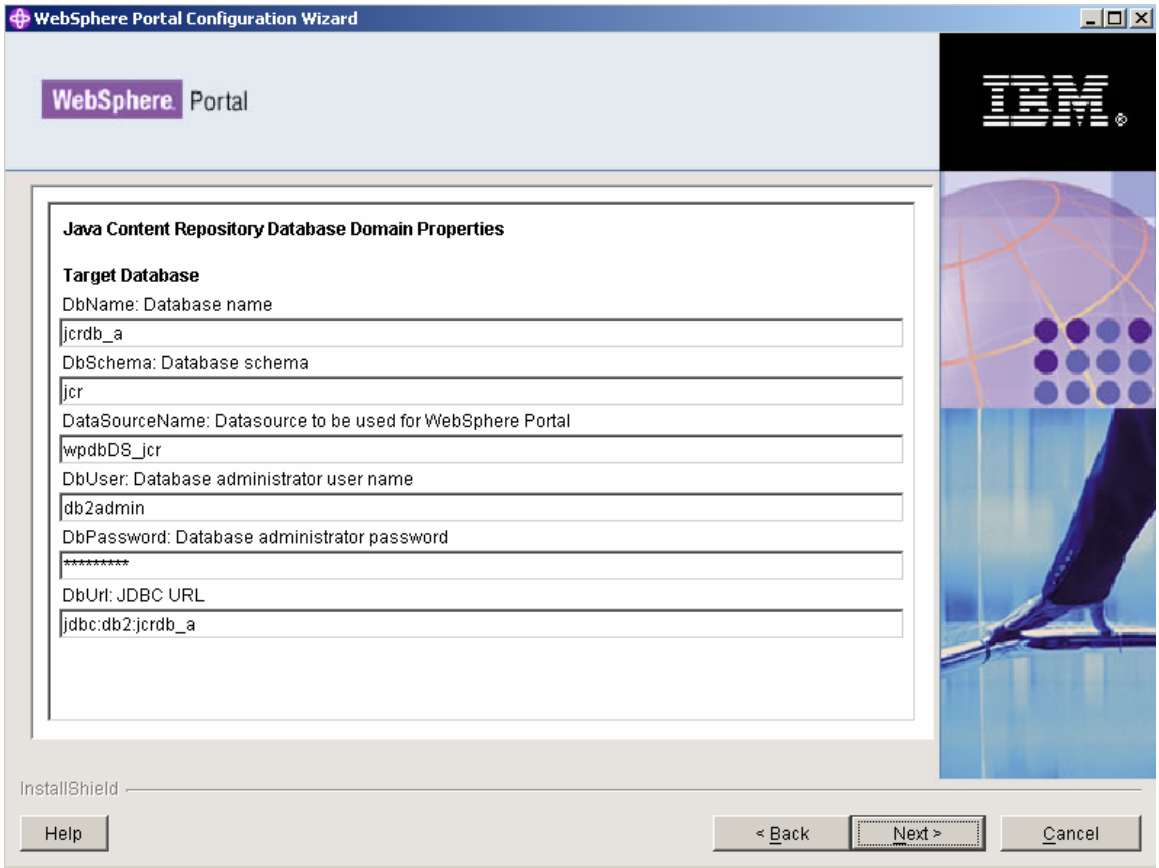
16. Fill the field as specified in the screenshot and click Next button.



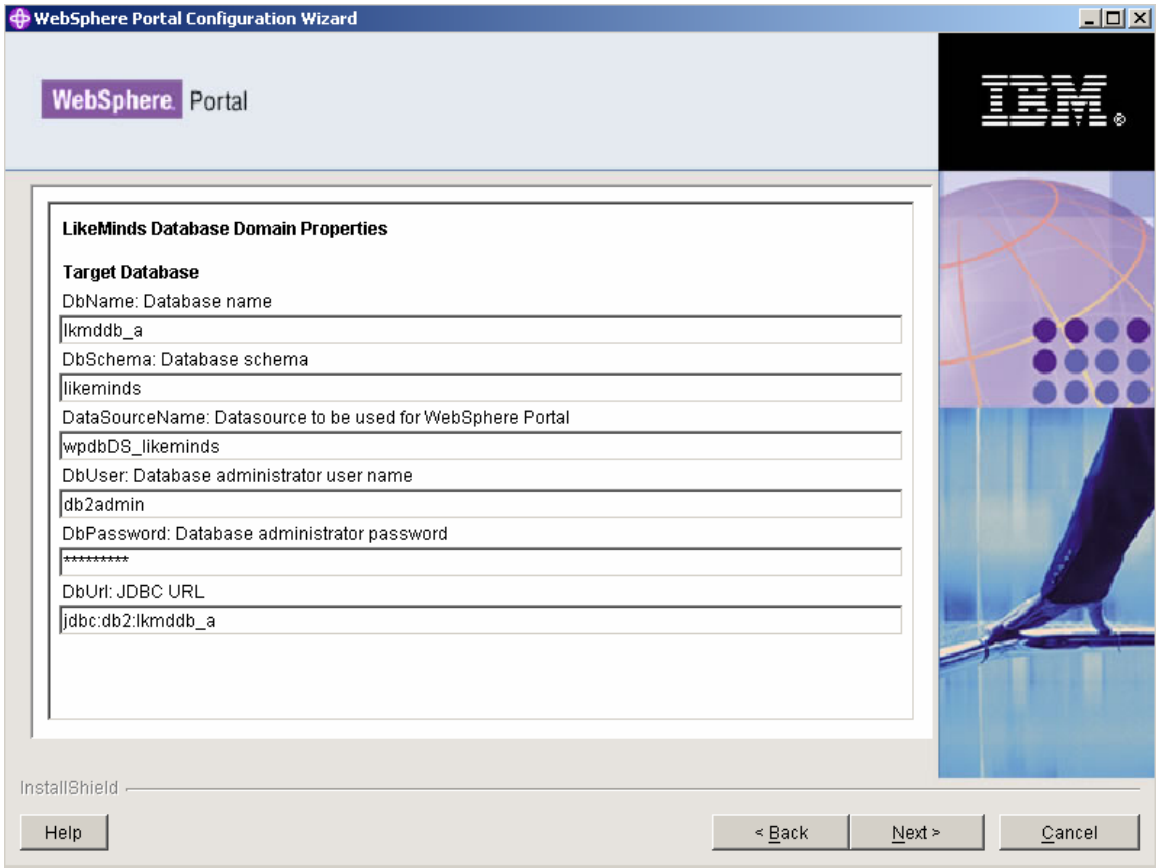
17. Fill the field as specified in the screenshot and click Next button.



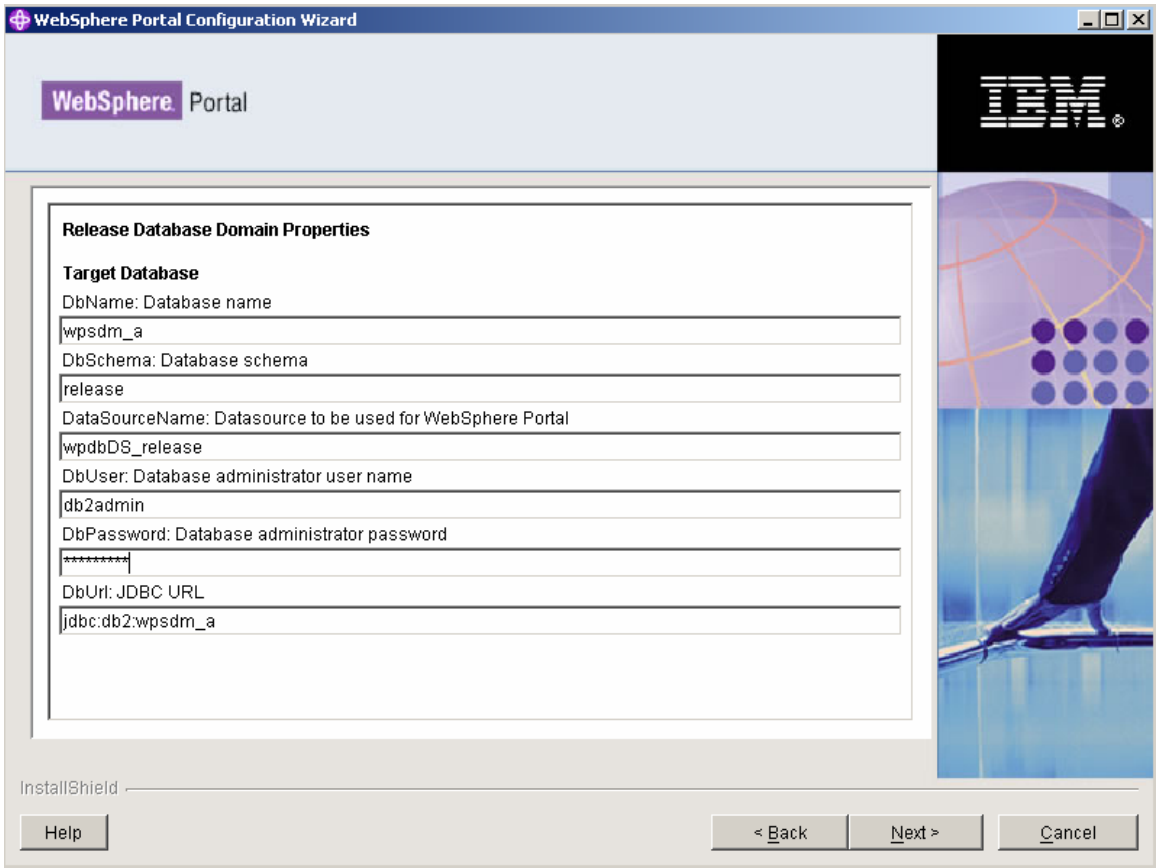
18. Fill the field as specified in the screenshot and click Next button.



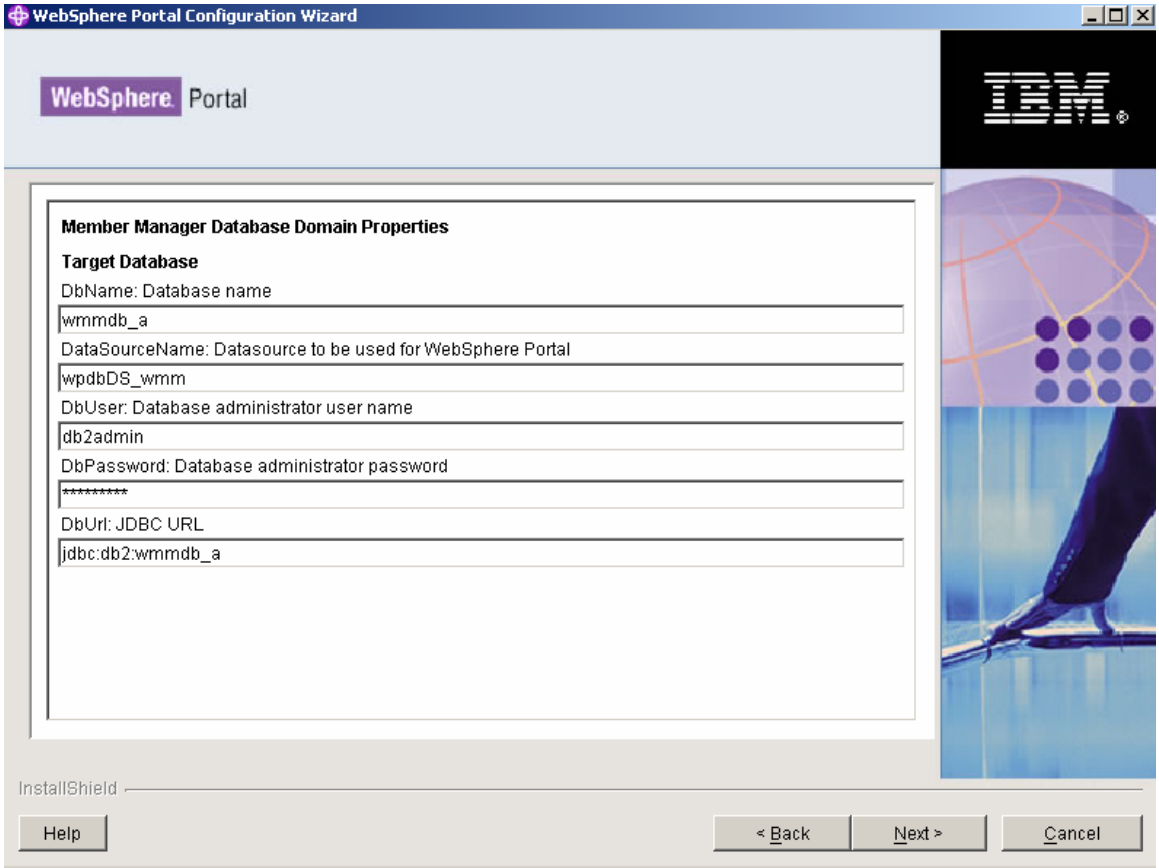
19. Fill the field as specified in the screenshot and click Next button.



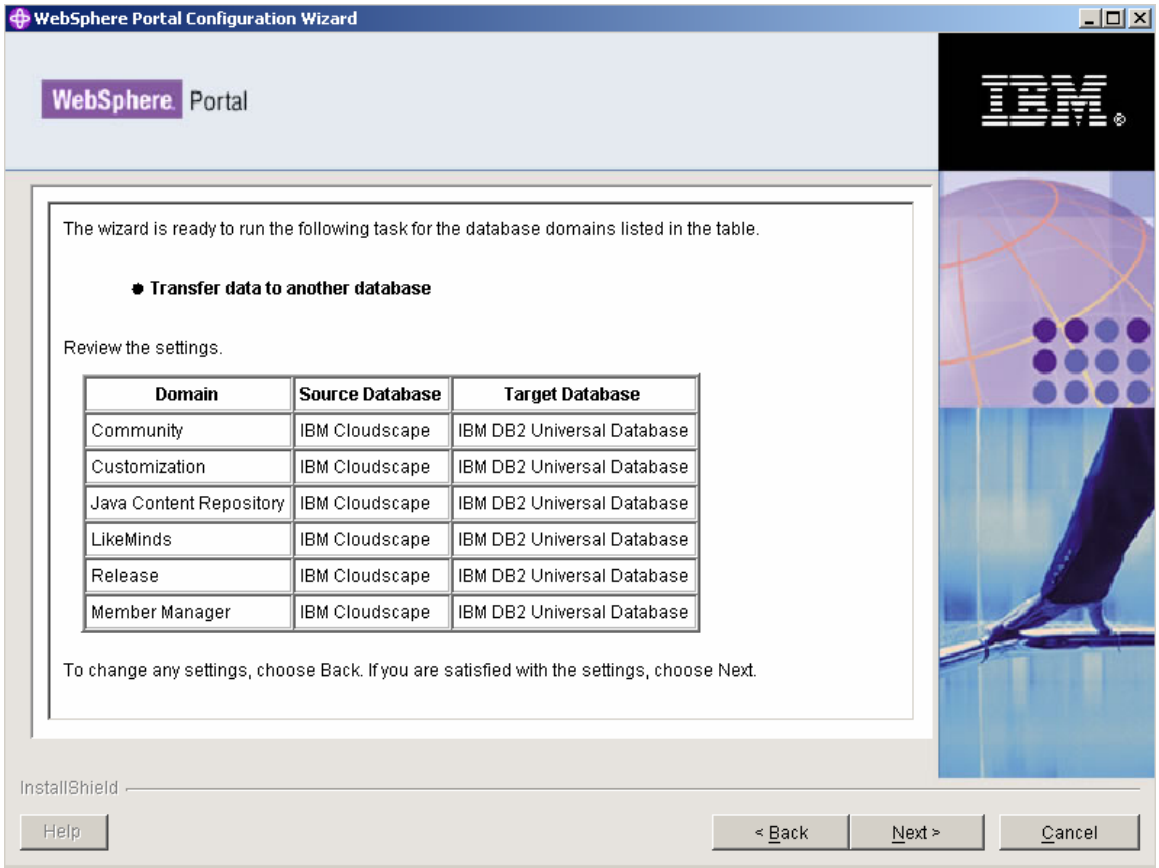
20. Fill the field as specified in the screenshot and click Next button.



21. Fill the field as specified in the screenshot and click Next button.



22. Fill the field as specified in the screenshot and click Next button.



23. After the task completes successfully, ensure Portal is started and please verify the Portal by rendering the Portal from a browser:

The default Portal URL is http://pnode:9080/wps/portal

Configure Portal to use a remote IBM HTTP Server

With WAS 6, the web server architecture has changed significantly. The web server is now listed as a separate Server in the AdminConsole and can be managed from there as well.
Details on how to configure a web server to WAS 6 can be found in the WAS InfoCenter at the following links:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/topic/com.ibm.websphere.nd.doc/info/ae/ae/tins_webplugins_single.html
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/topic/com.ibm.websphere.nd.doc/info/ae/ae/tins_webplugins_remotesa.html

1. Install the Web server on a remote machine
/<cd root>/W-9/IHS/install.exe

2. Install the plugin on a remote machine

/<cd_root>/W-9/plugin/install.exe

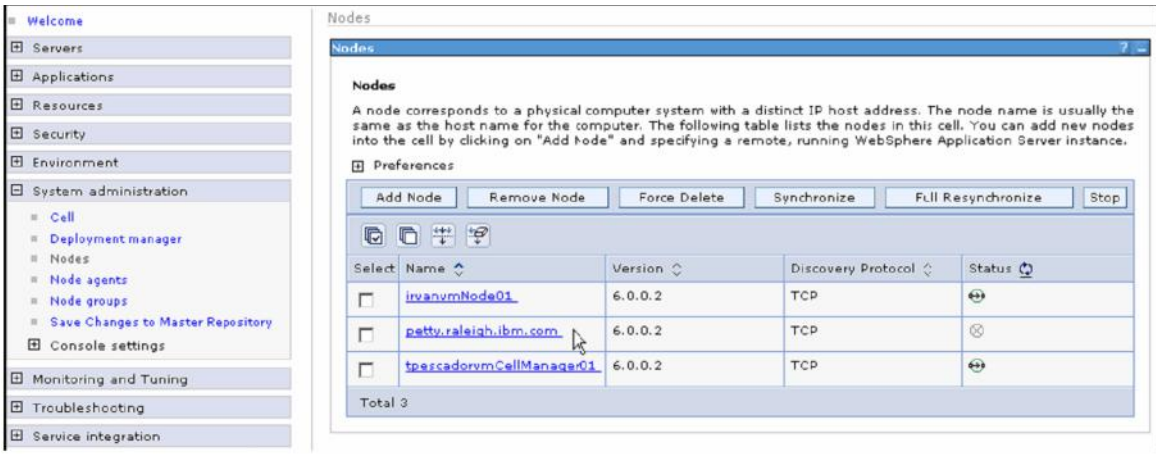
3. Move configurewebserver1.bat script from < /<plugin_root>/bin to the /<was_root>/bin on the DMGR machine.

4. Run configurewebserver1.bat script on dmgr.

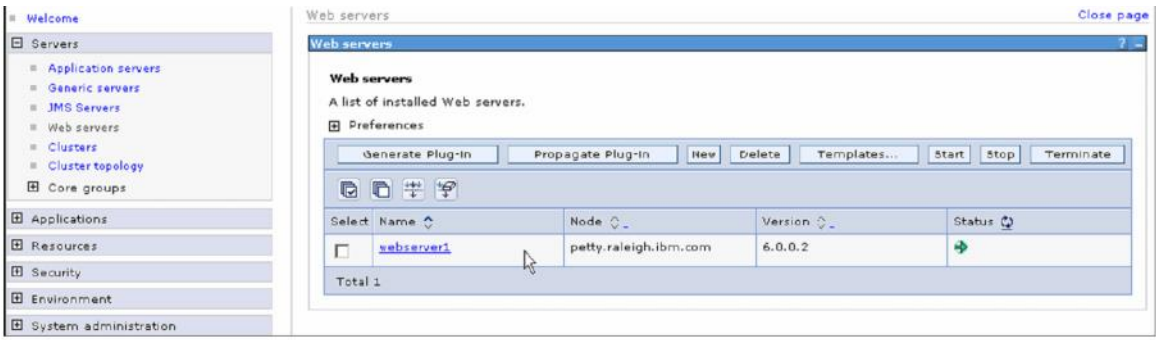
Note: When running the configurewebserver1.bat script you should be prompted by a pop-up box to provide the WSAS admin user credentials.
Providing these credentials to essential for the script to be able to make a SOAP connection to the DMGR since security has been enabled by the Portal install.
On UNIX environments the pop-up box may not appear and you will receive a credential error when attempting to run the configurewebserver1.sh script. If this occurs, please edit the <dmgr_profile_root>/properties/soap.client.props file temporarily and add the current userid and password for the following properties:

com.ibm.SOAP.loginUserid
com.ibm.SOAP.loginPassword
After adding the values and saving the file, simply re-run the configurewebserver1 script. Once the script has completed, please edit the soap.client.props file again and remove the userid and password you just supplied.

This script creates the Web server node in the AdminConsole.



and the Web server server entry in the AdminConsole

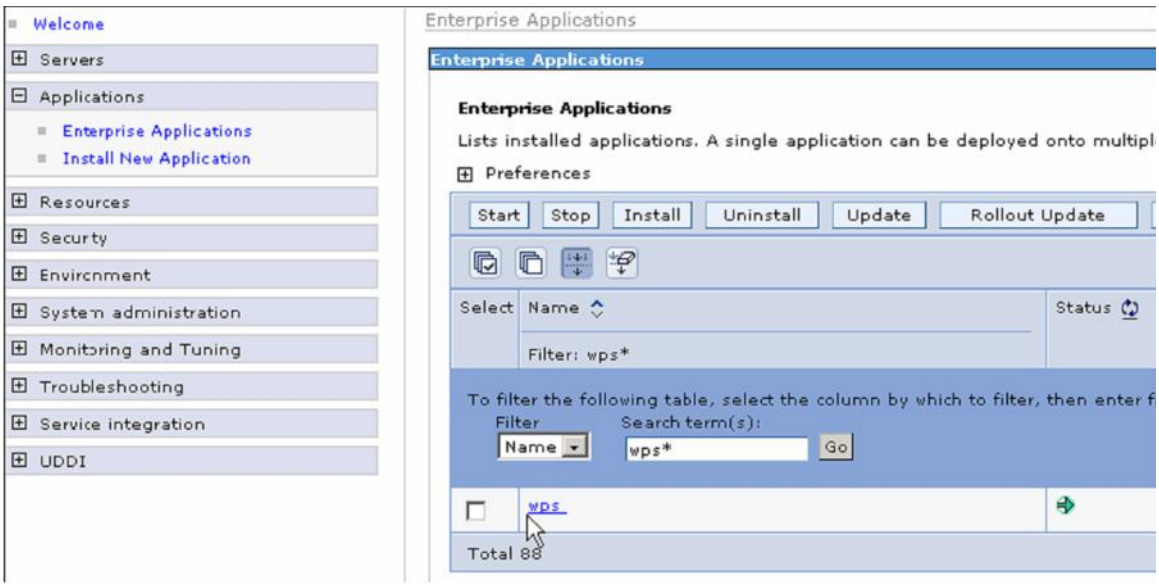


The script also tries to map all the existing Enterprise Applications (EAs) to the Web server entry, but may fail on some Windows environments because of the fact that some of the Portal EAs have more than 256 characters in their paths.
The results are that after this fails the node and server entry are created successfully, but none of the EAs are mapped to the Web server. This means that when you regenerate the Web server plugin it does not know about any of the EAs and therefore none of them are listed in the plugin-cfg, which means that if the plugin is moved to Web server it will not be able to serve the EAs.

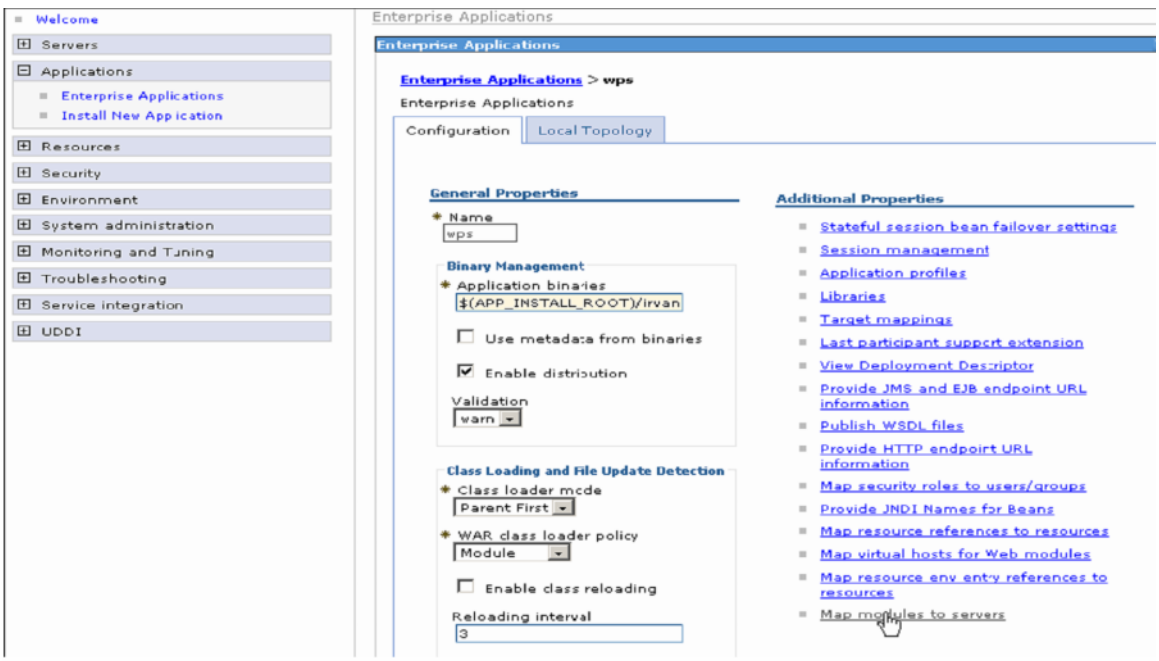
If the **configurewebserver1.bat** script completes successfully then please move forward to Step 6. If the script runs successfully you will need to logout and login back into the DMGR AdminConsole to see the changes before moving to Step 6.
If you are on Windows and the script fails because of the 256 character limit, you must follow the following procedure, Step 5, to manually map the EAs to the web server.

5. So to accomplish this you must manually map each of the Enterprise Applications to the WebSphere_Portal server AND the webserver1 server thru the AdminConsole by first navigating to:

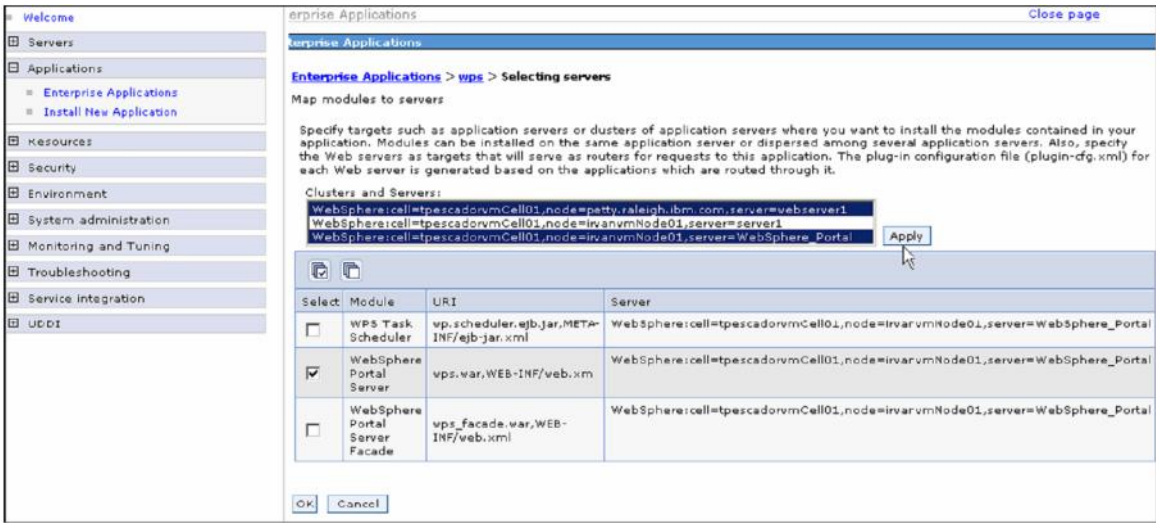
Applications>Enterprise Applications
In this example, we will map the wps EA as an example. This should be done for each EA that you wish the Web server to serve.
Click on the EA name, in this case “wps”…



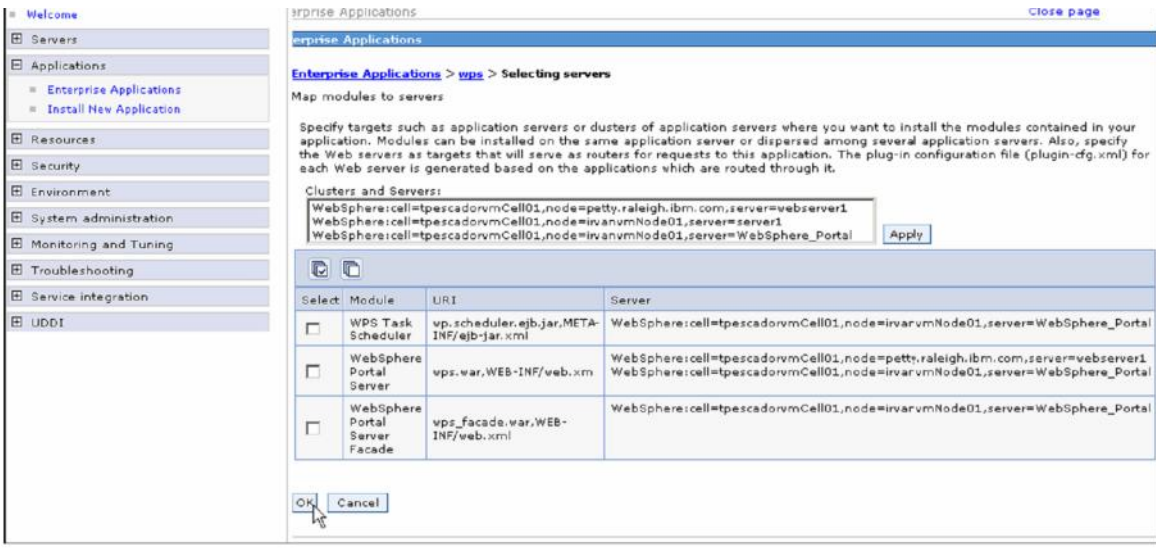
Click on Map modules to servers



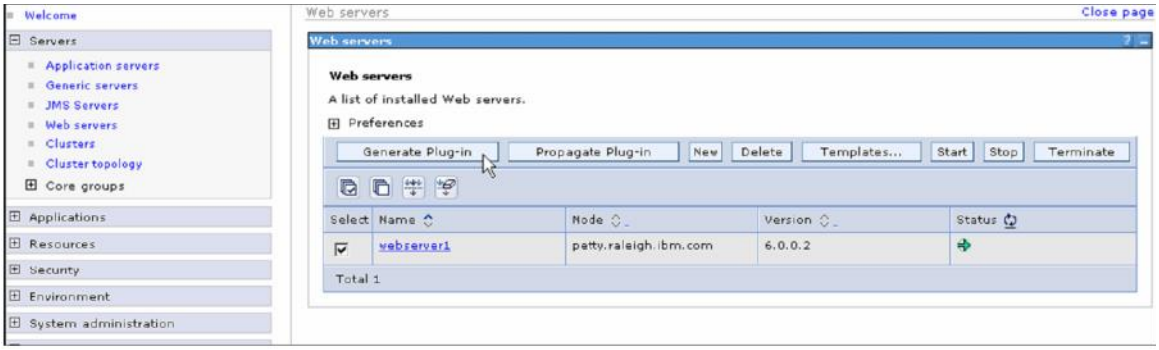
Select the Module, WebSphere Portal Server (wps.war) and then highlight both the webserver1 and WebSphere_Portal entries listed in the Clusters and Servers box and click Apply



Now you will see that the Module WebSphere Portal Server (wps.war) is now mapped to both servers:



6. Then regen the plugin by navigating to Servers>Web servers and select the webserver1 entry and click Generate Plug-in. This is written to: <dmgr_profile_root>/<profile_name>/config/cells/<cellname>/nodes/<no dename>/servers/webserver1/plugin-cfg.xml



7. Move the plugin to the remote Web server which is under <plugin_root>/config/webserver1

8. Restart the DMGR, Web server and Portal

9. Change the WpsHostName and WpsHostPort properties in the wpconfig.properties to reflect the Web server values

10. Verify the Portal can be accessed thru the Web server

Create the cluster definition

Note: You must add the PortalAdminPwd and the WasPassword values to the *wpconfig.properties* file and all the database password values to the *wpconfig_dbdomain.properties* file or supply these values on the command line. This is because of what was described before in that the ConfigWizard replaces all the password values with the string, “ReplaceWithYourPassword” for security reasons.
Also, please ensure that the **PrimaryNode** property in the *wpconfig.properties* is equal to **True**.
Important Note: If you wish to change the name of the cluster to something other than the default in the *wpconfig.properties* file, you MUST change is now BEFORE the cluster definition is created. This can be changed by editing the *wpconfig.properties* file and changing the *ClusterName* property.
Also, the cluster-setup task will automatically configure the DRS settings for the nodes in the cluster.
1. Run <wp_root>/config/WPSconfig.bat cluster-setup

2. Restart DMGR, nodeagent and WebSphere_Portal to load the new configuration

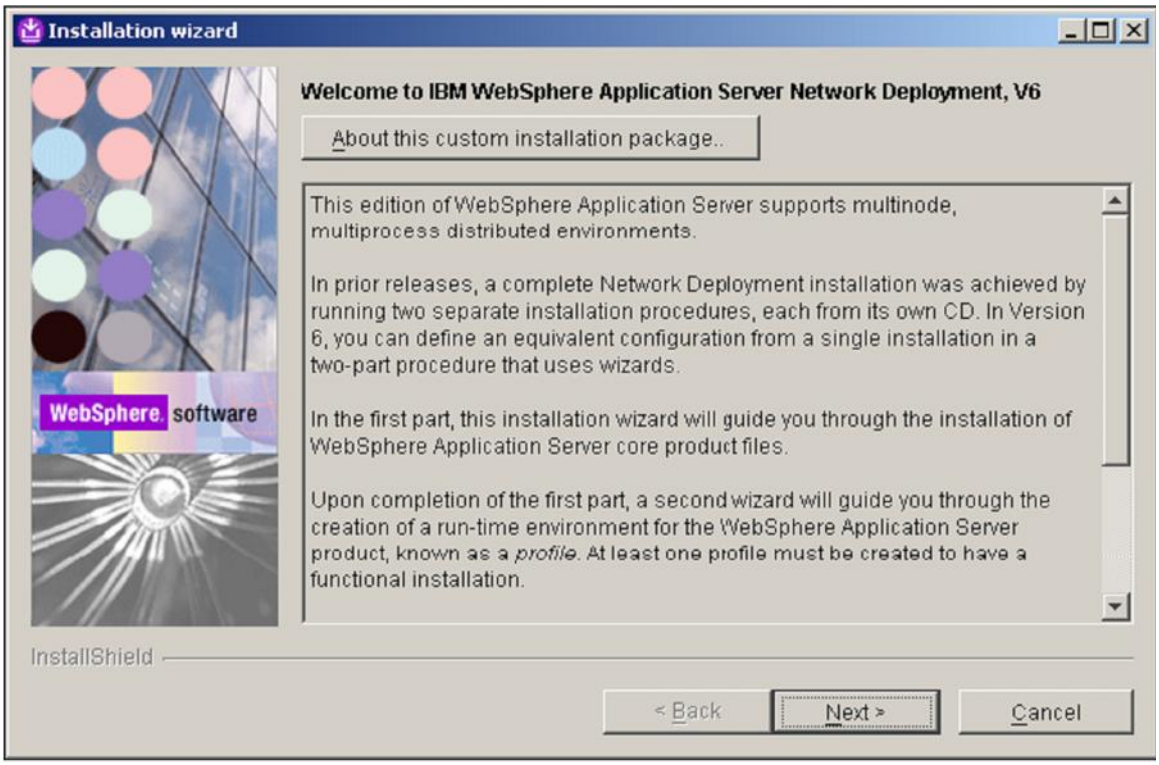
3. As a checkpoint in the process, you now have a 1 node cluster configured to an external database and using the WMM database for security.

Install WSAS 6.0.2.9/WPS 6.0.1.1 on future cluster node, Node2

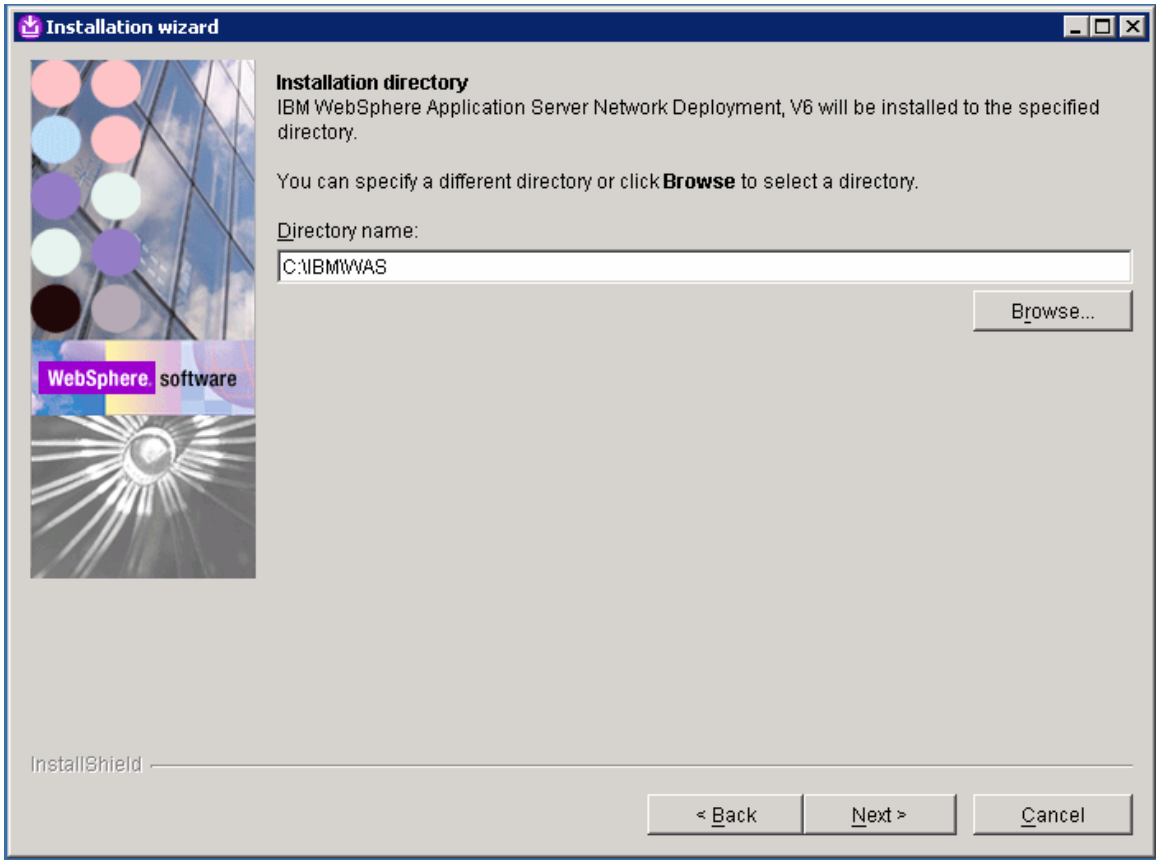
Important: This guide explicitly defines the required approach to build a Portal cluster which has been installed on WebSphere Process Server. To do this you must install Portal into an already federated WSAS/WPS profile. Because of this requirement, we MUST install WSAS/WPS from their native installers and federate the node BEFORE using the Portal installer to install Portal.

1. Install WSAS on Node2 by running the installer from:
<cd_root>/W-1/windows/ia32/ifpackage/WAS/install.exe

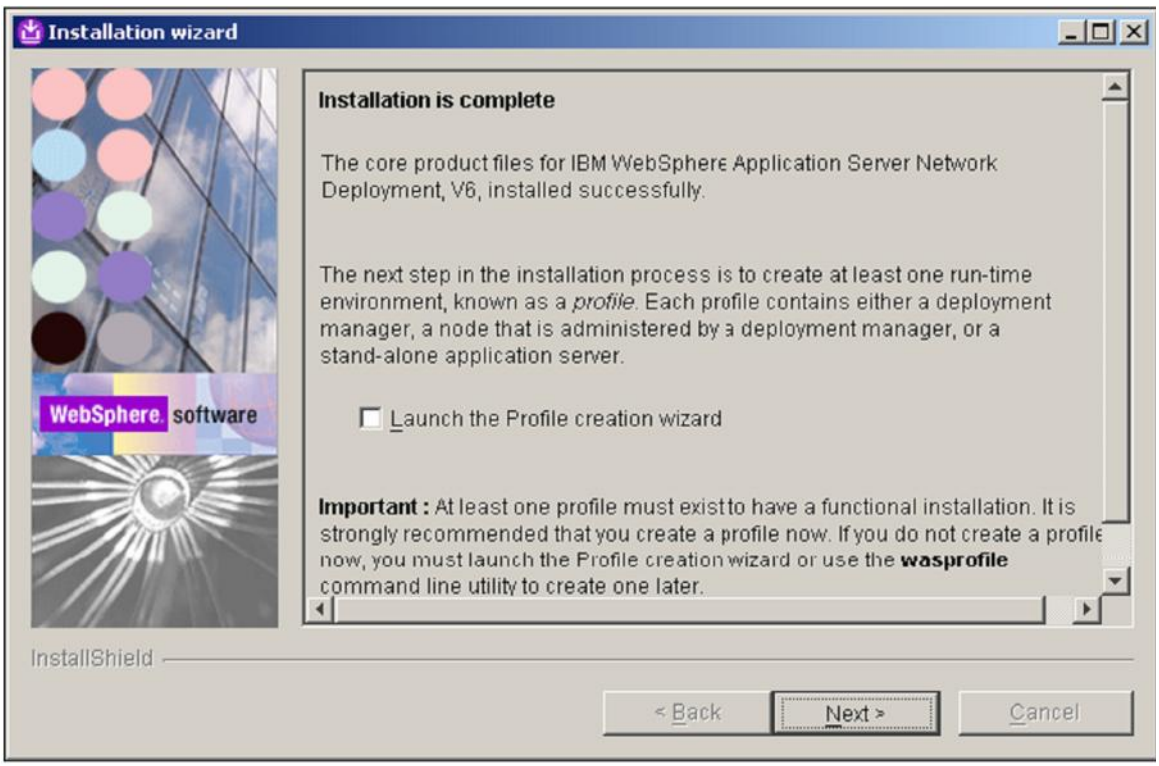
Note: Make sure the installer screen is titled "**Welcome to IBM WebSphere Application Server Network Deployment, V6**". This title means that you can use this installer to install either, DMGR or WSAS profiles. If the title is "WebSphere Application Server Version 6.0", you are using an installer that only has the ability to install WSAS profiles and not DMGR profiles:



2. If installing on Windows, when asked for install location, please shorten the default path. There is a path name limitation in Windows. Windows cannot handle path names longer than 256 characters.



3. You should be prompted during the install (with a panel near the end) if you would like to create a profile….at this time please choose NOT to create a profile by making sure the "Launch the Profile creation wizard" checkbox remains UNCHECKED. We will create a WPS profile at the end of the WPS install.



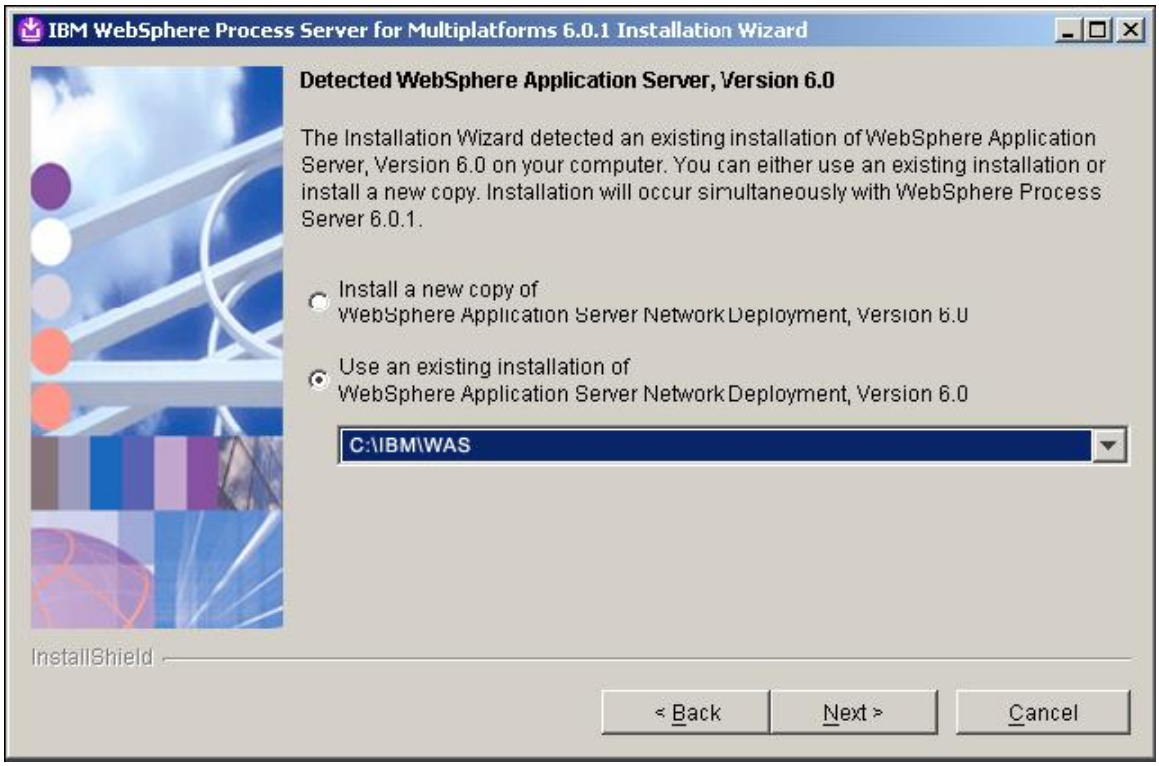
4. The WSAS installer from the Portal CDs will automatically upgrade WSAS to 6.0.2.9

Install WPS v6.0.1.1

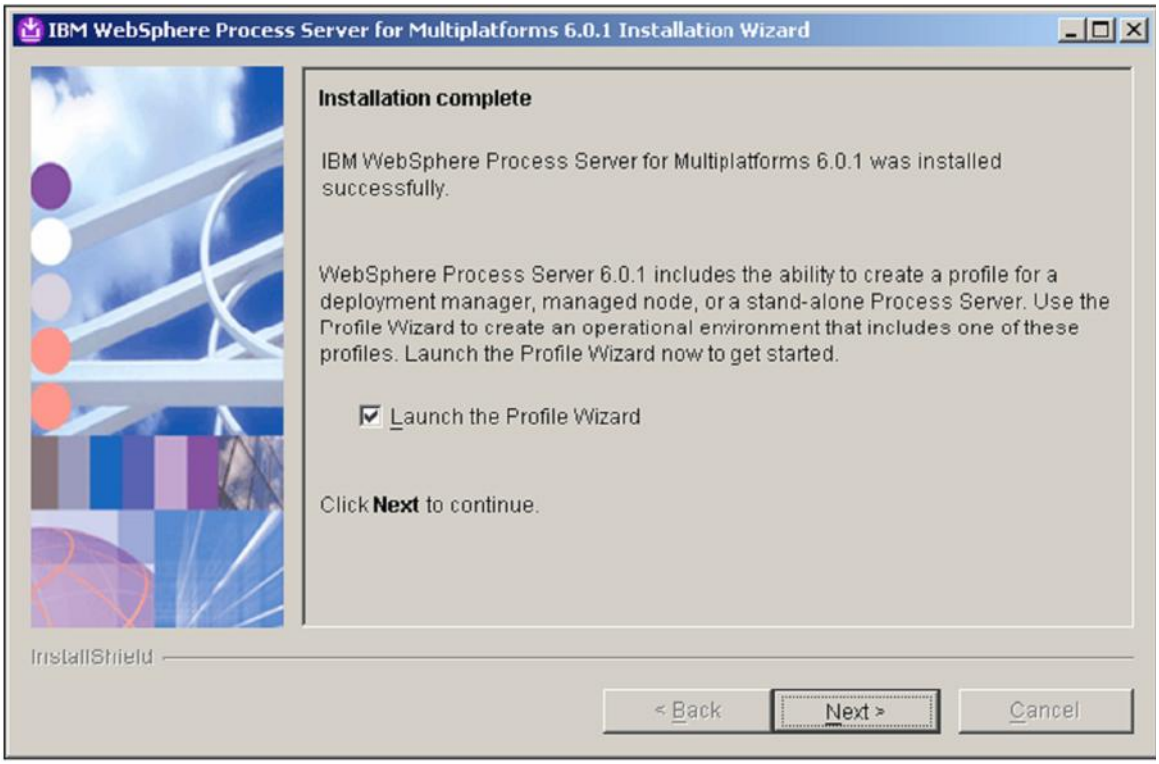
5. Install WPS 6.0.1.1 by running the installer from:
<cd_root>/W-2/windows/ia32/WBI/install.bat

Note: Please ensure you use the install.bat file and NOT the install.exe to install WPS

6. Ensure you use the existing WAS you just installed:

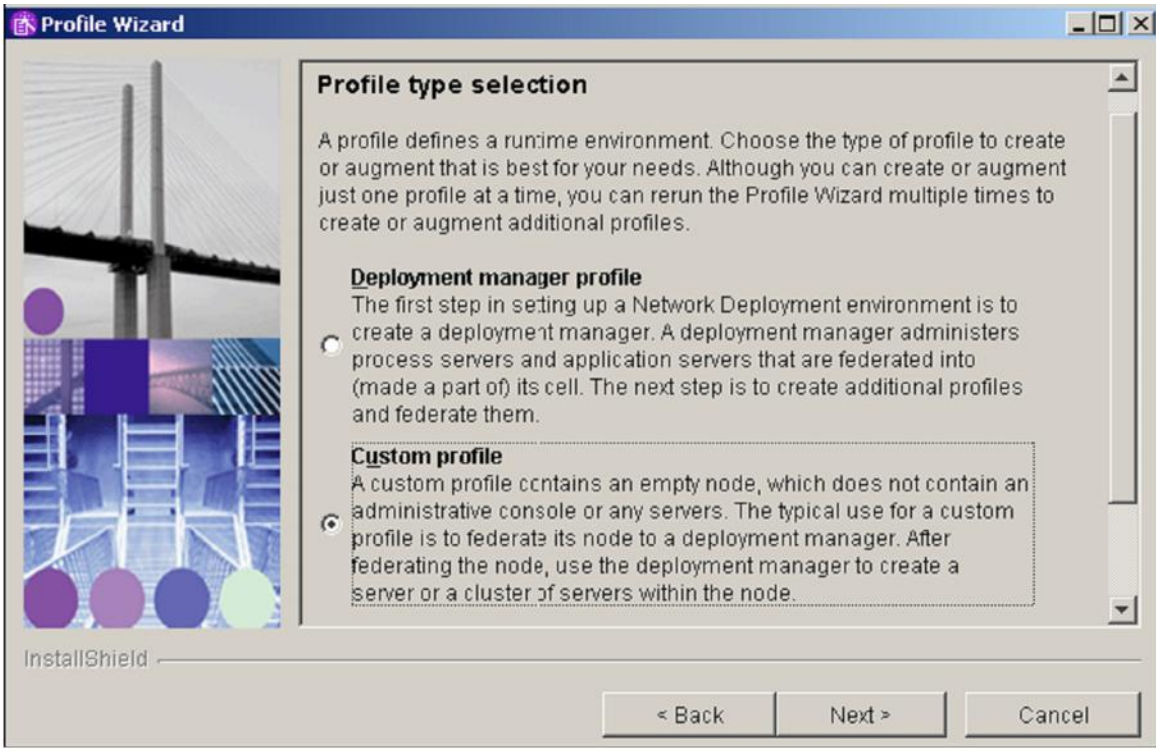


7. You should be prompted during the install (with a panel near the end) if you would like to create a profile. At this time we will create a WPS Custom profile. Please ensure the "Launch the Profile Wizard" checkbox is CHECKED and click Next to launch the WPS profile creation wizard.

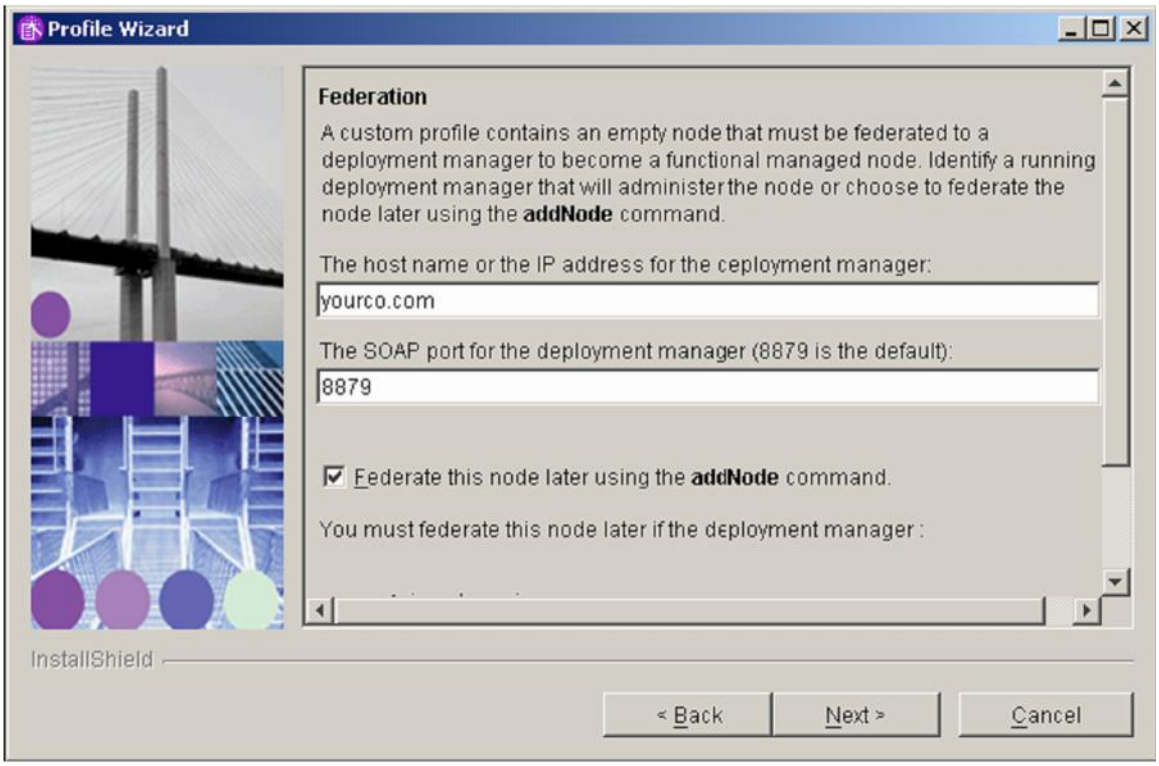


Note: If you have to launch the WPS profile creation wizard manually, please ensure you launch the WPS profile creation wizard and NOT the WSAS profile creation wizard. The WPS profile creation wizard script is located at:
<wsas_root>/bin/**ProfileCreator_wbi**/pcatWindows.exe

8. After the profile creation wizard is launched, ensure the “Custom profile” radio button is selected on the “Profile type selection” panel and click “Next”:



9. Because security is enabled in the cluster, you will not be able to use the automatic federation feature on secondary nodes. Please ensure the “Federate this node later using the addNode command” checkbox is checked.



Federate the profile to DMGR

10. After the profile is created we will federate the node using the addNode command
Before running the addNode.bat command ensure the DMGR has been started
To add a node to the deployment manager cell, run the script *addNode.bat* command on the command line of the snode to be added:

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

Where:
wsas_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*.

Note: This value can be determined by accessing the DMGR AdminConsole and navigating to:
System Administration>Deployment Manager and then expand the Ports property under Additional Properties and then you can see the value for SOAP_CONNECTOR_ADDRESS.

admin_user_id is the WebSphere Application Server administrative user name. This parameter is optional but is required if security is enabled.
admin_password is the administrative user password. This parameter is optional but is required if security is enabled.

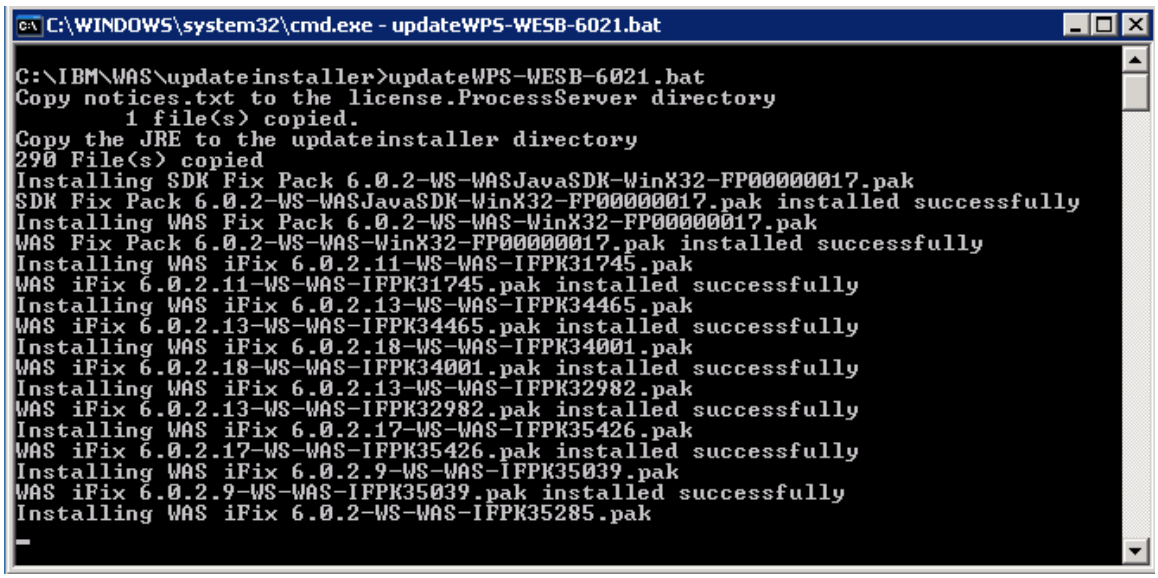
Example:
addNode.bat dmgr 8879 –username admin –password password

Note: To run the addNode command here you MUST supply username and password because security has been enabled on the DMGR.
See the appropriate Network Deployment Information Center for details on the addNode command.
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/welcome_nd.html

Upgrade WAS v6.0.2.9 to v6.0.2.17 and WPS v6.0.1.1 to v6.0.2.1

11. After the DMGR profile is created and federated to DMGR, then upgrade WAS v6.0.2.9 to version 6.0.2.17 and WPSv6.0.1.1 to version 6.0.2.1. WebSphere® Process Server Version 6.0 Refresh Pack 2 for Windows platforms, also known as Version 6.0.2, contains WebSphere Application Server v6.0.2 fix pack 17 for windows platform with all required fixes. You can download the fixpack 6.0-WS-WPS-ESB-WinX32-RP0000002.zip from:
http://www-1.ibm.com/support/docview.wss?rs=2307&uid=swg24014373

12. Extract the fixpack to <*was_root*>\updateinstaller and run the script *updateWPS-WESB-6021.bat* on the command line of the snode.



Note: If you get any errors during upgrade process, fix those errors and run the batch file again. You will not be able to start the nodeagent until you complete Step 12 of the next section titled, '*Install Portal onto the managed node, Node2*'. This is because of an incomplete wmm security configuration.

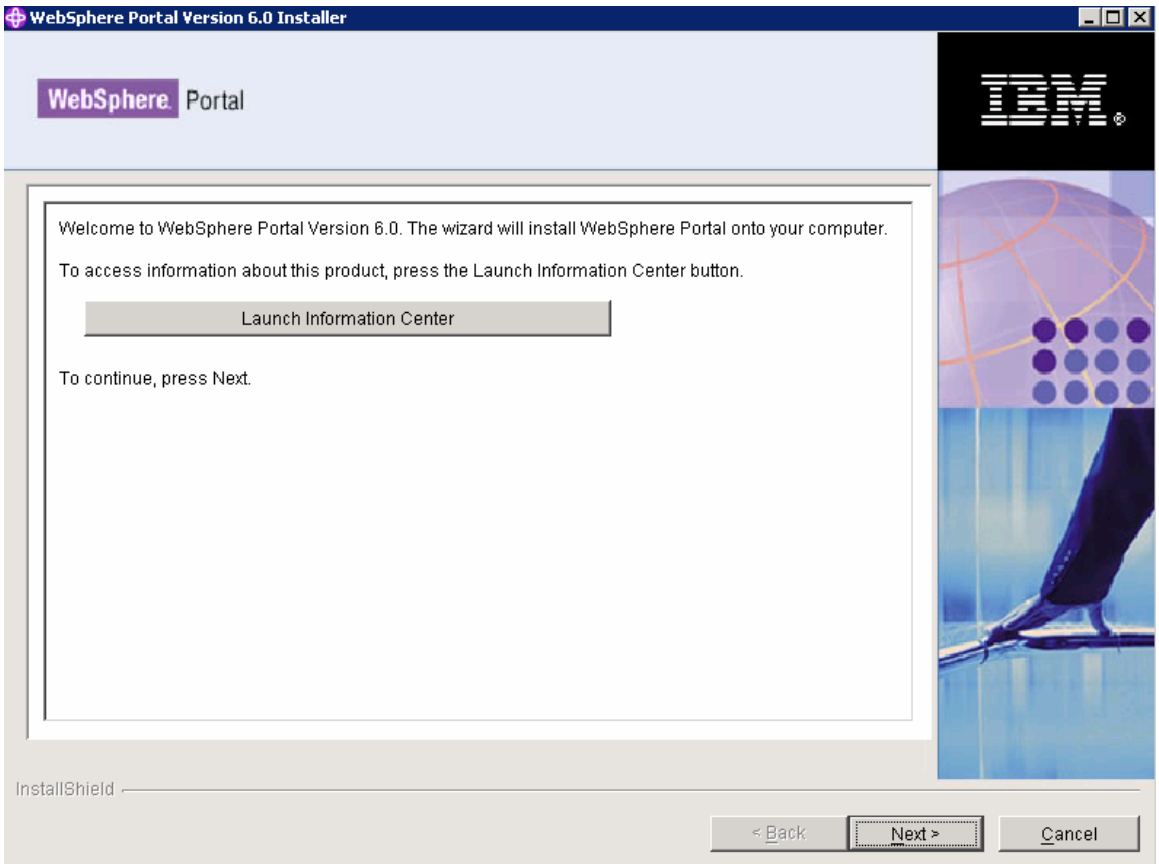
Install Portal onto the managed node, Node2

13. Before installing Portal please move the WMM jars. Update the secondary node with required WMM jar files. These files are located on the Setup CD provided as part of the installation package for WebSphere Portal. Copy the following files from the: *<cd_root>/W-Setup/dmgr_wmmjars* directory on the Setup CD to the <wsas_root>/lib directory on the secondary node:
wmm.jar
wmm.ejb.jar
wp.wire.jar

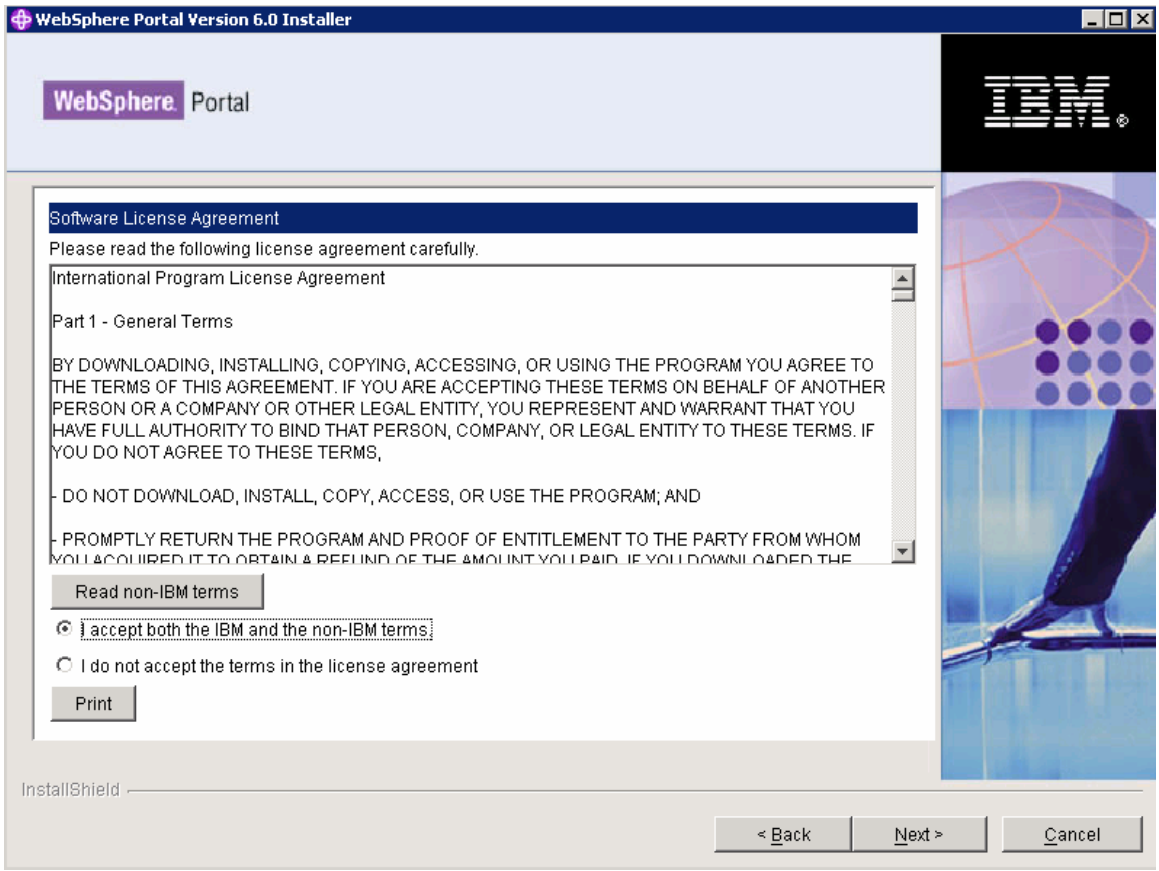
14. Ensure the time-out request for the Simple Object Access Protocol (SOAP) client for Node 2 has been increased to 6000. The default, in seconds, is 180.
Within the <wsas_profile_root>/properties/ directory, edit the *soap.client.props* file. Change the line to:

com.ibm.SOAP.requestTimeout=6000

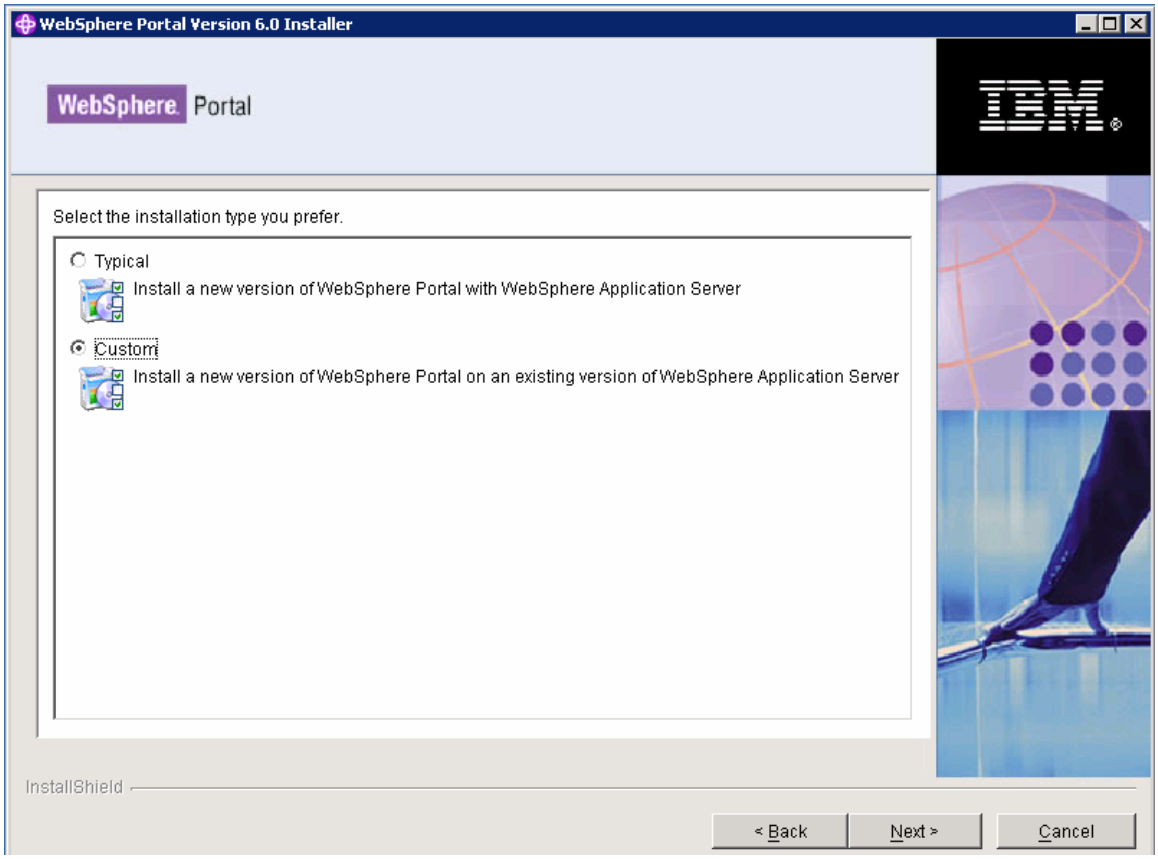
15. Begin the Portal install by using this command:
<cd_root>/W-Setup/install.bat -W startPortalServerSequence.active=false



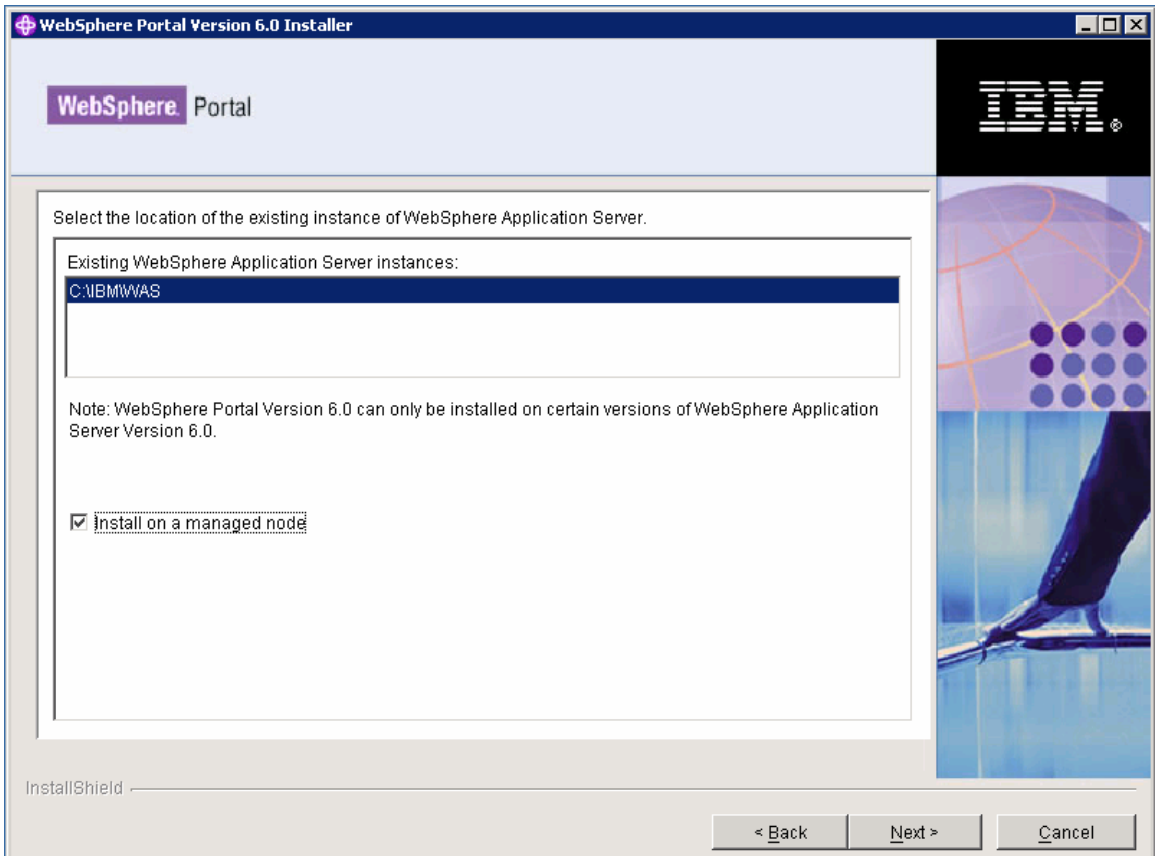
16. Accept the license agreement:



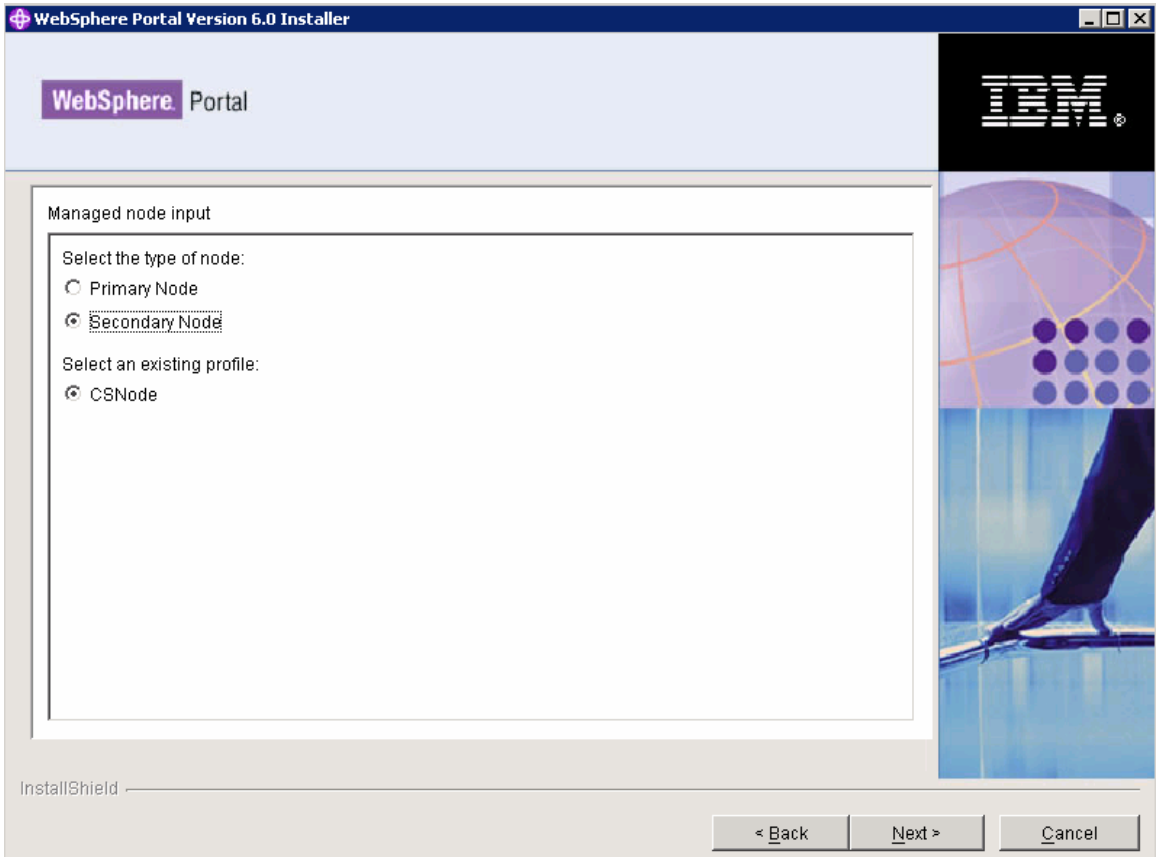
17. Select Custom as the install path



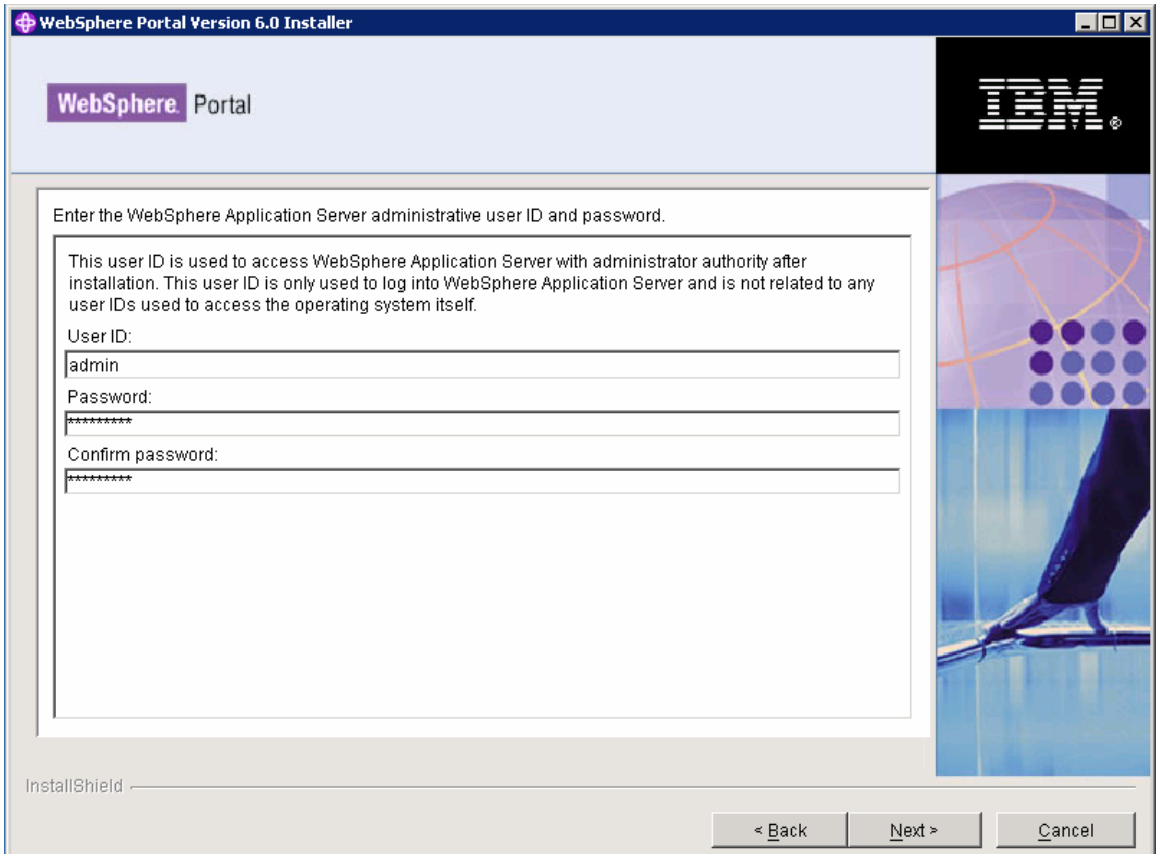
18. Select the existing WebSphere AppServer install location and check the box next to "Install on a managed node"



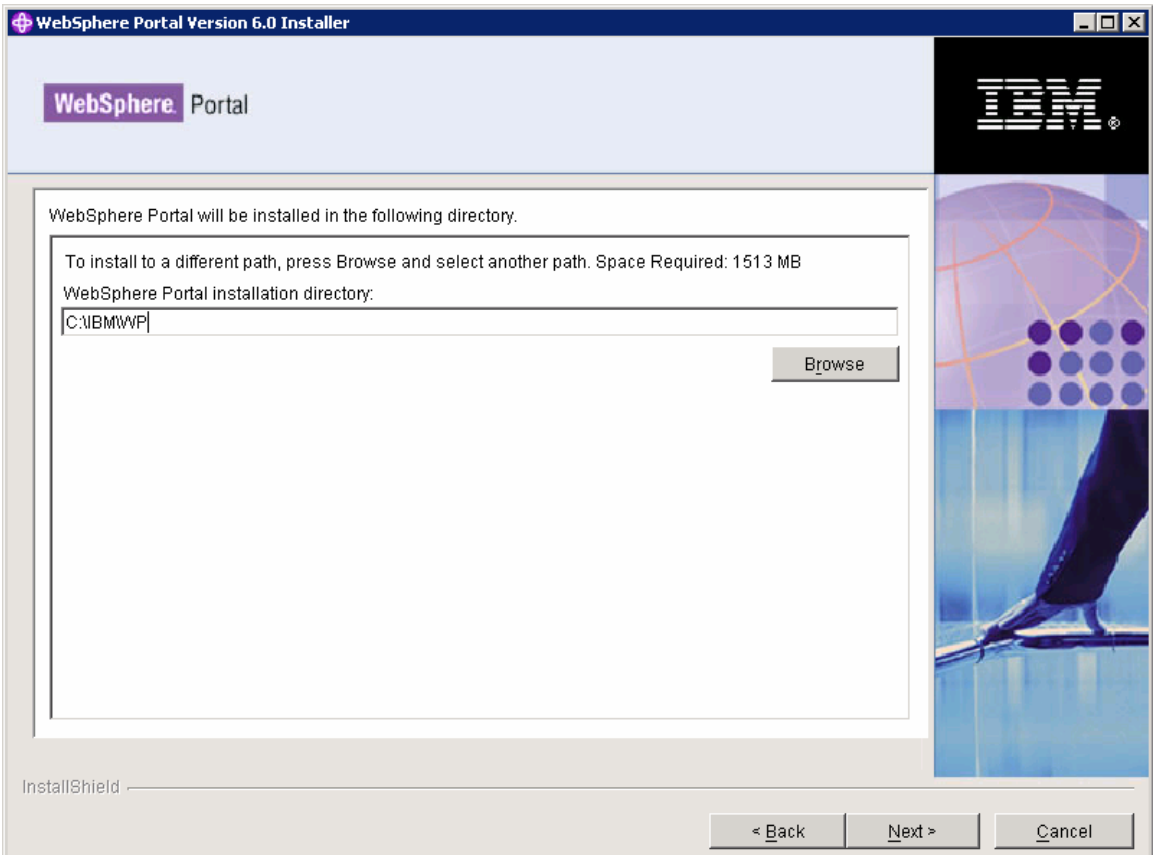
19. Select Secondary Node and select the desired profile that you wish to install Portal onto



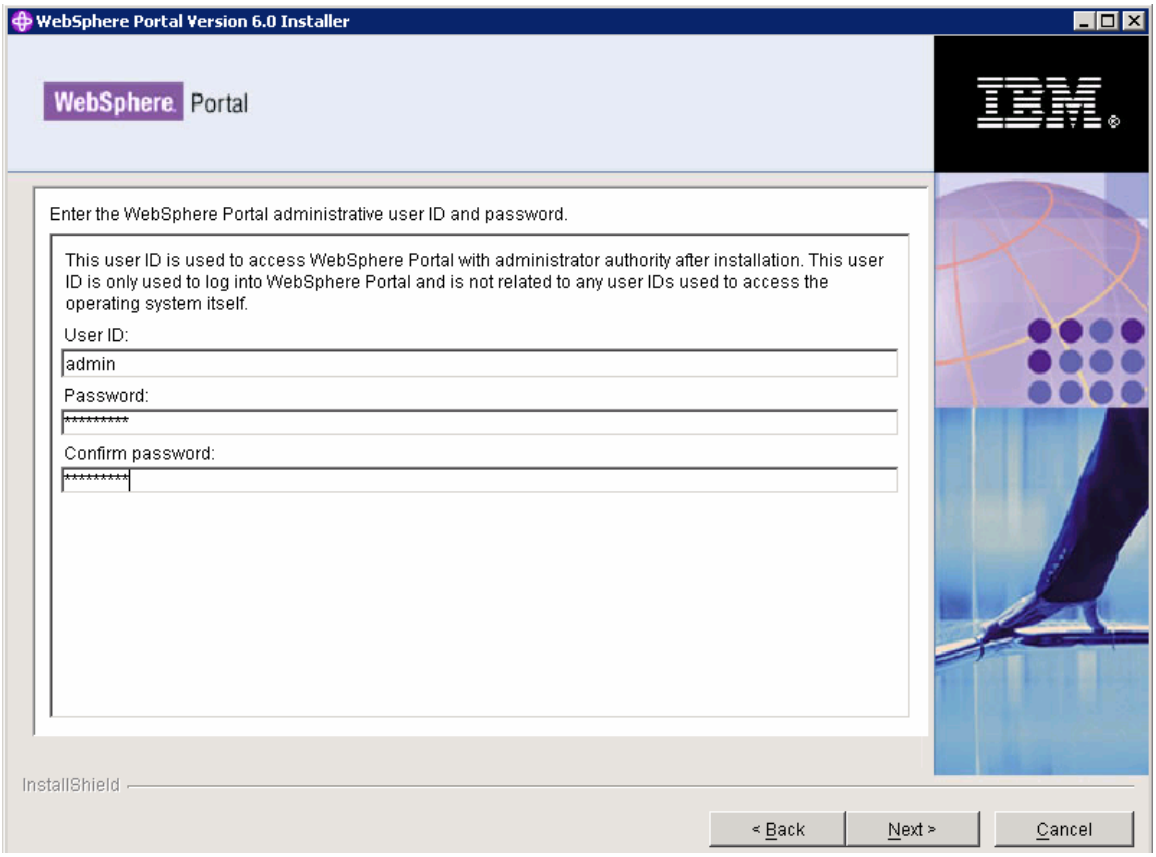
20. Provide the current WSAS Admin User and password.



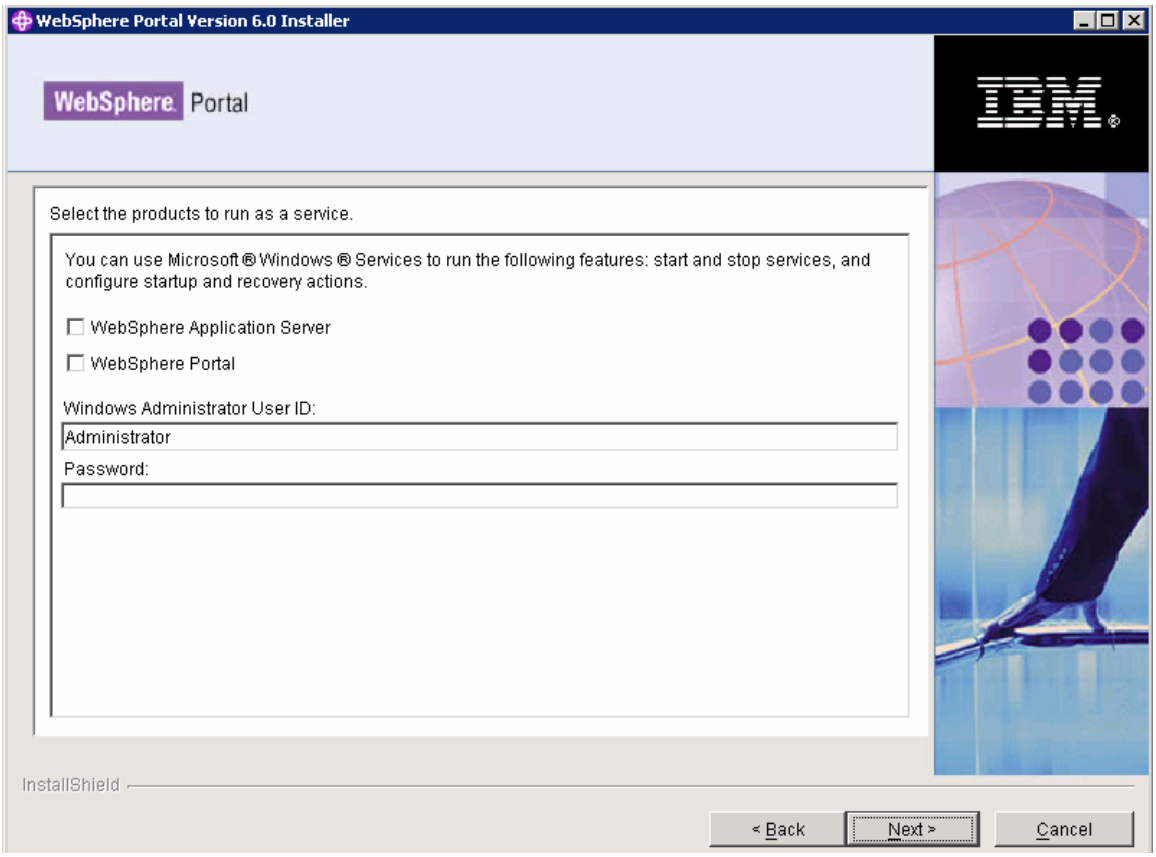
21. Define the desired location for Portal to be installed



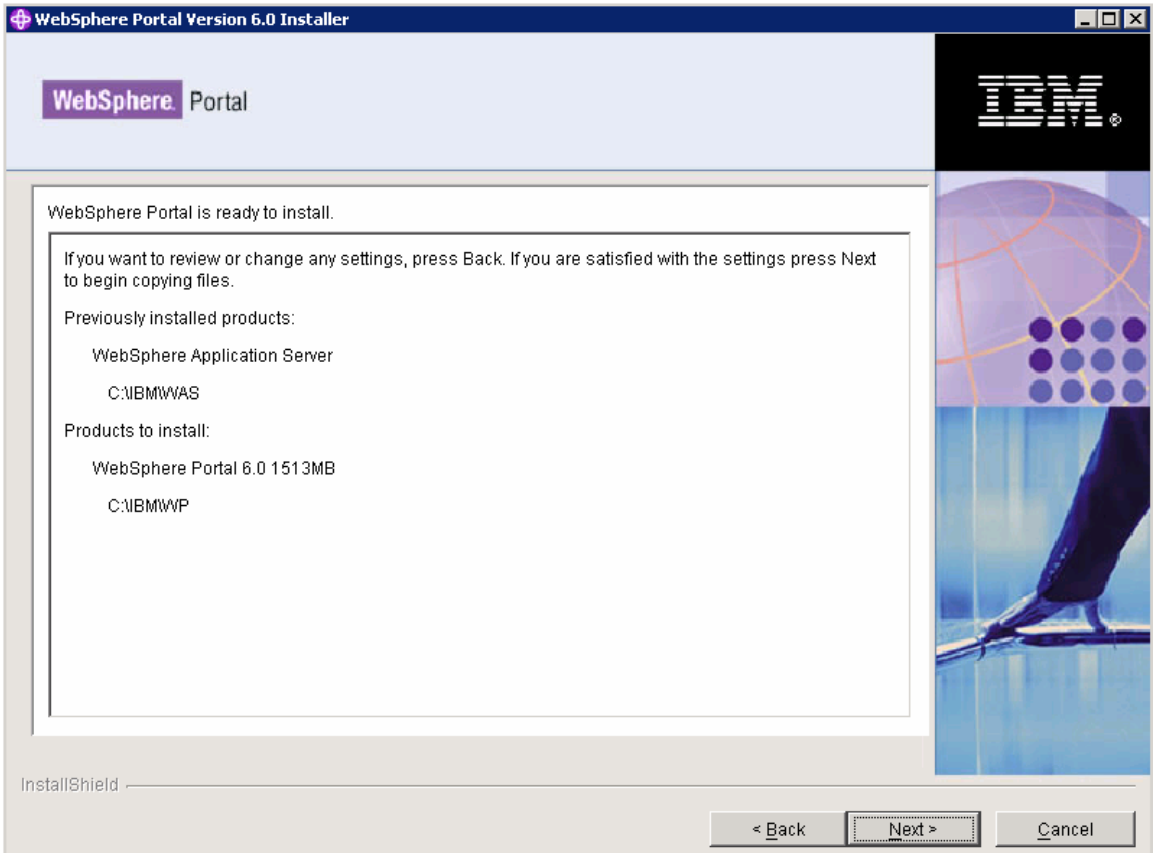
22. Define the Portal Admin User and password



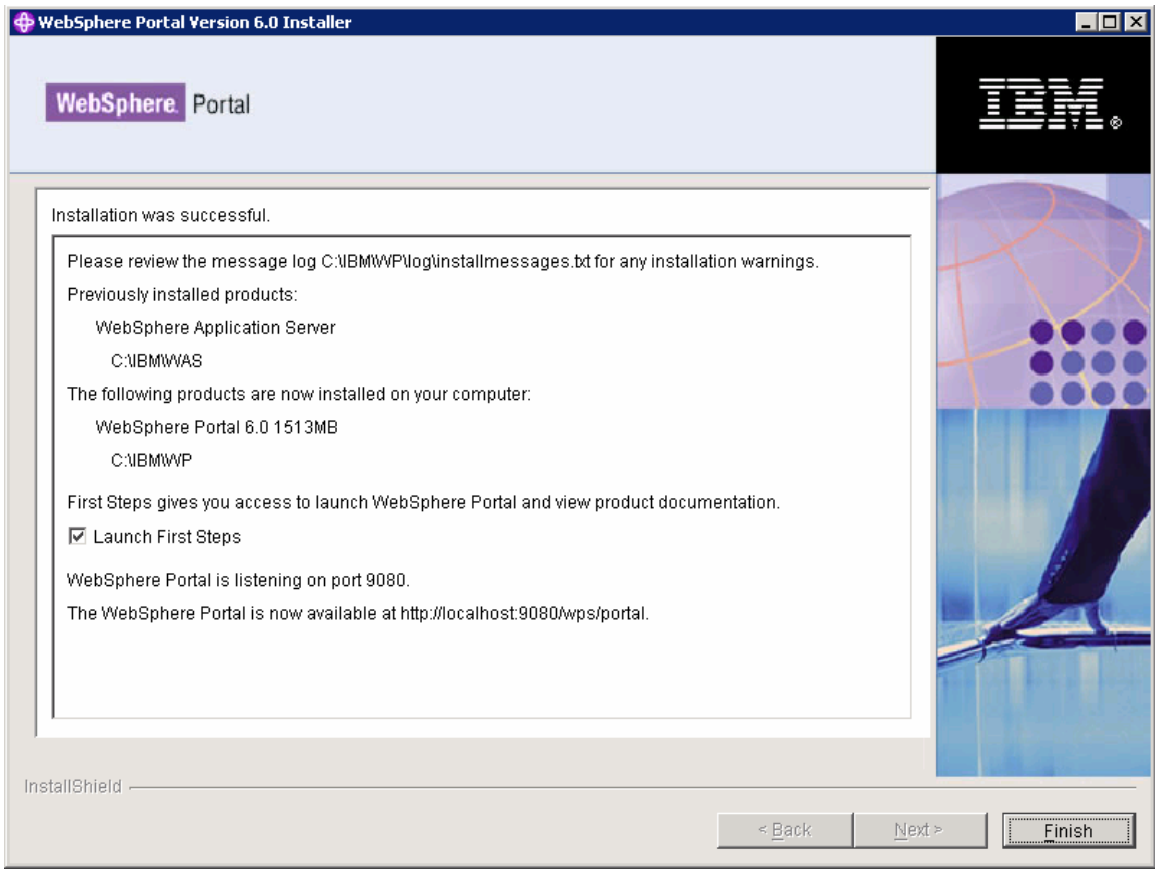
23. Decide whether you want WSAS and Portal to run as a service. In this guide we choose NOT to run either as a Windows service.



24. Review Summary panel and click Next to begin the install



25. Verify that portal install successfully and click Finish



Important: Do not attempt to start the WebSphere Portal to verify it's operational after installation. Because you installed as a secondary node, no enterprise applications or portlets will be installed onto the WebSphere Portal instance on the secondary node. This will make the Portal to not be operational until it is added to the cluster.

Add Node2 to the cluster definition

Important Note: Next we will run the cluster-setup task to add Node2 to the cluster. It is important to know that with Portal v6 the connect-database task has been integrated into the cluster-setup task. If the PrimaryNode property is defined as False, the cluster-setup task will perform the connect-database to point the secondary node to the existing cluster database. Therefore during this step we will be required to ensure that the database properties are correct in the wpconfig.properties files.

Also, the cluster-setup task will also automatically configure the DRS for the nodes in the cluster as well.

27. Make a backup of the original wpconfig_dbdomain.properties and wpconfig_dbtype.properties files on Node2 and then copy the wpconfig_dbdomain.properties and wpconfig_dbtype.properties from node1 to node2 to ensure the same database configuration.

28. Ensure the ClusterName and PrimaryNode and ServerName and PortalAdminPwd and WasPassword in the wpconfig.properties file have correct values.
ClusterName should be the name of the cluster created when running the clustersetup task on the Primary Node, Node1.

PrimaryNode should be set to “false” because this is a Secondary Node.
ServerName is REQUIRED to be changed from WebSphere_Portal. The clustersetup task is written to automatically remove the WebSphere_Portal server during the *action-remove-appserver-wps* task. This occurs at the end of the cluster-setup task and ONLY occurs when the PrimaryNode is set to “false”. This happens because of the fact in previous versions of Portal when you build a cluster you have 2 WebSphere_Portal server entries for the secondary nodes….like for example, WebSphere_Portal_2 (which was the true cluster member) and also a WebSphere_Portal entry (which was a “ghost” server) and most customers wanted the “ghost” server removed to avoid confusion.

Important Note: However, because of this requirement you will NOT be allowed to have the server name, WebSphere_Portal, across all the clustered nodes.
If the ServerName is NOT changed to something other than WebSphere_Portal, you will have an incorrect cluster configuration and to recover you will be required to reinstall Portal on Node2.

PortalAdminPwd should be set to the password defined at install which should be the same as the Portal password on Node1. WasPassword should be set to the WSAS password defined at install which should be the same as the WSAS password on Node1.

29. Install the client software, DB2 Connect, on the same machine as WebSphere Portal and WebSphere Application Server. Installing DB2 Connect enables the WebSphere Portal to use the required JDBC drivers. You must also ensure that the DB2 Connect

installation is the same name as the server profile name. Refer to the DB2information center for more information:
http://www.ibm.com/software/data/pubs/

30. The following pre-requested fix packs must be installed on DB2 client and server machines before database transfer.

a. For DB2 v8.1 Fix Pack 14 must be downloaded and installed.
b. For DB2 v9.1 Fix Pack 1 must be downloaded and installed.
c. Fix Pack can be downloaded from the link:
http://www-1.ibm.com/support/docview.wss?rs=71&uid=swg27007053

31. Again, in Portal v6 the connect-database task has been integrated into the clustersetup task. So, now because of this we must run the validate database tasks. If the passwords are defined in the wpconfig_dbdomain.properties file, the the –D options below are not required at the command line
.

WPSconfig.bat validate-database-driver

WPSconfig.bat validate-database-connection-wps - DDbPassword=*password*

WPSconfig.bat validate-database-connection-jcr
- DJcrDbPassword=*password*

WPSconfig.bat validate-database-connection-feedback -DFeedbackDbPassword=*password*

WPSconfig.bat validate-database-connection-likeminds
-DLikemindsDbPassword=*password*

WPSconfig.bat validate-database-connection-wmm
-DWmmDbPassword=*password*

32. Run <wp_root>/config/WPSconfig.bat *cluster-setup*.

33. Restart DMGR, and then the nodeagent and WebSphere_Portal_2 on Node2, and also restart the webserver to load the new configuration.

34. Verify the Portal install by accessing it thru a browser. By default Portal is installed onto port 9081:
http//<hostname>:9081/wps/portal

35. Also verify the new cluster member is available thru the webserver. The webserver plugin-cfg.xml may have been updated by the cluster-setup task if the webserver plugin is setup to be propagated via the WSAS config. Please see WSAS documentation for more information on this.

If the plugin-cfg.xml needs to be updated manually, please follow these instructions to regen the Web server plugin:

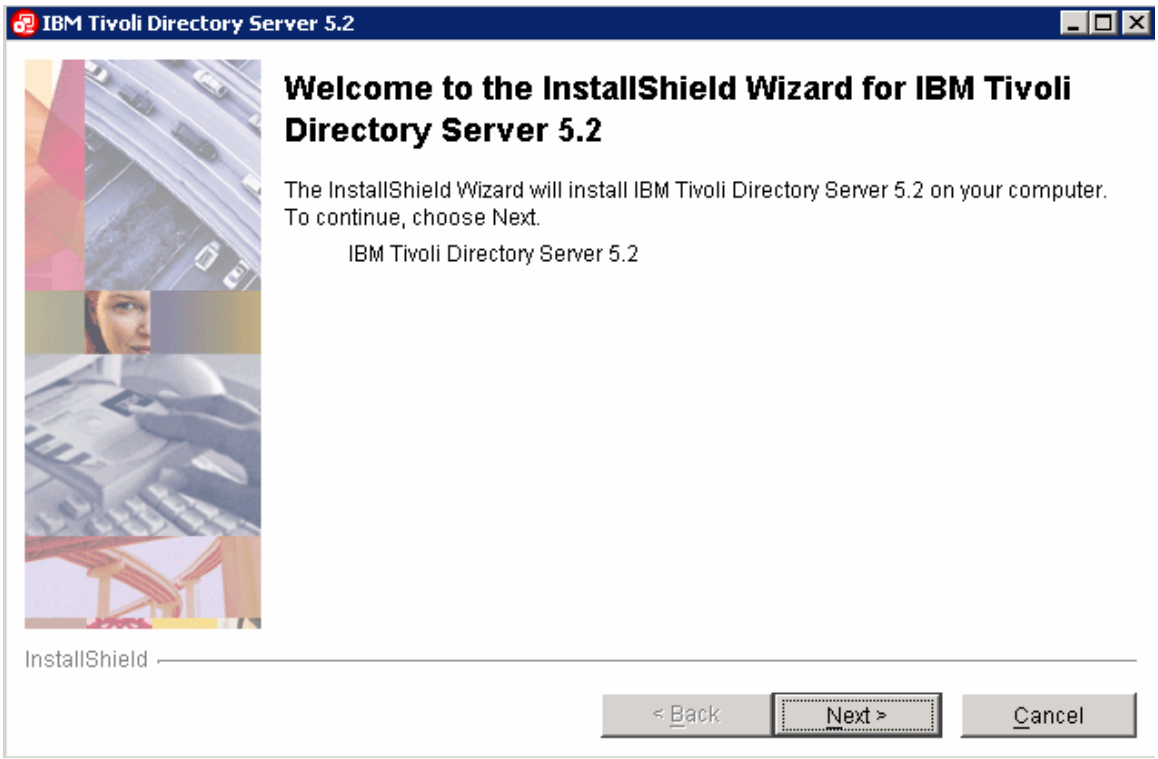
a. Regenerate the Web server plug-in using the deployment manager administrative console.
b. If you are using a remote Web server, copy the updated plug-in configuration file (plugin-cfg.xml) to the Web server's plug-in configuration directory.
c. Stop and start the Web server.
d. Restart all nodes in the cluster.

36. Edit the wpconfig.properties on Node2 to reflect the Web Server configuration. Change the following properties:
WpsHostName
WpsHostPort

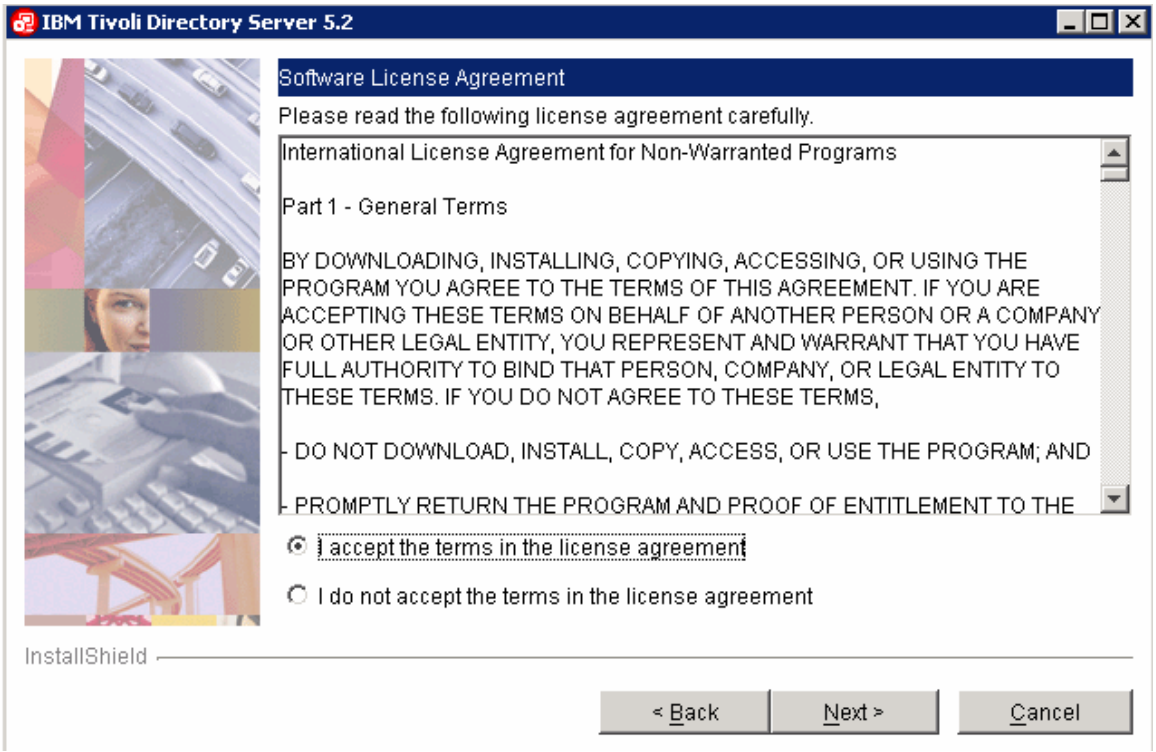
Configure Portal Node 1, Portal Node 2 and the DMGR for LDAP security with Realm Support

Installing an LDAP server is not part of the default IBM® WebSphere® Portal installation, so you must install, setup, and configure the IBM Tivoli® Directory Server separately. You can install the Tivoli Directory Server on the same machine as WebSphere Portal or you can install it on a remote machine. In this guide we will use Tivoli Directory Serve rv5.2 on the same machine where DB2 server is installed.

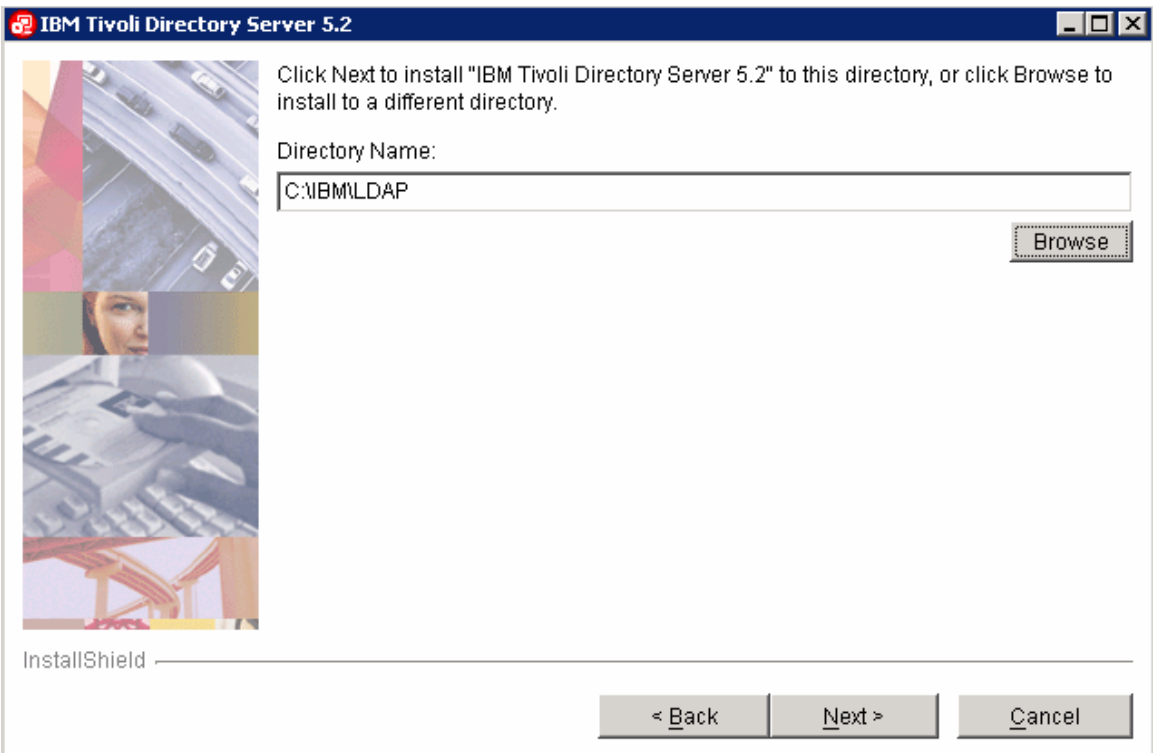
1. Install Tivoli Directory Server v5.2 by running the setup.exe file at: <tivoli_installation_root>\ismp\setup.exe



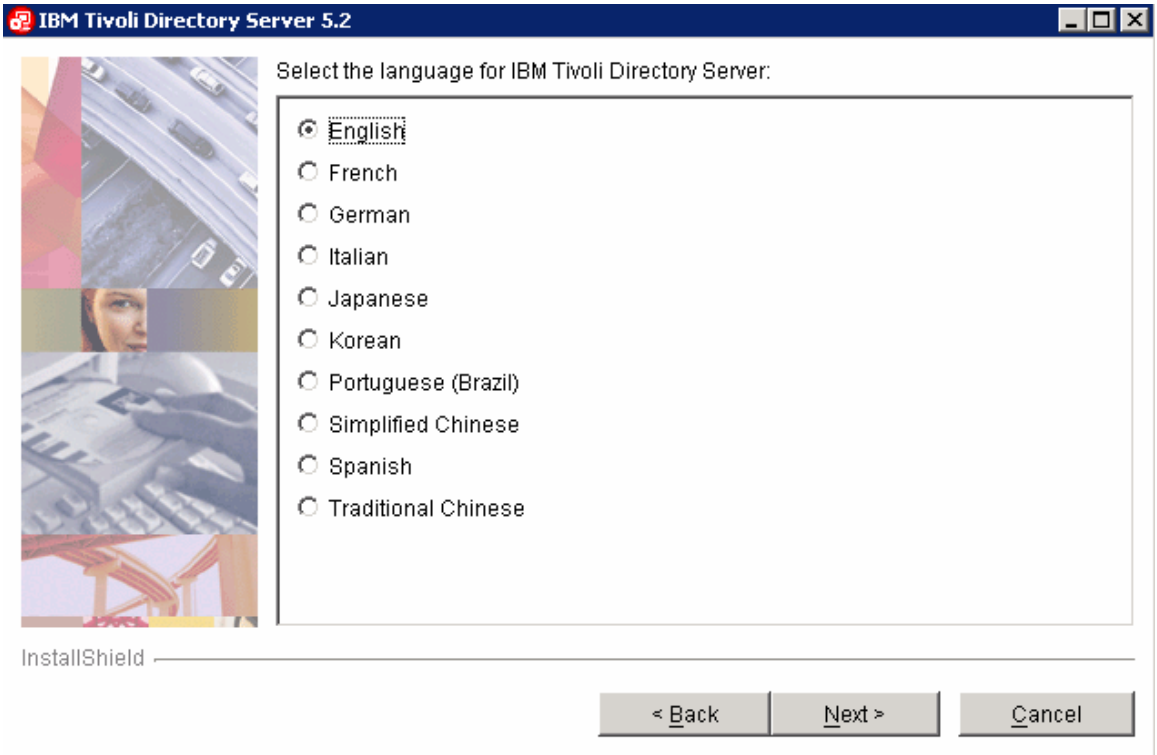
2. Accept the license agreement and click Next.



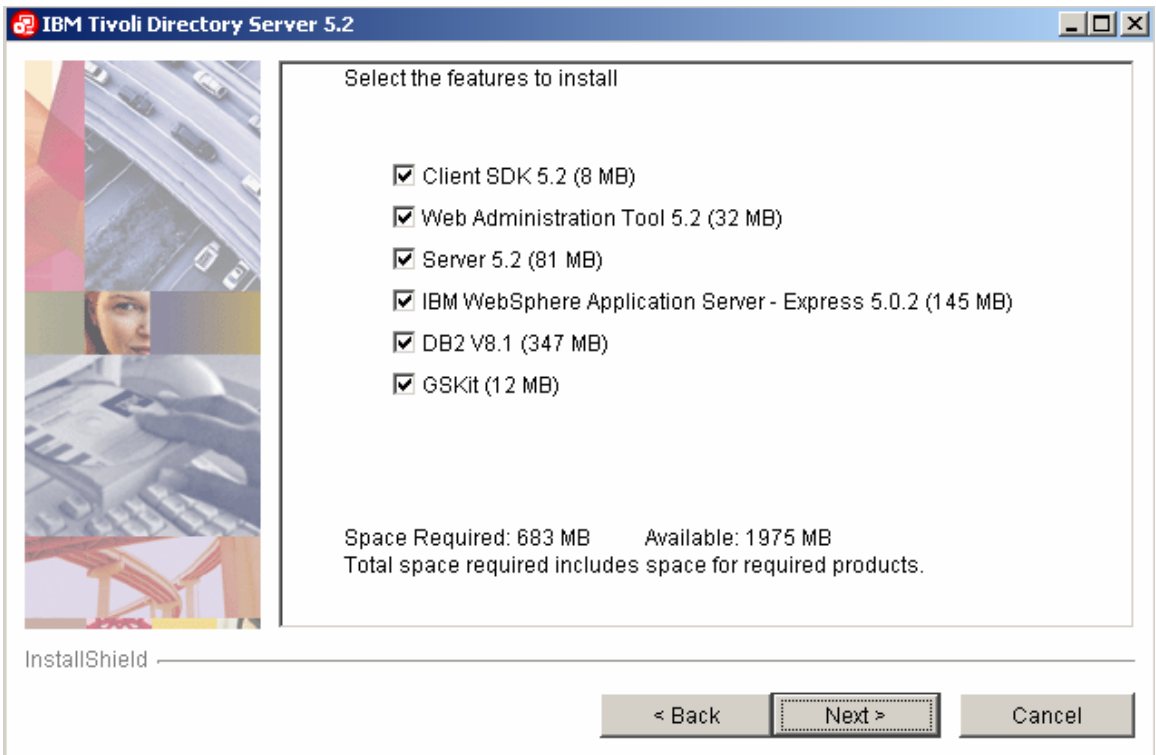
3. Specify the TDS installation location and click Next.



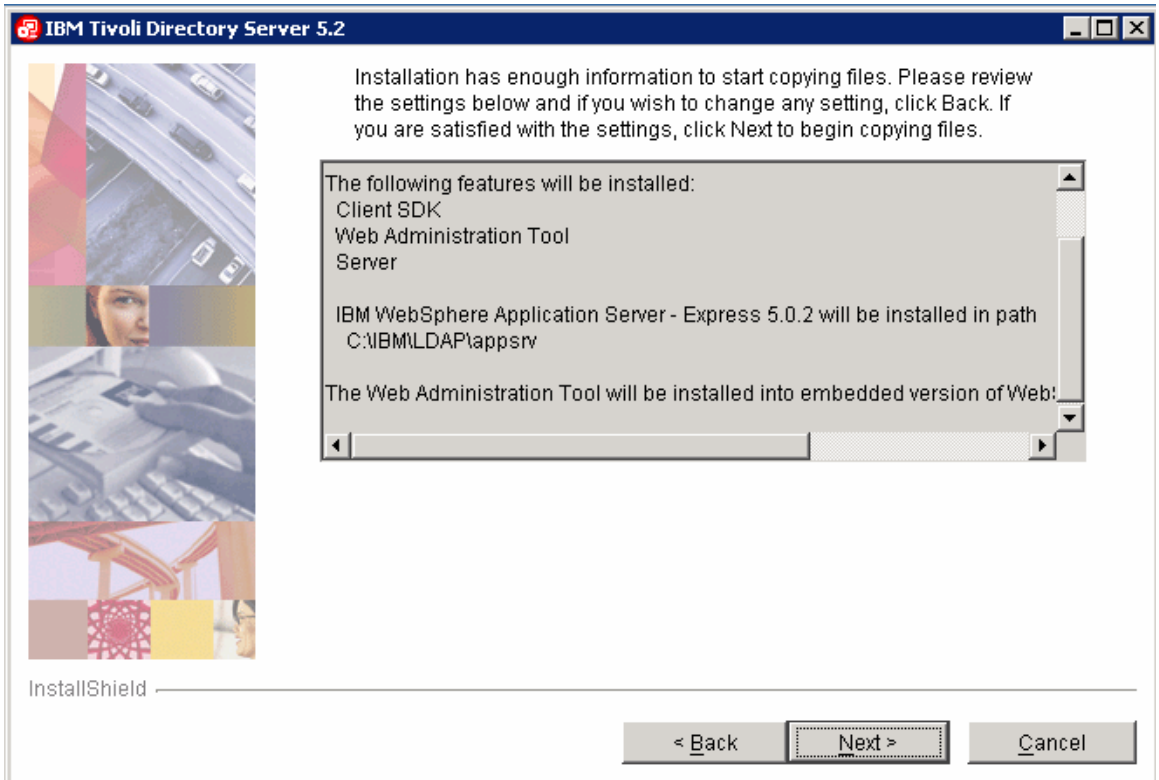
4. Select the language and click Next.



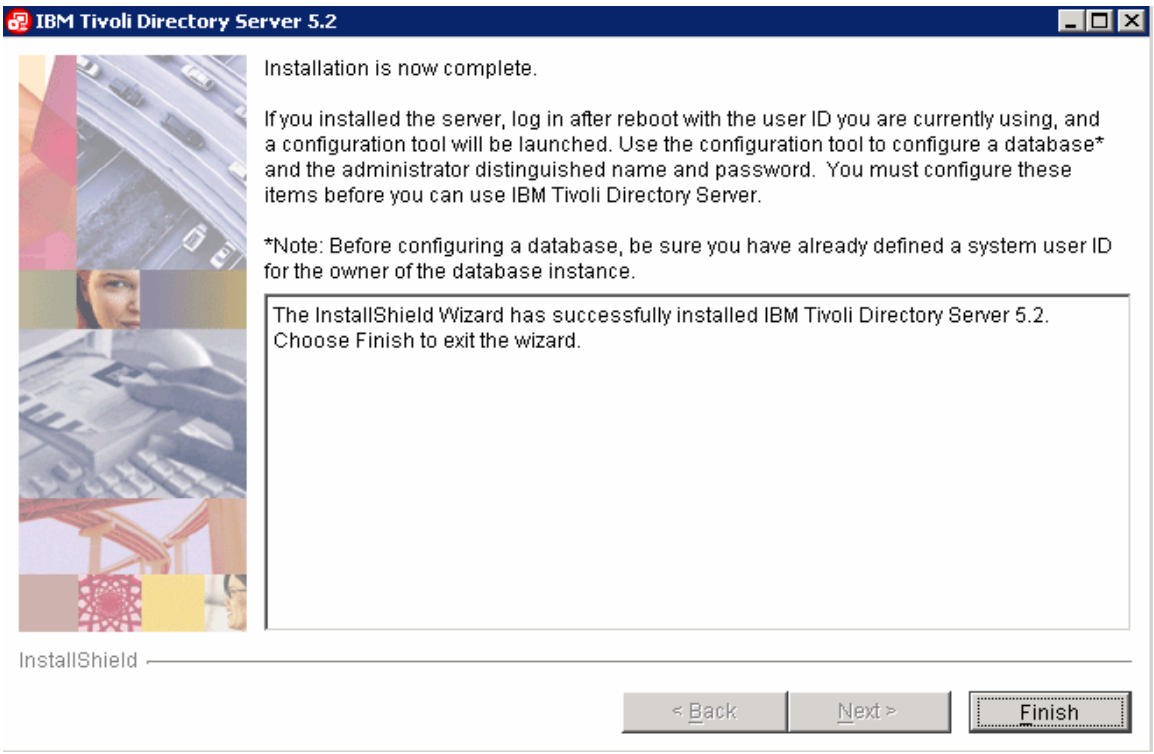
5. Select the features that should be installed on the server and click Next.



6. Click Next.



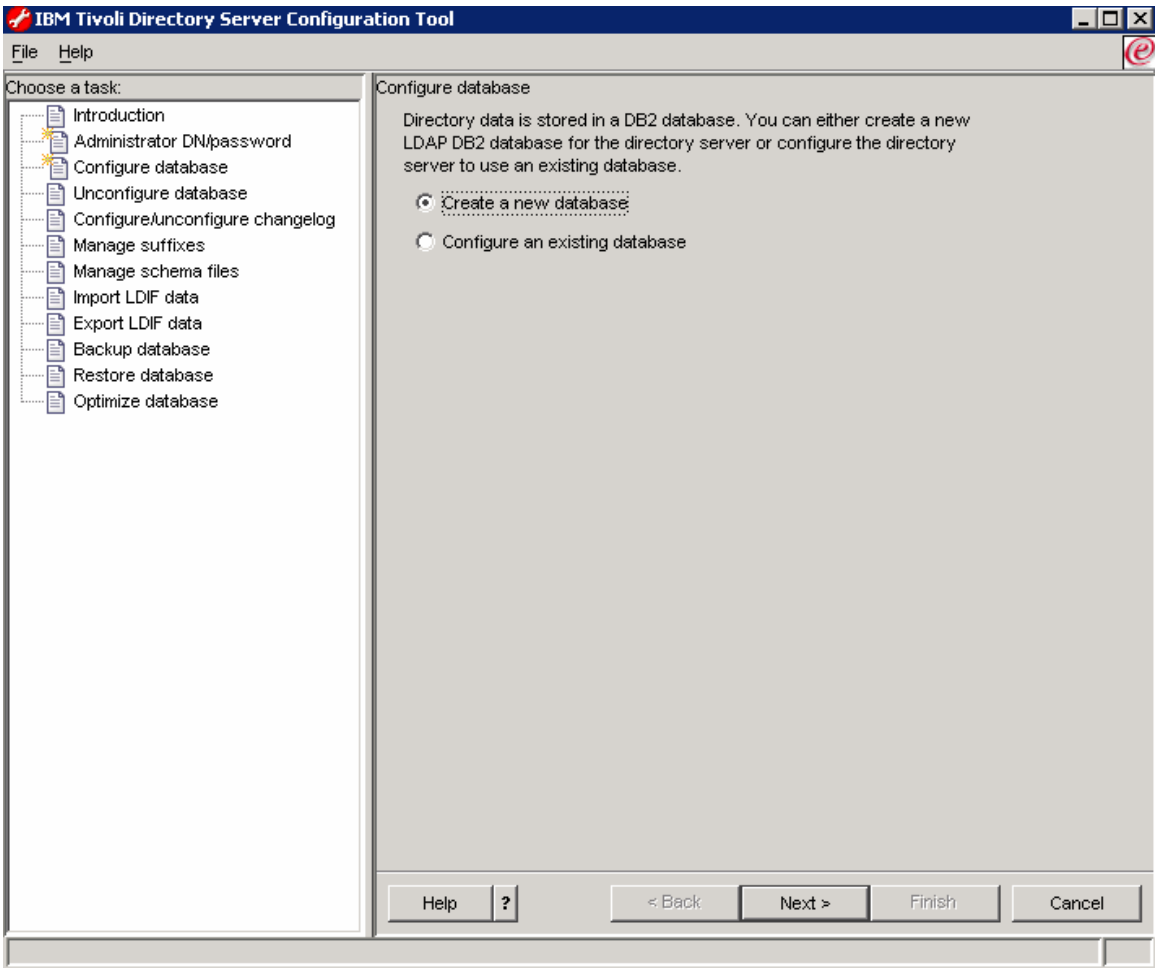
7. Click Finish.



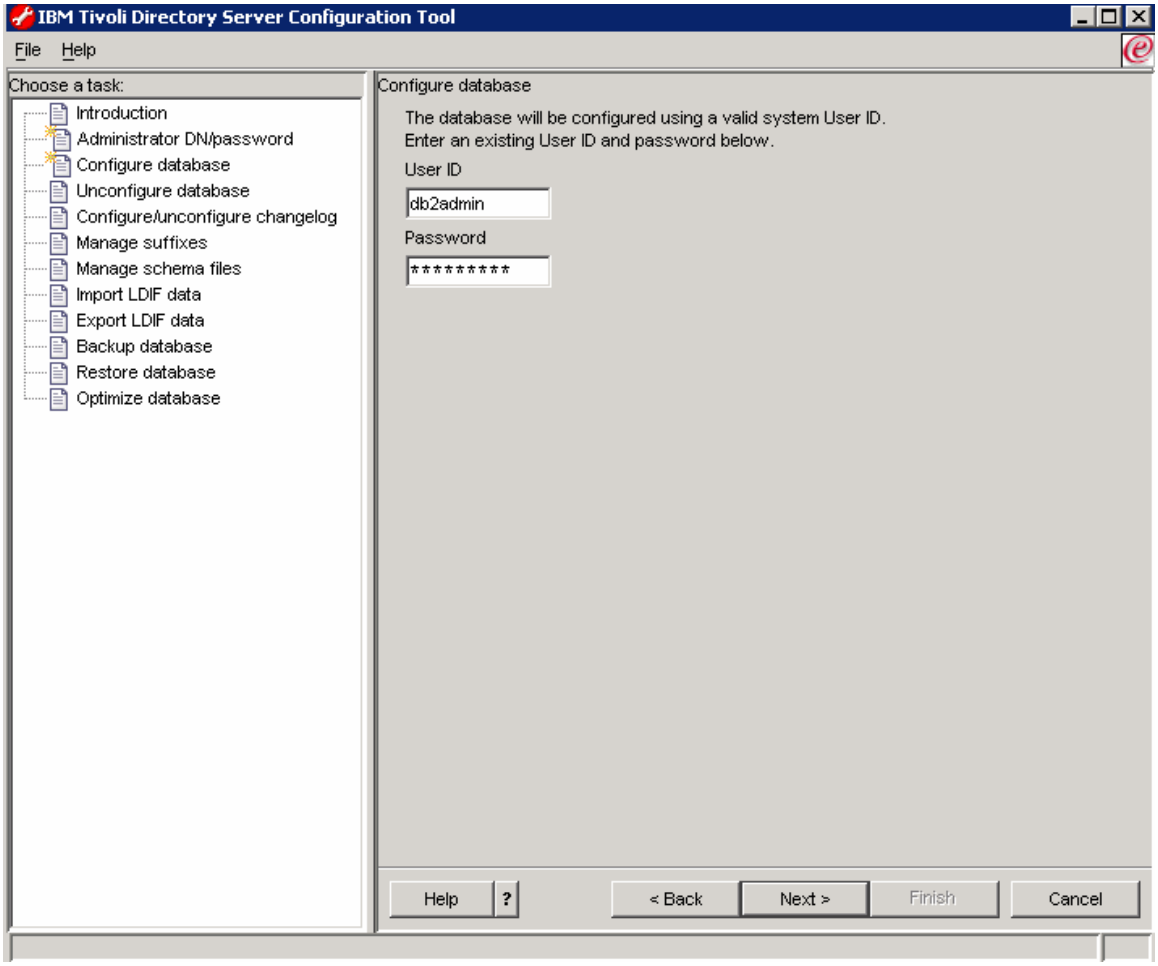
Configure the Tivoli Directory Server

1. Start the TDS administrative console by navigating to Start > All Programs > IBM Tivoli Directory Server v5.2 > Directory Configuration.

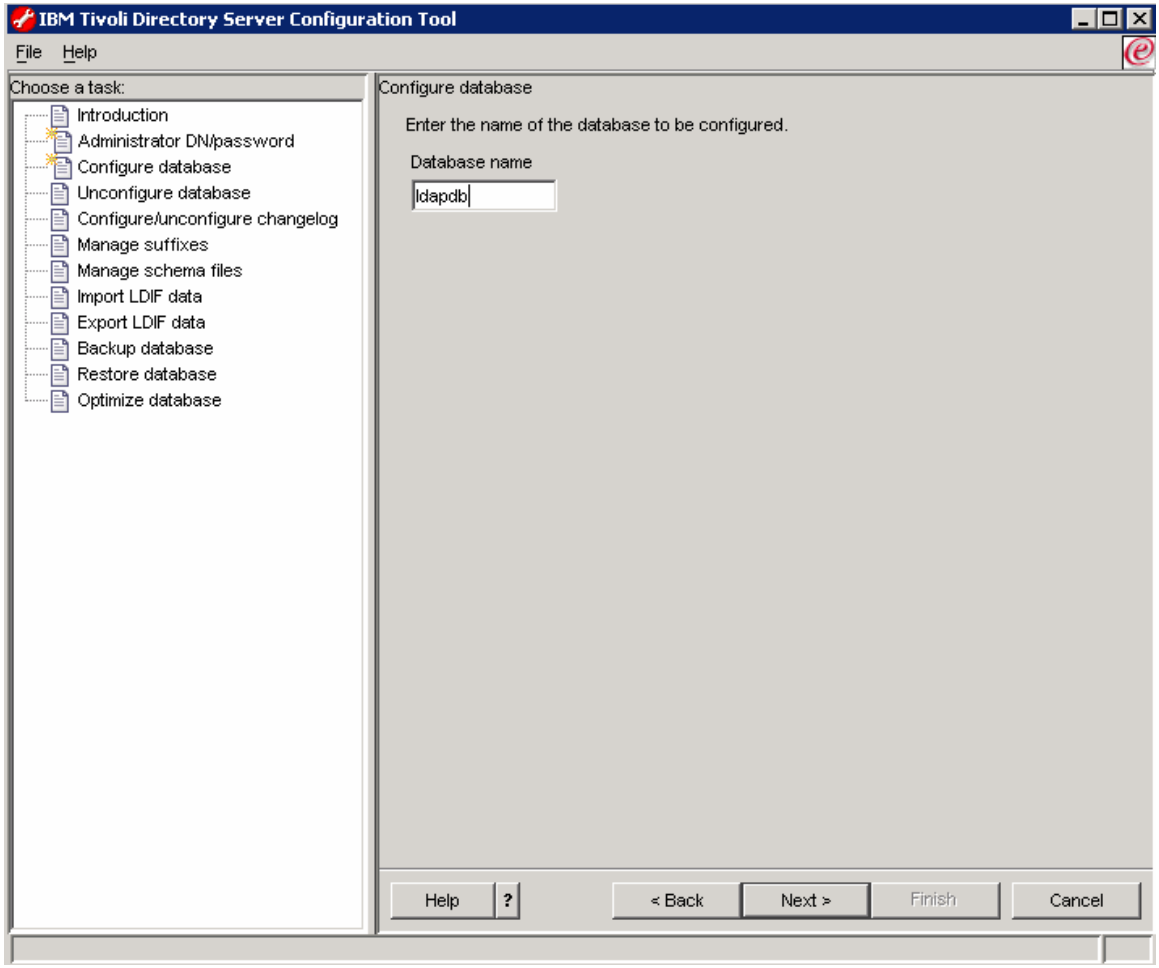
2. Navigate to Configure Database in the left hand side and select Create a New database. Then click Next.



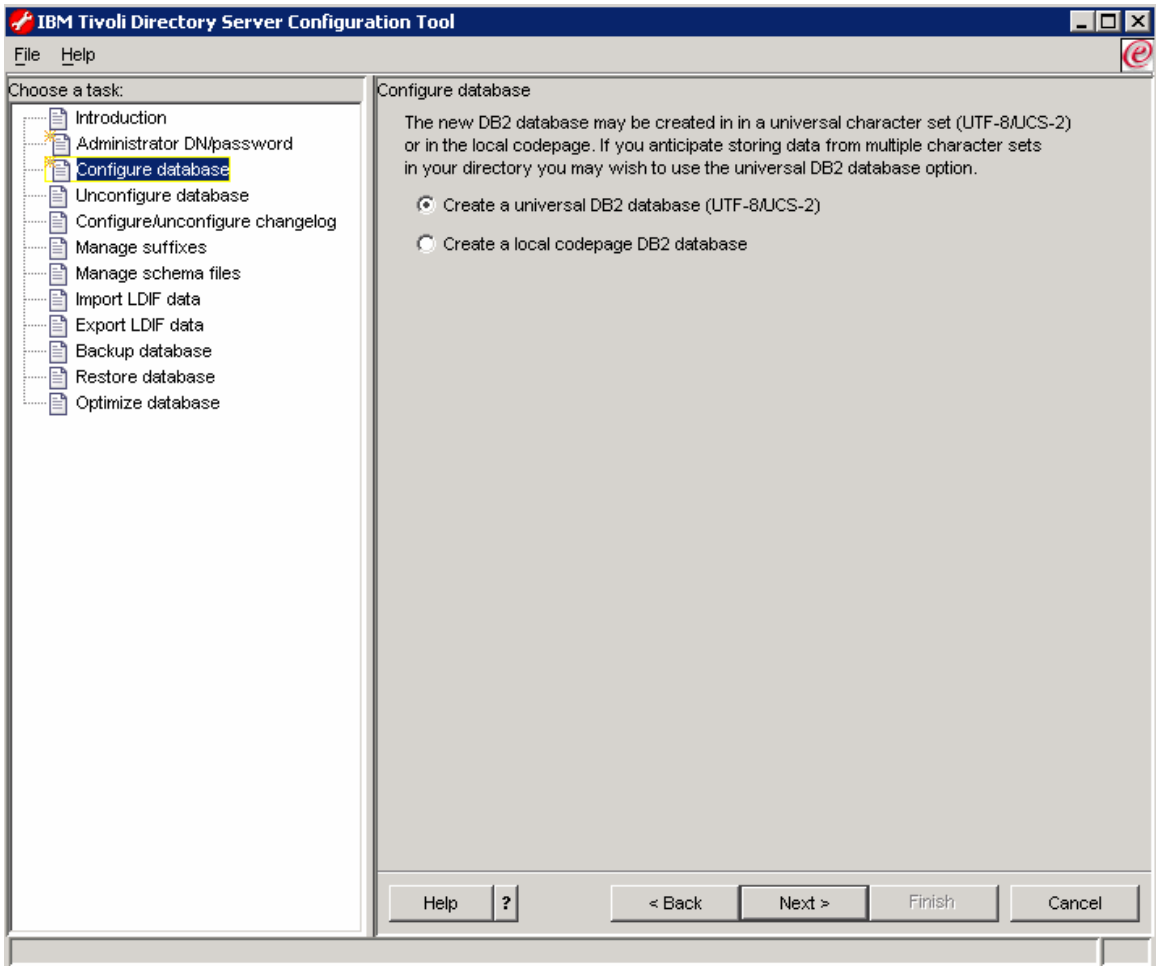
3. Provide DB2 user id and password.



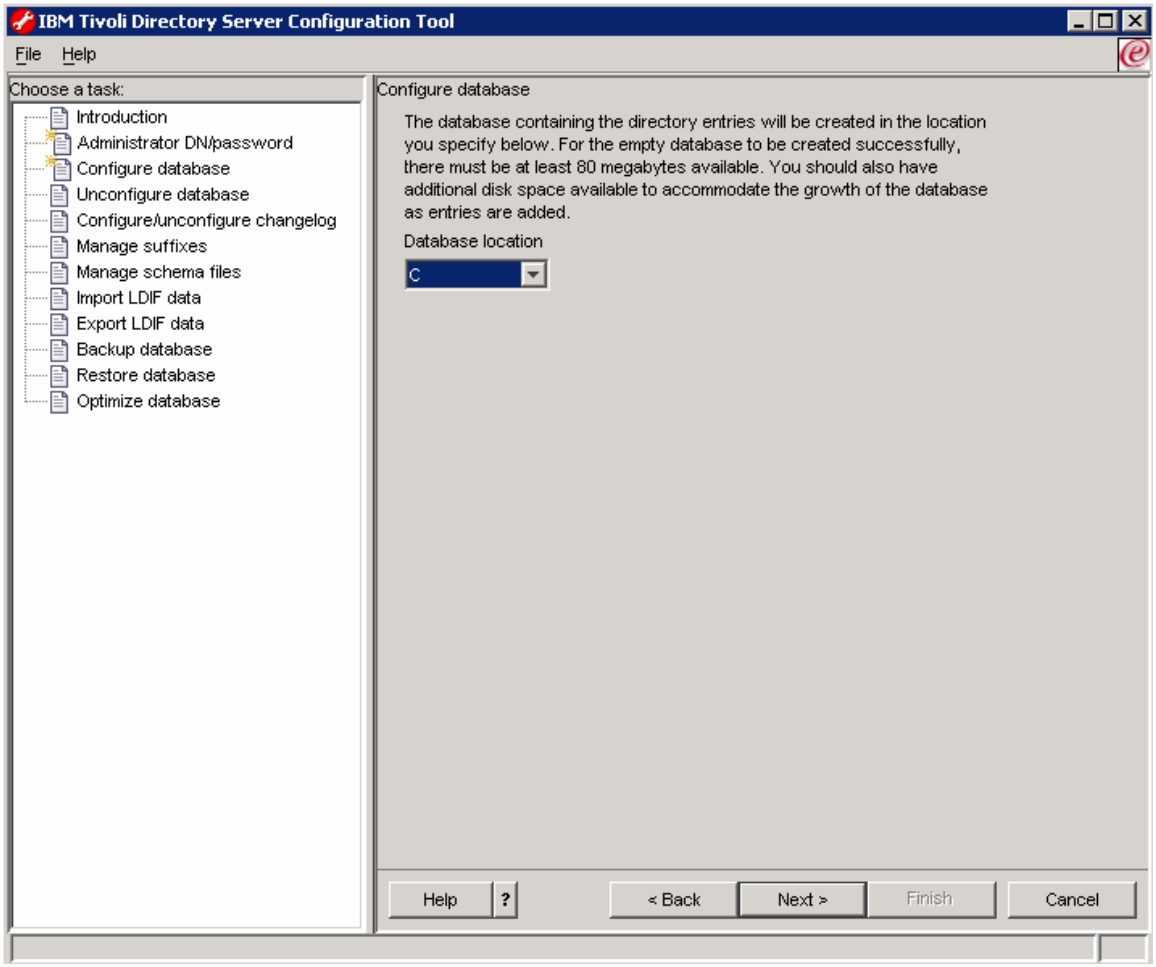
4. Enter database name and click Next button.



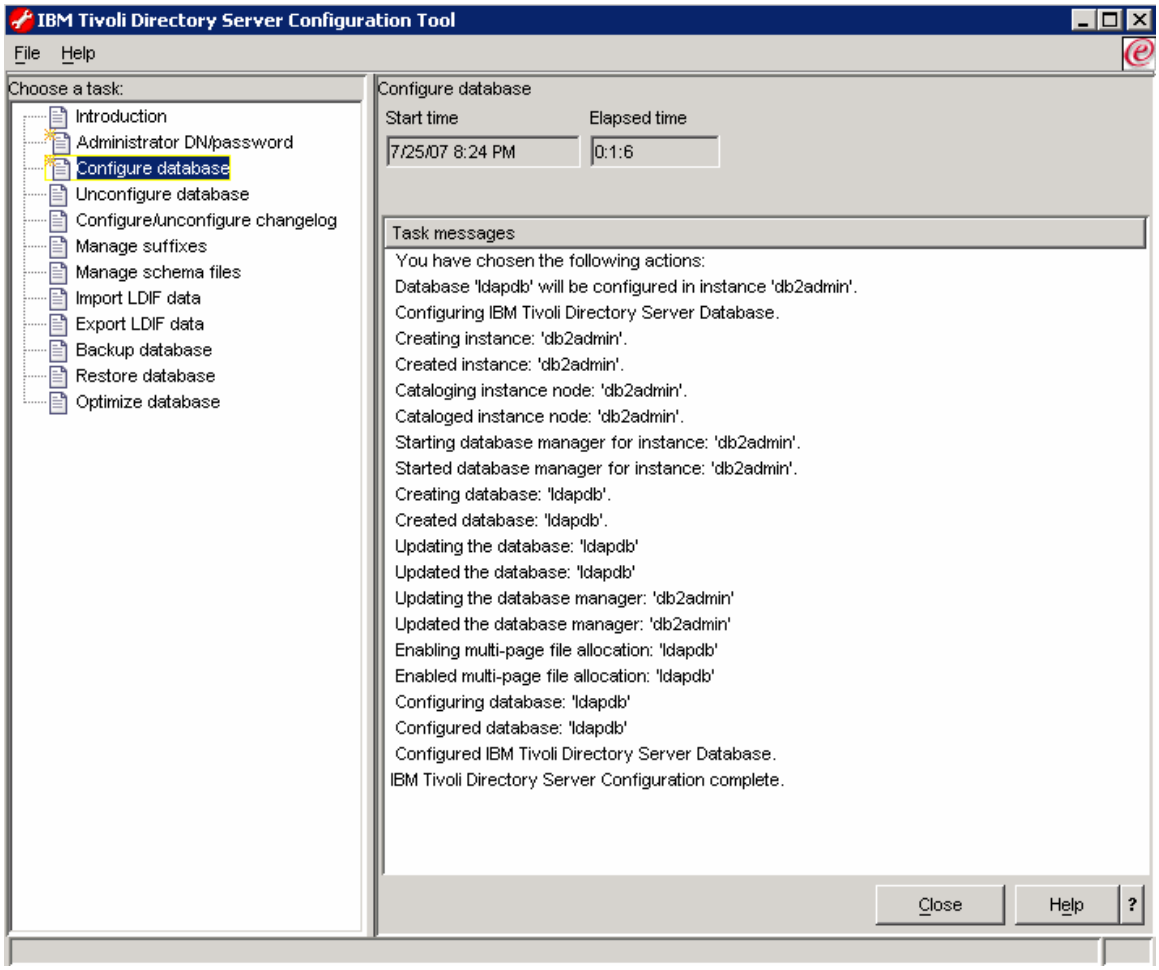
5. Select create a universal DB2 database (UTF-8/UCS-2) and click Next button.



6. Specify the drive where the database will be created.



7. Review the setting and click Close button.



Tivoli Directory server is now ready to be configured with portal server.

Creating required LDAP users and groups

Before you can configure IBM® WebSphere® Portal to work with the LDAP server, the LDAP user registry must have some minimal user and group information already populated. A minimum of one group that's **wpsadmins** or an equivalent (the group that is specified with the PortalAdminGroupId attribute in the wpconfig.properties file and one user that's specified with the PortalAdminId attribute in the wpsconfig.properties file is required for WebSphere Portal.

If content management functions are configured, it is recommended to also create the following groups in the LDAP:
wpsContentAdministrators
wpsDocReviewer
These groups should be created in the LDAP with the same authority as granted to the wpsadmins group.

1. In the Tivoli Directory Server console, click the **Server Administration** folder on the left-hand navigation. Click the **Manage Server Properties** folder underneath it, and then click on the **Suffixes** link on the right-hand side of the main page.

2. Type the name of the Base DN to be used as the suffix, for example, *dc=yourco,dc=com*. Click **Add** to add the suffix.

3. When you are finished adding the suffix, click **OK** to save your changes.

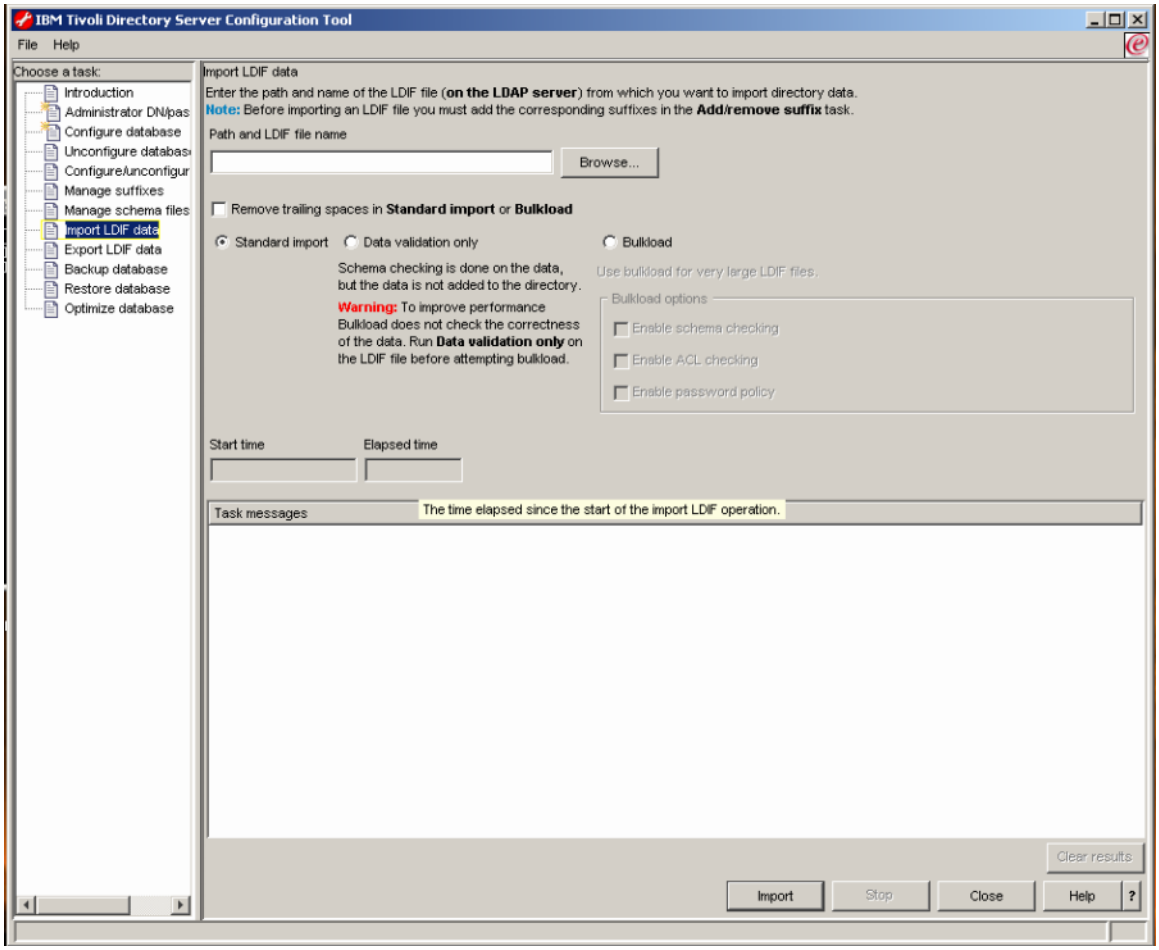
4. Stop and start the LDAP server.

5. If you choose to use the LDIF file, locate PortalUsers.ldif in the root directory on the CD setup of portal server.
<cd_root>/Setup_cd/

Notes: The PortalUsers.ldif file is provided as a working example and needs to be adapted appropriately to work with your LDAP server.

6. Replace all occurrences of *dc=yourco,dc=com* with the suffix that you are using. Also, replace any prefixes and suffixes that are unique to your LDAP server. You can specify user names other than wpsadmin and wpsbind if you want. For security reasons, you should specify non-trivial passwords for these administrator accounts because it is easier to specify them now than to change them after installation. Save your changes.

7. Start the TDS administrative console by navigating to Start > All Programs > IBM Tivoli Directory Server v5.2 > Directory Configuration and select Import LDIF data. Import the edited PortalUsers.ldif file and click Import button.



Note: Importing the PortalUsers.ldif file could overwrite existing user data.

8. Stop and restart the LDAP server.

9. After the portal installation, if you did not specify non-trivial passwords for the administrator IDs in the LDIF file, it is recommended that you change the passwords for these user IDs.

Disabling WebSphere Application Server global security

Please ensure that the Portal server has been stopped on each node. Also, because security comes enabled by default with Portal v6, we are now required to run the disablesecurity task BEFORE enabling any type of additional Portal security.**Also, the disable-security and the enable-security-wmmur-ldap tasks MUST be ran on the Primary node.**

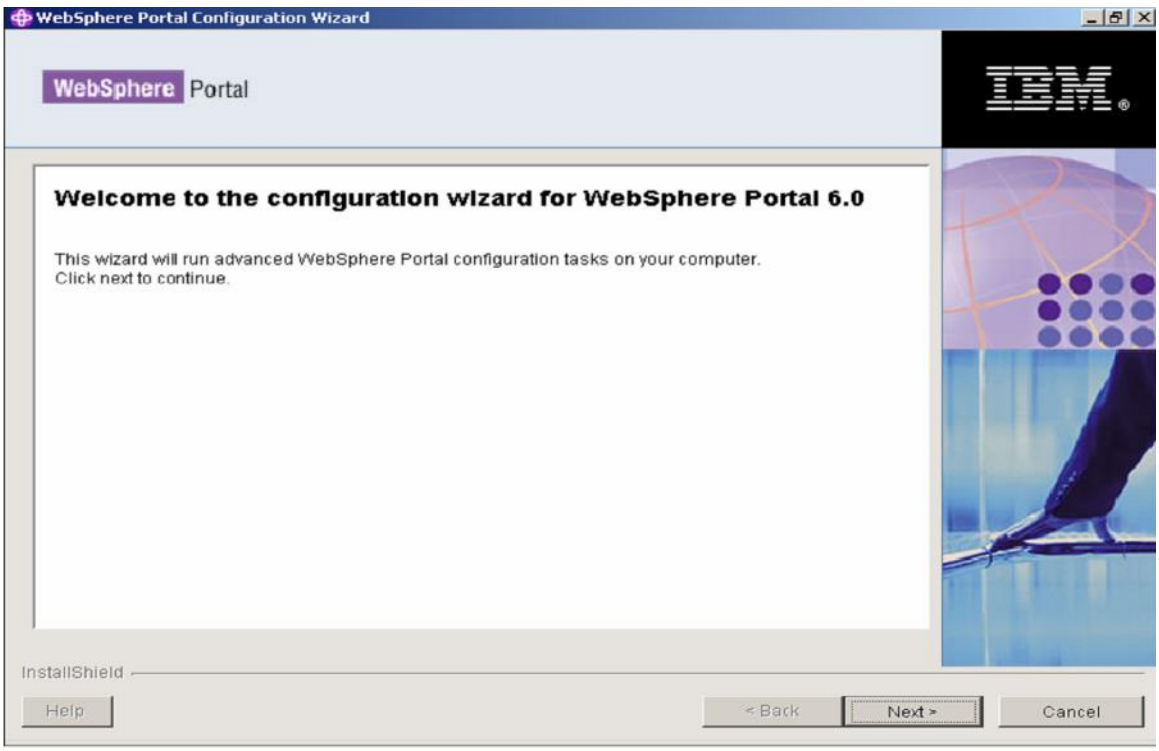
1. Make a copy of the original helper file. Edit the /<wp_root>/config/helpers/security_disable.properties helper file.

Change the following properties to match your current security configuration:
wmm.DbPassword
WasPassword

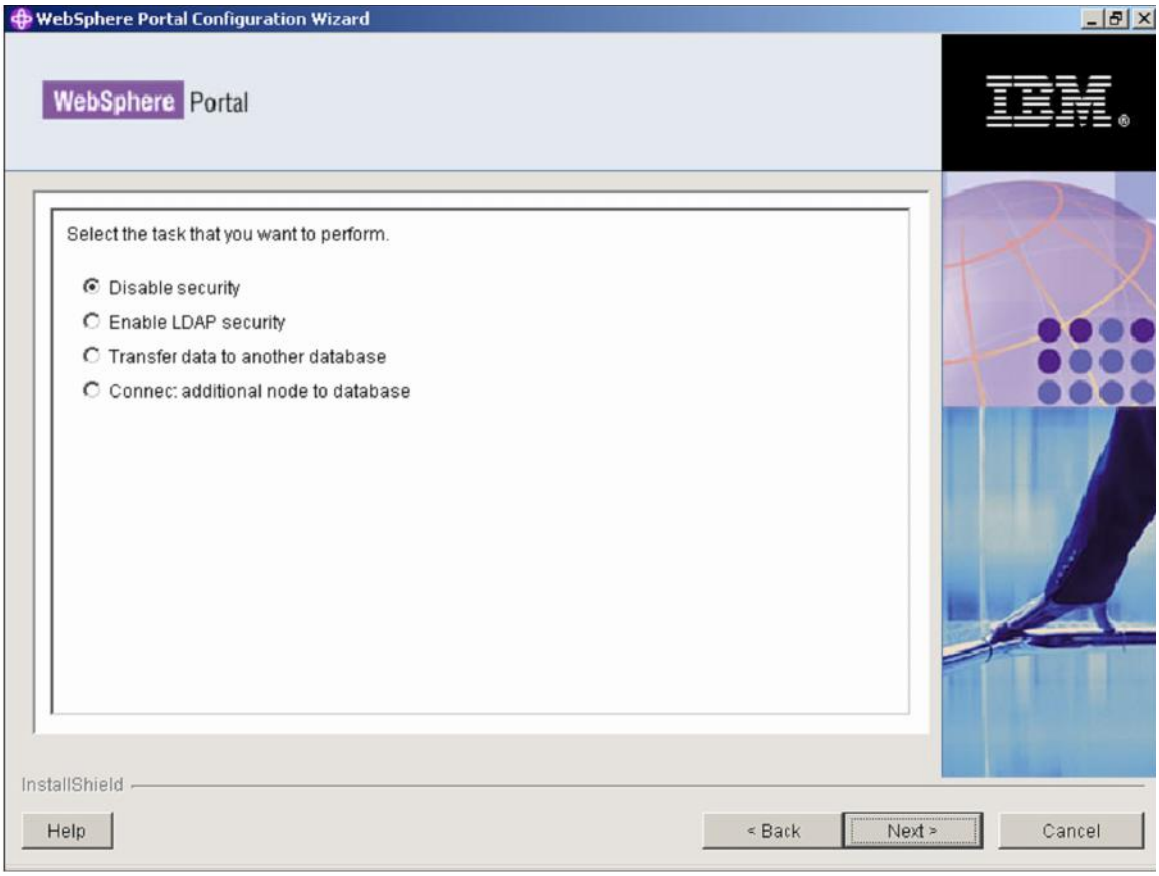
Change the following properties to match what you desire your Portal id/pwd to be after disabling security:
PortalAdminId
PortalAdminPwd
PortalAdminGroupId

2. Run the config wizard to disable security. Invoke the config wizard by running the following script, <wp_root>/config/wizard/configwizard.bat. Again, please make sure the task is ran on the Primary node.

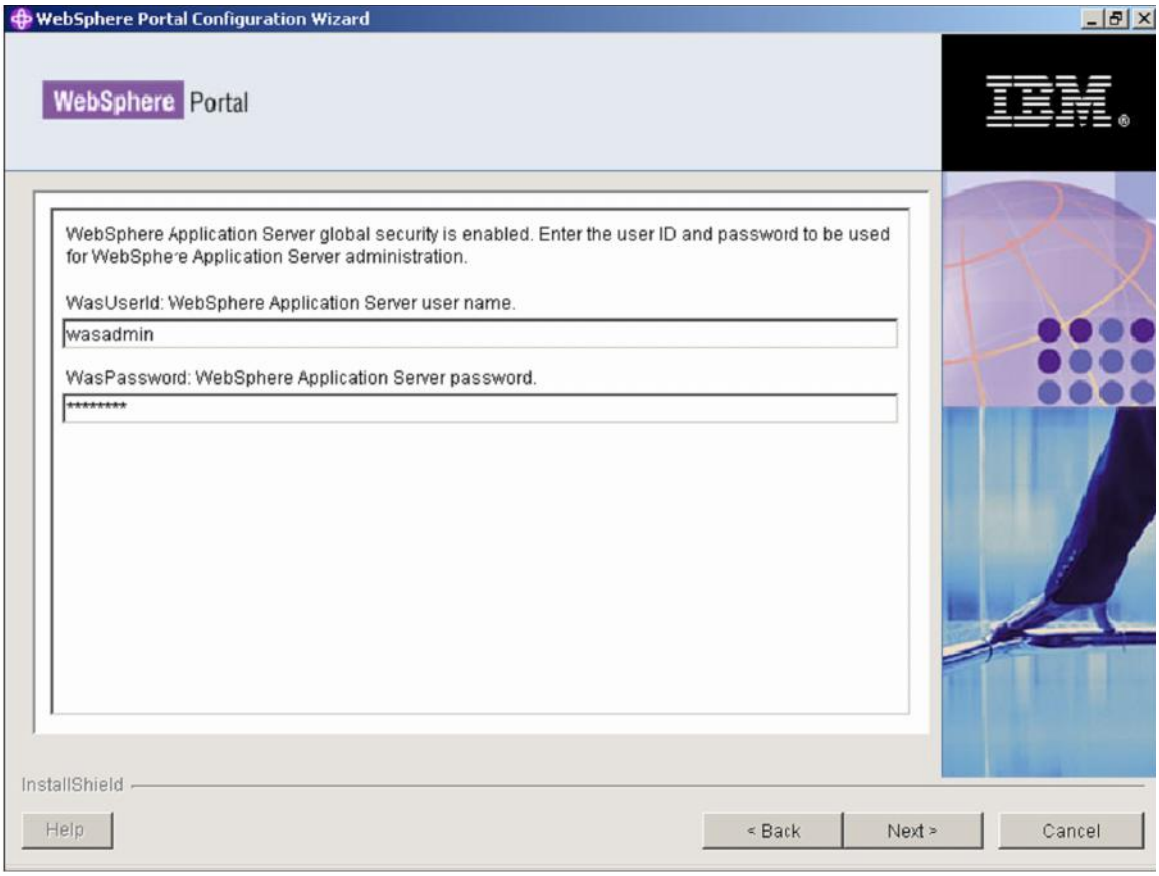
3. Click next on the Welcome Panel



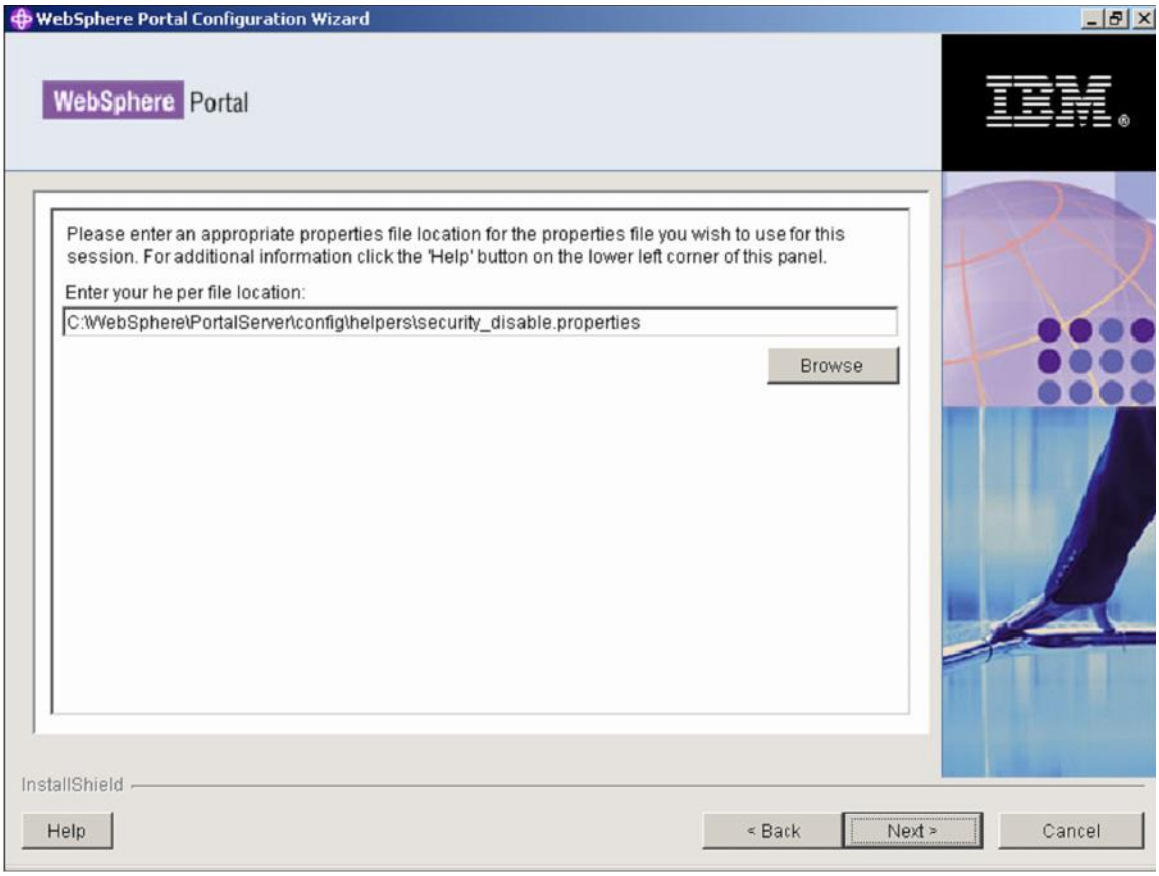
4. Choose Disable security and click next



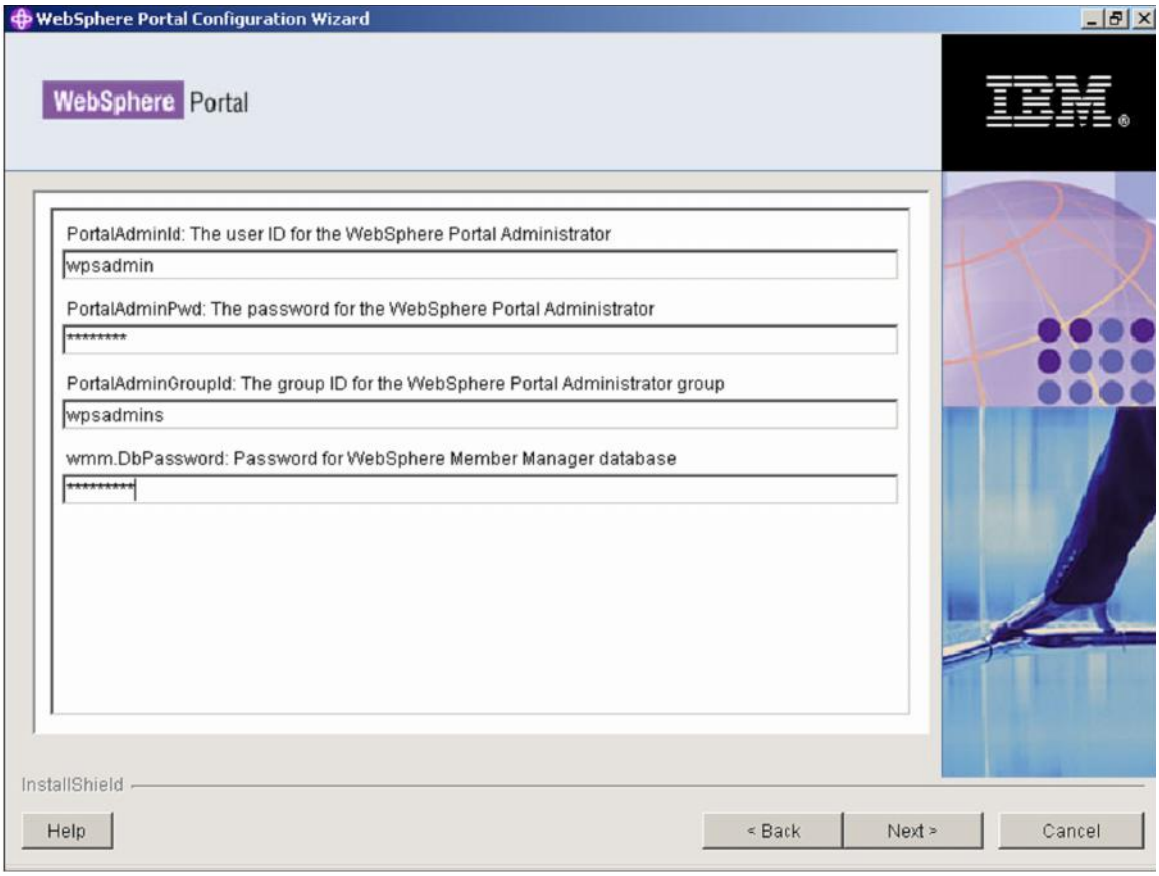
5. Enter the WSAS Admin password and click next



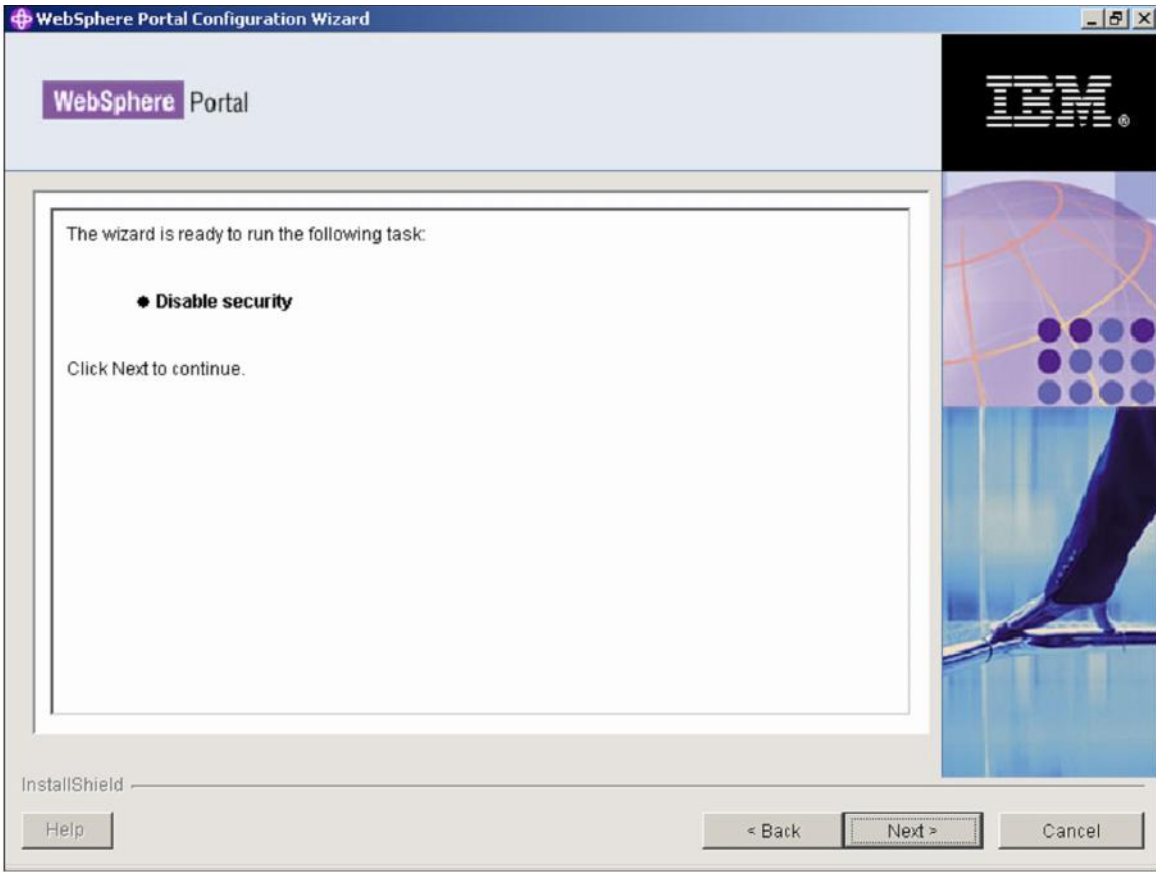
6. Select the proper location of the helper file and click next



7. Enter the WMM database ID password and click next



8. Review the summary panel and click next to start the task



Verify that task run successfully, if you got any errors, then correct the errors and rerun the task again.

Configure Portal Node 1, Portal Node 2 and the DMGR for LDAP security with Realm Support

Refer to the following InfoCenter link for the details of LDAP/security configuration
http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/topic/com.ibm.wp.ent.doc/wpf/intr_ldap.html
Note: In this guide we will enable security using the enable-security-wmmur-ldap task. In previous versions of the cluster guide we have always used enable-security-ldap. This guide recommends the use of the enable-security-wmmur-ldap task because overall Portal now recommends using this task to enable security so you can have the flexibility to configure realm support and virtual portals in the future. If you have no plans for these features running this task will NOT cause a problem. Or you can certainly choose to implement other security types at this step by running other tasks, such as enablesecurity-ldap, etc.

After the disable-security task finishes, please ensure all Portal servers are stopped and ensure the nodeagents and the DMGR are running before running the enablesecurity-wmmur-ldap task

1. Make a copy of the original security helper file. Edit the security helper file to change all the LDAP values to match your LDAP configuration.

```
################################################################################
# WebSphere Application Server Properties - BEGIN
################################################################################
# WasUserid: The user ID for WebSphere Application Server security authentication
WasUserid=uid=admin,cn=users,dc=rc,dc=com

# WasPassword: The password for WebSphere Application Server security authentication
(LDAP and CUR)
WasPassword=cyber2003

################################################################################
# WebSphere Application Server Properties - END
################################################################################

################################################################################
# Database Properties - BEGIN
################################################################################
# Connection information for wmm db will be acquired from
# wpconfig_dbdomain.properties and wpconfig_dbtype.properties
# DbPassword: The database administrator password
wmm.DbPassword=cyber2003
################################################################################
# Database Properties - END
################################################################################
```

```
################################################################################
# Portal Config Properties - BEGIN
################################################################################
# PortalAdminId: The user ID for the WebSphere Portal Administrator
PortalAdminId=uid=admin,cn=users,dc=rc,dc=com

# PortalAdminPwd: The password for the WebSphere Portal Administrator
PortalAdminPwd=cyber2003

# PortalAdminGroupId: The group ID for the WebSphere Portal Administrator group
PortalAdminGroupId=cn=wpsadmins,cn=groups,dc=rc,dc=com

################################################################################
# Portal Config Properties - END
################################################################################

#####################################################################
#
# WebSphere Portal Security Configuration - BEGIN
#
#####################################################################

#####################################################################
# WebSphere Portal Security LTPA and SSO configuration
#####################################################################

# LTPAPassword: Specifies the password to encrypt and decrypt the LTPA keys.
LTPAPassword=cyber2003

# LTPATimeout: Specifies the time period in minutes at which an LTPA token will
expire.
LTPATimeout=120

# SSORequiresSSL: Specifies that Single Sign-On function is enabled
# only when requests are over HTTPS Secure Socket Layer (SSL) connections.
SSORequiresSSL=false

# SSODomainName: Specifies the domain name (ibm.com, for example) for all Single
Sign-on hosts.
SSODomainName=<SSODomainName>

#####################################################################
# General Global Security Settings
#####################################################################

# Description: The values in this section should only be adapted by advanced users
```

```
# useDomainQualifiedUserNames: Specifies the user names to qualify with the security domain within which they reside.
useDomainQualifiedUserNames=false

# cacheTimeout: Specifies the timeout value in seconds for security cache.
cacheTimeout=600

# issuePermissionWarning: Specifies that when the Issue permission warning is enabled, during application deployment
# and application start, the security run time emits a warning if applications are granted any custom permissions.
issuePermissionWarning=true

# activeProtocol: Specifies the active authentication protocol for RMI/IIOP requests when security is enabled.
activeProtocol=BOTH

# activeAuthMechanism: Specifies the active authentication mechanism, when security is enabled.
activeAuthMechanism=LTPA

#####################################################################
# LDAP Properties Configuration - BEGIN
#####################################################################
# LookAside: To configure LDAP with an additional LookAside Database
# true  - LDAP + Lookaside database
# false - only LDAP
LookAside=false

# LDAPHostName: The LDAP server hostname
LDAPHostName=ishtiaque

# LDAPPort: The LDAP server port number
# For example, 389 for non-SSL or 636 for SSL
LDAPPort=389

# LDAPAdminUId: The LDAP administrator ID
LDAPAdminUId=cn=admin

# LDAPAdminPwd: The LDAP administrator password
LDAPAdminPwd=cyber2003

# LDAPServerType: The type of LDAP server to be used for WebSphere Portal
LDAPServerType=IBM_DIRECTORY_SERVER

#LDAPBindID: The user ID for LDAP Bind authentication
```

LDAPBindID=uid=admin,cn=users,dc=rc,dc=com

#LDAPBindPassword: The password for LDAP Bind authentication
LDAPBindPassword=cyber2003

##
LDAP Properties Configuration - END
##

##
Advanced LDAP Configuration - BEGIN
##

# LDAPSuffix: The LDAP suffix appropriate for your LDAP server
LDAPSuffix=dc=rc,dc=com

# LdapUserPrefix: The LDAP user prefix appropriate for your LDAP server
LdapUserPrefix=uid

# LDAPUserSuffix: The LDAP user suffix appropriate for your LDAP server
LDAPUserSuffix=cn=users

# LdapGroupPrefix: The LDAP group prefix appropriate for your LDAP server
LdapGroupPrefix=cn

# LDAPGroupSuffix: The LDAP group suffix appropriate for your LDAP server
LDAPGroupSuffix=cn=groups

# LDAPUserObjectClass: The LDAP user object class appropriate for your LDAP server
LDAPUserObjectClass=inetOrgPerson

# LDAPGroupObjectClass: The LDAP group object class appropriate for your LDAP server
LDAPGroupObjectClass=groupOfUniqueNames

# LDAPGroupMember: The LDAP group member attribute name appropriate for your LDAP server
LDAPGroupMember=uniqueMember
# LDAPUserFilter: The LDAP user filter appropriate for your LDAP server (to work with default values in WMM)
LDAPUserFilter=(&(uid=%v)(objectclass=inetOrgPerson))

# LDAPGroupFilter: The LDAP group filter appropriate for your LDAP server (to work with default values in WMM)
LDAPGroupFilter=(&(cn=%v)(objectclass=groupOfUniqueNames))

```
# LDAPGroupMinimumAttributes: This attribute is loaded for group search
(performance issues)
LDAPGroupMinimumAttributes=

# LDAPUserBaseAttributes: These attributes are loaded for user login (performance
issues)
LDAPUserBaseAttributes=givenName,sn,preferredLanguage

# LDAPUserMinimumAttributes: These attributes are loaded for user search
(performance issues)
LDAPUserMinimumAttributes=

#LDAPsearchTimeout: Specifies the timeout value in seconds for an LDAP server to
respond before aborting a request.
LDAPsearchTimeout=120

#LDAPreuseConnection: Should set to true by default to reuse the LDAP connection.
# { false | true }
LDAPreuseConnection=true

#LDAPIgnoreCase: Specifies that a case insensitive authorization check is performed.
# { false | true }
LDAPIgnoreCase=true

#LDAPsslEnabled: Specifies whether secure socket communications is enabled to the
LDAP server.
# { false | true }
# Set to true if configuring LDAP over SSL
LDAPsslEnabled=false

#################################################################
# Advanced LDAP Configuration - END
#################################################################

#################################################################################
# LDAP Properties - END
#################################################################################
#################################################################################
# PDM LDAP Properties - BEGIN
#################################################################################

# WpsContentAdministrators: The group ID for the WebSphere Content Administrator
group
# See LDAP examples below:
# IBM Directory Server: { cn=wpsContentAdministrators,cn=groups,dc=yourco,dc=com
}
```

WpsContentAdministrators=cn=wpsContentAdministrators,cn=groups,dc=rc,dc=com

# WpsContentAdministratorsShort: The WebSphere Content Administrators group ID
WpsContentAdministratorsShort=wpsContentAdministrators

# WpsDocReviewer: The group ID for the WebSphere Document Reviewer group
# See LDAP examples below:
# IBM Directory Server: { cn=wpsDocReviewer,cn=groups,dc=yourco,dc=com }
WpsDocReviewer=cn=wpsDocReviewer,cn=groups,dc=rc,dc=com

# WpsDocReviewerShort: The WebSphere Document Reviewer group ID
WpsDocReviewerShort=wpsDocReviewer

###
PDM LDAP Properties - END
###
###
WCM LDAP Properties - BEGIN
###

# WcmAdminGroupId: The group ID for the WCM Administrator group
# See LDAP examples below:
# IBM Directory Server: { cn=wcmadmins,cn=groups,dc=yourco,dc=com }
WcmAdminGroupId=cn=wcmadmins,cn=groups,dc=rc,dc=com

# WcmAdminGroupIdShort: The WCM admin group ID
WcmAdminGroupIdShort=wcmadmins
###
WCM LDAP Properties - END
###
###
#
WebSphere Portal Security Configuration - END
###

2. Import the contents of the helper file into the wpconfig.properties file by issuing this command:
<wp_root>/config/WPSconfig -DparentProperties="<full_path_to_helper_file>" -DSaveParentProperties=true

3. Open the wpconfig.properties file and make sure the WpsHostName and WpsHostPort are correct

4. Run the following task to validate the LDAP values:
WPSconfig.bat validate-wmmur-ldap

5. Run the following task on the primary node ONLY to configure the LDAP security settings for both WSAS/WP nodes and the DMGR. This will enable security on the entire cluster:
WPSconfig.bat enable-security-wmmur-ldap

6. Because we enabled security using the enable-security-wmmur-ldap task that enables realm support, we are required to manually edit the wmmWASAdmin.xml file on the DMGR. If this file is not edited with the shortname you will not be able to run the stopServer.bat or the serverStatus.bat on the nodes using the shortname as the username….rather you will be required to use the full LDAP DN.

The current <dmgr_profile_root>/config/wmm/wmmWASAdmin.xml should look something like this:
<?xml version="1.0" encoding="UTF-8"?>
<wmmWASAdmins>
<admin logonId="uid=wasadmin,ou=People,ou=portal6,ou=dancy,o=portin"
logonPassword="anvu7zPZ7jbrZLa4h89Tfg=="
uniqueUserId="uid=wasadmin,ou=People,ou=portal6,ou=dancy,o=portin"/>
</wmmWASAdmins>

Please add another line between the <wmmWASAdmins> tag that includes the shortname. Since both IDs will have the same password you can simply copy the current <admin logonId> tag entry and modify it like below:
<?xml version="1.0" encoding="UTF-8"?>
<wmmWASAdmins>
<adminlogonId="uid=wasadmin,ou=People,ou=portal6,ou=dancy,o=porti
n" logonPassword="anvu7zPZ7jbrZLa4h89Tfg=="
uniqueUserId="uid=wasadmin,ou=People,ou=portal6,ou=dancy,o=portin
"/>
<adminlogonId=**"wasadmin"** logonPassword="anvu7zPZ7jbrZLa4h89Tfg=="
uniqueUserId="uid=wasadmin,ou=People,ou=portal6,ou=dancy,o=portin
"/>
</wmmWASAdmins>

7. Please perform a full synchronization to ensure all the security settings are pushed from the DMGR to the nodes. Restart the DMGR and the nodeagents on each node. The nodeagents will have to be stopped by providing the full LDAP DN on the command line. After they restart the new config settings should take affect and then they should be able to be stopped using the shortname.

8. Update the <wp_root>/config/wpconfig.properties file on each secondary node in the cluster with the same LDAP user registry information you used to configure the primary node.

9.
Update the wpconfig.properties by moving the LDAP helper file from Node1 to Node2 and running the following command:
<wp_root>/config/WPSconfig -DparentProperties="<full_path_to_helper_file>" -

DSaveParentProperties=true
Complete the security configuration by running the enable-jcr-security configuration task on each secondary node.

Run the following command from the <wp_root>/config directory:
WPSconfig.bat enable-jcr-security -
DPortalAdminId=*portal_admin_id*

Where *portal_admin_id* is the fully qualified distinguished name (DN) of the portal administrator (for example,
uid=wpsadmin,cn=users,dc=example,dc=com).
Restart the Portal server cluster member on each secondary node.

10. Verify the new security settings by rendering the DMGR AdminConsole and Portal from a browser.

Perform the final tasks

1. Save your changes and resynchronize the nodes:
- In the administrative console for the deployment manager, click **System Administration>Save Changes to Master Repository** and save your administrative configuration.
- Select **System Administration > Nodes**, select the cluster nodes from the list, and click **Full Resynchronize**.

2. Regenerate the Web server plug-in.
Select **Servers > Web servers** in the deployment manager administrative console, select the Web server entry and click the **Generate Plug-in** button
- Move the plugin to the Web server which is under
<plugin_root>/config/webserver1

3. Restart the DMGR, Web server and Portal cluster

4. Verify the WpsHostName and WpsHostPort properties in the wpconfig.properties reflect the Web server values on all cluster nodes

5. Verify the Portal cluster can be accessed through the Web server

Conclusion

In this article, you saw how to build a fully-functional WebSphere Portal cluster using an external database and a LDAP for security. You also saw how to configure a Web server to allow for load balancing.

About the author

Ishtiaque Ali Daudpota is an IBM Certified Solution Developer, WebSphere Portal v5.1 working at Royal Cyber, Inc. as Sr. Software Engineer have about one and half year professional working experience on portlet development and portal administration for off-shore clients.

Resources

WebSphere Application Server Network Deployment Information Center
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/welcome_nd.html
WebSphere Portal InfoCenter
http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/index.jsp
A step-by-step guide to configuring a WebSphere Portal v6.0.0.0 cluster using WebSphere Application Server v6.0.2.9 and WebSphere Process Server v6.0.1.1
http://www-1.ibm.com/support/docview.wss?uid=swg21246630
A step-by-step guide to configuring a WebSphere Portal V5.1.x cluster using WebSphere Application Server V5.1.1.x
http://www-128.ibm.com/developerworks/websphere/library/techarticles/0509_dancy/0509_dancy.html

Trademarks

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.
Produced in the United States of America
08-10