A Step-By-Step Guide to Configuring a WebSphere Portal v6.1.0.0 Cluster using WebSphere Application Server v6.1.0.15

Hunter Tweed
WebSphere Portal Level 2 support Technical Lead
IBM Raleigh Lab

July, 2008

This guide describes a comprehensive procedure for installing, configuring, and building an IBM® WebSphere® Portal V6.1.0.0 cluster using:

- IBM WebSphere Application Server 6.1.0.15 – 32-bit
- Windows® 2003 Server
- DB2 v9.1.4 Server
- IBM Tivoli Directory Server v6.0
- IBM HTTP Server 6.1

Although this guide is specifically written for 32-bit Portal v6.1.0.0 and WSAS v6.1.0.15, the same approach will apply to Portal v6.1.0.1 and v6.1.0.2 versions and any WSAS v6.1.0.x version higher than fixpack 15, 32 or 64-bit, as well.

Table of Contents

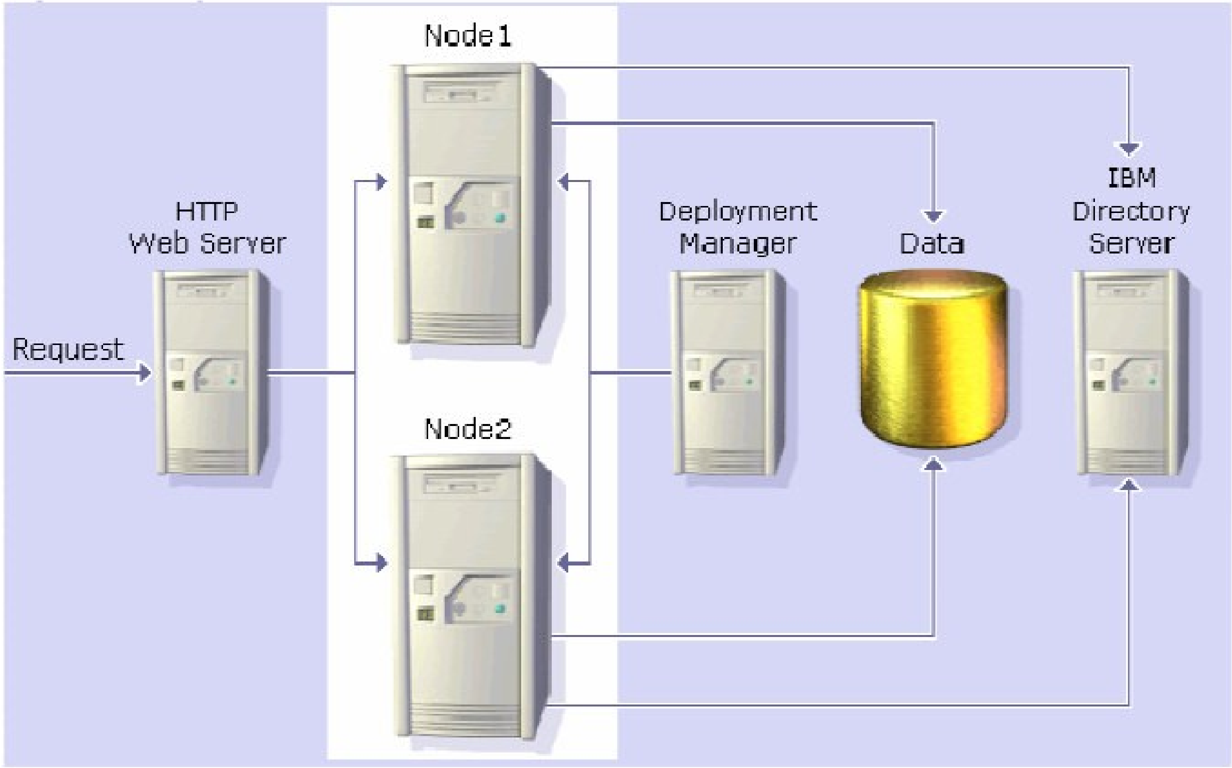
Introduction

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 version 6.1. 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 32-bit Portal v6.1.0.0 and WSAS v6.1.0.15, the same approach will apply to any Portal v6.1.x version and any WSAS v6.1.0.x version, 32 or 64-bit, as well.

NOTE: This guide does **NOT** apply to Portal v6.1.0.3/6.1.5 or higher. The cluster steps changed slightly with this version.

Figure 1 – Target Portal Cluster



In the instructions for configuring Portal with the database and LDAP, screens shots show valid examples. Use values which are appropriate for your database and LDAP.

Before you begin

This guide does **NOT** cover the following:

- Installing DB2
- Installing IBM Tivoli Directory Server
- Configuring the cluster with Web Content Management
- Configuring the cluster with WebSphere Process Server
- Configuring a dynamic cluster using WebSphere Application Server XD
- Creating multiple clusters in a single cell

For more information on these and other topics, please visit the IBM WebSphere Portal v6.1 Information Center:

http://publib.boulder.ibm.com/infocenter/wpdoc/v6r1m0/index.jsp

To perform the tasks described in this document, 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.

The following references to WebSphere Portal and WebSphere Application Server file paths will be used throughout the guide:

<AppServer root> - The root path of the AppServer directory, for example C:\IBM\WebSphere\AppServer

<PortalServer root> - The root path of the PortalServer directory, for example C:\IBM\WebSphere\PortalServer

<wp_profile> - The root path of the wp_profile directory, for example C:\IBM\WebSphere\wp_profile

<dmgr_profile> - The root path of the dmgr profile directory, for example C:\IBM\WebSphere\AppServer\profiles\Dmgr01

<plugin root> - The root path of the WebSphere Plugin directory, for example C:\IBM\WebSphere\Plugins

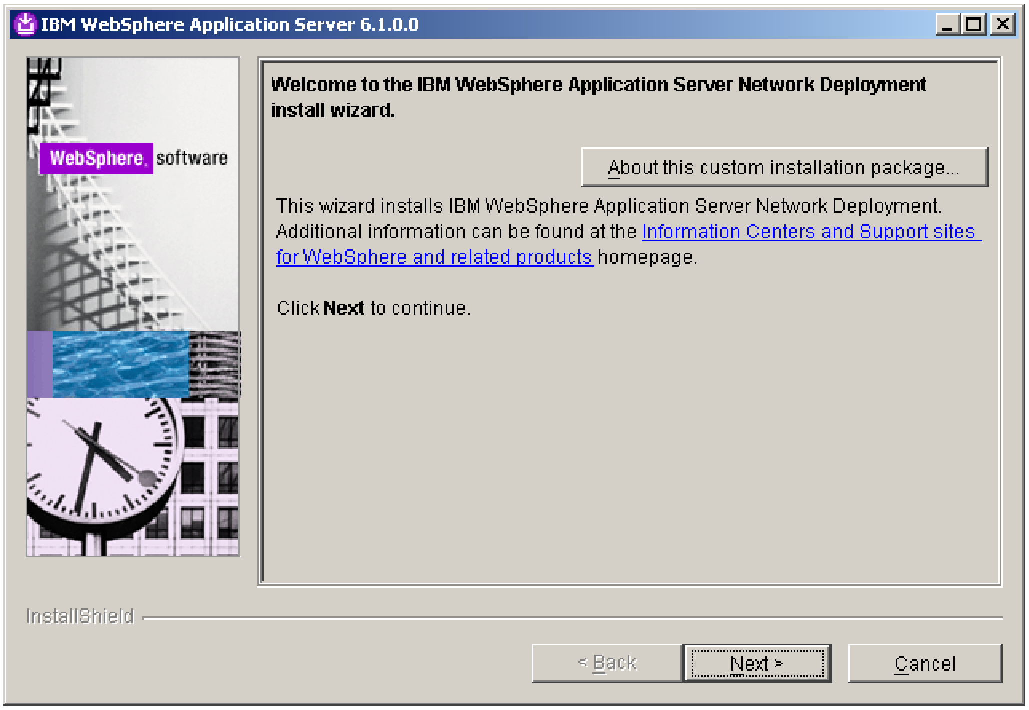
Install and configure the Deployment Manager

In this section, you will install the Deployment Manager and prepare it for the future Portal cluster. All of the following steps will be completed on the server you intend to use as your deployment manager.

1. From the W-1 CD, navigate to \windows\ia32\ifpackage\WAS\ and launch install.exe

   NOTE: This CD number may vary between operating systems. The CD title is WebSphere Application Server Network Deployment for Windows 32-bit.

2. Click Next on the Welcome Screen



IBM WebSphere Application Server 6.1.0.0

Welcome to the IBM WebSphere Application Server Network Deployment install wizard.

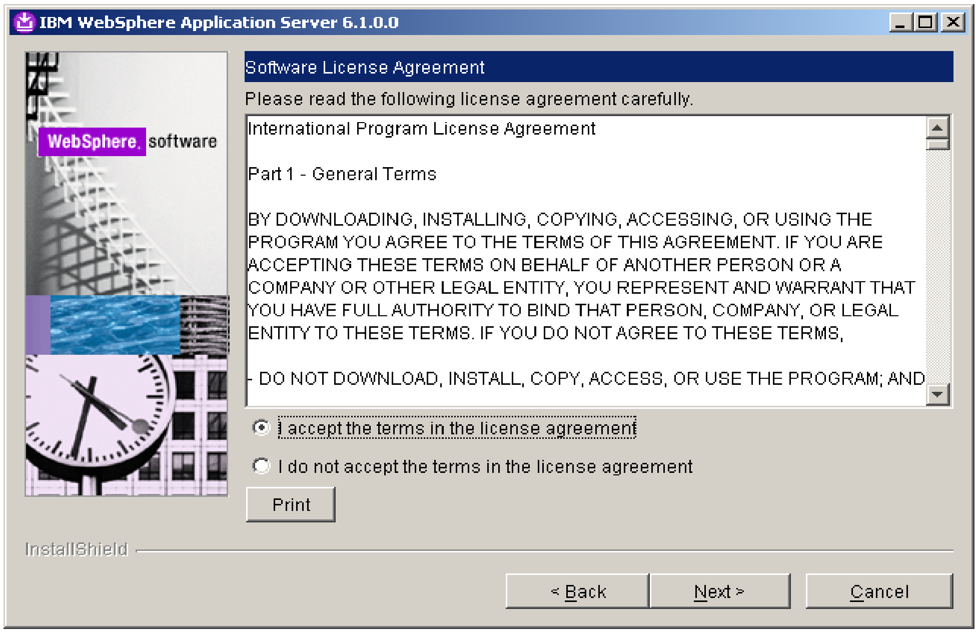
About this custom installation package...

This wizard installs IBM WebSphere Application Server Network Deployment. Additional information can be found at the Information Centers and Support sites for WebSphere and related products homepage.

Click **Next** to continue.

NOTE: This is a customized installation of WebSphere Application Server Network Deployment that will automatically install version 6.1.0.15. For details about the installation, click the "About this custom installation package" button from the Welcome Screen.

3. Select the radio button to accept the license agreement and click Next



Software License Agreement

Please read the following license agreement carefully.

International Program License Agreement

Part 1 - General Terms

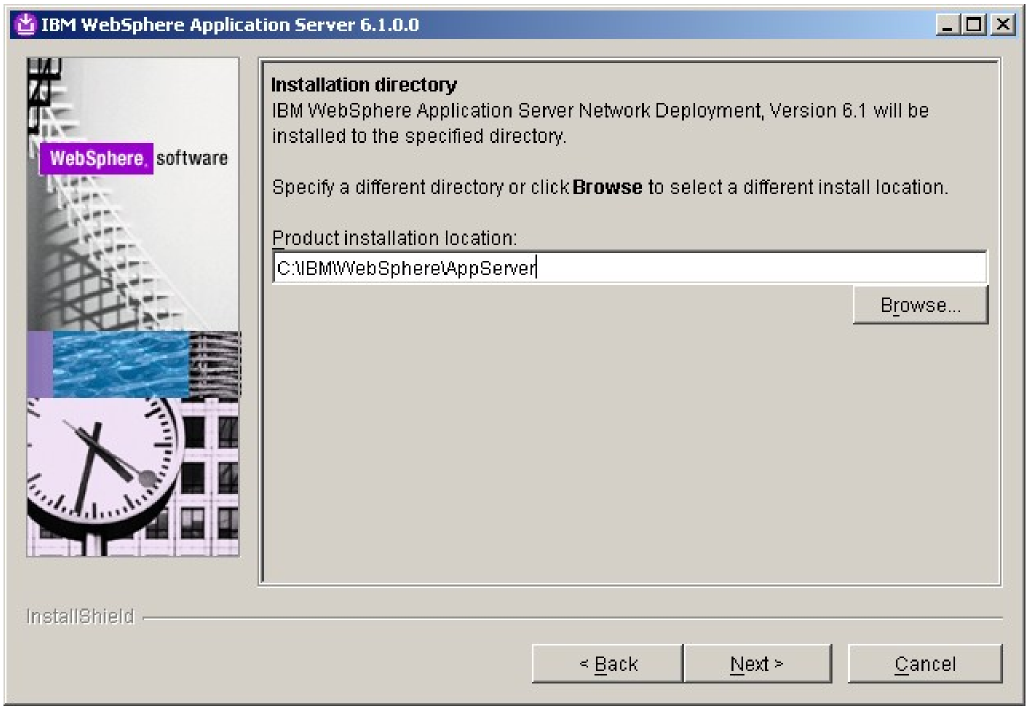
BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THE PROGRAM YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL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

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

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

4. Select the installation location you wish to use and click Next.



Installation directory

IBM WebSphere Application Server Network Deployment, Version 6.1 will be installed to the specified directory.

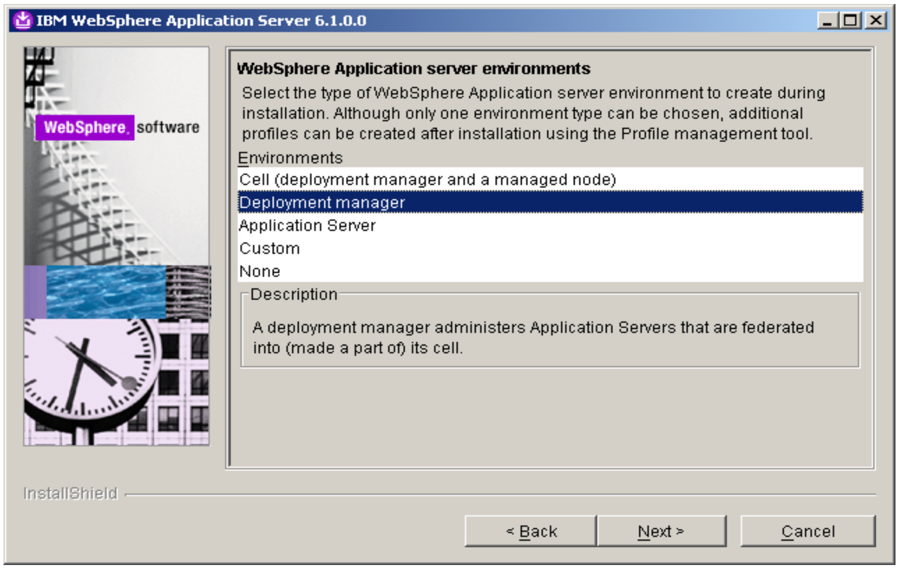
Specify a different directory or click **Browse** to select a different install location.

Product installation location:

C:\IBM\WebSphere\AppServer

5. From the list of environments, select Deployment Manager. Do NOT select Cell. WebSphere Portal cannot use the managed node that would be installed in the Cell environment. Alternatively you can select NONE and create a profile after installation completes. This will allow you to customize the DMGR profile name and profile location. For more information on creating a profile after installation, please see the following link the WebSphere Application Server Information Center:

   http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tpro_instancesdmgr.html



WebSphere Application server environments

Select the type of WebSphere Application server environment to create during installation. Although only one environment type can be chosen, additional profiles can be created after installation using the Profile management tool.

Environments

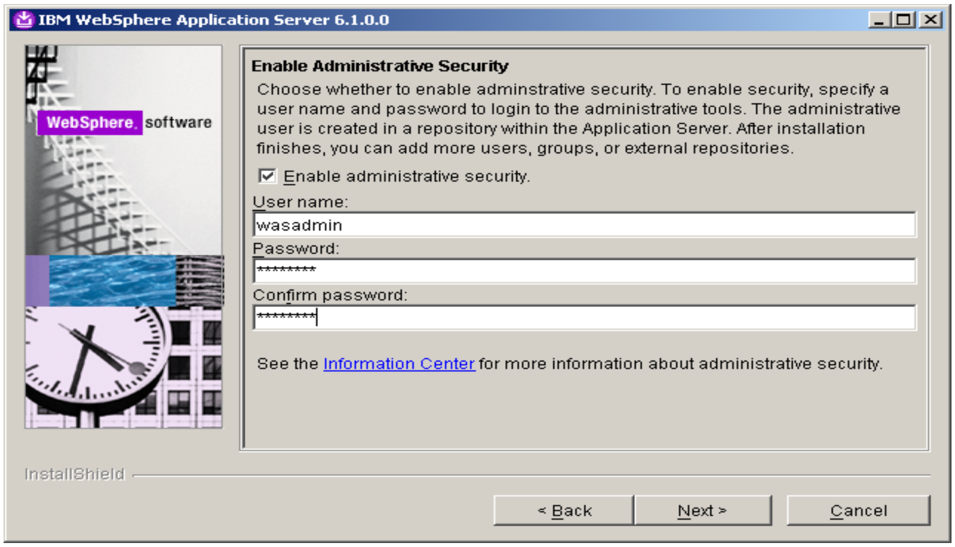
Cell (deployment manager and a managed node)
Deployment manager
Application Server
Custom
None

Description

A deployment manager administers Application Servers that are federated into (made a part of) its cell.

6. Click the checkbox to Enable Administrative security. Enter a user ID and a password and click next.

   NOTE: VMM Federated File Security is enabled here.



Enable Administrative Security

Choose whether to enable adminstrative security. To enable security, specify a user name and password to login to the administrative tools. The administrative user is created in a repository within the Application Server. After installation finishes, you can add more users, groups, or external repositories.

☑ Enable administrative security.

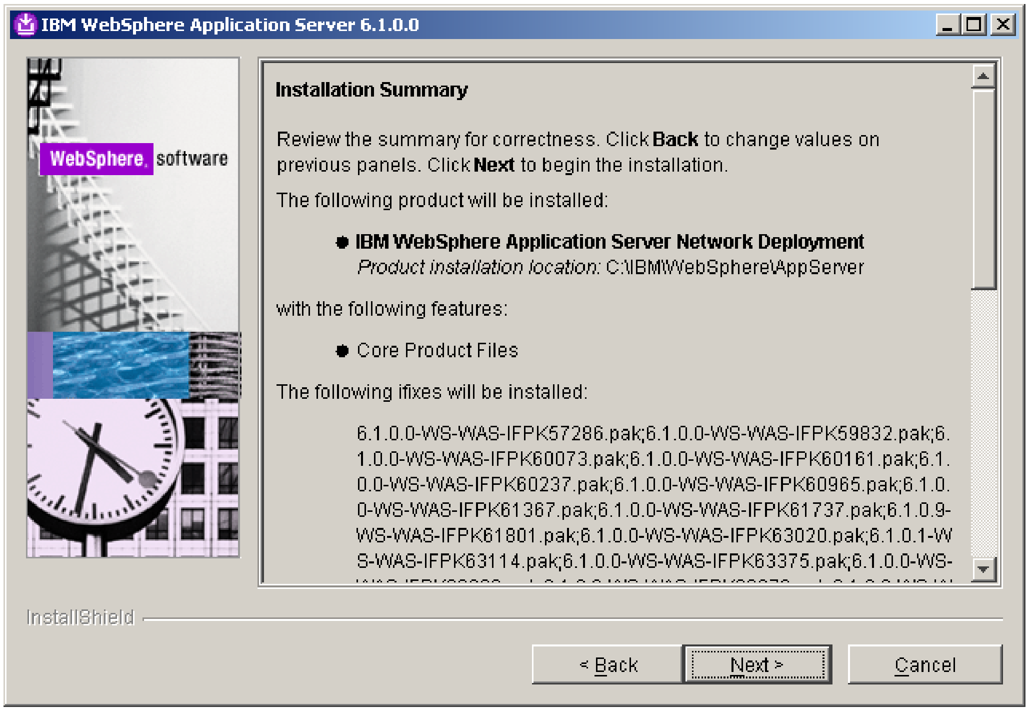
User name:
wasadmin

Password:
****

Confirm password:
****

See the Information Center for more information about administrative security.

7. On the summary screen, click Next to begin the installation.



Installation Summary

Review the summary for correctness. Click **Back** to change values on previous panels. Click **Next** to begin the installation.

The following product will be installed:

- **IBM WebSphere Application Server Network Deployment**
  Product installation location: C:\IBM\WebSphere\AppServer

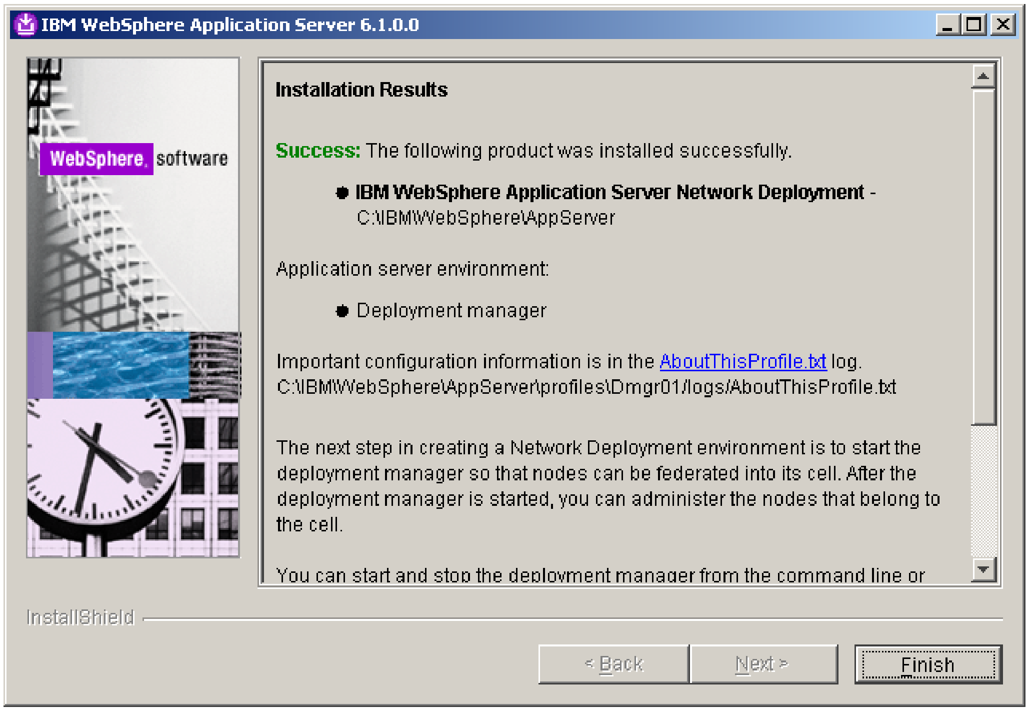
with the following features:

- Core Product Files

The following ifixes will be installed:

6.1.0.0-WS-WAS-IFPK57286.pak;6.1.0.0-WS-WAS-IFPK59832.pak;6.1.0.0-WS-WAS-IFPK60073.pak;6.1.0.0-WS-WAS-IFPK60161.pak;6.1.0.0-WS-WAS-IFPK60237.pak;6.1.0.0-WS-WAS-IFPK60965.pak;6.1.0.0-WS-WAS-IFPK61367.pak;6.1.0.0-WS-WAS-IFPK61737.pak;6.1.0.9-WS-WAS-IFPK61801.pak;6.1.0.0-WS-WAS-IFPK63020.pak;6.1.0.1-WS-WAS-IFPK63114.pak;6.1.0.0-WS-WAS-IFPK63375.pak;6.1.0.0-WS-

8. After the installation completes, click Finish.



Installation Results

Success: The following product was installed successfully.

- **IBM WebSphere Application Server Network Deployment** - C:\IBM\WebSphere\AppServer

Application server environment:

- Deployment manager

Important configuration information is in the AboutThisProfile.txt log.
C:\IBM\WebSphere\AppServer\profiles\Dmgr01/logs/AboutThisProfile.txt

The next step in creating a Network Deployment environment is to start the deployment manager so that nodes can be federated into its cell. After the deployment manager is started, you can administer the nodes that belong to the cell.

You can start and stop the deployment manager from the command line or

9. From a command window, navigate to <AppServer root>/profiles/Dmgr01/bin

10. Execute the following command:

    ```
    startManager.bat
    ```

11. Once the DMGR is open for e-business, launch a web browser and access the DMGR Administrative Console:

    http://<yourhostname>:9060/ibm/console

12. Enter the User ID and Password you used during installation and click 'Log in'

13. Increase the HTTP Connection timeouts for the deployment manager:
    a) Navigate to **System Administration -> Deployment Manager -> Web Container Transport Chains**
    b) For each entry in the table (WCInboundAdmin and WCInboundAdminSecure), complete the following:
        1. Click HTTP Inbound Channel
        2. Change Read Timeout to 180
        3. Change Write Timeout to 180
        4. Click OK
        5. Save configuration changes

14. Change the timeout request period for the Java Management Extensions (JMX) connector.
    a) Navigate to **System Administration -> Deployment Manager -> Administration Services -> JMX connectors -> SOAPConnector -> Custom Properties**
    b) Select the requestTimeout property, and increase the value from `600` to `6000`.
    c) Save configuration changes.

15. Update the maximum Java heap size used by the deployment manager:

    a) Click System administration > Deployment manager > Java and Process Management > Process Definition > Java Virtual Machine.

    b) Specify **256** for **Initial Heap Size** and **1024** for **Maximum Heap Size**.

       For information about appropriate heap sizes see the documentation for your operating system and the Performance Guides located on the WebSphere Portal and Web Content Management Product Documentation page.

       NOTE: If using a 32-bit operating system, you will need to set the heap size to a lower size than a 64-bit operating system.

    c) Click OK, and then save your changes.

16. One significant change to the way clusters are created in Portal v6.1 is the security configuration. Because we use VMM security by default, the node will inherit the security settings of the DMGR when it is federated. We will need to create a Portal Administrative Group and Portal Administrative User in the current DMGR security configuration that will ultimately be used once our future Portal node is federated.

    Navigate to **Users and Groups -> Manage Groups**

17. Click Create

18. Create a group called **wpsadmins**. Please use the value of wpsadmins.

19. Navigate to **Users and Groups -> Manage Users**

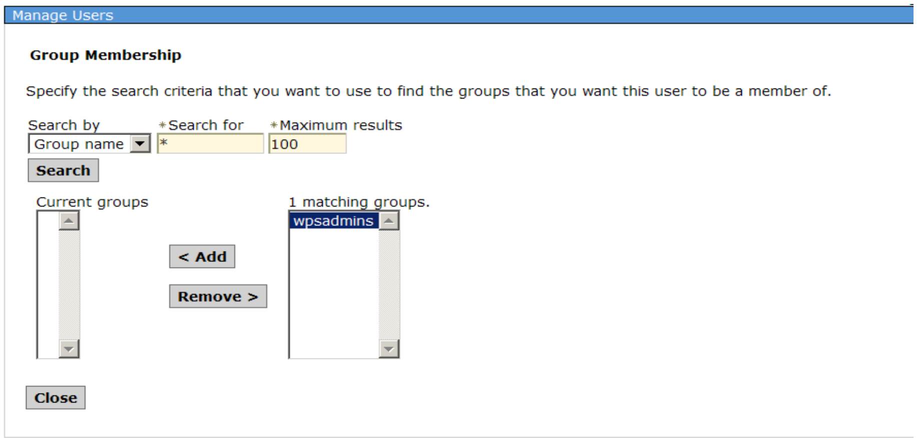
20. Click Create

21. Perform the following steps to create the Portal Administrative user:

   a) Enter the following values (these can be whatever you wish):
   User ID = wpsadmin
   First name = wps
   Last name = admin
   Password = wpsadmin
   Confirm Password = wpsadmin

   b) Click the 'Group Membership' button

   c) From the right hand menu, select 'wpsadmins' and click Add



Manage Users

Group Membership

Specify the search criteria that you want to use to find the groups that you want this user to be a member of.

Search by: Group name
*Search for: *
*Maximum results: 100

Current groups

1 matching groups.
wpsadmins

   d) Click Close

   e) Click Create to create the user

22. Logout of the Deployment Manager Admin Console and close the browser.

23. Edit the soap.client.props file from the <dmgr_profile>/properties directory in a text editor.

24. Change the com.ibm.SOAP.timeout entry to 6000:

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

25. Save the file

26. Restart the DMGR by issuing the following commands in a command window from the <dmgr_profile>/bin directory:

```
stopManager.bat -user wasadmin -password wasadmin

startManager.bat
```

Install the Primary Portal Node

In this section, you will install the primary Portal node. The Portal installer automatically installs WebSphere Application Server v6.1.0.15. All of the steps in this section will be done on the server you intend to use as your primary node.

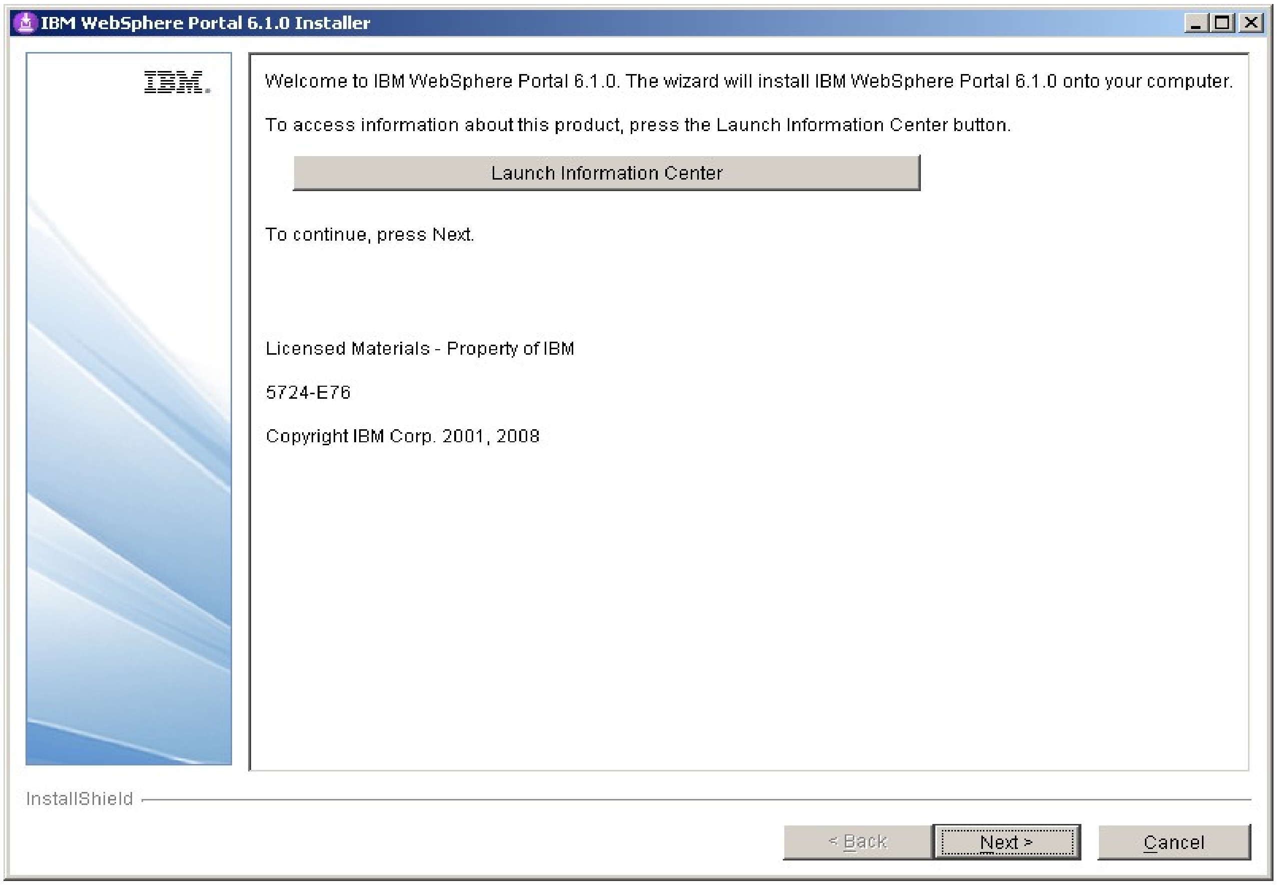
1. Open a command window and enter:

   ping yourserver.yourcompany.com

   where yourserver.yourcompany.com is your actual fully qualified hostname, to verify the fully qualified hostname of your machine is configured properly
2. Enter:

   ping localhost

   to verify the network settings are configured properly on your machine.
3. From the W-Setup CD, double-click install.bat
4. Click 'Next' on the Welcome screen.



IBM WebSphere Portal 6.1.0 Installer
IBM.

Welcome to IBM WebSphere Portal 6.1.0. The wizard will install IBM WebSphere Portal 6.1.0 onto your computer.

To access information about this product, press the Launch Information Center button.

Launch Information Center

To continue, press Next.

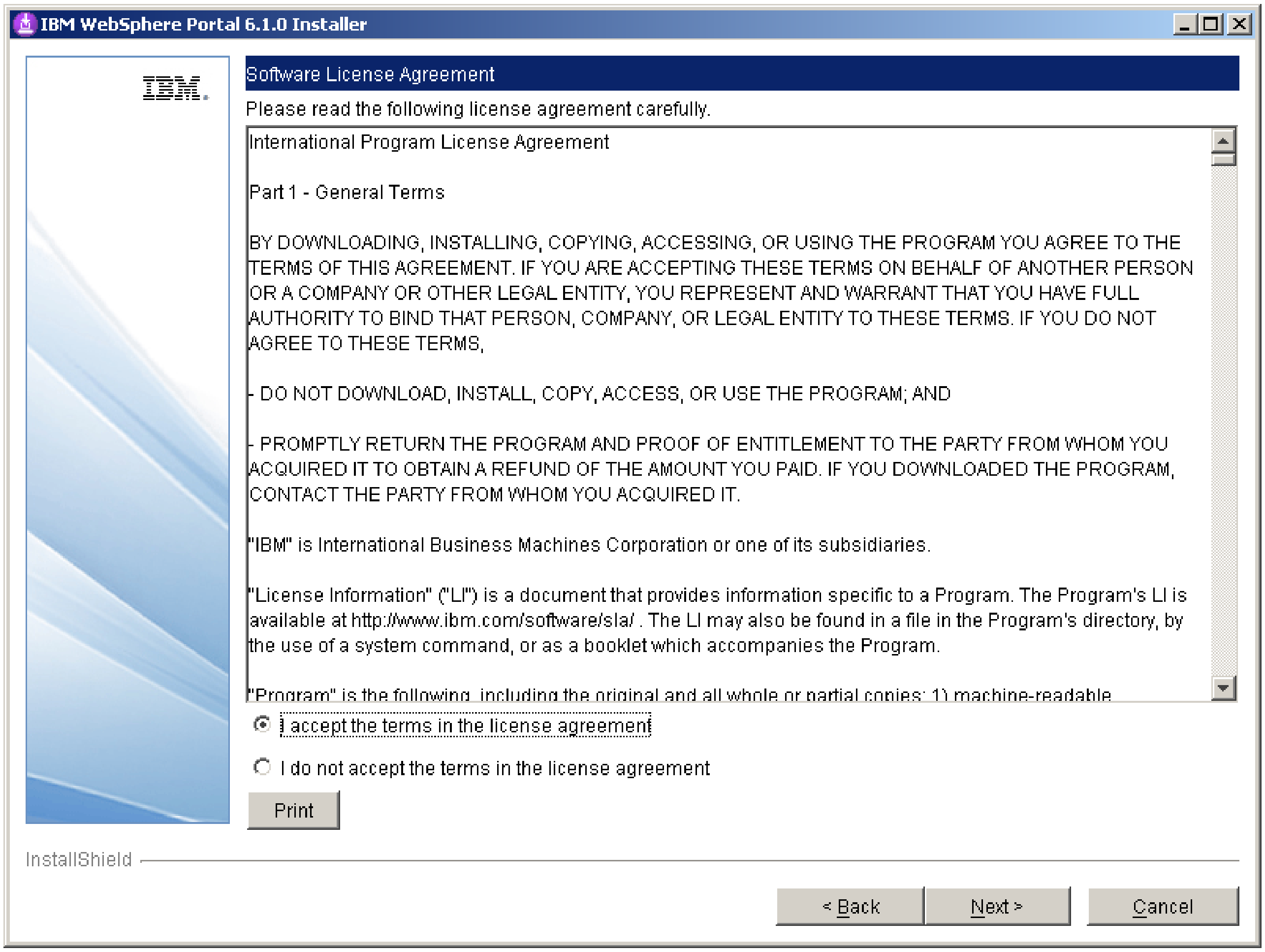
Licensed Materials - Property of IBM

5724-E76

Copyright IBM Corp. 2001, 2008

InstallShield
< Back
Next >
Cancel

5. Accept the license agreement and click 'Next'



Software License Agreement

Please read the following license agreement carefully.

International Program License Agreement

Part 1 - General Terms

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

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

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

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

"License Information" ("LI") is a document that provides information specific to a Program. The Program's LI is available at http://www.ibm.com/software/sla/ . The LI may also be found in a file in the Program's directory, by the use of a system command, or as a booklet which accompanies the Program.

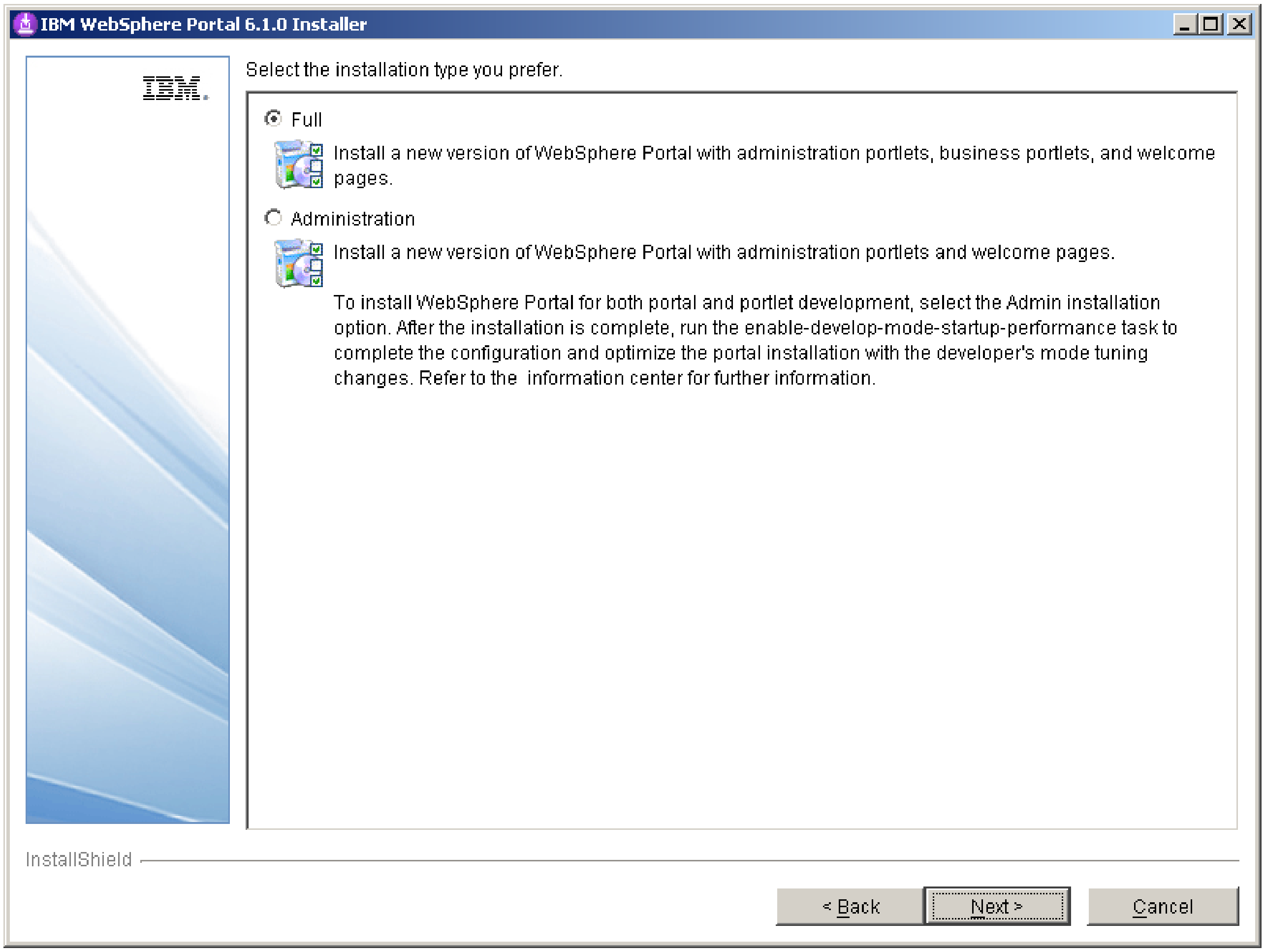
"Program" is the following, including the original and all whole or partial copies: 1) machine-readable

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

6. On the installation type screen, select 'Full' and click 'Next'

   NOTE: Select Administration to install only administrative portlets.



IBM WebSphere Portal 6.1.0 Installer

Select the installation type you prefer.

● Full

Install a new version of WebSphere Portal with administration portlets, business portlets, and welcome pages.

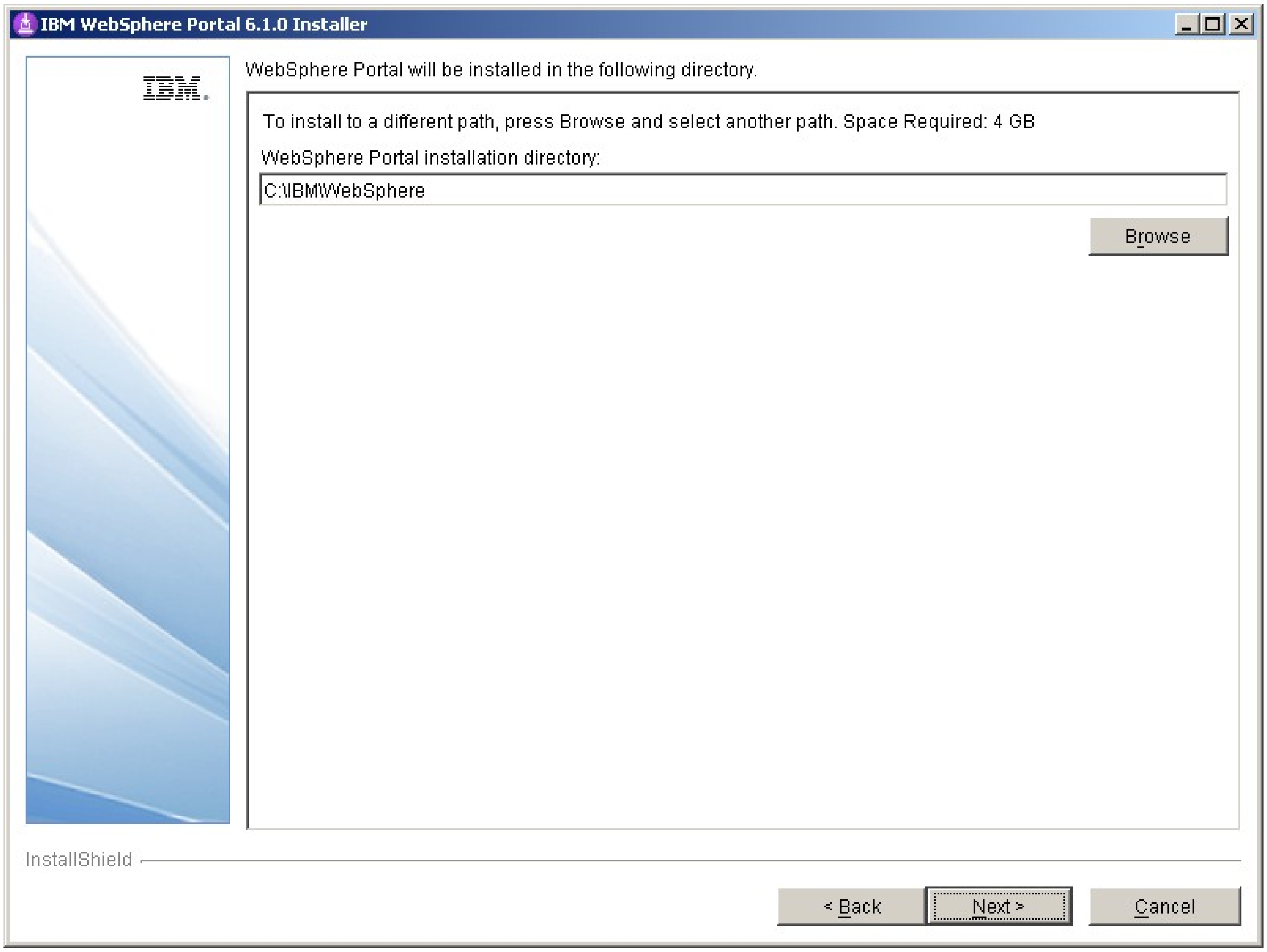
○ Administration

Install a new version of WebSphere Portal with administration portlets and welcome pages.

To install WebSphere Portal for both portal and portlet development, select the Admin installation option. After the installation is complete, run the enable-develop-mode-startup-performance task to complete the configuration and optimize the portal installation with the developer's mode tuning changes. Refer to the information center for further information.

7. Select the desired path for the WebSphere directory and click 'Next'

   NOTE: Both the AppServer directory and the PortalServer directory will be created in this WebSphere directory.
   NOTE: Ensure that the desired path does not already exist in your environment. The Portal installer will create it for you.



IBM WebSphere Portal 6.1.0 Installer

WebSphere Portal will be installed in the following directory.

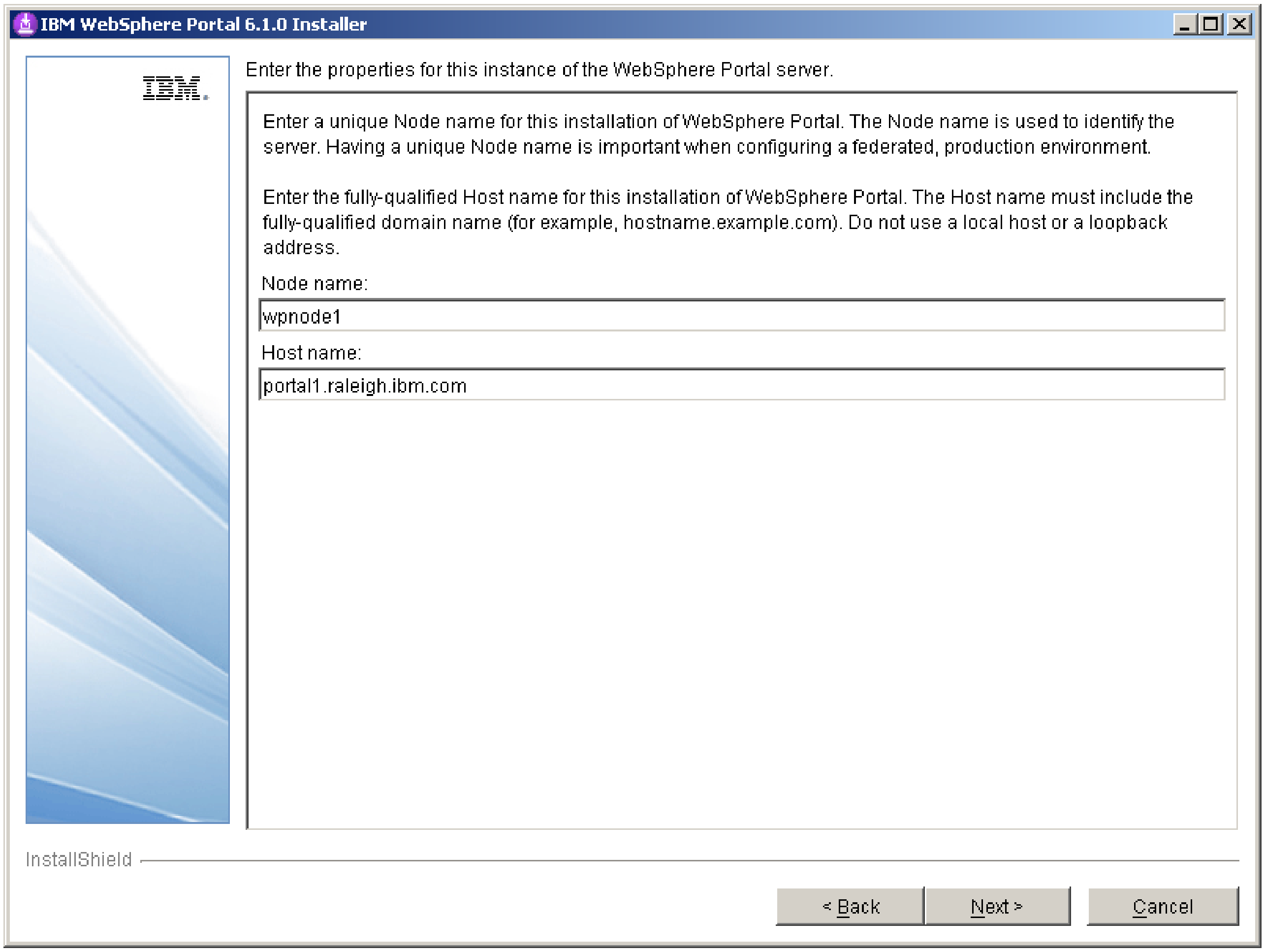
To install to a different path, press Browse and select another path. Space Required: 4 GB

WebSphere Portal installation directory:

C:\IBM\WebSphere

8. Enter a node name and the fully qualified hostname of your server and click 'Next'.

   NOTE: The value for node name will also be used as the cell name in the standalone environment.



Enter the properties for this instance of the WebSphere Portal server.

Enter a unique Node name for this installation of WebSphere Portal. The Node name is used to identify the server. Having a unique Node name is important when configuring a federated, production environment.

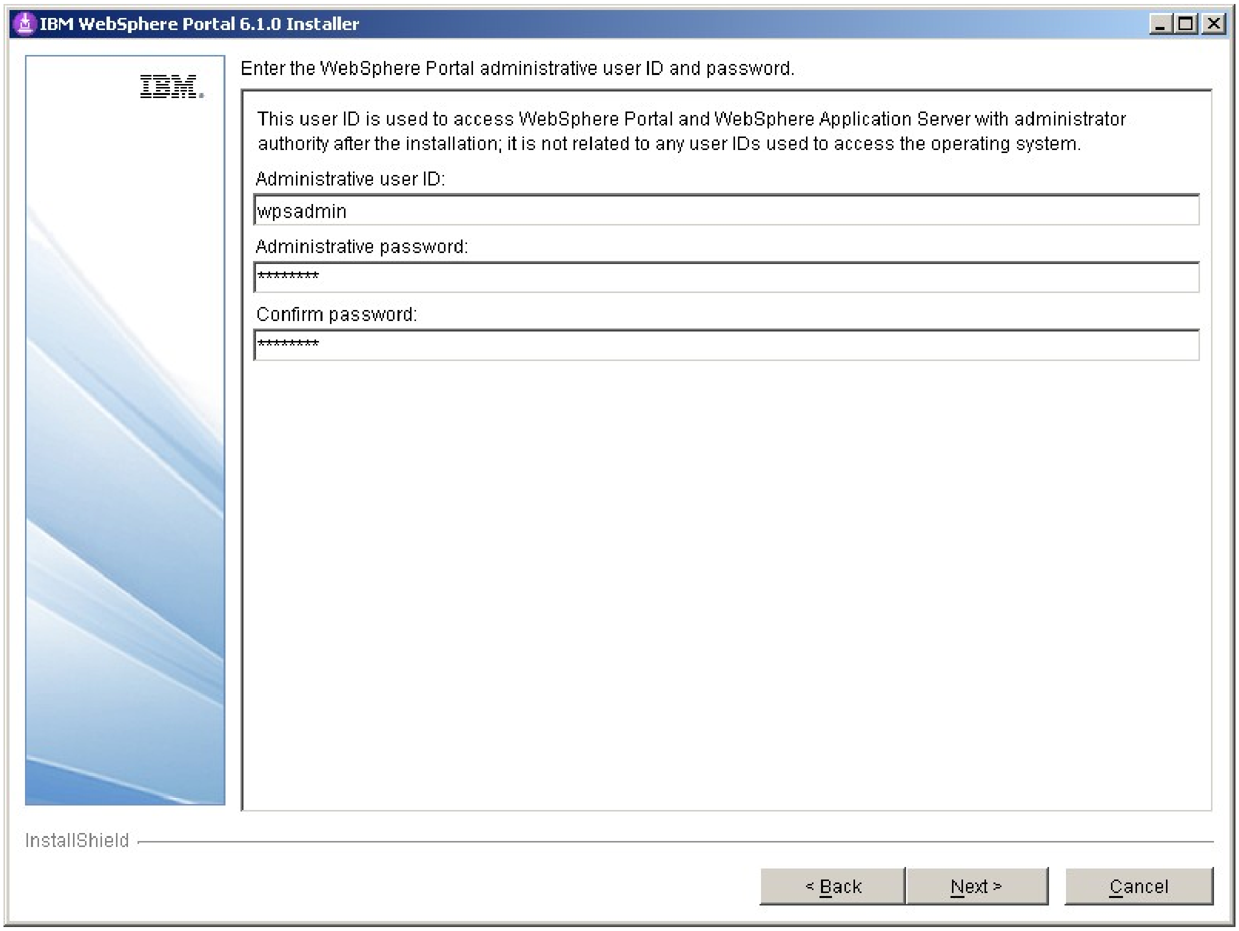
Enter the fully-qualified Host name for this installation of WebSphere Portal. The Host name must include the fully-qualified domain name (for example, hostname.example.com). Do not use a local host or a loopback address.

Node name: wpnode1

Host name: portal1.raleigh.ibm.com

9. Security is enabled for Portal by default. Enter a user ID and password you wish to use. This ID will be used to access both server1 and WebSphere_Portal after installation completes.

   IMPORTANT: Use the same Portal Admin ID that you used in step 21 from the previous section.



IBM WebSphere Portal 6.1.0 Installer

Enter the WebSphere Portal administrative user ID and password.

This user ID is used to access WebSphere Portal and WebSphere Application Server with administrator authority after the installation; it is not related to any user IDs used to access the operating system.

Administrative user ID: wpsadmin

Administrative password: *********

Confirm password: *********

10. **Windows** only. Do NOT check the box to use Windows services. Click 'Next'

11. Verify the information is accurate in the summary screen and click 'Next' to begin the installation.

12. Once the installation finishes, uncheck Launch First Steps and Launch the Configuration Wizard. Click 'Finish'.

13. Verify you can access Portal in a web browser. The default URL is:

    http://yourserver.yourcompany.com:10040/wps/portal

Install IBM Support Assistant Lite

In this section, you will install IBM Support Assistant Lite for WebSphere Portal (ISALite). This step is optional but **highly** recommended. ISALite provides automatic log collection and symptom analysis support for WebSphere Portal problem determination scenarios. Installing this tool now can save you time in the future if you have any problems with WebSphere Portal that require you to contact support.

1. Visit the website below and download ISALite for WebSphere Portal v6.1 to a temporary directory:

   http://www-01.ibm.com/support/docview.wss?rs=688&uid=swg24008662

2. Extract the downloaded zip file into the wp_profile/PortalServer directory. This will create a directory called ISALite.

3. The tool is installed and ready for use. If you have an issue with WebSphere Portal and require support, instructions for using this tool can be found in Appendix D.

Configure the Primary Portal node to an external database

In this section, Portal will be configured to use an external database. For the purposes of this document, DB2 will be used as the external database with Type 4 drivers. This may vary in your environment. For more information about other databases that can be used with Portal, please visit the WebSphere Portal v6.1 Information Center for configuring external databases at this link and follow the instructions there as appropriate:

http://publib.boulder.ibm.com/infocenter/wpdoc/v6r1m0/index.jsp?topic=/com.ibm.wp.ent.doc/config/win_remote_db.html

In the environment used for this guide, 6 databases were created following the instructions in the Information Center:

RELDB61
COMDB61
CUSDB61
JCRDB61
FDBKDB61
LMDB61

In addition, the database administrator user "db2admin" will be used as the user ID for each database.

All of the steps in this section will be done from the primary Portal node.

1. Stop the WebSphere_Portal and server1 by executing the following commands from the command window in the <wp_profile>/bin directory:

   ```
   stopServer.bat WebSphere_Portal -user <admin user> -password <admin pwd>
   stopServer.bat server1 -user <admin user> -password <admin pwd>
   ```

2. Ensure the database client is installed and configured on the node. Since we are using Type 4 drivers for DB2, all that is needed is to copy the db2jcc.jar and db2jcc_license_cu.jar files from the DB2 server to some directory on the primary Portal server.
3. From the <wp_profile>/ConfigEngine/properties directory, make a backup of the following files:

   wkplc.properties
   wkplc_dbtype.properties
   wkplc_comp.properties

4. Edit the wkplc_dbtype.properties file and make the following changes:

```
db2.DbDriver=com.ibm.db2.jcc.DB2Driver
db2.DbLibrary=C:/IBM/db2drivers/db2jcc.jar;C:/IBM/db2drivers/db2jcc_license_cu.jar

db2.JdbcProviderName=wpdbJDBC_db2
```

NOTE: The entry for db2.DbLibrary is an example only. Please ensure this is a valid path on your system.

5. Edit the wkplc_comp.properties file and make the following changes:

```
feedback.DbType=db2
feedback.DbName=fdbkdb61
feedback.DbSchema=FEEDBACK
feedback.DataSourceName=wpdbDS_fdbk
feedback.DbUrl=jdbc:db2://mydbserver.ibm.com:50000/fdbkdb61:returnAlias=0;
feedback.DbUser=db2admin
feedback.DbPassword=password
feedback.DBA.DbUser=db2admin
feedback.DBA.DbPassword=password

likeminds.DbType=db2
likeminds.DbName=lmdb61
likeminds.DbSchema=likeminds
likeminds.DataSourceName=wpdbDS_lmdb
likeminds.DbUrl=jdbc:db2://mydbserver.ibm.com:50000/lmdb61:returnAlias=0;
likeminds.DbUser=db2admin
likeminds.DbPassword=password
likeminds.DBA.DbUser=db2admin
likeminds.DBA.DbPassword=password

release.DbType=db2
release.DbName=reldb61
release.DbSchema=release
release.DataSourceName=wpdbDS_reldb
release.DbUrl=jdbc:db2://mydbserver.ibm.com:50000/reldb61:returnAlias=0;
release.DbUser=db2admin
release.DbPassword=password
release.DBA.DbUser=db2admin
release.DBA.DbPassword=password

community.DbType=db2
community.DbName=comdb61
community.DbSchema=community
community.DataSourceName=wpdbDS_comdb
community.DbUrl=jdbc:db2://mydbserver.ibm.com:50000/comdb61:returnAlias=0;
community.DbUser=db2admin
community.DbPassword=password
community.DBA.DbUser=db2admin
community.DBA.DbPassword=password
```

```
customization.DbType=db2
customization.DbName=cusdb61
customization.DbSchema=customization
customization.DataSourceName=wpdbDS_cusdb
customization.DbUrl=jdbc:db2://mydbserver.ibm.com:50000/cusdb61:returnAlias=0
;
customization.DbUser=db2admin
customization.DbPassword=password
customization.DBA.DbUser=db2admin
customization.DBA.DbPassword=password

jcr.DbType=db2
jcr.DbName=jcrdb61
jcr.DbSchema=jcr
jcr.DataSourceName=wpdbDS_jcrdb
jcr.DbUrl=jdbc:db2://mydbserver.ibm.com:50000/jcrdb61:returnAlias=0;
jcr.DbUser=db2admin
jcr.DbPassword=password
jcr.DBA.DbUser=db2admin
jcr.DBA.DbPassword=password
```

6. From a command window, change directories to <wp_profile root>/ConfigEngine
7. Execute the following ConfigEngine scripts to validate the database properties:

   ```
   ConfigEngine.bat validate-database-driver
   ConfigEngine.bat validate-database-connection
   ```

8. Execute the following ConfigEngine script to transfer the database from Derby to DB2:

   ```
   ConfigEngine.bat database-transfer -DPortalAdminPwd=<password>
   -DWasPassword=<password>
   ```

9. After the database-transfer completes, change directories to <wp_profile>/bin and execute the following command to start the Portal server:

   ```
   startServer.bat WebSphere_Portal
   ```

10. Verify that you can render Portal successfully in a web browser.

    http://myserver.mycompany.com:10040/wps/portal

At this point, you have successfully installed WebSphere Portal and configured it to use an external database.

Federate and Cluster the Primary Node

The next step is to federate and cluster the newly installed WebSphere Portal node. The clustering process has changed significantly from Portal v6.0 to v6.1. You are no longer required to manually execute the AddNode command to add the node to the Deployment Manager cell. Instead, a ConfigEngine script has been created that does this, among other things for you. After the following steps have been completed, you will have a one node cluster.

1. From the primary node, open a command window and change directories to the <wp_profile>/ConfigEngine directory.
2. Collect files from the Portal node that will need to be added to the Deployment Manager file structure. To collect the files, execute the following ConfigEngine script:

   ```
   ConfigEngine.bat collect-files-for-dmgr -DWasPassword=password
   ```

   This will create a zip file called filesforDmgr.zip in the <wp_profile root>/filesforDmgr directory.
3. Copy the filesforDmgr.zip file from your primary node to a temporary directory on your Deployment Manager server.
4. Extract the filesforDmgr.zip into a temporary directory on the Deployment Manager server.
5. From the temporary directory on your Deployment Manager, copy the AppServer/lib/wkplc.comp.registry.jar and wp.wire.jar into your <AppServer root>/lib directory.
6. From the temporary directory on your Deployment Manager, copy the AppServer/plugins/com.ibm.ws.portletcontainer.deploytask_6.1.0.jar file into your <AppServer root>/plugins directory.
7. From the temporary directory on your Deployment Manager, copy the AppServer/profiles/Dmgr01/config/.repository/metadata_wkplc.xml file into your <dmgr profile>/config/.repository directory.
8. Stop the deployment manager by issuing the following command from the <dmgr profile>/bin directory:

   ```
   stopManager.bat -user wasadmin -password password
   ```
9. Start the deployment manager by issuing the following command from the <dmgr profile root>/bin directory:

   ```
   startManager.bat
   ```

10. On the primary node, edit the <wp_profile>/ConfigEngine/properties/wkplc.properties file and ensure all of the following properties are set appropriately for your enviornment:

    ```
    WasPassword=<standalone WAS admin password>
    PortalAdminPwd=password
    WasRemoteHostName=<fully qualified hostname of DMGR>
    WasSoapPort=<soap port for DMGR; default is 8879>
    PrimaryNode=true
    ClusterName=PortalCluster
    ```

11. Edit <wp_profile>/ConfigEngine/properties/wkplc_comp.properties and ensure all database user IDs and passwords are accurate.

12. Ensure that the operating system time on the Deployment Manager server and the time on the primary node are within 5 minutes of each other. This is necessary for Steps 13-14 to complete successfully.

13. In a command window from the primary node, change directories to <wp_profile>/ConfigEngine

14. Add the node to the deployment manager cell by executing the following ConfigEngine script:

    ```
    ConfigEngine.bat cluster-node-config-pre-federation -DDMgrUserid=uid=<dmgr
    user id>,o=defaultWIMFileBasedRealm -DDMgrPassword=<dmgr password>
    ```

    For example:

    ```
    ConfigEngine.bat cluster-node-config-pre-federation
    -DDMgrUserid=uid=wasadmin,o=defaultWIMFileBasedRealm -DDMgrPassword=wasadmin
    ```

    IMPORTANT FOR PORTAL 6.1.0.3 OR HIGHER: This step does NOT apply to Portal v6.1.0.3+. The -DDMgrUserid and -DDMgrPassword properties are no longer used in 6.1.0.3. Instead you must do the following:

    - Update wkplc.properties and change WasUserid and WasPassword to the DMGR user ID values.

    - Run the ConfigEngine script as follows, without the DmgrUserid and DMgrPassword:

      ```
      ConfigEngine.bat cluster-node-config-pre-federation
      ```

    NOTE: If you are prompted to accept an SSL certificate, type Y and press Enter to continue

    NOTE: If you specify the -DDMgrUserid parameter when running the cluster-node-config-pre-federation task, it resets the WasUserid parameter in the wkplc.properties file to the -DDMgrUserid value.

NOTE: After you receive a BUILD SUCCESSFUL, you may see an error message displayed to the screen:

```
BUILD SUCCESSFUL

Total time: 12 minutes 8 seconds
isIseries currently set to: null
uploading registry
Created admin client: com.ibm.ws.management.AdminClientImpl@24e624e6
Created config Service Proxy:
com.ibm.websphere.management.configservice.ConfigS
erviceProxy@5bd85bd8
CELL: wpnode1
CELL: wpnode1
com.ibm.websphere.management.exception.ConfigServiceException:
javax.management.
JMRuntimeException: ADMN0022E: Access is denied for the resolve operation on
Con
figService MBean because of insufficient or empty credentials.
        at
com.ibm.websphere.management.configservice.ConfigServiceProxy.resolve
(ConfigServiceProxy.java:473)
.
.
.
Return Value: 0
```

This error message may vary in your environment but it is expected and can be ignored. Details of this and others like it can be found in the following technote:

http://www-1.ibm.com/support/docview.wss?rs=688&ca=port&uid=swg21303105

IMPORTANT: If you receive a BUILD FAILED for the cluster-node-config-pre-federation script, you MUST do the following before running the script again:

1. Remove the node in case AddNode went through successfully
2. Login to the DMGR and do the following (if these exist):
   a) Remove all Enterprise applications
   b) Remove the WebSphere_Portal server definition
   c) Remove the JDBC Provider information for WebSphere_Portal

15. After the previous step completes, your node will be part of the deployment manager cell. The node is now using the Deployment Manager security configuration and cell name. The original WAS ID that had been used in the standalone environment will no longer be used.

    Edit the <wp_profile>/ConfigEngine/properties/wkplc.properties file and ensure the following properties are set correctly:

    ```
    WasUserId=<dmgr admin user id>
    WasPassword=<dmgr password>
    CellName=<dmgr cell name>
    ```

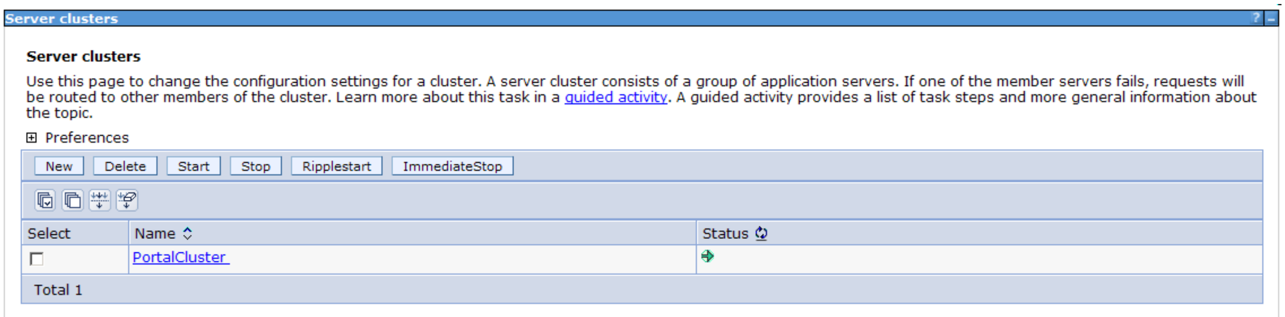
16. Update the deployment manager configuration for the new WebSphere Portal server by executing the following ConfigEngine script:

    ```
    ConfigEngine.bat cluster-node-config-post-federation
    ```

17. Create the cluster definition and add the WebSphere_Portal server as a cluster member by executing the following ConfigEngine script:

    ```
    ConfigEngine.bat cluster-node-config-cluster-setup
    ```

18. Ensure that the cluster definition was created correctly by logging into the DMGR Admin Console and browse to Server -> Clusters. An entry for your Portal cluster should be present.



Server clusters

Use this page to change the configuration settings for a cluster. A server cluster consists of a group of application servers. If one of the member servers fails, requests will be routed to other members of the cluster. Learn more about this task in a guided activity. A guided activity provides a list of task steps and more general information about the topic.

Select	Name	Status
□	PortalCluster	➜
Total 1		

19. Verify Portal is functional by accessing it in your web browser:

    http://myserver.mycompany.com:10040/wps/portal

Install the Secondary Portal Node

In this section, you will install the secondary Portal node. The Portal installer automatically installs WebSphere Application Server v6.1.0.15. All of the steps in this section will be done on the server you intend to use as your secondary node.

1. Open a command window and enter:

   ping yourserver.yourcompany.com

   where yourserver.yourcompany.com is your fully qualified hostname. This will verify the fully qualified hostname of your machine is configured properly

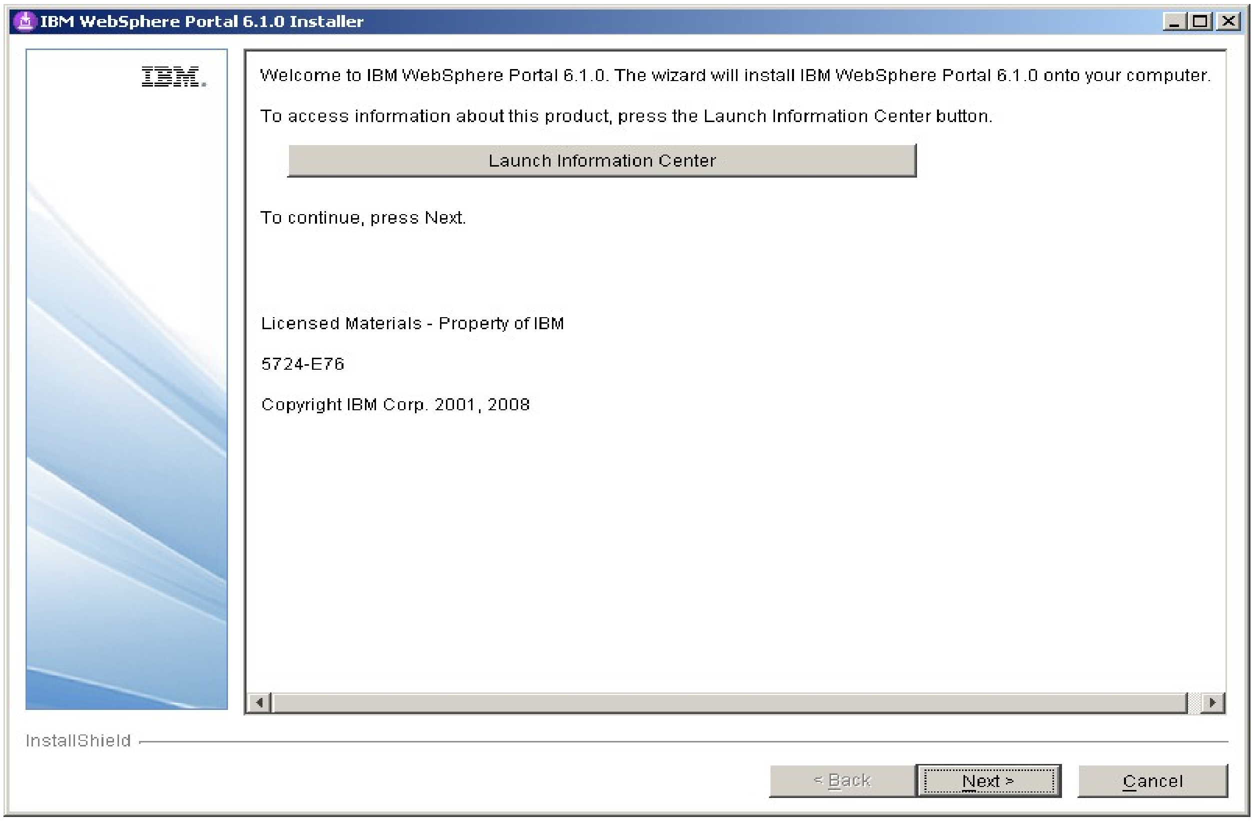
2. Type:

   ping localhost

   to verify the network settings are configured properly on your machine.

3. From the W-Setup CD, double-click install.bat

4. Click 'Next' on the Welcome screen.



Welcome to IBM WebSphere Portal 6.1.0. The wizard will install IBM WebSphere Portal 6.1.0 onto your computer.

To access information about this product, press the Launch Information Center button.

To continue, press Next.

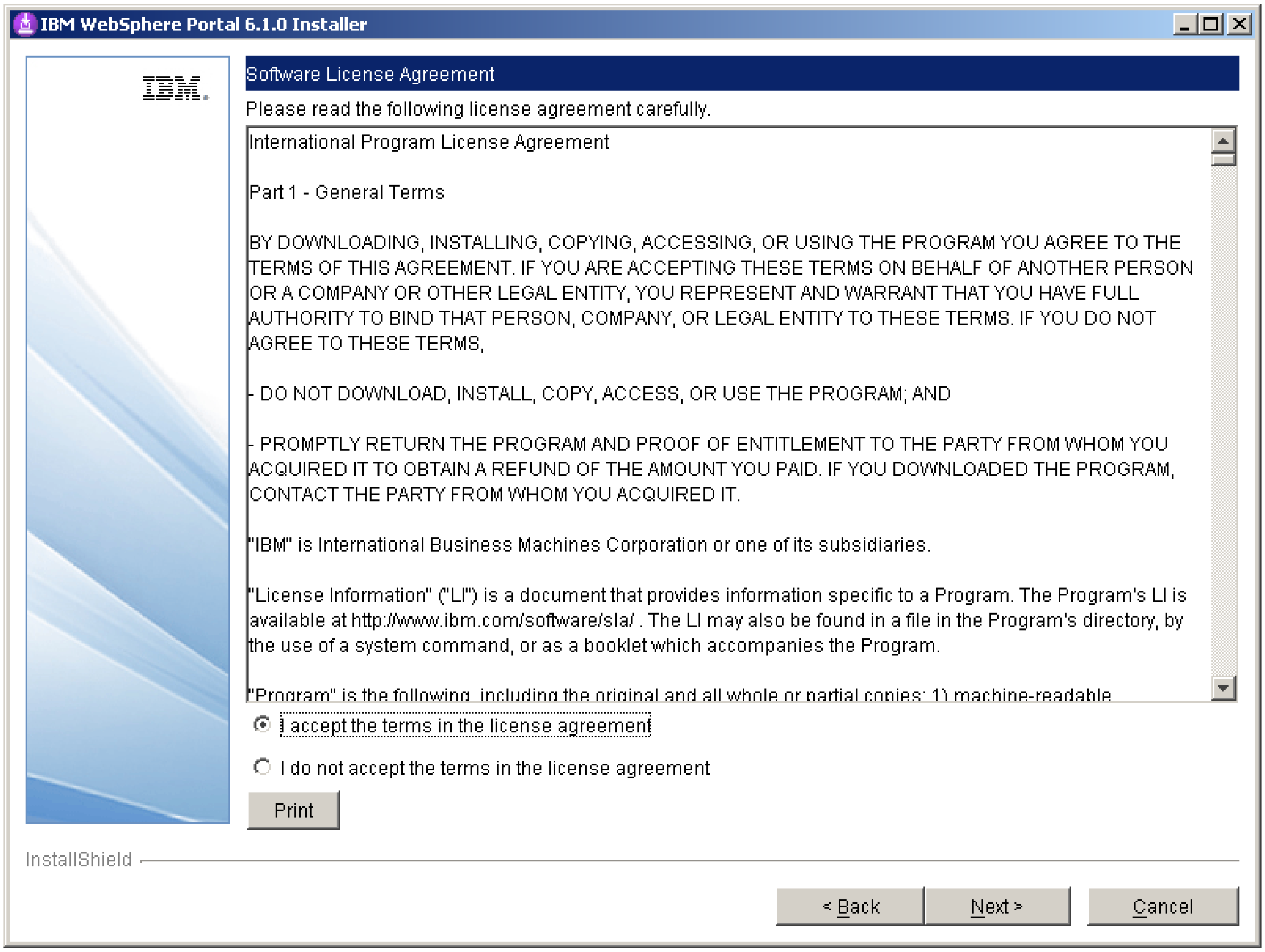
Licensed Materials - Property of IBM

5724-E76

Copyright IBM Corp. 2001, 2008

IBM WebSphere Portal 6.1.0 Installer
IBM.
Launch Information Center
InstallShield
< Back
Next >
Cancel

5. Accept the license agreement and click 'Next'


IBM WebSphere Portal 6.1.0 Installer
IBM.
Software License Agreement

Please read the following license agreement carefully.

International Program License Agreement

Part 1 - General Terms

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

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

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

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

"License Information" ("LI") is a document that provides information specific to a Program. The Program's LI is available at http://www.ibm.com/software/sla/ . The LI may also be found in a file in the Program's directory, by the use of a system command, or as a booklet which accompanies the Program.

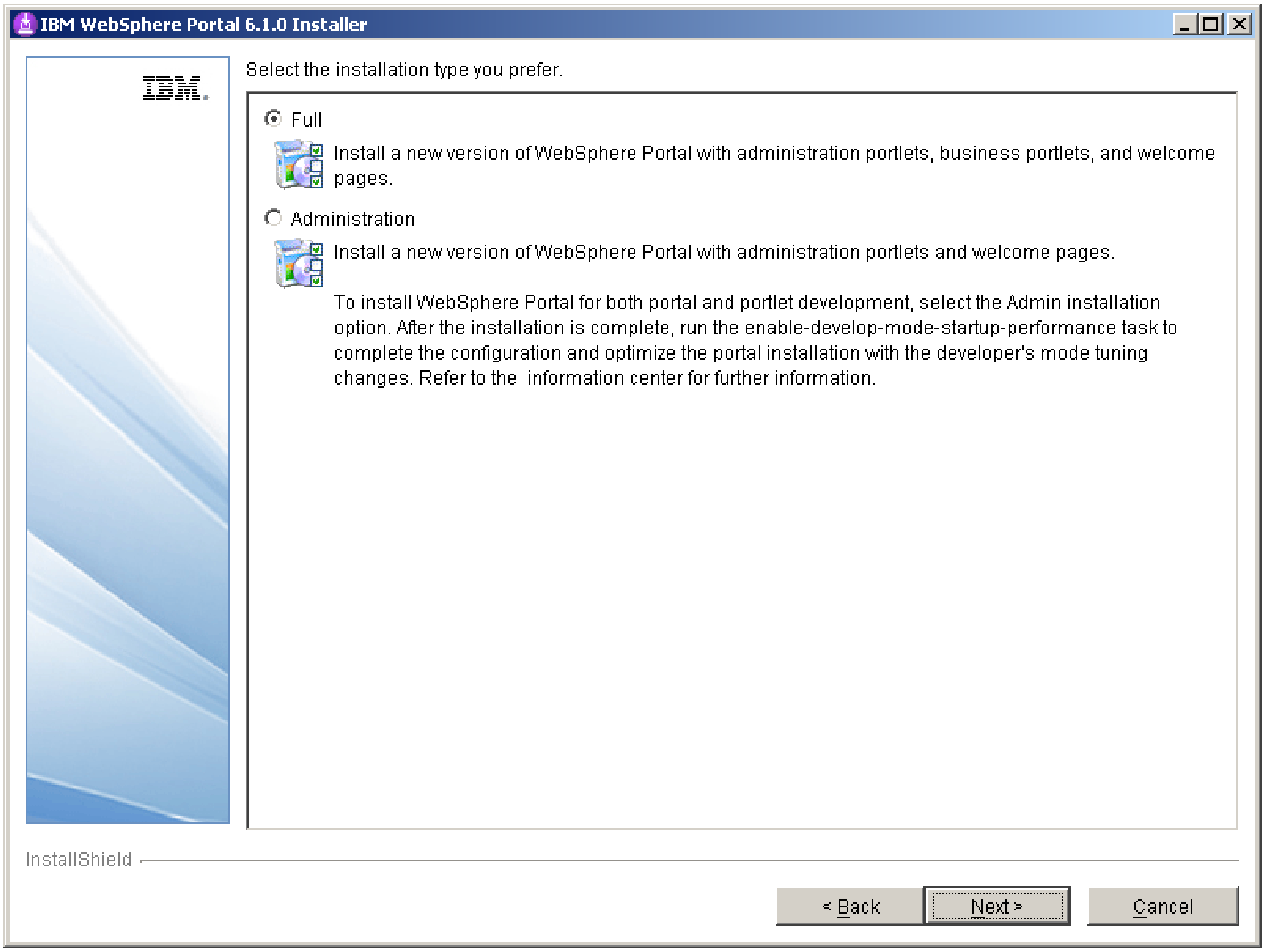
"Program" is the following, including the original and all whole or partial copies: 1) machine-readable

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

6. On the installation type screen, select 'Full' and click 'Next'

   NOTE: Select Administration to install only administrative portlets.



Select the installation type you prefer.

● Full

Install a new version of WebSphere Portal with administration portlets, business portlets, and welcome pages.

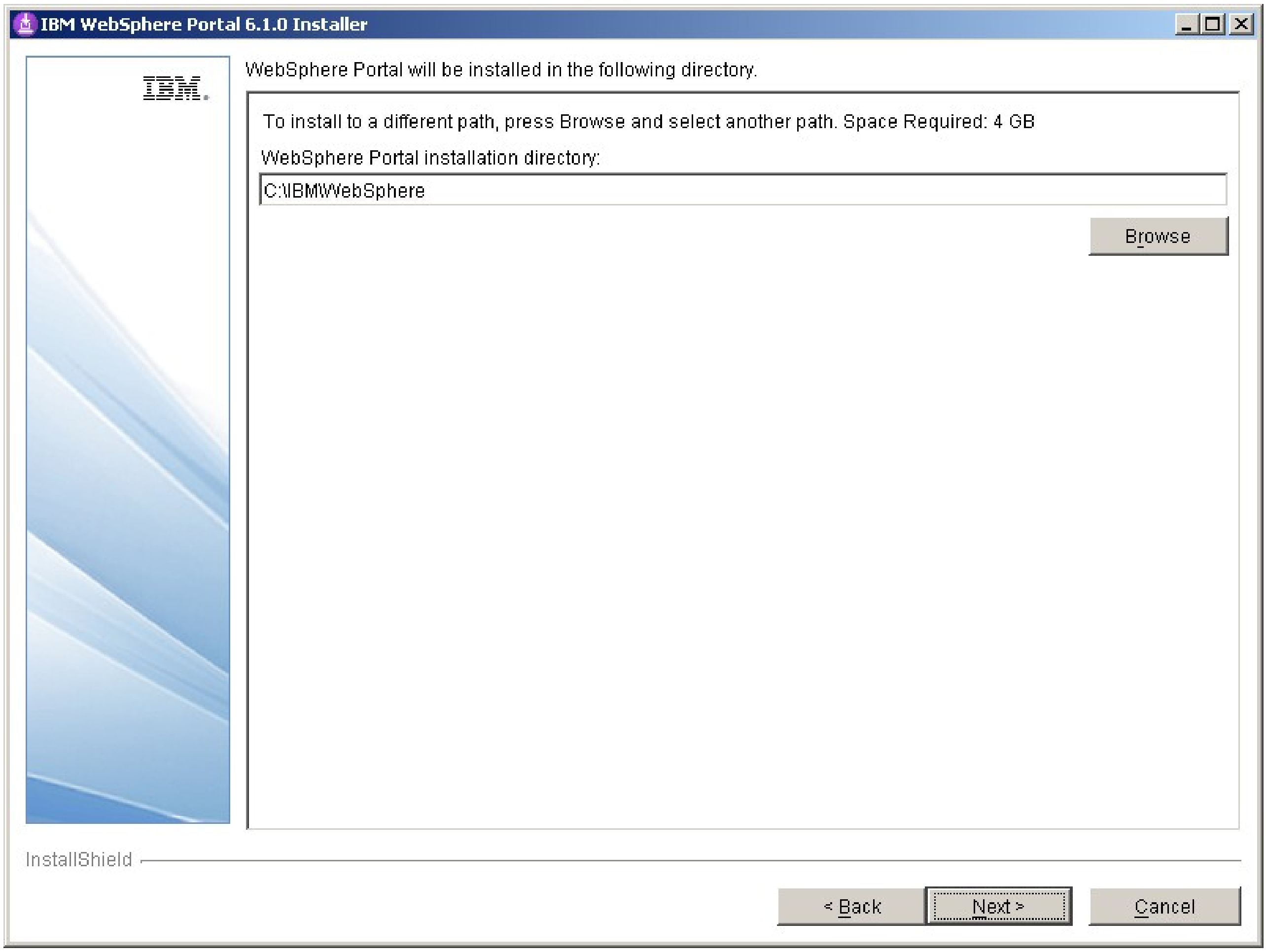
○ Administration

Install a new version of WebSphere Portal with administration portlets and welcome pages.

To install WebSphere Portal for both portal and portlet development, select the Admin installation option. After the installation is complete, run the enable-develop-mode-startup-performance task to complete the configuration and optimize the portal installation with the developer's mode tuning changes. Refer to the information center for further information.

7. Select the desired path for the WebSphere directory and click 'Next'

   NOTE: Both the AppServer directory and the PortalServer directory will be created in this WebSphere directory.
   NOTE: Ensure that the desired path does not already exist in your environment. The Portal installer will create it for you.



WebSphere Portal will be installed in the following directory.

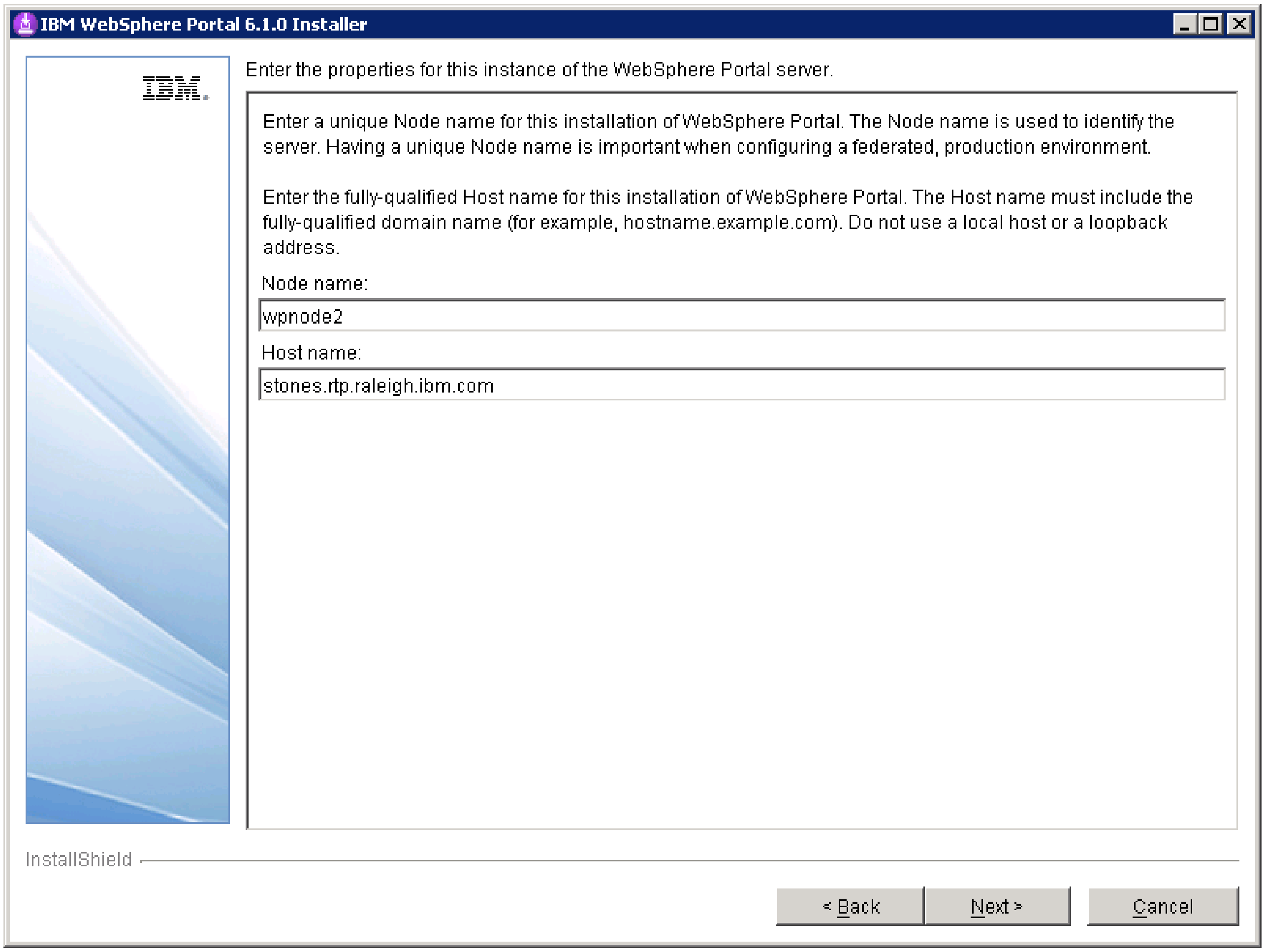
To install to a different path, press Browse and select another path. Space Required: 4 GB

WebSphere Portal installation directory:

C:\IBMWebSphere

8. Enter a node name and the fully qualified hostname of your server and click 'Next'

   NOTE: The node name will also be used as the cell name in the standalone environment.



Enter the properties for this instance of the WebSphere Portal server.

Enter a unique Node name for this installation of WebSphere Portal. The Node name is used to identify the server. Having a unique Node name is important when configuring a federated, production environment.

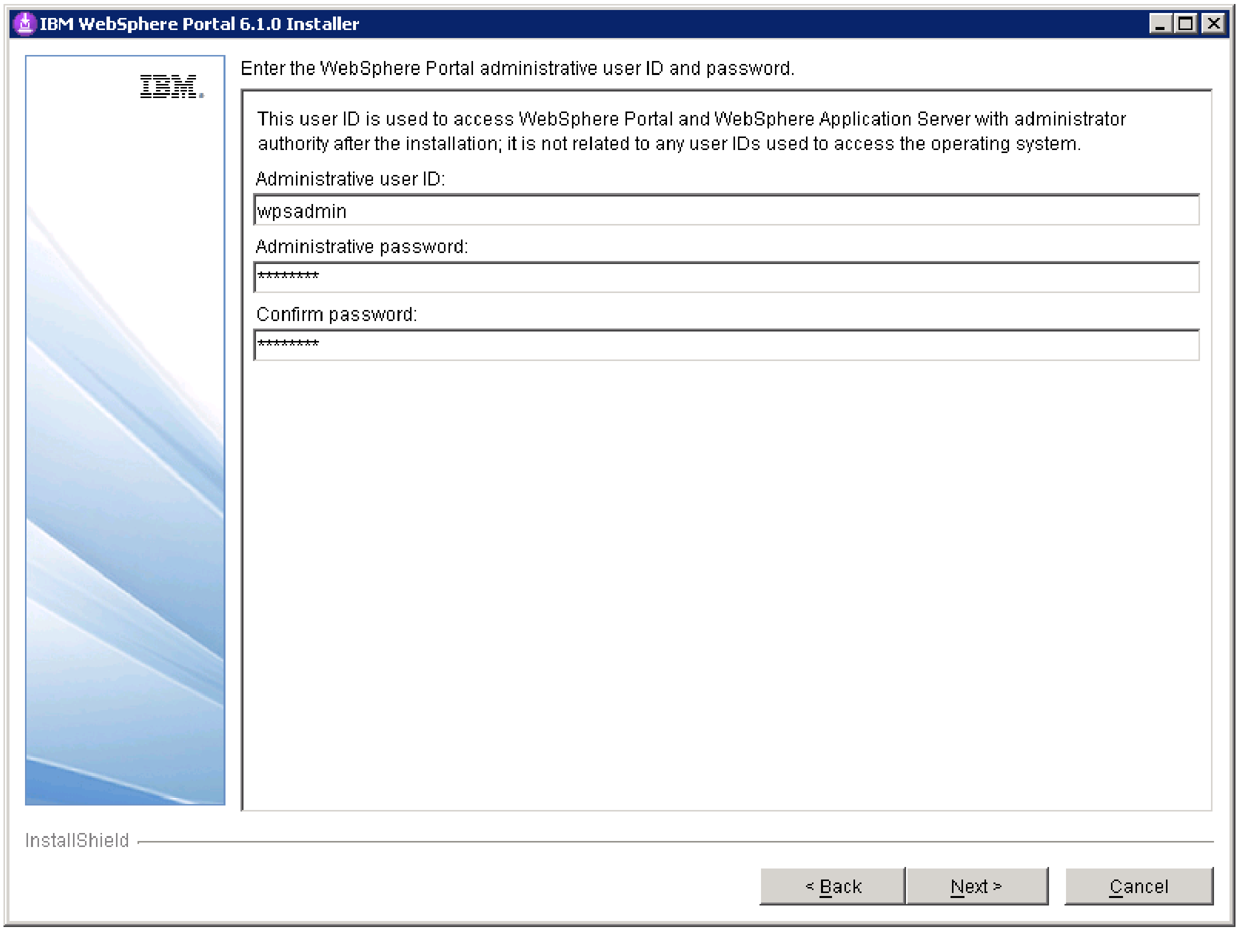
Enter the fully-qualified Host name for this installation of WebSphere Portal. The Host name must include the fully-qualified domain name (for example, hostname.example.com). Do not use a local host or a loopback address.

Node name: wpnode2

Host name: stones.rtp.raleigh.ibm.com

9. Security is enabled for Portal by default. Enter a user ID and password you wish to use. This ID will be used to access both server1 and WebSphere_Portal after installation completes.

   IMPORTANT: Use the same Portal Admin ID that you used in steps 21 from the Deployment Manager installation section.



Enter the WebSphere Portal administrative user ID and password.

This user ID is used to access WebSphere Portal and WebSphere Application Server with administrator authority after the installation; it is not related to any user IDs used to access the operating system.

Administrative user ID: wpsadmin

Administrative password: ********

Confirm password: ********

10. **Windows** only. Do NOT check the box to use Windows services. Click 'Next'

11. Verify the information is accurate in the summary screen and click 'Next' to begin the installation.

12. Once the installation finishes, uncheck Launch First Steps and Launch the Configuration Wizard. Click 'Finish'

13. Verify you can access Portal in a web browser. The default URL is:

    http://yourserver.yourcompany.com:10040/wps/portal

Install IBM Support Assistant Lite

In this section, you will install IBM Support Assistant Lite for WebSphere Portal (ISALite). This step is optional but **highly** recommended. ISALite provides automatic log collection and symptom analysis support for WebSphere Portal problem determination scenarios. Installing this tool now can save you time in the future if you have any problems with WebSphere Portal that require you to contact support.

1. Visit the website below and download ISALite for WebSphere Portal v6.1 to a temporary directory:

   http://www-01.ibm.com/support/docview.wss?rs=688&uid=swg24008662

2. Extract the downloaded zip file into the wp_profile/PortalServer directory. This will create a directory called ISALite.

3. The tool is installed and ready for use. If you have an issue with WebSphere Portal that requires support, instructions for using this tool can be found in Appendix D.

Federate and Cluster the Secondary Portal node

This section covers adding the secondary node to the Deployment Manager cell and adding its WebSphere_Portal server as a secondary member to the previously created cluster. Once this section is completed, you will have a functional two-node cluster using the default VMM security configuration and configured to an external database.

1. Ensure the database client is installed and configured on the secondary node. For DB2 with Type 4 drivers, copy the db2jcc.jar and db2jcc_license_cu.jar files from the DB2 server to some directory on the secondary Portal server.
2. From the <wp_profile>/ConfigEngine/properties directory, make a backup of the following files:

   wkplc.properties
   wkplc_dbtype.properties
   wkplc_comp.properties

3. Copy the wkplc_comp.properties and wkplc_dbtype.properties from Node1 to Node2 to ensure the same database configuration.

   NOTE: Ensure that the value of db2.DbLibrary in wkplc_dbtype.properties contains valid directory paths for this node.

4. From the <wp_profile>/ConfigEngine/properties directory, edit the wkplc.properties file and change the following entries:

   ```
   WasPassword=<standalone WAS password>
   PortalAdminPwd=password
   WasRemoteHostName=<fully qualified hostname of DMGR>
   WasSoapPort=<soap port for DMGR; default is 8879>
   PrimaryNode=false
   ClusterName=PortalCluster
   ```

   NOTE: Ensure that the value for ClusterName matches the value for ClusterName on the primary node.

5. In a command window from the secondary node, change directories to <wp_profile>/ConfigEngine

6. Add the node to the deployment manager cell by executing the following ConfigEngine script:

   ```
   ConfigEngine.bat cluster-node-config-pre-federation
   -DDMgrUserid=uid=<dmgr user id>,o=defaultWIMFileBasedRealm
   -DDMgrPassword=<dmgr password>
   ```

   For example:

   ```
   ConfigEngine.bat cluster-node-config-pre-federation
   -DDMgrUserid=uid=wasadmin,o=defaultWIMFileBasedRealm -DDMgrPassword=wasadmin
   ```

   IMPORTANT FOR PORTAL 6.1.0.3 OR HIGHER: This step does NOT apply to Portal v6.1.0.3+. The -DDMgrUserid and -DDMgrPassword properties are no longer used in 6.1.0.3. Instead you must do the following:

   - Update wkplc.properties and change WasUserid and WasPassword to the DMGR user ID values.
   - Run the ConfigEngine script as follows, without the DmgrUserid and DMgrPassword:

     ```
     ConfigEngine.bat cluster-node-config-pre-federation
     ```

   NOTE: Ensure that the time on the Deployment Manager server and the time on the primary node are within 5 minutes of each other. Failure to do so can cause this step to fail. This will also create the NodeAgent server for you on your node.

   NOTE: If you are prompted to accept an SSL certificate, type Y and press Enter to continue

   NOTE: If you specify the -DDMgrUserid parameter when running the `cluster-node-config-pre-federation` task, it resets the WasUserid parameter in the wkplc.properties file to the -DDMgrUserid value.

7. After the previous step completes, your node will be part of the deployment manager cell. As a result, this node is now using the Deployment Manager security configuration and cell name. The original WAS ID that had been used in the standalone environment will no longer be used.

   Edit the <wp_profile>/ConfigEngine/properties/wkplc.properties file and ensure the following properties are set correctly:

   ```
   WasUserId=<dmgr admin user>
   WasPassword=<dmgr password>
   CellName=<dmgr cell name>
   ```

8. Update the deployment manager configuration for the new WebSphere Portal server by executing the following ConfigEngine script:

   ```
   ConfigEngine.bat cluster-node-config-post-federation
   ```

9. Ensure the NodeAgent is started on this node:

   ```
   <wp_profile>/bin/startNode.bat
   ```

10. Specify the name of the future secondary cluster member.

    Edit the <wp_profile>/ConfigEngine/wkplc.properties file and change the following property:

    ```
    ServerName=<name of new cluster member>
    ```

    NOTE: When you open the properties file, you should see WebSphere_Portal_*nodename*. You can use this value if you like. Otherwise you can change this to anything EXCEPT 'WebSphere_Portal'. DO NOT use the value of 'WebSphere_Portal' for your secondary cluster member.

11. Add this newly federated WebSphere_Portal server as a cluster member to the existing cluster by executing the following ConfigEngine script:

    ```
    ConfigEngine.bat cluster-node-config-cluster-setup
    ```

    NOTE: This will automatically add a secondary cluster member to your existing cluster based on whatever value you set for ServerName in step 10. In this example, the default value was used. The node name is wpnode2 so our cluster member will be called WebSphere_Portal_wpnode2.

12. Allow **30 minutes** for ear expansion to complete on the secondary node. Failure to do so may result in several applications being unavailable on this node.

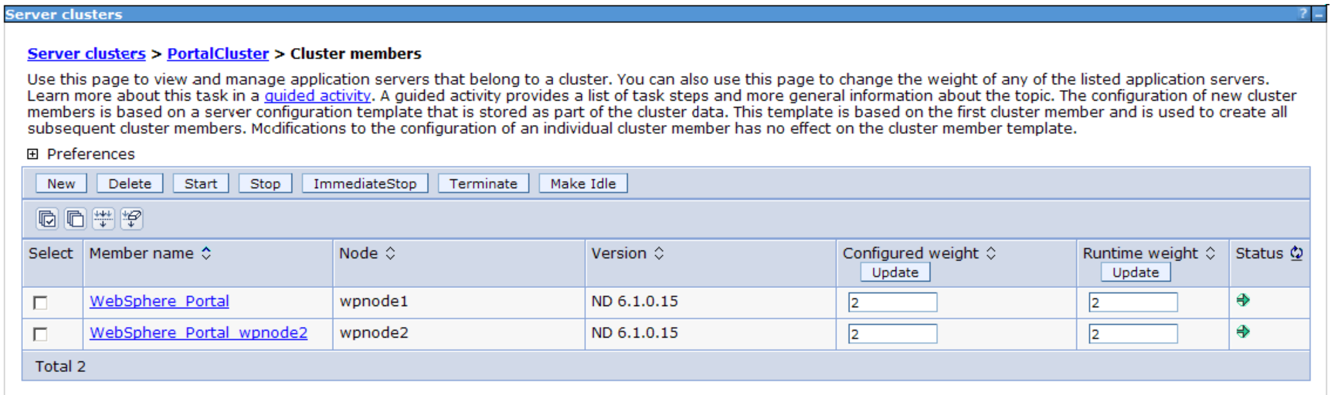
13. Start the new cluster member WebSphere_Portal_*nodename*:

    ```
    <wp_profile>/bin/startServer.bat WebSphere_Portal_nodename
    ```

14. To verify that the cluster was created successfully, log in to the DMGR Administrative Console and browse to:

```
Servers -> Cluster -> ClusterName -> Cluster Members
```

An entry for WebSphere_Portal_*nodename* should be available.



Server clusters > PortalCluster > Cluster members

Use this page to view and manage application servers that belong to a cluster. You can also use this page to change the weight of any of the listed application servers. Learn more about this task in a guided activity. A guided activity provides a list of task steps and more general information about the topic. The configuration of new cluster members is based on a server configuration template that is stored as part of the cluster data. This template is based on the first cluster member and is used to create all subsequent cluster members. Mcdifications to the configuration of an individual cluster member has no effect on the cluster member template.

⊞ Preferences

Select	Member name	Node	Version	Configured weight Update	Runtime weight Update	Status
□	WebSphere_Portal	wpnode1	ND 6.1.0.15	2	2	➔
□	WebSphere_Portal_wpnode2	wpnode2	ND 6.1.0.15	2	2	➔
Total 2						

NOTE: In this example, the WebSphere_Portal_wpnode2 server is a new server in this configuration. The original WebSphere_Portal server from the secondary node gets removed during the cluster-node-config-cluster-setup ConfigEngine script. As a result, new port numbers have been assigned to the WebSphere_Portal_*nodename* server. To check what ports are in use with this server, navigate to:

```
Servers -> Application Servers -> WebSphere_Portal_nodename -> Ports
```

The WC_defaulthost is the port used to access Portal. The default port in this case is 10048.

If you need to change these port numbers, you can do so from this screen. Alternatively, ConfigEngine scripts are provided to modify port numbers. Details can be found in Step 8 of the Information Center instructions found here (note this link is for Windows, but the same steps will apply to all Operating Systems):

http://publib.boulder.ibm.com/infocenter/wpdoc/v6r1m0/index.jsp?topic=/com.ibm.wp.ent.doc_v6101/install/stdalone_win_inst_wp.html

15. Verify functionality of the secondary node by accessing it in a web browser:

http://mycompany.myserver.com:10048/wps/portal

Configure the Portal Cluster for Security

This section covers changing the security configuration from the default user registry to a standalone LDAP Server. For more details about LDAP/Security configuration, please refer to the Information Center:

http://publib.boulder.ibm.com/infocenter/wpdoc/v6r1m0/index.jsp?topic=/com.ibm.wp.ent.doc/install/win_cfg_wp_ureg.html

In Portal v6.1, security configuration has changed significantly. There is no more disable-security script. Instead, a single ConfigEngine script is executed to change from one user registry to another, or to update an existing user registry. There are several different options for security configuration and we encourage you to review all options in the Information Center from the link above to determine what is best for your environment.

In this guide, we will configure security in our cluster to a standalone ldap server using IBM Tivoli Directory Server v6.0.

3. From the primary node, edit the wp_security_ids.properties file in the <wp_profile>/ConfigEngine/config/helpers directory.
4. Modify the values in this helper file to match your LDAP configuration. The values used in this guide are listed in Appendix A of this Guide.
5. From a command window, change directories to the <wp_profile>/ConfigEngine directory and execute the following ConfigEngine script to validate the properties:

   ```
   ConfigEngine.bat validate-standalone-ldap
   -DparentProperties=<wp_profile>/ConfigEngine/config/helpers/wp_security_ids.p
   roperties -DsaveParentProperties=true
   ```

   NOTE: By using the `-DparentProperties=<wp_profile>/ConfigEngine/config/helpers/wp_security_ids.properties -DsaveParentProperties=true` flags, ConfigEngine will automatically save the properties from the helper file into the wkplc.properties file.
6. Execute the following ConfigEngine script to modify the security settings from the default VMM file security settings to the new LDAP settings:

   ```
   ConfigEngine.bat wp-modify-ldap-security
   ```

   NOTE: This script will automatically change WasUserId, PortalAdminId and PortalAdminGroupId in wkplc.properties to match that of standalone.ldap.primaryAdminId, standalone.ldap.primaryPortalAdminId, and standalone.ldap.primaryPortalAdminGroup.

7. Restart the DMGR, all NodeAgents, and all Cluster Members.

8. Copy the wp_security_ids.properties from the <wp_profile>/ConfigEngine/config/helpers directory on your Primary node to the <wp_profile>/ConfigEngine/config/helpers directory on the secondary node.

9. From the secondary node, copy the contents of the helper file into the main wkplc.properties file by running the following command (all on one line):

   ```
    ConfigEngine.bat
   -DparentProperties=<wp_profile>/ConfigEngine/config/helpers/wp_security_ids.p
   roperties -DsaveParentProperties=true
   ```

10. In the wkplc.properties on the secondary node, edit WasUserid and WasPassword to reflect your new LDAP values if they are not already set.

11. Update the Portal security information on the secondary node by executing the following ConfigEngine script from the <wp_profile>/ConfigEngine directory on your secondary node:

    ```
    ConfigEngine.bat wp-change-portal-admin-user -DnewAdminId=<full DN of Portal
    admin ID> -DnewAdminPwd=<new password> -DnewAdminGroupId=<full DN of Portal
    Admin Group ID> -Dskip.ldap.validation=true
    ```

    Note: The -Dskip.ldap.validation=true flag can be used if the script fails during ldap validation.

12. Restart the secondary node's WebSphere_Portal server by executing the following commands from the <wp_profile>/bin directory on the secondary node:

    ```
    stopServer.bat WebSphere_Portal_nodename -user <WAS user ID> -password
    password
    startServer.bat WebSphere_Portal_nodename
    ```

Configure the Portal cluster with an external web server

This section describes how to configure the Portal cluster with an external web server. For more details about web server configuration, please visit the WebSphere Application Server Information Center at this link:

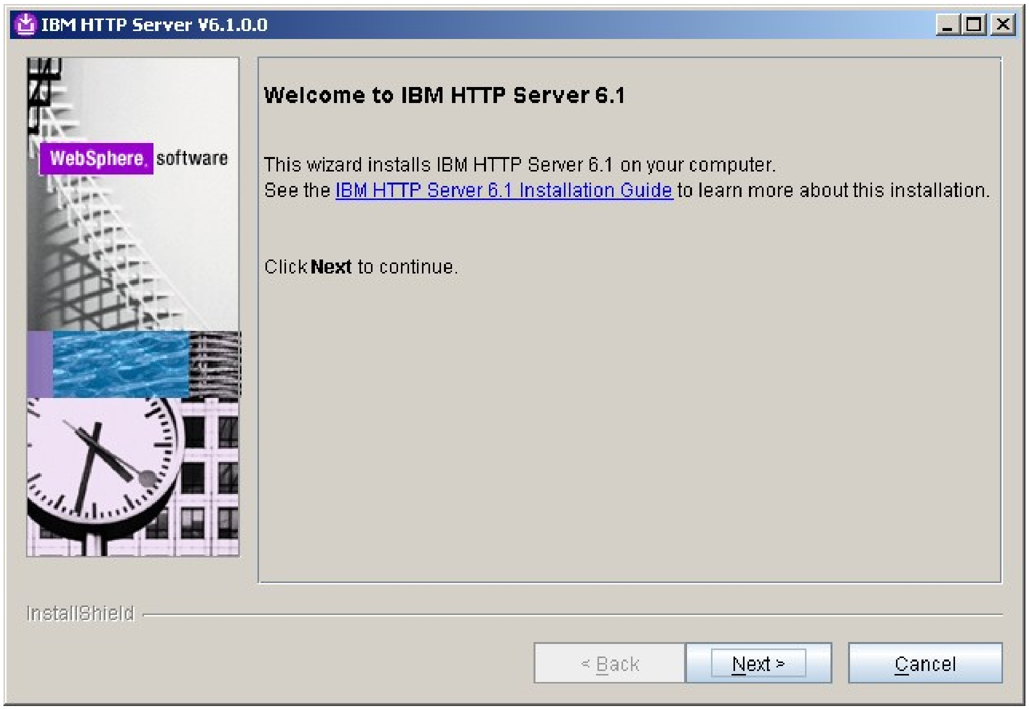
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?
topic=/com.ibm.websphere.base.doc/info/aes/ae/tins_road_plugins.html

In this guide, we will configure the Portal cluster with IBM HTTP Server v6.1.

1. From CD W-15, navigate to \IHS\ and run install.exe.

   NOTE: The CD that contains the IHS installer will vary on each operating system. The title of the CD is Edge Components for "WebSphere Application Server Network Deployment".

2. On the Welcome screen, click Next.

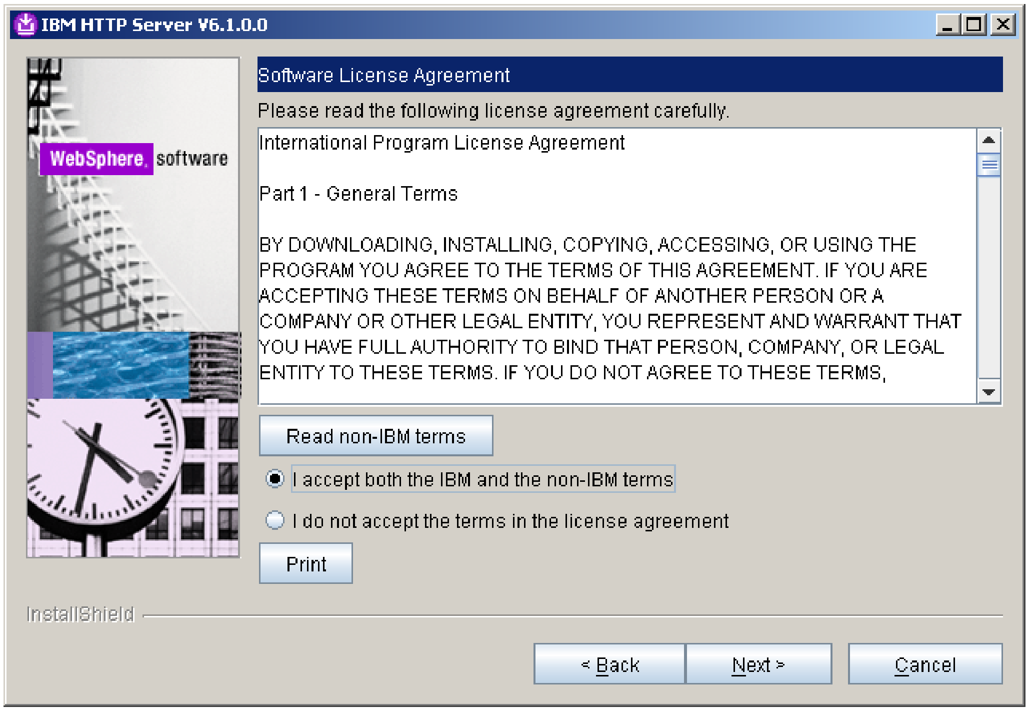


Welcome to IBM HTTP Server 6.1

This wizard installs IBM HTTP Server 6.1 on your computer.
See the IBM HTTP Server 6.1 Installation Guide to learn more about this installation.

Click **Next** to continue.

3. Accept the license agreement and click Next.



Software License Agreement

Please read the following license agreement carefully.

International Program License Agreement

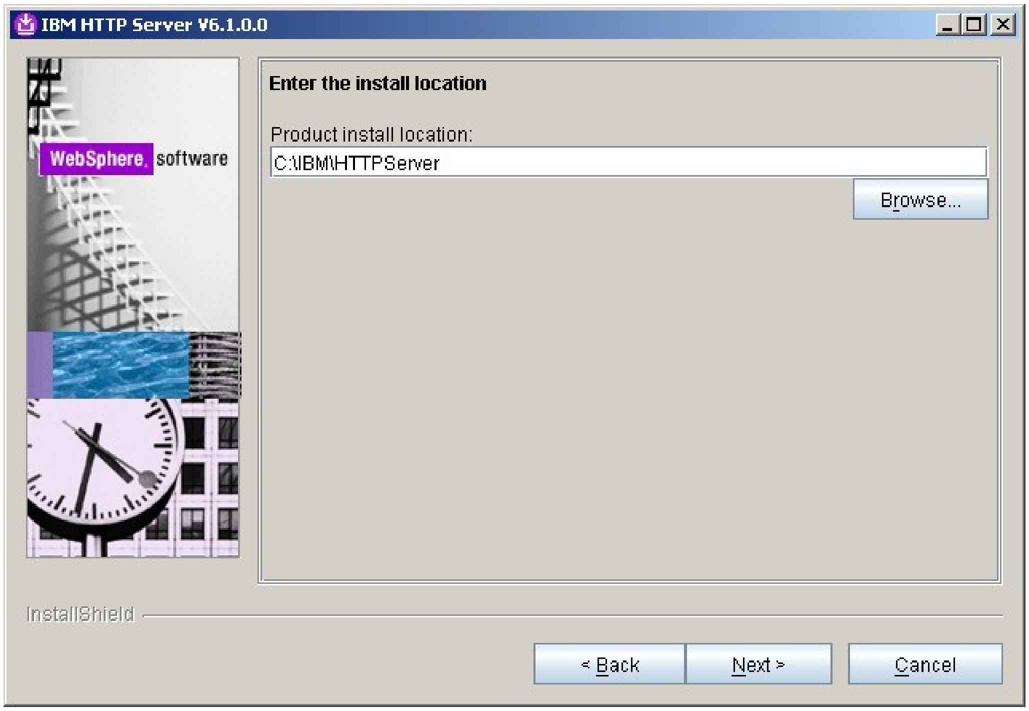
Part 1 - General Terms

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

● I accept both the IBM and the non-IBM terms

○ I do not accept the terms in the license agreement

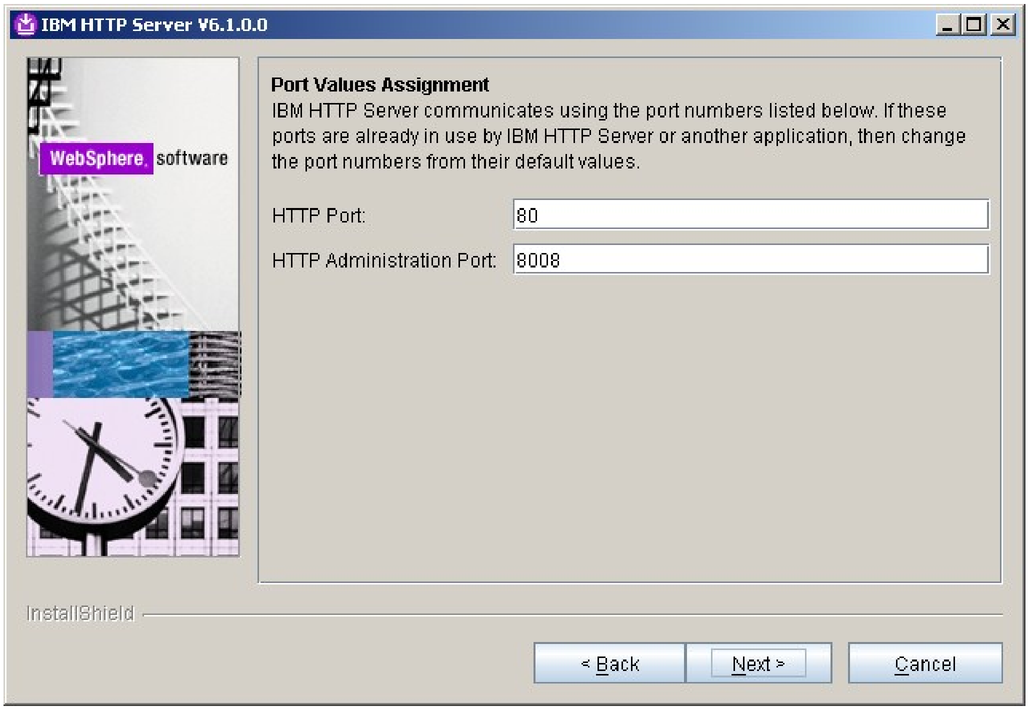
4. Select the installation path for the web server and click Next.



Enter the install location

Product install location: C:\IBM\HTTPServer

5. Change the port numbers if needed and click Next.



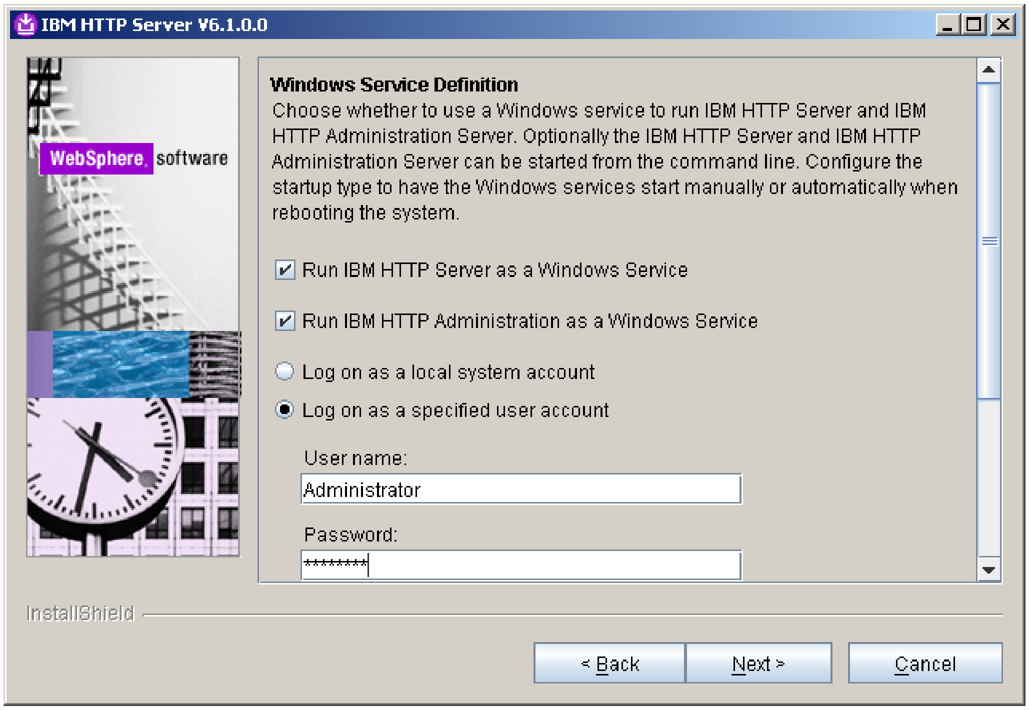
Port Values Assignment

IBM HTTP Server communicates using the port numbers listed below. If these ports are already in use by IBM HTTP Server or another application, then change the port numbers from their default values.

HTTP Port: 80

HTTP Administration Port: 8008

6. **Windows only.** Run the web server as a windows service if you'd like and click Next.



Windows Service Definition

Choose whether to use a Windows service to run IBM HTTP Server and IBM HTTP Administration Server. Optionally the IBM HTTP Server and IBM HTTP Administration Server can be started from the command line. Configure the startup type to have the Windows services start manually or automatically when rebooting the system.

☑ Run IBM HTTP Server as a Windows Service

☑ Run IBM HTTP Administration as a Windows Service

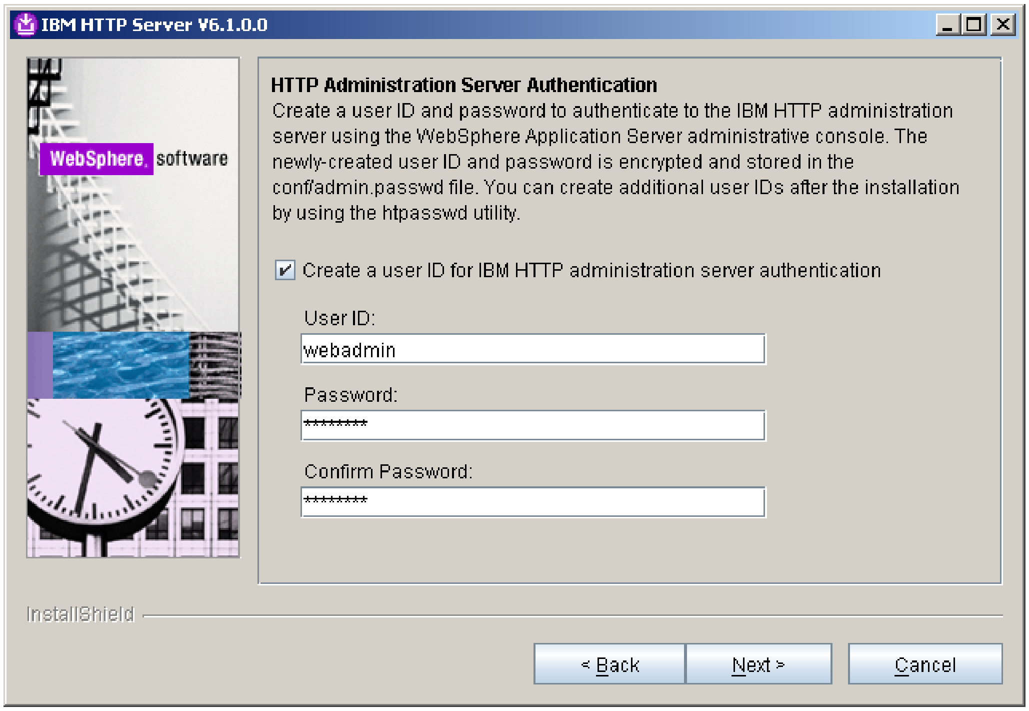
○ Log on as a local system account

● Log on as a specified user account

User name: Administrator

Password: ********

7. Create a user ID and password to be used for authentication to the IBM HTTP Administration server and click Next.



HTTP Administration Server Authentication

Create a user ID and password to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. The newly-created user ID and password is encrypted and stored in the conf/admin.passwd file. You can create additional user IDs after the installation by using the htpasswd utility.

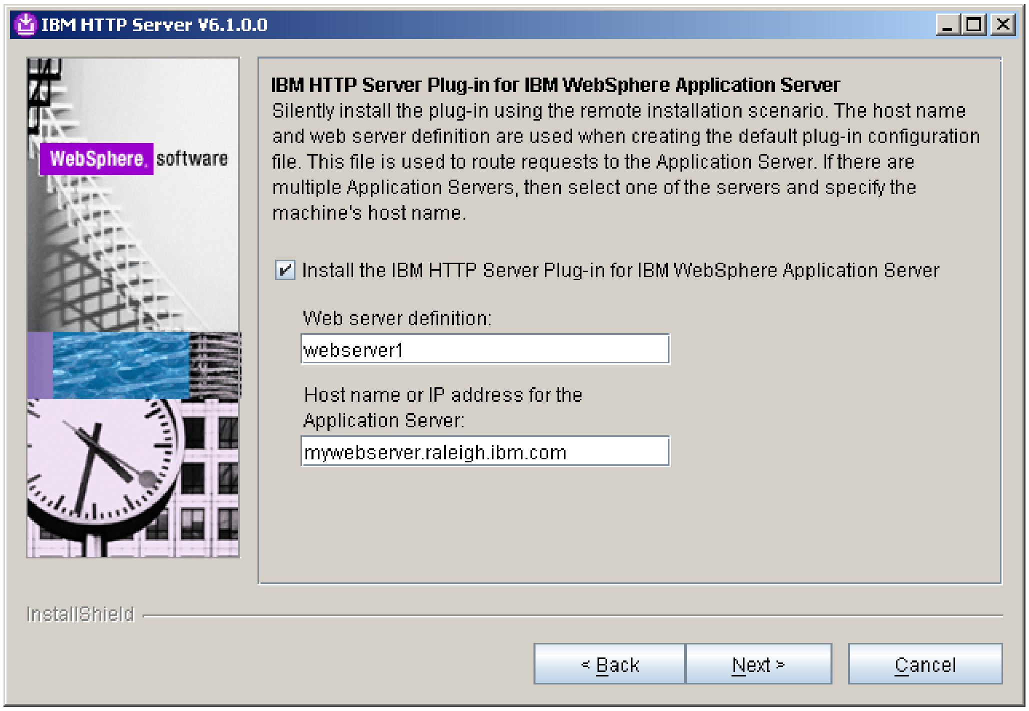
☑ Create a user ID for IBM HTTP administration server authentication

User ID: webadmin

Password: ********

Confirm Password: ********

8. Select the checkbox to install the Web Server plugin as part of the Web Server installation. Select a web server definition value and ensure the hostname is correct for this server. Click Next.



IBM HTTP Server Plug-in for IBM WebSphere Application Server

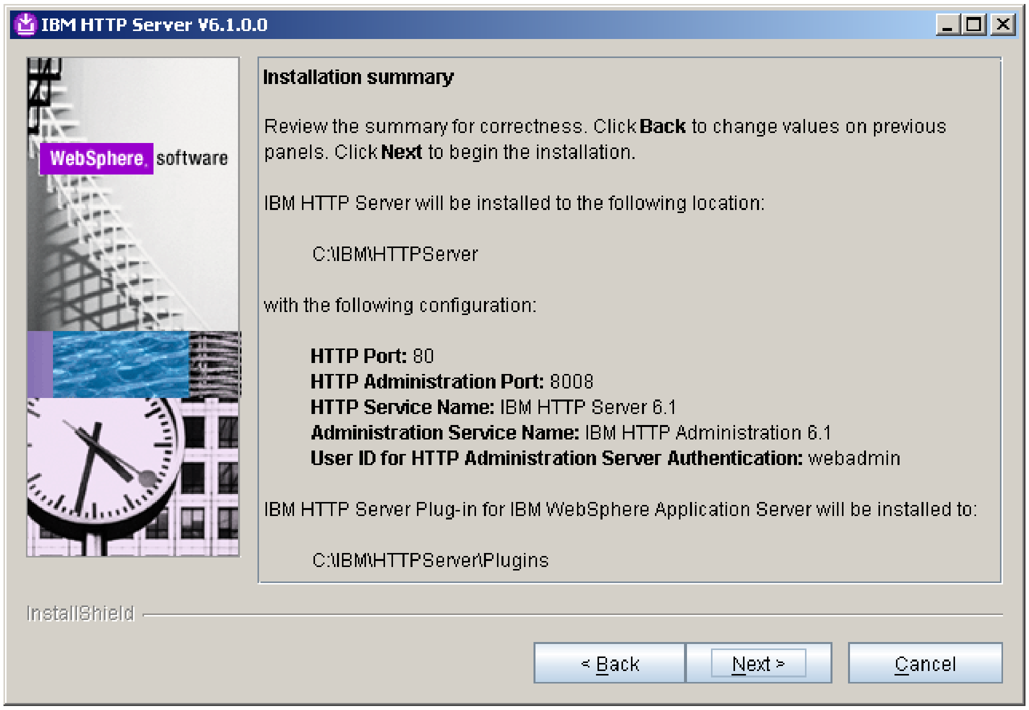
Silently install the plug-in using the remote installation scenario. The host name and web server definition are used when creating the default plug-in configuration file. This file is used to route requests to the Application Server. If there are multiple Application Servers, then select one of the servers and specify the machine's host name.

☑ Install the IBM HTTP Server Plug-in for IBM WebSphere Application Server

Web server definition: webserver1

Host name or IP address for the Application Server: mywebserver.raleigh.ibm.com

9. On the summary screen, ensure everything is correct and click Next to begin the installation.



Installation summary

Review the summary for correctness. Click **Back** to change values on previous panels. Click **Next** to begin the installation.

IBM HTTP Server will be installed to the following location:

C:\IBM\HTTPServer

with the following configuration:

HTTP Port: 80
HTTP Administration Port: 8008
HTTP Service Name: IBM HTTP Server 6.1
Administration Service Name: IBM HTTP Administration 6.1
User ID for HTTP Administration Server Authentication: webadmin

IBM HTTP Server Plug-in for IBM WebSphere Application Server will be installed to:

C:\IBM\HTTPServer\Plugins

10. Once the installation finishes, click Finish to exit the installer.
11. Navigate to <plugin root>/bin and find the configure*webservername*.bat script where *webservername* is the web server definition name you defined on step 8. In this case, we used webserver1 so our script is called:

    configurewebserver1.bat

12. Copy the configurewebserver1.bat script from the <plugin root>/bin directory to the <dmgr_profile>/bin directory on your Deployment Manager server.
13. Ensure that the DMGR is running.
14. In a command line from the <dmgr_profile>/bin directory, run the following command:

    configurewebserver1.bat -user <was_admin_user> -password password

    NOTE: This script will create the web server definition in the DMGR configuration and map all of the installed applications to the web server.

15. Regenerate the web server plugin by performing the following steps:
    1. Login to the DMGR Admin Console
    2. Navigate to Servers -> Web Servers
    3. Select the Checkbox for the new web server definition
    4. Click the "Generate Plug-in" button

    NOTE: This will be written to the <dmgr_profile>/config/cells/<cellname>/nodes/<nodename>/servers/webserver1/plugin-cfg.xml file.

16. Copy the plugin-cfg.xml file to the remote web server at the following directory, overwriting the existing one:

    <plugin_root>/config/webserver1

17. Restart the DMGR, web server, and cluster.

18. Verify that you can access the Portal cluster via the web server:

    http://mywebserver.hostname.com/wps/portal

Conclusion

In this guide, you saw how to build a fully functional WebSphere Portal v6.1 cluster using an external database and a LDAP for security. You also saw how to configure a web server to allow for load balancing.

Appendix A – Properties used for LDAP security

The following properties were used in the wp_security_ids.properties file to configure the Portal Cluster used in this guide with IBM Tivoli Directory Server.

```
###############################################################################
###############################################################################
##
##
## VMM Stand-alone LDAP configuration
## wp-modify-ldap-security
## wp-update-standalone-ldap
##
## IDS, SECUREWAY
##
###############################################################################
###############################################################################


# The id specifies a unique identifier for the repository within the cell
# Characters that are not allowed in normal XML strings ( &  <   >  "   '   )
cannot be used in the repository ID.
standalone.ldap.id=ClusterLdap


# Specifies the host name of the primary LDAP server. This host name is either an
IP address or a domain name service (DNS) name.
standalone.ldap.host=myldapserver.raleigh.ibm.com


# Specifies the LDAP server port.
standalone.ldap.port=389


# Specifies the distinguished name for the application server to use when binding
to the LDAP repository.
standalone.ldap.bindDN=uid=wpsbind,cn=users,dc=ibm,dc=com


# Specifies the password for the application server to use when binding to the LDAP
repository.
```

```
standalone.ldap.bindPassword=wpsbind


# Specifies the type of LDAP server to which you connect

# Supported values: IDS4, IDS51, IDS52, IDS6, SECUREWAY

# Note: If your LDAP server version is not listed, enter the value for the highest
listed version of your server

standalone.ldap.ldapServerType=IDS6


# Specifies the LDAP filter that maps the short name of a user to an LDAP entry.

# For example, to display entries of the object class = inetOrgPerson type by their
IDs, specify inetOrgPerson:uid.

# This field takes multiple objectclass:property pairs delimited by a semicolon
(;).

# note: not used during node federation to DMGR with WAS ldap security enabled

standalone.ldap.userIdMap=*:uid


# Specifies the LDAP filter that maps the short name of a group to an LDAP entry.

# Specifies the piece of information that represents groups when groups display.
For example, to display groups by their names, specify *:cn.

# The asterisk (*) is a wildcard character that searches on any object class in
this case.

# This field takes multiple objectclass:property pairs, delimited by a semicolon
(;).

# note: not used during node federation to DMGR with WAS ldap security enabled

standalone.ldap.groupIdMap=*:cn


# Specifies the LDAP filter that identifies user-to-group relationships.

# Specifies which property of an objectclass stores the list of members belonging
to the group represented by the objectclass.

# For directory types SecureWay, and Domino, this field takes multiple
objectclass:property pairs, delimited by a semicolon (;).

# For IBM Directory Server, Sun ONE, and Active Directory, this field takes
multiple group attribute:member attribute pairs delimited by a semicolon (;).

# For more information about this syntax, see the LDAP directory service
documentation.

# note: not used during node federation to DMGR with WAS ldap security enabled

standalone.ldap.groupMemberIdMap=ibm-allGroups:member;ibm-allGroups:uniqueMember


# Specifies the LDAP user filter that searches the user registry for users.

# For example, to look up users based on their user IDs, specify (%(uid=%v)
(objectclass=inetOrgPerson))
```

```
# note: not used during node federation to DMGR with WAS ldap security enabled
standalone.ldap.userFilter=(&(uid=%v)(objectclass=inetOrgPerson))

# Specifies the LDAP group filter that searches the user registry for groups.
# note: not used during node federation to DMGR with WAS ldap security enabled
standalone.ldap.groupFilter=(&(cn=%v)(objectclass=groupOfUniqueNames))

# Specifies a user ID and password in the repository that is used for internal
process communication.
# note: not used during node federation to DMGR with WAS ldap security enabled
standalone.ldap.serverId=uid=wpsbind,cn=users,dc=ibm,dc=com
standalone.ldap.serverPassword=wpsbind

# The security context of this server. A realm with this name will be created.
standalone.ldap.realm=PortalRealm



# The ID of the WAS admin user. The ID must exist in the LDAP server.
standalone.ldap.primaryAdminId=uid=wpsbind,cn=users,dc=ibm,dc=com
standalone.ldap.primaryAdminPassword=wpsbind

# The ID of the portal admin user. The ID must exist in the LDAP server.
standalone.ldap.primaryPortalAdminId=uid=wpadmin,cn=users,dc=ibm,dc=com
standalone.ldap.primaryPortalAdminPassword=wpadmin

# The user group with admin permission in portal. The group must exist in the LDAP
server.
standalone.ldap.primaryPortalAdminGroup=cn=wpsadmins,cn=groups,dc=ibm,dc=com

# The LDAP base entry.
# This is the startpoint for all LDAP searches of Websphere Application Server
Security
standalone.ldap.baseDN=dc=ibm,dc=com

########################
##
## LDAP entity types
##
```

```
########################

# Entity type Group

# The search filter that you want to use to search the entity type.
# VMM uses this filter as an addition during search requests in your environment
# The syntax is like a standard LDAP searchfilter like
(objectclass=groupOfUniqueNames)
# In general this value can be left blank
standalone.ldap.et.group.searchFilter=objectclass=groupOfUniqueNames

# One or more object classes for the entity type.
standalone.ldap.et.group.objectClasses=groupOfUniqueNames

# The object class to use when an entity type is created. If the value of this
parameter is the same as the objectClass parameter, you do not need to specify this
parameter.
standalone.ldap.et.group.objectClassesForCreate=

# The search base or bases to use while searching the entity type.
standalone.ldap.et.group.searchBases=cn=groups,dc=ibm,dc=com


# Entity type PersonAccount

# The search filter that you want to use to search the entity type.
# VMM uses this filter as an addition during search requests in your environment
# The syntax is like a standard LDAP searchfilter like (objectclass=inetOrgPerson)
# In general this value can be left blank
standalone.ldap.et.personaccount.searchFilter=objectclass=inetOrgPerson

# One or more object classes for the entity type.
# Please check this value with the objectclass used in your LDAP for type User
standalone.ldap.et.personaccount.objectClasses=inetOrgPerson

# The object class to use when an entity type is created. If the value of this
parameter is the same as the objectClass parameter, you do not need to specify this
parameter.
standalone.ldap.et.personaccount.objectClassesForCreate=
# The search base or bases to use while searching the entity type.

standalone.ldap.et.personaccount.searchBases=cn=users,dc=ibm,dc=com


########################

##

## End LDAP entity types

##

########################


###################################################

##

## Group member attributes

##

###################################################


# The name of the LDAP attribute that is used as the group member attribute. For example, member or uniqueMember.

standalone.ldap.gm.groupMemberName=uniqueMember


# The group object class that contains the member attribute. For example, groupOfNames or groupOfUnqiueNames.

# If you do not define this parameter, the member attribute applies to all group object classes.

standalone.ldap.gm.objectClass=groupOfUniqueNames


# The scope of the member attribute. The valid values for this parameter include the following:

# direct - The member attribute only contains direct members.

# nested - The member attribute that contains the direct members and the nested members.

standalone.ldap.gm.scope=direct


# If you create a group without specifying a member, a dummy member will be filled in to avoid creating an exception about missing a mandatory attribute.

standalone.ldap.gm.dummyMember=uid=dummy



###############################
```

```
# Default parent, RDN attribute
###############################

# The default parents to be set for the the entity types PersonAccount and Group
standalone.ldap.personAccountParent=cn=users,dc=ibm,dc=com
standalone.ldap.groupParent=cn=groups,dc=ibm,dc=com

# The RDN attribute names for the entity types PersonAccount and Group
# To reset all the values of the rdnProperties parameter, specify a blank string
("").
standalone.ldap.personAccountRdnProperties=uid
standalone.ldap.groupRdnProperties=cn

###################################################
##
## End Group member attributes
##
###################################################



###############################################################################
##
##     Advanced Properties
##
###############################################################################


###################
# Group config
###################

# The name of the membership attribute. For example, memberOf in an active
directory server and ibm-allGroups in IDS.
standalone.ldap.gc.name=ibm-allGroups

# Updates the group membership if the member is deleted or renamed. Some LDAP
servers, for example, Domino server, do not clean up
```

```
# the membership of the user when a user is deleted or renamed. If you choose these LDAP server types in the ldapServerType property,
# the value of this parameter is set to true. Use this parameter to change the value. The default value is false.
standalone.ldap.gc.updateGroupMembership=


# The scope of the membership attribute. The valid values for this parameter include the following:
# direct - The membership attribute only contains direct groups.
# nested - The membership attribute that contains the direct groups and the nested groups.
# all - The membership attribute contains direct groups, nested groups, and dynamic members.
# The default value is direct.
standalone.ldap.gc.scope=direct



# Controls how aliases are dereferenced. The default value is always. Valid values include:
#       always - always deference aliases
#     never - never deference aliases
#     finding - deference aliases only during name resolution
#     searching - deference aliases only after name resolution
standalone.ldap.derefAliases=always


# Indicates the authentication method to use. The default value is simple. Valid values include: none or strong.
standalone.ldap.authentication=simple


# The LDAP referral. The default value is ignore. Valid values include: follow, throw, or false.
standalone.ldap.referral=ignore


# Specifies the delimiter used for this realm. The default value is /.
standalone.ldap.delimiter=/


# Whether the query matches case sensitivity.
# note: not used during node federation to DMGR with WAS ldap security enabled
standalone.ldap.ignoreCase=true
```

```
# Specifies whether secure socket communication is enabled to the LDAP server.
# When enabled (sslEnabled=true), the Secure Sockets Layer (SSL) settings for LDAP are used.
# The default value is false.
standalone.ldap.sslEnabled=false

# Specifies the name of the application server SSL configuration to be used for SSL enabled LDAP server.
# This property is used to specify a non default SSL configuration if standalone.ldap.sslEnabled=true is set
standalone.ldap.sslConfiguration=

# Specifies whether to map X.509 certificates into a LDAP directory by exact distinguished name or certificate filter.
# Specify the certificate filter to use the specified filter for the mapping, if client certificate authentication is used
# for portal server.
# Valid values include: EXACT_DN, CERTIFICATE_FILTER
standalone.ldap.certificateMapMode=EXACT_DN

# Specifies the filter certificate mapping property for the LDAP filter, if client certificate authentication is used
# for portal server.
# The filter is used to map attributes in the client certificate to entries within the LDAP repository.
standalone.ldap.certificateFilter=

# Should be set to true by default to reuse the LDAP connection.
# note: not used during node federation to DMGR with WAS ldap security enabled
standalone.ldap.reuseConnection=true

# Specifies the timeout value in miliseconds for an LDAP server to respond before aborting a request.
standalone.ldap.searchTimeLimit=120000

# Defines if VMM will enable the ConnectionPool
standalone.ldap.connectionPool=true

# Indicates if sorting is supported or not. The default value is false.
standalone.ldap.supportSorting=false
```

```
# Indicates if paging is supported or not.
standalone.ldap.supportPaging=false

# Indicates if transactions are supported or not. The default value is false.
standalone.ldap.supportTransactions=false

# Specifies if the external ID is unique. The default value is true.
standalone.ldap.isExtIdUnique=true

# Indicates if external names are supported or not. The default value is false.
standalone.ldap.supportExternalName=false

# Indicates to translate RDN or not. The default value is false.
standalone.ldap.translateRDN=false

# The value of the search count limit.
standalone.ldap.searchCountLimit=500

# The value of search page size.
standalone.ldap.searchPageSize=

# Indicates to return to the primary LDAP server when it is available. The default
value is true.
standalone.ldap.returnToPrimaryServer=

# Indicates the polling interval for testing the primary server availability.
# The value of this parameter is specified in minutes. The default value is 15.
standalone.ldap.primaryServerQueryTimeInterval=

# Indicates the property name used for login.
standalone.ldap.loginProperties=uid

# The maximum number of context instances that can be maintained concurrently by
the context pool.
# The default value is 20.
standalone.ldap.cp.maxPoolSize=20
```

```
################################################################################
################################################################################
##
##
##  End - VMM Stand-alone LDAP configuration
##
##
################################################################################
################################################################################
```

Appendix B - Adding a Vertical Cluster member

After creating your cluster, you may need to add additional members to the cluster. This section will describe how to properly add a vertical cluster member to your cluster.

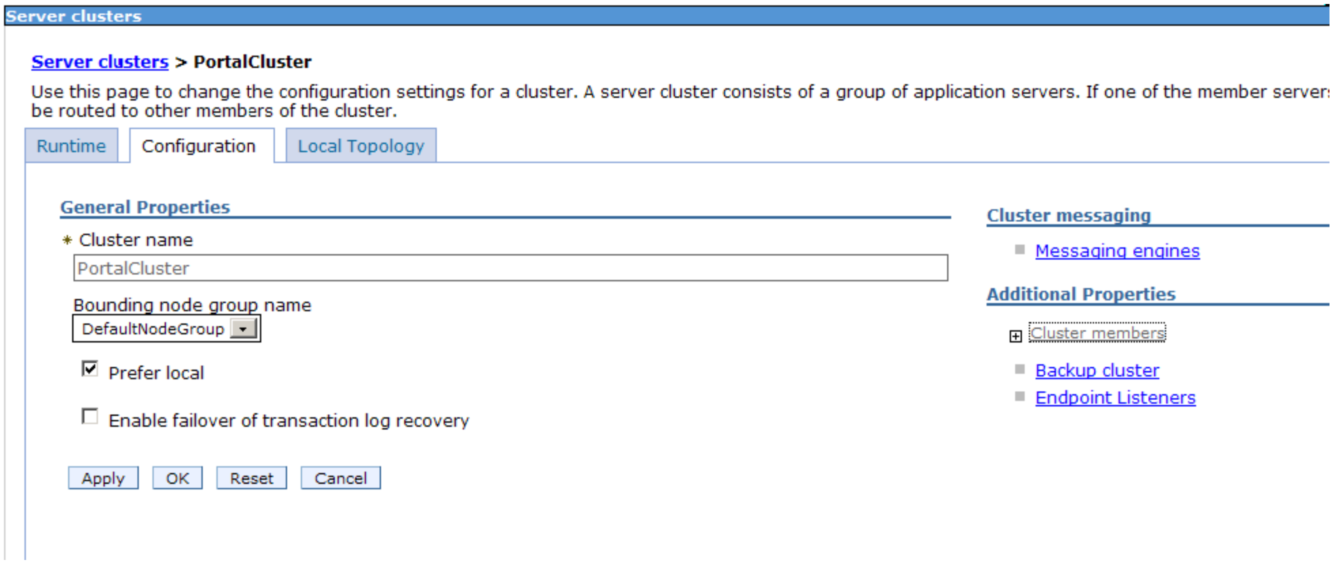
1. From a command window, navigate to <AppServer root>/profiles/Dmgr01/bin
2. Execute the following command:

   ```
   startManager.bat
   ```

3. Once the DMGR is open for e-business, launch a web browser and access the DMGR Administrative Console:

   http://<yourhostname>:9060/ibm/console

4. Navigate to Servers -> Clusters -> *PortalCluster* -> Cluster Members



Server clusters

Server clusters > PortalCluster

Use this page to change the configuration settings for a cluster. A server cluster consists of a group of application servers. If one of the member server be routed to other members of the cluster.

General Properties

* Cluster name

PortalCluster

Bounding node group name

DefaultNodeGroup

☑ Prefer local

□ Enable failover of transaction log recovery

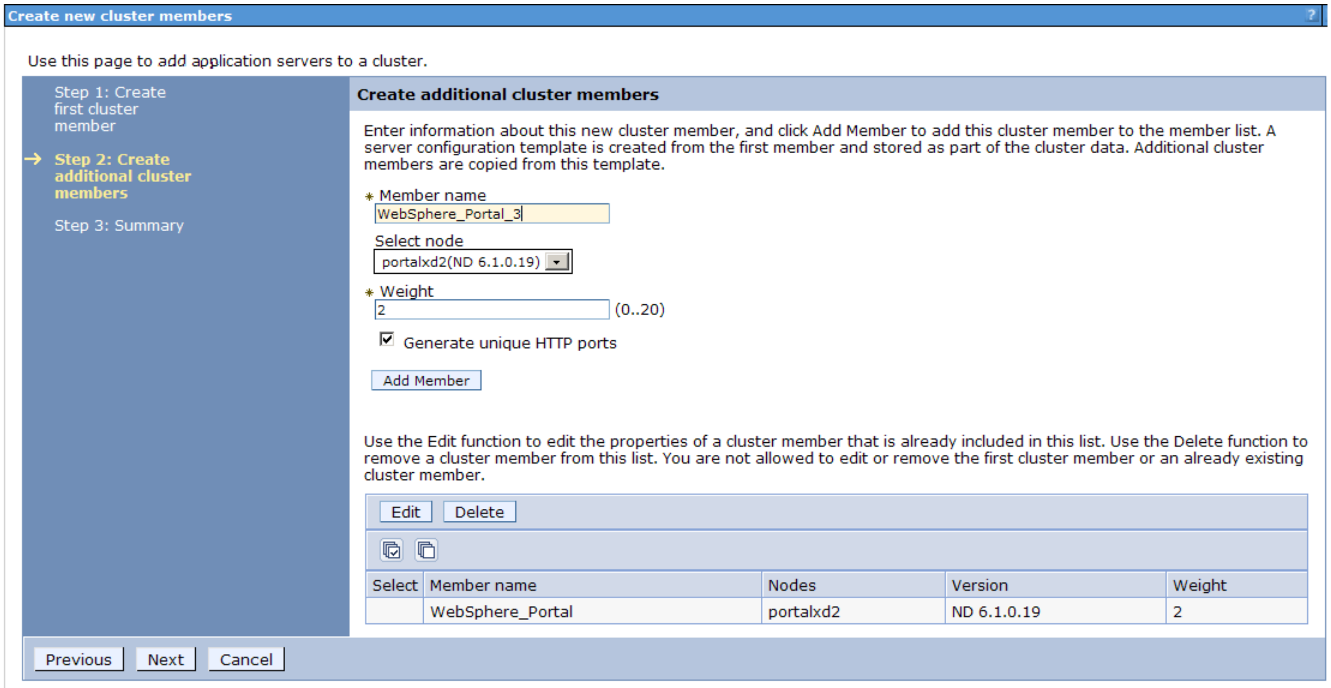
5. Click 'New'

6. On the next screen, enter the following information:

   Member Name - The new member name (for example WebSphere_Portal_3)
   NOTE: Do not use any name that contains a space

   Select Node – Select a node that is part of your cluster

   Generate Unique HTTP Ports – Ensure this is checked



Create new cluster members

Use this page to add application servers to a cluster.

Step 1: Create first cluster member

→ **Step 2: Create additional cluster members**

Step 3: Summary

Create additional cluster members

Enter information about this new cluster member, and click Add Member to add this cluster member to the member list. A server configuration template is created from the first member and stored as part of the cluster data. Additional cluster members are copied from this template.

* Member name: WebSphere_Portal_3

Select node: portalxd2(ND 6.1.0.19)

* Weight: 2 (0..20)

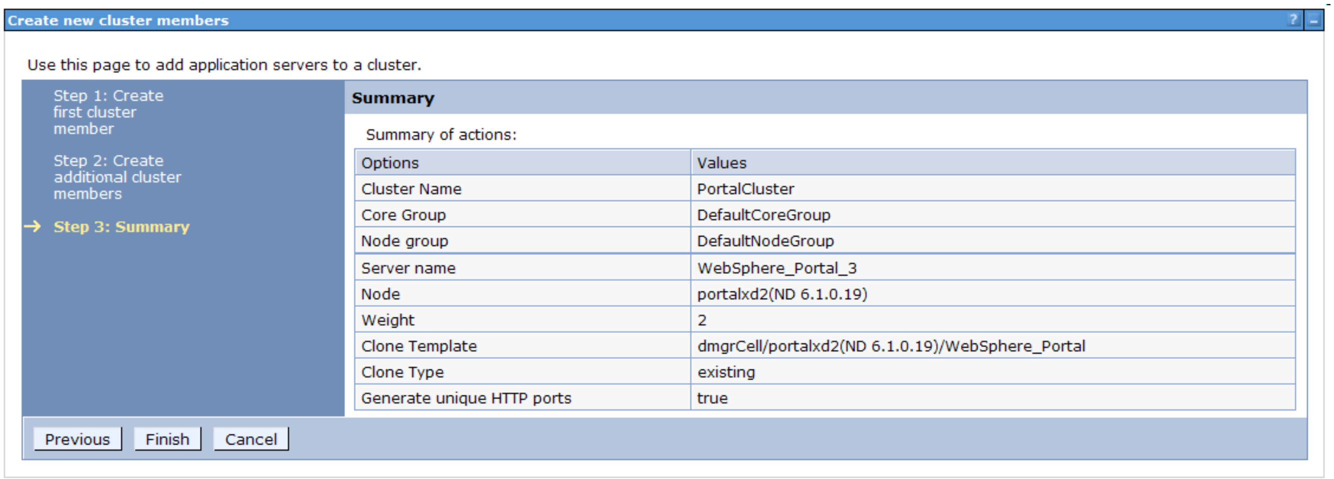
☑ Generate unique HTTP ports

Use the Edit function to edit the properties of a cluster member that is already included in this list. Use the Delete function to remove a cluster member from this list. You are not allowed to edit or remove the first cluster member or an already existing cluster member.

Select	Member name	Nodes	Version	Weight
	WebSphere_Portal	portalxd2	ND 6.1.0.19	2

7. Click “Add Member”
8. Click “Next”

9. Review the summary screen and click Finish.


Create new cluster members
?
Step 1: Create first cluster member
Step 2: Create additional cluster members
Step 3: Summary
Previous
Finish
Cancel

Use this page to add application servers to a cluster.

Summary

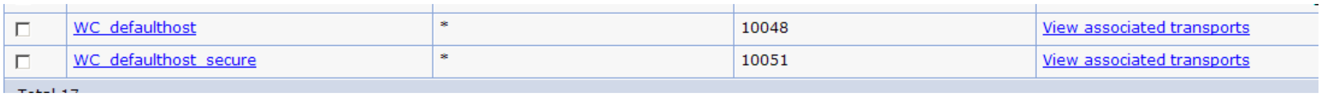
Summary of actions:

Options	Values
Cluster Name	PortalCluster
Core Group	DefaultCoreGroup
Node group	DefaultNodeGroup
Server name	WebSphere_Portal_3
Node	portalxd2(ND 6.1.0.19)
Weight	2
Clone Template	dmgrCell/portalxd2(ND 6.1.0.19)/WebSphere_Portal
Clone Type	existing
Generate unique HTTP ports	true

10. Save changes

11. Navigate to Servers -> Application Servers -> *WebSphere_Portal_3* -> Ports and not the following two port values:

WC_defaulthost
WC_defaulthostsecure



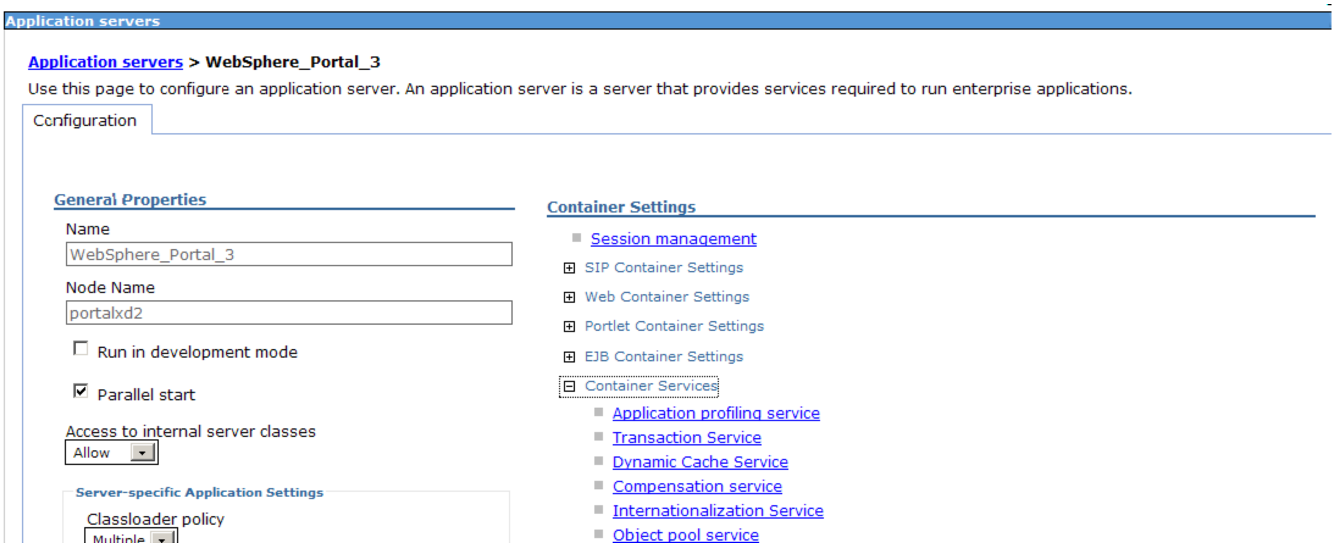
□	WC_defaulthost	*	10048	View associated transports
□	WC_defaulthost_secure	*	10051	View associated transports

12. Update the Virtual Hosts to include these two ports

    a) Navigate to Environment -> Virtual Hosts -> default_host -> Host Aliases
    b) Click "New"
    c) Set Hostname to *
    d) Set Port to the value of WC_defaulthost
    e) Click "OK"
    f) Repeat a-e for WC_defaulthost_secure
    g) Save changes

13. Enable Dynamic Replication on the new cluster member.

    a) Navigate to **Servers -> Application Servers ->** ***WebSphere_Portal_3*** **-> Container Services -> Dynamic Cache Service**



Application servers

Application servers > WebSphere_Portal_3

Use this page to configure an application server. An application server is a server that provides services required to run enterprise applications.

Configuration

General Properties

Name: WebSphere_Portal_3

Node Name: portalxd2

□ Run in development mode

☑ Parallel start

Access to internal server classes: Allow

Server-specific Application Settings

Classloader policy: Multiple

Container Settings

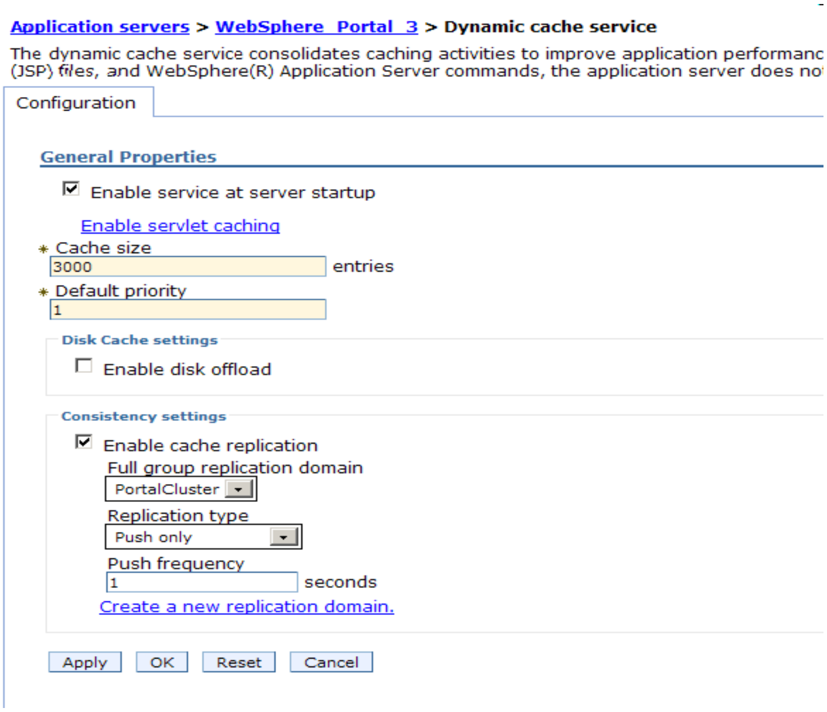
- Session management
- ⊞ SIP Container Settings
- ⊞ Web Container Settings
- ⊞ Portlet Container Settings
- ⊞ EJB Container Settings
- ⊟ Container Services
  - Application profiling service
  - Transaction Service
  - Dynamic Cache Service
  - Compensation service
  - Internationalization Service
  - Object pool service

    b) Set Cache Size to 3000 entries

    c) Check the Enable Cache Replication Box

    d) Select "Push Only" from the Replication Type drop-down menu

    e) Click "OK" and save changes.



Application servers > WebSphere_Portal_3 > Dynamic cache service

The dynamic cache service consolidates caching activities to improve application performanc
(JSP) files, and WebSphere(R) Application Server commands, the application server does no

Configuration

General Properties

☑ Enable service at server startup

Enable servlet caching

* Cache size: 3000 entries

* Default priority: 1

Disk Cache settings

□ Enable disk offload

Consistency settings

☑ Enable cache replication

Full group replication domain: PortalCluster

Replication type: Push only

Push frequency: 1 seconds

Create a new replication domain.

14. From the node that you created the vertical cluster member on, open a command prompt and change directories to the <wp_profile root>/ConfigEngine directory.

15. Execute the following ConfigEngine script to remove server-scoped entries from the new cluster member:

    IMPORTANT: Failure to do this step will result in an inoperable vertical cluster member

    ```
    ConfigEngine.bat cluster-node-config-vertical-cluster-setup
    -DServerName=WebSphere_Portal_3
    ```

    where ServerName is set to your new vertical cluster member name. In this case, WebSphere_Portal_3 is my new vertical cluster member.

16. Synchronize the nodes and restart the DMGR, nodeagents and cluster members.

17. Verify you can access your new cluster member in a URL using the port defined for WC_defaulthost in step 11:

    http://hostname:10048/wps/portal

Appendix C – Adding a new secondary node to an existing cluster

You may need to add a new node to your cluster in the future. In this section, we will add a new node to an existing cluster that already has standalone LDAP security enabled.

1. Install your new Portal following the steps on pages 25-31.

   NOTE: At this point, you have a standalone Portal server using the default VMM federated file registry security.

2. Copy the wp_security_ids.properties from the <wp_profile>/ConfigEngine/config/helpers directory on your Primary node to the <wp_profile>/ConfigEngine/config/helpers directory on the secondary node.

3. From the secondary node, copy the contents of the helper file into the main wkplc.properties file by running the following command (all on one line):

   ```
    ConfigEngine.bat
   -DparentProperties=<wp_profile>/ConfigEngine/config/helpers/wp_security_ids.p
   roperties -DsaveParentProperties=true
   ```

   NOTE: If you did not use a helper file when setting up security, then manually update the standalone.ldap values in the wkplc.properties file to match those of your existing nodes.

4. Ensure the database client is installed and configured on the secondary node. For DB2 with Type 4 drivers, copy the db2jcc.jar and db2jcc_license_cu.jar files from the DB2 server to some directory on the secondary Portal server.

5. Ensure the DMGR is STARTED.

   <dmgr profile>/bin/startManager.bat

6. From the <wp_profile>/ConfigEngine/properties directory, make a backup of the following files:

   wkplc.properties
   wkplc_dbtype.properties
   wkplc_comp.properties

7. Copy the wkplc_comp.properties and wkplc_dbtype.properties from the primary node to the new node to ensure the same database configuration.

   NOTE: Ensure that the value of db2.dbLibrary in wkplc_dbtype.properties contains valid directory paths for this node.

8. From the <wp_profile>/ConfigEngine/properties directory, edit the wkplc.properties file and change the following entries:

   ```
   WasPassword=<standalone WAS password>
   PortalAdminPwd=password
   WasRemoteHostName=<fully qualified hostname of DMGR>
   WasSoapPort=<soap port for DMGR; default is 8879>
   PrimaryNode=false
   ClusterName=PortalCluster
   ```

   NOTE: Ensure that the value for ClusterName matches the value for ClusterName on the primary node.

9. In a command window from the secondary node, change directories to <wp_profile>/ConfigEngine

10. Add the node to the deployment manager cell by executing the following ConfigEngine script:

    ```
    ConfigEngine.bat cluster-node-config-pre-federation
    -DDMgrUserid=uid=<full LDAP DN of dmgr user id> -DDMgrPassword=<dmgr
    password>
    ```

    For example:

    ```
    ConfigEngine.bat cluster-node-config-pre-federation
    -DDMgrUserid=uid=wasadmin,ou=users,ou=myStandaloneLdap,o=com
    -DDMgrPassword=wasadmin
    ```

    NOTE: Ensure that the time on the Deployment Manager server and the time on the primary node are within 5 minutes of each other. Failure to do so can cause this step to fail. This will also create the NodeAgent server for you on your node.

    NOTE: If you are prompted to accept an SSL certificate, type Y and press Enter to continue

    NOTE: If you specify the -DDMgrUserid parameter when running the cluster-node-config-pre-federation task, it resets the WasUserid parameter in the wkplc.properties file to the -DDMgrUserid value.

11. After the previous step completes, your node will be part of the deployment manager cell. As a result, this node is now using the Deployment Manager security configuration and cell name. The original WAS ID that had been used in the standalone environment will no longer be used.

    Edit the <wp_profile>/ConfigEngine/wkplc.properties file and ensure the following properties are set correctly:

    ```
    WasUserId=<dmgr admin user>
    WasPassword=<dmgr password>
    CellName=<dmgr cell name>
    ```

12. Update the deployment manager configuration for the new WebSphere Portal server by executing the following ConfigEngine script:

    ```
    ConfigEngine.bat cluster-node-config-post-federation
    ```

13. Ensure the NodeAgent is started on this node:

    ```
    <wp_profile>/bin/startNode.bat
    ```

14. Specify the name of the future secondary cluster member.

    Edit the <wp_profile>/ConfigEngine/wkplc.properties file and change the following property:

    ```
    ServerName=<name of new cluster member>
    ```

    NOTE: When you open the properties file, you should see WebSphere_Portal_*nodename*. You can use this value if you like. Otherwise you can change this to anything EXCEPT 'WebSphere_Portal'. DO NOT use the value of 'WebSphere_Portal' for your secondary cluster member.

15. Add this newly federated WebSphere_Portal server as a cluster member to the existing cluster by executing the following ConfigEngine script:

    ```
    ConfigEngine.bat cluster-node-config-cluster-setup
    ```

    NOTE: This will automatically add a secondary cluster member to your existing cluster based on whatever value you set for ServerName in step 10. In this example, the default value was used. The node name is wpnode3 so our cluster member will be called WebSphere_Portal_wpnode3.

16. Allow **30 minutes** for ear expansion to complete on the secondary node. Failure to do so may result in several applications being unavailable on this node.

17. Because the security configuration for the Portal node changed when we federated the node (step 9), we need to update the Portal configuration to reference the new Portal Admin ID and group by running the following ConfigEngine script:

    ```
    ConfigEngine.bat wp-change-portal-admin-user -DnewAdminId=<full DN of Portal
    admin ID> -DnewAdminPwd=<new password> -DnewAdminGroupId=<full DN of Portal
    Admin Group ID> -Dskip.ldap.validation=true
    ```

    Note: The -Dskip.ldap.validation=true flag can be used if the script fails during ldap validation.

18. Start the new cluster member WebSphere_Portal_*nodename*:

    ```
    <wp_profile>/bin/startServer.bat WebSphere_Portal_nodename
    ```

Appendix D – Running IBM Support Assistant Lite

At some point you may run into a failure when executing WebSphere Portal and require assistance from IBM Remote Technical Support. In order to save time with troubleshooting your issue, IBM Support strongly recommends you use ISALite to collect the logs and configuration information from your system.

These instructions assume you already installed the ISALite tool from earlier in this guide.

To watch a video demonstration of the tool, please visit the WebSphere Portal Wiki at this URL:

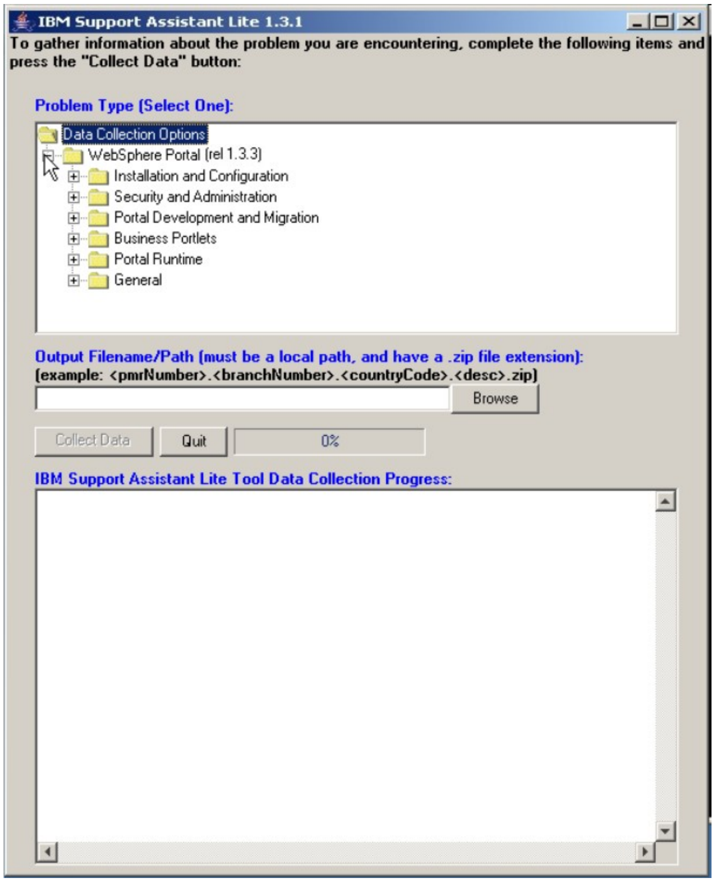
http://www-10.lotus.com/ldd/portalwiki.nsf/dx/demo-isalite-fundamentals-version-1.3.3-for-ibm-websphere-portal

1. Open a command prompt and change directories to <wp_profile root>/PortalServer/ISALite.

2. Launch the tool by executing the following command:

   ```
   runISALite.bat
   ```

3. When the tool launches, you should see a window similar to the following:



IBM Support Assistant Lite 1.3.1

To gather information about the problem you are encountering, complete the following items and press the "Collect Data" button:

Problem Type (Select One):

Data Collection Options
WebSphere Portal (rel 1.3.3)
Installation and Configuration
Security and Administration
Portal Development and Migration
Business Portlets
Portal Runtime
General

Output Filename/Path (must be a local path, and have a .zip file extension):
(example: <pmrNumber>.<branchNumber>.<countryCode>.<desc>.zip)

Browse
Collect Data
Quit
0%

IBM Support Assistant Lite Tool Data Collection Progress:

4. Expand WebSphere Portal and select your problem type. If you are unsure of what your problem type is, select one of the following:

   WebSphere Portal -> General -> Portal General Problem

   WebSphere Portal -> General -> Portal General File Collection

5. In the Output Filename filed, specify the path and name of the zip file that will be created by the tool. If you have a PMR number, please use include this number in the zip name. For example:

   C:/temp/12345.123.000.PortalProblem.zip

6. Click the button for "Collect Data"

7. You will receive several prompts as the script runs. Answer all questions you see as accurately as possible. This includes PortalServer and AppServer root, WAS credentials, and whether or not the server is part of a cluster.

   Note: If you selected the **"Portal General File Collection"** problem type, you will not see these prompts. This option is only available in versions 1.3.3 and higher, and requires minimal user interaction.

8. Select to FTP the logs when prompted. If you choose not to do so here or are unable to do this, you can do so manually following the instructions in this link:

   http://www-01.ibm.com/support/docview.wss?rs=688&uid=swg21201571