Course Exercises Guide

WebSphere Application Server V9 Administration in a Federated Environment

Course code WA599 / ZA599 ERC 1.0

IBM Training

November 2016 edition

Notices

This information was developed for products and services offered in the US.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

Trademarks

IBM, the IBM logo, and ibm.com 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” at www.ibm.com/legal/copytrade.shtml.

© Copyright International Business Machines Corporation 2016.
This document may not be reproduced in whole or in part without the prior written permission of IBM.

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

Contents

Trademarks . . . . . **iv**

Exercises description . . . . . **v**

Exercise 1. Configuring the lab workstation **1-1**
Section 1: Resetting the WebSphere environment 1-2
Section 2: Logging in 1-2
Section 3: Validating 1-7

Exercise 2. Creating a federated cell **2-1**
Section 1: Resetting the WebSphere environment 2-2
Section 2: Using the Profile Management Tool to create a deployment manager profile 2-2
Section 3: Backing up the Dmgr profile configuration 2-13
Section 4: Federating profile1 into the cell of the deployment manager 2-15
Section 5: Creating a custom profile and federating it into the deployment manager cell 2-23
Section 6: Adding the IBM HTTP Server to the cell 2-29
Section 7: Adding the web server to the configuration 2-31
Section 8: Mapping modules to servers 2-36
Section 9: Working with the plug-in configuration file 2-38
Section 10: Testing the plug-in configuration 2-42

Exercise 3. Clustering and workload management **3-1**
Section 1: Resetting the WebSphere environment 3-2
Section 2: Checking nodes and node agents 3-2
Section 3: Creating the PlantsCluster cluster 3-2
Section 4: Setting the applications to run on the cluster 3-10
Section 5: Creating a cluster scoped JDBC resource 3-13
Section 6: Testing the application 3-21
Section 7: Configuring session replication settings 3-30
Section 8: Testing the application for session failover 3-33

Exercise 4. Configuring SSL for WebSphere **4-1**
Section 1: Resetting the WebSphere environment 4-3
Section 2: Creating a backup 4-3
Section 3: Creating a profile 4-4
Section 4: Examining the node certificates 4-8
Section 5: Examining certificate expiration and updating 4-14
Section 6: Propagating the plug-in key ring 4-18
Section 7: Configuring SSL for IBM HTTP Server (optional) 4-22
Section 8: Testing the SSL connection 4-26

Appendix A. Resetting the WebSphere environment **A-1**

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Trademarks

The reader should recognize that the following terms, which appear in the content of this training document, are official trademarks of IBM or other companies:

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide.

The following are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide:

AIX®	DataPower®	DB™
DB2®	developerWorks®	Express®
HACMP™	OS/400®	Rational®
Redbooks®	Tivoli®	WebSphere®
z/OS®		

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

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

Windows is a trademark of Microsoft Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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

VMware and the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks (the "Marks") of VMware, Inc. in the United States and/or other jurisdictions.

Social® is a trademark or registered trademark of TWC Product and Technology, LLC, an IBM Company.

Other product and service names might be trademarks of IBM or other companies.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercises description

This course includes the following exercises:

- Exercise 1. Configuring the lab workstation
- Exercise 2. Creating a federated cell
- Exercise 3. Clustering and workload management
- Exercise 4. Configuring SSL for WebSphere

In the exercise instructions, you can check off the line before each step as you complete it to track your progress.

Most exercises include required sections, which should always be completed. It might be necessary to complete these sections before you can start later exercises. If you have sufficient time and want an extra challenge, some exercises might also include optional sections that you can complete.

Important

Online course material updates might exist for this course. To check for updates, see the Instructor wiki at http://ibm.biz/CloudEduCourses.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise 1. Configuring the lab workstation

Estimated time

00:20

Overview

This exercise puts the lab workstation into the proper state to start the course exercises.

Objectives

After completing this exercise, you should be able to:

- Configure the course lab workstation to start the exercises

Introduction

To start the exercises, the lab workstation needs to be set up with several products installed. These product installations are executed for you by using an automated script, which configures the lab machine as necessary for you to start the lab exercises.

Requirements

You need to have access to your course workstation.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise instructions

Section 1: Resetting the WebSphere environment

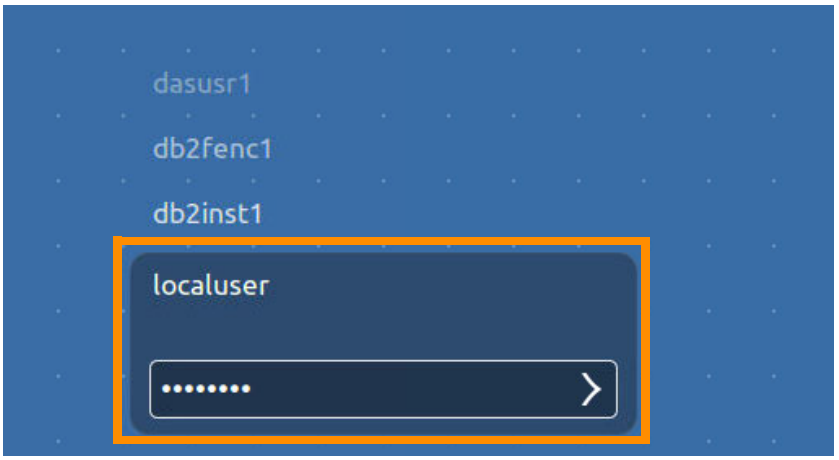
Note

To reset your WebSphere environment, read **Appendix A** for instructions on how to complete this procedure.

Section 2: Logging in

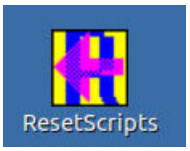
__ 1. When you start your computer, you are prompted for a user ID and password. At this prompt, enter:

- User ID: `localuser`
- Password: `passw0rd` (lowercase with a zero replacing the o)



__ 2. Run the ResetScripts.

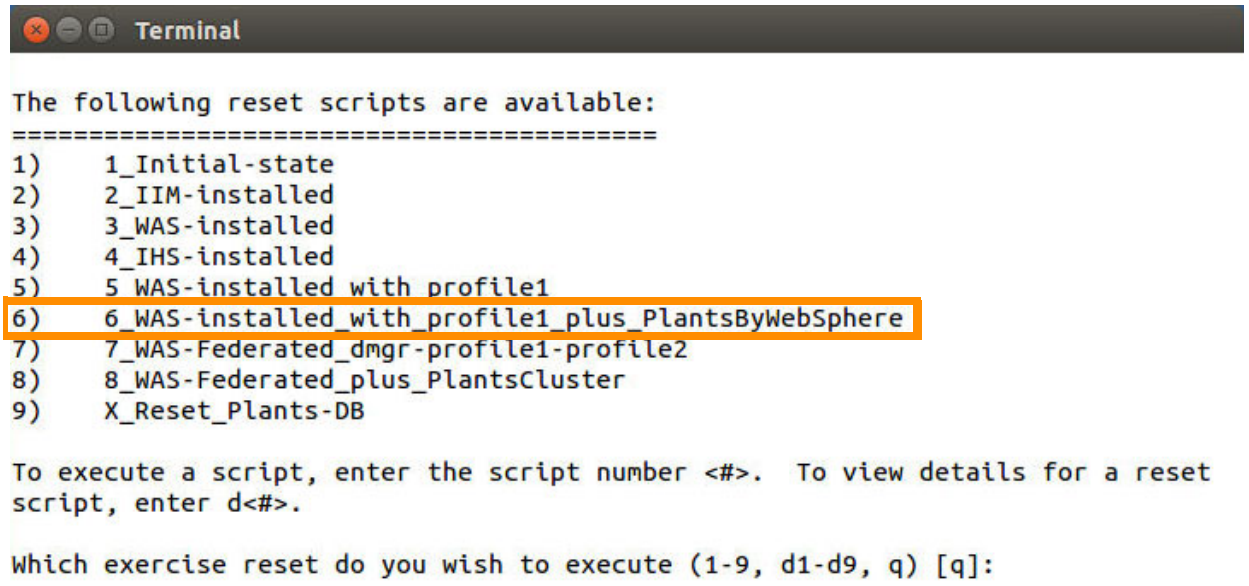
__ a. Double-click the **ResetScripts** icon on the desktop.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ b. A shell window displays the list of possible reset states to choose from. If you have problems with the lab exercises, these reset states can be used to set up the initial machine configuration or to recover the current state.



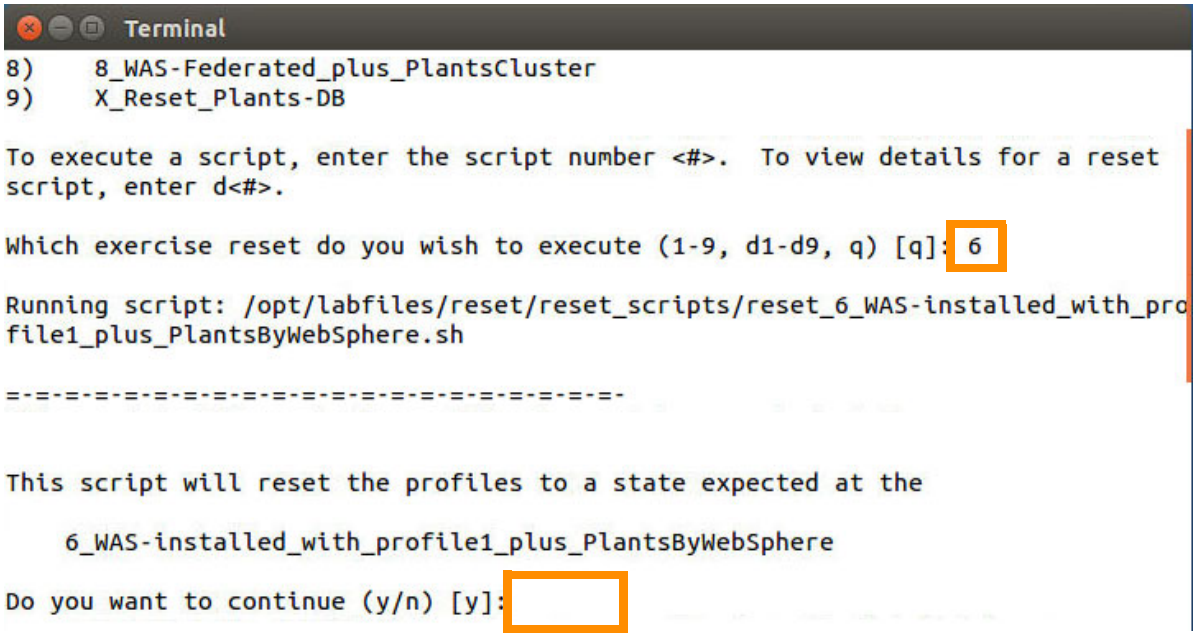
__ c. Type `6` and press Enter. This option represents the state **6_WAS-installed_with_profile1_plus_PlantsByWebSphere** where the following products are installed and configured:

- IBM Installation Manager
- WebSphere Application Server
- IBM HTTP Server
- IBM HTTP Server Plug-in
- WebSphere Customization Toolbox
- profile1 configuration with PlantsByWebSphere restored

© Copyright IBM Corp. 2016

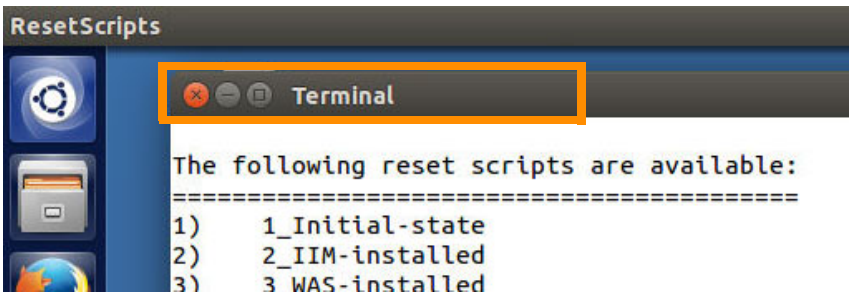
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ d. The script confirms the reset state and prompts you whether you would like to continue. Press Enter.

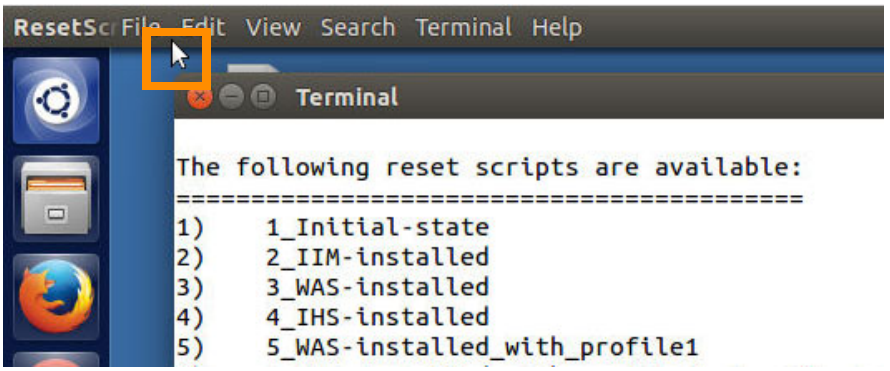


Note

The Unity desktop interface is a little different than many other desktops in a subtle way. Notice that menu options for the active application do not appear on the title bar.



To make the menu options appear, move the mouse to the top of the desktop.



Moving the mouse to the top of the desktop has the same behavior in most applications.

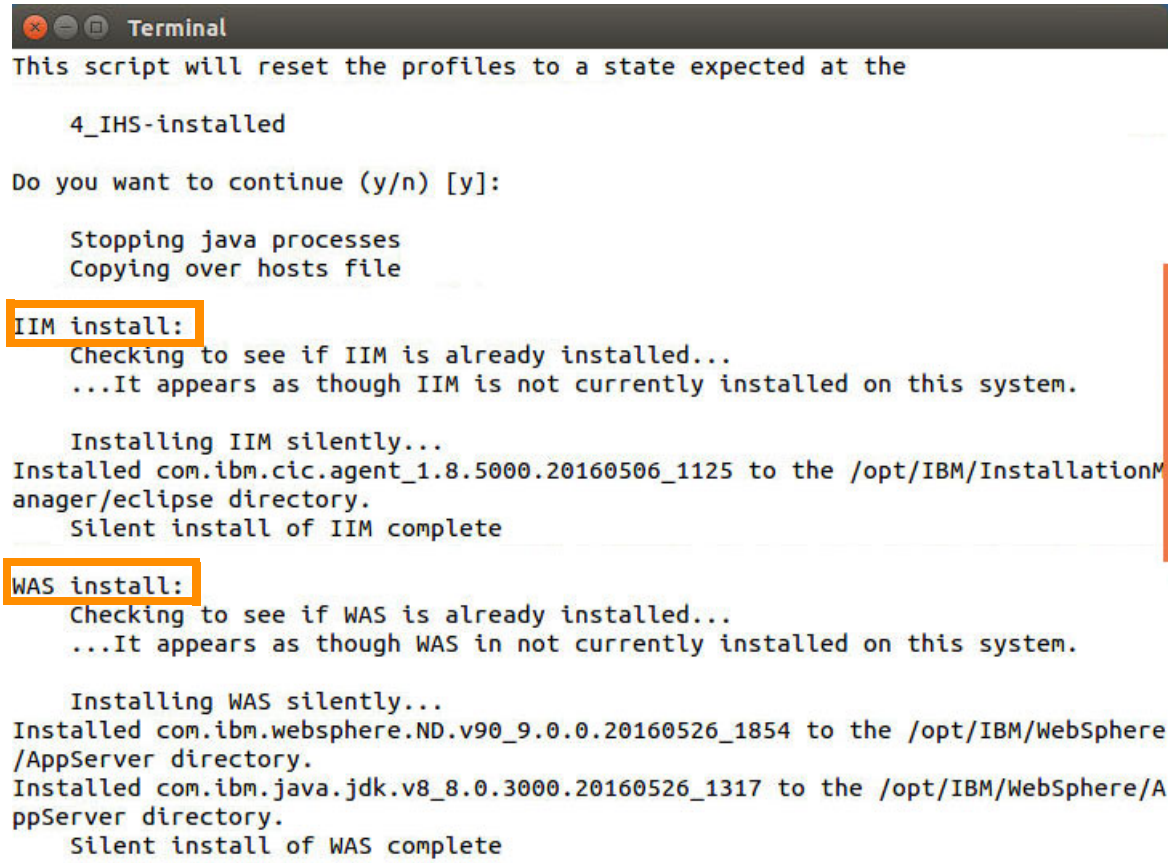
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ 3. Wait for the scripts to complete and review the output.

__ a. The installation process starts with the following tasks:

- Stopping any running Java processes
- Installing IBM Installation Manager
- Installing WebSphere Application Server

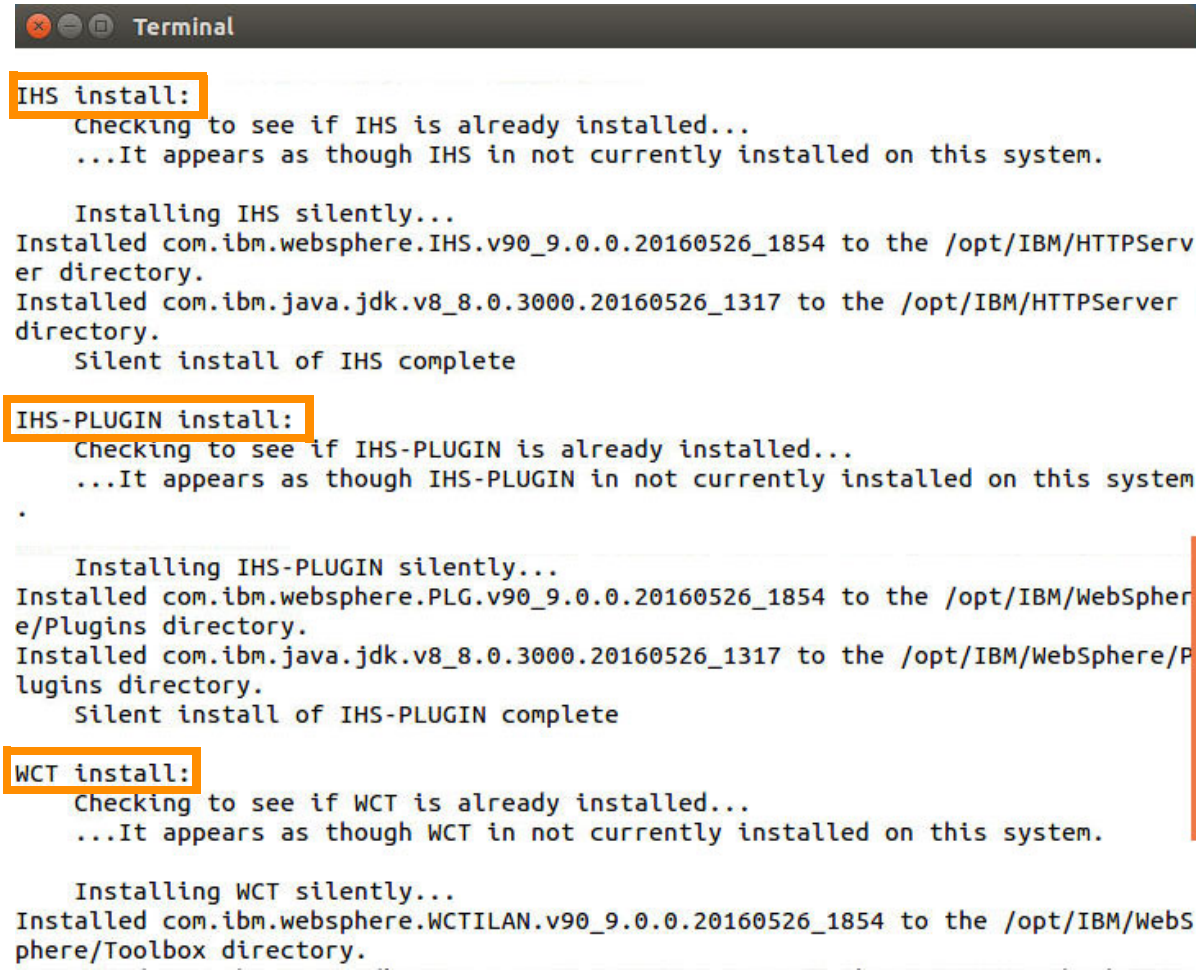


© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ b. The installation then continues with these tasks:

- Installing IBM HTTP Server
- Installing the IBM HTTP Server plug-in
- Installing WebSphere Customization Toolbox

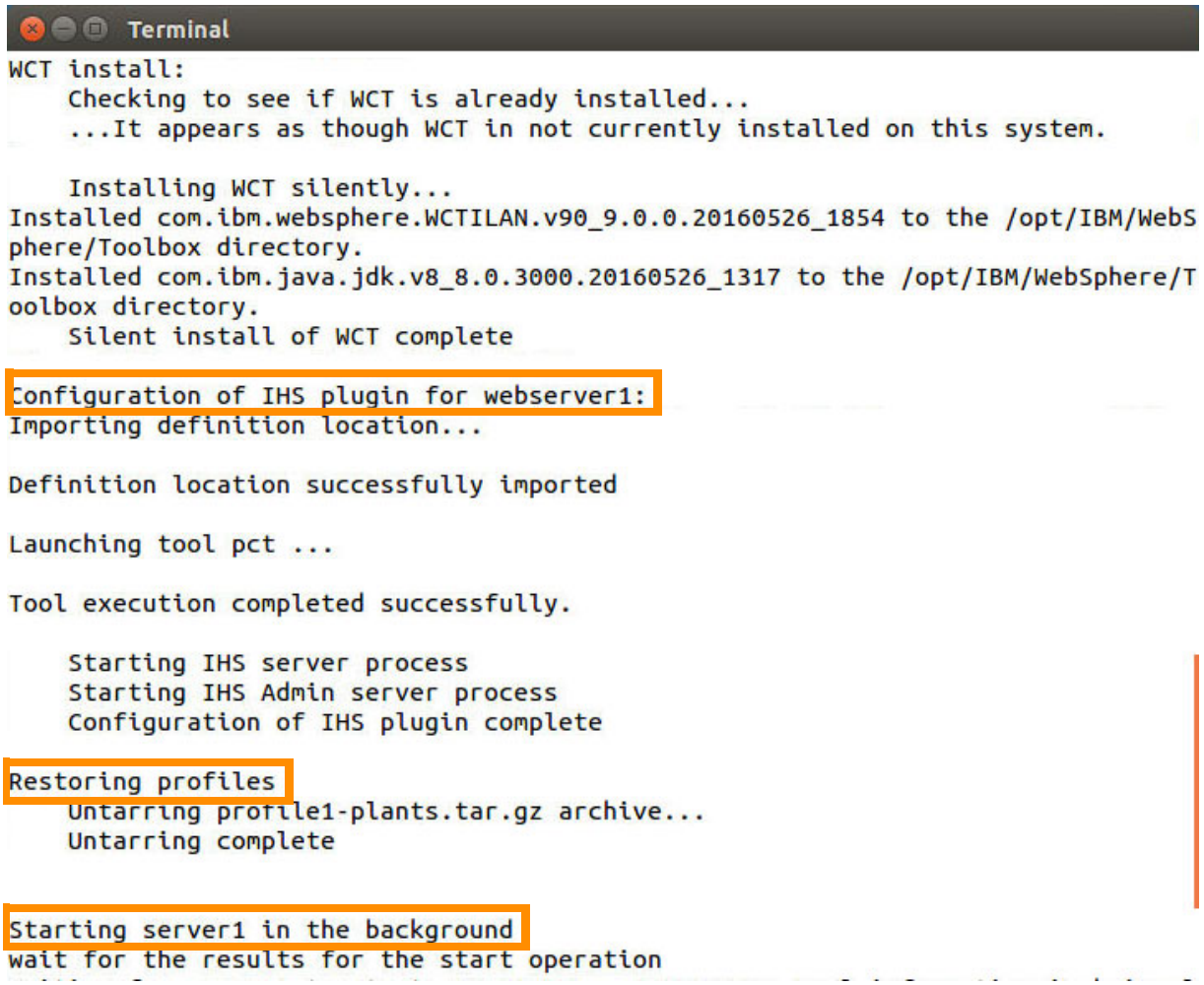


© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ c. Finally, the installation script completes these tasks:

- Configuring the IBM HTTP Server plug-in
- Starting the IBM HTTP Server processes
- Restoring the profile1 configuration
- Starting server1



__ d. When the installation script is finished, press Enter to close the window.

Section 3: Validating

__ 1. Confirm that the WebSphere Application Server is installed.

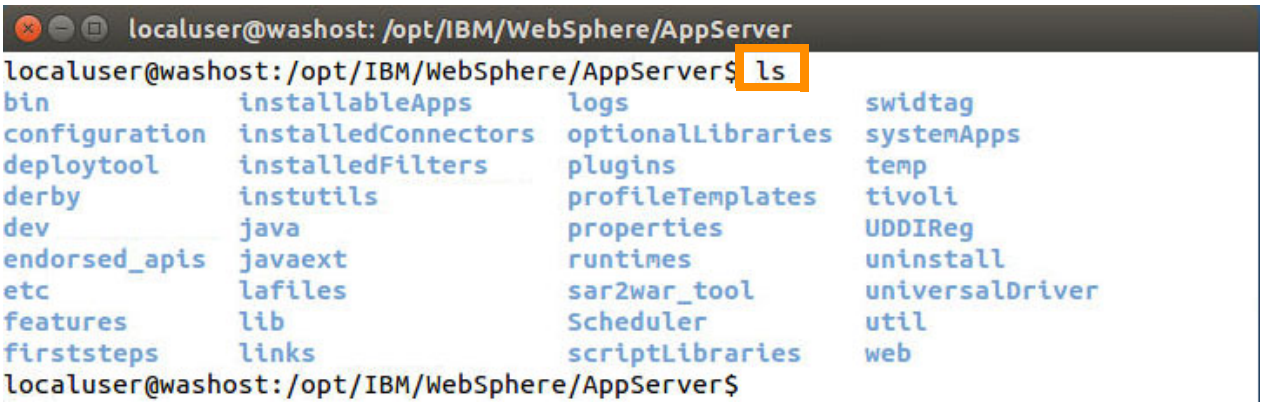
__ a. Open a terminal window and change to the following directory:

```
/opt/IBM/WebSphere/AppServer/
```

© Copyright IBM Corp. 2016

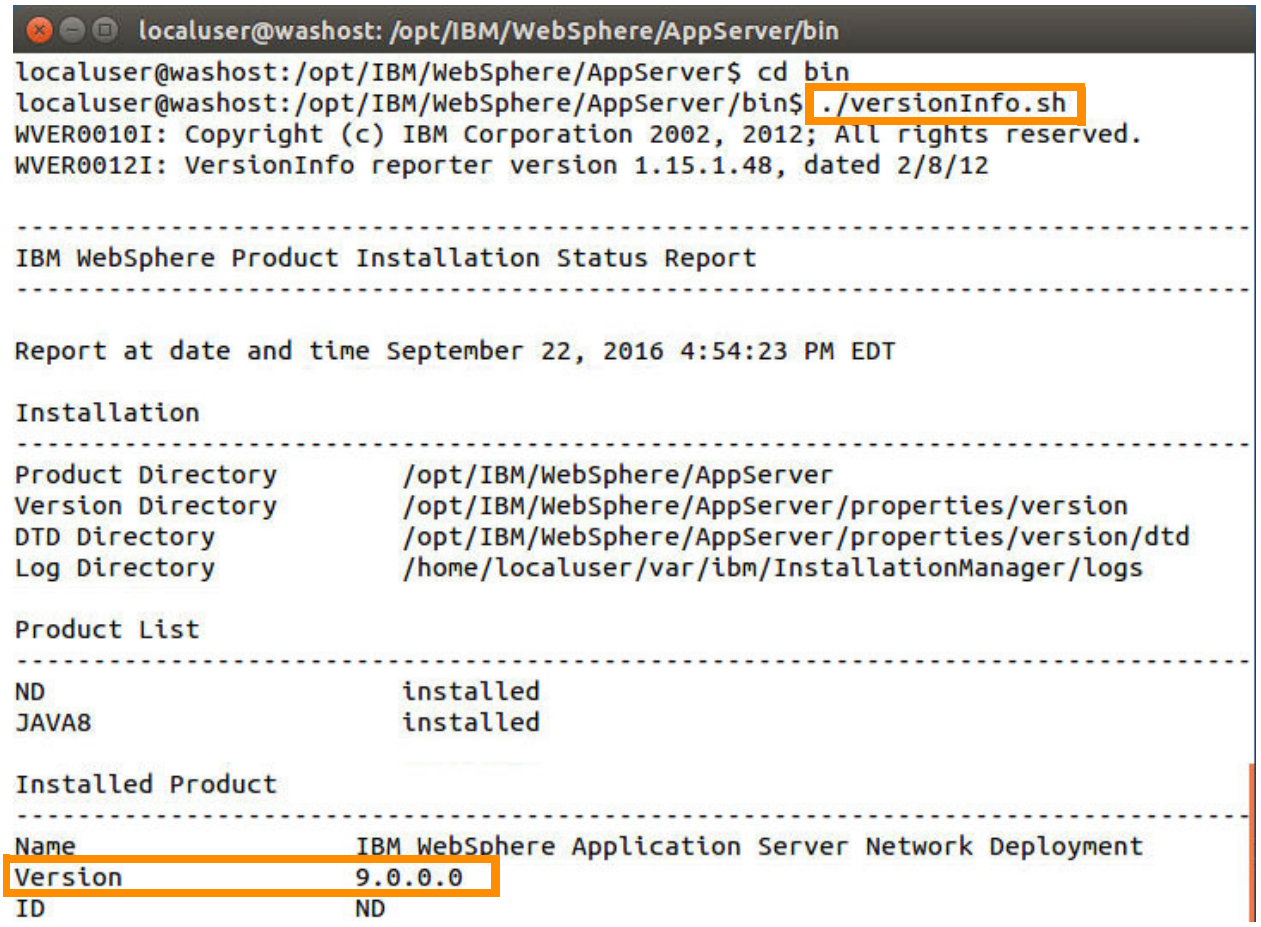
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ b. Use the `ls` command to confirm that the directory has been populated.



__ c. Change into the `bin` directory and use the following command to check the version:

```
./versionInfo.sh
```



© Copyright IBM Corp. 2016

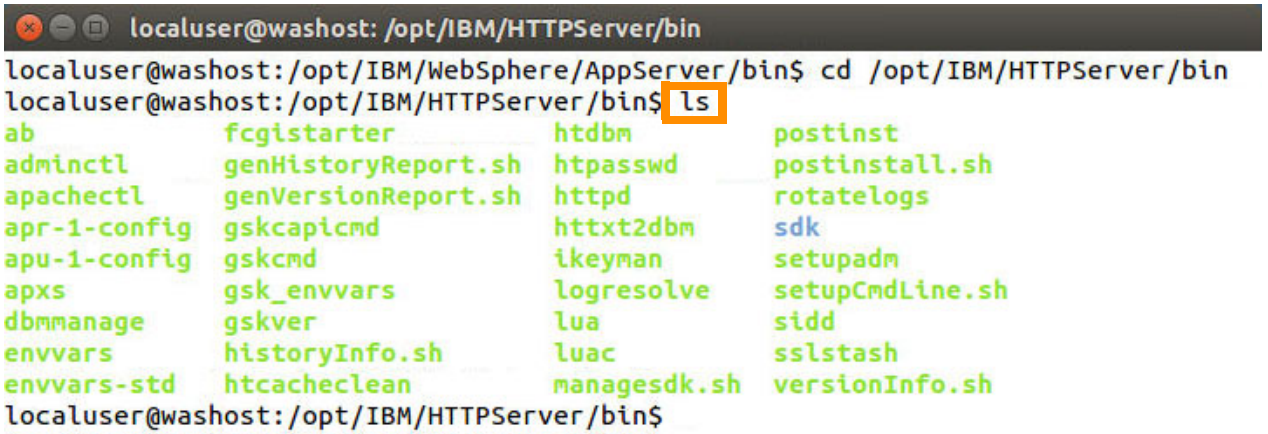
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ 2. Confirm that the IBM HTTP Server is installed.

__ a. In the terminal window, change to the following directory:

```
/opt/IBM/HTTPServer/bin
```

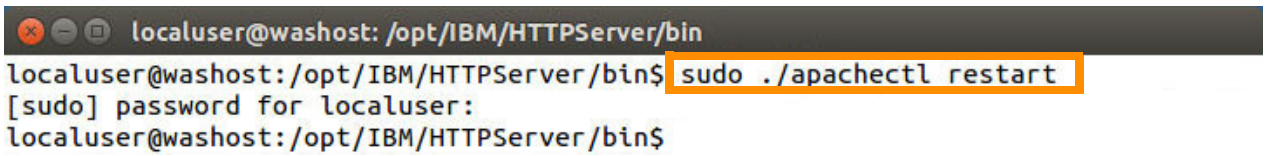
__ a. Use the `ls` command to confirm that directory has been populated.



__ b. Use the following command to restart the web server:

```
sudo ./apachectl restart
```

When prompted, enter `passw0rd` for the password.



End of exercise

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise review and wrap-up

In this exercise, you configured the lab machine so that it is ready to start the lab exercises.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise 2. Creating a federated cell

Estimated time

01:30

Overview

In this lab exercise, you experience the process of creating a WebSphere cell through the generation of a deployment manager profile and by the federation of application server profiles.

Objectives

After completing this exercise, you should be able to:

- Create a deployment manager profile
- Back up the deployment manager configuration
- Perform basic tasks by using the deployment manager administrative console
- Federate a node into the deployment manager cell
- Create a custom profile
- Create an unmanaged web server node
- Start and stop a web server by using the administrative console
- Map an application to a web server

Introduction

This exercise examines the process of creating and federating a cell. The initial steps include creating two more profiles, the first of which is a deployment manager profile. After the deployment manager profile is created, profile1 is federated into the cell. Then, a custom profile is created and federated at the same time.

This exercise demonstrates the process of creating a cell and prepares the lab environment for other important steps, including creating a node to manage a remote web server and clustering an application server.

Requirements

To complete this exercise, the application server that is named server1 must be started. The DefaultApplication and PlantsByWebSphere applications must be installed and running on server1.

This exercise is required for the remaining exercises. This exercise requires that WebSphere is installed with profile1 and the PlantsByWebSphere application.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise instructions

Preface

To do this exercise, you must complete the Installing IBM Installation Manager and Installing WebSphere Application Servers exercises as those exercises set up the environment that is used in this exercise.

Important

The labs use two variables to define various installation paths. On Linux, the variable definitions are as follows:

```
<was_root>: /opt/IBM/WebSphere/AppServer
<profile_root>: /opt/IBM/WebSphere/AppServer/profiles
```

During this exercise, you change your stand-alone application server environment to a cell environment that contains two federated nodes and an unmanaged node for a web server. It is important as you progress through the exercise that you have a good understanding of what you are creating.

As you begin the exercise, you have one stand-alone application server, named `server1`, contained in a node, named `washostNode01`.

When you complete the exercise, you have a cell, named `washostCell01`, containing the following nodes:

- Deployment manager node, named `washostCellManager01`
- A federated node, named `washostNode01`, containing a node agent and an application server, named `server1`
- A federated node, named `washostNode02`, containing only a node agent
- An unmanaged node, named `ihsnode`, containing an IBM HTTP Server administrative process and a web server, named `webserver1`

Section 1: Resetting the WebSphere environment

Note

To reset your WebSphere environment, read **Appendix A** for instructions on how to complete this procedure.

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

During this section of the exercise, you use the Profile Management Tool to create a deployment management profile. The deployment manager profile defines a cell, named `washostCell01`,

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

containing a deployment manager node, named `washostCellManager01`. The existing application server, `server1`, continues to be a stand-alone server that is contained in the node `washostNode01`.

The Profile Management Tool is part of the WebSphere Customization Toolbox, and is a GUI tool for creating WebSphere profiles. Using the profile wizard, you can create an application server profile, deployment manager profile, custom profile, or cell profile (which creates both a deployment manager and managed node).

Information

It is possible to create profiles from the command line by using the `manageprofiles -create` script that is in the `/opt/IBM/WebSphere/AppServer/bin` directory.

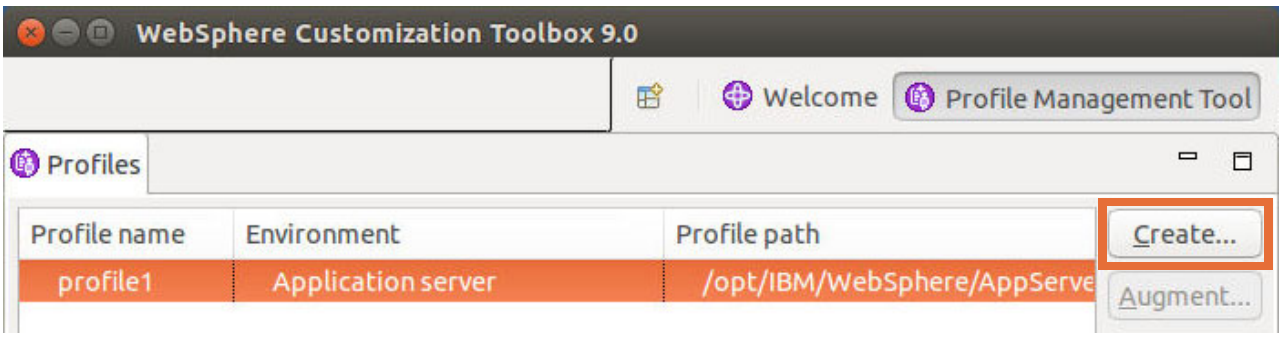
```
./manageprofiles.sh -create -profileName profile2
-profilePath /opt/IBM/WebSphere/AppServer/profiles/profile2
-templatePath /opt/IBM/WebSphere/AppServer/profileTemplates/default
-nodeName washostNode02 -cellName washostCell02
-hostName washost
```

__ 1. Start the WebSphere Customization Toolbox.

__ a. The command to start the WebSphere Customization Toolbox is:

```
/opt/IBM/WebSphere/AppServer/bin/ProfileManagement/wct.sh
```

__ b. Select the **Profile Management Tool** and click **Create**.

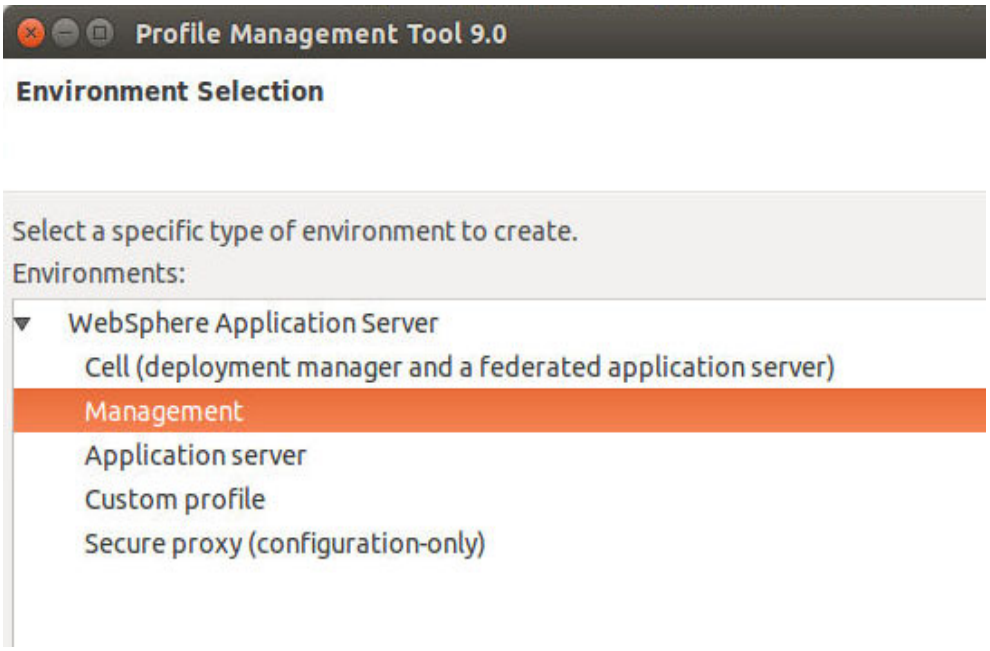


© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

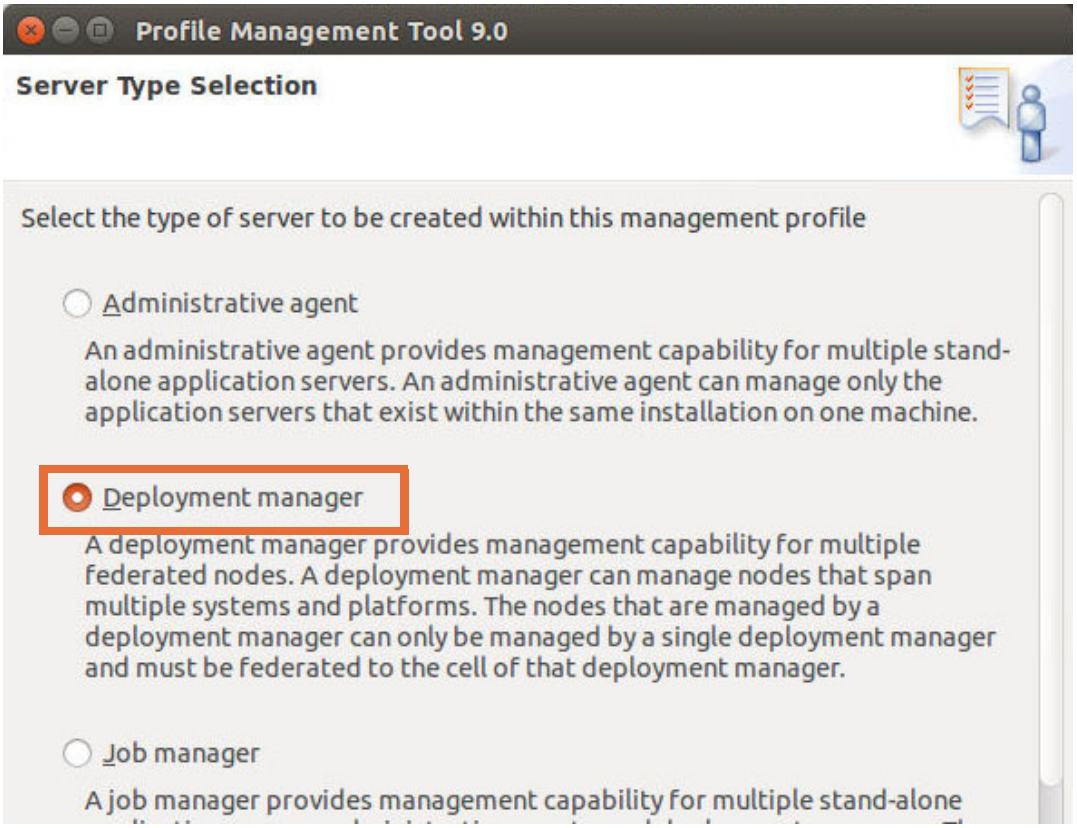
__ 2. Create a deployment manager profile called Dmgr.

__ a. From the Environment Selection panel, select **Management** and click **Next**.



__ b. From the Server Type Selection panel, select **Deployment manager**.

__ c. Click **Next**.



__ d. Select **Advanced profile creation** to specify your own configuration values during profile creation. Click **Next**.

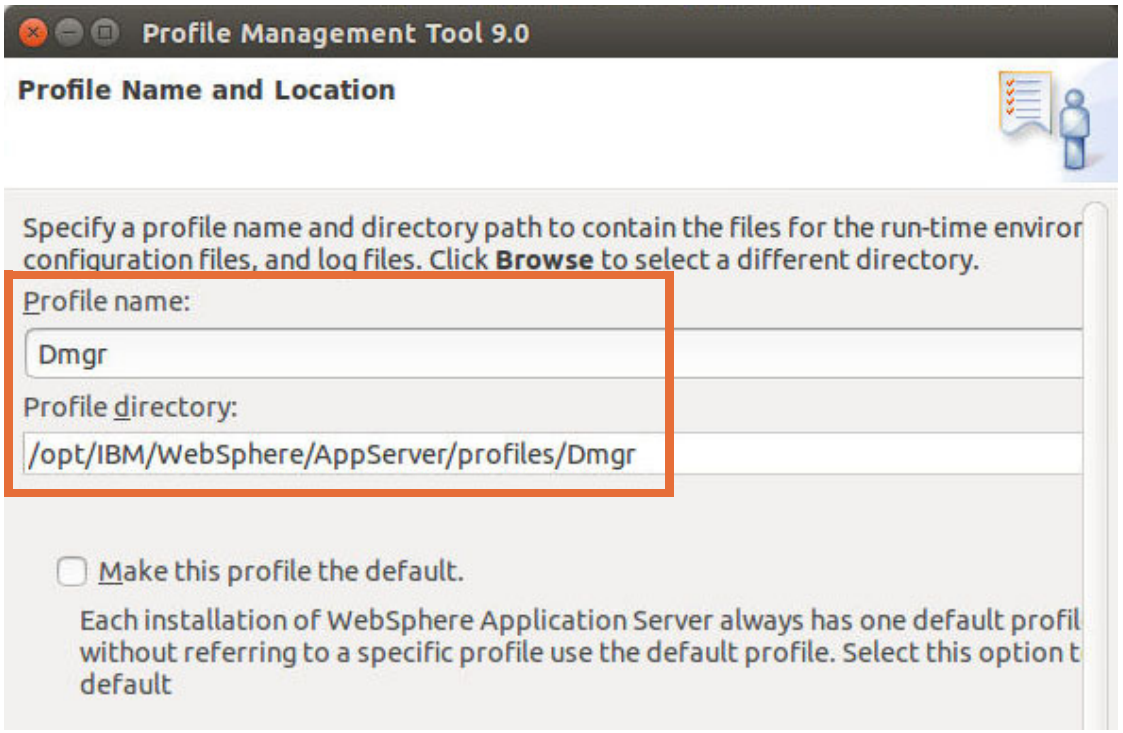
© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ e. Ensure that the **Deploy the administrative console (recommended)** check box is selected. The administrative console is needed for this class. Click **Next**.

__ f. From the Profile Name and Location panel, 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** check box.

__ g. Click **Next**.



© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Information

The default profile is the first profile created. It is also possible to change which profile is designated as the default with the Profile Management Tool or the `manageprofiles` command.

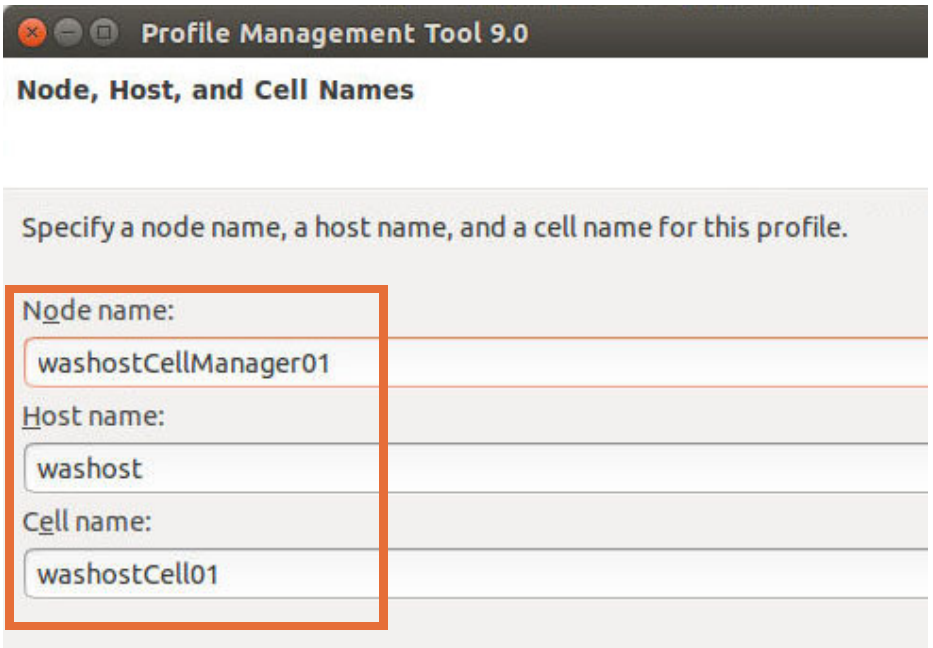
When running commands from the `/opt/IBM/WebSphere/AppServer/bin` directory, commands are run against the runtime that the default profile defines. It is also possible to use the `-profileName` argument to specify a particular profile.

__ h. You can use the **Node, Host, and Cell Names** panel to set the node name, cell name, and host name. Default values are completed based on the detected host name for your server.

Note

On UNIX systems, the host name can be the long name (`washost.ibm.com`). Accept whatever the default is. Make sure that you are consistent in later exercises.

Ensure that the **Node name**, **Host name**, and **Cell name** are correct (they are based on the short form of the host name and not localhost: for example, `washostCellManager01`, `washost`, and `washostCell01`). If the fields include `localhost` as part of the name, replace `localhost` with the **host name**. For example, change `localhostCellManager01` to: `washostCellManager01`



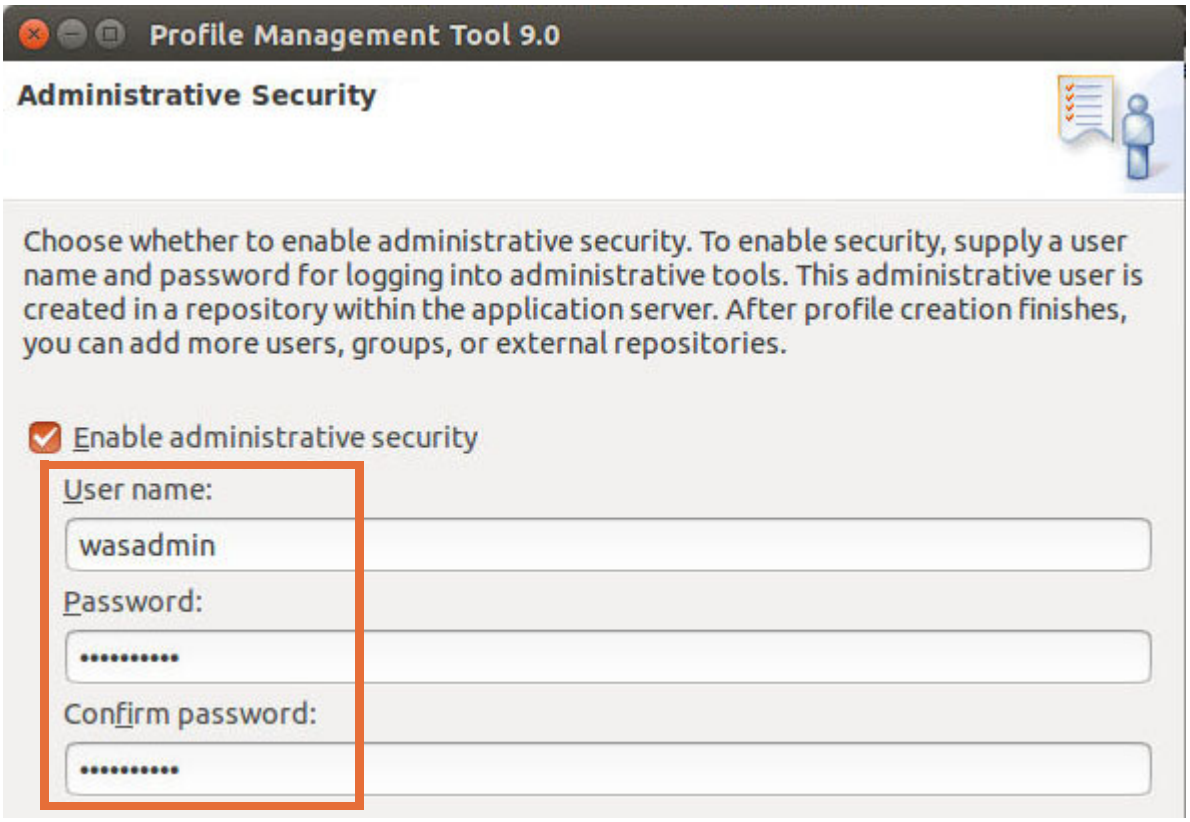
__ i. Click **Next**.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ j. From the Administrative Security panel, you choose whether to enable administrative security. Verify that the **Enable administrative security** check box is selected. Enter the following information:

- **User name**: `wasadmin`
- **Password**: `web1sphere`
- **Confirm password**: `web1sphere`

__ k. Click **Next**.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ l. From the Security Certificate (Part 1) panel, accept the default selections:

- Create a default personal certificate
- Create a root signing certificate

Click **Next**.

Note

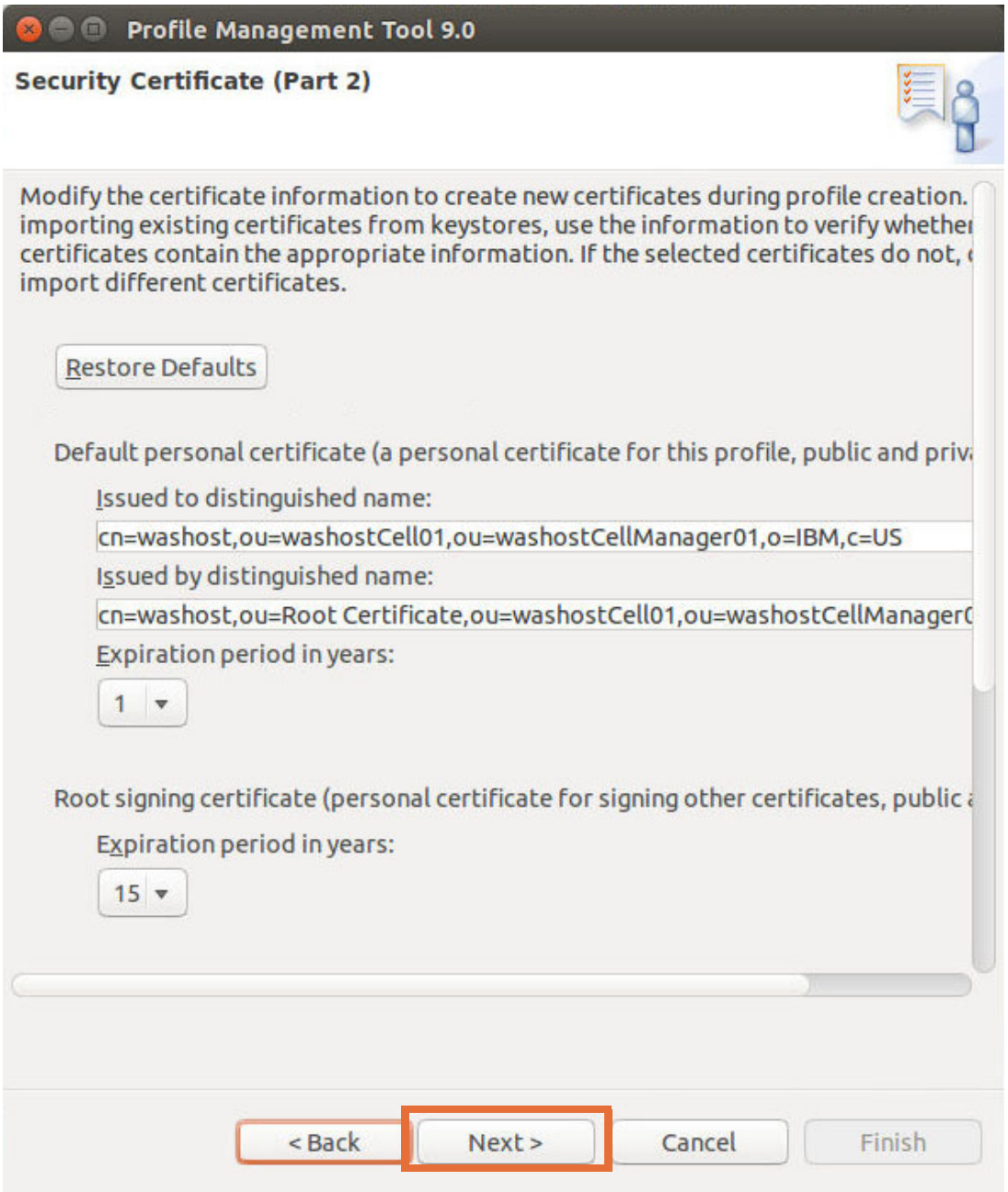
The **Issued to distinguished name** and the **Issued by distinguished name** on the Security Certificate (Part 2) panel have a common name (CN) that can take different forms, depending on your environment:

- IP address (such as `192.168.192.128`)
- Fully qualified domain name (FQDN) (such as `washost.localdomain` or `washost.ibm.com`)

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ m. Accept the Security Certificate (Part 2) panel defaults. Click **Next**.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

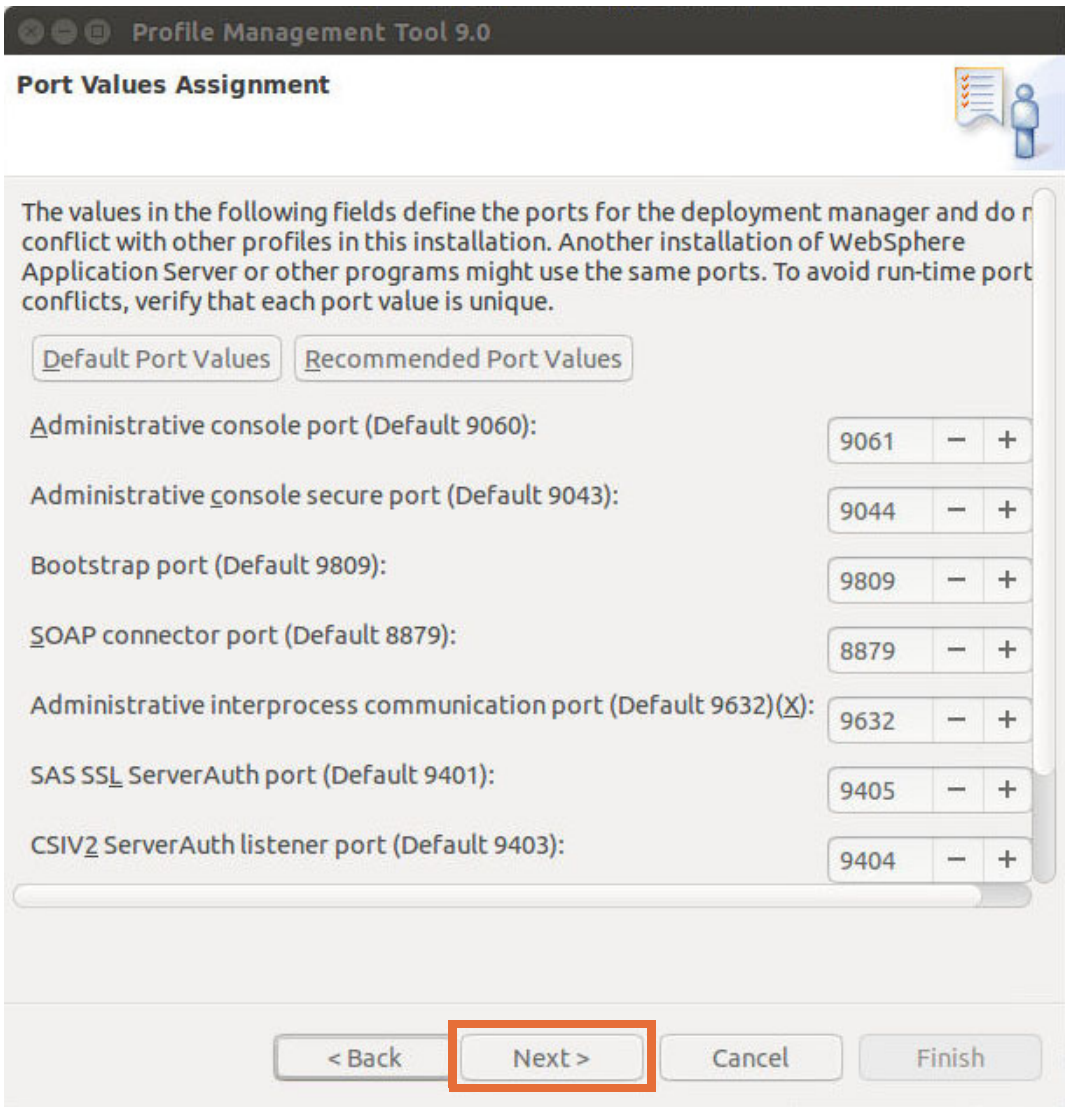
__ n. You can use the Port Values Assignment panel to set any ports for the deployment manager to prevent conflicts with other profiles. Accept the default port values (which can be different from the example shown).

Information

Note the administrative console port for the deployment manager. This port is used later in this exercise.

Ordinarily, the administrative console port would use port 9060. However, since a stand-alone application server is installed, the Profile Management Tool avoids reuse of any ports. It uses port 9061 instead.

__ o. Click **Next**.



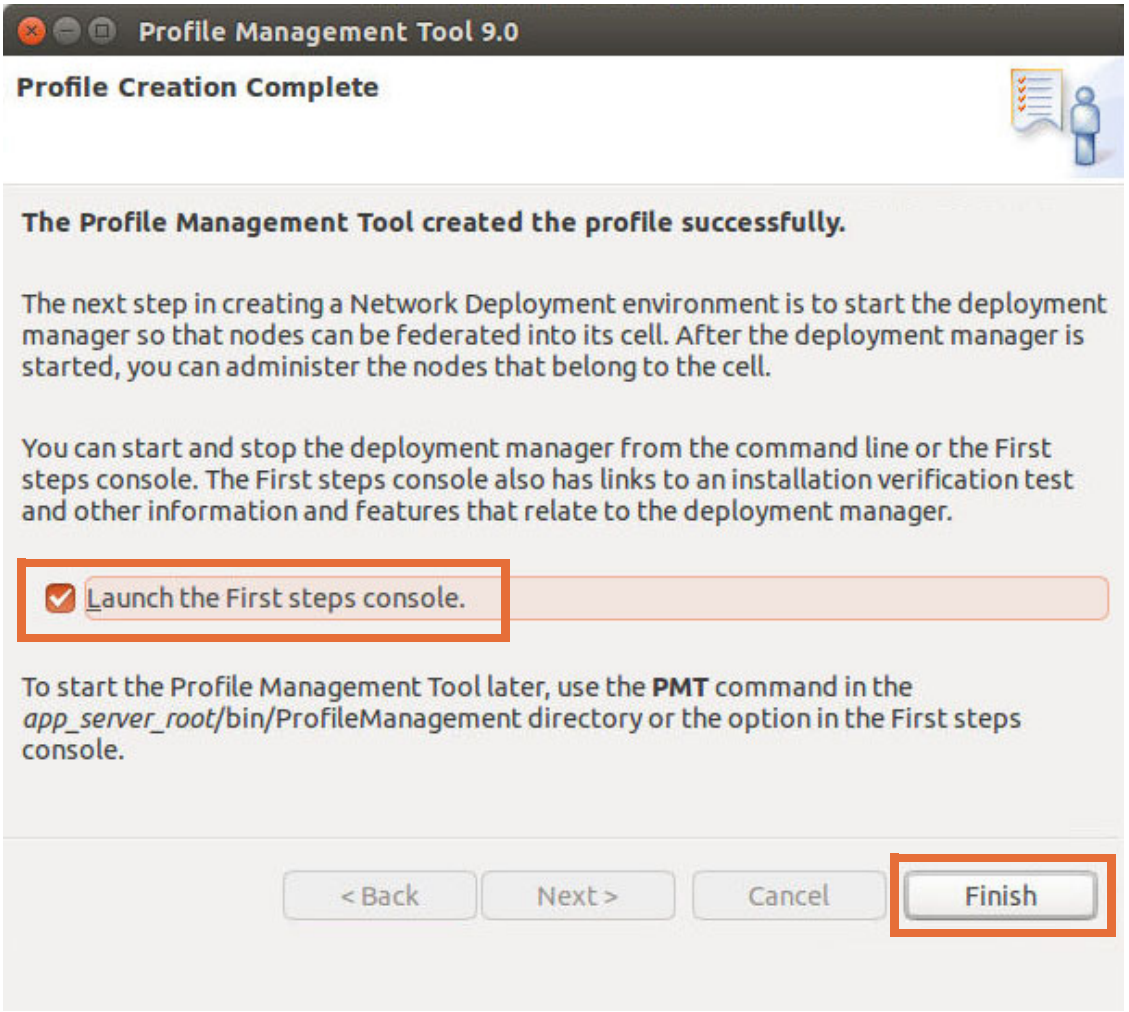
__ p. The Profile Creation Summary panel shows all of the choices you made on previous panels. Verify the summary information with what you entered previously. Click **Create**.

Creation of the profile usually takes several minutes to complete.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ q. The profile creation completes and the Dmgr profile is created. Notice that the **Launch the First steps console** check box is selected. Click **Finish**, and the First steps console launches.

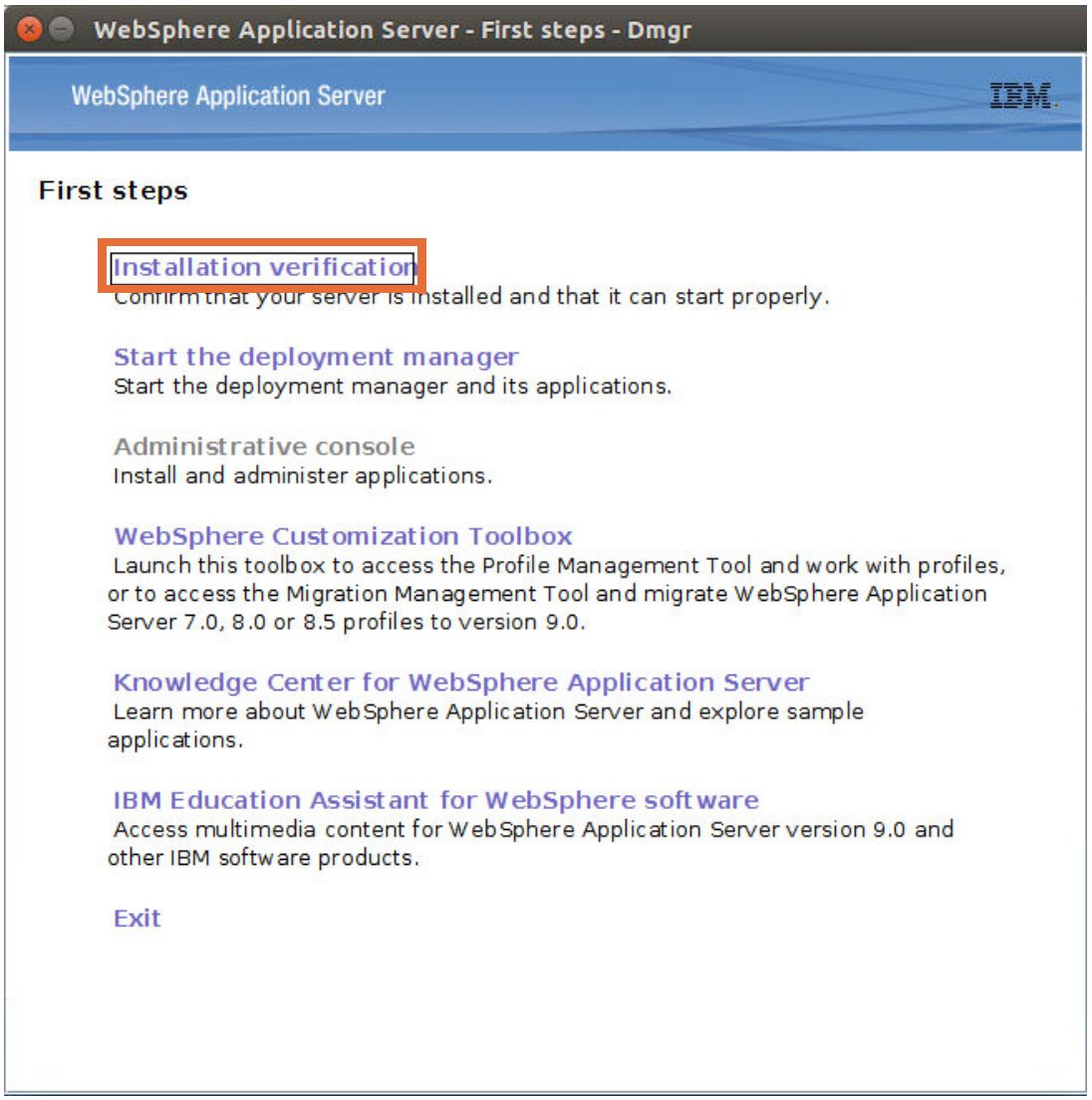


__ 3. The First steps console is associated with the deployment manager profile, `Dmgr`, that was created. Each profile has its own First steps console.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Click **Installation verification** from the First steps console.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ a. The installation verification test tool runs and shows messages to indicate verification status. Use the scroll bar to scroll to the bottom to see all the messages. If the installation verification was successful, the following messages are shown:

```
IVTL00701: The Installation Verification Tool verification succeeded.
IVTL00801: The installation verification is complete.
```

Information

It is possible that several warnings might be shown. These warning messages can be ignored.

__ 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: Backing up the Dmgr profile configuration

Before continuing, it is a good practice to back up the configuration for the Dmgr profile that was created.

__ 1. Create a backup.

Information

In a previous lab, the `backupConfig` command was used to create a backup. Another WebSphere tool makes backups of a profile as well (other than operating system-level backups). The backupConfig tool backs up only the configuration directory of a profile. The command `manageprofiles -backupProfile` backs up the configuration directory and other metadata.

The IBM Knowledge Center article on the `manageprofiles` command defines the `-backupProfile` attribute as follows:

> This attribute forms a file system backup of a profile folder and the profile metadata from the profile registry file. Any servers that use the profile that you want to back up must first be stopped before starting the `manageprofiles` command with the `-backupProfile` option. The `-backupProfile` parameter must be used with the `-backupFile` and `-profileName` parameters, for example:
>
> `./manageprofiles.sh -backupProfile -profileName /opt/IBM/WebSphere/AppServer -backupFile <backupFile_name>`

__ a. In a terminal window, navigate to the `/opt/IBM/WebSphere/AppServer/profiles/Dmgr/bin` directory.

__ b. Verify the status of the deployment manager process by entering the following command:

```
./serverStatus.sh -all
```

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Enter the user ID **wasadmin** and password **web1sphere** in the dialog box when you are prompted.

__ c. If the deployment manager process is running, stop the process by entering the following command:

```
./stopManager.sh
```

Enter the user ID **wasadmin** and password **web1sphere** in the dialog box when prompted.

__ d. If the `/opt/labfiles/backups` directory does not exist, create it.

__ e. After the deployment manager stops, enter the following command to back up the entire profile:

```
./manageprofiles.sh -backupProfile -profileName Dmgr -backupFile
/opt/labfiles/backups/Dmgr_initial_backup.zip
```

Wait for the message:

```
INSTCONFSUCCESS: Success: The profile backup operation was successful.
```

__ 2. Since profile1 is federated later, create a backup for it as well.

__ a. Navigate to the `/opt/IBM/WebSphere/AppServer/profiles/profile1/bin` directory, and stop server1 by entering the following command:

```
./stopServer.sh server1
```

__ b. Make sure to enter the `manageprofiles` command from the *<profile_root>*`/profile1/bin` directory. After server1 stops, enter the following command to back up the entire profile:

```
./manageprofiles.sh -backupProfile -profileName profile1 -backupFile
/opt/labfiles/backups/Profile1_prefederation.zip
```

Wait for the message:

```
INSTCONFSUCCESS: Success: The profile backup operation was successful.
```

__ 3. Start the deployment manager.

__ a. In a terminal window, navigate to `/opt/IBM/WebSphere/AppServer/profiles/Dmgr/bin` and enter the following command to start the deployment manager:

```
./startManager.sh
```

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Section 4: Federating profile1 into the cell of the deployment manager

During this section of the exercise, you federate the application server node, which profile1 defines (and is named `washostNode01`), into the cell that is named `washostCell01`, which the deployment manager profile defines. The federation process adds a node agent to the application server node.

__ 1. Verify that server `server1` is running.

__ a. If you backed up the profile for profile1 in the previous section, the server `server1` must be started. Backing up a profile causes the profile server to stop. Navigate to the `/opt/IBM/WebSphere/AppServer/profiles/profile1/bin` folder and enter the following command:

```
./serverStatus.sh server1
```

__ b. If server1 is not running, start server1.

__ 2. Open the administrative console for the deployment manager.

Reminder

The port in this case is not the default port, but instead is port 9061. This difference is because the system already has profile1, which is using port 9060, for its administrative console port. Therefore, the profile creation process chose the next available port (9061) for the deployment manager administrative console.

__ a. Open a web browser and enter the following address:

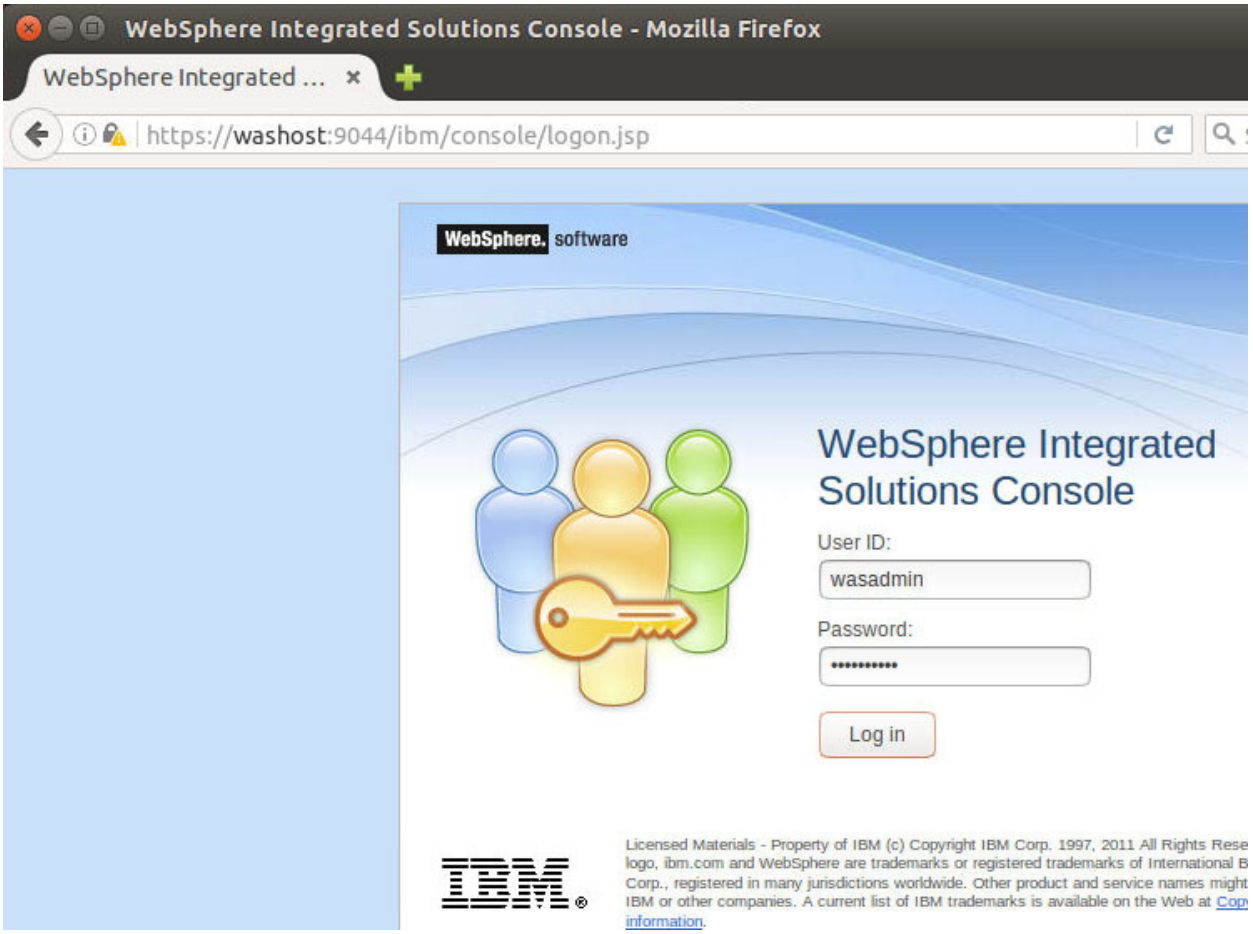
```
http://washost:9061/ibm/console
```

__ b. The browser might show a message that says the connection is not secure. Assuming you are using Firefox, click **Advanced** and then click **Add Exception.** In the **Add Security Exception** dialog box, click **Confirm Security Exception**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ c. Log in to the administrative console with `wasadmin` as the user name and `web1sphere` as the password.



__ 3. Federate a node into the cell.

This process takes the existing application server within profile1 and federates it to the deployment manager. This action means that it no longer is a stand-alone application server, but instead is part of the newly created cell.

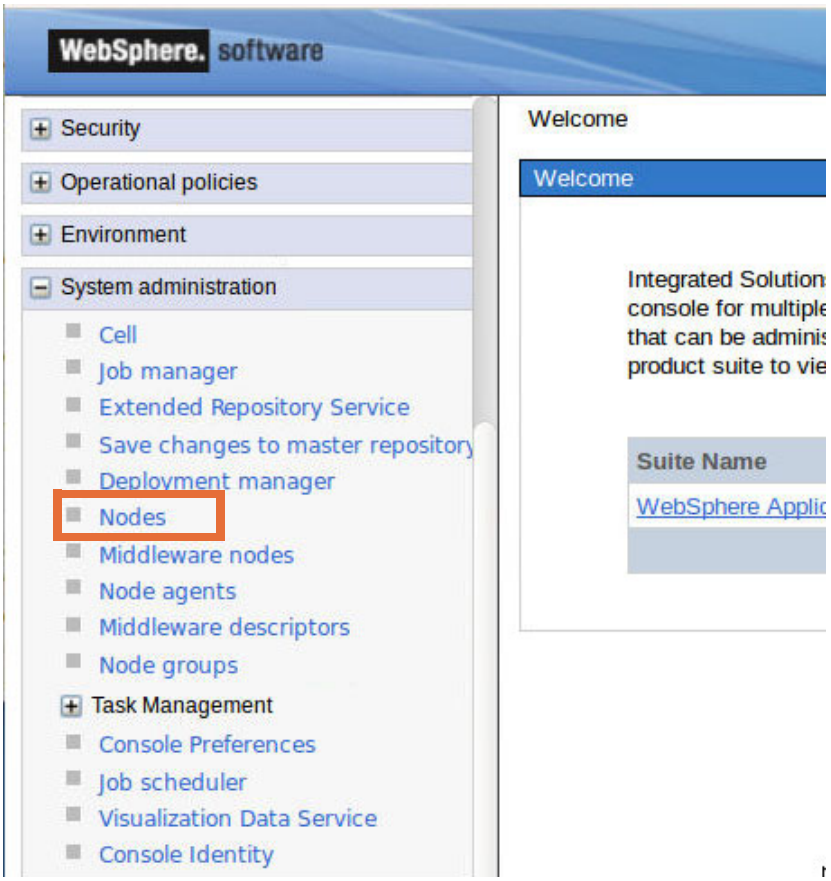
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Information

In this lab environment, synchronizing clocks is not an issue since the cell is running on a single computer. But, when federating distributed computers, it is necessary to make sure that the clocks on all nodes are within 5 minutes of each other.

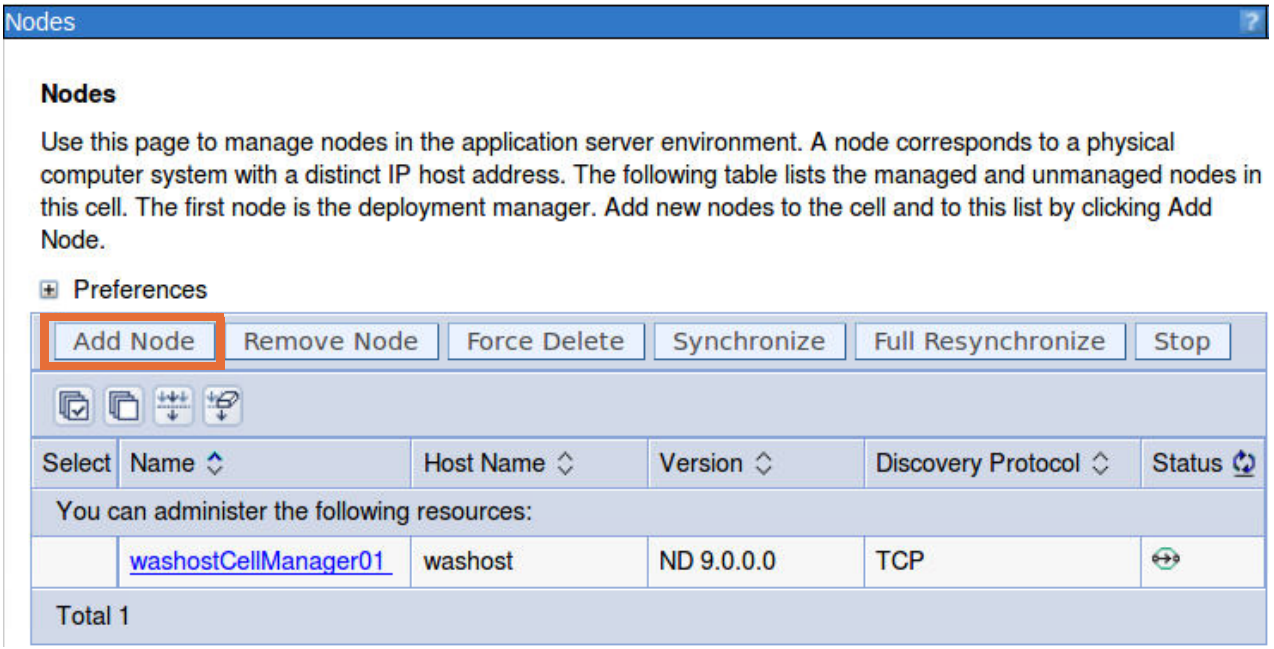
__ a. From the deployment manager administrative console, click **System administration > Nodes**.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

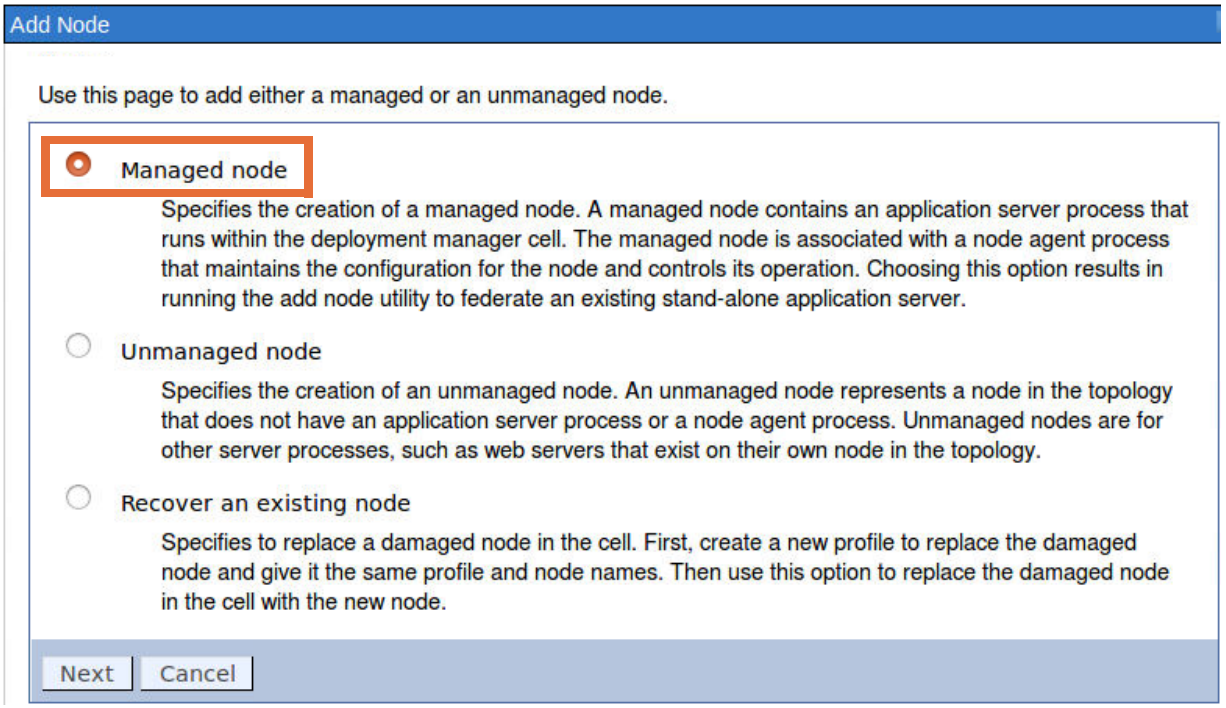
__ b. Click **Add Node**.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ c. The **Managed node** option is selected as default. A managed node contains an application server and a node agent. The application server runs as part of the network deployment environment. Keep the default setting and click **Next**.



Information

As the description on the screen capture indicates, a managed node is a node with an application server and a node agent that belongs to a deployment manager cell. However, a managed node contains a node agent, but initially might not contain an application server.

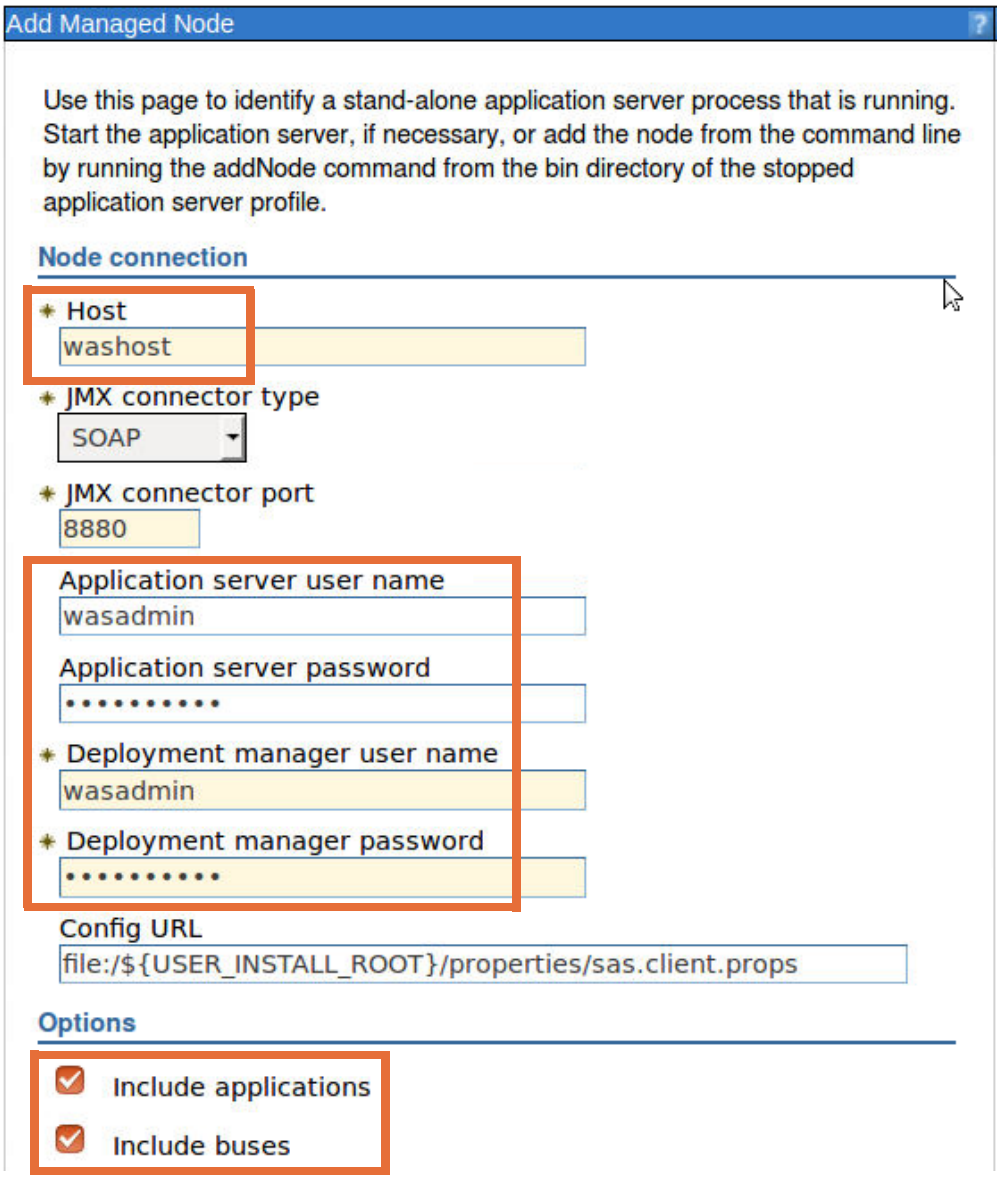
In this part of the exercise, you are adding a stand-alone node. Adding a managed node in this way, you have an application server, server1, and it is the node agent process that makes it a managed node.

__ d. Enter your host name `washost` for the host. Specify security user names and passwords for both profile1 and the deployment manager. Enter `wasadmin` and `web1sphere` for the user name and password.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ e. Select the **Include applications** and **Include buses** check boxes. Keep all remaining defaults.



__ f. Click **OK**. The federation process can take several minutes to complete.

Note

The **Include buses** check box is selected in this example, which specifies whether to move the bus configuration at the node to the deployment manager. However, no buses currently exist in the cell. When federating a stand-alone node, it is a good idea to select this option to ensure that any bus configuration at the node level is moved over into the cell.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Note

If you see the following message in the console, proceed as described:

"`The console has not received information for the add operation in a timely manner. The state of the operation is indeterminate. Check the add node log for details.`"

Check the `/opt/IBM/WebSphere/AppServer/profiles/profile1/logs/addNode.log` file for error messages. Look for a message that indicates the node is successfully federated.

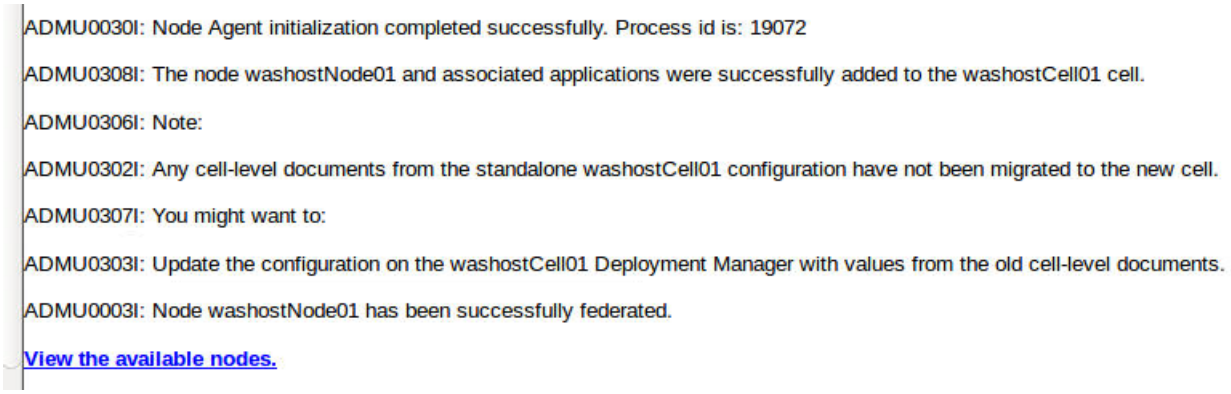
If you see the following message, proceed as explained:

`ADMC0009E: The system failed to make the SOAP RPC call: invoke`

- One option is to increase the timeout value for the type of connection you are using, in this case SOAP, by editing the file `/opt/IBM/WebSphere/AppServer/profiles/`*`profiles`*`/profile1/properties/soap.client.properties` and changing the value of the `com.ibm.SOAP.requestTimeout` property to `6000`. The value is in seconds.
- If using an RMI connection, edit the file `/opt/IBM/WebSphere/AppServer/profiles/profile1/properties/sas.client.props`, and increase the value for the `com.ibm.CORBA.requestTimeout` property to `6000`.

If the federation failed, repeat the previous steps to add a node.

__ g. When the federation is complete, the console shows several log messages, including a link to **View the available nodes**.

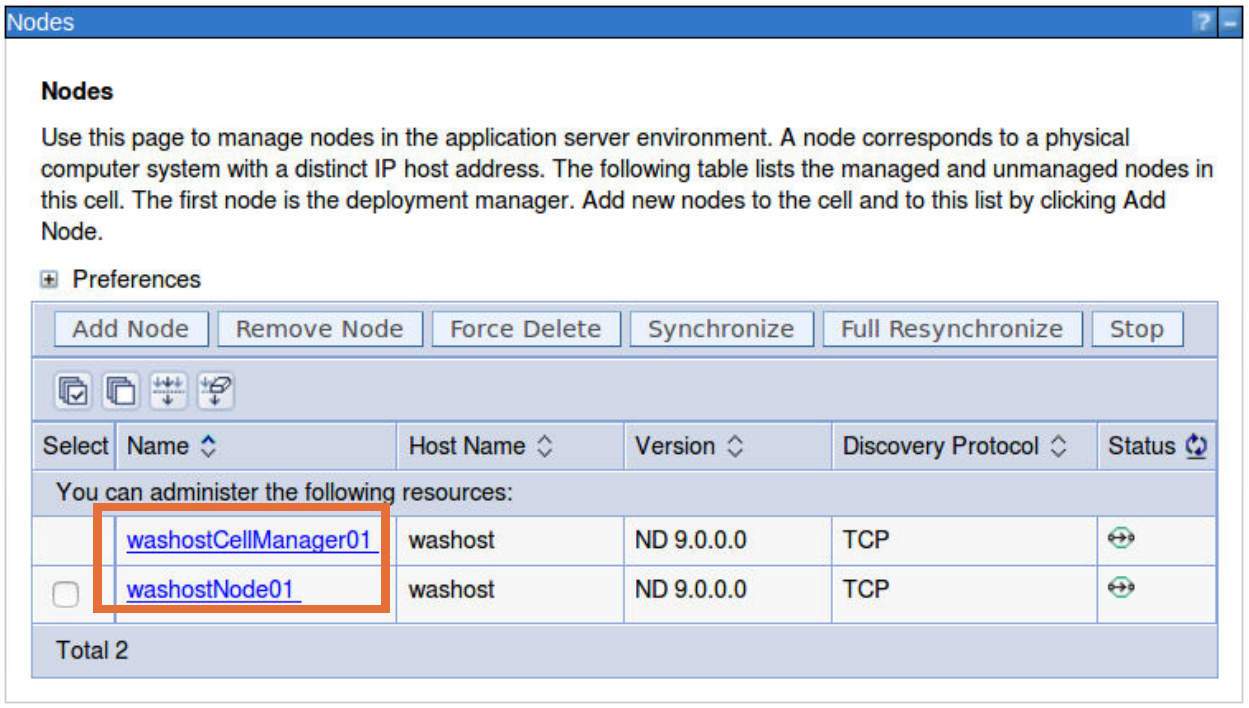


© Copyright IBM Corp. 2016

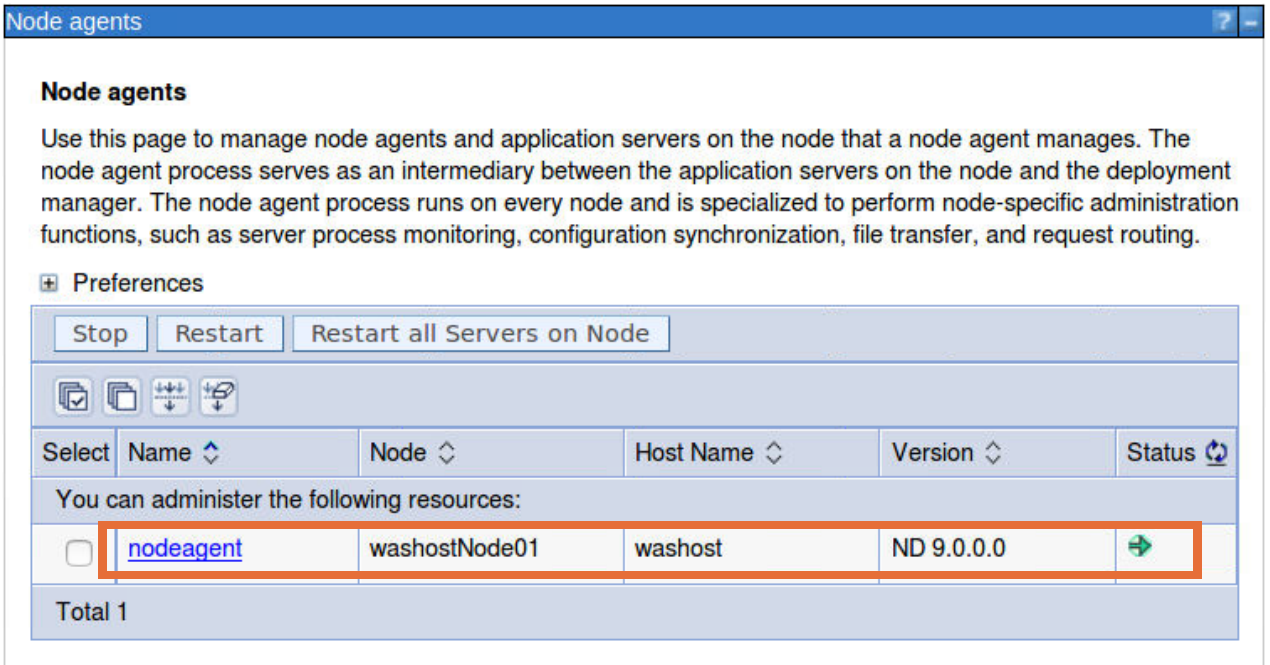
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ 4. Verify the cell configuration.

__ a. Click **View the available nodes** or **System Administration > Nodes**. Two nodes are listed: the deployment manager (`washostCellManager01`), and the `washostNode01` node that was added.



__ b. Click **System Administration > Node agents**. Verify that the node agent on `washostNode01` started.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ 5. Start the application server and test the Snoop servlet.

__ a. Click **Servers > Server Types > WebSphere application servers**.

__ b. Select **server1** and click **Start**. Wait for server1 to start.

__ c. Click **Applications > Application Types > WebSphere enterprise applications**. Check the status for the DefaultApplication. Verify that the **DefaultApplication** is running.

__ d. Open another browser window and enter the following address:

`http://washost:9080/snoop`

If you get information back regarding the server, it verifies that the Snoop servlet works.

Section 5: Creating a custom profile and federating it into the deployment manager cell

During this section of the exercise, you are going to create a custom profile, `profile2`, that defines a node, named `washostNode02`. The custom profile is automatically federated into the cell `washostCell01`.

A custom profile is useful because it does not create any application servers on the node; it creates the configuration and the node agent only. Therefore, no server1 is created on that node. This feature is helpful for expanding clusters.

__ 1. Start the WebSphere Customization Toolbox.

__ a. Enter the following command to start the WebSphere Profile Management tool:

`/opt/IBM/WebSphere/AppServer/bin/ProfileManagement/pmt.sh`

__ b. The Welcome window for the WebSphere Customization Toolbox opens, and you are placed on the **Profile Management Tool** tab.

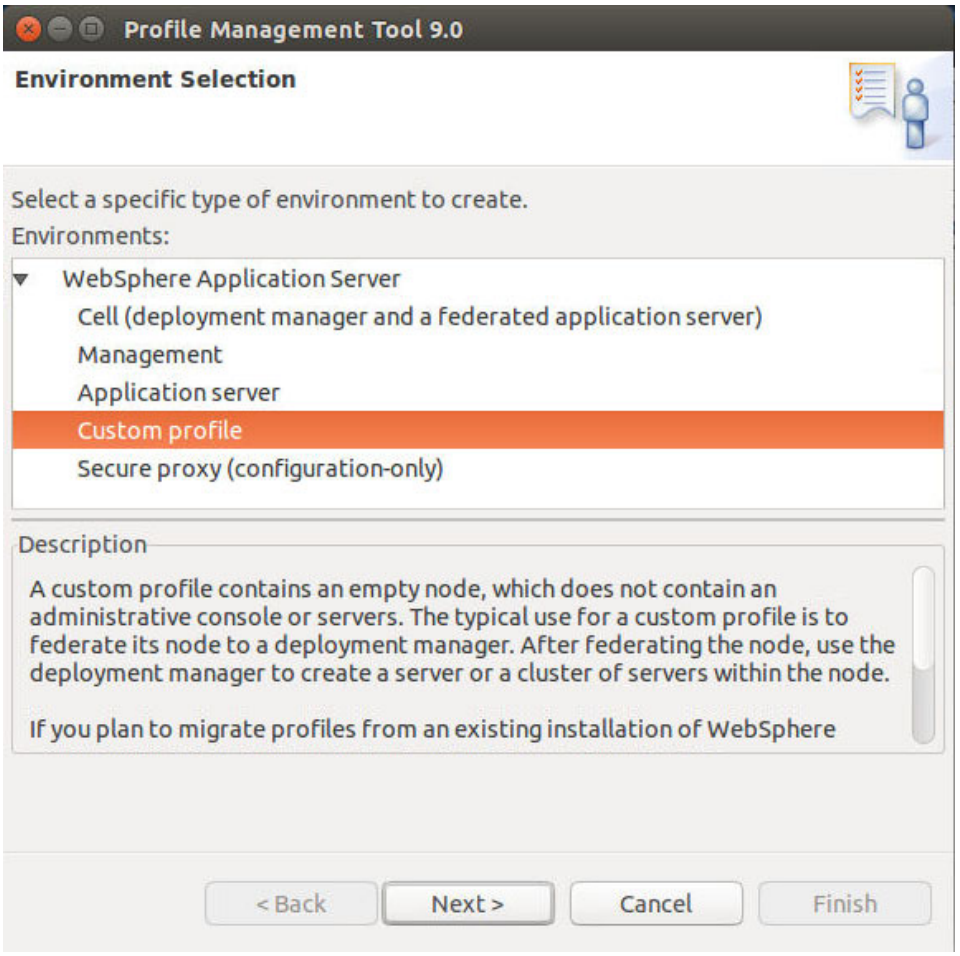
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ 2. Create a custom profile that is named profile2, and federate it to the deployment manager's configuration.

__ a. Click **Create** from the Profiles list panel.

__ b. On the Environment Selection panel, click **Custom profile**. Click **Next**.



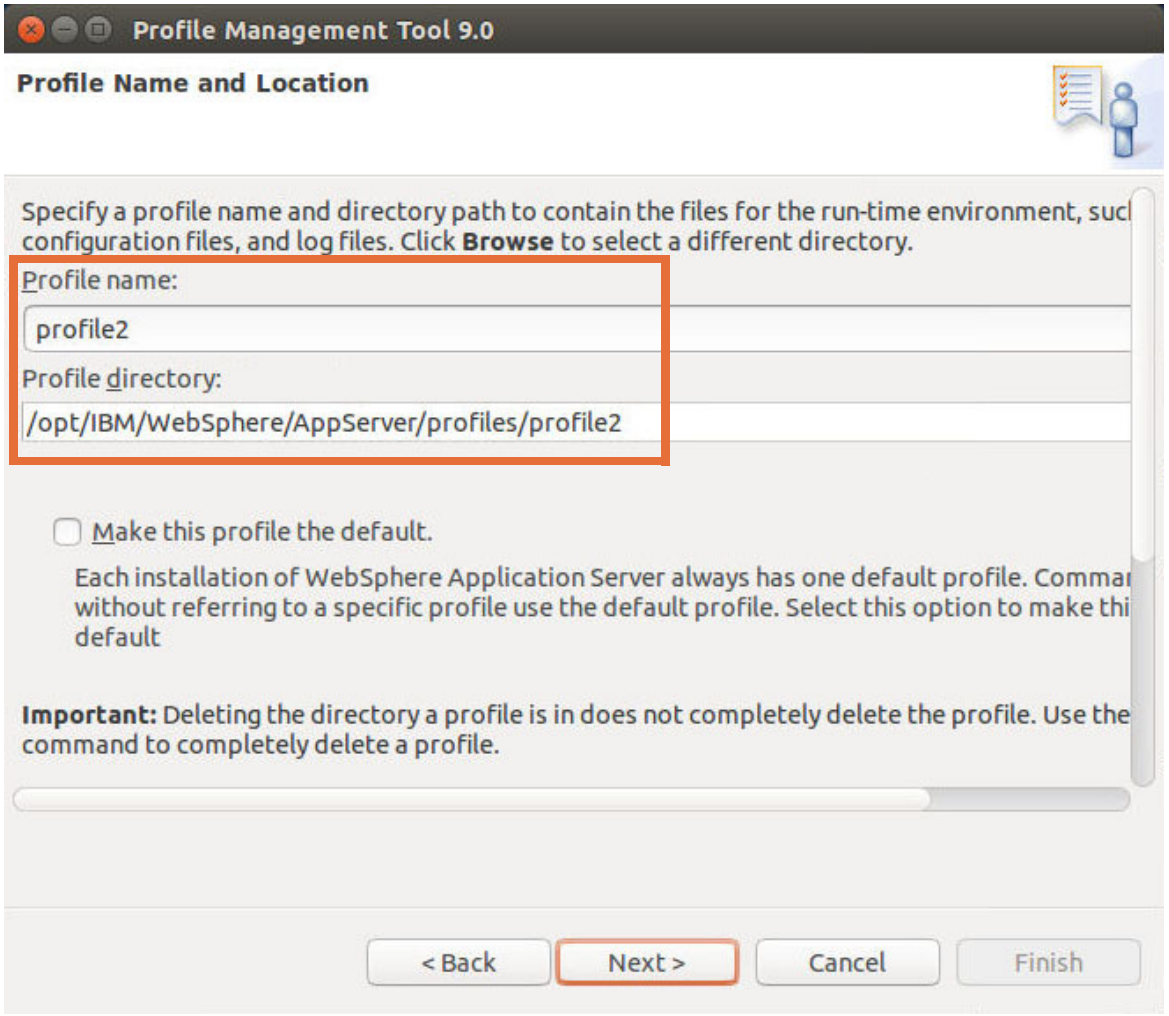
__ c. On the Profile Creation Options page, select **Advanced profile creation** to specify your own configuration values during profile creation. Click **Next**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ d. For the profile name and location, enter the following information:

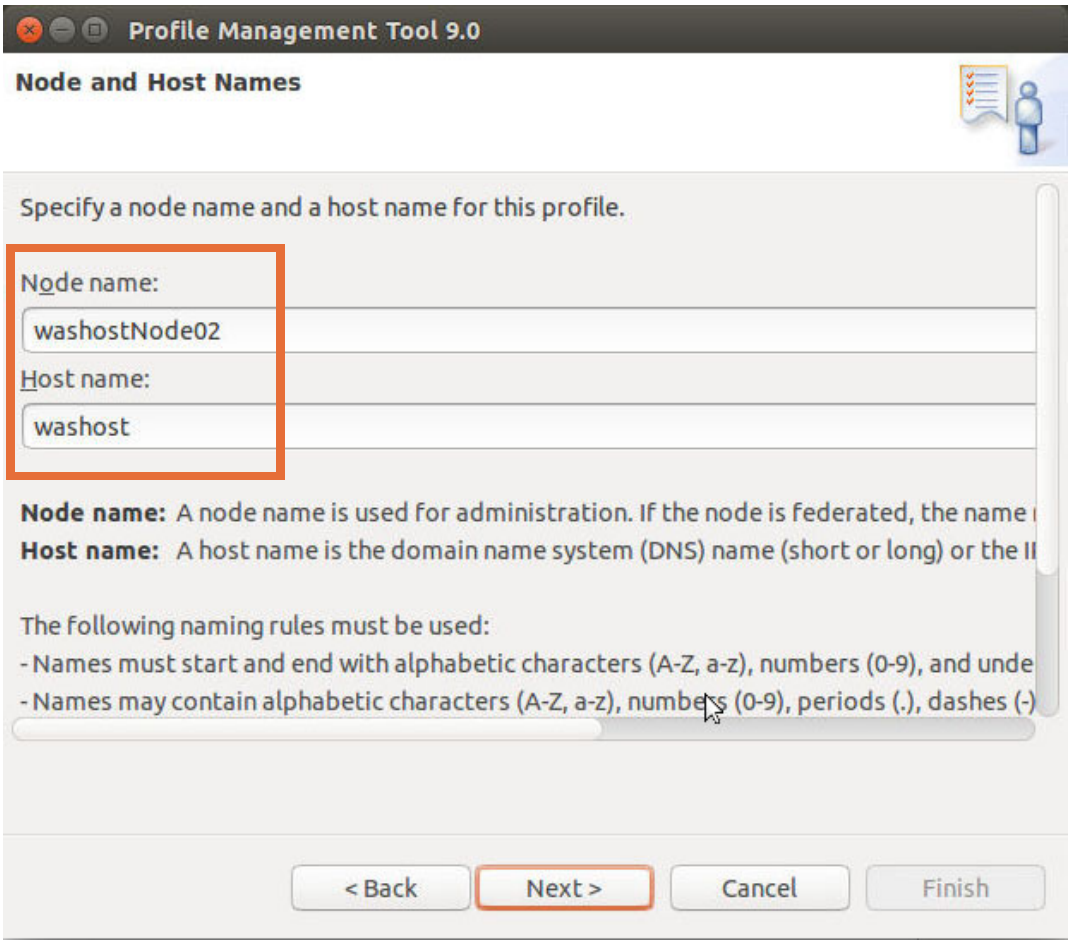
- **Profile name**: `profile2`
- **Profile directory**: `/opt/IBM/WebSphere/AppServer/profiles/profile2`



__ e. Click **Next**.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ f. Ensure that the **Node name** and **Host name** are `washostNode02` and `washost` (they are based on the short form of the host name and not localhost: for example, `washostNode02`). Notice that the **Node name** ends with a **02** (not **01**, as that would conflict with the existing node). Click **Next**.



Information

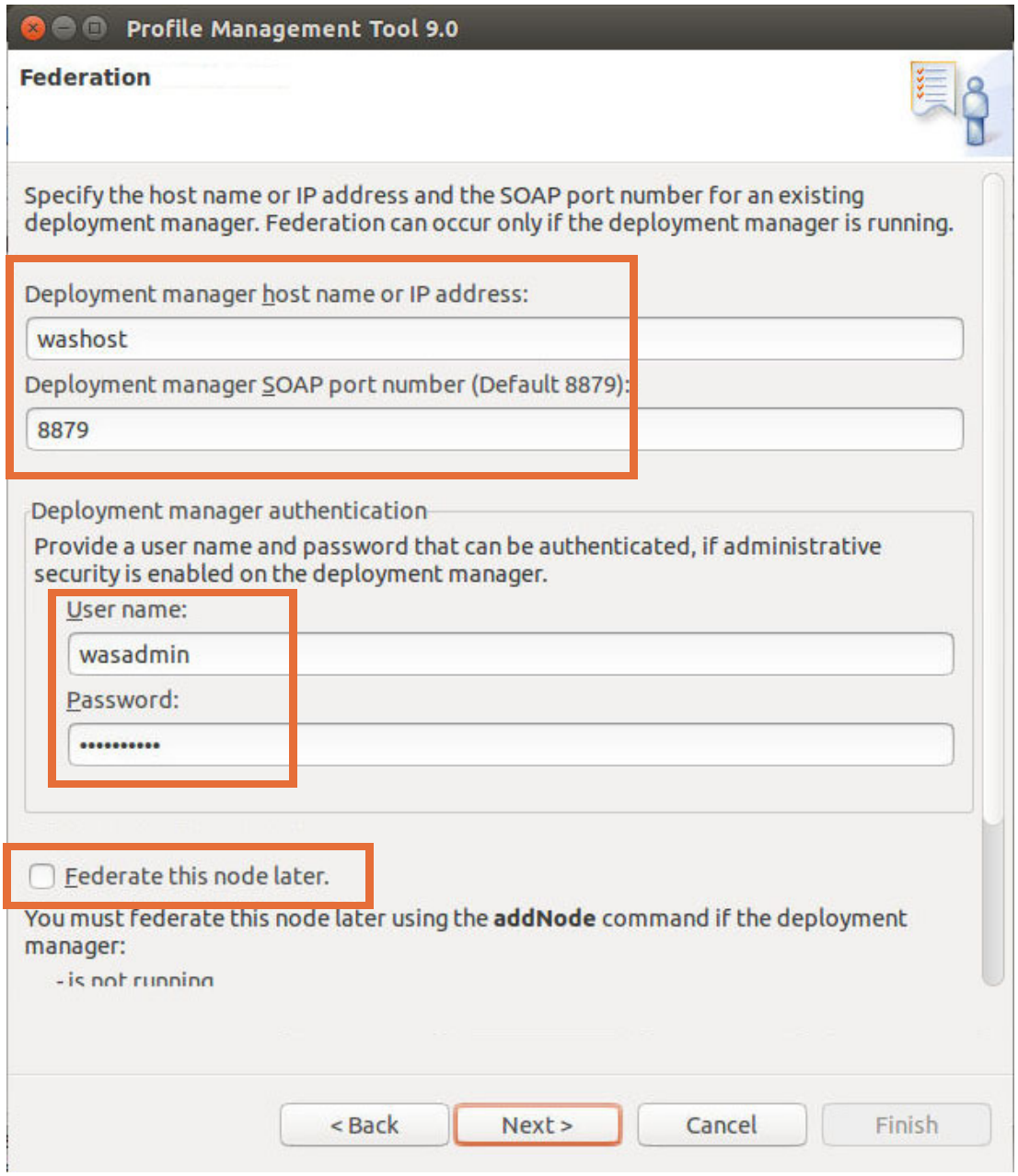
For these labs, use the short name for your host. Although it is acceptable to use another form of the host name, it is important to be consistent. Since the short name was used in the initial WebSphere installation lab, the short name is used here as well.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ g. On the Federation panel, enter the following information:

- Deployment manager host name: `washost`
- User name: `wasadmin`
- Password: `web1sphere`
- Do not select the **Federate this node later** check box.



__ h. Click **Next**.

Information

By not selecting **Federate this node later**, the wizard process federates the node now. Select this check box only if you want to create the profile, but want to federate it later.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ i. Accept the defaults on the Security Certificate (Part 1) panel. Click **Next**.

__ j. Accept the defaults on the Security Certificate (Part 2) panel. Click **Next**.

__ k. Accept the default on the Port Values Assignment panel. Click **Next**.

__ l. On the Profile Creation Summary panel, click **Create**.

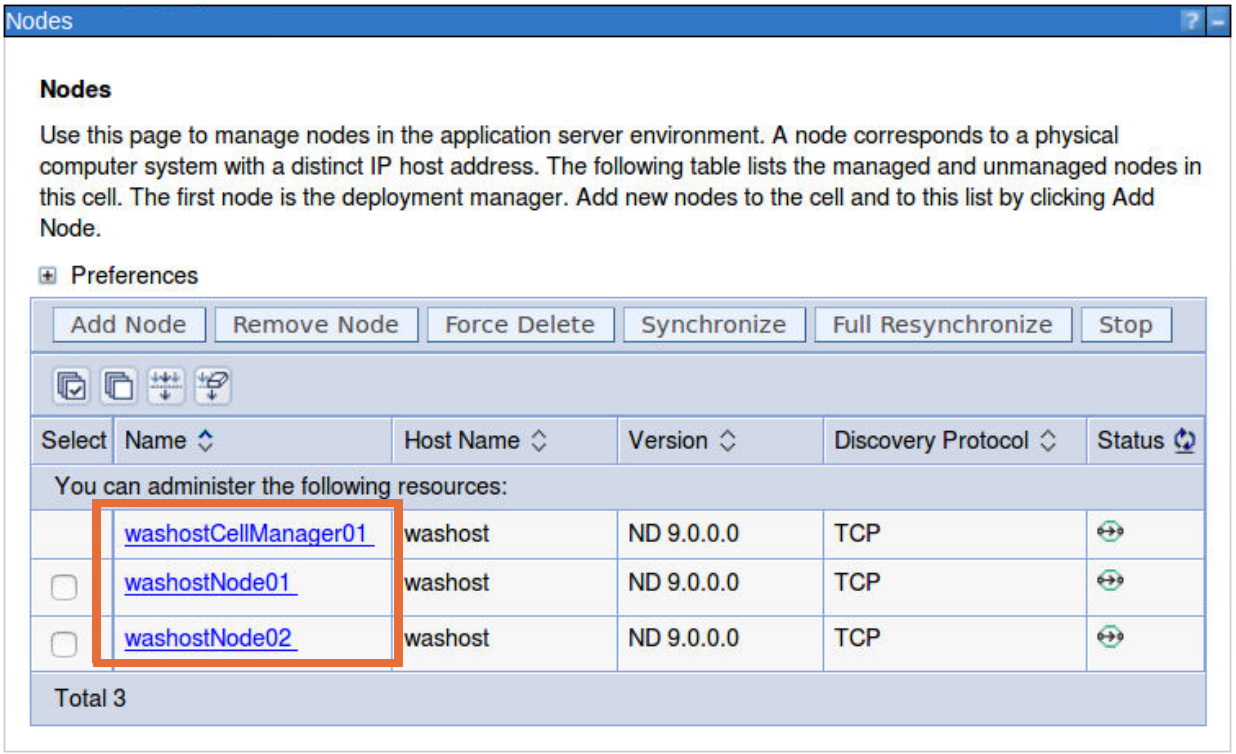
__ m. After a couple of minutes, the profile creation is complete. On the Profile Creation Complete panel, clear the **Launch the First steps console** check box.

__ n. Click **Finish** to exit the wizard.

__ o. Close the WebSphere Customization Toolbox.

__ 3. Verify that the node is added to the deployment manager's configuration.

__ a. Using the administrative console, click **System administration > Nodes**. The federated node washostNode02 is listed. If the node is not displayed, refresh the administrative console.



Information

Using a custom profile does not create a server instance. This feature is useful when adding nodes to a cell. The intention of federating a new node into a cell is normally to either add cluster members to the node or create servers that are named something other than server1.

__ 4. Verify that both node agents started.

__ a. From the navigation tree, click **Node agents**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ b. Start any node agents that are not started by entering the following command in a terminal window:

`/opt/IBM/WebSphere/AppServer/profiles/profileX/bin/startNode.sh` (where `X` is `1` or `2`)

Wait for the node agent to start.

Section 6: Adding the IBM HTTP Server to the cell

During this section of the exercise, you add an unmanaged node, ihsnode, to the cell washostCell01. You also add a web server, webserver1, to the unmanaged node. Information about the web server is communicated to the deployment manager through the IBM HTTP Server administrative process.

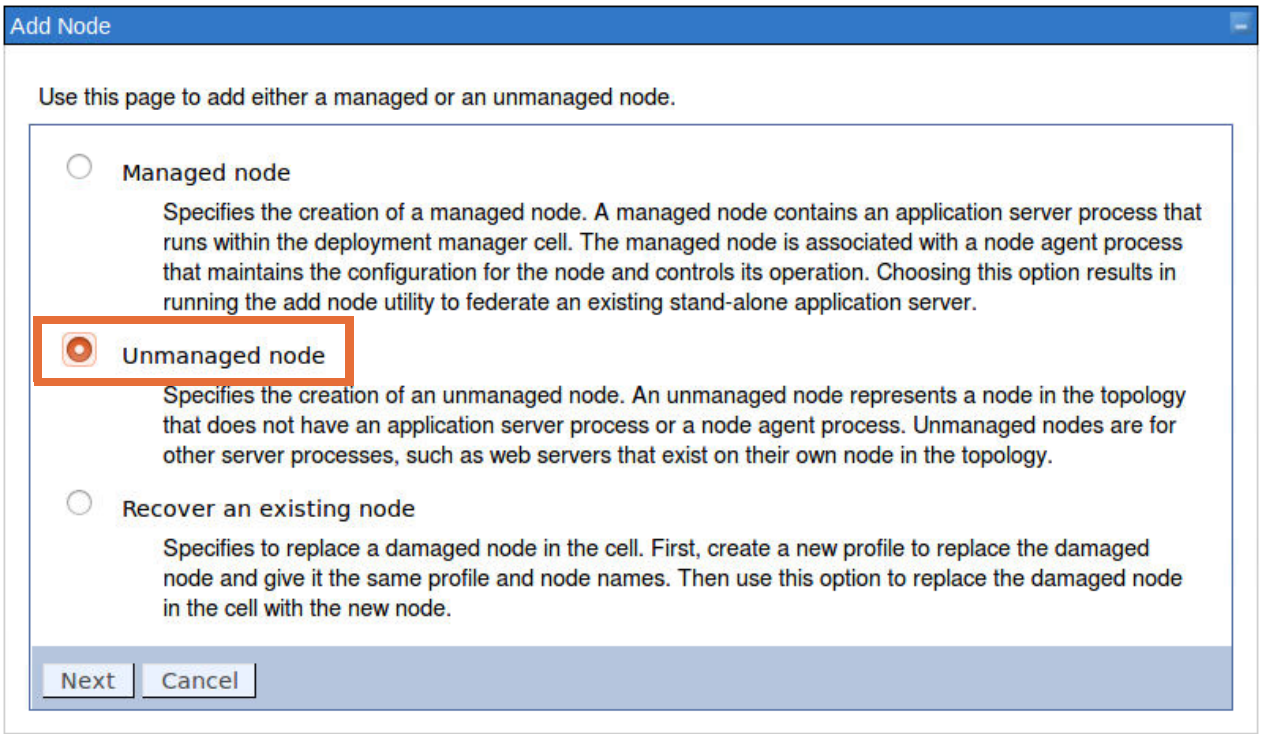
Create a node and add the web server to the node. When adding a node, you can create either a managed node or an unmanaged node. A managed node contains a WebSphere Application Server and a node agent. An unmanaged node does not have a node agent and is used for defining remote web servers in the topology.

__ 1. Create an unmanaged node for the web server. The web server definition uses this new node definition to define the host on which it lives.

__ a. Click **System administration > Nodes**.

__ b. Click **Add Node**.

__ c. In the Add Node window, select **Unmanaged node** and click **Next**.

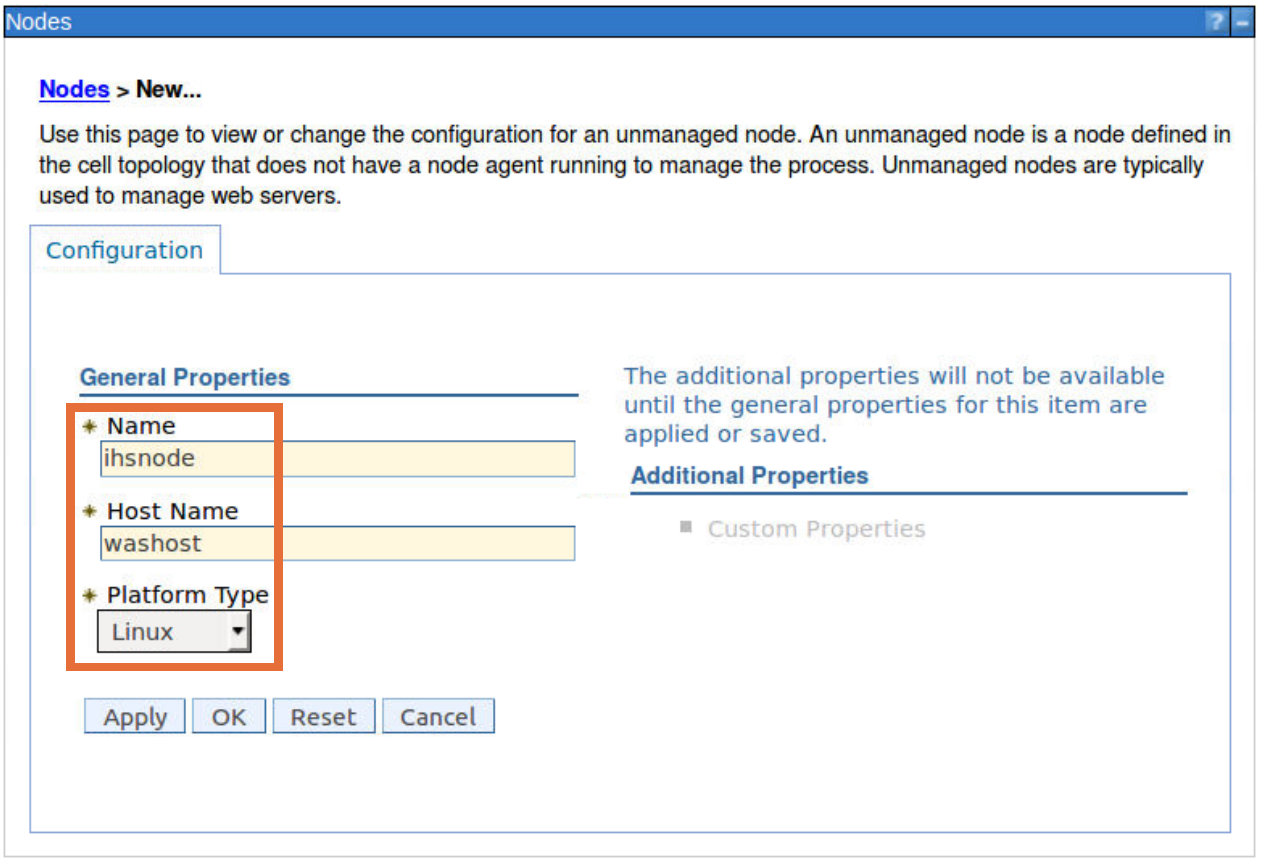


© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ d. In the Nodes window, enter configuration information for the node:

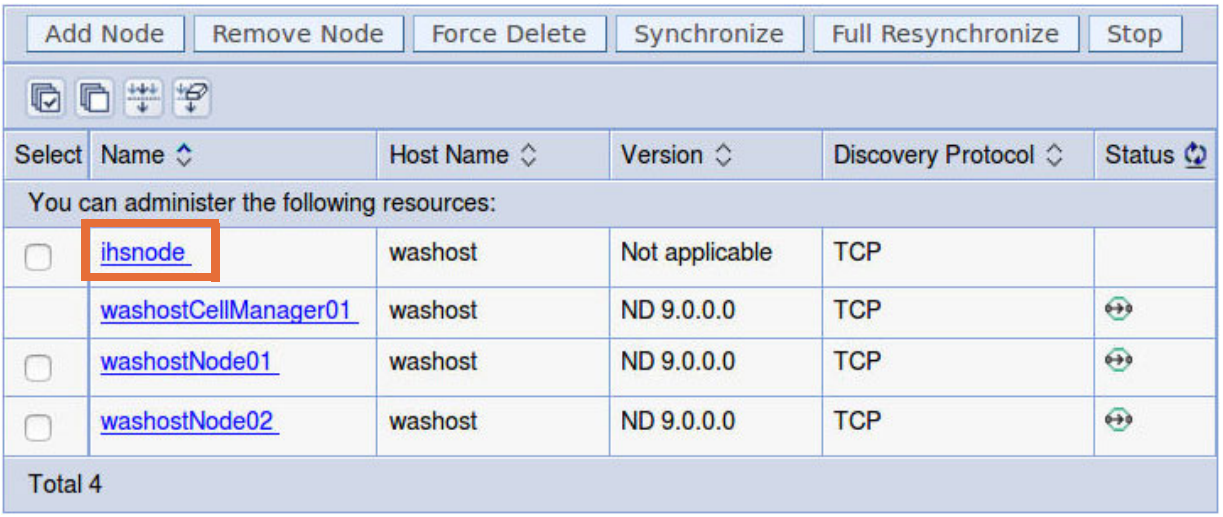
- **Name**: `ihsnode`
- **Host Name**: `washost`
- **Platform Type**: `Linux`



__ e. Click **OK**.

__ f. Save the changes.

__ g. The node **ihsnode** is now shown in the list of nodes.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Section 7: Adding the web server to the configuration

In this section, the web server definition is added to the ihsnode.

__ 1. Add the web server to the ihsnode configuration. This action allows the web server to be managed from the administrative console.

__ a. Click **Servers > Server Types > Web servers**.

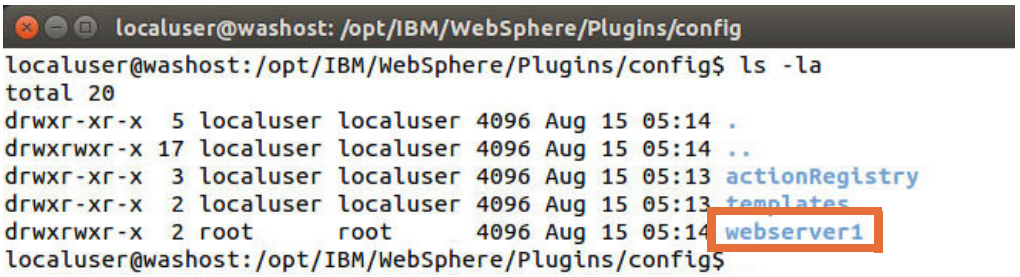
__ b. Click **New** to add a web server.

__ c. On **Step 1** of creating a web server, enter the following information:

- Select **ihsnode** from the **Select node** list.
- For **Server name**, enter: `webserver1`
- Select I**BM HTTP Server** from the **Type** list.

Information

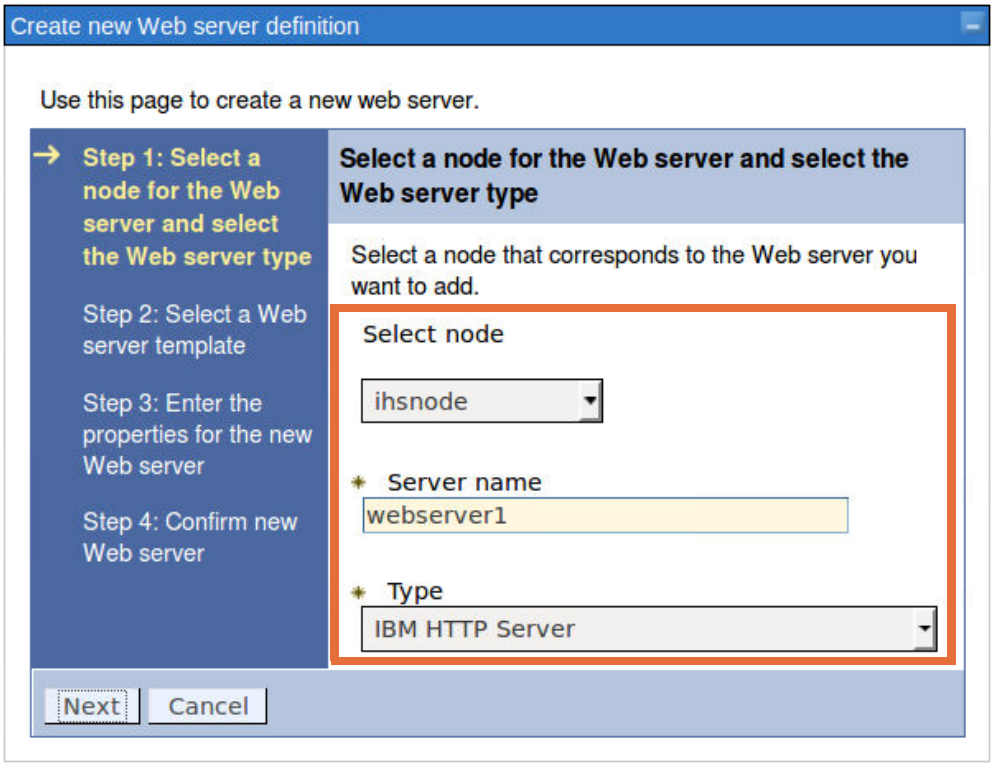
The web server name must match the name that you assigned during the IBM HTTP Server installation. You can check the web server name by looking in `/opt/IBM/WebSphere/Plugins/config/`



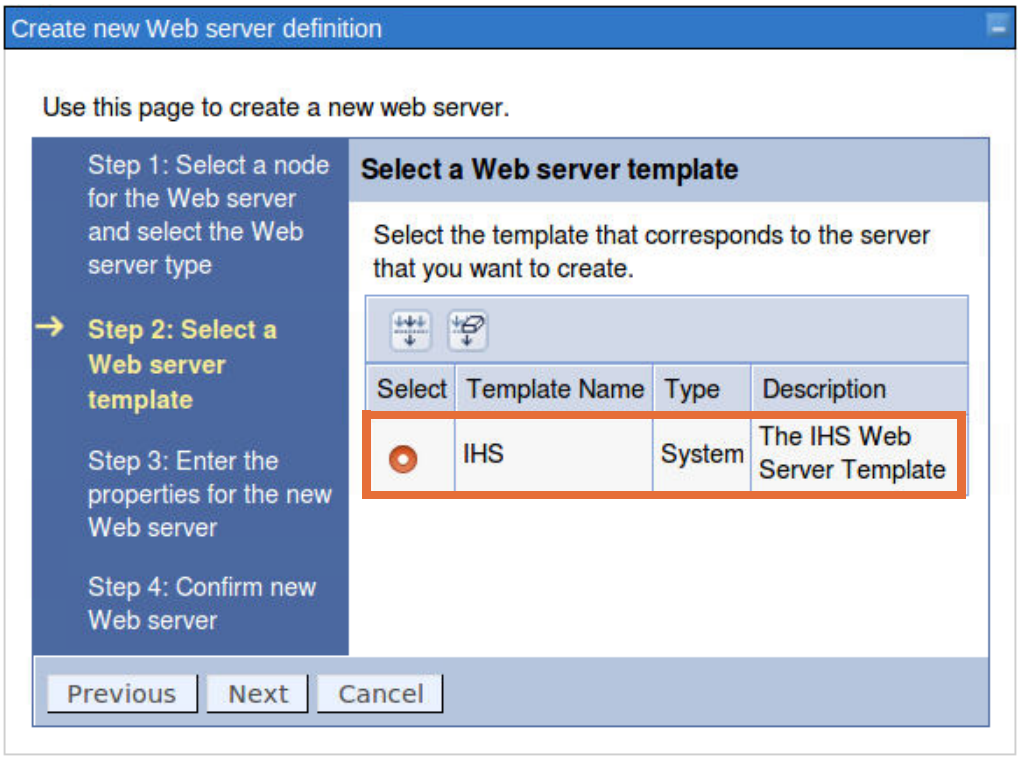
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Click **Next**.



__ d. On **Step 2** of selecting a web server template, verify that **IHS** is selected and click **Next**.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

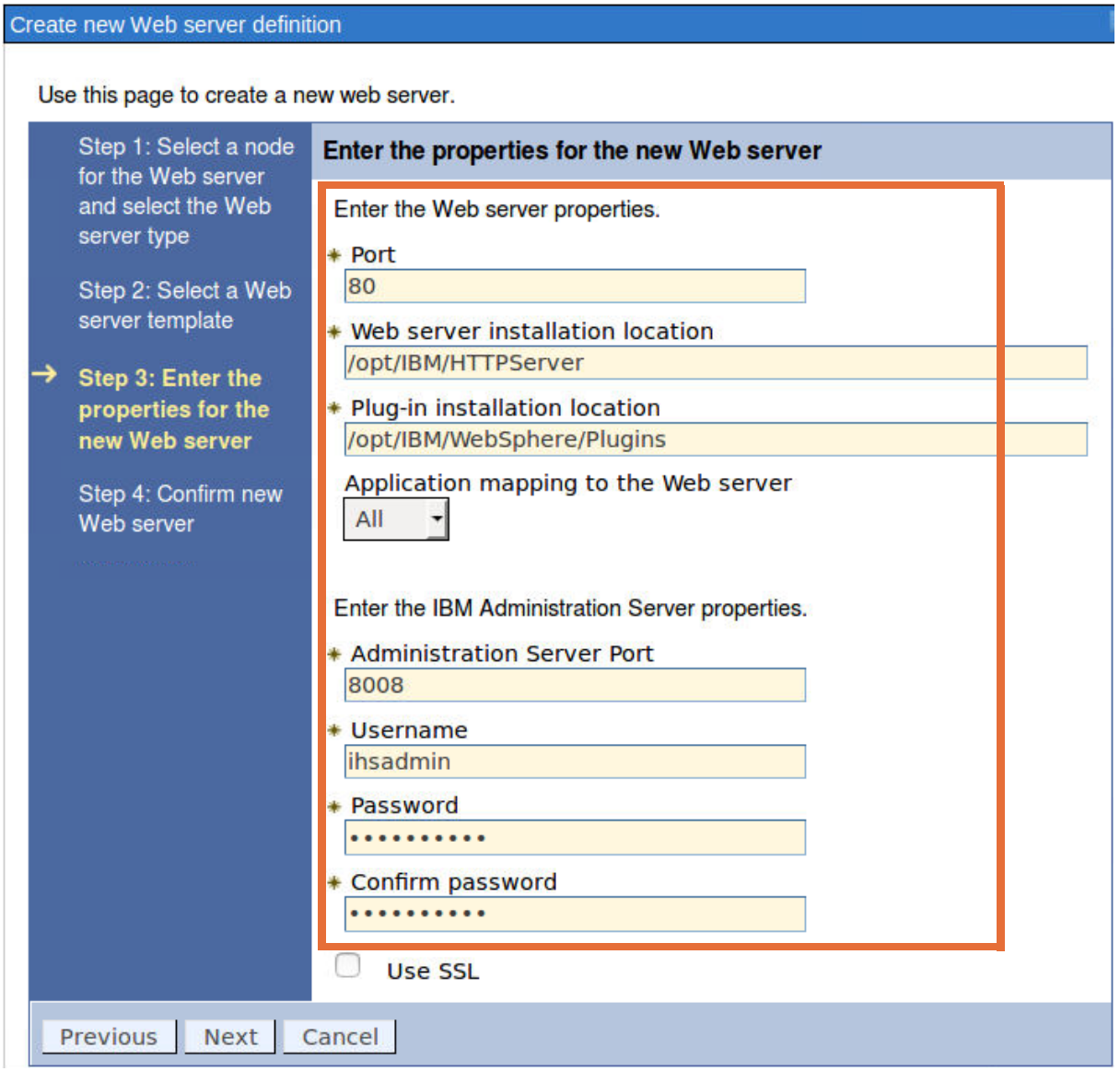
__ e. On **Step 3**, specify the properties for the new web server. Enter the following information in the fields as provided:

Table 1: Web server configuration details

Field name	Value
Port	`80`
Web server Installation location	`/opt/IBM/HTTPServer`
Plug-in installation location	`/opt/IBM/WebSphere/Plugins`
Application mapping	`All`
Port	`8008`
User name	`ihsadmin`
Password	`web1sphere`
Confirm password	`web1sphere`

© Copyright IBM Corp. 2016

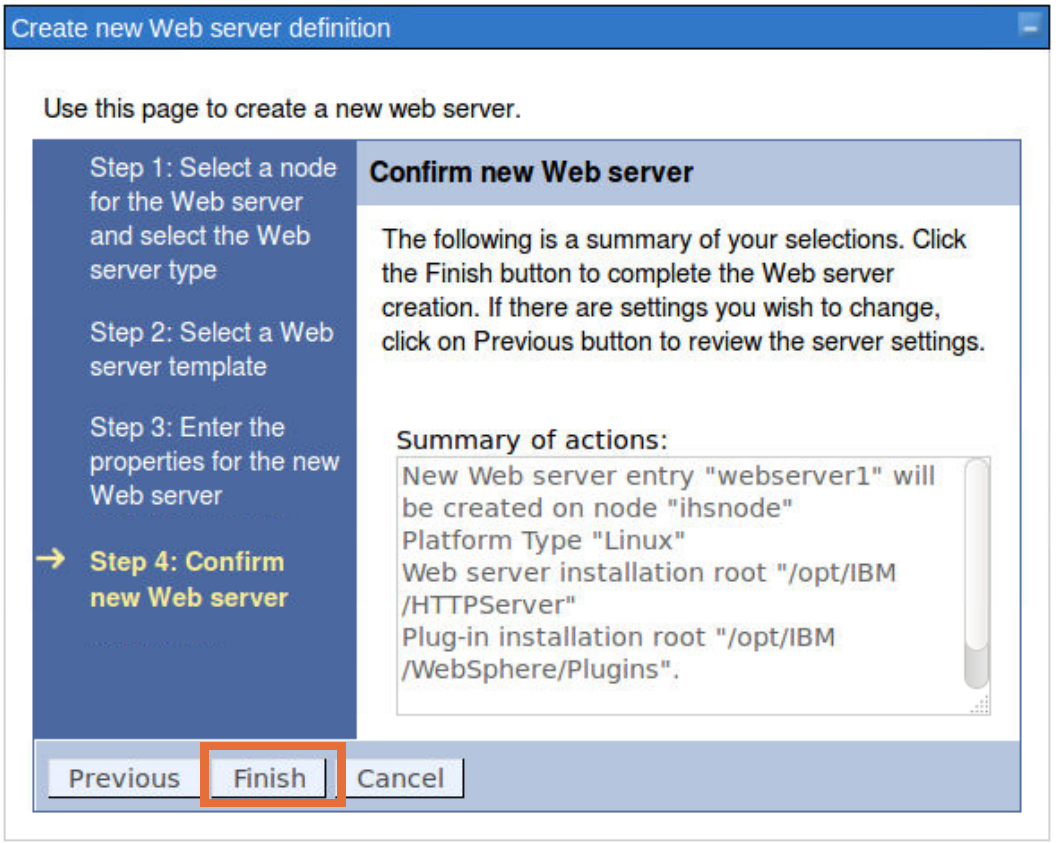
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.



__ f. Click **Next** when complete.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ g. On Step 4, the summary, click **Finish**.



__ h. Save the changes.

__ i. Minimize the administrative console browser window.

__ 2. Use a terminal window to verify the web server status.

__ a. Open a terminal window and navigate to:
`/opt/IBM/HTTPServer/bin/`

__ b. Use the following command to check whether the web server processes are running:

```
ps -ef | grep -i httpd
```

__ c. If the web server or IBM HTTP Server administrative process is not running, you can use the following commands to start them (enter `passw0rd` if prompted for the localuser password):

```
sudo ./apachectl start
sudo ./adminctl start
```

__ d. Again, use the following command to check whether the web server processes are running:

```
ps -ef | grep -i httpd
```

Verify that several processes are now running.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ e. Another way to verify that the web server is started is to open a web browser and connect to the IBM HTTP Server welcome page. Enter the following address:

`http://washost`

Section 8: Mapping modules to servers

Each module of an application is mapped to one or more target servers. The target server can be an application server, a cluster of application servers, or a web server. Web servers that are specified as targets have the routing information for the application, which is generated in their plug-in configuration files.

This mapping usually takes place during application deployment. But since the DefaultApplication is deployed when this particular web server was added, the DefaultApplication still must be mapped to your new web server. That, in fact, is done for you during the last step of defining the web server properties when **All** is selected for the **Application mapping to the web server**. That step mapped all installed applications to the new web server.

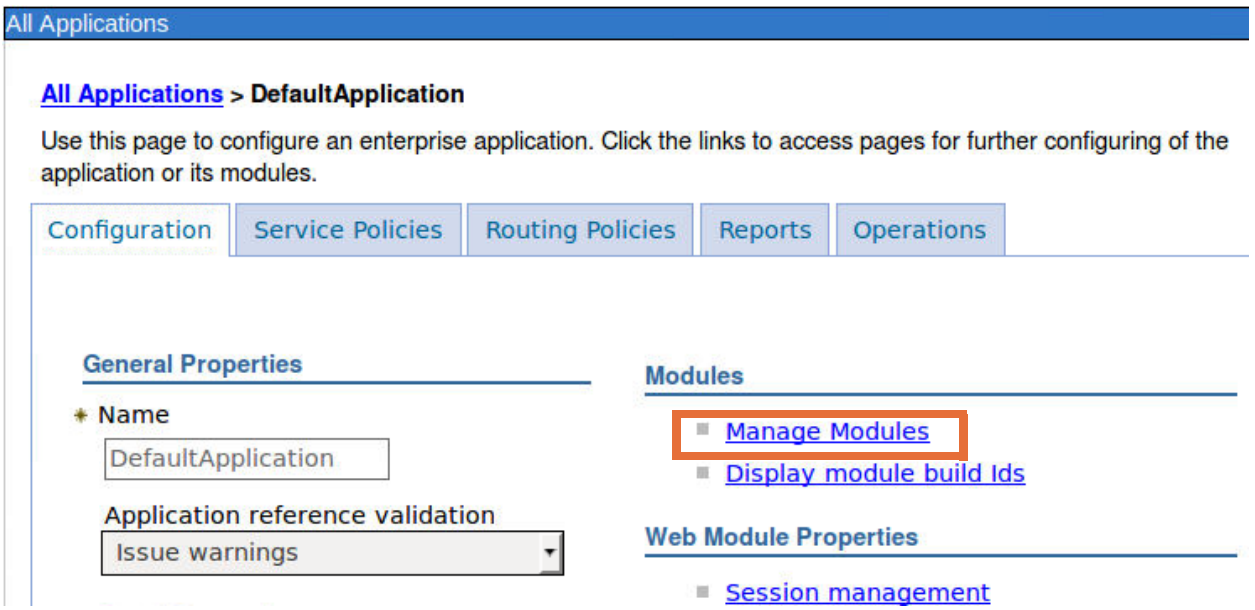
This section of the lab verifies that the applications are correctly mapped to the new web server.

__ 1. Using the deployment manager administrative console, verify the mapping of the DefaultApplication modules to the web server.

__ a. From the administrative console, click **Applications > Application Types > WebSphere enterprise applications**.

__ b. Click **DefaultApplication**.

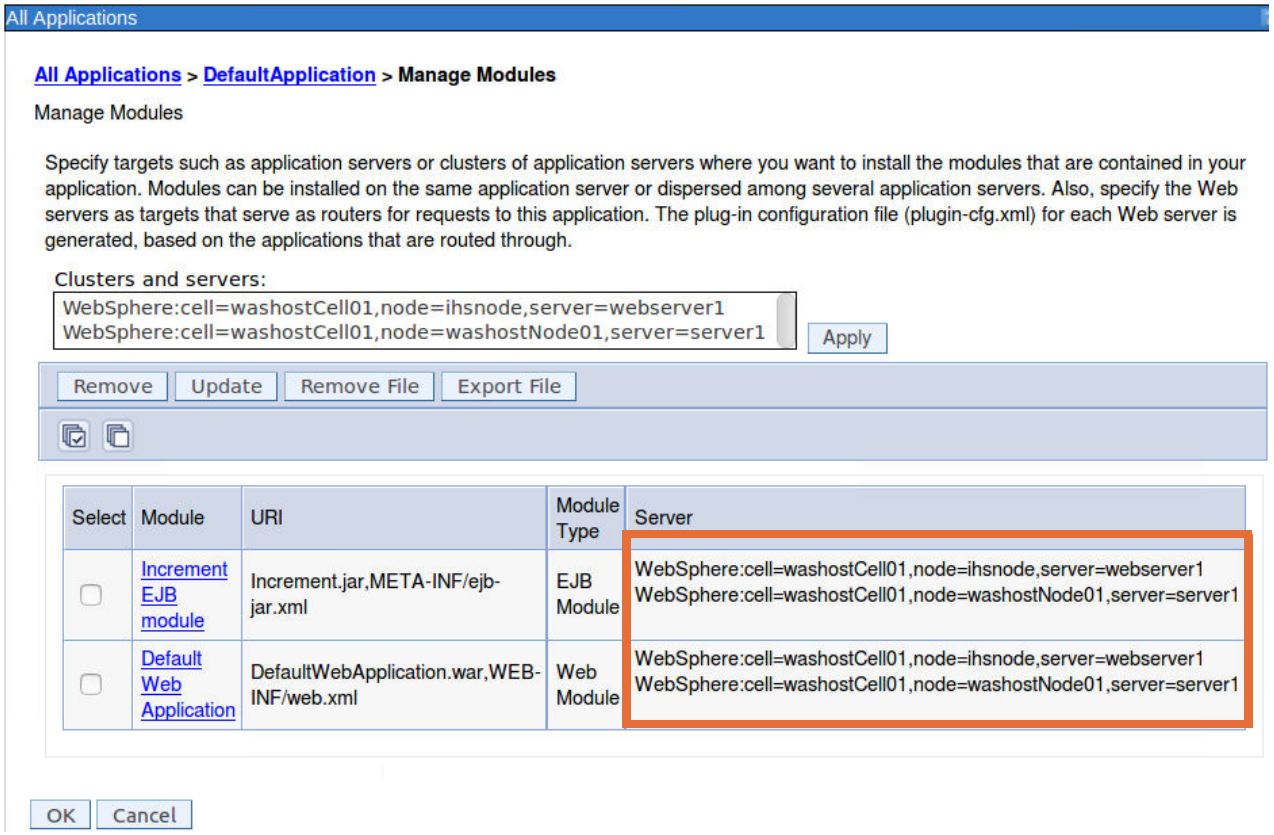
__ c. Under Modules, click **Manage Modules**.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

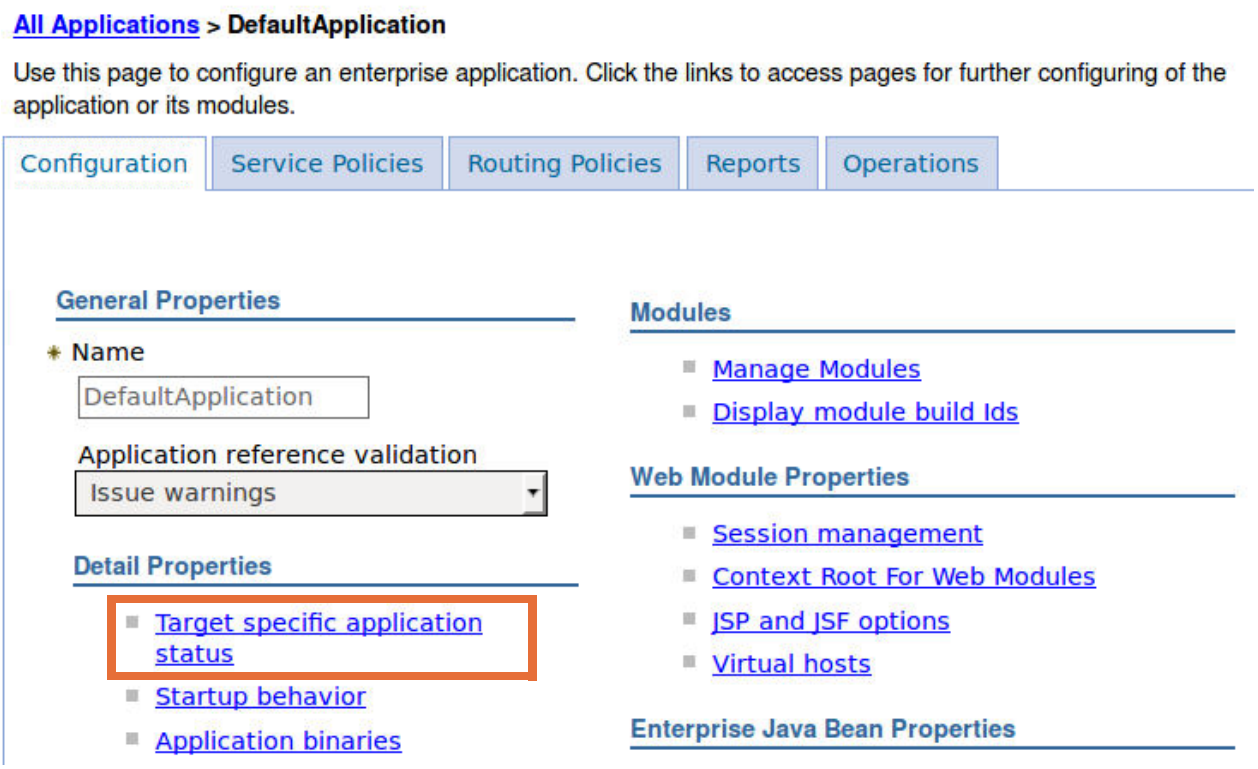
__ d. Notice that the Default Web Application module maps to both the application server **server1** and the **webserver1**. This page can also be used to modify the mappings manually if they do not exist.



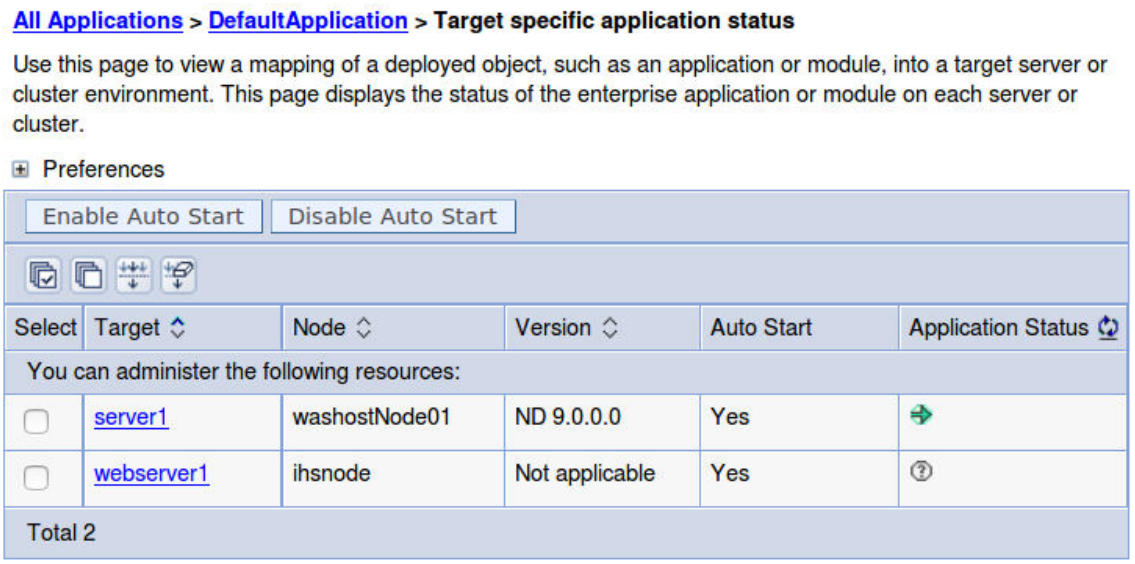
__ e. Click **DefaultApplication** in the breadcrumb trail to return to the configuration window.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ f. Under Detail Properties, click **Target specific application status**.



__ g. This view shows the mapping of a deployed object to servers.



Section 9: Working with the plug-in configuration file

The plug-in configuration file contains routing information for all applications that are mapped to the web server. The plug-in configuration file must be regenerated and propagated to the web server

© Copyright IBM Corp. 2016

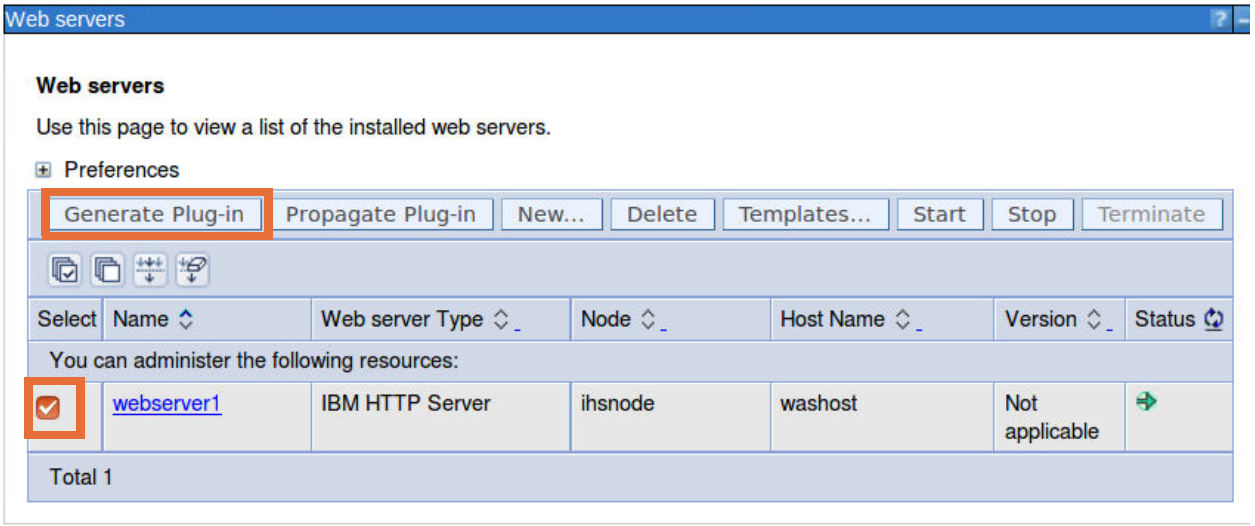
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

whenever changes that are made to the WebSphere configuration affect how requests are routed from the web server to the application server.

__ 1. Regenerate the plug-in configuration file. This process generates a plug-in configuration file that is specific to the web server that is defined within the cell. If multiple web servers are defined within the cell, you can generate customized plug-in configuration files for each of those web servers.

__ a. From the administrative console, click **Servers > Server Types > Web servers**.

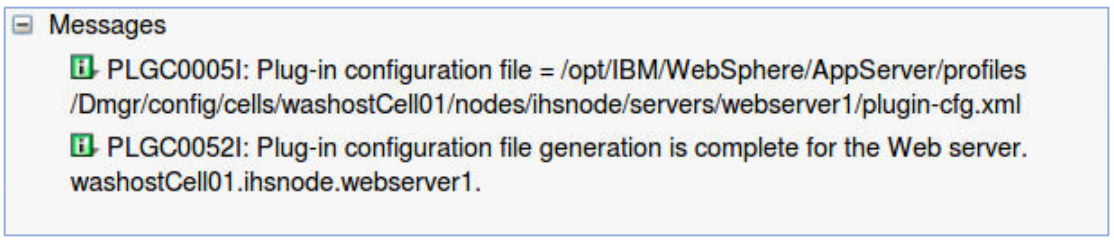
__ b. Select the web server and click **Generate Plug-in**.



Information

This step is not necessary because the default behavior is to automatically generate a new plug-in configuration file whenever an update is made. However, this step confirms that the setup is working correctly.

__ c. Verify that the generation was successful by viewing the messages.



__ 2. View the plug-in configuration file, `plugin-cfg.xml`, from the administrative console. This `plugin-cfg.xml` file is specific to the web server. If you have multiple web servers, it is possible for each `plugin-cfg.xml` file to be unique.

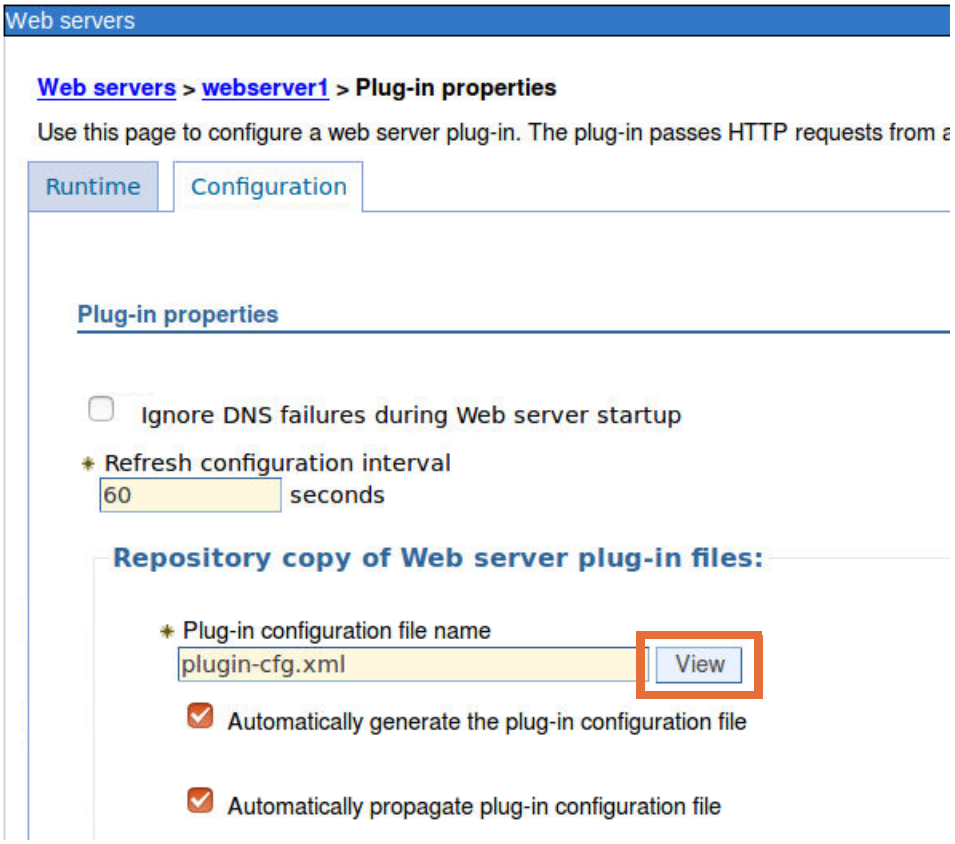
__ a. Click **webserver1**.

__ b. Under Additional Properties, click **Plug-in properties**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ c. Under **Plug-in properties**, click **View** to see the `plugin-cfg.xml` file.



__ d. The next window shows the plug-in configuration file. Verify that the element

`<UriGroup Name="default_host_server1_washostNode01_Cluster_URIs">`

includes the element

`<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/snoop/*"/>`

This element ensures that the plug-in recognizes URLs containing `/snoop` and that they get forwarded to the application server.

```
<UriGroup Name="default_host_server1_washostNode01_Cluster_URIs">
   <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/PlantsByWebSphere/*"/>
   <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/ivt/*"/>
   <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/snoop/*"/>
   <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/hello"/>
   <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/hitcount"/>
   <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="*.jsp"/>
   <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="*.jsv"/>
   <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="*.jsw"/>
   <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/j_security_check"/>
   <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/ibm_security_logout"/>
   <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/servlet/*"/>
</UriGroup>
```

__ e. Look through the list of URIs for the `/PlantsByWebSphere` entry.

__ 3. Propagate the plug-in configuration file. After a plug-in configuration file is regenerated, it must be propagated to the web server.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

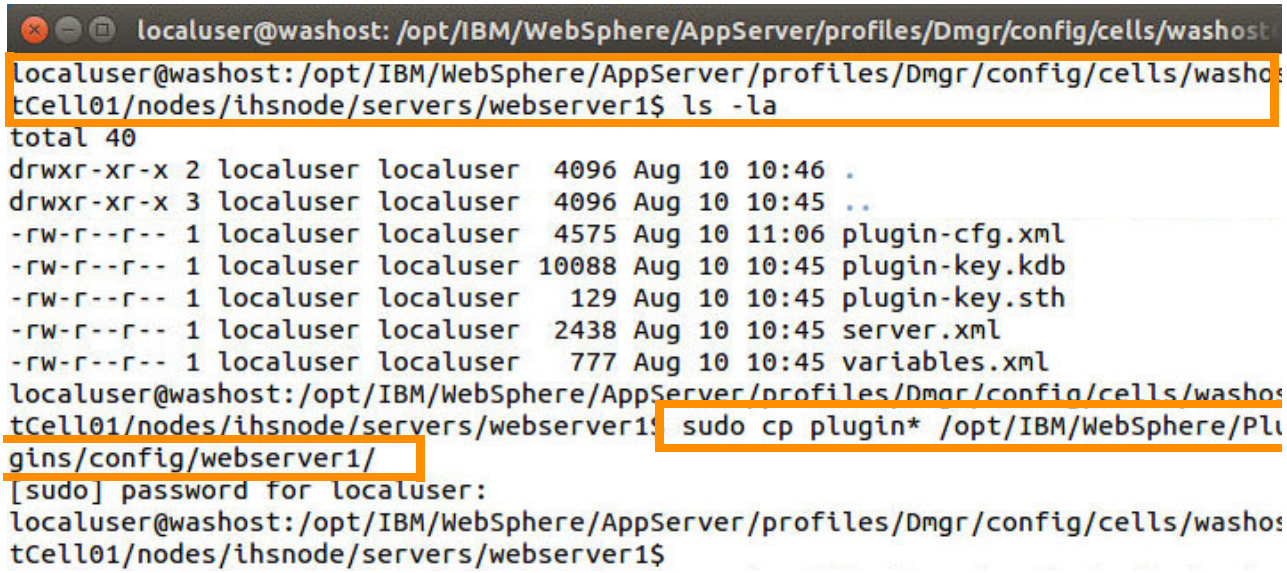
Information

The most common approaches for `plugin-cfg.xml` and key ring propagation are to move the files manually or create a custom automated mechanism. IHS provides a means of propagation through the IHS admin service, but that is only available through IHS and not any of the other supported web servers.

__ a. Use the terminal window and copy the `plugin-cfg.xml` file to the `plugin` directory. Use the following commands to change directory and then copy the file:

```
cd /opt/IBM/WebSphere/AppServer/profiles/Dmgr/config/cells/
washostCell01/nodes/ihsnode/servers/webserver1/
sudo cp plugin* /opt/IBM/WebSphere/Plugins/config/webserver1/
```

Enter `passw0rd` when prompted for localuser's password.



Information

The `sudo` is required as part of the `cp` command because the IBM HTTP Server was installed as a different user.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Section 10:Testing the plug-in configuration

By default, the web server plug-in module checks for a new configuration file every 60 seconds. You can wait for the plug-in to find the changes, or you can restart the web server to pick up the changes immediately.

__ 1. Verify that the application server, server1, is running.

__ a. Click **Servers > Server Types > WebSphere application servers**. If the server is not running, start server1.

__ b. Minimize the administrative console.

__ 2. Access the Snoop servlet.

__ a. Open a new web browser and enter the following address:

`http://washost:9080/snoop`

By using the port 9080, you are bypassing the external IBM HTTP Server.

__ b. The details for the Snoop servlet are visible in the browser window.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ 3. Verify that the web server is forwarding requests to the application server.

__ a. Using a browser, enter the following address:

```
http://washost/snoop
```

__ b. The details are visible in the Snoop servlet. This request first goes to the external web server.

End of exercise

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise review and wrap-up

In this lab exercise, you experience the process of creating a WebSphere cell through the generation of a deployment manager profile, and then the federation of application server profiles.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise 3. Clustering and workload management

Estimated time

01:00

Overview

This exercise covers the creation of a cluster. During the creation of the cluster, two cluster members are added. After the cluster is created, you configure the PlantsByWebSphere application to run in the cluster. You set up a replication domain to use the memory-to-memory replication mechanism. You then ensure that session failover works as expected by stopping one of the two servers in the cluster and watching the requests fail over to the remaining running server.

Objectives

After completing this exercise, you should be able to:

- Create a cluster and add cluster members
- Map modules to clusters and web servers
- Test load balancing and failover between two cluster members
- Configure a data replication domain for session management

Introduction

Up to this point you worked with WebSphere Application Server in a single-server environment. In this lab, after federating, you work with a cell and use the deployment manager. You create a cluster so that the workload can be managed between two servers, one on each node you already have.

You also set up a memory-to-memory replication domain so that if one of the servers would fail, HTTP sessions can be shared.

Requirements

The lab requires that you successfully completed the previous lab on federation.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise instructions

Preface

To do this exercise, you must complete the Federating a cell exercise as it sets up the environment of the nodes, node agents, and servers that are clustered in this exercise.

Important

The labs use two variables to define various installation paths. On Linux, the variable definitions are as follows:

`<was_root>: /opt/IBM/WebSphere/AppServer`
`<profile_root>: /opt/IBM/WebSphere/AppServer/profiles`

Section 1: Resetting the WebSphere environment

Note

To reset your WebSphere environment, read **Appendix A** for instructions on how to complete this procedure.

Section 2: Checking nodes and node agents

Before you can begin creating the cluster, you must make sure that both node agents are running and the nodes are synchronized.

__ 1. Log in to the deployment manager's administrative console.

__ a. Log in with `wasadmin` and `web1sphere` as the user name and password.

__ 2. Make sure that both federated nodes, washostNode01 and washostNode02, are started and synchronized.

__ a. Click **System Administration > Node agents**.

__ b. Click **System Administration > Nodes**.

Information

If the node agents are not started, use the `startNode.sh` script from a terminal window to start them. Make sure that you are in the correct `bin` folder for the profile you are trying to start.

Section 3: Creating the PlantsCluster cluster

A cluster is composed of two or more servers in a cell, which are assigned to run the same applications. Clusters are logical abstractions that are equivalent to servers. In this section, you

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

create the cluster that contains the cluster members that participate in workload management of the Plants application. You create a cluster that is called PlantsCluster. This cluster is created based on the existing server1 application server. This action means that all of the applications that are already deployed to server1 are included in the cluster.

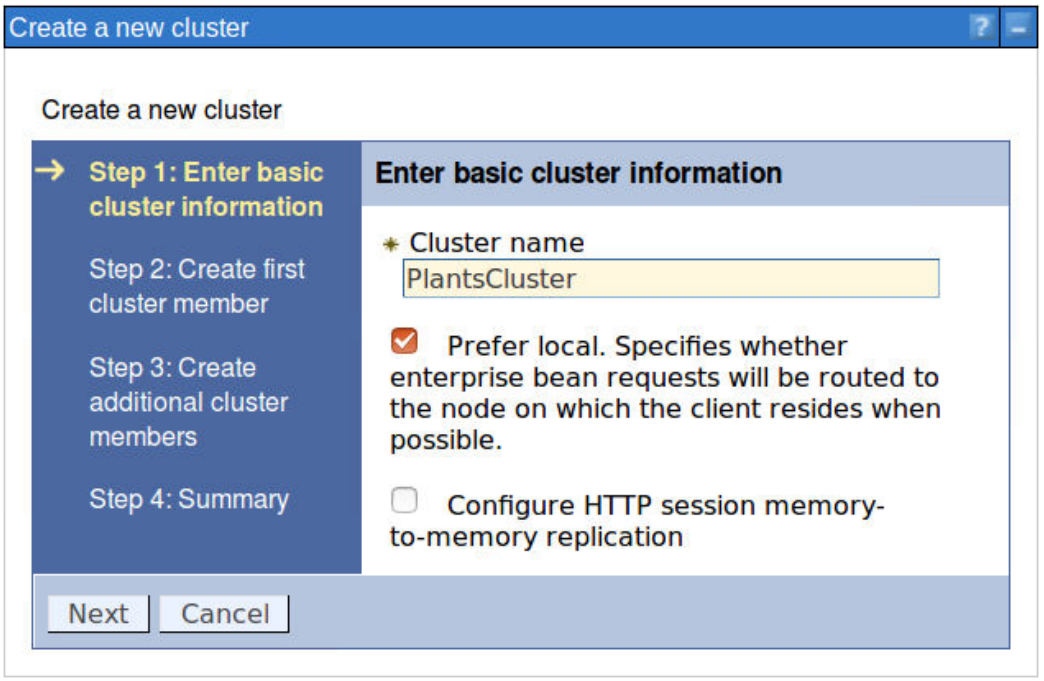
__ 1. Create the PlantsCluster.

__ a. Click **Servers > Clusters > WebSphere application server clusters**.

__ b. Click **New**.

__ c. Enter the following basic cluster information:

- Enter `PlantsCluster` for the **Cluster name**.
- Select the **Prefer local** option.
- Clear the **Configure HTTP session memory-to-memory replication** check box.

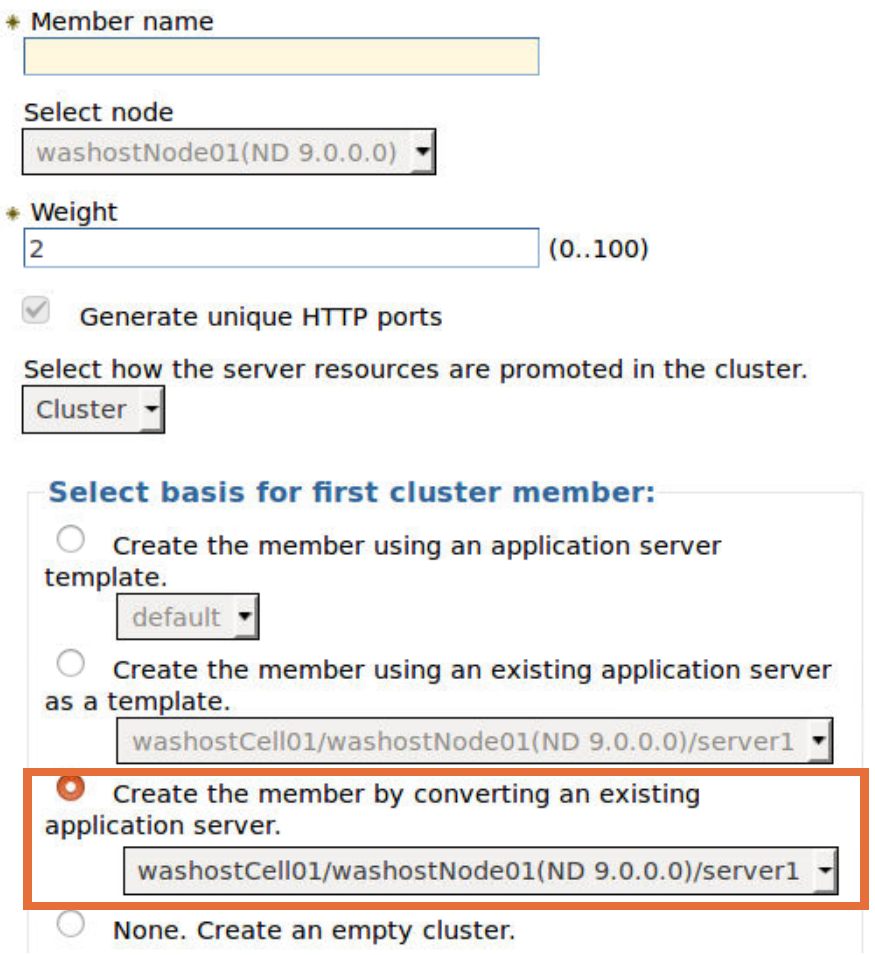


Click **Next**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ d. Under Select basis for first cluster member, click **Create the member by converting an existing application server**, and from the list, select the existing **server1** server.



Click **Next**.

__ 2. Add a server, **server2**, to the cluster. This server is created in node washostNode02. More cluster members can be created either during or after the cluster creation process.

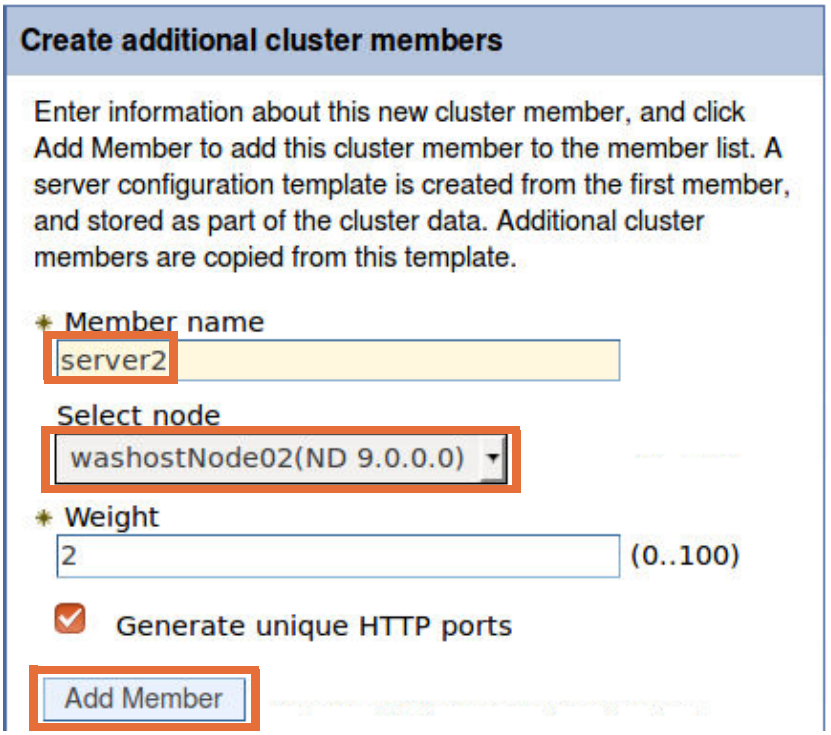
__ a. Enter `server2` for the **Member name**. This name becomes the name of a new server that is created.

__ b. Select **washostNode02** from the list for the node name. This node was created in the previous lab by using a custom profile.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ c. Make sure that **Generate unique HTTP ports** is selected.



__ d. Click **Add Member**.

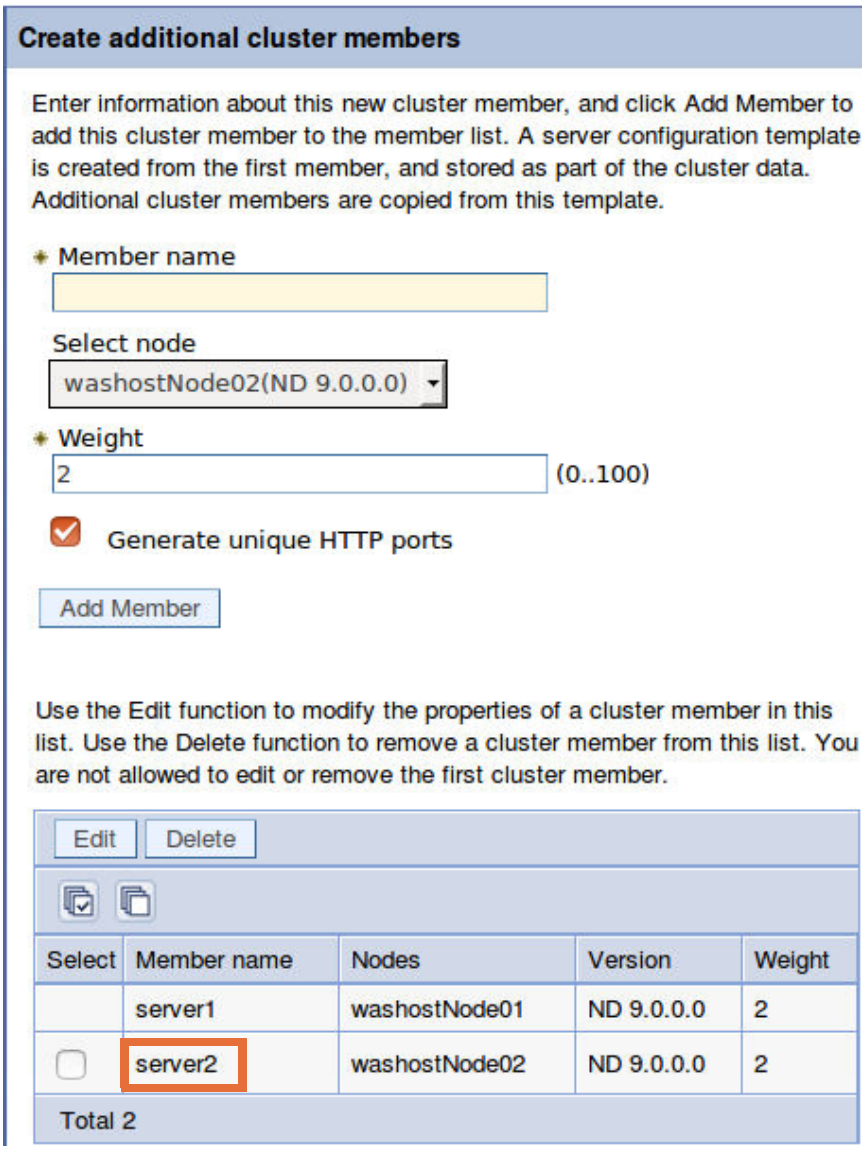
Information

Notice that the first server of the cluster is already listed at the bottom of the page. As new servers are added to the cluster, they are also listed here.

© Copyright IBM Corp. 2016

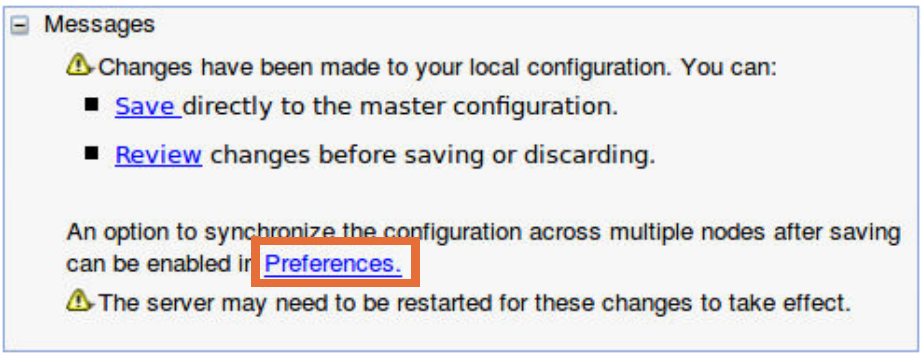
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ e. Notice that the new server now shows at the bottom of the page. More cluster members can be created now or after cluster creation.



__ f. Click **Next**, and then click **Finish** on the Summary page.

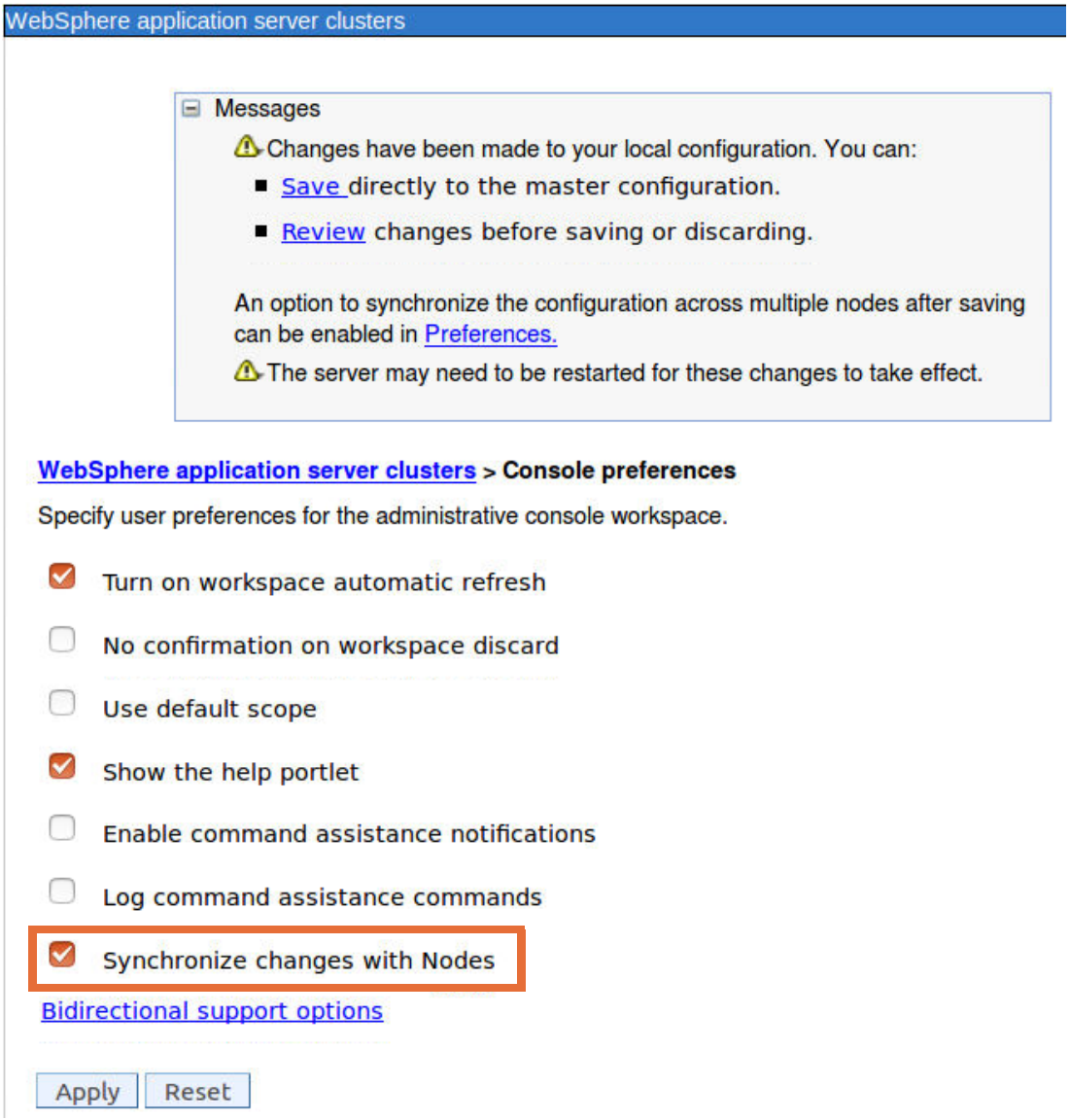
__ g. Before saving the changes, if not already done, set the console preferences to synchronize configuration changes with the nodes when saving. Click the **Preferences** link.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ h. On the Preferences page, select **Synchronize changes with Nodes**.



__ i. Click **Apply**, and then click **Save** to save and synchronize with the nodes.

Information

From now on, any saves are automatically synchronized with the nodes during a save. Preferences settings are persistent and are retained throughout browser invocations.

__ j. Click **OK** on the Synchronize changes with Nodes page.

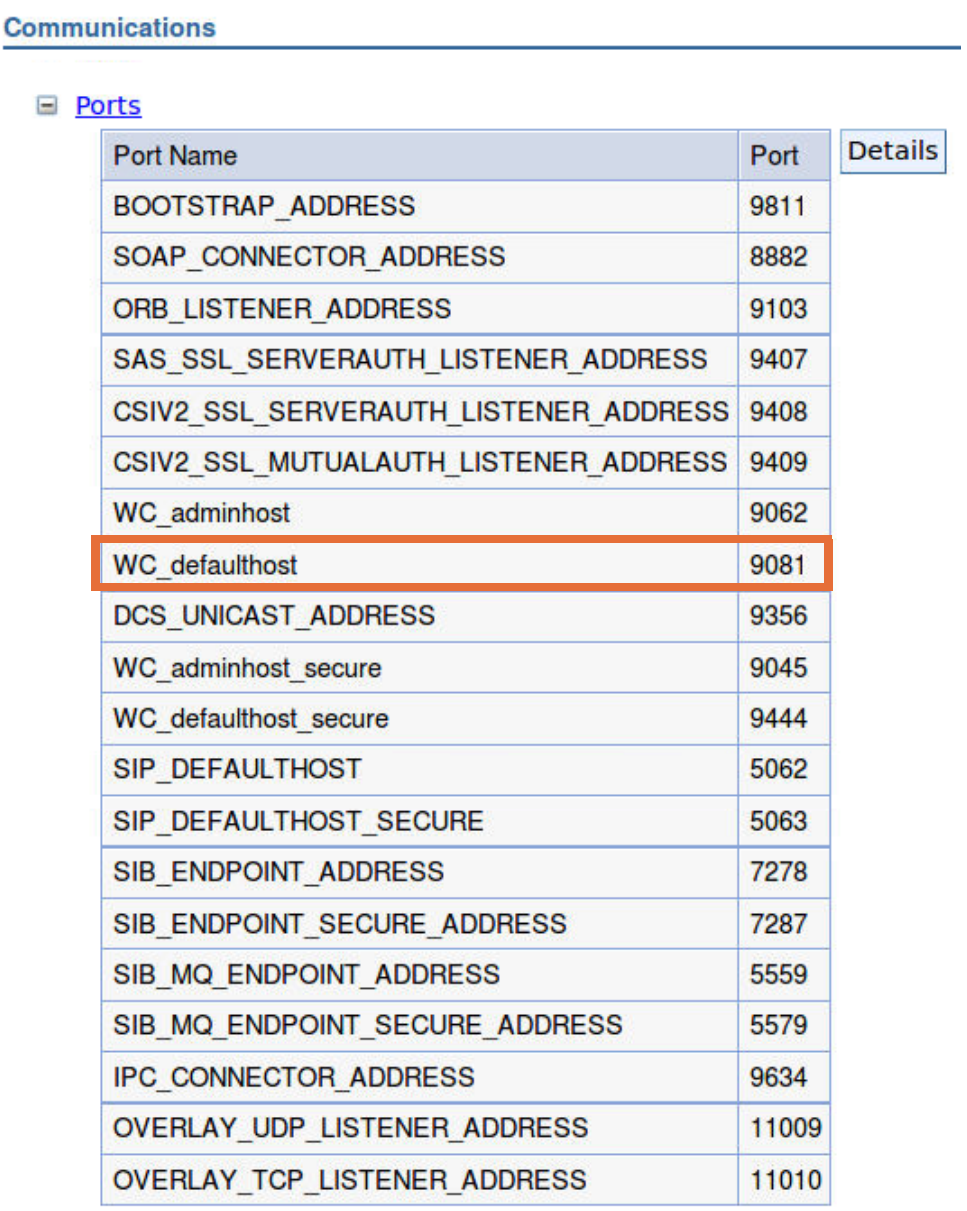
__ 3. Modify the default_host virtual host configuration. This action allows browsers to have direct access to server2 without being forced to use the external IBM HTTP Server.

__ a. View the HTTP Transport for server2. Click **Servers > Server Types > WebSphere application servers > server2**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ b. Expand **Ports** under Communications.



Port Name	Port
BOOTSTRAP_ADDRESS	9811
SOAP_CONNECTOR_ADDRESS	8882
ORB_LISTENER_ADDRESS	9103
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS	9407
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS	9408
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS	9409
WC_adminhost	9062
WC_defaulthost	9081
DCS_UNICAST_ADDRESS	9356
WC_adminhost_secure	9045
WC_defaulthost_secure	9444
SIP_DEFAULTHOST	5062
SIP_DEFAULTHOST_SECURE	5063
SIB_ENDPOINT_ADDRESS	7278
SIB_ENDPOINT_SECURE_ADDRESS	7287
SIB_MQ_ENDPOINT_ADDRESS	5559
SIB_MQ_ENDPOINT_SECURE_ADDRESS	5579
IPC_CONNECTOR_ADDRESS	9634
OVERLAY_UDP_LISTENER_ADDRESS	11009
OVERLAY_TCP_LISTENER_ADDRESS	11010

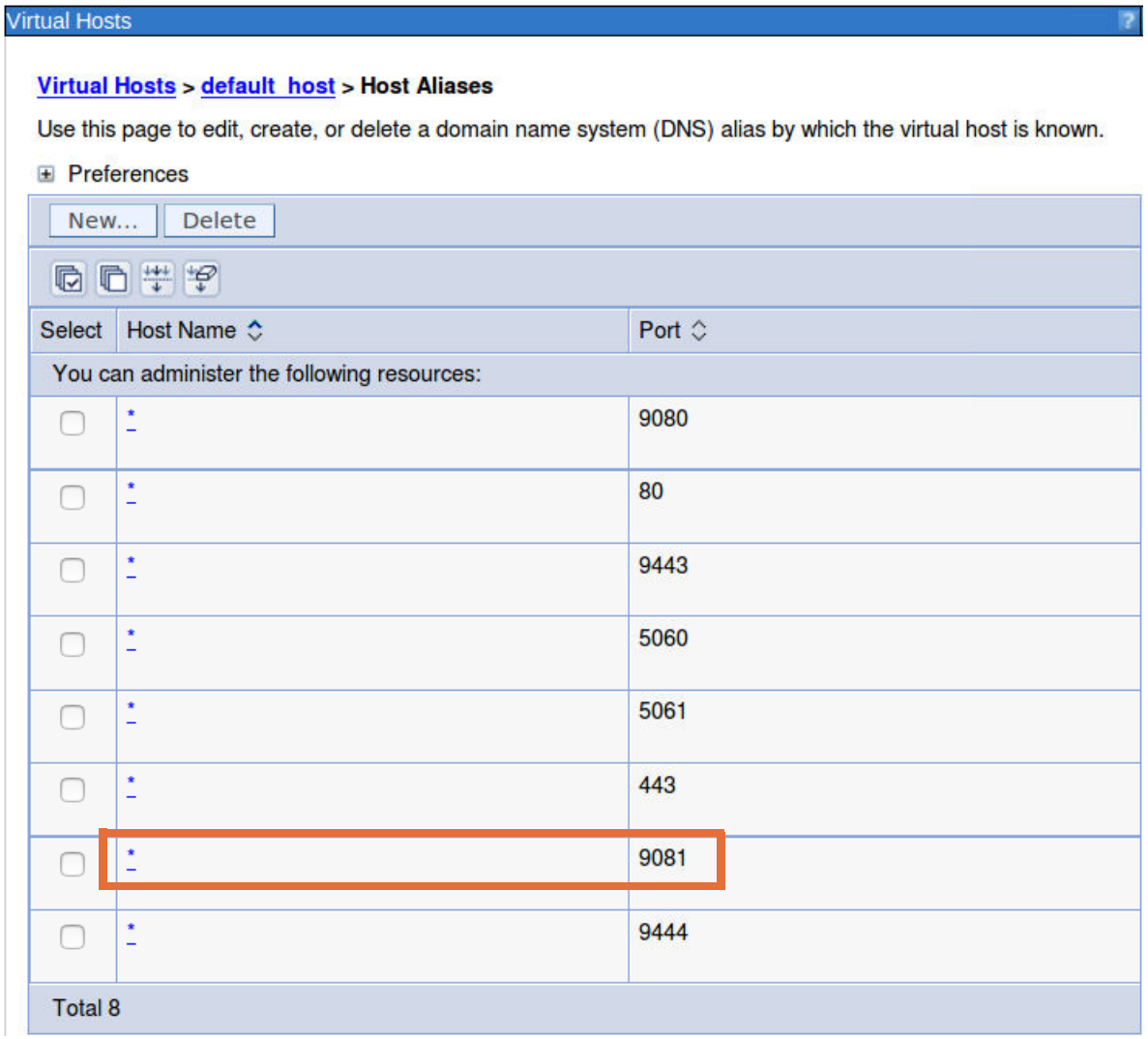
The ports for server2 are listed. The **WC_defaulthost** for server2 is **9081**. You must add this port number to the host aliases list for the default_host.

__ c. Click **Environment > Virtual Hosts > default_host**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ d. Click **Host Aliases** under Additional Properties. The host aliases for default_host are listed. Look for the port 9081 for server2.



Note

If 9081 is not already defined, add it by clicking **New**. Leave the default `*` for the **host name** and specify `9081` for **Port**. Click **OK** and save the changes.

__ 4. Verify that the new cluster is added to the server configuration and start the cluster.

__ a. Click **Servers > Clusters > WebSphere application server clusters**. The PlantsCluster cluster is shown on the page.

© Copyright IBM Corp. 2016

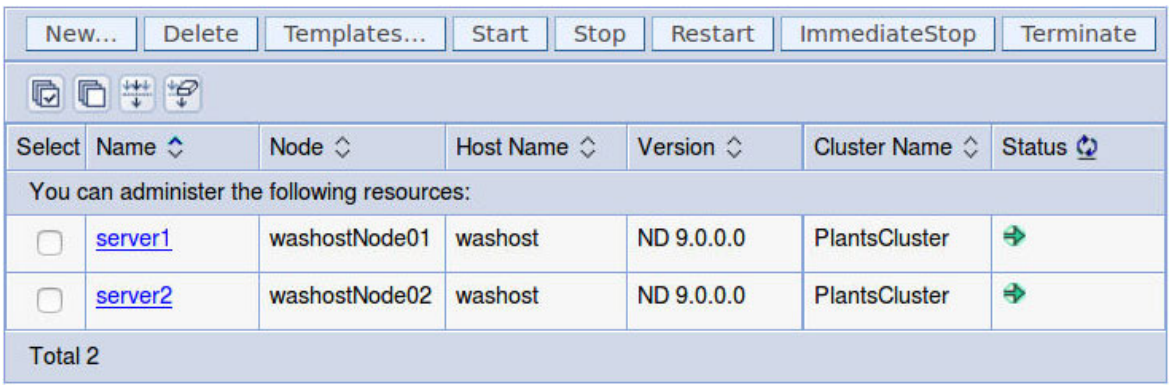
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ b. Select **PlantsCluster** and click **Start** to start the servers on the cluster. Starting the cluster has the same result as starting all the application servers that are cluster members.

Information

Ripplestart is used when you want to restart a cluster without having all members of the cluster stopped at the same time. This function restarts the individual cluster members one at a time, ensuring that the other members are available to handle requests.

__ c. Make sure that both application servers in the cluster are started. This operation can take a few minutes. You can look at the **Servers > Server Types > WebSphere application servers** page to see the status of the cluster members.



Section 4: Setting the applications to run on the cluster

Now that the cluster is defined, the next step is to configure the applications to run on the cluster, rather than on individual servers. Since the web server is used to workload manage the web containers, the web server also must be mapped to the applications. This step is important as it allows the customized `plugin.cfg.xml` files to include the appropriate URIs for each of the applications they are supposed to host.

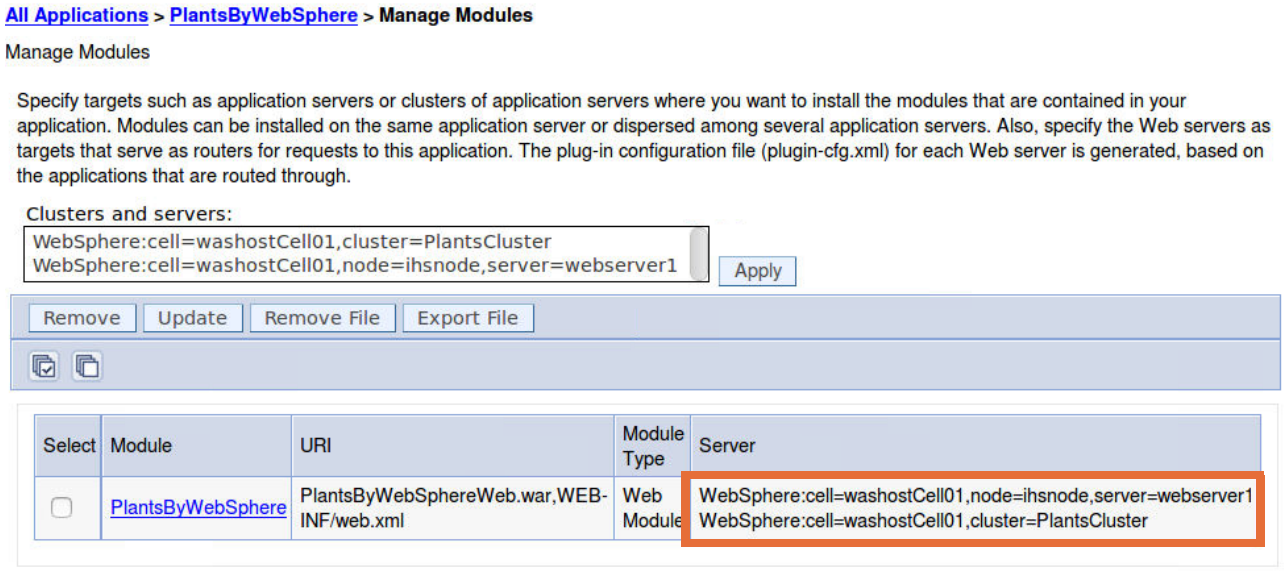
__ 1. For the PlantsByWebSphere application, verify the next series of steps to map the modules to the PlantsCluster cluster and the webserver1 web server.

__ a. Click **Applications > Application Types > WebSphere enterprise applications > PlantsByWebSphere**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ b. Under Modules, click **Manage Modules**. The server area indicates to which server or servers the modules are mapped. In this case, the modules are mapped to webserver1 and the PlantsCluster.



Information

WebSphere automatically mapped the application to the cluster and web server since no other reasonable choices are available. The steps to map an application are provided to show you the steps to map an application to a server or servers. For example, to map the application to the PlantsCluster, complete the following steps:

1) Select the module of the application. Then, in the Clusters and servers list, select both the **PlantsCluster** cluster and the **webserver1** web server (use the Ctrl key to select multiple servers).
2) Click **Apply**. This action creates the mapping.
3) Click **OK**.
4) Make sure that the modules are mapped to both the **PlantsCluster** and the web server.
5) Save the configuration changes.
6) Start the application if necessary.

__ 2. Enable JPA 2.0 on the cluster servers. The PlantsByWebSphere application is written according to the JPA 2.0 standard, and the newest WebSphere runtime defaults to JPA 2.1. A Jython script automates the process of updating both server configurations and restarting the cluster members.

__ a. In a terminal window, change to the deployment manager's bin directory.

```
cd /opt/IBM/WebSphere/AppServer/profiles/Dmgr/bin
```

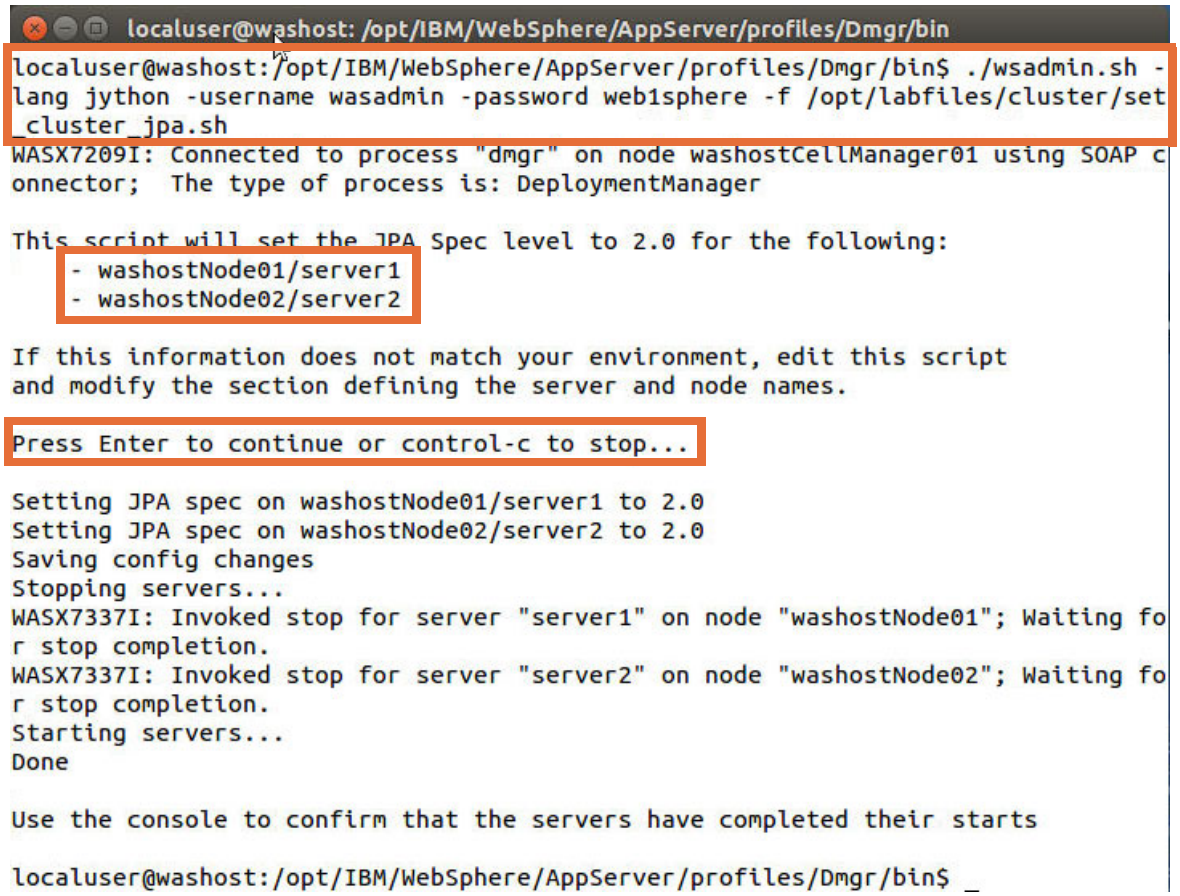
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ b. Execute the following command:

```
./wsadmin.sh -lang jython -username wasadmin -password web1sphere -f
/opt/labfiles/cluster/set_cluster_jpa.sh
```

__ c. The script confirms the configuration. If the node and server names are correct, press Enter to continue. If the information presented is not correct, press Ctrl+C and edit the script before running the command again.



__ d. Wait until both servers complete their restarts.

__ 3. Regenerate and propagate the web server plug-in configuration file.

Although this process happens automatically, do it manually so that you can see the status results and verify that the propagation succeeded.

__ a. Click **Servers > Server Types > Web servers**.

__ b. Select the web server and click **Generate Plug-in**.

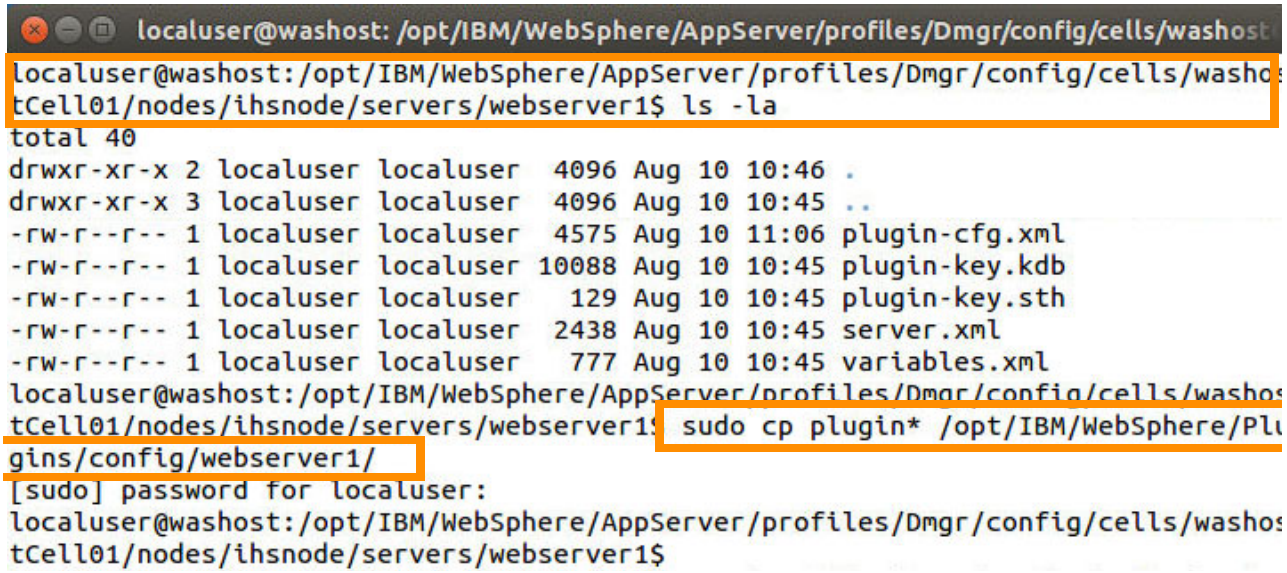
__ c. Propagate the web server plug-in configuration file. Use the terminal window and copy the `plugin-cfg.xml` file to the `plugin` directory. Use the following commands to change directory and then copy the file:

```
cd /opt/IBM/WebSphere/AppServer/profiles/Dmgr/config/cells/
washostCell01/nodes/ihsnode/servers/webserver1/
sudo cp plugin* /opt/IBM/WebSphere/Plugins/config/webserver1/
```

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Enter `passw0rd` when prompted for the localuser's password.



Section 5: Creating a cluster scoped JDBC resource

When creating the first cluster member from the existing server1, all resources that are already defined at the server and node scope are maintained. Unfortunately, when adding the second server on the washostNode02 node, the resource definitions from server1 and washostNode01 are not automatically defined. You now have a problem: since both servers run the same applications, by virtue of being on the same cluster, they both need access to the same resources.

One solution is to re-create the resources at the node scope for each additional node as its servers are added to the cluster. That solution works, but the disadvantage is that you must do it every time a new node server is added to the cluster. A better solution is to define resources at the cluster scope.

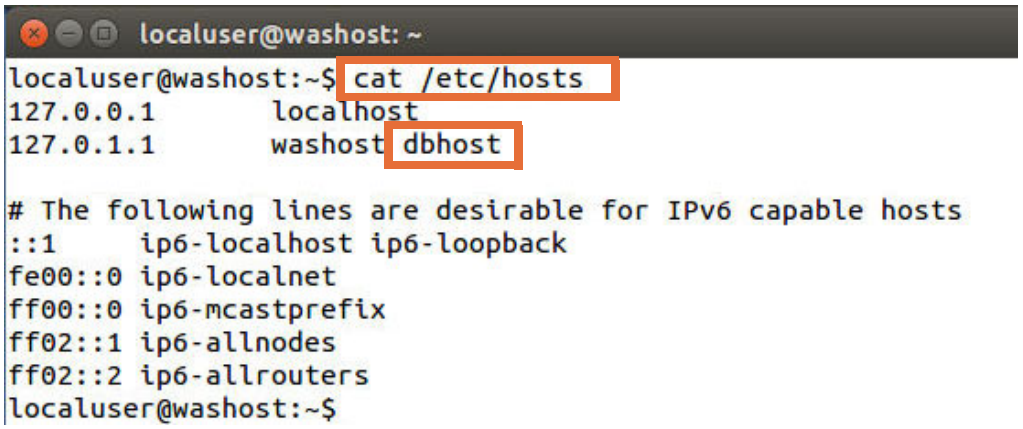
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Information

Resources can be added at the cluster scope only if the cluster members are running in similar operating environments. Since many resources require pointers to a file system location, it does not work to define resources at the cluster scope for cluster members that run in both Windows and Linux. In that case, you must define the resources at the node level.

__ 1. Verify that `dbhost` is defined as an alias in the `/etc/hosts` file.



__ 2. Remove the existing node scoped DB2 Universal JDBC Driver Provider (XA) provider.

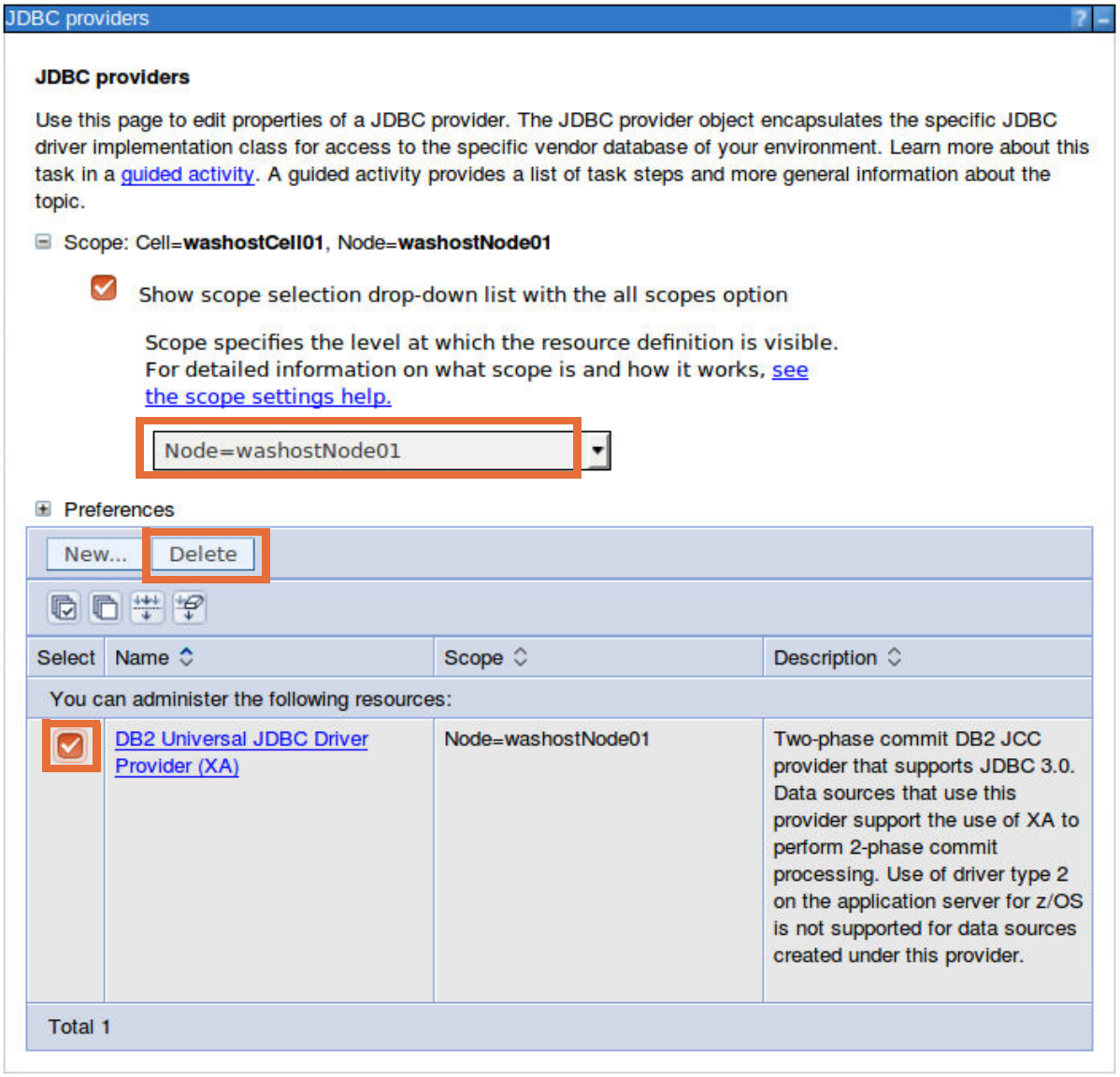
__ a. Click **Resources > JDBC > JDBC providers**.

__ b. From the **Scope** list, select **Node=washostNode01**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ c. Select the **DB2 Universal JDBC Driver Provider (XA)** provider that is defined at the Node=washostNode01 scope, and click **Delete**.



Information

Cluster scope takes precedence over node scope, so node scoped resources do not have to be deleted. However, deleting them does avoid ambiguity.

Deleting the JDBC provider also deletes any data sources that are defined under it.

__ d. Save your changes.

__ e. Click **OK** at the prompt to confirm that the nodes are synchronized.

__ 3. Create a cluster-scoped JDBC provider and data source.

__ a. Click **Resources > JDBC > Data sources**.

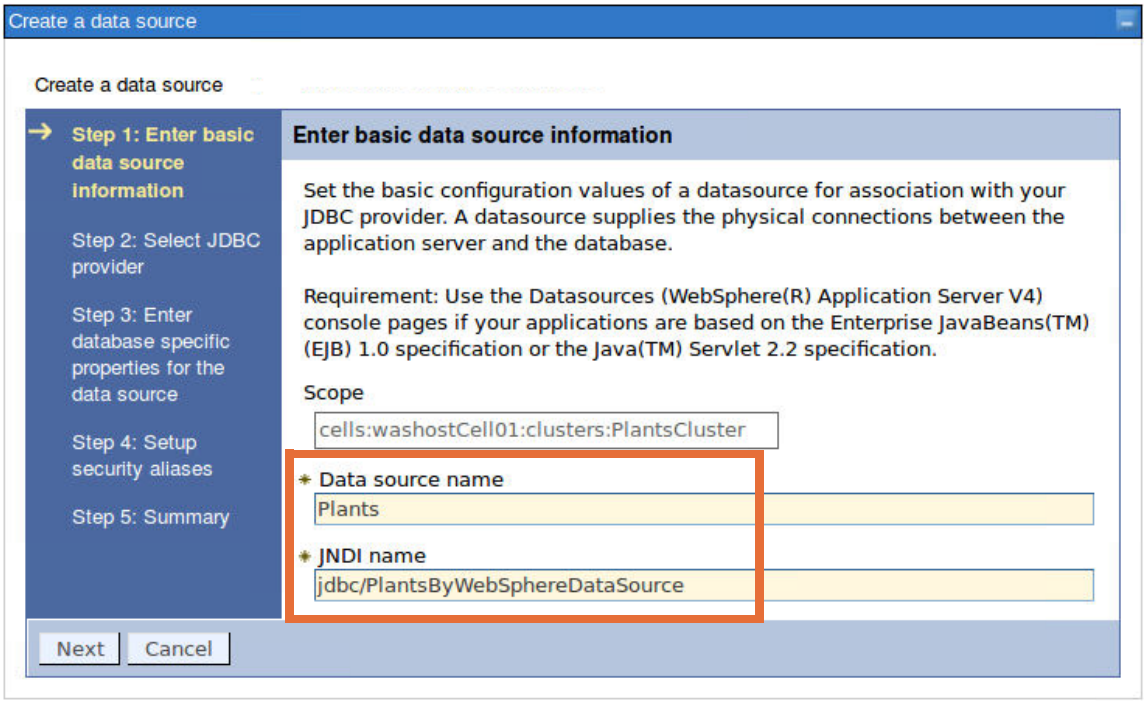
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ b. From the **Scope** list, select **Cluster=PlantsCluster**.

__ c. Click **New**.

__ d. Enter `Plants` for the data source name and `jdbc/PlantsByWebSphereDataSource` for the JNDI name.

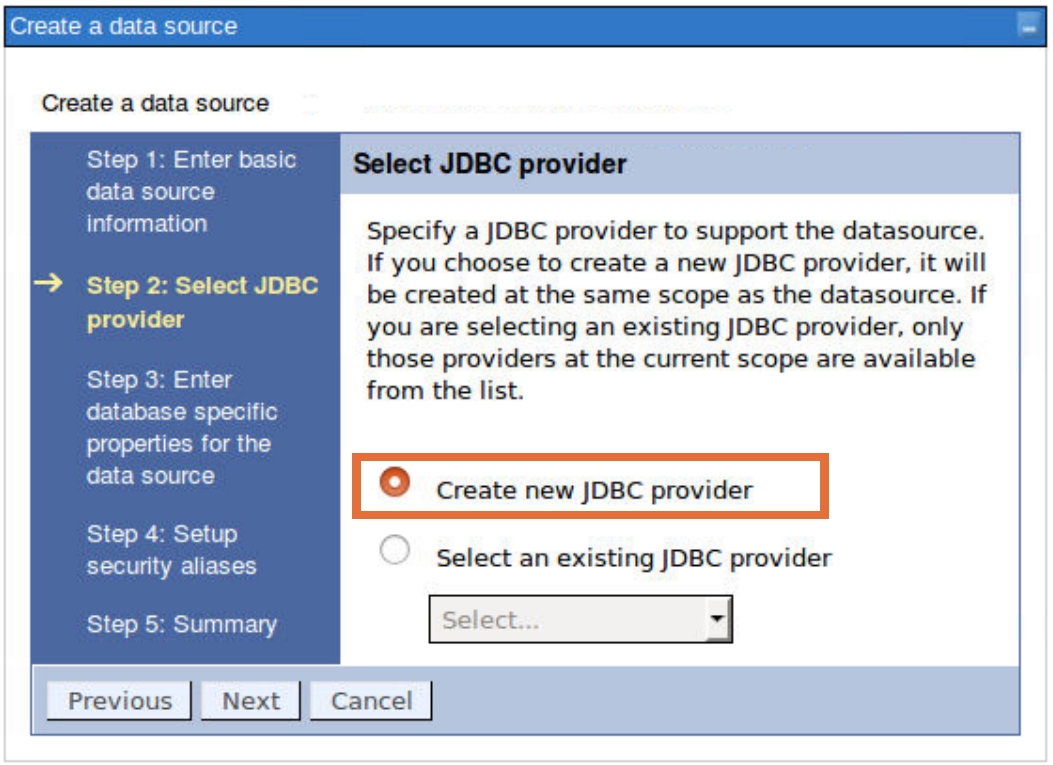


__ e. Click **Next**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ f. Since you do not yet have a cluster-scoped JDBC provider, select **Create new JDBC provider**.



__ g. Click **Next**.

Note

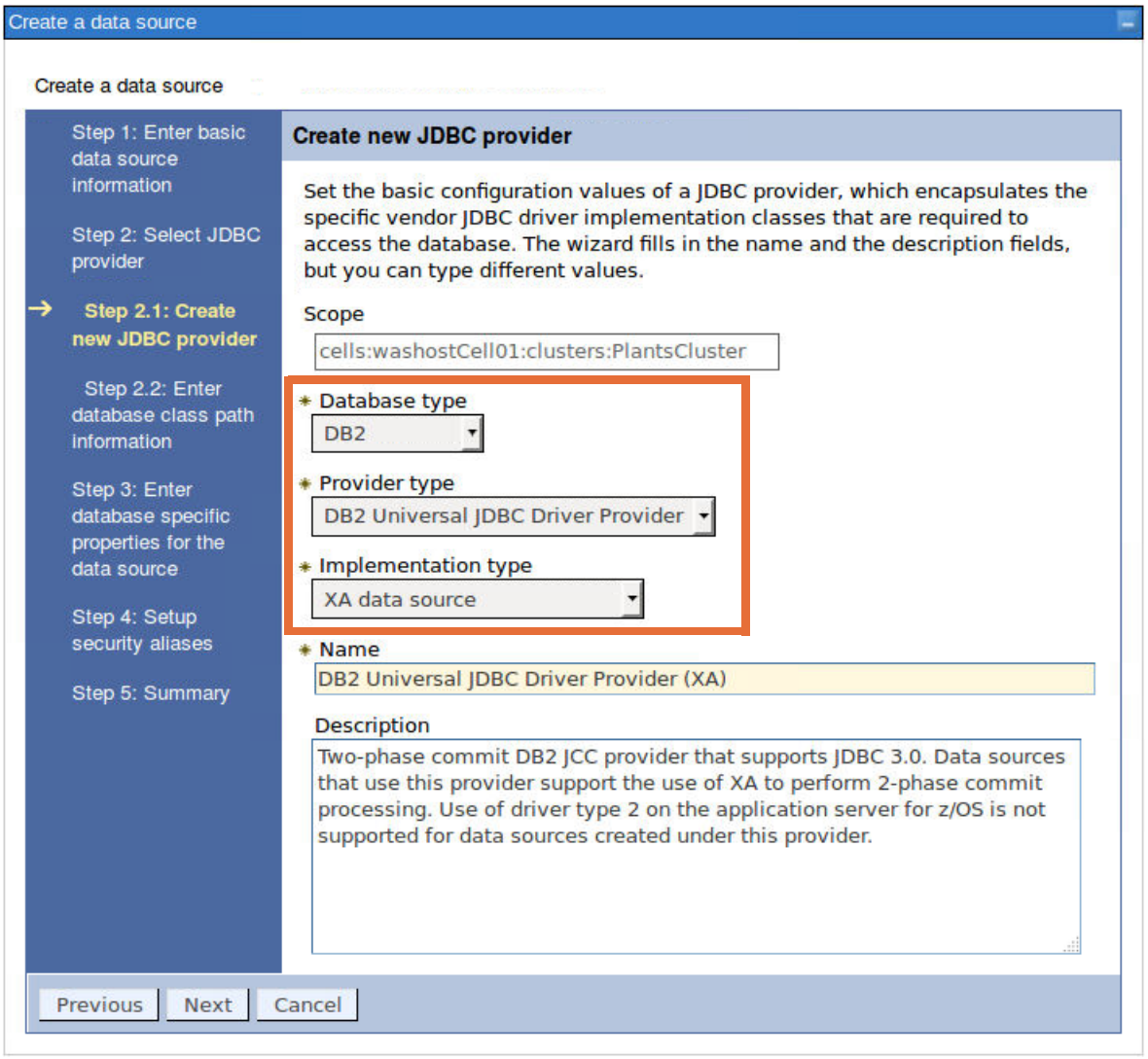
The Create Data source wizard temporarily goes to the Create JDBC provider wizard.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ h. Enter the following selections:

- Select **DB2** for the Database type.
- Select **DB2 Universal JDBC Driver Provider** for the Provider type.
- Select **XA data source** for the Implementation type.

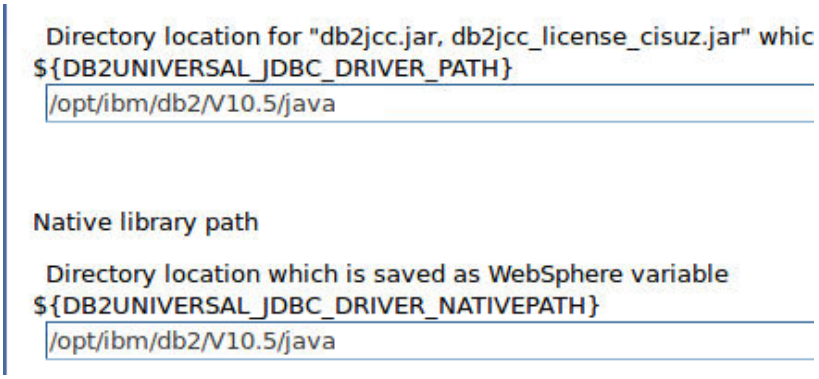


Click **Next**.

© Copyright IBM Corp. 2016

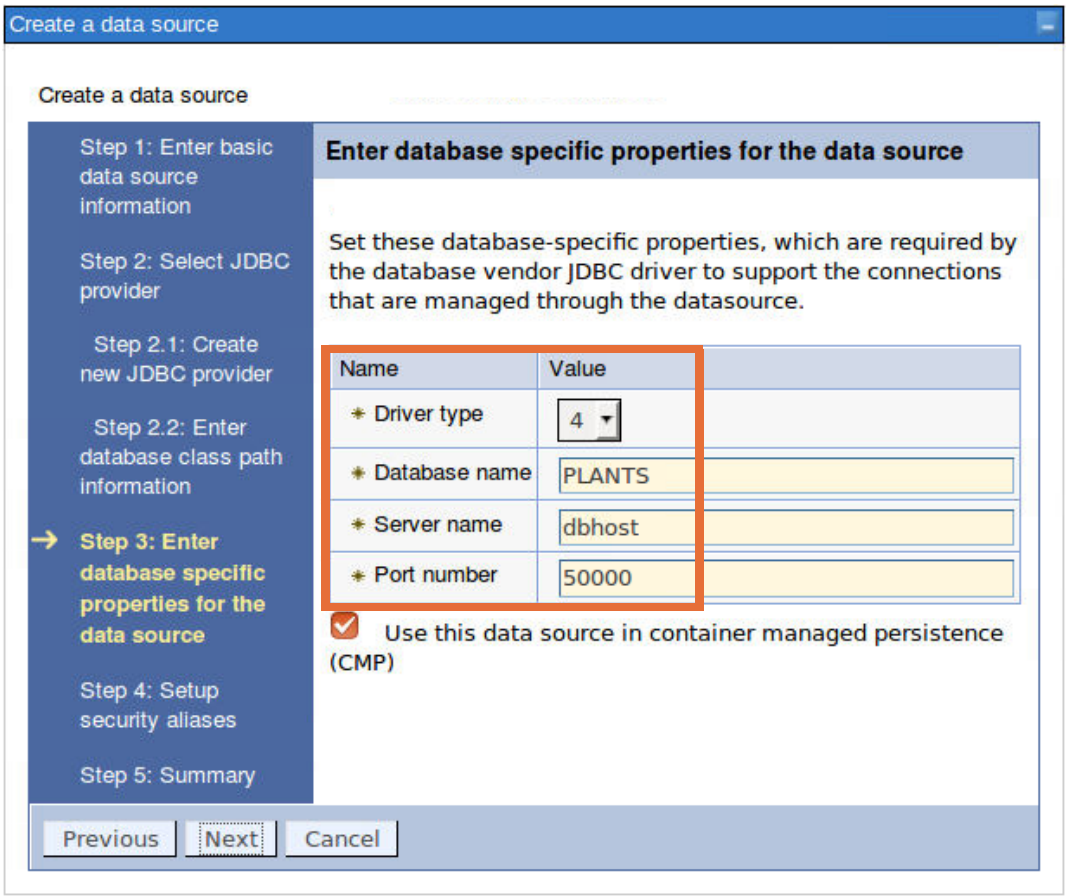
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ i. On the next step, enter the database class path information in both directory location fields. On Linux, this path is `/opt/ibm/db2/V10.5/java`. Click **Next**.



__ j. Enter the following database-specific properties for the data source:

- **Driver type**: `4`
- **Database name**: `PLANTS`
- **Server name**: `dbhost`
- **Port number**: `50000`



Click **Next**.

__ k. From the **Component-managed authentication alias** list, select **washostNode01/PlantsApp**. Click **Next**.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ l. On the Summary page, click **Finish**.

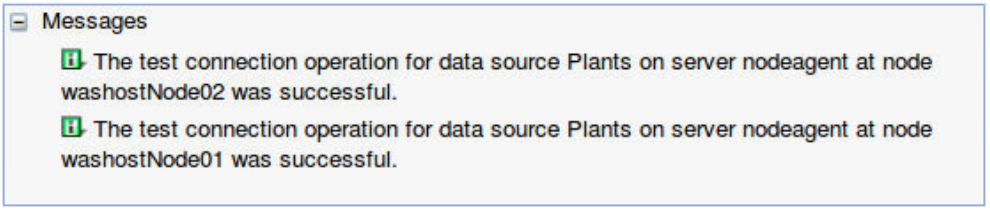
__ m. Save your changes. Click **OK**.

__ 4. Test the data source connection.

__ a. If you are not placed on the Data sources page, click **Resources > JDBC > Data sources**.

__ b. Make sure the **Cluster=PlantsCluster** scope is selected.

__ c. Select the **Plants** data source and click **Test connection**. Examine the messages that are generated to make sure that both node agents were able to connect.



Note

For the test to succeed, DB2 and the node agents must be running.

This exercise also assumes that the dbhost definition is added to your hosts file. This procedure is done in a previous exercise. If not, add dbhost as an alias for your host.

__ 5. Disable the HTTPOnly setting.

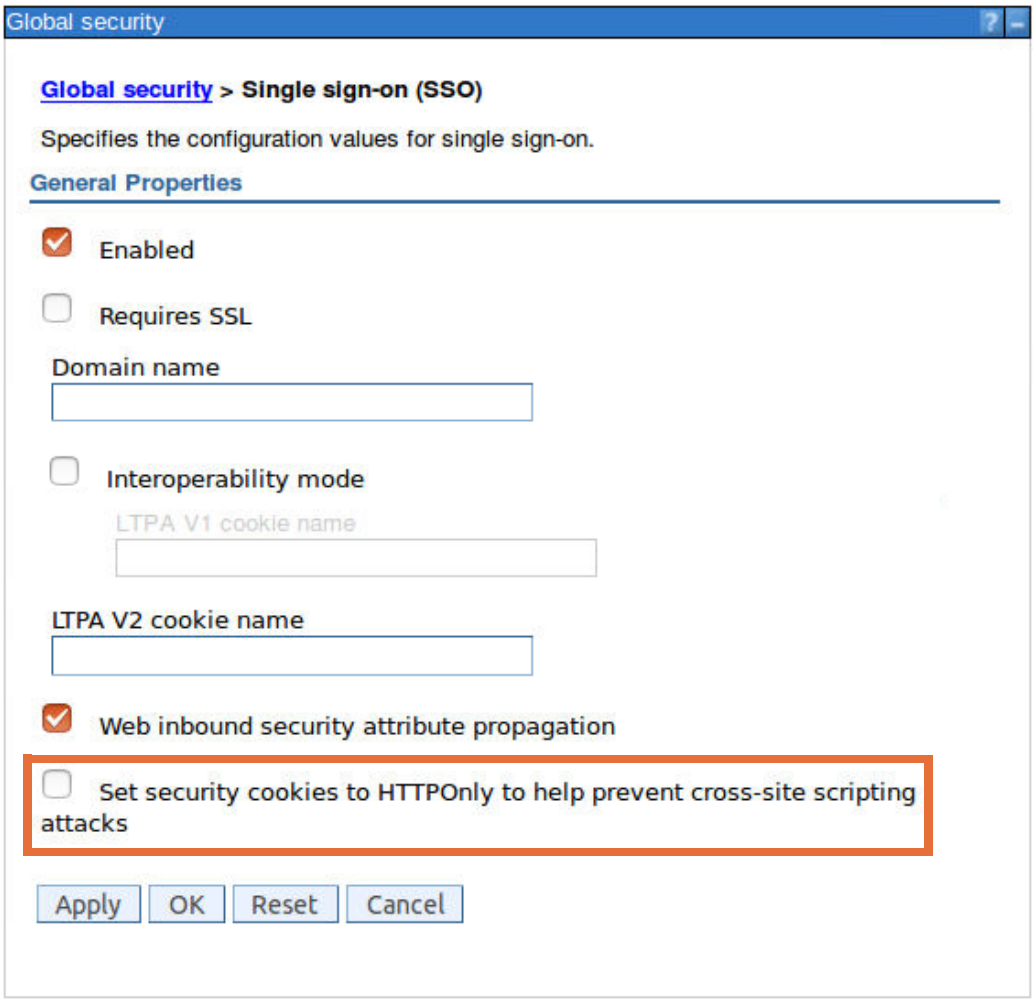
__ a. Click **Security > Global security**.

__ b. Under Authentication, expand **Web and SIP Security** and click **Single sign-on (SSO)**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ c. Clear the **Set security cookies to HTTPOnly to help prevent cross-site scripting attacks** check box.



__ d. Click **OK** and save the changes.

__ e. Click **OK** to complete the node synchronization.

Note

This setting is enabled by default to help limit the ability of JavaScript to access your cookies. Although this setting is beneficial from a security perspective, it prevents you from seeing the JSESSIONID cookie, which is interesting to see later in this exercise.

This setting is *not* something that you would typically disable in your production environment.

Section 6: Testing the application

In this section of the exercise, the application is tested in a clustered environment. The application is served from both application servers (cluster members) until the application creates an HTTP session object. At that point, affinity is established. This condition means that from that point on, all

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

requests are directed to the same application server. This action is done so that the user's session information is available locally.

If the cluster member that is holding the user session becomes unavailable, the web server plug-in reroutes the request to another cluster member. However, this situation presents a problem because the new application server does not (by default) have access to the session information.

The exercise initially demonstrates this "problem," but then later configures a solution that allows the cluster members to share their session information. As a result, even if a cluster member fails, users are still able to access their session through another cluster member.

__ 1. Restart your environment.

__ a. Using the administrative console from a Firefox browser, stop all the application servers (**Servers > Server Types > WebSphere application servers**).

__ b. Using the administrative console, stop all the node agents (**System administration > Node agents**).

__ c. Using the administrative console, stop the deployment manager (**System administration > Deployment manager**).

__ d. Use the `startManager` and `startNode` scripts in the `bin` directories to start your cell. Or use the following script, which starts the deployment manager and both node agents:

```
/opt/labfiles/scripts/start_cell.sh
```

__ e. Start the PlantsCluster (**Servers > Clusters > WebSphere application server clusters**).

__ f. Verify that the web server is running (**Servers > Server Types > Web servers**).

__ 2. Use a Chrome browse to access the PlantsByWebSphere application.

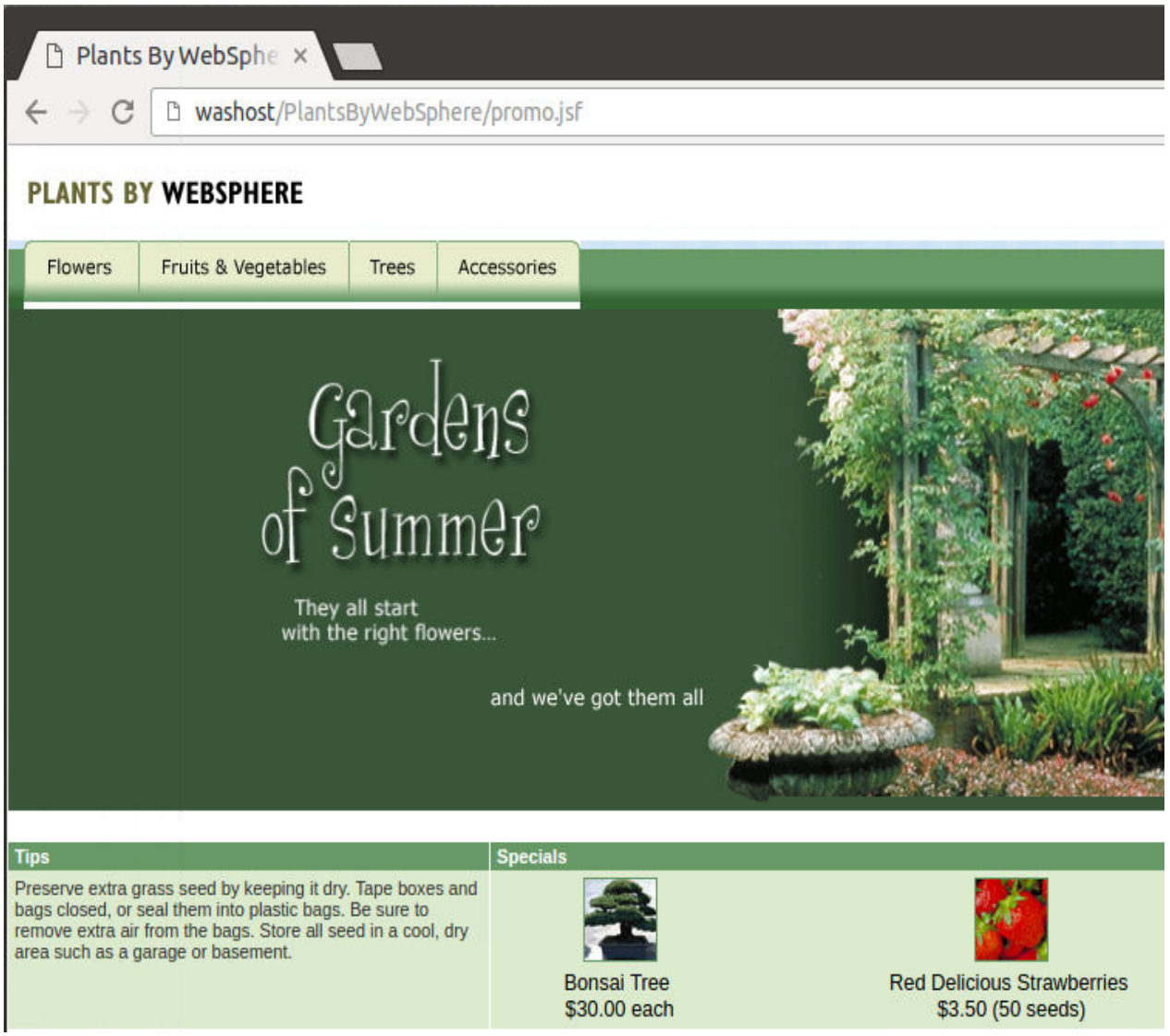
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

A different browser than the one used by the administrative console needs to be used by PlantsByWebSphere so that the application and authentication cookies do no interfere with those used by the administrative console.

__ a. Open a new Chrome browser window and access the PlantsByWebSphere application by entering the following URL:

```
http://washost/PlantsByWebSphere
```



Important

It is important to note that the URL does not include a port number. As a result, the request is going to go through the external web server. This condition is important because it is the WebSphere plug-in that is running within the web server process that has the intelligence to route the requests to the various cluster members.

__ b. Click **Flowers** in the upper left.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ c. Click any of the available flowers, and then click **Add to cart**.

__ d. This action takes you to the shopping cart. Notice the flower that you selected is listed.

__ e. Click the **Trees** tab in the upper left, select a tree entry, and add it to your cart. Notice that both your flower and your tree are in your shopping cart.

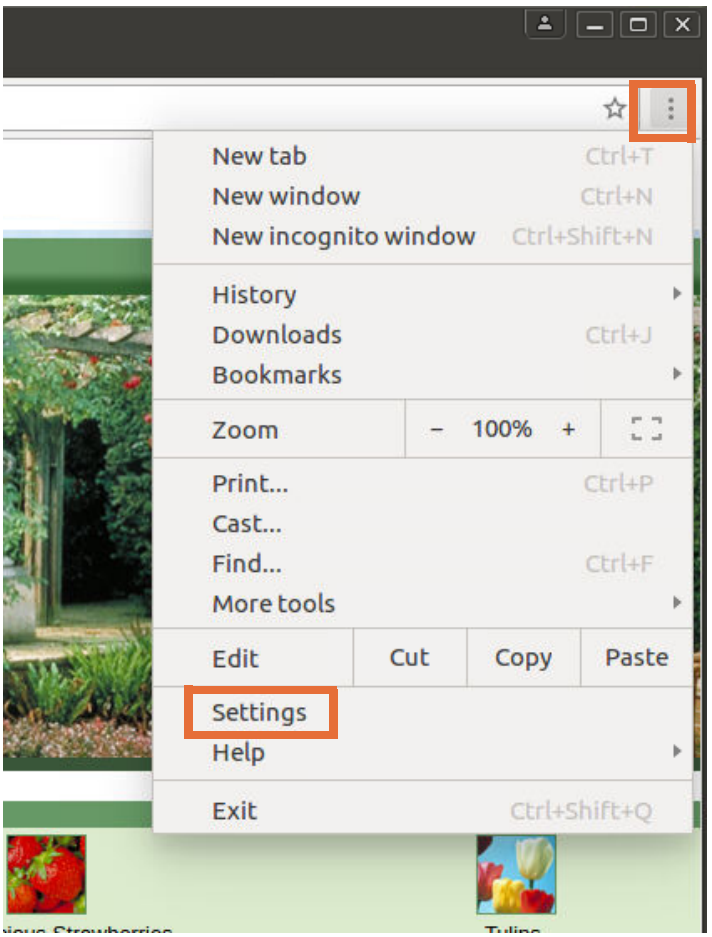
Information

Based on the content of the JSESSIONID cookie, the web server plug-in knows which server is hosting your information. Given that affinity, the plug-in makes sure to route all of your requests to the same server (or cluster member).

This feature allows the server to store what is in your shopping cart and make it available as you continue to shop.

__ 3. Look for the session cookie.

__ a. To view the cookies for the application, open the browser settings windows by clicking the **three vertical dots** in the upper-right corner of the browser window and clicking **Settings**.



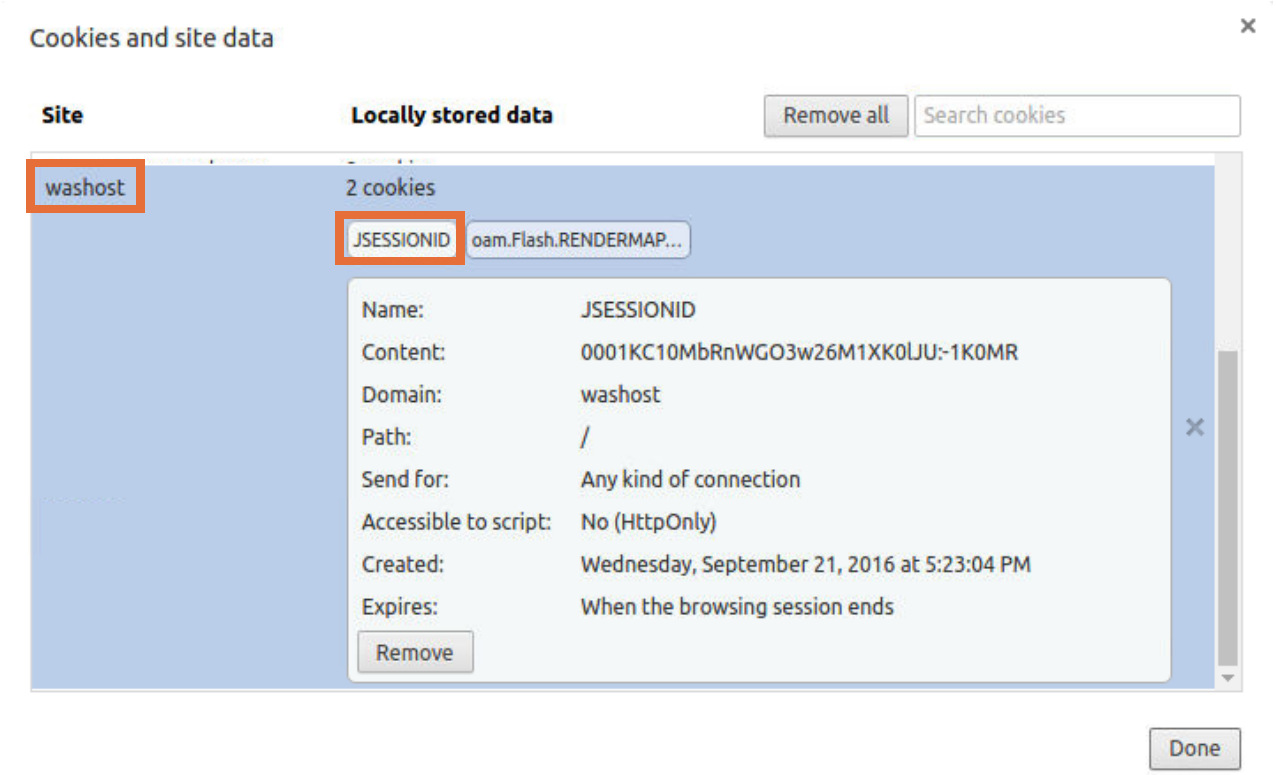
__ b. Scroll to the bottom of the settings window and click **Show advanced settings**.

__ c. In the **Privacy** area, click **Content settings**.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ d. In the **Cookies** area, click **All cookies and site data**.

__ e. From the **Site** list, select **washost** and click **JSESSIONID**.



__ f. Click the **JSESSIONID** cookie in the list to see its contents.

Information

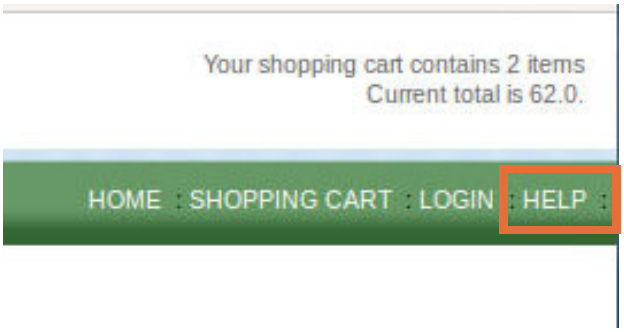
The value of the JSESSIONID cookie contains various pieces of information, including the cluster member (called the CloneID) for which you have affinity. In some cases, the CloneID is obscured because it contains a list of CloneIDs.

__ g. Close the settings tab.

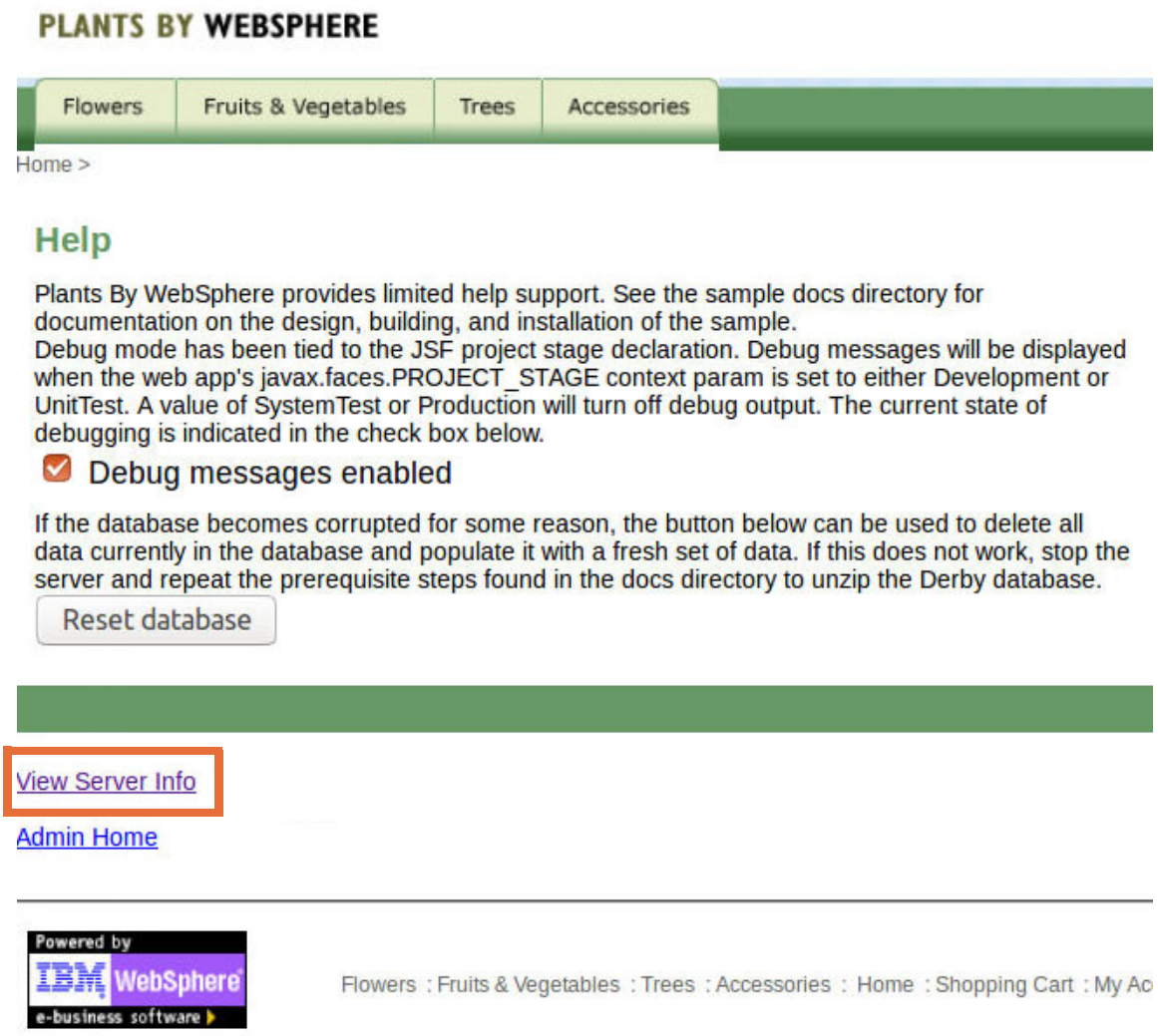
© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ 4. View the server runtime information. This information is useful to understand the failover testing that is done later in this exercise.

__ a. To view the runtime server information, click **Help** in the navigation bar at the top of the screen.



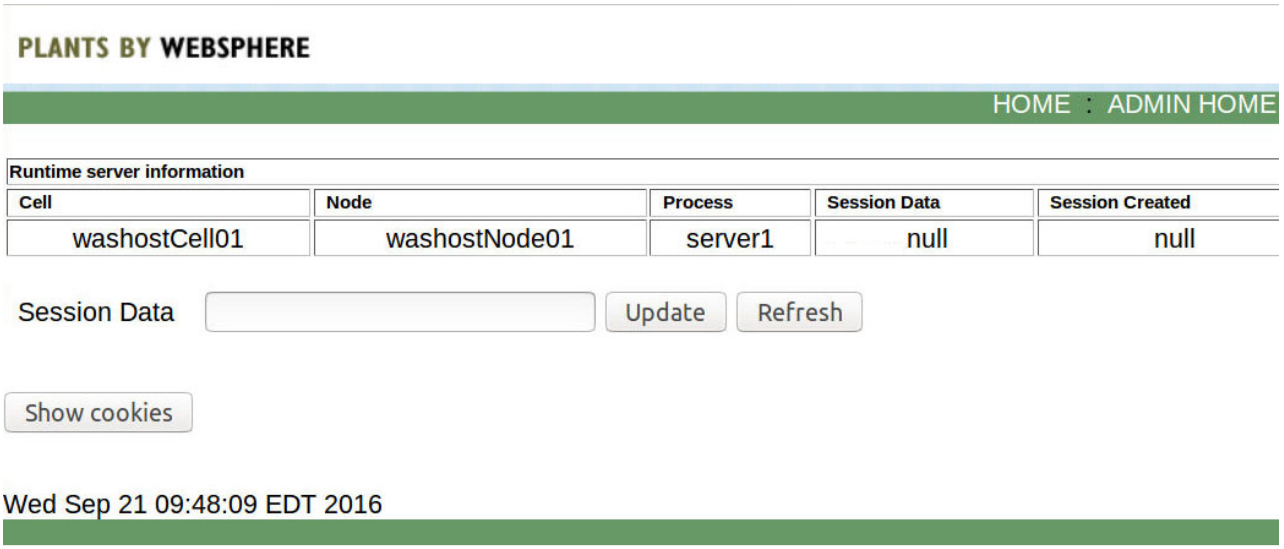
__ b. On the Help page, click the **View Server Info** link near the bottom of the page.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ c. On the server information page, notice that the **Process** field shows the server name and that the **Session Data** and **Session Created** fields are **null**.



__ d. Take note of the server name in the **Process** field: _____

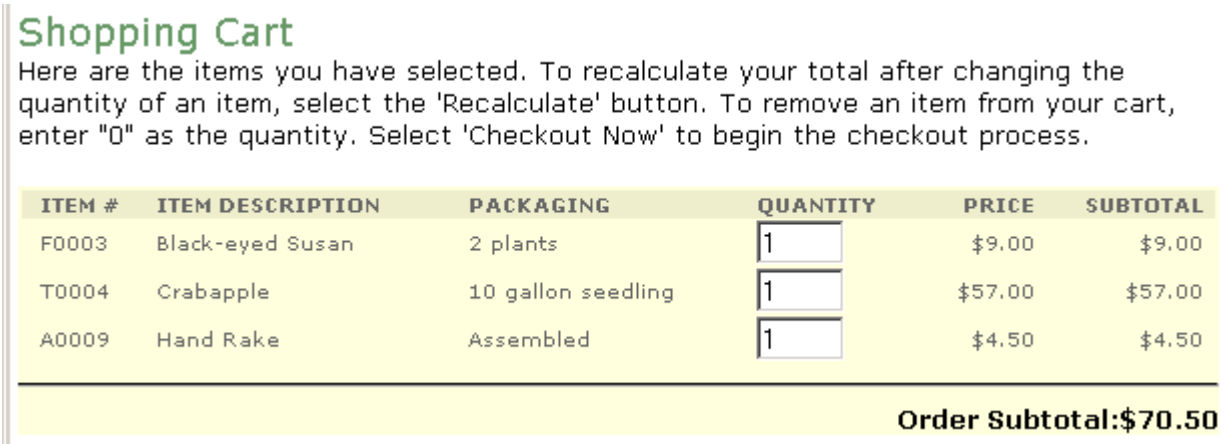
Important

This information is important because this server is the server to which your browser currently has affinity. Thus the session information is stored specifically on that server. If that server fails, your session information can be lost.

__ 5. Continue shopping.

__ a. Click **HOME** in the top navigation bar of the View Server Info page.

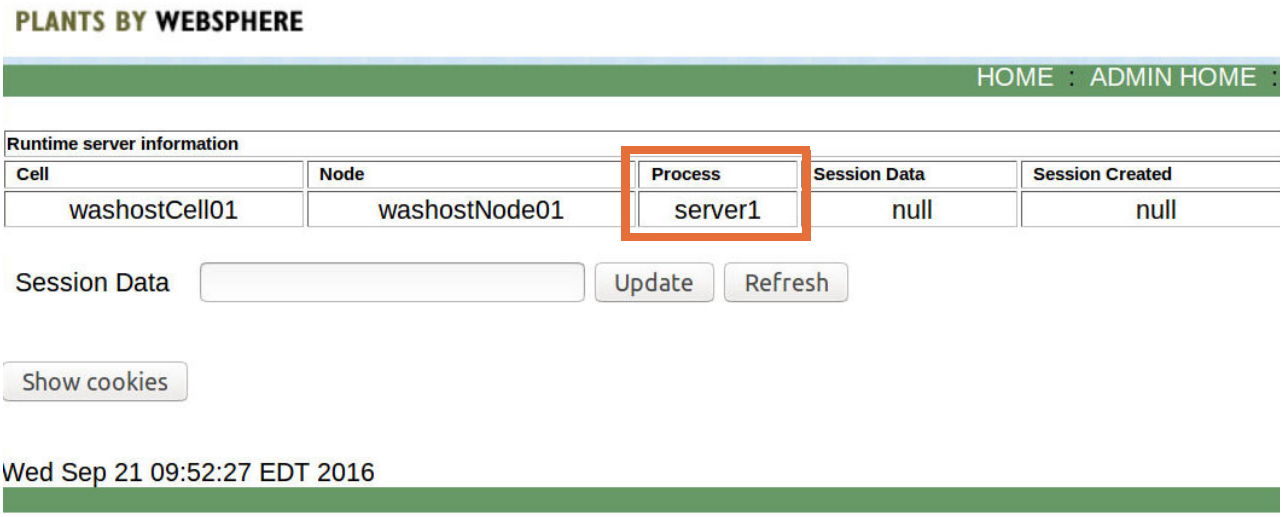
__ b. Add several more items to your shopping cart. Notice that the shopping cart continues to include your previously added items.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ c. Return to the View Server Info page (**Help > View Server Info**) and notice that the server name in the **Process** field remains the same. This information does not change because of the affinity with that server.



__ 6. Stop the server to which you have affinity.

__ a. Leave your browser window to PlantsByWebSphere open.

__ b. Open a new browser tab for the administrative console.

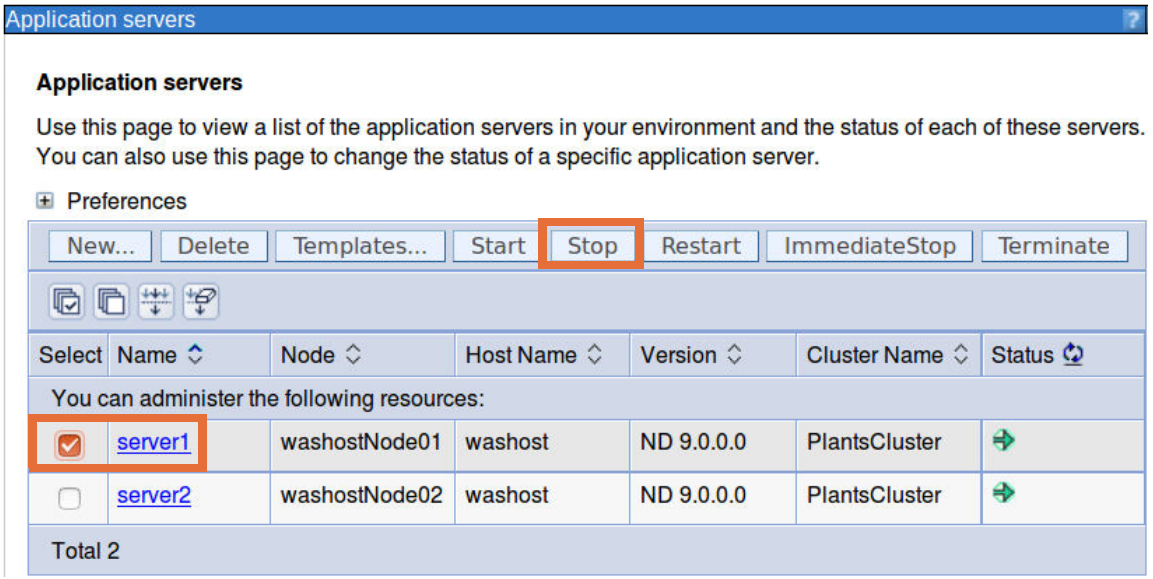
__ c. Click **Servers > Server types > WebSphere application servers**, select the server to which you have affinity, and click **Stop**. If you are prompted to confirm the stop in the **Stop server** panel, click **OK**.

Information

This action simulates a server failure and forces a failover to the other cluster member.

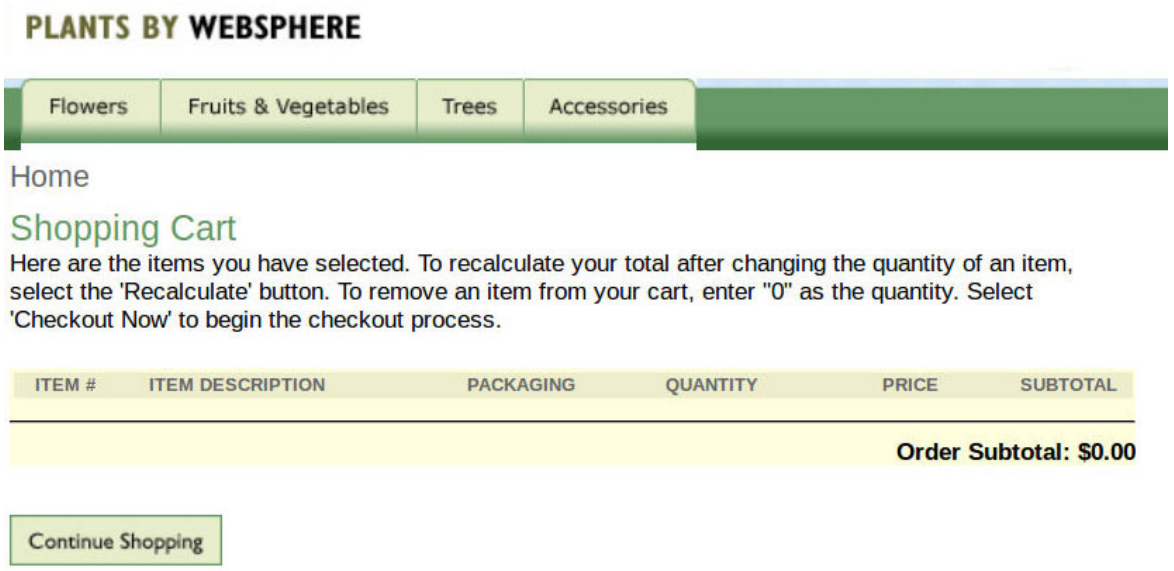
© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ d. Make sure that the server is stopped before returning to the PlantsByWebSphere window. Click the **Status** refresh icon until the Status shows a complete stop.



__ e. Return to the PlantsByWebSphere browser tab and click **Home**.

__ f. Return to the **Shopping Cart**. Notice that the shopping cart is empty.



__ g. Close the PlantsByWebSphere browser window.

Information

The PlantsByWebSphere application is not coded to store the shopping cart in the session information. Therefore, a server failure causes the loss of the shopping cart contents.

If the failover of your session information is important, it is necessary to design your application with session failover in mind. A number of different designs are possible, but that discussion is outside of the scope of this course.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

One possible approach is to store the contents of the shopping cart in the HTTP session object. This approach is demonstrated in the next part of this exercise.

Section 7: Configuring session replication settings

In order for members of a cluster to share session information, a strategy to share session data must be put in place. WebSphere Application Server provides various mechanisms to achieve this goal. The main strategies are database and memory-to-memory replication. Setting up either of these mechanisms is straightforward. In this exercise, memory-to-memory replication is set up to handle session data replication.

Session management can be configured on each of the servers in the cluster. This action can be completed when you create the cluster or at a later point.

In this section, you configure session replication settings.

__ 1. Stop the remaining server in the PlantsCluster.

__ a. Click **Servers > Server types > WebSphere application servers**.

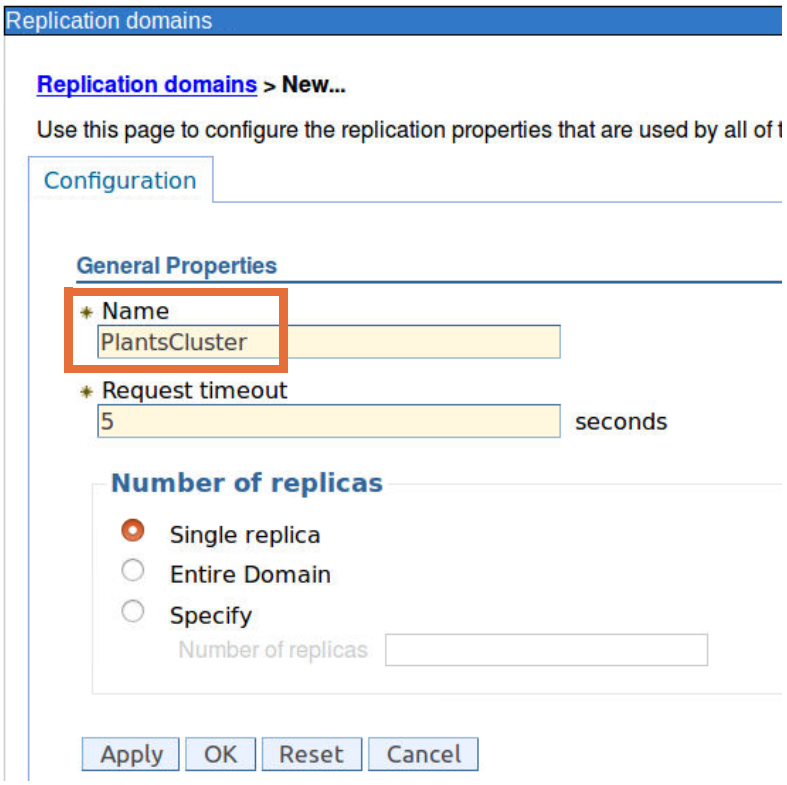
__ b. Select the server that is still running, and click **Stop**. If you are prompted to confirm the stop in the **Stop server** panel, click **OK**.

__ 2. Configure a replication domain.

__ a. Click **Environment > Replication domains**.

__ b. Click **New** to create a Replication domain.

__ c. Enter `PlantsCluster` for the **Name**. Keep all remaining defaults.



__ d. Click **OK**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ e. Save the changes.

__ 3. Configure the memory-to-memory session replication settings for the cluster members.

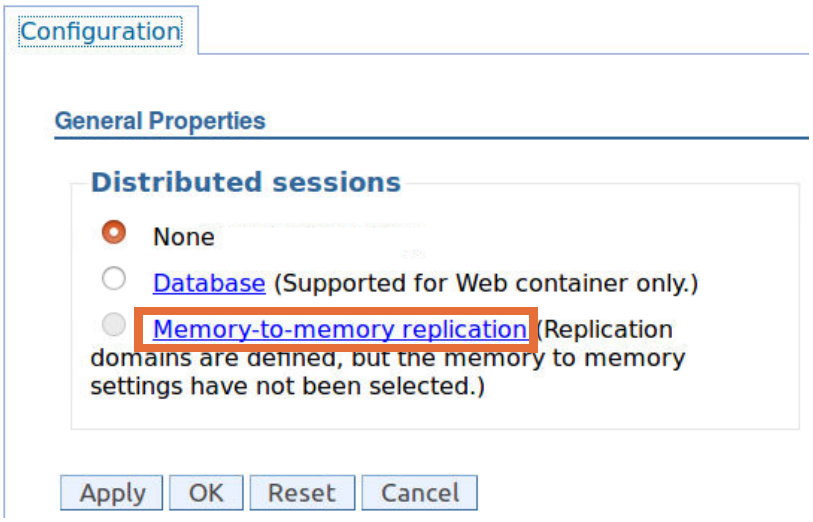
__ a. Click **Servers > Server Types > WebSphere application servers**.

__ b. Click the hyperlink for either one of the servers.

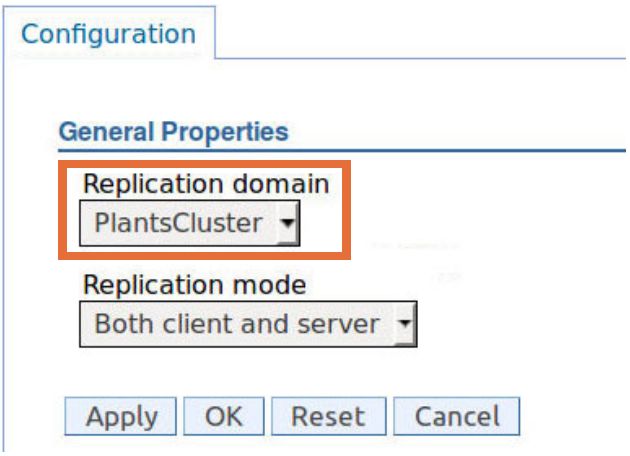
__ c. Under Container Settings, click **Session management**.

__ d. Under Additional Properties, click **Distributed environment settings**.

__ e. Click the **Memory-to-memory replication** hyperlink.



__ f. In the General Properties area, select **PlantsCluster** for the replication domain. Verify that the replication mode is **Both client and server**.



__ g. Click **OK**.

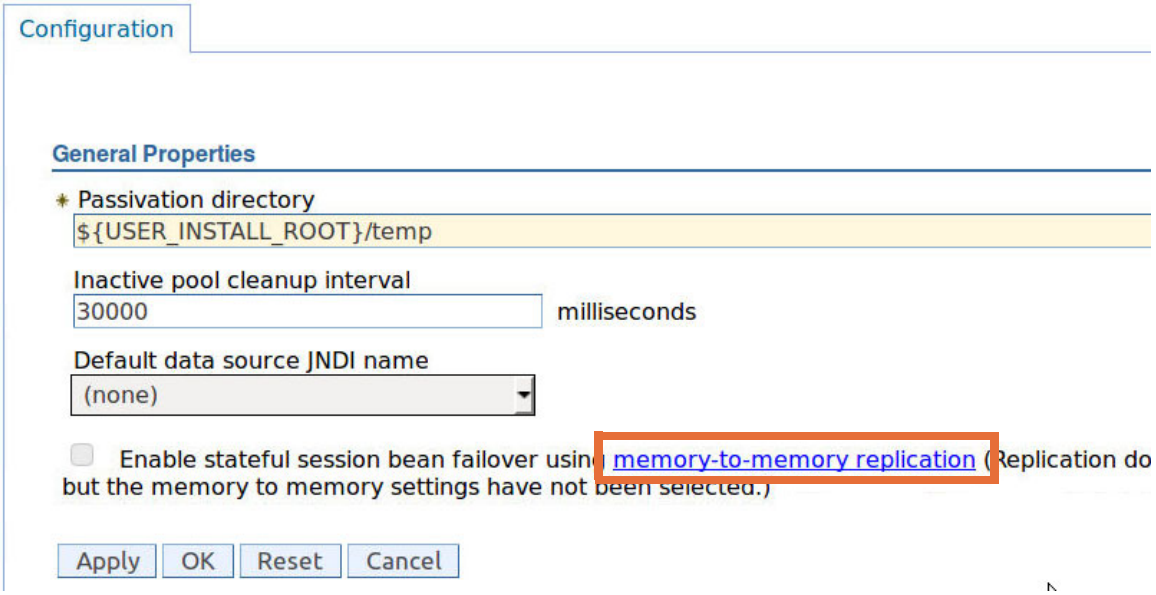
__ h. On the Distributed environment settings page, click **OK**.

__ i. On the breadcrumb trail, click the server name.

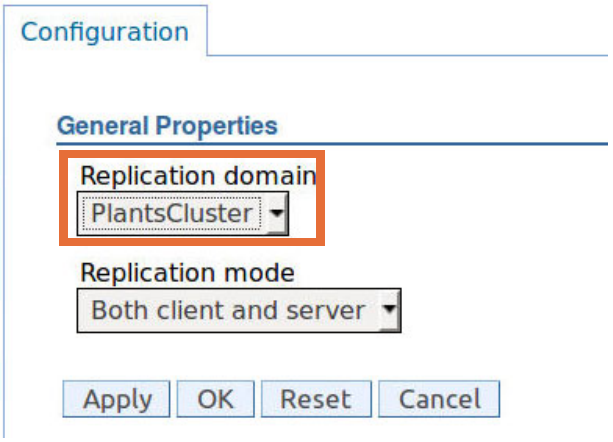
__ j. Under Container Settings, click **EJB Container Settings > EJB container**.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ k. Click the **memory-to-memory replication** hyperlink.



__ l. In the General Properties area, select **PlantsCluster** for the replication domain. Verify that the replication mode is **Both client and server**.

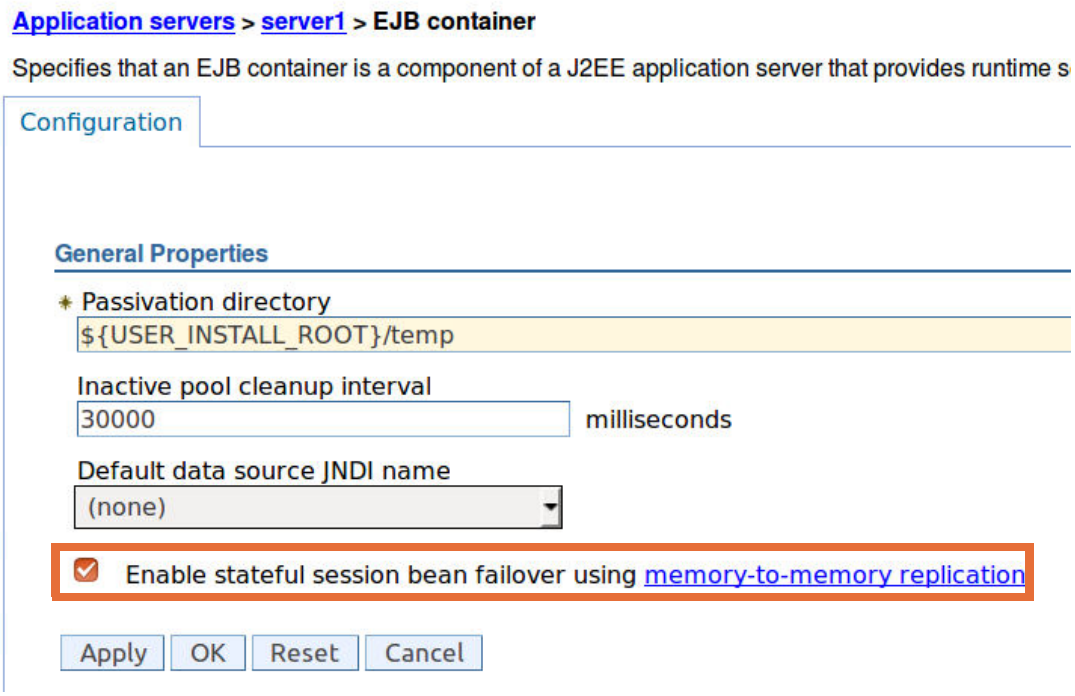


__ m. Click **OK**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ n. Now that you selected the replication domain, you can see that the check box for **Enable stateful session bean failover** is selected. Click **OK**.



__ o. Save the changes.

__ p. Repeat the previous steps for the other server.

Section 8: Testing the application for session failover

In this section, you test the failover of the session information. Although the PlantsByWebSphere application was not designed to fail over to the shopping cart, you can store content in the session object. After that is done, you stop the application server that is holding session information to demonstrate that the information does indeed fail over to the other cluster member.

__ 1. Start the cluster.

__ a. Click **Servers > Clusters > WebSphere application server clusters**.

__ b. Select the **PlantsCluster** and click **Start**. Wait for all cluster members to start.

__ 2. Continue shopping in the PlantsByWebSphere application.

For the remaining steps, use the Chrome browser. By using a different browser for Plants than for the administrative console, you can be assured that the cookies do not interfere with each other.

__ a. Open a Chrome browser window and access the PlantsByWebSphere application by entering the following URL:

`http://washost/PlantsByWebSphere`

__ b. Click **Home**.

__ c. Click **Help** and proceed to the View Server Info page.

__ d. Take note of the server name in the **Process** field: _____

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

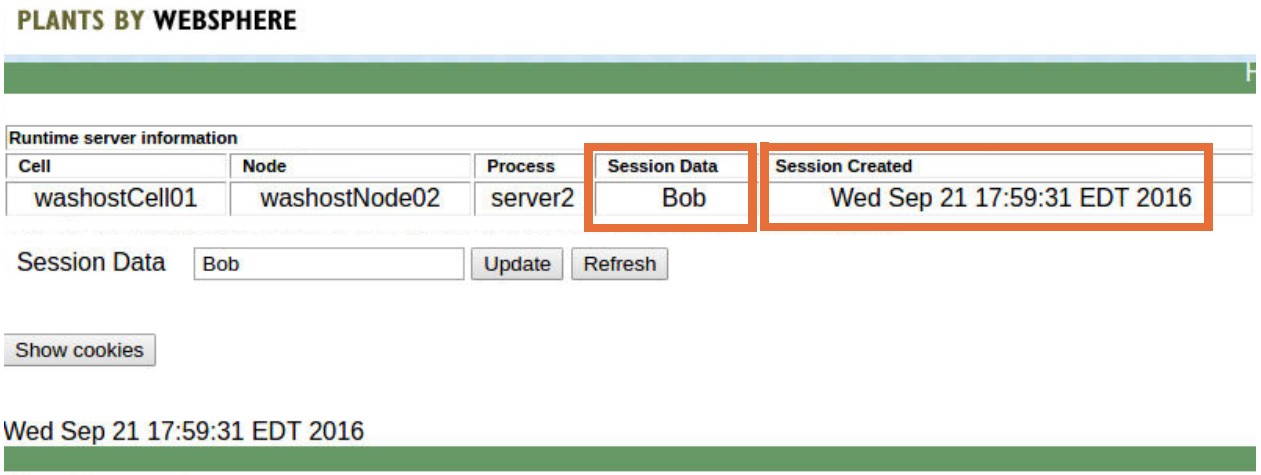
__ e. Click **Home** and browse through the store. Add a couple of items to your shopping cart.

__ f. Return to the View Server Info page and confirm that the server name is the same.

__ 3. Add some content to the HTTP session object. Now, you have objects in the shopping cart and know to which server you have affinity.

__ a. From the View Server Info page, enter a name in the **Session Data** field and click **Update**.

__ b. Notice that not only does the data show in the Session Data field, but the time that the session object was created is shown in the **Session Created** field.



__ c. Take note of the time that is shown in the **Session Created** field: _____

__ d. Click **HOME** and add several items to your shopping cart.

__ e. Return to the View Server Info page (through the Help page) and notice that the session data and time for session that are created are not changed.

__ 4. Simulate a server failure.

__ a. Return the administrative console and stop the server that hosted your session.

__ b. Wait for the server to stop completely.

__ 5. Verify the session data failover.

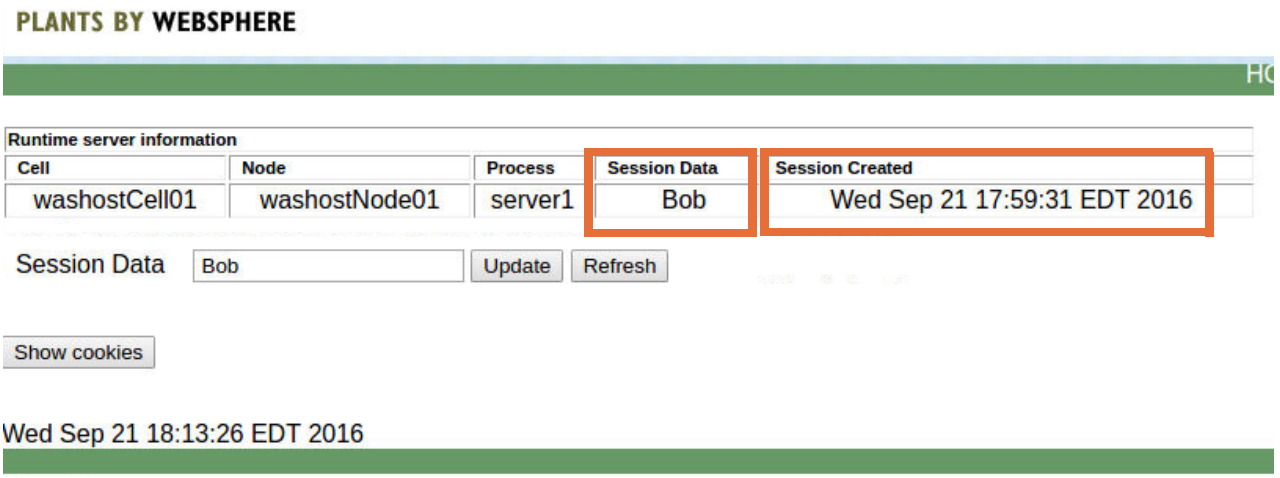
__ a. Return to the browser window that you used for accessing the PlantsByWebSphere application.

__ b. Click **Home > Shopping Cart**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ c. Return to the View Server Info page. Notice that the server name is changed to the other cluster member. Also, notice that the **Session Data** and **Session Created** fields stayed the same.



Information

You can see that the session information failed over from the server that was holding affinity for the session to the other cluster member. All subsequent requests for this session are routed to the running cluster member.

End of exercise

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise review and wrap-up

The first part of the exercise looked at creating a cluster of two servers, each in its own node.

Next, the applications are configured to run on the cluster by assigning the modules of the applications to the web server and the cluster.

Finally, the application was thoroughly tested in the clustered environment, and failover scenarios were created by stopping one of the servers.

To make failover work when session data is involved, the Data Replication Service used memory-to-memory replication.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise 4. Configuring SSL for WebSphere

Estimated time

01:00

Overview

This exercise explores some of the features and configurations within the WebSphere SSL environment. You create a profile and then examine the certificates that are created specifically for the node within the profile. You explore some of the administration tasks that are required for managing the certificates within a cell. Finally, in an optional part of the exercise, you configure IBM HTTP Server to use a self-signed certificate to secure the communications between a browser and the web server.

Objectives

After completing this exercise, you should be able to:

- Define the certificate life span of a profile
- Use the administrative console to find and view certificates within the cell
- Configure and run the certificate expiration service
- Propagate the generated plug-in keystore out to the plug-in
- Create a keystore for a web server
- Generate a self-signed key
- Configure IBM HTTP Server to load and use HTTPS

Introduction

WebSphere Application Server V9 configures and manages many of the SSL configurations that are required to secure communication within a cell. But it is important to understand how this infrastructure works so that it can be maintained correctly. This exercise creates a profile and examines the certificates and keystores that are created for that new profile or node. The exercise then looks at the interfaces that deal with expiring certificates. It also examines the log files and security reports that are helpful in tracking when certificates are about to expire.

Another important step in managing a WebSphere environment is propagating keystores out to the web server plug-in. This lab goes through the steps to view the plug-in generated keystore, followed by propagating them out to the web server.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

As an optional part of the lab, the last section configures IBM HTTP Server for inbound SSL. iKeyman is used to generate a new keystore and self-signed certificate. IBM HTTP Server is then configured to support HTTPS communications by using the newly created certificate.

Requirements

This lab requires a computer that is properly set up with WebSphere Application Server V9 installed. This exercise assumes that the federated cell exists and that PlantsByWebSphere is installed on server1 (on node washostNode01).

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise instructions

Preface

Important

The labs use two variables to define various installation paths. On Linux, the variable definitions are as follows:

<was_root>: /opt/IBM/WebSphere/AppServer
<profile_root>: /opt/IBM/WebSphere/AppServer/profiles

Section 1: Resetting the WebSphere environment

Note

If your WebSphere environment must be reset for any reason, see **Appendix A** for instructions to correctly reset the environment.

Section 2: Creating a backup

This exercise changes the existing environment. If the change is done incorrectly, it can cause problems for the rest of the exercises, so creating a backup is a good idea.

__ 1. Create a backup for the deployment manager.

__ a. In a command window, navigate to the `/opt/IBM/WebSphere/AppServer/profiles/Dmgr/bin` directory.

__ b. If the deployment manager process is running, stop the process by entering the following command:

```
./stopManager.sh -username wasadmin -password web1sphere
```

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ c. After the deployment manager is stopped, enter the following command to back up the entire profile:

```
./manageprofiles.sh -backupProfile -profileName Dmgr -backupFile
/opt/labfiles/backups/pre-SSL.zip
```

Section 3: Creating a profile

To better understand the various pieces of SSL within the WebSphere Application Server environment, a custom profile is created.

__ 1. Restart the deployment manager.

__ a. From a terminal window, in the `bin` directory for the deployment manager, enter the following command:

```
./startManager.sh
```

__ 2. Create a custom profile that is named SSL and federate it to the deployment manager.

__ a. Start the Profile management tool by typing the following command in a terminal window:

```
/opt/IBM/WebSphere/AppServer/bin/ProfileManagement/pmt.sh
```

__ b. The WebSphere Customization Toolbox window starts. Click **Create** on the right to create a profile.

__ c. Select the **Custom profile** option and click **Next**.

__ d. On the Profile Creation Options page, select **Advanced profile creation** and click **Next**.

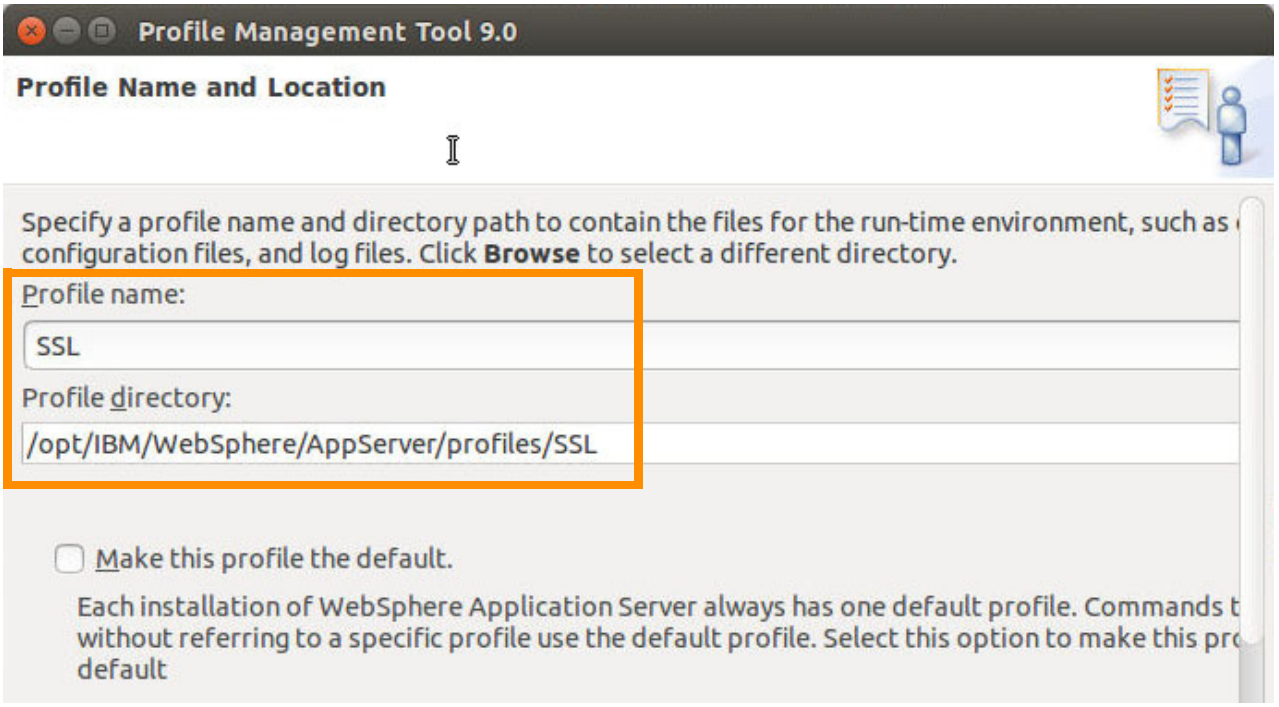
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ e. For the profile name and location, enter the following information:

- **Profile name**: `SSL`
- **Profile directory**: `/opt/IBM/WebSphere/AppServer/profiles/SSL`

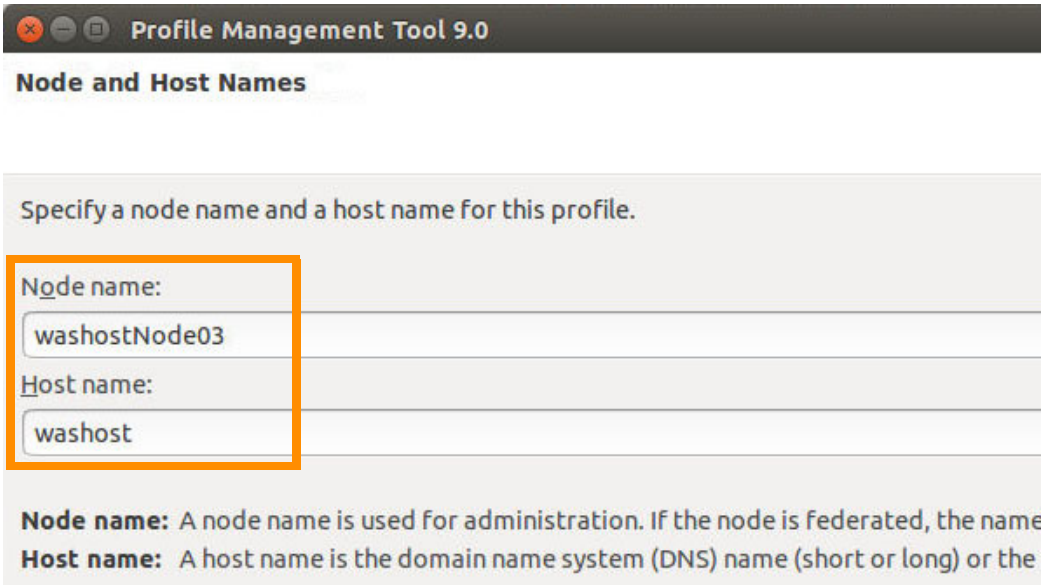
Click **Next**.



__ f. On the Node and Host Names page, enter the following values:

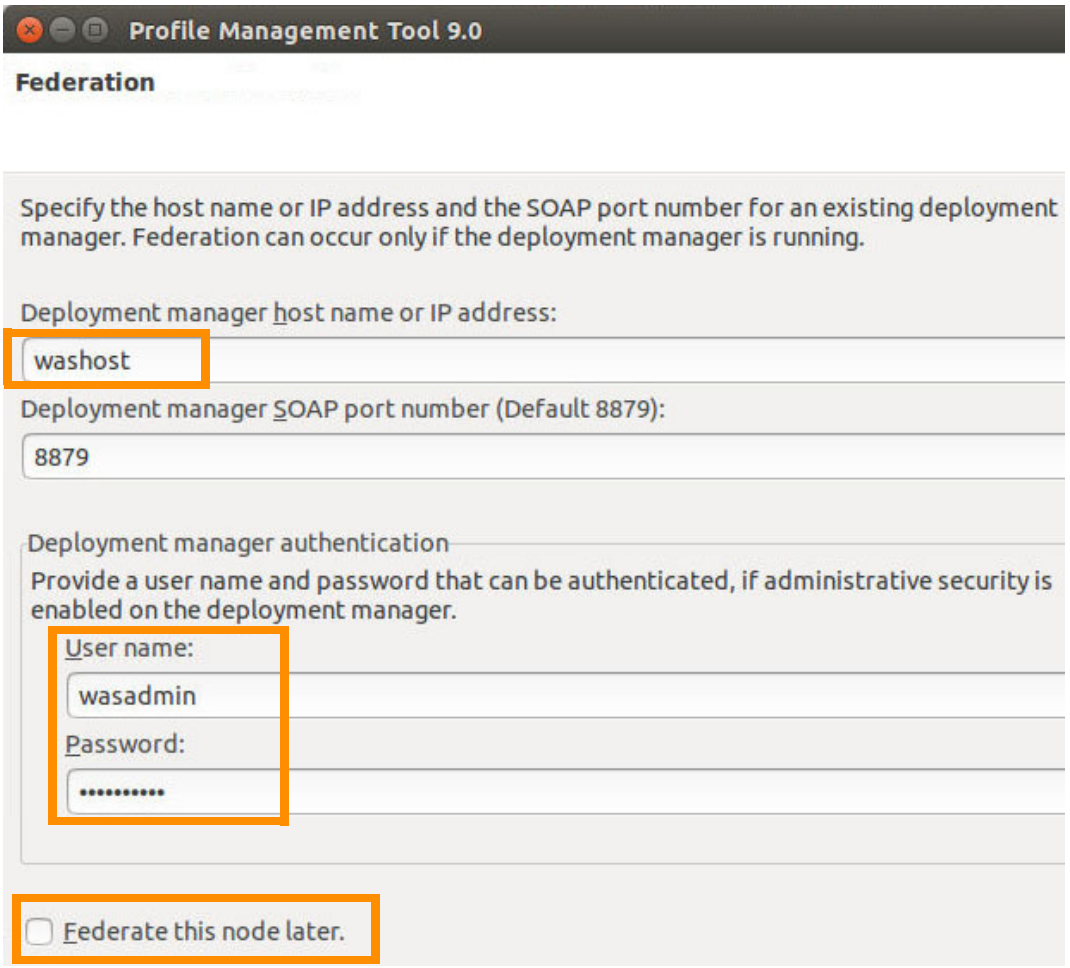
- **Node name**: `washostNode03`
- **Host name**: `washost`

Click **Next**.



© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ g. On the Federation page, enter `washost` for the deployment manager host name. The default SOAP port (8879) is shown. Enter `wasadmin` for the security user name and `web1sphere` for the password. Be sure that the **Federate this node later** check box is not selected. The node is automatically federated to the cell during creation.



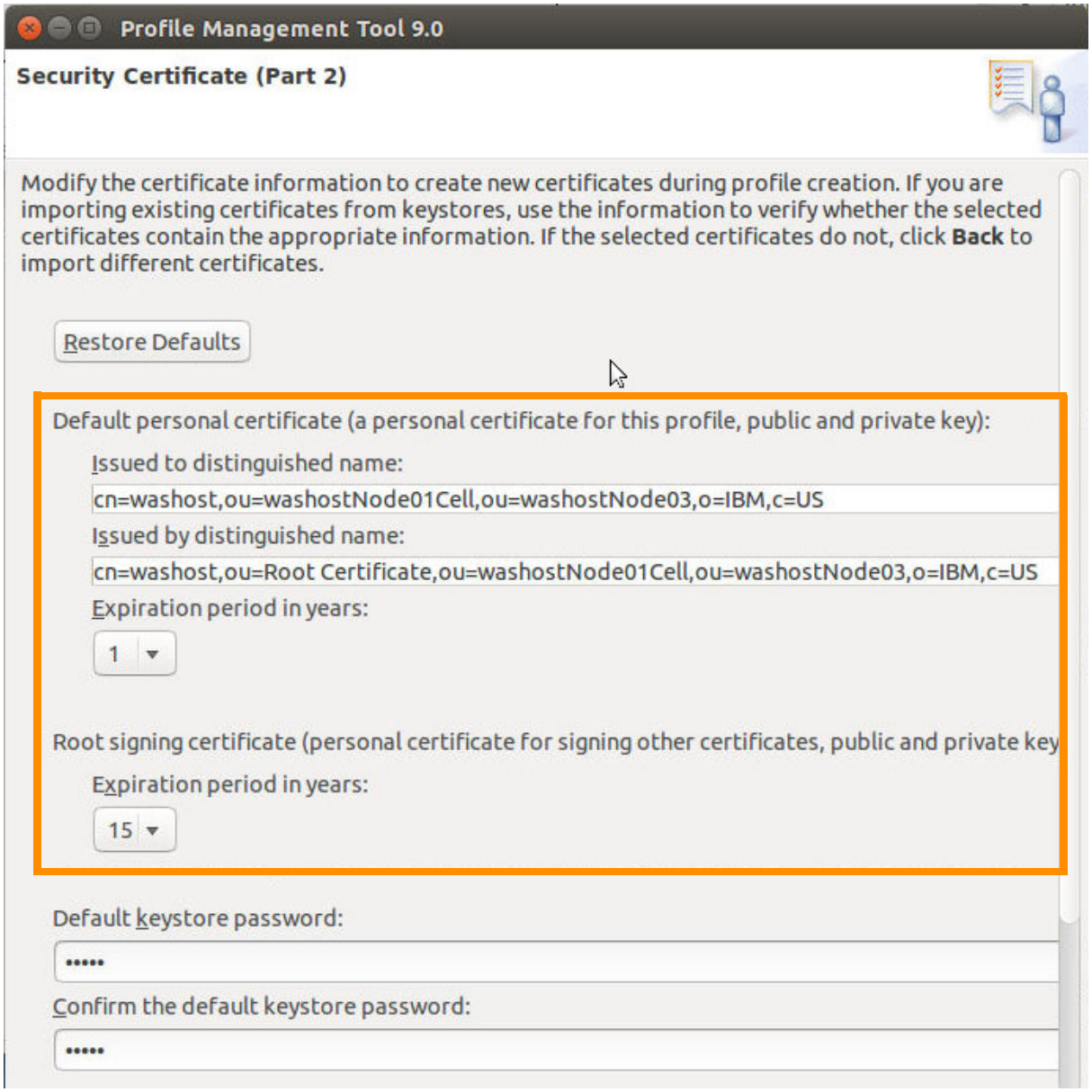
__ h. Click **Next**.

__ i. On the next page, accept the defaults for creating the default personal certificate and a new root signing certificate. Click **Next**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ j. On the next screen, which specifies the node certificate information, accept the defaults and click **Next**. Make sure that you read the information block as it explains the importance of these entries and how they relate to SSL.



Information

Unlike in older versions of WebSphere Application Server, each node (or profile) no longer gets a single self-signed certificate. Instead, as of WebSphere Application Server V7, two certificates are created. The first one is the node personal certificate that is used by default for secured communication with the node and any application servers on that node. This personal certificate has a default life span of one year and it is not a self-signed certificate. Instead, the second

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

certificate that is specified on this page signed it. The second certificate is the root certificate. This relationship is called a chained certificate.

Unlike the node personal certificate, the root certificate has a default life span of 15 years. This longer life span helps when the personal certificate is renewed as it gets close to its expiration date. Since the same root certificate signed all the personal certificates, any processes that must communicate securely already have access to a valid copy of the node root signer certificate. This condition is true regardless of whether the personal certificates are updated.

This model helps solve some of the certificate propagation problems since updating personal certificates no longer requires any certificate propagation to occur.

Signer certificate propagation within a cell is accomplished through standard node synchronization. All of the node signer certificates are included in the cell default truststore file, which is synchronized throughout the cell. However, propagation to the web server plug-in is tricky.

For the plug-in to be able to communicate securely with the application servers, they need access to the appropriate signer certificates. The root signer certificates are made available to the plug-in in their generated key rings. Since the root certificates are now being used as the signers, updating expiring personal certificates is no longer a problem.

The keystore password default is: `WebAS`

__ k. Accept the default ports on the next page. Click **Next**.

__ l. On the summary page, click **Create**.

__ m. The profile creation is now complete; clear the check box for **Launch the First steps console** and click **Finish**.

__ n. Close the Profile Management Tool.

__ 3. Verify the new node in the administrative console.

__ a. Open an instance of the administrative console and use `wasadmin` with the password `web1sphere` to log in to the deployment manager.

__ b. Click **System administration > Nodes** and verify that the new node, washostNode03, now exists.

__ c. Stop the node agent for node washostNode03. Since it is not necessary for the node agent to be running for this exercise, select the node and click **Stop** (which helps free up some of the system resources).

Section 4: Examining the node certificates

This new node has a couple of certificates that are associated with it. This section of the exercise uses the administrative console to examine them.

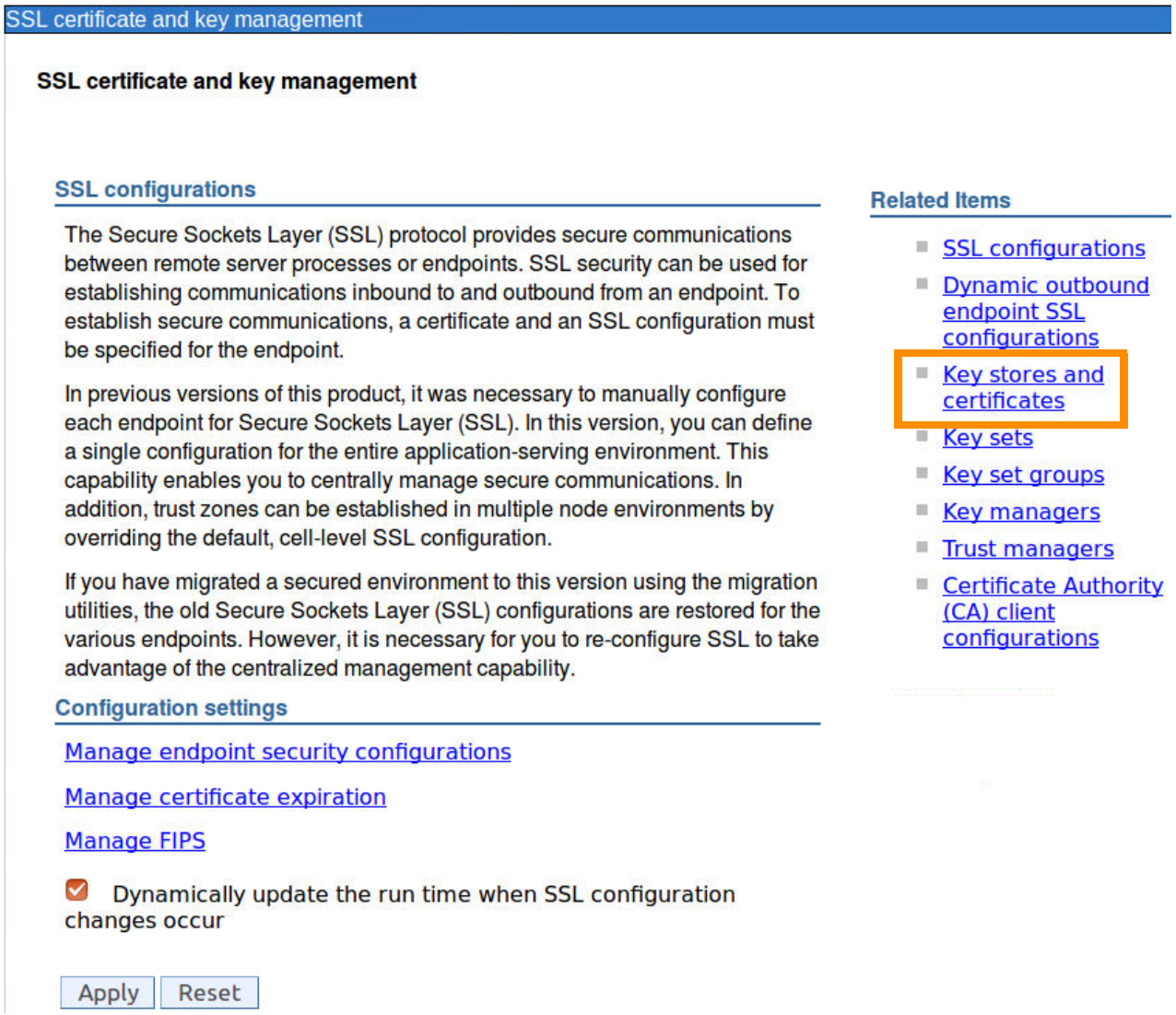
__ 1. Examine the node certificates.

__ a. In the administrative console, click **Security > SSL certificate and key management**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

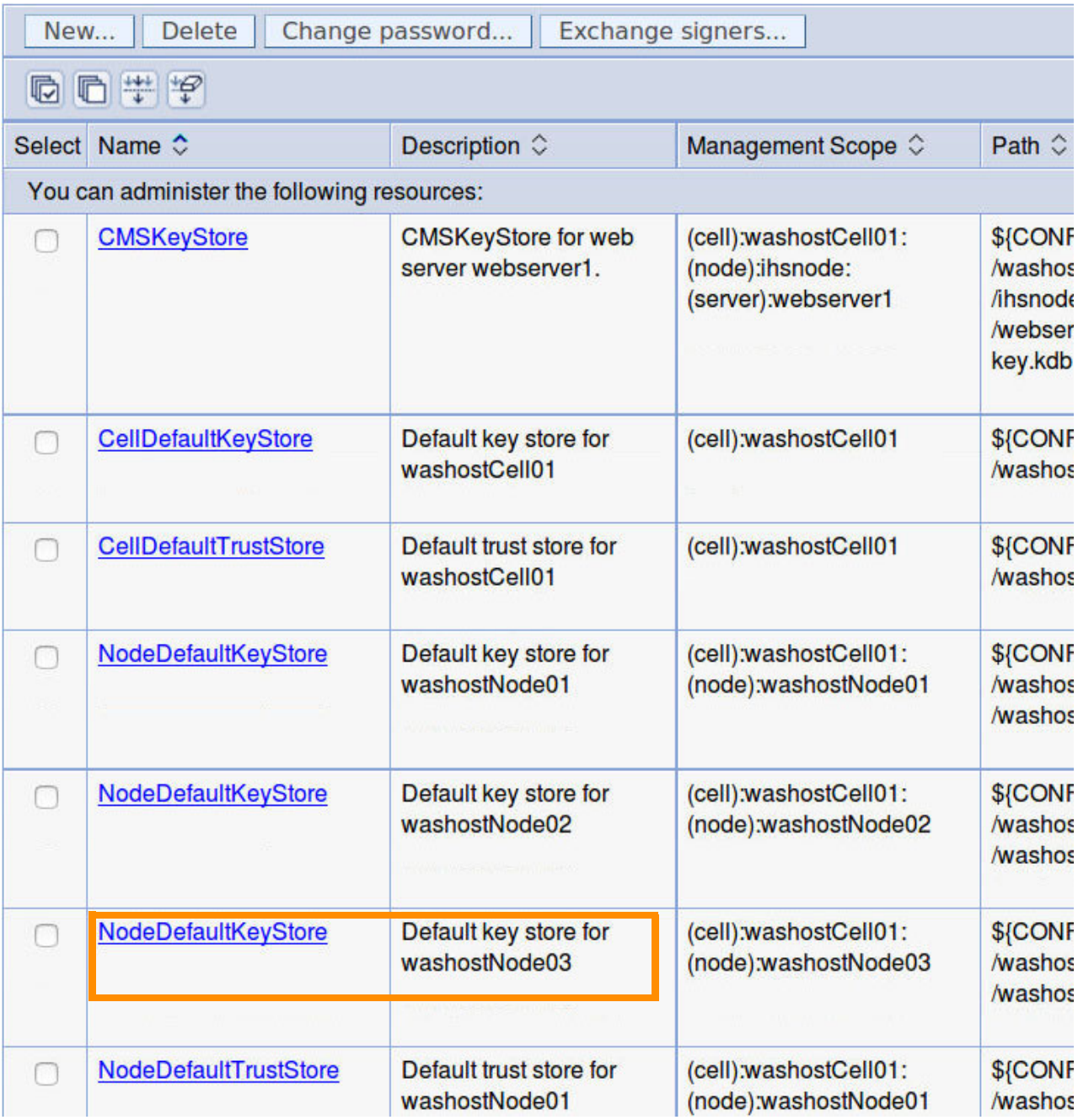
__ b. On the right side, under Related Items, click **Key stores and certificates**.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

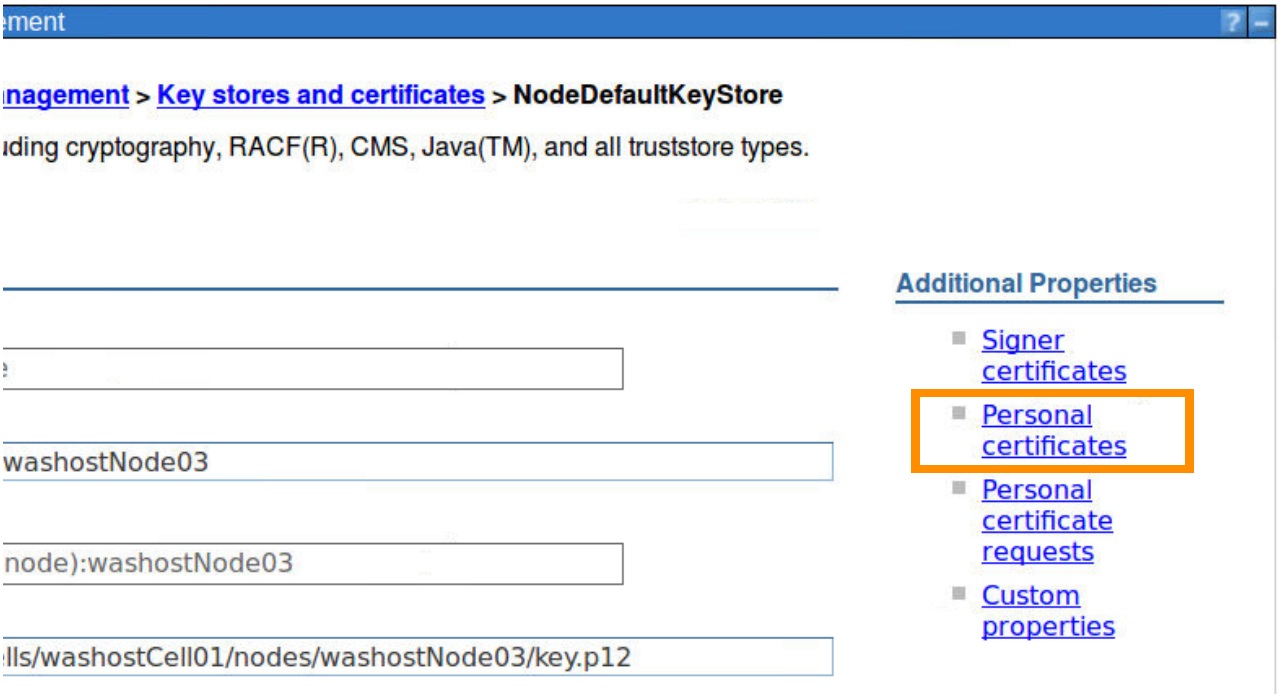
__ c. This page shows a list of the keystores and trust files for the cell. Click **NodeDefaultKeyStore** for the node that was created (`washostNode03`) earlier in this exercise.



© Copyright IBM Corp. 2016

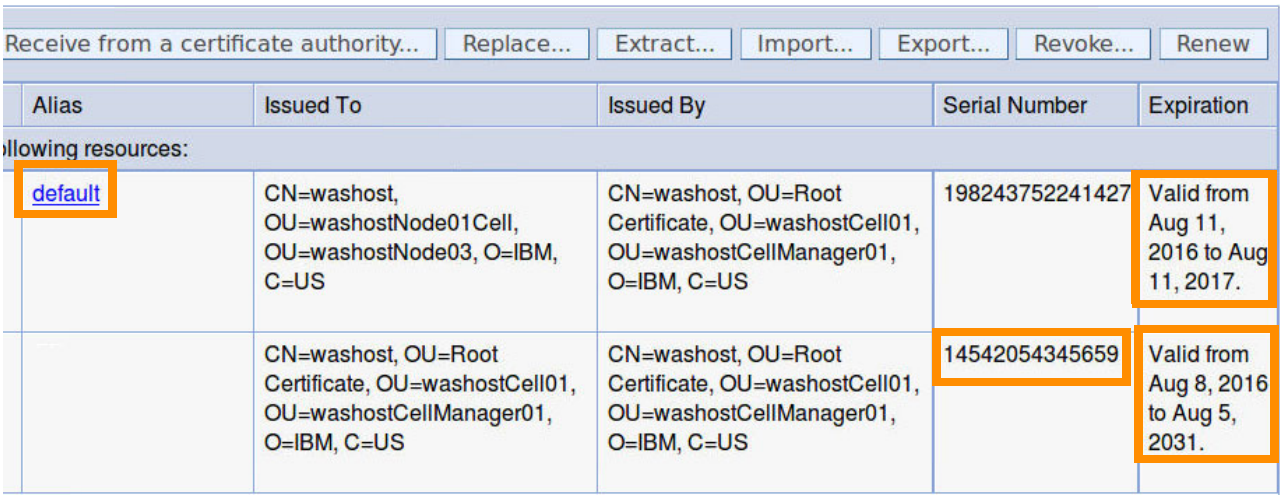
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ d. The next page shows the basic information for the node keystore. On the right, under Additional Properties, click **Personal certificates**.



__ e. This page shows the keystore entries for the node that was created. Notice the two chained certificates. The first, whose alias is default, is the personal certificate for the new node. Notice that it is set to expire in one year.

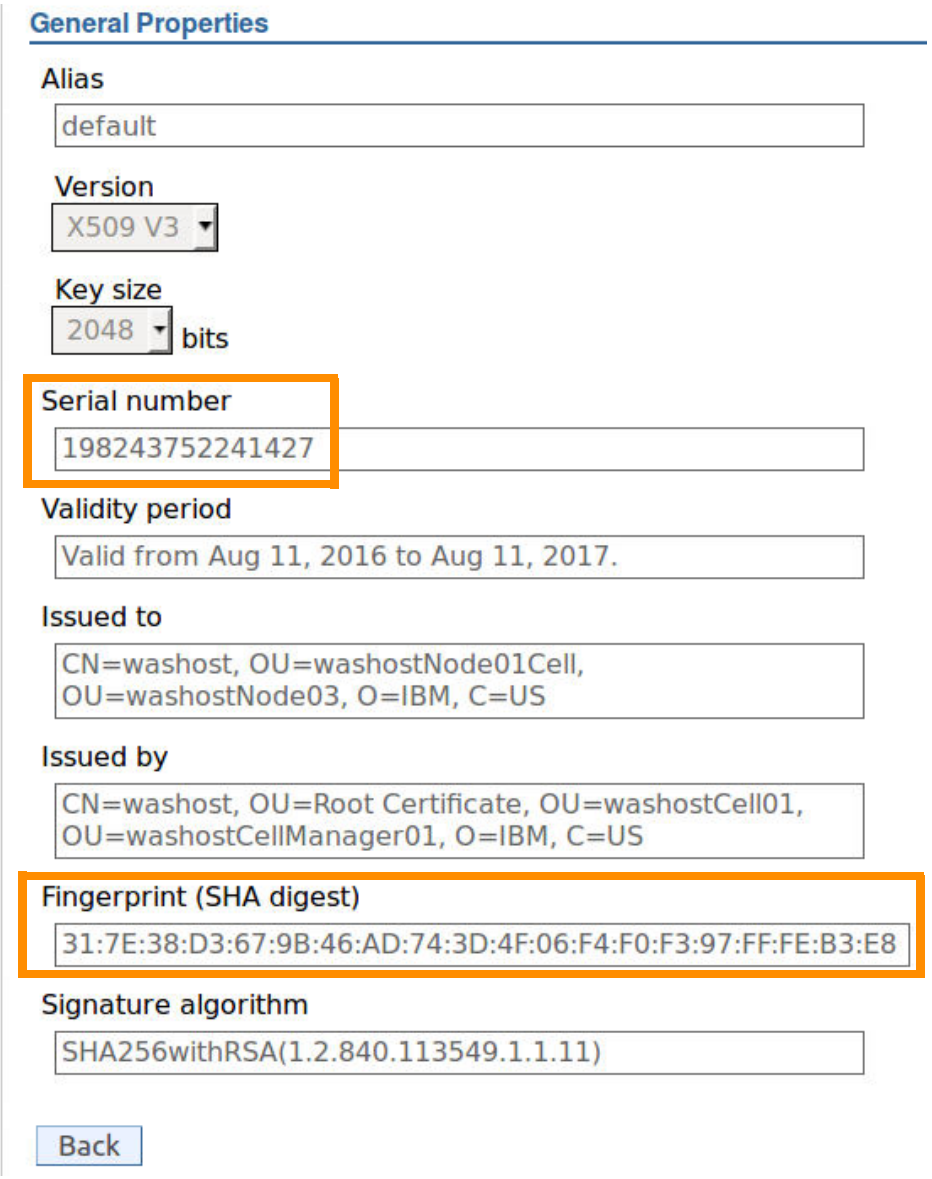
The second is the root certificate for the new node, which expires in 15 years. Note the serial number for the root certificate (Serial #:_____) and expiration date (date: _____).



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ f. Tracking the serial numbers can be helpful. In other parts of the administrative console, the representation of the certificates can change. To tell which certificate is which, knowing the serial number is helpful. Click the alias **default** for further information. Also, take note of the fingerprint. Usually knowing just the last couple of bits is sufficient: _____ (B3:E8**)**



__ g. Using the breadcrumb trail, return to the **NodeDefaultKeyStore**.

__ h. Click **Signer certificates**. Notice that none are listed (signers are stored in the truststore files while personal certificates are stored in keystores).

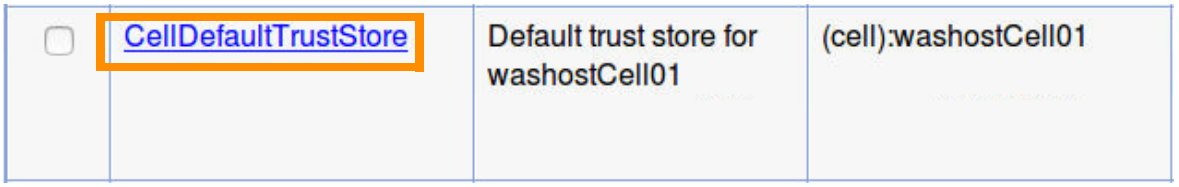
__ 2. Examine the cell signer certificates.

__ a. Using the breadcrumb trail, return to the **Keystores and certificates**.

© Copyright IBM Corp. 2016

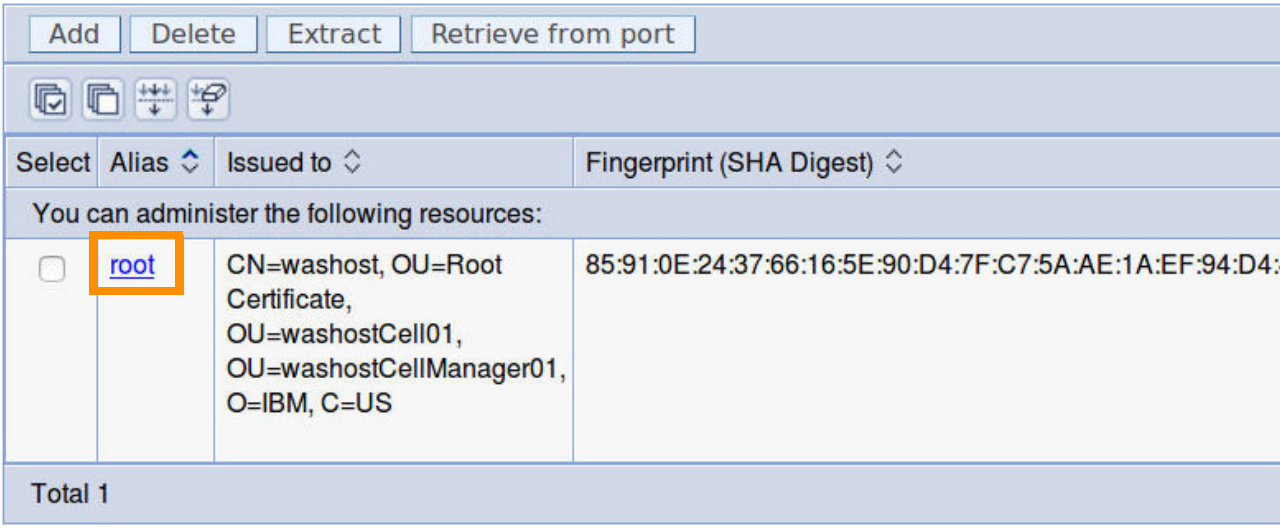
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ b. Click **CellDefaultTrustStore**. The file includes all of the signer certificates within the cell.



__ c. On the right, under Additional Properties, click **Signer certificates**.

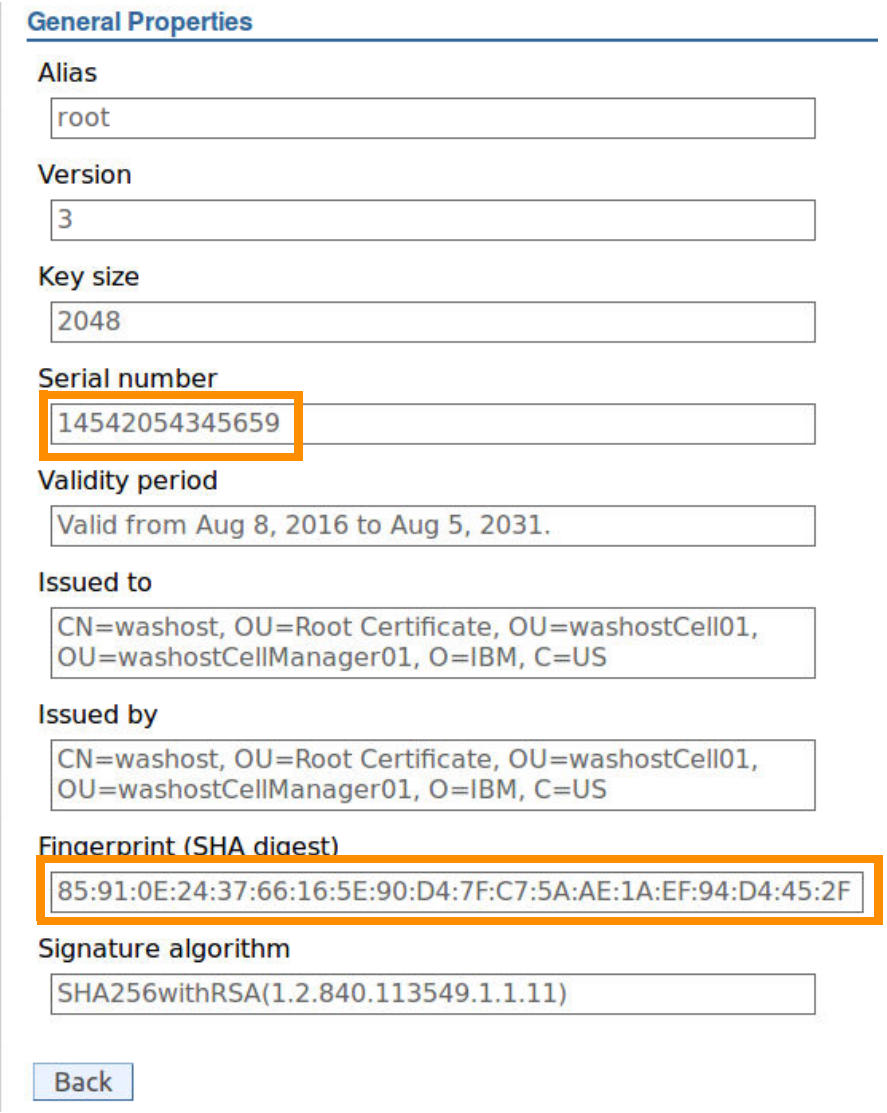
__ d. Notice a root signer certificate in the cell default truststore. Specifically, this certificate is the cell root signer certificate (not the personal certificate), and is the signer for all of the node certificates in the cell. Notice that it has a 15-year life span.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ e. Click **root** for the details.



__ f. Notice that the serial number matches the serial number from the previous step where you noted the information for the root certificate. This match verifies the fact that the signer certificate for the root certificate is indeed added to the cell default truststore. And since the cell default truststore is synchronized to all nodes within a cell, all nodes and all application servers have access to the cell root signer certificate.

The plug-in needs the cell root signer certificate so that it can communicate securely with the application servers. That subject is covered later in this exercise.

Take note of the serial number and fingerprint for the root certificate: _____ (5659). Usually knowing just the last couple of bits is sufficient: _____ (45:2F).

Section 5: Examining certificate expiration and updating

Since the personal certificates have a life span of only one year, administrators must be aware that these certificates expire. Fortunately, WebSphere has a built-in mechanism to automatically renew

© Copyright IBM Corp. 2016

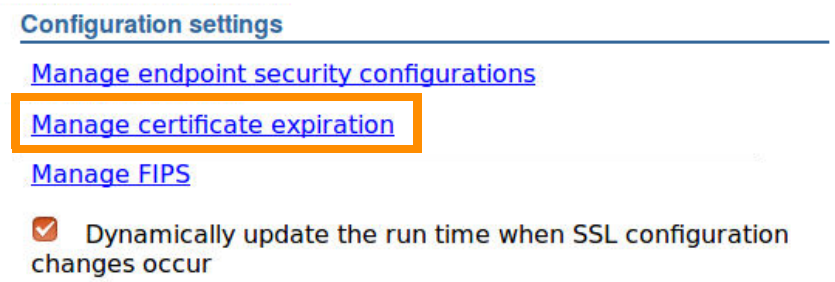
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

these certificates when they are about to expire. And, since the signer certificates remain the same, it is not necessary to propagate anything new to the remote nodes or plug-in.

__ 1. Examine the certificate expiration settings.

__ a. In the administrative console, click **Security > SSL certificate and key management**.

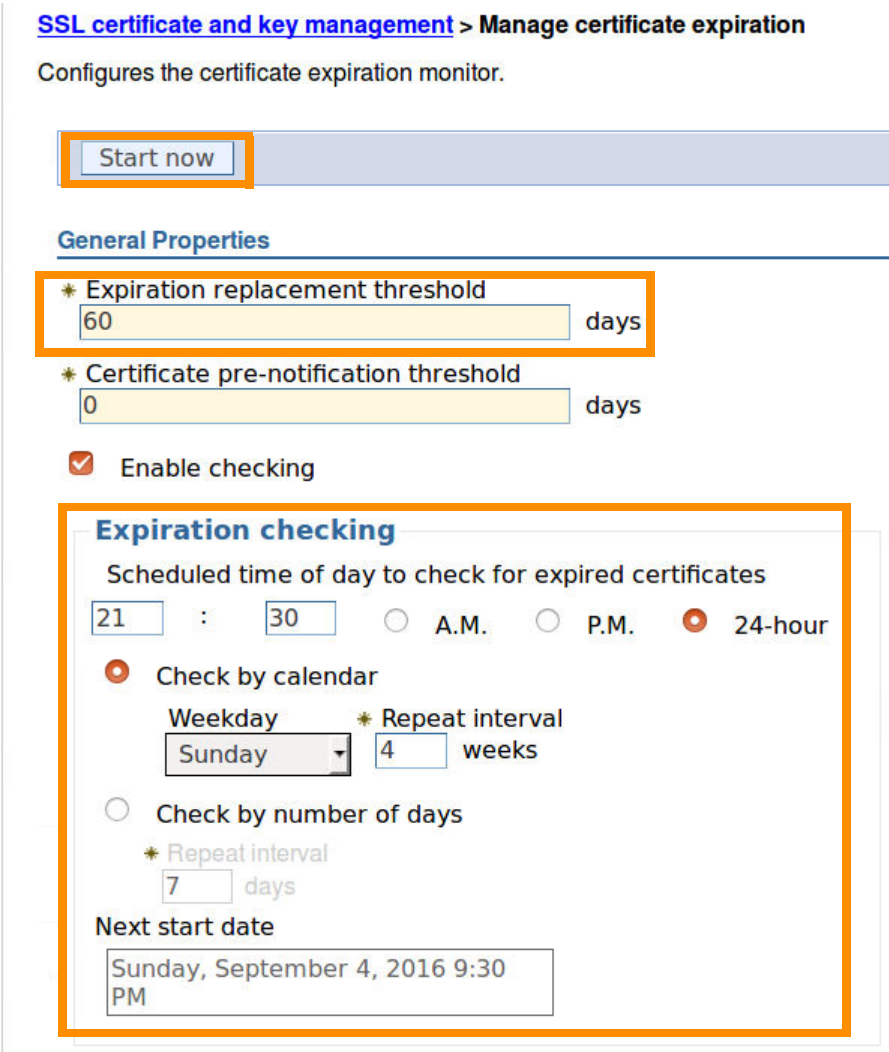
__ b. Under Configuration settings, click **Manage certificate expiration**.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ c. Built into WebSphere is a service that runs through the list of all certificates and replaces those certificates that are about to expire. This screen configures when that service is run. It can be run immediately by clicking **Start now**, or it can be scheduled. The default is to run on every fourth Sunday at 21:30. This service can be turned off by clearing the **Enable** check box. It is also possible to run the checking service but to not automatically replace the existing certificates or to not delete the replaced expiring certificates.



By default, the expiration notifications are written to the log file. More notifications, including email, can be configured by clicking **Notifications** under Related Items.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

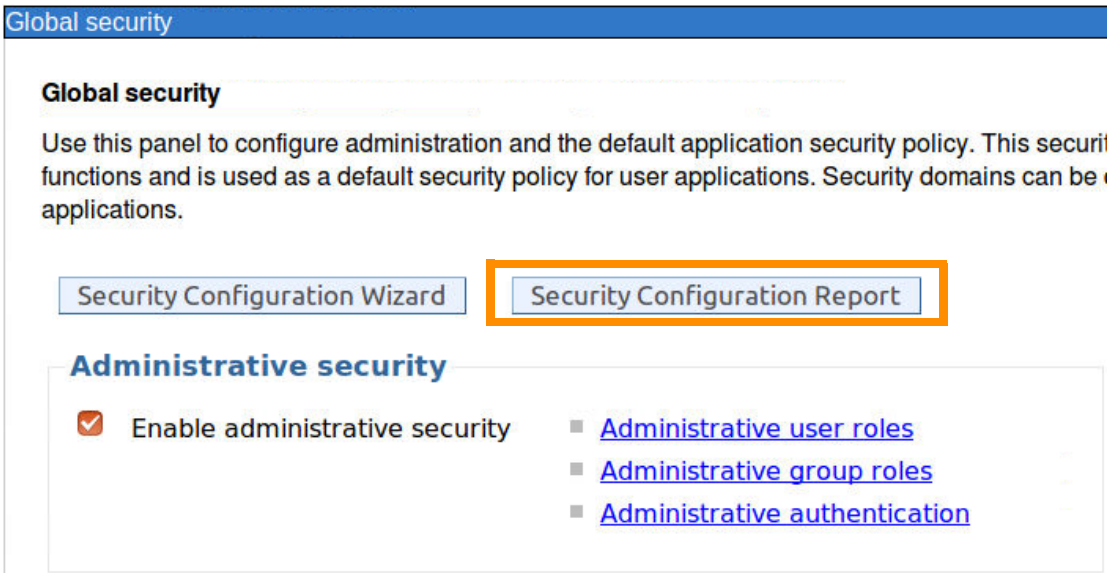
__ d. Run the expiration notification service now by clicking **Start now**. Using a text editor such as gedit, open the `SystemOut.log` file for the deployment manager. Near the end of the file, an entry that starts with “Expiration Monitor” looks like the following screen capture:

__ e. Since the cell is newly created, no certificates need replacing. Close the editor.

__ 2. Use the security report to view the list of all the certificates and their expiration dates.

__ a. In the administrative console, click **Security > Global security**.

__ b. Click **Security Configuration Report**.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ c. A new browser window shows the HTML report. Scroll to the bottom of the report and find the Certificate Management section.

Certificate Management	default (CellDefaultKeyStore)	Valid from Aug 8, 2016 t
Certificate Management	root (CellDefaultTrustStore)	Valid from Aug 8, 2016 t
Certificate Management	default (CellRSATokenKeyStore)	Valid from Aug 8, 2016 t
Certificate Management	root (CellRSATokenTrustStore)	Valid from Aug 8, 2016 t
Certificate Management	root (DmgrDefaultRootStore)	Valid from Aug 8, 2016 t
Certificate Management	dummyclientsigner (DmgrDefaultDeletedStore)	Valid from Jul 30, 2003 t
Certificate Management	dummyserversigner (DmgrDefaultDeletedStore)	Valid from Jul 30, 2003 t
Certificate Management	root (DmgrDefaultSignersStore)	Valid from Aug 8, 2016 t
Certificate Management	root (DmgrRSATokenRootStore)	Valid from Aug 8, 2016 t
Certificate Management	default (NodeDefaultKeyStore)	Valid from Aug 8, 2016 t
Certificate Management	default (NodeDefaultTrustStore)	Valid from Aug 8, 2016 t
Certificate Management	root (NodeDefaultTrustStore)	Valid from Aug 8, 2016 t
Certificate Management	default (NodeDefaultKeyStore)	Valid from Aug 8, 2016 t
Certificate Management	default (NodeDefaultTrustStore)	Valid from Aug 8, 2016 t
Certificate Management	root (NodeDefaultTrustStore)	Valid from Aug 8, 2016 t
Certificate Management	default (CMSKeyStore)	Valid from Aug 9, 2016 t
Certificate Management	CN=washost, OU=Root Certificate, OU=washostCell01, OU=washostCellManager01, O=IBM, C=US (CMSKeyStore)	Valid from Aug 8, 2016 t
Certificate Management	default (NodeDefaultKeyStore)	Valid from Aug 11, 2016
Certificate Management	default (NodeDefaultTrustStore)	Valid from Aug 8, 2016 t
Certificate Management	root (NodeDefaultTrustStore)	Valid from Aug 11, 2016

__ d. Notice the list of the certificates and the expiration dates. This report can be a helpful tool for administrators in dealing with their certificate management.

__ e. Close the security configuration report window.

Section 6: Propagating the plug-in key ring

Not only are the processes within cells (deployment managers, node agents, and application servers) required to have certificates and know about other signer certificates, so are the web server plug-ins. To secure the communication between the web server plug-ins and the application servers, the plug-ins and application servers must be able to negotiate an SSL session. They must have personal certificates (by default the application servers use the node personal certificate) and have access to the other signer certificates.

WebSphere is able to make sure that all of the required certificates are available to the web server plug-in by creating the plug-in keystores from within WebSphere. By doing so, WebSphere can make sure that not only does the plug-in have a valid personal certificate, but it also has the necessary cell root signer certificate. At the same time, WebSphere can ensure that the plug-in signer certificate is also available in the cell truststore.

The real problem with this approach is that after WebSphere generates the plug-in keystore, it still must be propagated to the host that is running the web server. The propagation process of plug-in keystores is similar to the propagation of the `plugin-cfg.xml` file. It is usually done manually, but in some cases can be configured to be done automatically (usually not desirable).

__ 1. View the contents of the plug-in keystore.

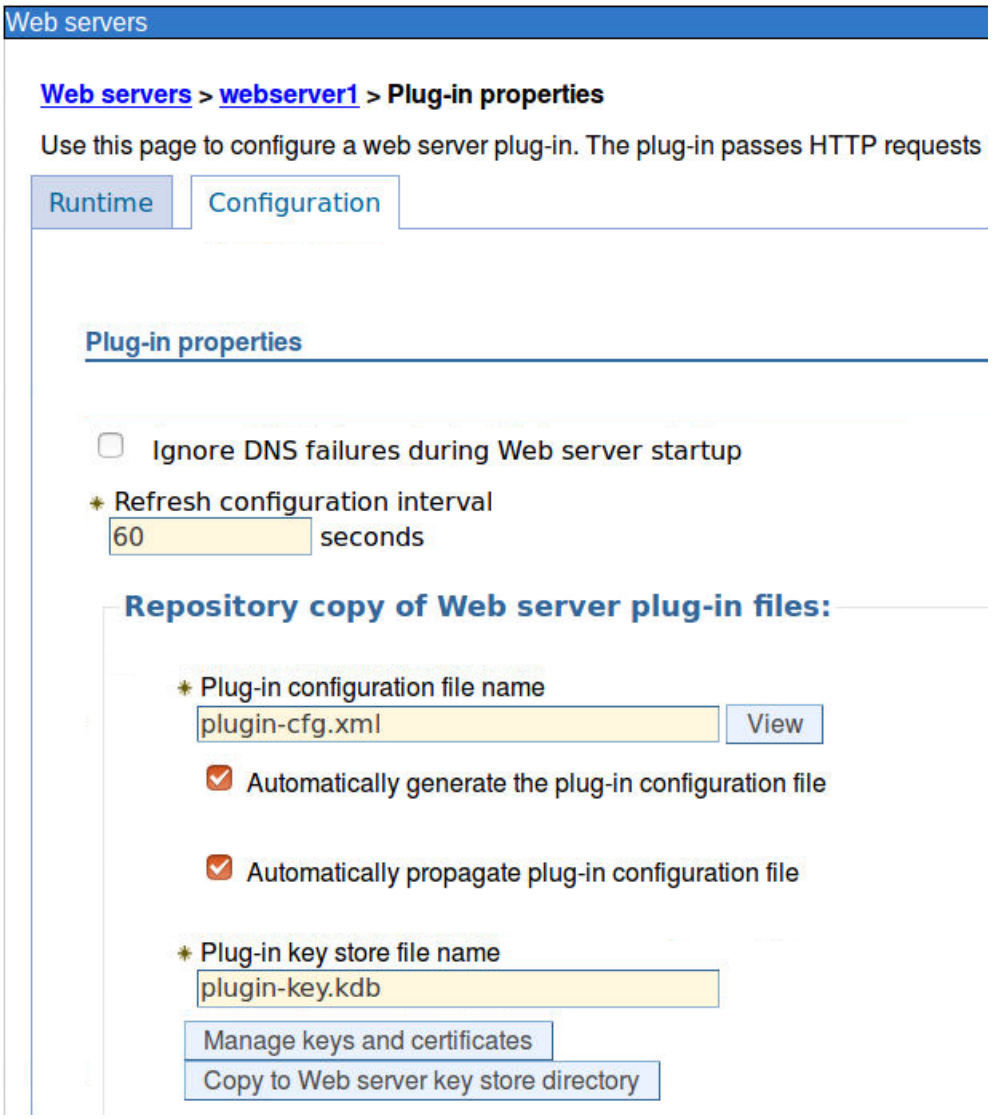
__ a. In the administrative console, click **Servers > Server Types > Web servers**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ b. Click your web server link, **webserver1**.

__ c. Under Additional Properties, click **Plug-in properties**.



__ d. Notice the plug-in key store file name. This file can be found within the configuration structure of the deployment manager under the `ihsnode` directory. More specifically, the directory would be:

`/opt/IBM/WebSphere/AppServer/profiles/Dmgr/config/cells/<cell-name>/nodes/<node-name>/servers/webserver1/nodes/ihsnode/servers/<web-server>`

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

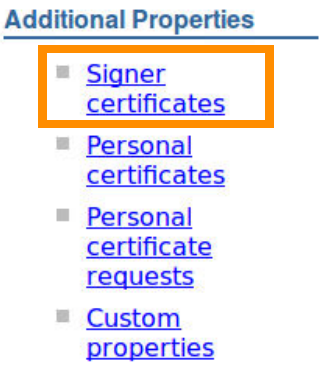
The directory is also the same directory where the web server-specific version of the `plugin-cfg.xml` file exists.

```
localuser@washost: /opt/IBM/WebSphere/AppServer/profiles/Dmgr/config/cells/washost
localuser@washost:/opt/IBM/WebSphere/AppServer/profiles/Dmgr/config/cells/washos
tCell01/nodes/ihsnode/servers/webserver1$ ls -la
total 40
drwxr-xr-x 2 localuser localuser  4096 Aug 10 10:46 .
drwxr-xr-x 3 localuser localuser  4096 Aug 10 10:45 ..
-rw-r--r-- 1 localuser localuser  4575 Aug 10 11:06 plugin-cfg.xml
-rw-r--r-- 1 localuser localuser 10088 Aug 10 10:45 plugin-key.kdb
-rw-r--r-- 1 localuser localuser   129 Aug 10 10:45 plugin-key.sth
-rw-r--r-- 1 localuser localuser  2438 Aug 10 10:45 server.xml
-rw-r--r-- 1 localuser localuser   777 Aug 10 10:45 variables.xml
localuser@washost:/opt/IBM/WebSphere/AppServer/profiles/Dmgr/config/cells/washos
tCell01/nodes/ihsnode/servers/webserver1$
```

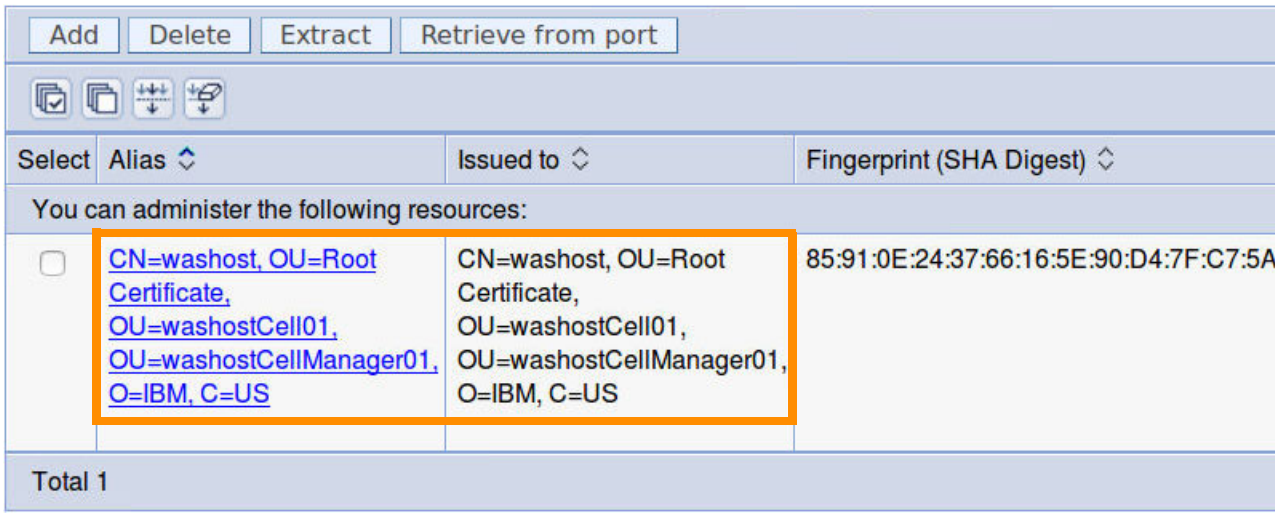
__ e. Take note of the date, time, and size of the file.

__ f. Next, examine the contents of this file. In the console, click **Manage keys and certificates**.

__ g. On the right, click **Signer certificates**.

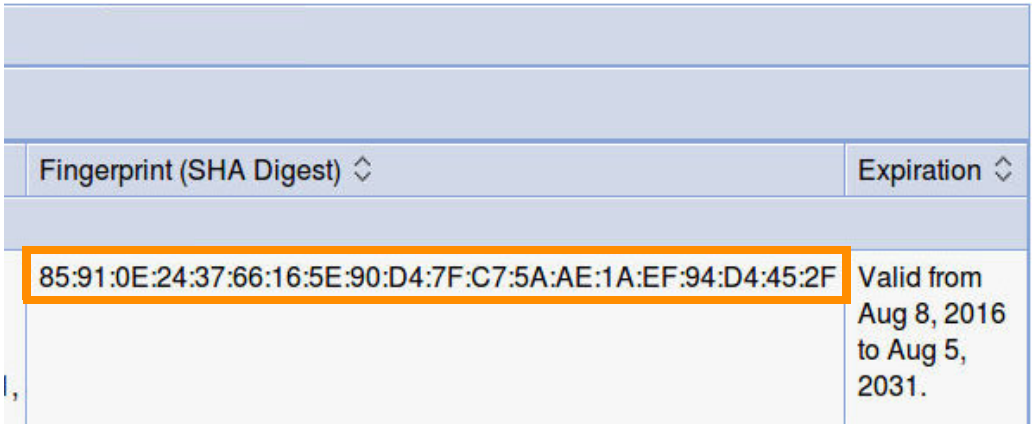


__ h. One signer certificate is available. Verify that the cell root signer certificate is among the list. Notice that the fingerprint matches what was seen previously in this exercise.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.



Information

Seeing the cell root signer certificate (in this case, the certificate that ends with a fingerprint of 01:66) validates the fact that WebSphere generated the keystore for the plug-in and included the cell root certificate signer.

__ 2. Propagate the plug-in keystore file. Although propagation is usually a manual process, in some cases it can be configured to be done automatically or through the administrative console.

__ a. Using the command window, navigate to the `/opt/IBM/WebSphere/Plugins/config/webserver1` directory.

__ b. Use the `ls -la` command to get a directory listing. Take note of the size and date-time stamp for the current `plugin-key.kdb`: _____

```
localuser@washost: /opt/IBM/WebSphere/Plugins/config/webserver1
localuser@washost:/opt/IBM/WebSphere/Plugins/config/webserver1$ ls -la
total 144
drwxrwxr-x 2 root      root        4096 Aug 15 05:14 .
drwxr-xr-x 5 localuser localuser   4096 Aug 15 05:14 ..
-rw-rw-r-- 1 root      ihs        15647 Aug 15 05:14 plugin-cfg.xml
-rw-rw-r-- 1 root      ihs       110080 Aug 15 05:14 plugin-key.kdb
-rw-rw-r-- 1 root      ihs           80 Aug 15 05:14 plugin-key.rdb
-rw-rw-r-- 1 root      ihs          129 Aug 15 05:14 plugin-key.sth
-rw-r--r-- 1 root      root         594 Aug 15 05:14 webserver1.responseFile
localuser@washost:/opt/IBM/WebSphere/Plugins/config/webserver1$
```

Information

The most common approaches for `plugin-cfg.xml` and key ring propagation is to move the files manually or create a custom automated mechanism. IHS provides a means of propagation through the IHS admin service, but that is only available through IHS and not any of the other supported web servers.

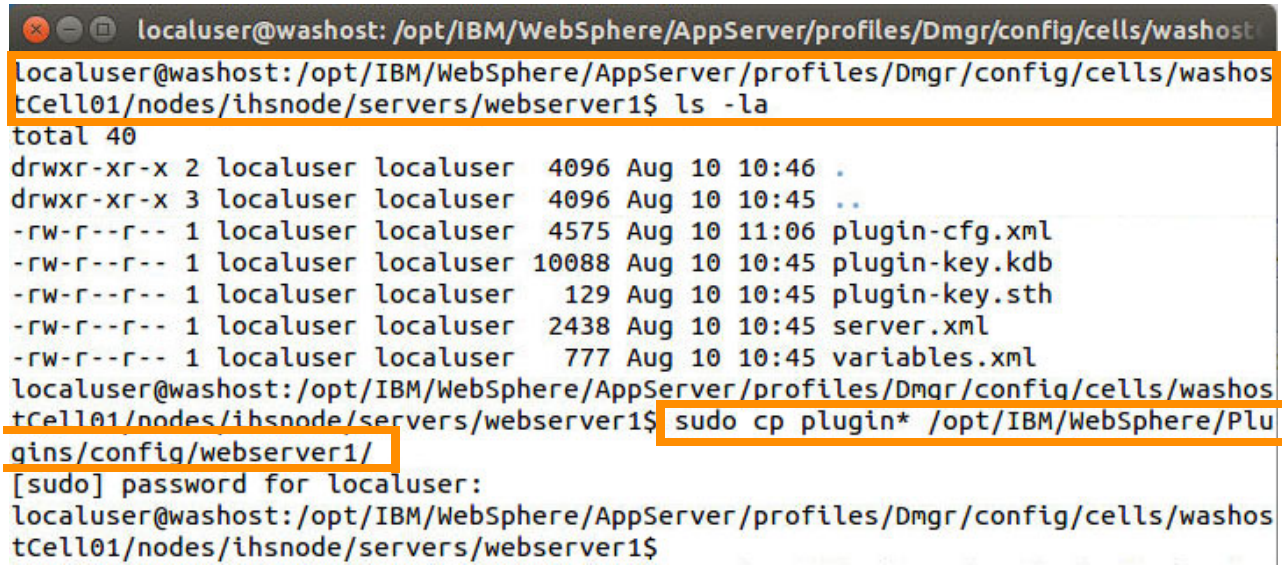
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ c. Return to the terminal window and copy the plug-in key ring files to the `plugin` directory. Use the following commands to change directory and then copy the files:

```
cd /opt/IBM/WebSphere/AppServer/profiles/Dmgr/config/cells/
washostCell01/nodes/ihsnode
sudo cp plugin* /opt/IBM/WebSphere/Plugins/config/webserver1/
```

Enter `passw0rd` when prompted for the localuser's password.

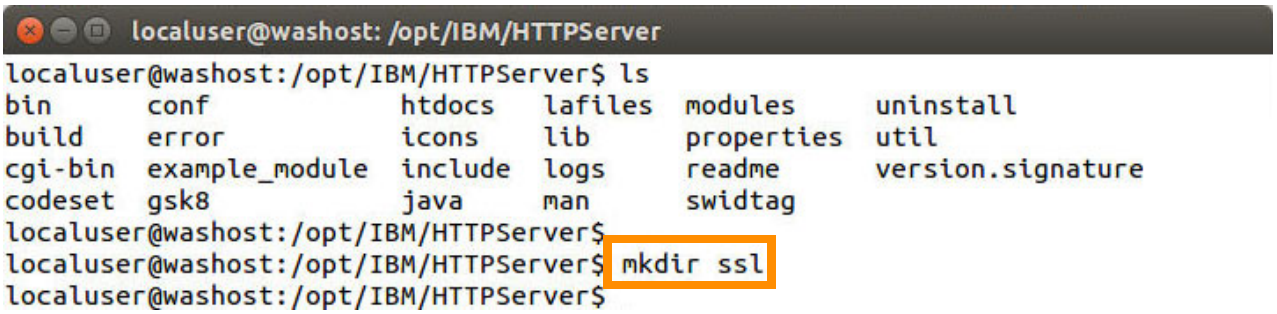


Section 7: Configuring SSL for IBM HTTP Server (optional)

This part of the exercise examines the process of creating a certificate and a key ring for the web server. The steps are used to configure SSL on the connection between the client browser and the web server.

__ 1. Create a directory to hold the key ring.

__ a. Using the `mkdir` command, create the directory `ssl` in `/opt/IBM/HTTPServer`.



__ 2. Create a key ring with a self-signed certificate for IBM HTTP Server.

__ a. Run the iKeyman for IBM HTTP Server by entering the following command:

```
/opt/IBM/HTTPServer/bin/ikeyman
```

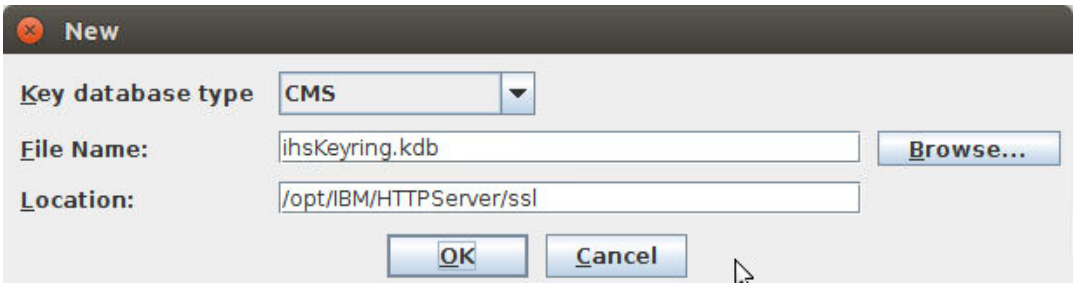
__ b. Create a key ring by clicking **Key Database File > New**.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

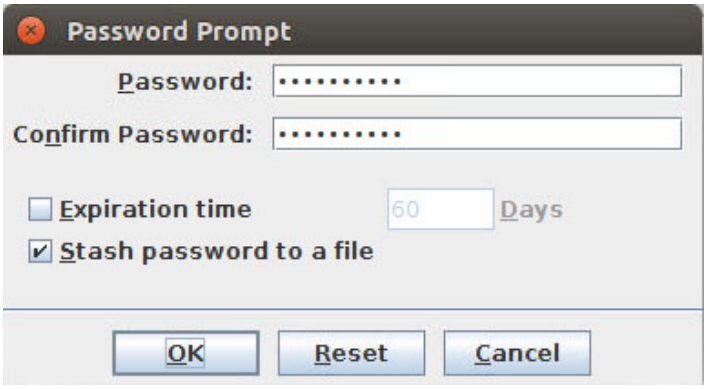
__ c. Supply the following information:

- **Key database type**: `CMS`
- **File Name**: `ihsKeyring.kdb`
- **Location**: `/opt/IBM/HTTPServer/ssl`



__ d. Click **OK**.

__ e. When prompted for a password for the key ring, enter and confirm `web1sphere` as the password. If you want to modify the expiration time, you can do so. Select the **Stash password to a file** check box.



Attention

The stash file is created containing an encoded form of the password. This encoding prevents casual viewing of the password, but is not highly secure. Therefore, you must protect this file by using operating system file permissions to prevent all access from unauthorized principals.

The file name of the stash file is the same as the name of the key file, only it has a `.sth` suffix. The stash file gets stored in the same directory as the key file.

__ f. Click **OK**.

__ 3. Create a self-signed certificate.

© Copyright IBM Corp. 2016

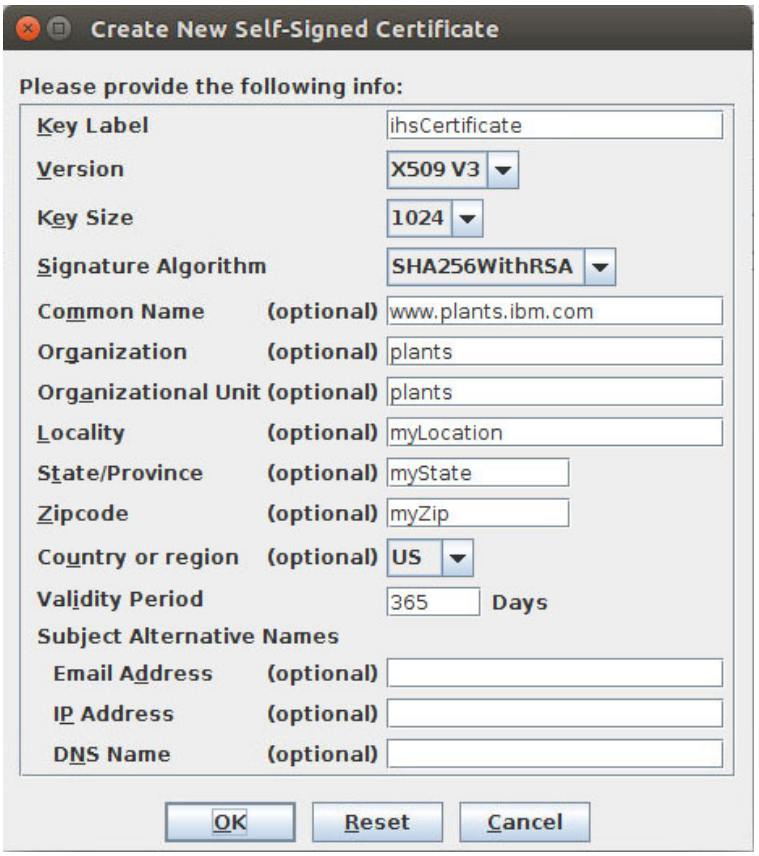
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ a. In iKeyman, click **Create > New Self-Signed Certificate** and enter the following information:

Table 2: Self-signed certificate details

Example	Description
Key label	`ihsCertificate`
Signature Algorithm	`SHA256WithRSA`
Common name	`www.plants.ibm.com`
Organization	`plants`
Organization unit	`plants`
Locality	`myLocation`
State or province	`myState`
Zip code	`myZipcode`

__ b. Accept the defaults for the **Version**, **Key Size**, and **Validity Period**.



__ c. Click **OK**.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Information

This operation stores the certificate in the key file in the **Personal Certificates** section. Optionally, it is possible to extract the public signing certificate so that clients can use it. To extract, click **Extract Certificate**, and then enter a **File Name** and **Location**. Click **OK**.

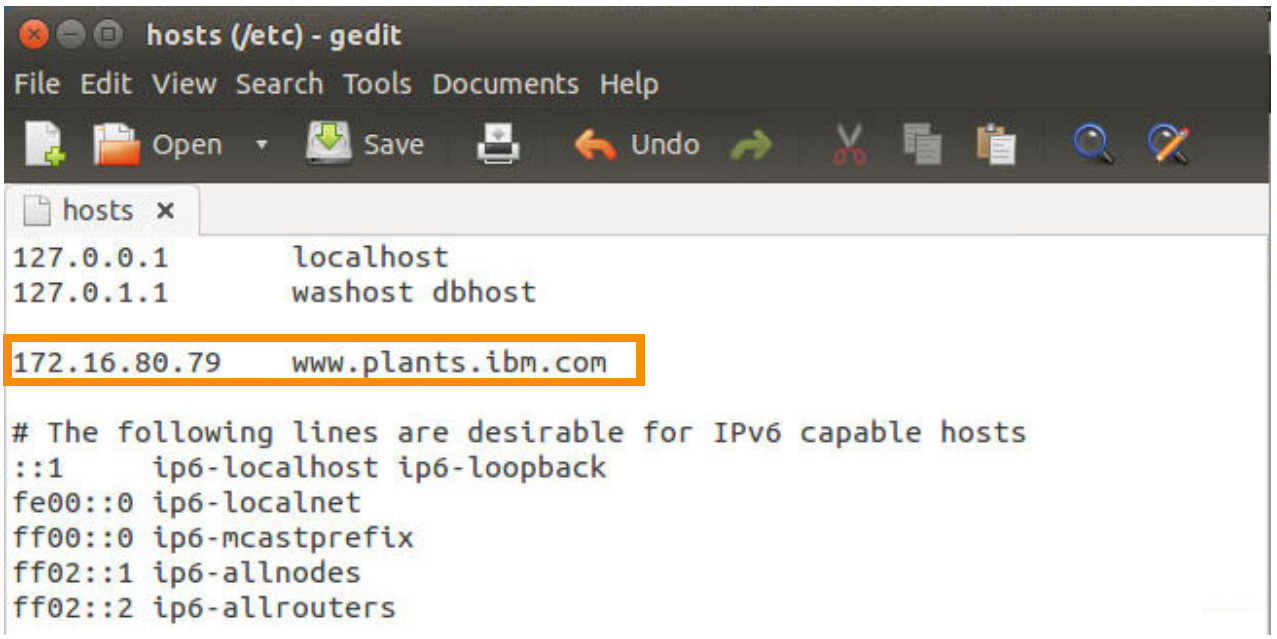
__ d. Exit iKeyman by clicking **Key Database File > Exit**.

__ e. Check the contents of the `/opt/IBM/HTTPServer/ssl/` directory and verify that the following files were created: `ihsKeyring.kdb`, `ihsKeyring.sth`, and `ihsKeyring.rdb`.

__ 4. Configure IBM HTTP Server for HTTPS, which requires modifying the `httpd.conf` file to define the required setting to enable SSL for IBM HTTP Server. It also includes loading the SSL module, defining a listener port, defining a virtual host, and enabling SSL.

__ a. Add `www.plants.ibm.com` to the hosts file by editing the file `/etc/hosts` and adding a line at the bottom to define the host name: `www.plants.ibm.com`
Map it to the IP address for your system. You can use the command `ifconfig` in a terminal window to find your IP address.

Use the following command `sudo gedit /etc/hosts` to edit the hosts file by using root access:



__ b. Save and exit the file.

__ c. Use the following command in a terminal window to confirm that you can reach `www.plants.ibm.com`:

```
ping -c 4 www.plants.ibm.com
```

__ d. Back up the `httpd.conf` file. Copy the `httpd.conf` file in `/opt/IBM/HTTPServer/conf` to `httpd-backup.conf`.

__ e. Using a text editor, open `httpd.conf` in `/opt/IBM/HTTPDServer/conf`.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ f. Add a virtual host definition for HTTPS, which allows for the definition of HTTPS on a separate virtual host from HTTP. Place these lines near the bottom of the `httpd.conf` file after the VirtualHost examples and just before the comment:

```
# Enable IBM HTTP Server diagnostic features

LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 0.0.0.0:443
<VirtualHost www.plants.ibm.com:443>
SSLEnable
</VirtualHost>
KeyFile "/opt/IBM/HTTPServer/ssl/ihsKeyring.kdb"
SSLDisable
```

Information

There are sample configuration files in `/opt/labfiles/ssl/` that can be used to copy and paste. These files include only this section of a completed `httpd.conf` file.

__ g. Save your changes and exit the editor.

Section 8: Testing the SSL connection

__ 1. Restart the IBM HTTP Server process so that the new `httpd.conf` settings take effect.

__ a. Using a terminal window, use the following command to restart the web server process:

```
sudo /opt/IBM/HTTPServer/bin/apachectl restart
```

__ b. Verify that the IBM HTTP Server process is running by checking the system process list for httpd. If IBM HTTP Server failed to start, check the `/opt/IBM/HTTPServer/logs/error.log` and `/opt/IBM/WebSphere/Plugins/logs/webserver1/http_plugin.log` files for the possible cause.

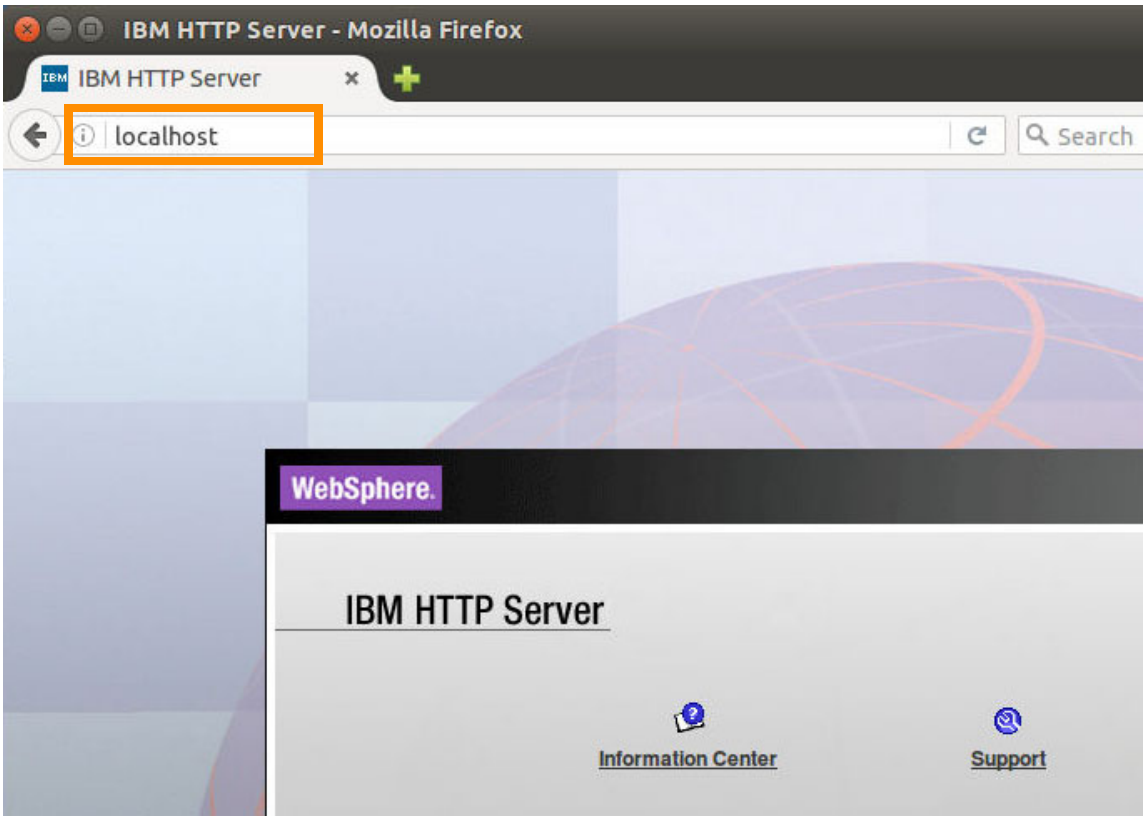
__ 2. Use HTTPS to connect to IBM HTTP Server.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

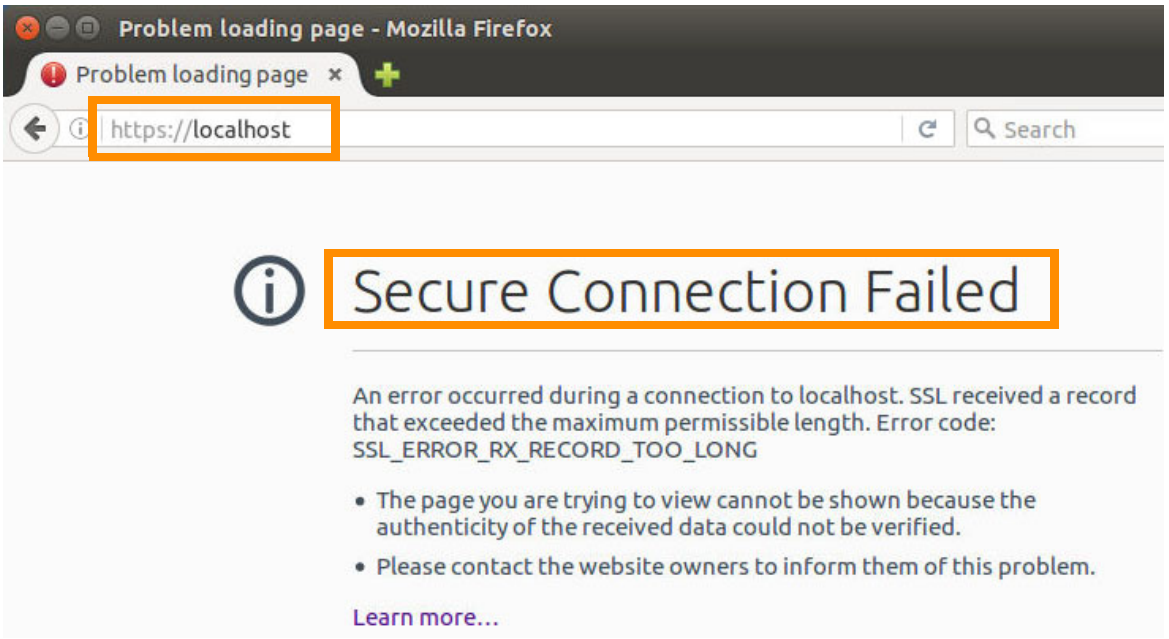
__ a. First, verify that the web server is running. Connect to the following site:

```
http://localhost/
```



__ b. Now that the web server is known to be running, enter the following address to verify that HTTPS is working (notice, the only difference is that the HTTP protocol is replaced with HTTPS):

```
https://localhost/
```

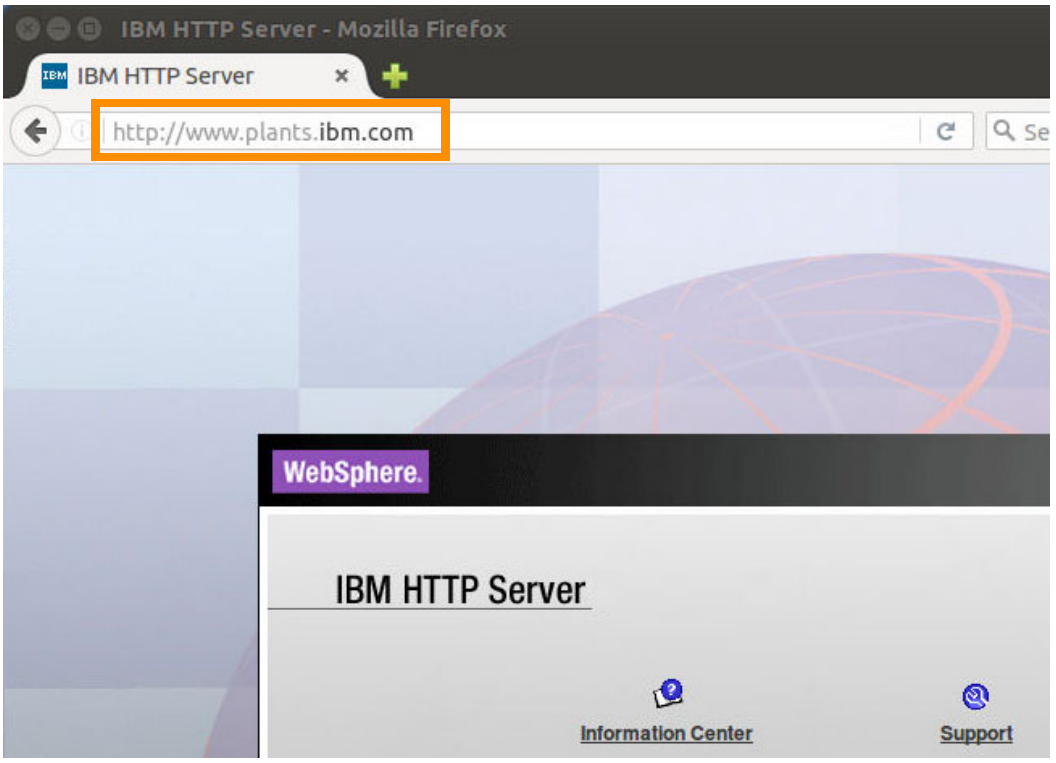


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Localhost fails because the virtual host definition for the SSL configuration is defined for the host named `www.plants.ibm.com`.

__ c. Using the same browser window, enter the following URL:

`http://www.plants.ibm.com/`



This request works since the host name `www.plants.ibm.com` is mapped to the local system and there is no https necessary.

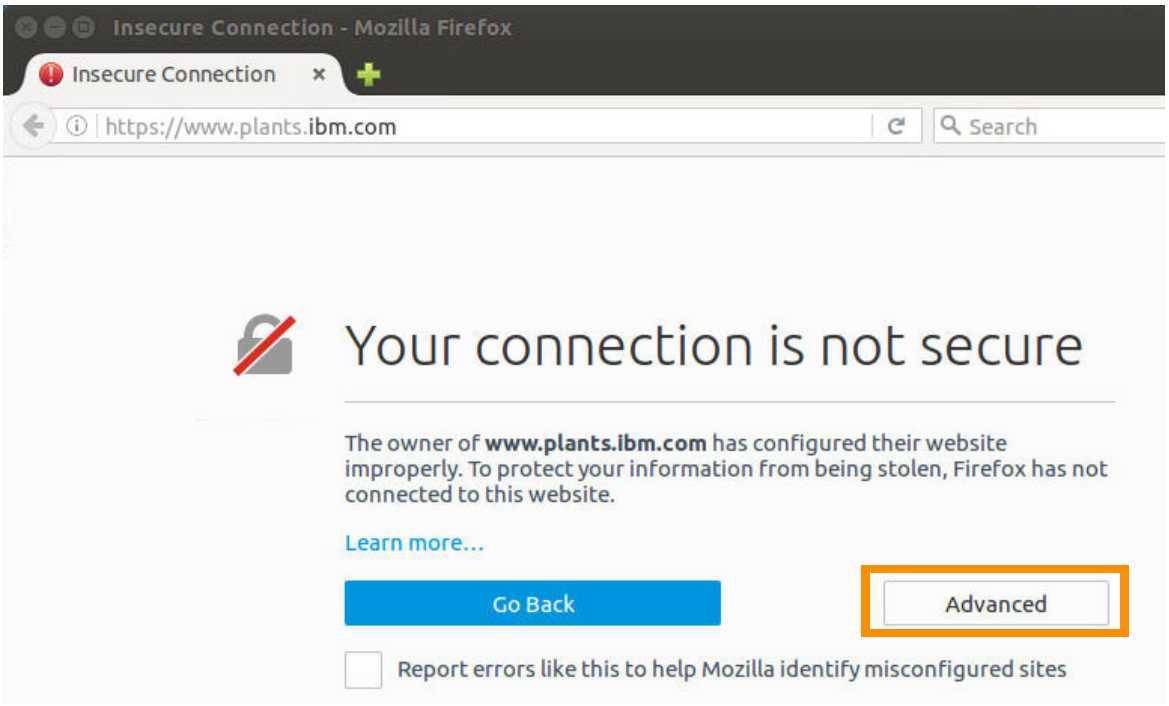
__ d. Now that you verified that the new host name works, change the protocol to HTTPS so that the URL is:

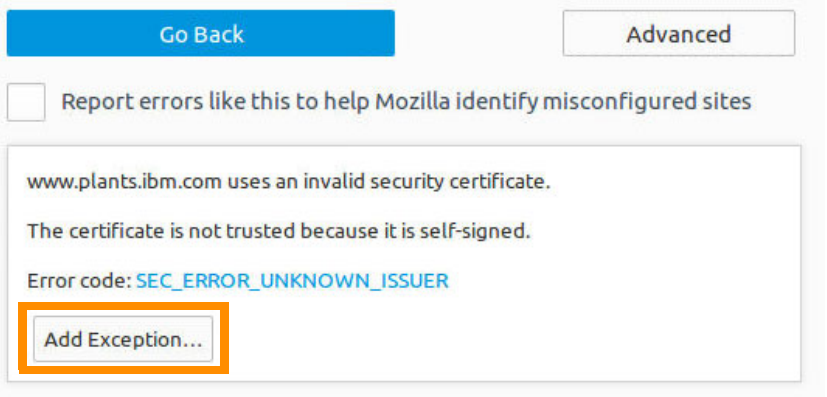
`https://www.plants.ibm.com/`

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ e. Assuming that the certificate is not added to the browser key ring, you receive a certificate warning. The warning happens because the SSL connection is presenting a self-signed certificate. Therefore, the browser is unable to validate the signer. Click **Advanced** and then **Add Exception**.

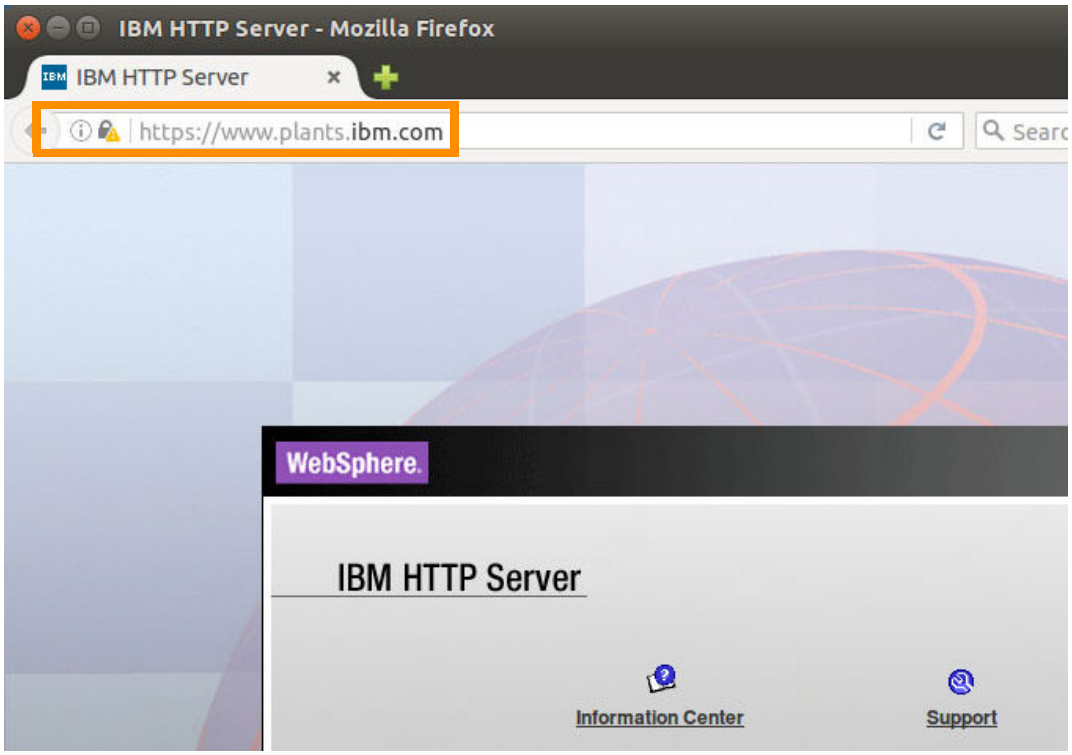




__ f. Click **Confirm Security Exception** to confirm that you accept the new certificate.

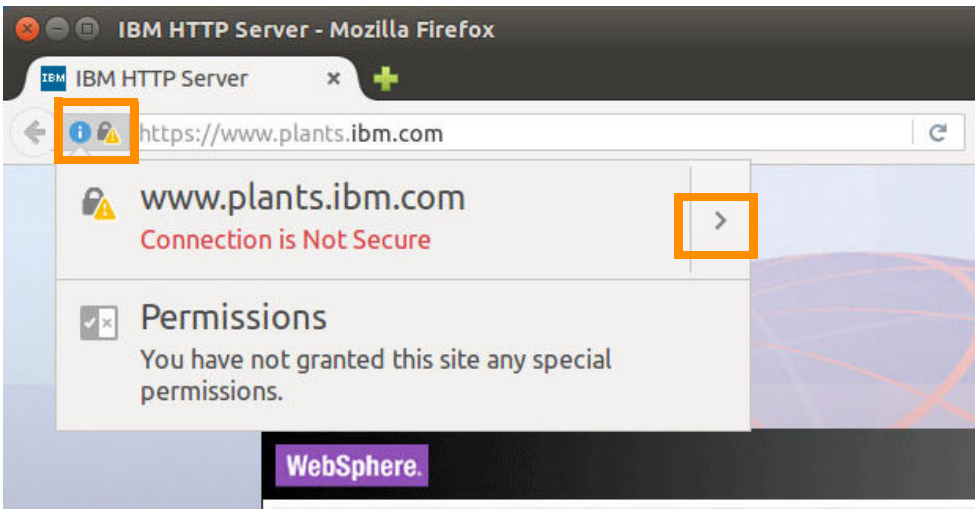
© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ g. The browser then takes you to the HTTPS connection for the web server home page.



The page works as expected because the host name (`www.plants.ibm.com`) matches the virtual host in the SSL configuration within the `httpd.conf` file.

__ h. Click the lock icon to the left of the https to view more information about the connection.



__ i. Click the **right arrow** and then **More Information** to view detailed information about the certificate that is being used for the SSL connection.

__ 3. Next, use HTTPS to connect to the application server.

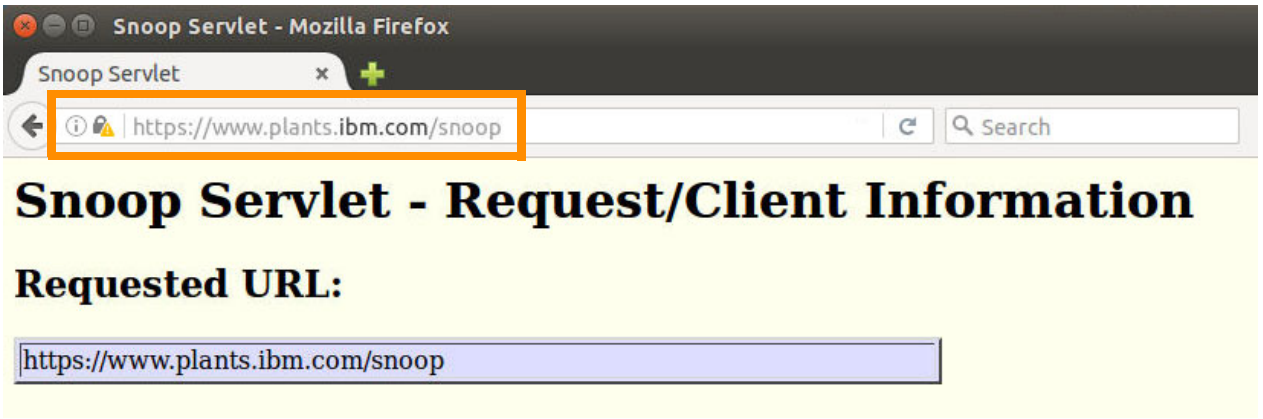
__ a. Verify that the **PlantsCluster** is running.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ b. Using the existing browser, enter the following URL to access the snoop servlet:

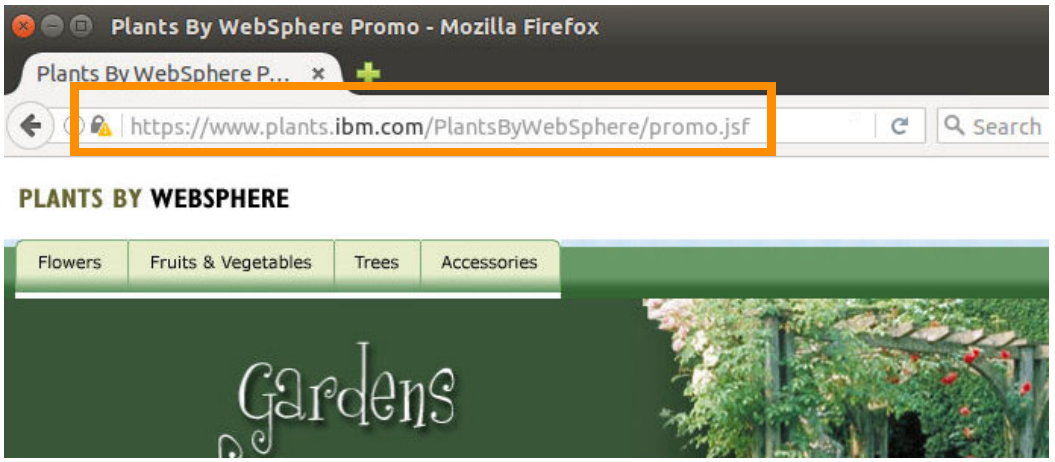
`https://www.plants.ibm.com/snoop`



Notice that it works as expected. If it does not, start by verifying that the plug-in key ring was propagated (which was done earlier in the exercise) and checking the plug-in log file for information.

__ c. Finally, use the following URL to access the PlantsByWebSphere application:

`https://www.plants.ibm.com/PlantsByWebSphere`



End of exercise

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise review and wrap-up

This exercise introduced basic HTTPS configuration concepts for both IBM HTTP Server and WebSphere Application Server.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

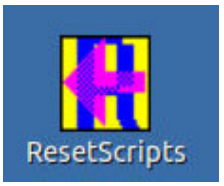
Appendix A. Resetting the WebSphere environment

To complete some lab exercises, specific lab exercises must first be completed. However, occasionally you might have a problematic configuration or want to skip labs. For these cases, a reset function is provided to set your environment to an appropriate state.

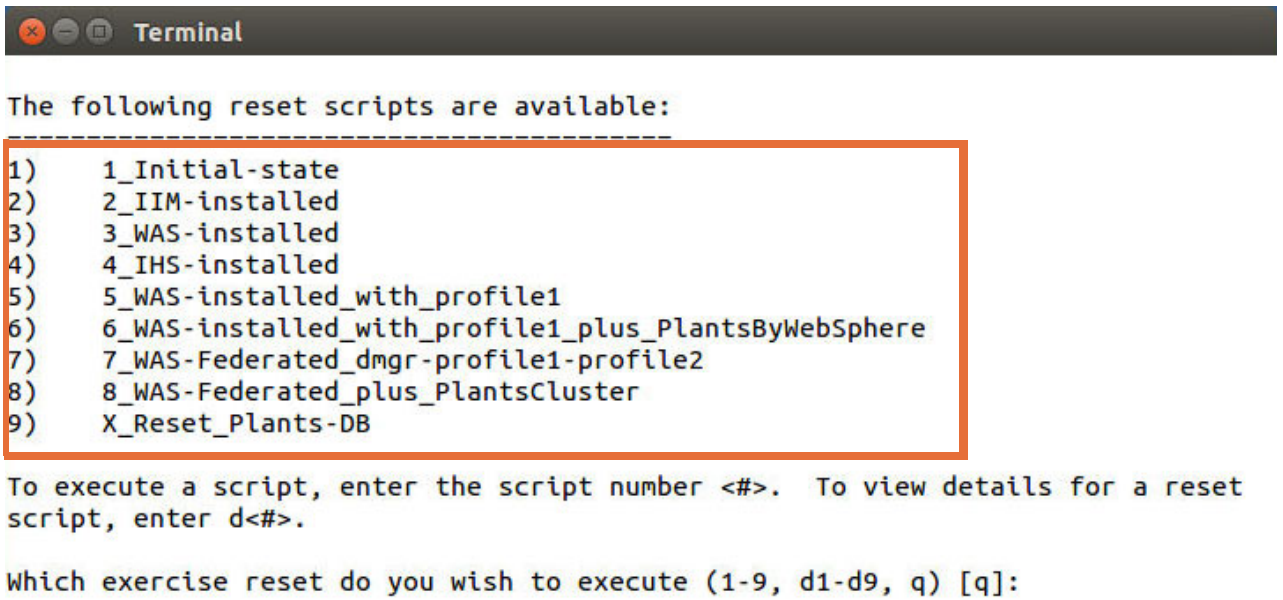
The reset scripts are initiated from a desktop icon and allow users to choose which state they want to restore. The reset scripts can take some time to run, depending on what software is already installed on the lab computer. For example, if none of the exercises are completed, it might be necessary for the reset scripts to install numerous pieces of software; this action would take 5 – 10 minutes. However, if all of the software installation is completed, it might be necessary for the reset scripts to restore only the profiles directories, and this action would take only 1 – 2 minutes.

__ 1. Run the reset script.

__ a. From the desktop, locate and click the **ResetScripts** icon.



__ b. The reset script interface lists the available states that are available.



__ c. A number of reset scripts are available. Locate the name of the exercise that directed you here and select the associated reset script state. Running the script that is listed resets the lab to a state usable to start that exercise. For example, if you wanted to start the exercise **Installing an application**, you would select the reset script **5_WAS-installed_with_profile1**.

- Reset script: ***4_IHS-installed***
  - Exercise (WA590): Profile creation

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

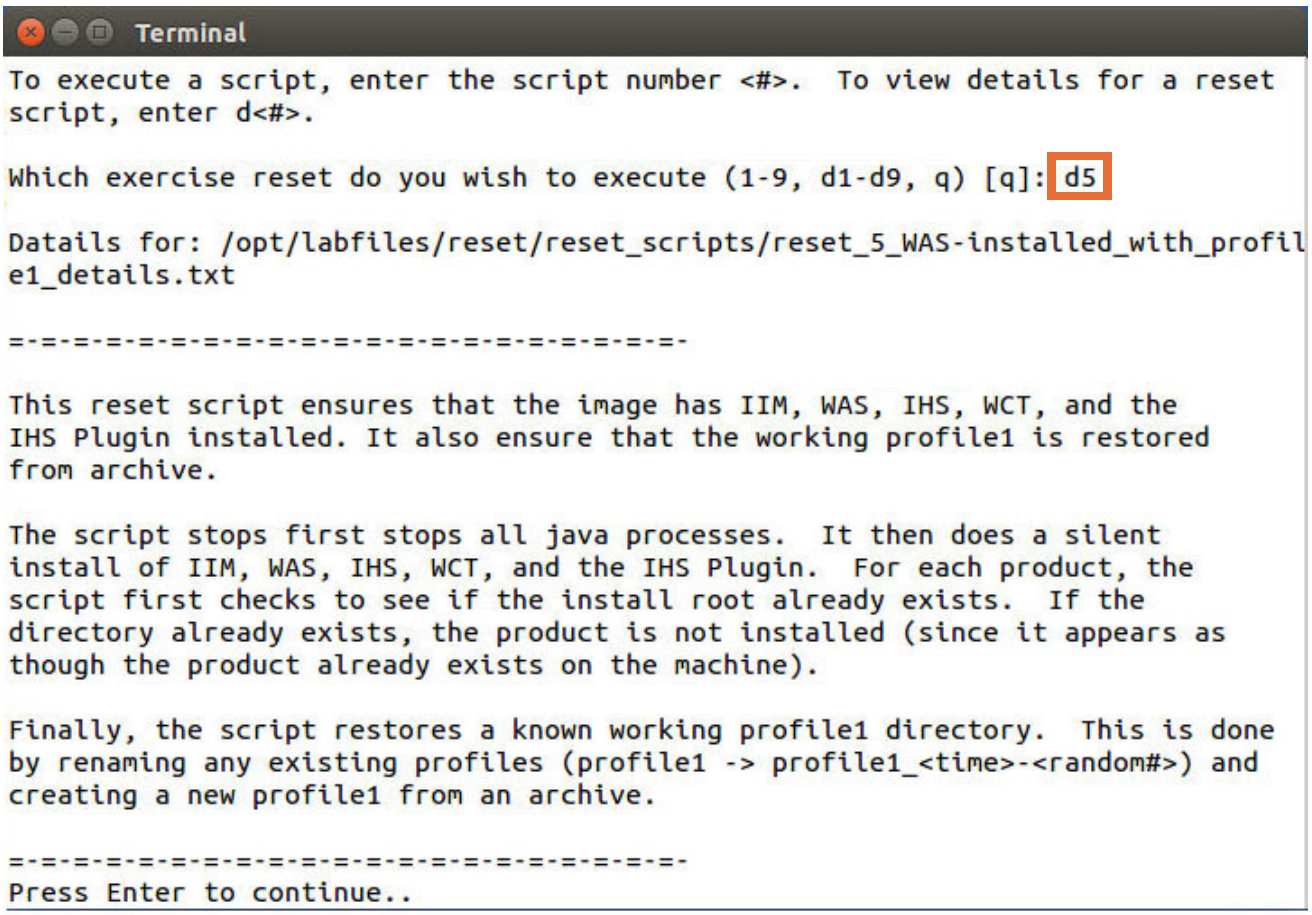
- Reset script: ***5_WAS-installed_with_profile1***
  - Exercise (WA590): Exploring the administrative console
  - Exercise (WA590): Assembling an application
  - Exercise (WA590): Installing an application
- Reset script: ***6_WAS-installed_with_profile1_plus_PlantsByWebSphere***
  - Exercise (WA590): Problem determination
  - Exercise (WA590): Using wsadmin
  - Exercise (WA590): Configuring WebSphere security
  - Exercise (WA590): Configuring application security
  - Exercise (WA590): Using the performance monitoring tools
- Reset script: ***6_WAS-installed_with_profile1_plus_PlantsByWebSphere***
  - Exercise (WA599): Creating a federated cell
- Reset script: ***7_WAS-Federated_dmgr-profile1-profile2***
  - Exercise (WA599): Clustering and workload management
- Reset script: ***7_WAS-Federated_plus_PlantsCluster***
  - Exercise (WA599): Configuring SSL for WebSphere
- Reset script: ***X*_Reset_Plants-DB**
  - This script rebuilds the Plants database.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Information

If you would like more information about the specific reset scripts, type the letter `d` followed by the number for the reset script.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

__ d. Depending on how much work the reset script must do, the wait is several minutes. When the script finishes, press Enter to close the window.

```
Terminal
To execute a script, enter the script number <#>.  To view details for a reset
script, enter d<#>.

Which exercise reset do you wish to execute (1-9, d1-d9, q) [q]: 5

Running script: /opt/labfiles/reset/reset_scripts/reset_5_WAS-installed_with_pro
file1.sh

=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-


This script will reset the profiles to a state expected at the

    5_WAS-installed_with_profile1

Do you want to continue (y/n) [y]:
```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

IBM Training

© Copyright International Business Machines Corporation 2016.