

Exercise instructions

Preface

- Access your lab image by using the instructions that your instructor provides.



Substitution values

Use the following substitution values when you encounter them in the exercise instructions.

<wps_home> is /opt/IBM/WebSphere/PortalServer

<was_home> is /opt/IBM/WebSphere/AppServer

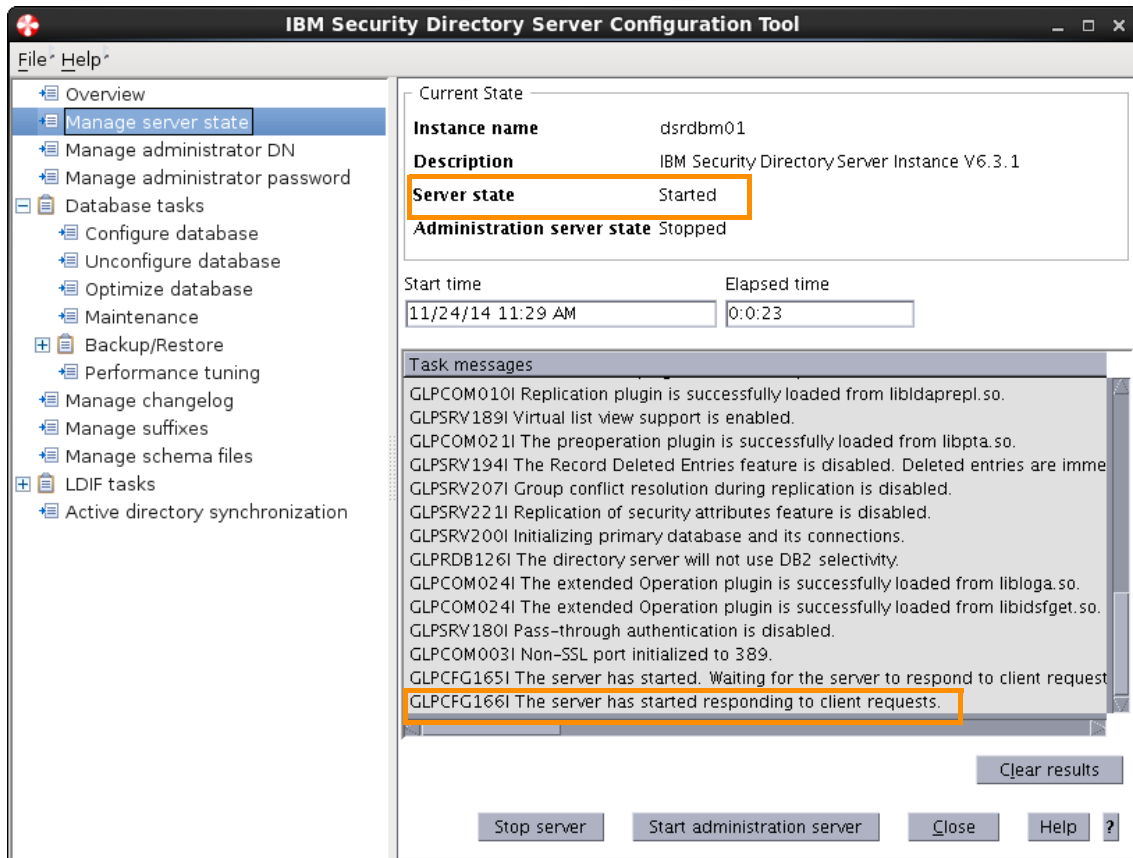
<wp_profile> is /opt/IBM/WebSphere/wp_profile

<dmgr_profile> is /opt/IBM/WebSphere/AppServer/profiles/Dmgr

Section 1: Stop the WebSphere Portal and server1

- __ 1. Verify that WebSphere Portal is stopped.
 - __ a. Open a terminal window and change directories to <wp_profile>/bin.
 - __ b. Enter the following command: `./serverStatus.sh -all -user wpsadmin -password IBMp0rtal`
 - __ c. If WebSphere Portal is started, enter the following command: `./stopServer.sh WebSphere_Portal -user wpsadmin -password IBMp0rtal`
- __ 2. Verify that server1 is stopped.
 - __ a. Open a terminal window and change directories to <was_home>/profiles/cw_profile/bin.
 - __ b. Enter the following command: `./serverStatus.sh -all -user installadmin -password IBMp0rtal`
 - __ c. If server1 is started, enter the following command: `./stopServer.sh server1 -user installadmin -password IBMp0rtal`
- __ 3. Ensure that IBM Security Directory Server Instance V6.3.1 is started.
 - __ a. Open a terminal window and change directory to /opt/IBM/ldap/V6.3.1/sbin
 - __ b. Enter the command: `./idsxcfg`
 - __ c. When the IBM Security Directory Server Configuration tool opens, click **Manage server state**.
 - __ d. If the server state is “Stopped”, click **Start server**.

___ e. Click **OK** on the task completed message box.



___ f. Close the tool by clicking **File > Exit**.

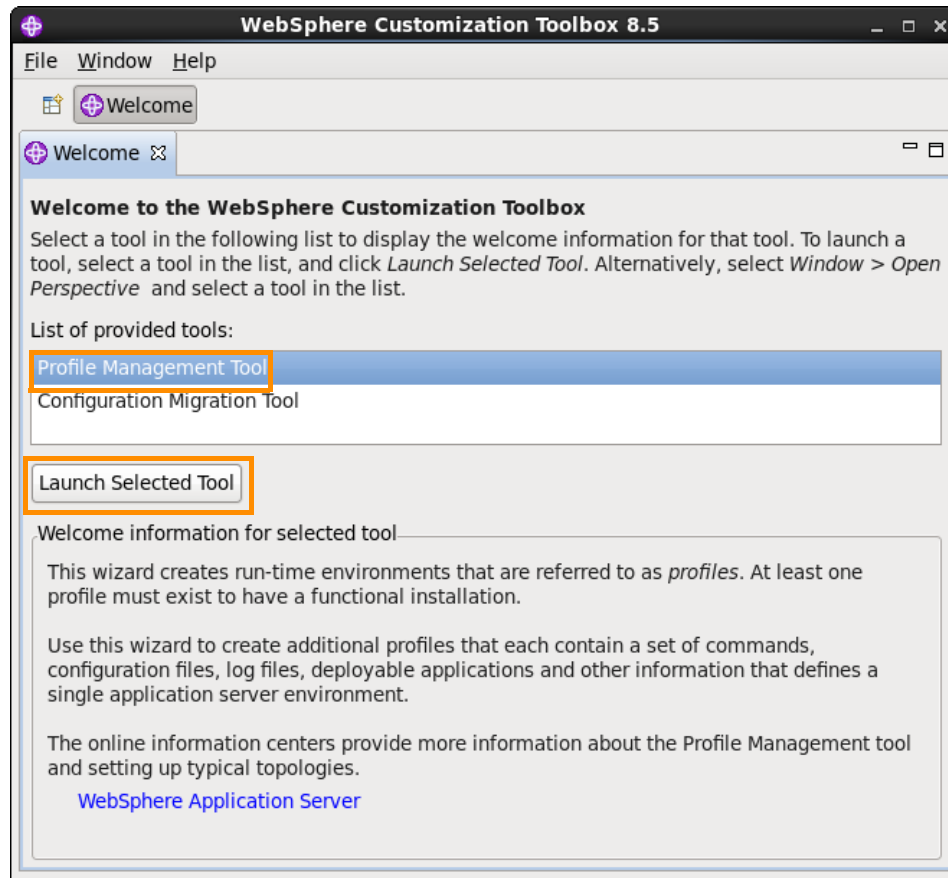
Section 2: Use the Profile Management Tool to create a deployment manager profile

___ 1. Start the WebSphere Customization Toolbox.

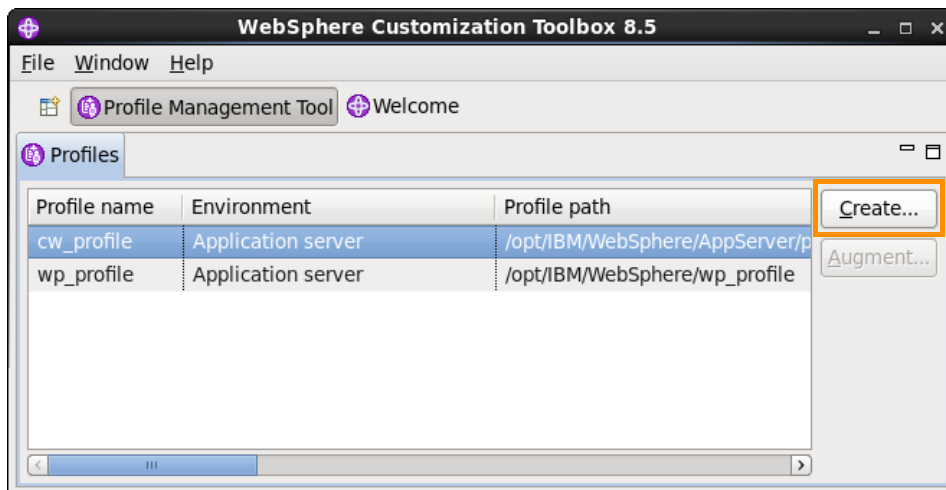
___ a. Enter the command to start the WebSphere Customization Toolbox is:

```
<was_home>/bin/ProfileManagement/wct.sh
```

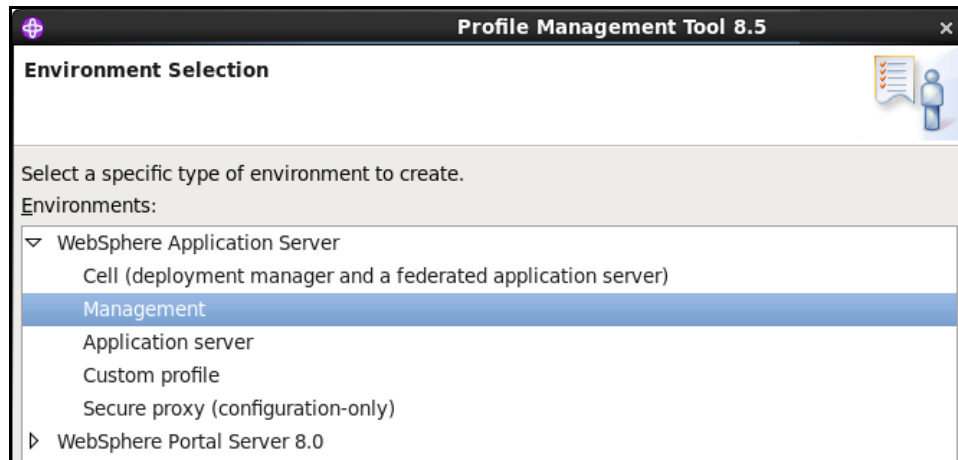
- ___ b. The WebSphere Customization Toolbox opens. Select **Profile Management Tool**, and click **Launch Selected Tool**.



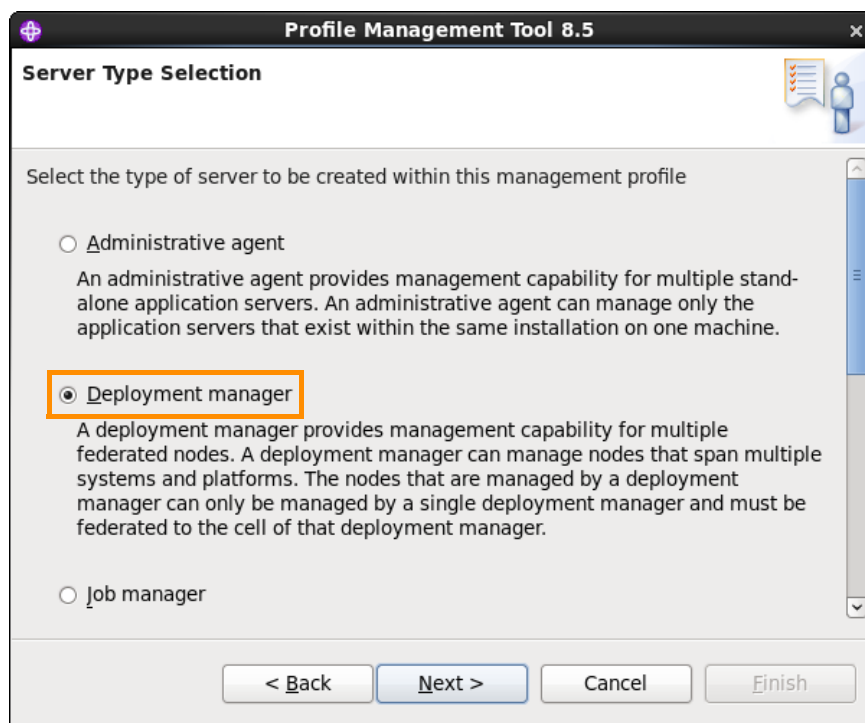
- ___ c. The Profile Management Tool opens. Click **Create**.



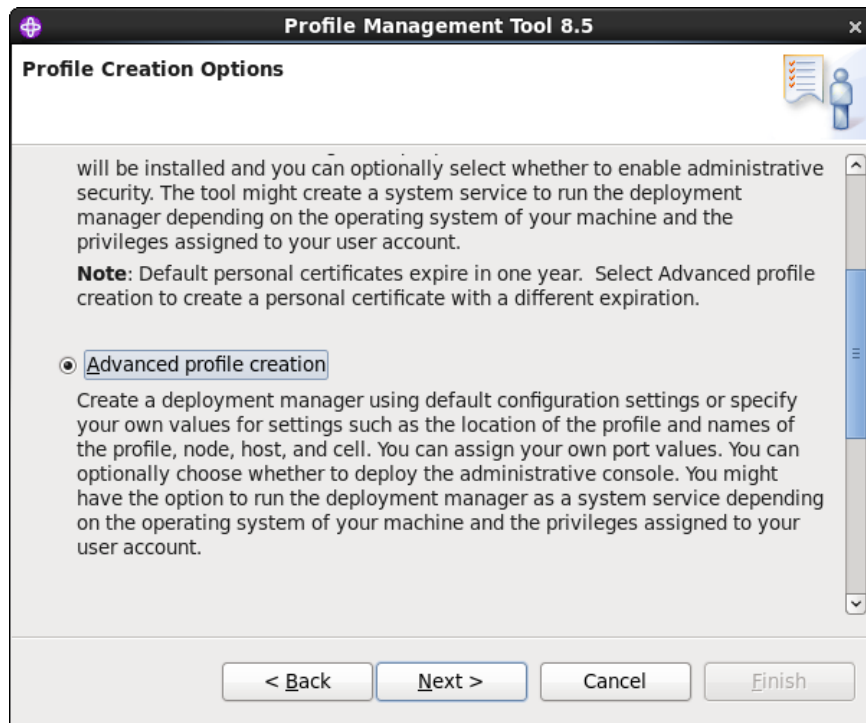
- ___ 2. Create a deployment manager profile called Dmgr.
- ___ a. From the Environment Selection pane, select **Management** and click **Next**.



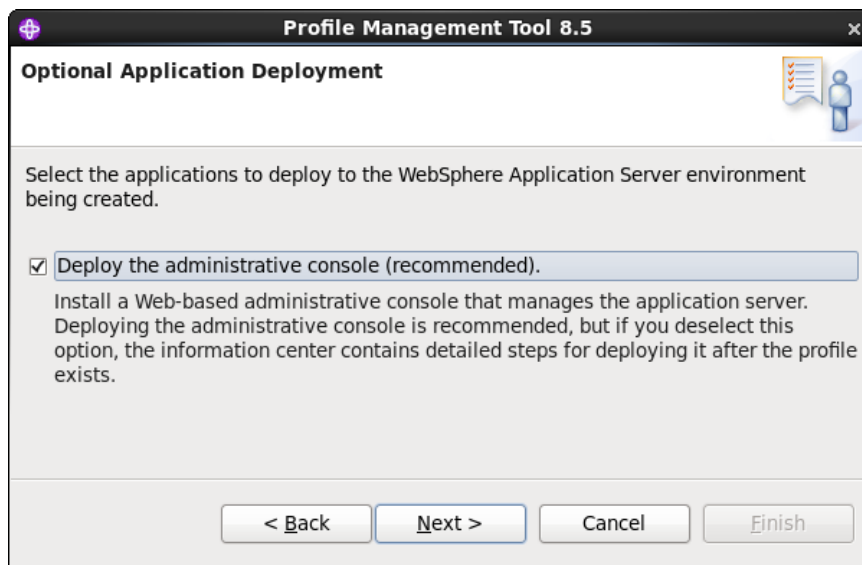
- ___ b. From the Server Type Selection pane, select **Deployment manager** and click **Next**.



- ___ c. Select **Advanced profile creation** to specify your own configuration values during profile creation. Click **Next**.



- ___ d. Ensure that the **Deploy the administrative console** check box is selected. Click **Next**.



- ___ e. From the Profile Name and Location pane, provide the following name and location information:
- Profile name: Dmgr

- Profile directory: /opt/IBM/WebSphere/AppServer/profiles/Dmgr
- Do **not** select the **Make this profile the default** option.

The screenshot shows the 'Profile Management Tool 8.5' window with the 'Profile Name and Location' tab selected. The window contains the following elements:

- Title Bar:** Profile Management Tool 8.5
- Tab:** Profile Name and Location
- Instructions:** Specify a profile name and directory path to contain the files for the run-time environment configuration files, and log files. Click **Browse** to select a different directory.
- Profile name:** A text field containing 'Dmgr'.
- Profile directory:** A text field containing '/opt/IBM/WebSphere/AppServer/profiles/Dmgr'.
- Checkbox:** ☐ **Make this profile the default.**
- Text:** Each installation of WebSphere Application Server always has one default profile. When referring to a specific profile use the default profile. Select this option to make this profile the default.
- Important:** Deleting the directory a profile is in does not completely delete the profile. Use the command to completely delete a profile.
- Buttons:** < Back, Next >, Cancel, Finish.

An orange rectangle highlights the 'Profile name' and 'Profile directory' text fields.

___ f. Click **Next**.

- ___ g. The **Node, Host, and Cell Names** pane allows you to set the node name, cell name, and host name. Default values are completed based on the detected host name for your server.

Profile Management Tool 8.5

Node, Host, and Cell Names

Specify a node name, a host name, and a cell name for this profile.

Node name:
portal00CellManager01

Host name:
portal00

Cell name:
portal00Cell01

Node name: A node name is for administration by the deployment manager. The name must be unique within the cell.

Host name: A host name is the domain name system (DNS) name (short or long) or IP address of the host.

Cell name: A cell name is a logical name for the group of nodes administered by this profile.

The following naming rules must be used:

- Node name: 1 to 64 characters, alphanumeric, and hyphen.
- Host name: 1 to 64 characters, alphanumeric, and hyphen.
- Cell name: 1 to 64 characters, alphanumeric, and hyphen.

< Back Next > Cancel Finish

- ___ h. Accept the defaults, and click **Next**.
- ___ i. From the Administrative Security pane, you choose whether to enable administrative security. Verify that the Enable administrative security option check box is selected. Enter the following information:
- User name: installadmin
 - Password: IBMp0rtal
 - Confirm password: IBMp0rtal

Profile Management Tool 8.5

Administrative Security

Choose whether to enable administrative security. To enable security, supply a user name and password for logging into administrative tools. This administrative user is created in a repository within the application server. After profile creation finishes, you can add more users, groups, or external repositories.

☒ **Enable administrative security**

User name:
installadmin

Password:
.....

Confirm password:
.....

< Back Next > Cancel Finish

- ___ j. Click **Next**.
- ___ k. From the Security Certificate (Part 1) pane, accept the default selections:
 - Create a default personal certificate
 - Create a root signing certificate

The screenshot shows the 'Profile Management Tool 8.5' window with the 'Security Certificate (Part 1)' tab selected. The window contains a scrollable area with the following text: 'the certificate information. To import existing certificates from keystores, locate the certificates then proceed to Part 2 and verify the certificate information.' Below this text are two radio button options: 'Create a new default personal certificate.' (which is selected) and 'Import an existing default personal certificate.' Below these options is a section titled 'Default personal certificate' containing four input fields: 'Path:' with a 'Browse...' button, 'Password:', 'Keystore type:', and 'Keystore alias:'. At the bottom of the scrollable area are two more radio button options: 'Create a new root signing certificate.' (selected) and 'Import an existing root signing certificate.' At the very bottom of the window are four buttons: '< Back', 'Next >', 'Cancel', and 'Finish'.

___ I. Click **Next**.

__ m. Accept the Security Certificate (Part 2) pane defaults.

The screenshot shows the 'Security Certificate (Part 2)' dialog box in the 'Profile Management Tool 8.5'. The dialog has a title bar with a plus icon, the text 'Profile Management Tool 8.5', and a close button. Below the title bar, the text 'Security Certificate (Part 2)' is displayed next to a help icon. The main area contains instructional text: 'Modify the certificate information to create new certificates during profile creation. If you are importing existing certificates from keystores, use the information to verify whether the selected certificates contain the appropriate information. If the selected certificates do not, click **Back** to import different certificates.' Below this is a 'Restore Defaults' button. The 'Default personal certificate (a personal certificate for this profile, public and private key):' section includes three fields: 'Issued to distinguished name:' with the value 'cn=portal00,ou=portal00Cell01,ou=portal00CellManager01,o=IBM,c=US', 'Issued by distinguished name:' with the value 'cn=portal00,ou=Root Certificate,ou=portal00Cell01,ou=portal00CellManager01,o=IBM,c=US', and 'Expiration period in years:' with a spinner set to '1'. The 'Root signing certificate (personal certificate for signing other certificates, public and private key):' section is currently empty. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Finish'.

Profile Management Tool 8.5

Security Certificate (Part 2)

Modify the certificate information to create new certificates during profile creation. If you are importing existing certificates from keystores, use the information to verify whether the selected certificates contain the appropriate information. If the selected certificates do not, click **Back** to import different certificates.

Restore Defaults

Default personal certificate (a personal certificate for this profile, public and private key):

Issued to distinguished name:
cn=portal00,ou=portal00Cell01,ou=portal00CellManager01,o=IBM,c=US

Issued by distinguished name:
cn=portal00,ou=Root Certificate,ou=portal00Cell01,ou=portal00CellManager01,o=IBM,c=US

Expiration period in years:
1

Root signing certificate (personal certificate for signing other certificates, public and private key):

< Back Next > Cancel Finish

__ n. Click **Next**.

- ___ o. The Port Values Assignment pane allows you to set any ports for the deployment manager to prevent conflicts with other profiles. Accept the default port values..

Profile Management Tool 8.5

Port Values Assignment

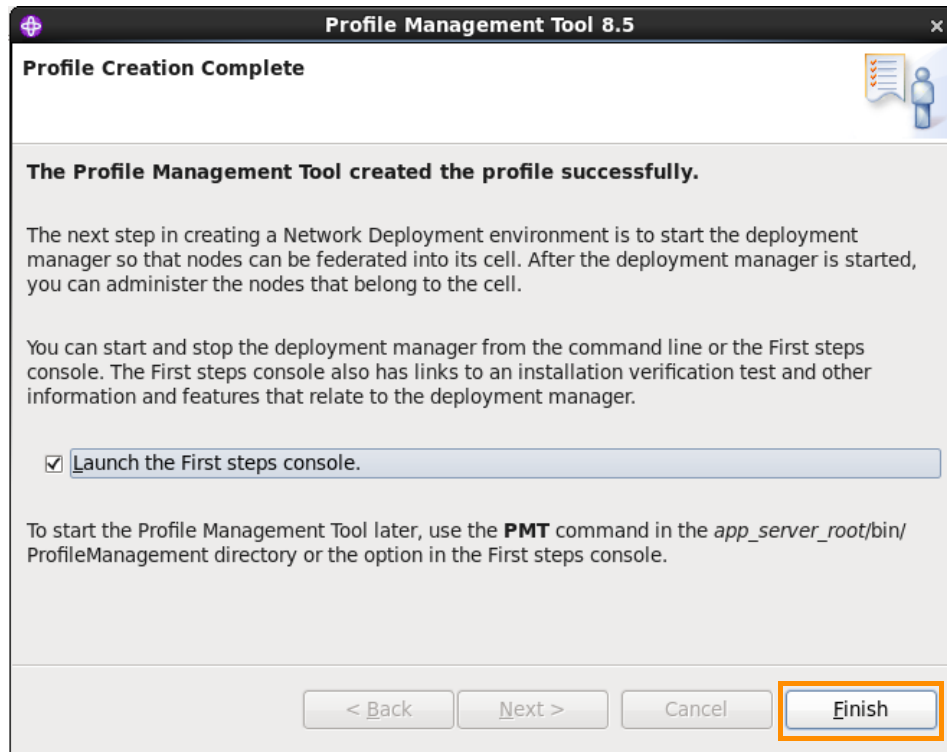
The values in the following fields define the ports for the deployment manager and do not conflict with other profiles in this installation. Another installation of WebSphere Application Server or other programs might use the same ports. To avoid run-time port conflicts, verify that each port value is unique.

Administrative console port (Default 9060):	9060
Administrative console secure port (Default 9043):	9043
Bootstrap port (Default 9809):	9809
SOAP connector port (Default 8879):	8879
Administrative interprocess communication port (Default 9632)(X):	9632
SAS SSL ServerAuth port (Default 9401):	9401
CSIV2 ServerAuth listener port (Default 9403):	9403
CSIV2 MultiAuth listener port (Default 9402):	9402

< Back Next > Cancel Finish

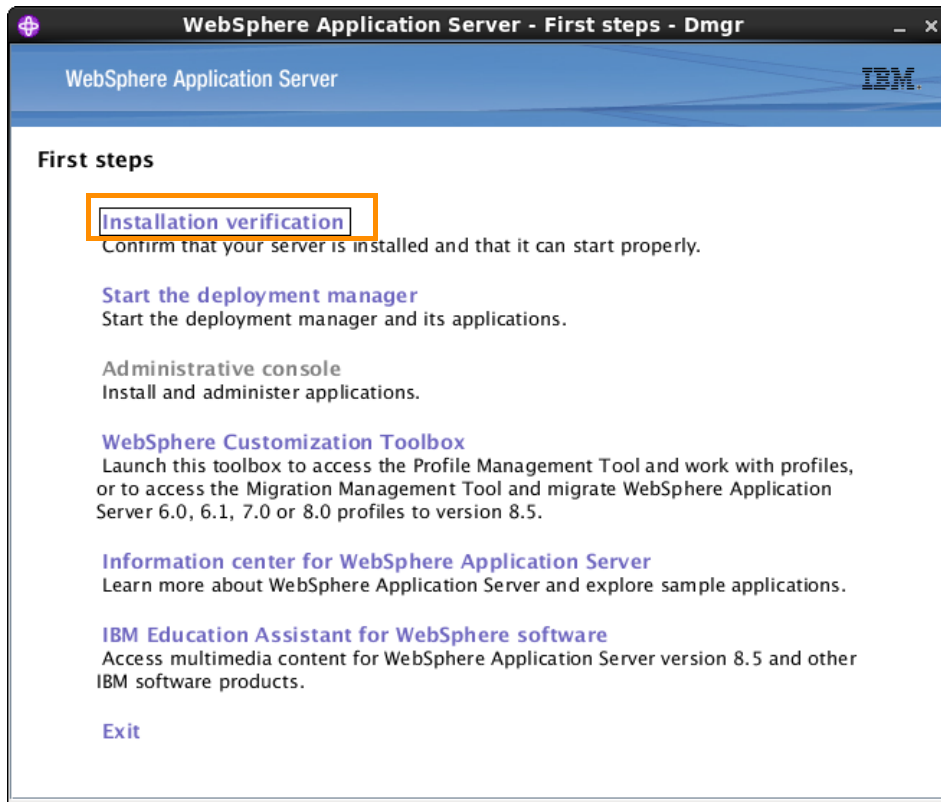
- ___ p. Click **Next**.
- ___ q. On the Linux Service Definition pane, take the defaults and click **Next**.
- ___ r. The Profile Creation Summary pane shows all of the choices you made on previous panes. Verify the summary information with what you entered previously. Click **Create**.
Creation of the profile usually takes several minutes to complete.

- ___ s. The profile creation completes and the Dmgr profile is created. Notice that the Launch the First steps console check box is selected.



- ___ t. Click **Finish**, and the First steps console launches.
- ___ 3. The First steps console is associated with the deployment manager profile, Dmgr, that was created. Each profile has its own First steps console.

- ___ 4. Click **Installation verification** from the First steps console.




- ___ a. The installation verification test tool starts the Dmgr and shows messages to indicate verification status. Use the scroll bar to scroll to the bottom to see all the messages. The following messages are shown if the installation verification was successful:
- ```
IVTL00701: The Installation Verification Tool verification
succeeded.
IVTL00801: The installation verification is complete.
```
- \_\_\_ b. Close the **First steps output - Installation verification** window.
- \_\_\_ c. Click **Exit** to close the First steps console.
- \_\_\_ d. Click **File > Exit** to close the WebSphere Customization Toolbox.

### Section 3: Configure LDAP security for the deployment manager

- \_\_\_ 1. Log in to the administration console (WebSphere Integrated Solutions Console) for the deployment manager.
- \_\_\_ a. Start a Firefox web browser and enter the web address:  
`http://portal00:9060/ibm/console`

- \_\_\_ b. The browser might show a message that the server connection is untrusted.



### This Connection is Untrusted

You have asked Firefox to connect securely to **portal00:9043**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

#### What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

- **Technical Details**
- **I Understand the Risks**

- \_\_\_ c. Click “I understand the Risks” and then click **Add Exception...**
- \_\_\_ d. Click **Confirm Security Exception**.
- \_\_\_ e. Log in with the user ID `installadmin` and password `IBMp0rtal`.



## WebSphere Integrated Solutions Console

User ID:

Password:

 Licensed Materials - Property of IBM (c) Copyright IBM Corp. 1997, 2011 All Rights Reserved. IBM, the IBM logo, ibm.com and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at [Copyright and trademark information](#).

- \_\_\_ 2. Configure LDAP security for the deployment manager identical to the WebSphere Portal configuration.
- \_\_\_ a. In the left navigation tree of the administrative console, click **Security > Global security**.

Global security

Security Configuration Wizard   Security Configuration Report

**Administrative security**

☒ Enable administrative security   [Administrative user roles](#)  
[Administrative group roles](#)  
[Administrative authentication](#)

**Application security**

☒ Enable application security

**Java 2 security**

☐ Use Java 2 security to restrict application access to local resources  
☒ Warn if applications are granted custom permissions  
☐ Restrict access to resource authentication data

**User account repository**

Realm name  
defaultWIMFileBasedRealm

Current realm definition  
Federated repositories

Available realm definitions  
Federated repositories   **Configure...**   Set as current

- \_\_\_ b. Click the check box for **Enable application security**. Click **Configure**, next to the Available realm definitions menu.

- \_\_\_ c. Change the Primary administrative user name to  
uid=wpsadmin,cn=users,dc=hal,dc=com

Global security

[Global security](#) > Federated repositories

**General Properties**

\* Realm name  
defaultWIMFileBasedRealm

\* Primary administrative user name  
uid=wpsadmin,cn=users,dc=hal,dc=com

**Server user identity**

☒ Automatically generated server identity  
☐ Server identity that is stored in the repository  
 Server user ID or administrative user on a Version 6.0.x node  
  
 Password

☒ Ignore case for authorization

- \_\_\_ d. Scroll down to Repositories in the realm, and click **Add repositories**.

Repositories in the realm:

Add repositories (LDAP, custom, etc)... Use built-in repository Remove

| Select                                      | Base Entry                 | Repository Identifier  | Repository Type |
|---------------------------------------------|----------------------------|------------------------|-----------------|
| You can administer the following resources: |                            |                        |                 |
| <input type="checkbox"/>                    | o=defaultWIMFileBasedRealm | InternalFileRepository | File            |
| Total 1                                     |                            |                        |                 |

- \_\_\_ e. On the Repository reference pane, click **New Repository**, then click **LDAP repository**.
- \_\_\_ f. Enter the following properties.
- Repository identifier: PortalClusterLDAP
  - Directory type: IBM Tivoli Directory Server
  - Primary host name: portal00
  - Bind distinguished name: uid=wpsbind,cn=users,dc=hal,dc=com
  - Bind password: IBMp0rtal



Global security > Federated repositories > Repository reference > New...

Specifies the configuration for secure access to a Lightweight Directory Access Protocol (LDAP) repository with optional failover servers.

**General Properties**

\* Repository identifier  
PortalClusterLDAP

Repository adapter class name  
com.ibm.ws.wim.adapter.Idap.LdapAdapter

**LDAP server**

\* Directory type  
IBM Tivoli Directory Server

\* Primary host name  
portal00

Port  
389

Failover server used when primary is not available:

| Select                   | Failover Host Name | Port |
|--------------------------|--------------------|------|
| <input type="checkbox"/> | None               |      |

**Security**

Bind distinguished name  
uid=wpsbind,cn=users,dc=hal,dc=com

Bind password  
\*\*\*\*\*

Federated repository properties for login  
uid

LDAP attribute for Kerberos principal name

Certificate mapping  
EXACT\_DN

Certificate filter

- \_\_\_ g. Scroll down, and click **OK**. You should now be back on the Repository reference pane, and the Repository field should show the identifier PortalClusterLDAP. Enter the following properties.
- Unique distinguished name of the base: `dc=hal,dc=com`
  - Check the box for Distinguished name in the repository is different
  - Distinguished name of a subtree in the main repository: `dc=hal,dc=com`

Global security > Federated repositories > Repository reference

**General Properties**

\* Repository  
PortalClusterLDAP

\* Unique distinguished name of the base (or parent) entry in federated repositories  
dc=hal,dc=com

☒ Distinguished name in the repository is different

Distinguished name of a subtree in the main repository  
dc=hal,dc=com

Apply OK Reset Cancel

- \_\_\_ h. Click **OK**.

- \_\_\_ i. You should return to the Federated repositories pane. Change the Primary administrative user name to `uid=wpsadmin,cn=users,dc=hal,dc=com`

[Global security](#) > **Federated repositories**

**General Properties**

\* Realm name  
defaultWIMFileBasedRealm

\* Primary administrative user name  
uid=wpsadmin,cn=users,dc=hal,dc=com

**Server user identity**

☒ Automatically generated server identity

☐ Server identity that is stored in the repository  
 Server user ID or administrative user on a Version 6.0.x node  
  
 Password

☒ Ignore case for authorization

☐ Allow operations if some of the repositories are down

Repositories in the realm:

| Select                                      | Base Entry                    | Repository Identifier             | Repository Type |
|---------------------------------------------|-------------------------------|-----------------------------------|-----------------|
| You can administer the following resources: |                               |                                   |                 |
| <input type="checkbox"/>                    | <a href="#">dc=hal,dc=com</a> | <a href="#">PortalClusterLDAP</a> | LDAP:IDS        |
| <input type="checkbox"/>                    | o=defaultWIMFileBasedRealm    | InternalFileRepository            | File            |

- \_\_\_ j. Scroll down and make sure that you see PortalClusterLDAP listed as a repository in the realm. Click **OK**.
- \_\_\_ k. Click **Save** to save changes to the master configuration.

**Messages**

⚠ Changes have been made to your local configuration. You can:

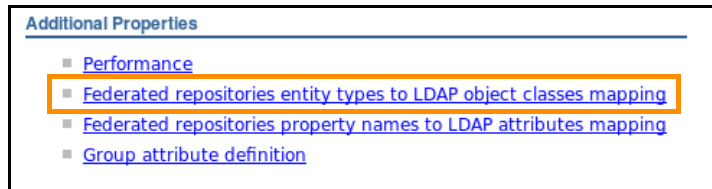
- [Save](#) directly to the master configuration.
- [Review](#) changes before saving or discarding.

An option to synchronize the configuration across multiple nodes after saving can be enabled in [Preferences](#).

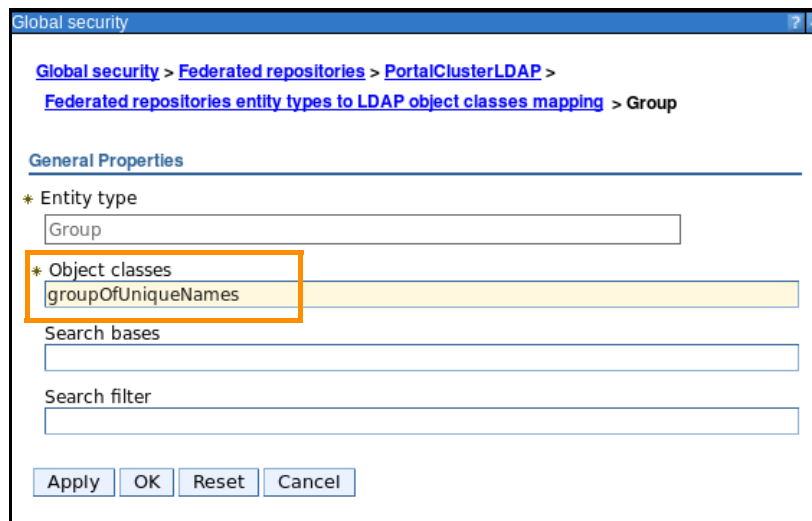
⚠ The server may need to be restarted for these changes to take effect.

- \_\_\_ l. Double check that the Primary administrative user name is changed to `uid=wpsadmin,cn=users,dc=hal,dc=com`. If not, change it again, and click **Save**.
- \_\_\_ 3. Change the LDAP object classes name of the group entity type.
- \_\_\_ a. Return to the Federated repositories pane. (Click **Global security > Configure**).
- \_\_\_ b. Scroll down and click the **PortalClusterLDAP** link in the list of repositories.

- \_\_\_ c. Under Additional properties, click **Federated repositories entity types to LDAP object classes mapping**.



- \_\_\_ d. Click entity type **Group**, and change the object classes name to **groupOfUniqueNames**.



- \_\_\_ e. Click **OK**.
- \_\_\_ f. Click **Save** to save changes to the master configuration.

## Section 4: Verify the new LDAP repository configuration

- \_\_\_ 1. Restart the deployment manager server. You must restart the server so that the new configuration is initialized.
- \_\_\_ a. Open a terminal window, and change directory to `<dmgr_profile>/bin`
- \_\_\_ b. Stop the server by entering the command:
- ```
./stopManager.sh -user installadmin -password IBMp0rtal
```



Important

After the server is restarted, the primary administrative user name is in effect. So you must stop the deployment manager by using the command:

```
stopManager.sh -user uid=wpsadmin -password IBMp0rtal.
```

- ___ c. Start the server with the command: `./startManager.sh`
- ___ 2. Log in to the administration console (WebSphere Integrated Solutions Console) for the deployment manager.
 - ___ a. Start a Firefox web browser and enter the web address:
`http://portal00:9060/ibm/console`
 - ___ b. Log in with the user ID `wpsadmin` and password `IBMp0rtal.`
- ___ 3. Verify access to the LDAP repository.
 - ___ a. In the left navigation of the admin console, click **Users and Groups > Manage Users**.
 - ___ b. You see a list of users from the LDAP repository and the file-based repository.

Manage Users

Search for Users

Search by * Search for * Maximum results

20 users matched the search criteria.

Select	User ID	First name	Last name	E-mail	Unique Name
<input type="checkbox"/>	ajones	Aida Jones	Jones	aiJones@hal.com	uid=ajones,cn=users,dc=hal,dc=com
<input type="checkbox"/>	alones	Alex Jones	jones	alJones@hal.com	uid=alones,cn=users,dc=hal,dc=com
<input type="checkbox"/>	anjones	Andrew Jones	Jones	anjones@hal.com	uid=anjones,cn=users,dc=hal,dc=com
<input type="checkbox"/>	connie	Connie Hohn	Hohn	connie@hal.com	uid=connie,cn=users,dc=hal,dc=com
<input type="checkbox"/>	elaine	Elaine Nemesi	Nemesi	elaine@hal.com	uid=elaine,cn=users,dc=hal,dc=com
<input type="checkbox"/>	installadmin	installadmin	installadmin		uid=installadmin,o=defaultWIMFileBasedRealm
<input type="checkbox"/>	john	John	Brown	john@hal.com	uid=johnbrown,cn=users,dc=hal,dc=com
<input type="checkbox"/>	leisha	Leisha Penny	Penny	leisha@hal.com	uid=leisha,cn=users,dc=hal,dc=com
<input type="checkbox"/>	lisa	Lisa Jones	Jones	lisa@hal.com	uid=lisa,cn=users,dc=hal,dc=com
<input type="checkbox"/>	mjones	Mike Jones	Edwards	mJones@hal.com	uid=mjones,cn=users,dc=hal,dc=com
<input type="checkbox"/>	nyadmin1	nyadmin1	nyadmin1		uid=nyadmin1,cn=users,ou=newyork,dc=hal,dc=com
<input type="checkbox"/>	nymgr1	nymgr1	nymgr1		uid=nymgr1,cn=users,ou=newyork,dc=hal,dc=com
<input type="checkbox"/>	nyuser1	nyuser1	nyuser1		uid=nyuser1,cn=users,ou=newyork,dc=hal,dc=com
<input type="checkbox"/>	paul	Paul Johnson	Johnson	paul@hal.com	uid=paul,cn=users,dc=hal,dc=com
<input type="checkbox"/>	postmaster	Post Master	Master	postmaster@hal.com	uid=postmaster,cn=users,dc=hal,dc=com

- ___ 4. Verify the primary administrative user.
 - ___ a. In the left navigation of the administrative console, click **Users and Groups > Administrative users roles**.

__ b. You should see the user `wpsadmin` listed.

Select	User	Role(s)	Login Status
<input type="checkbox"/>	wpsadmin	Primary administrative user name	Active

Total 1

__ 5. Log out of the administrative console by clicking **Logout**.



Information

Using the Configuration Wizard

In WebSphere Portal 8.5, you can use the Configuration Wizard to complete the tasks that you did manually in this exercise.

In the Configuration Wizard, select the following tasks.

- **Set Up a Cluster > Create a Deployment Manager**
- **Set Up a Cluster > Enable Federated Security**

For each of these tasks, you follow these steps.

- Provide information about your environment.
- Save your configuration settings.
- Choose one of the following options:
 - Click **Download Files** to run the steps remotely.
 - Click **Run All Steps** to run the steps locally.

End of exercise