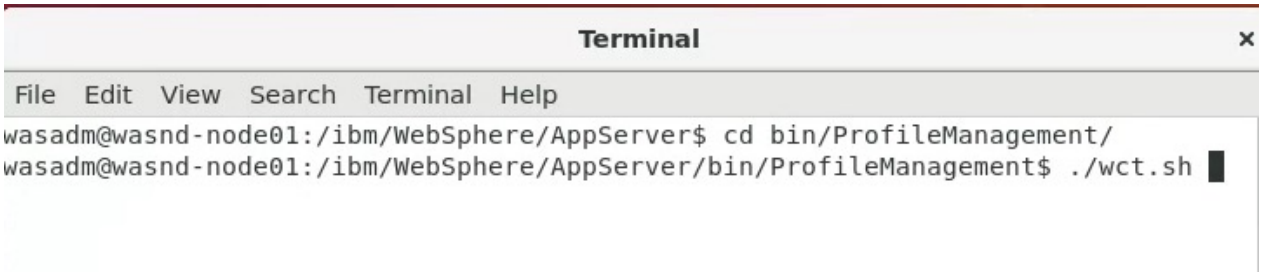
Exercise 9 – Federating a Cell

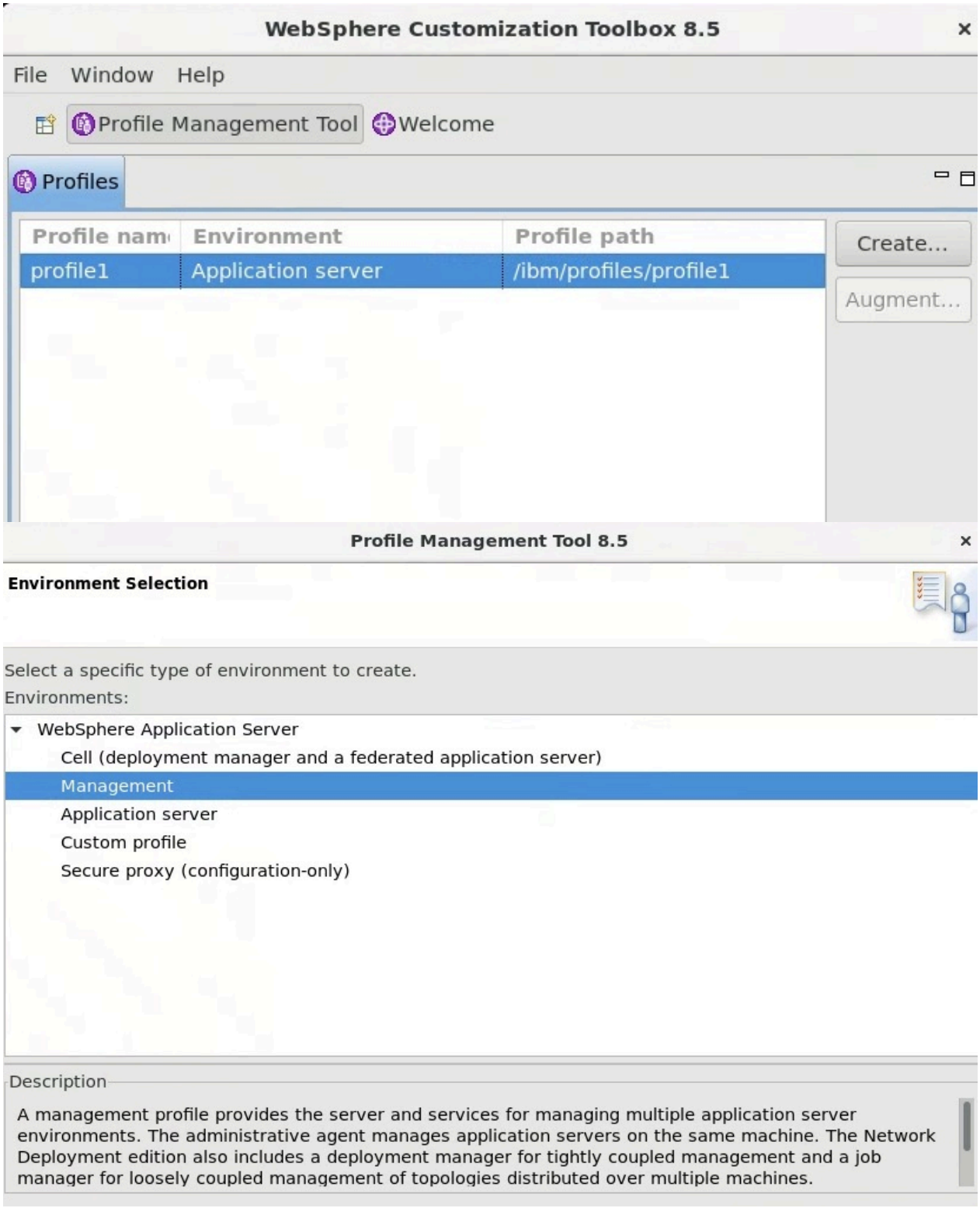
At the end of the lab, you should be able to:• Create a deployment manager profile• Back up the deployment manager configuration• Use the deployment manager administrative console• Federate a node into the deployment manager cell• Create a custom profile• Create an unmanaged web server node• Use the administrative console to start and stop a web server • Map an application to a web server
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.

When you complete the exercise, you have a cell, named was85hostCell01, containing the following nodes:
- Deployment manager node, named was85hostCellManager01
- A federated node, named was85hostNode01, containing a node agent and an application server, named server1
- A federated node, named was85hostNode02, containing only a node agent
- An unmanaged node, named ihsnode, containing an IBM HTTP Server administrative process and a web server, named webserver1

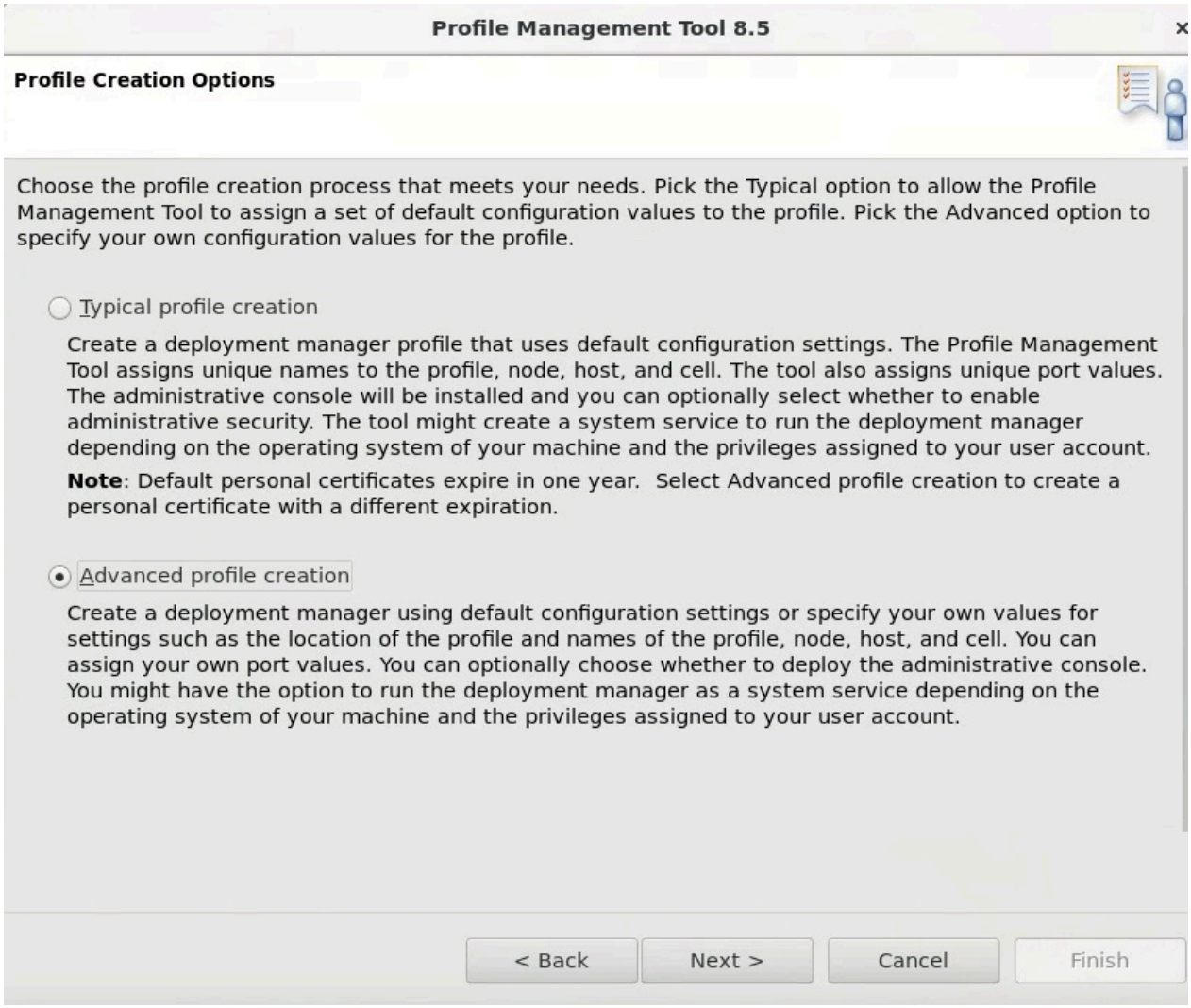
Section 1: Use the Profile Management Tool to create a deployment manager profile

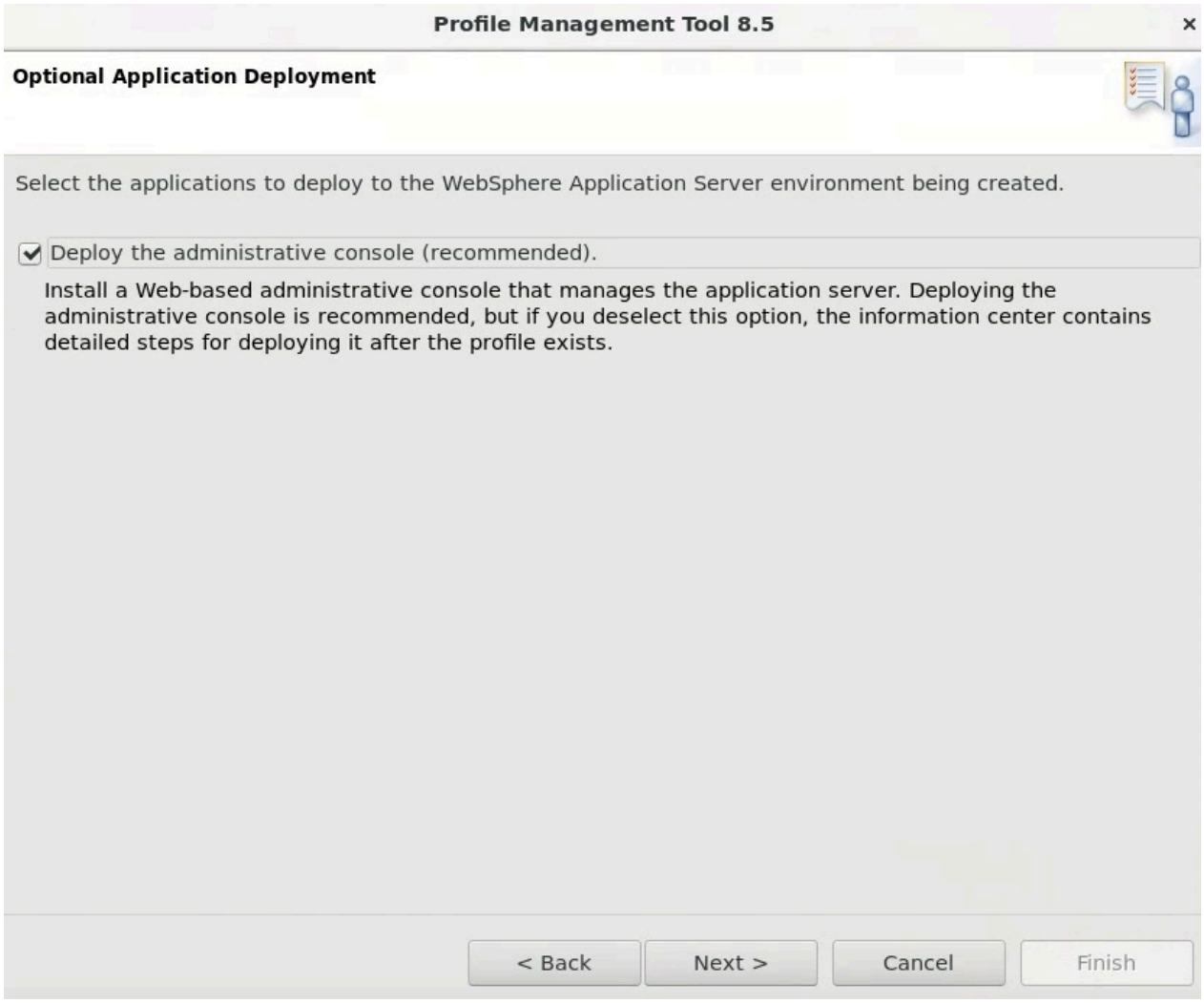
During this section of the exercise, you use the Profile Management Tool to create a deployment management profile. The deployment manager profile defines a cell, named was85hostCell01, containing a deployment manager node, named was85hostCellManager01. The existing application server, server1, continues to be a stand-alone server that is contained in the node was85hostNode01.

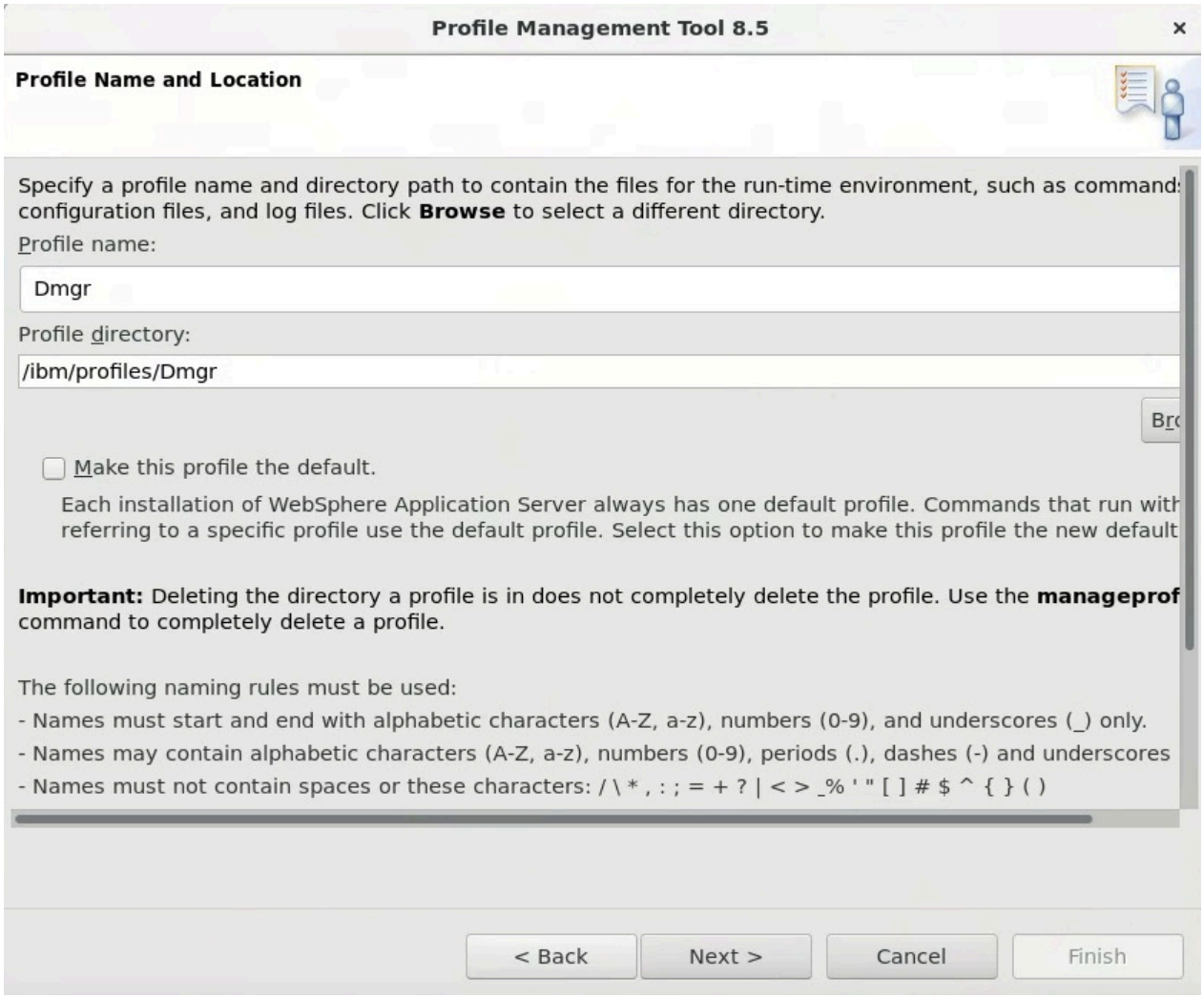


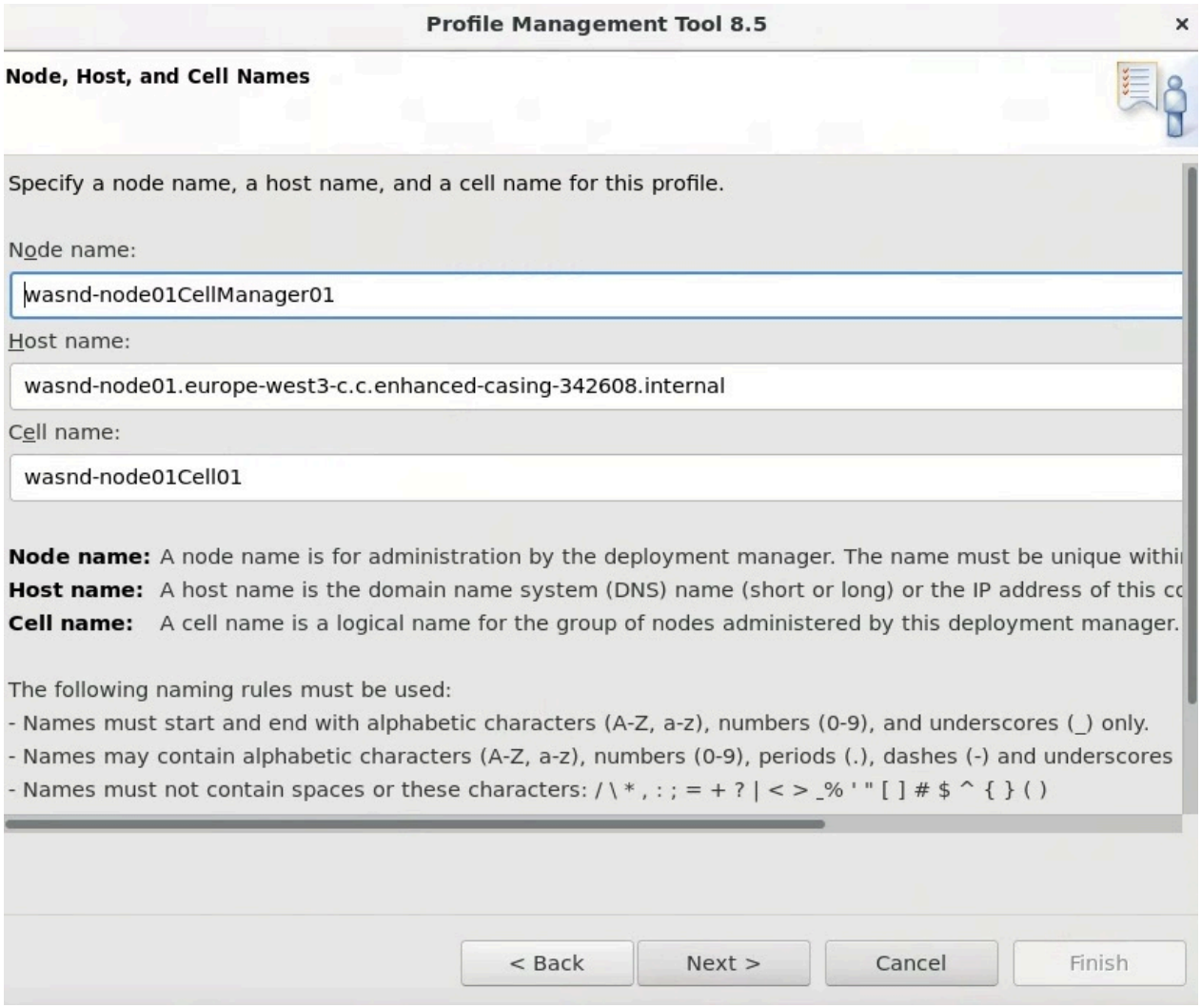

WebSphere Customization Toolbox 8.5
File
Window
Help
Profile Management Tool
Welcome
Profiles
Profile nam
Environment
Profile path
profile1
Application server
/ibm/profiles/profile1
Create...
Augment...
Profile Management Tool 8.5
Environment Selection
Select a specific type of environment to create.
Environments:
WebSphere Application Server
Cell (deployment manager and a federated application server)
Management
Application server
Custom profile
Secure proxy (configuration-only)
Description
A management profile provides the server and services for managing multiple application server environments. The administrative agent manages application servers on the same machine. The Network Deployment edition also includes a deployment manager for tightly coupled management and a job manager for loosely coupled management of topologies distributed over multiple machines.


Profile Management Tool 8.5
Server Type Selection
Select the type of server to be created within this management profile
Administrative agent
An administrative agent provides management capability for multiple stand-alone application servers. An administrative agent can manage only the application servers that exist within the same installation on one machine.
Deployment manager
A deployment manager provides management capability for multiple federated nodes. A deployment manager can manage nodes that span multiple systems and platforms. The nodes that are managed by a deployment manager can only be managed by a single deployment manager and must be federated to the cell of that deployment manager.
Job manager
A job manager provides management capability for multiple stand-alone application servers, administrative agents, and deployment managers. The job manager can manage nodes that span multiple systems and platforms. The nodes that are managed by one job manager also can be managed by other job managers.
< Back
Next >
Cancel
Finish


Profile Management Tool 8.5
Profile Creation Options
Choose the profile creation process that meets your needs. Pick the Typical option to allow the Profile Management Tool to assign a set of default configuration values to the profile. Pick the Advanced option to specify your own configuration values for the profile.
Typical profile creation
Create a deployment manager profile that uses default configuration settings. The Profile Management Tool assigns unique names to the profile, node, host, and cell. The tool also assigns unique port values. The administrative console will be installed and you can optionally select whether to enable administrative security. The tool might create a system service to run the deployment manager depending on the operating system of your machine and the privileges assigned to your user account.
Note: Default personal certificates expire in one year. Select Advanced profile creation to create a personal certificate with a different expiration.
Advanced profile creation
Create a deployment manager using default configuration settings or specify your own values for settings such as the location of the profile and names of the profile, node, host, and cell. You can assign your own port values. You can optionally choose whether to deploy the administrative console. You might have the option to run the deployment manager as a system service depending on the operating system of your machine and the privileges assigned to your user account.
< Back
Next >
Cancel
Finish


Profile Management Tool 8.5
Optional Application Deployment
Select the applications to deploy to the WebSphere Application Server environment being created.
Deploy the administrative console (recommended).
Install a Web-based administrative console that manages the application server. Deploying the administrative console is recommended, but if you deselect this option, the information center contains detailed steps for deploying it after the profile exists.
< Back
Next >
Cancel
Finish


Profile Management Tool 8.5
Profile Name and Location
Specify a profile name and directory path to contain the files for the run-time environment, such as command
configuration files, and log files. Click Browse to select a different directory.
Profile name:
Dmgr
Profile directory:
/ibm/profiles/Dmgr
Br
Make this profile the default.
Each installation of WebSphere Application Server always has one default profile. Commands that run with
referring to a specific profile use the default profile. Select this option to make this profile the new default
Important: Deleting the directory a profile is in does not completely delete the profile. Use the manageprof
command to completely delete a profile.
The following naming rules must be used:
- Names must start and end with alphabetic characters (A-Z, a-z), numbers (0-9), and underscores (_) only.
- Names may contain alphabetic characters (A-Z, a-z), numbers (0-9), periods (.), dashes (-) and underscores
- Names must not contain spaces or these characters: / \ * , : ; = + ? | < > _% ' " [ ] # $ ^ { } ( )
< Back
Next >
Cancel
Finish


Profile Management Tool 8.5
Node, Host, and Cell Names
Specify a node name, a host name, and a cell name for this profile.
Node name:
wasnd-node01CellManager01
Host name:
wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal
Cell name:
wasnd-node01Cell01
Node name: A node name is for administration by the deployment manager. The name must be unique withi
Host name: A host name is the domain name system (DNS) name (short or long) or the IP address of this cc
Cell name: A cell name is a logical name for the group of nodes administered by this deployment manager.
The following naming rules must be used:
- Names must start and end with alphabetic characters (A-Z, a-z), numbers (0-9), and underscores (_) only.
- Names may contain alphabetic characters (A-Z, a-z), numbers (0-9), periods (.), dashes (-) and underscores
- Names must not contain spaces or these characters: / \ * , : ; = + ? | < > _% ' " [ ] # $ ^ { } ( )
< Back
Next >
Cancel
Finish


Profile Management Tool 8.5
Administrative Security
Choose whether to enable administrative security. To enable security, supply a user name and password for logging into administrative tools. This administrative user is created in a repository within the application server. After profile creation finishes, you can add more users, groups, or external repositories.
Enable administrative security
User name:
wasadmin
Password:
Confirm password:
See the information center for more information about administrative security.
View the online information center
< Back
Next >
Cancel
Finish

Profile Management Tool 8.5

Security Certificate (Part 1)

Choose whether to create a default personal certificate and root signing certificate, or import them from keystores. To create new certificates, proceed to Part 2 and provide the certificate information. To import existing certificates from keystores, locate the certificates then proceed to Part 2 and verify the certificate information.

- (•) Create a new default personal certificate.
- ( ) Import an existing default personal certificat

Default personal certificate

Path:

Browse...

Password:

Keystore type:

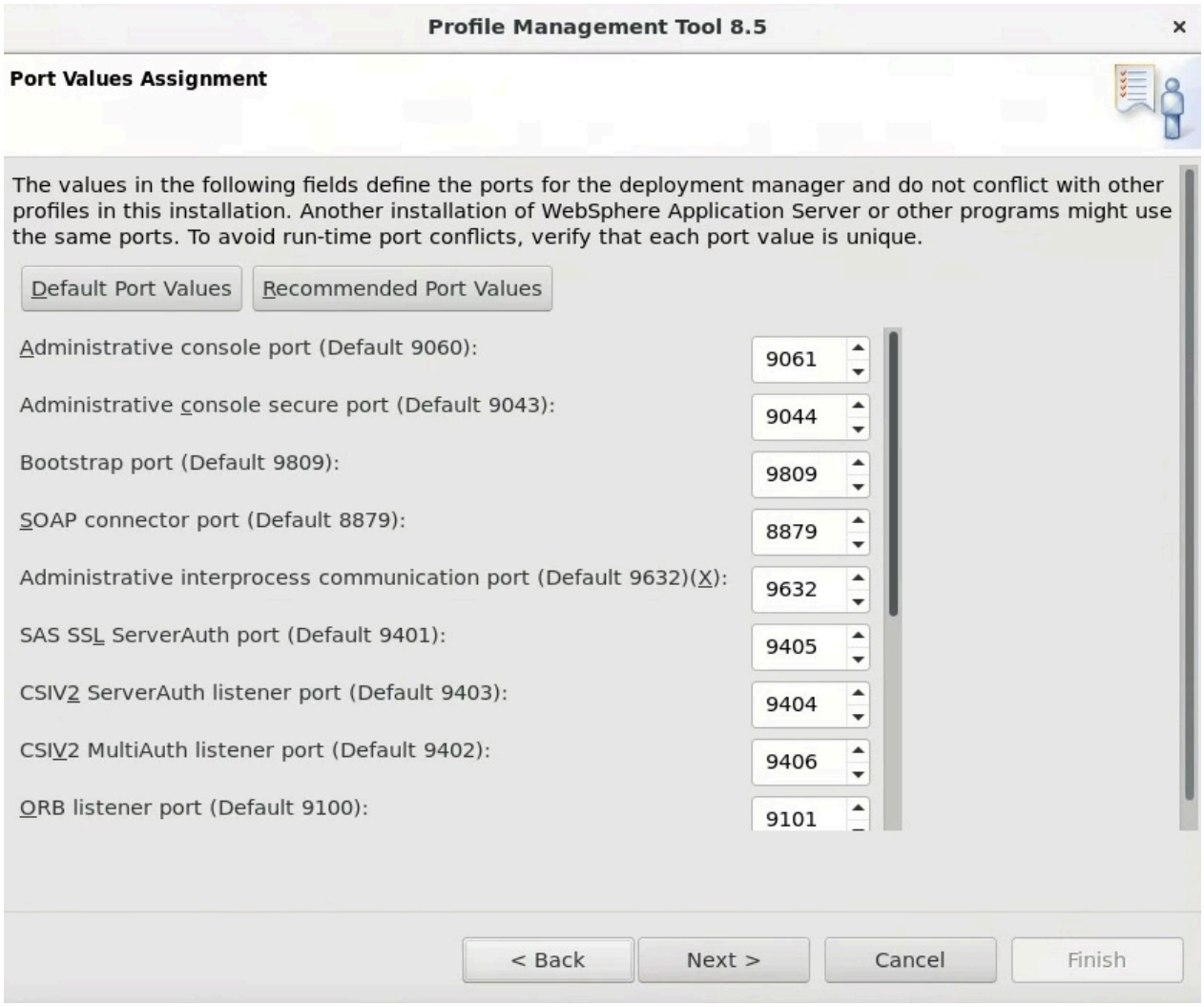
Keystore alias:

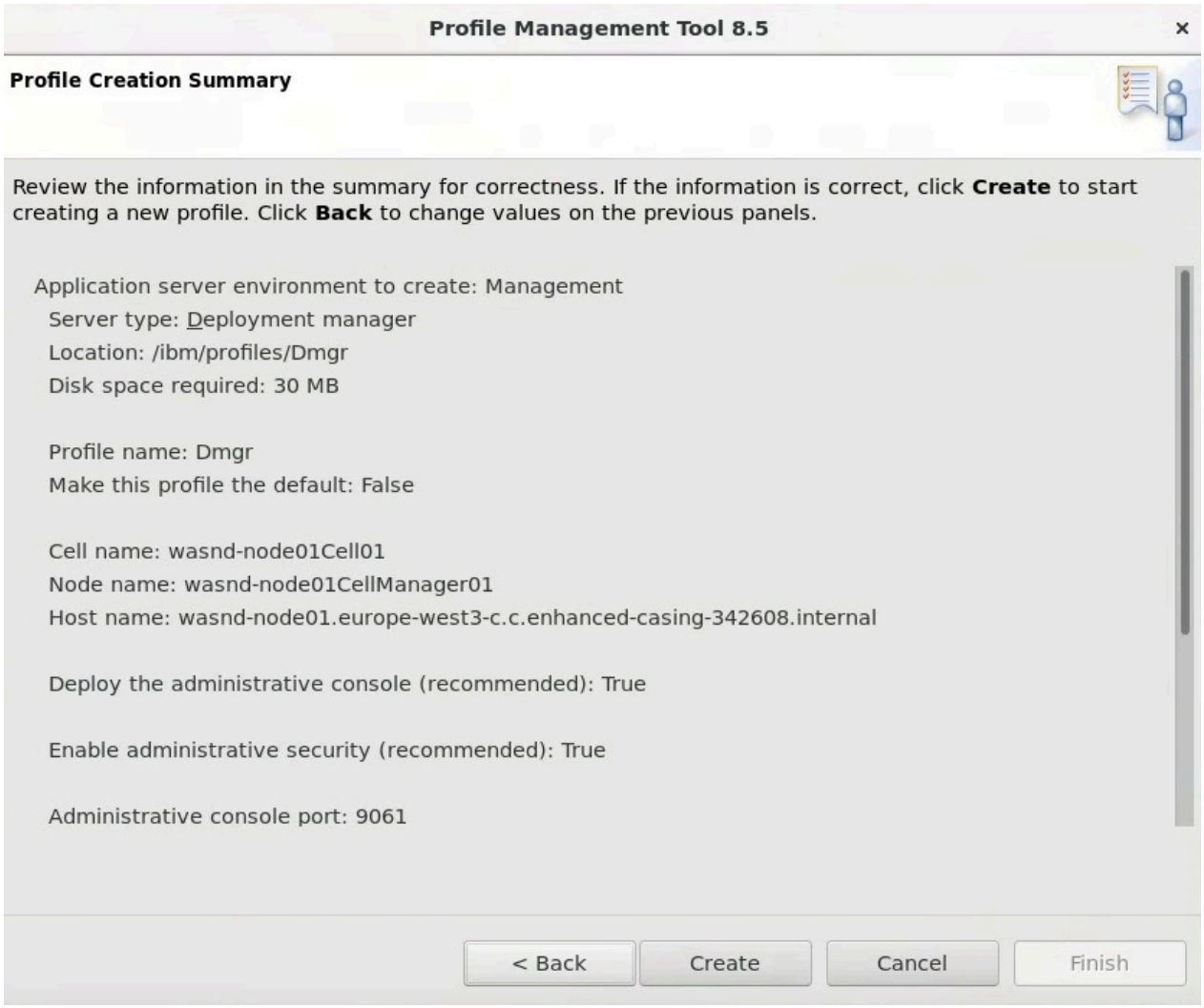
- (•) Create a new root signing certificate.
- ( ) Import an existing root signing certificate.

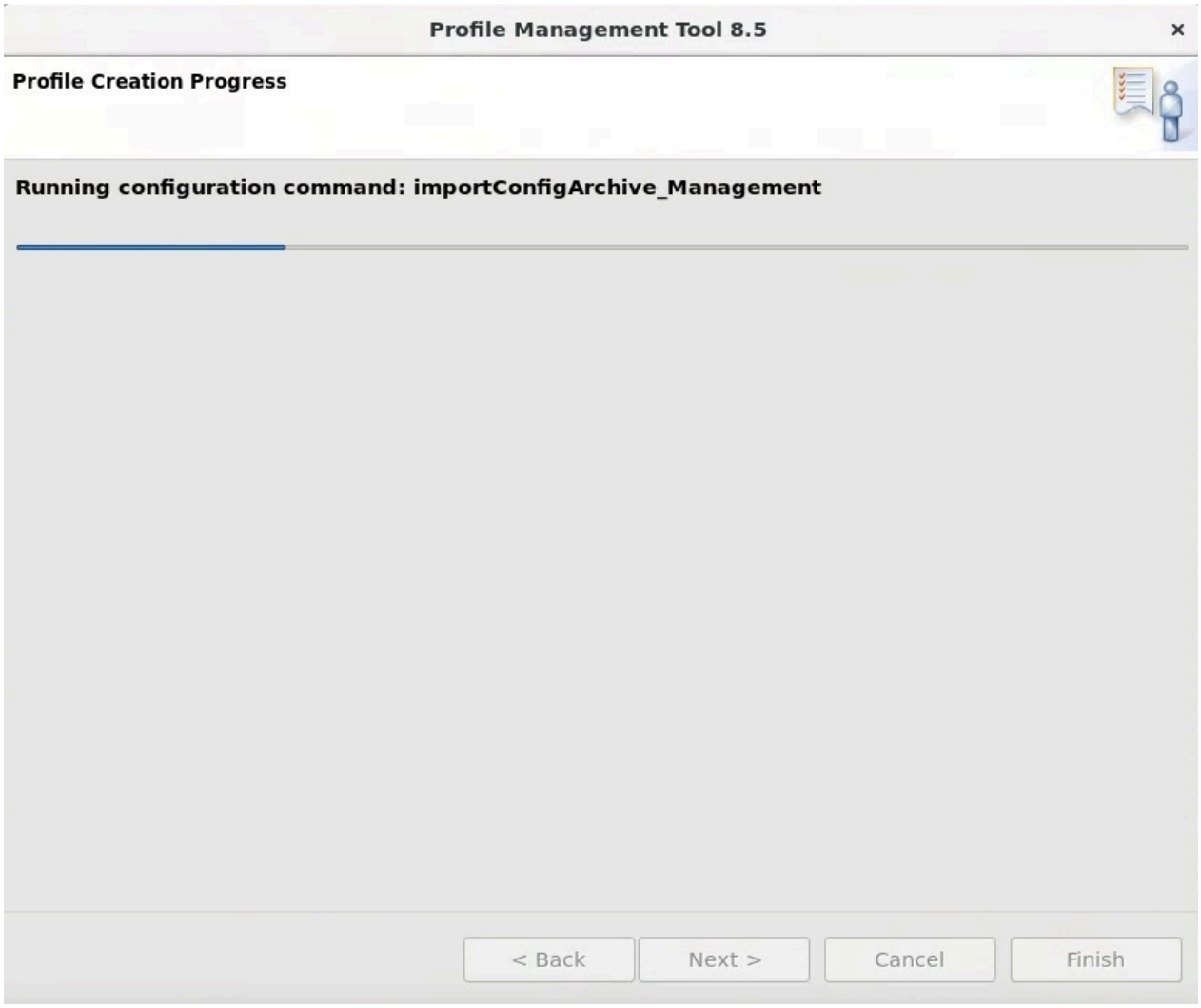
Root signing certificate

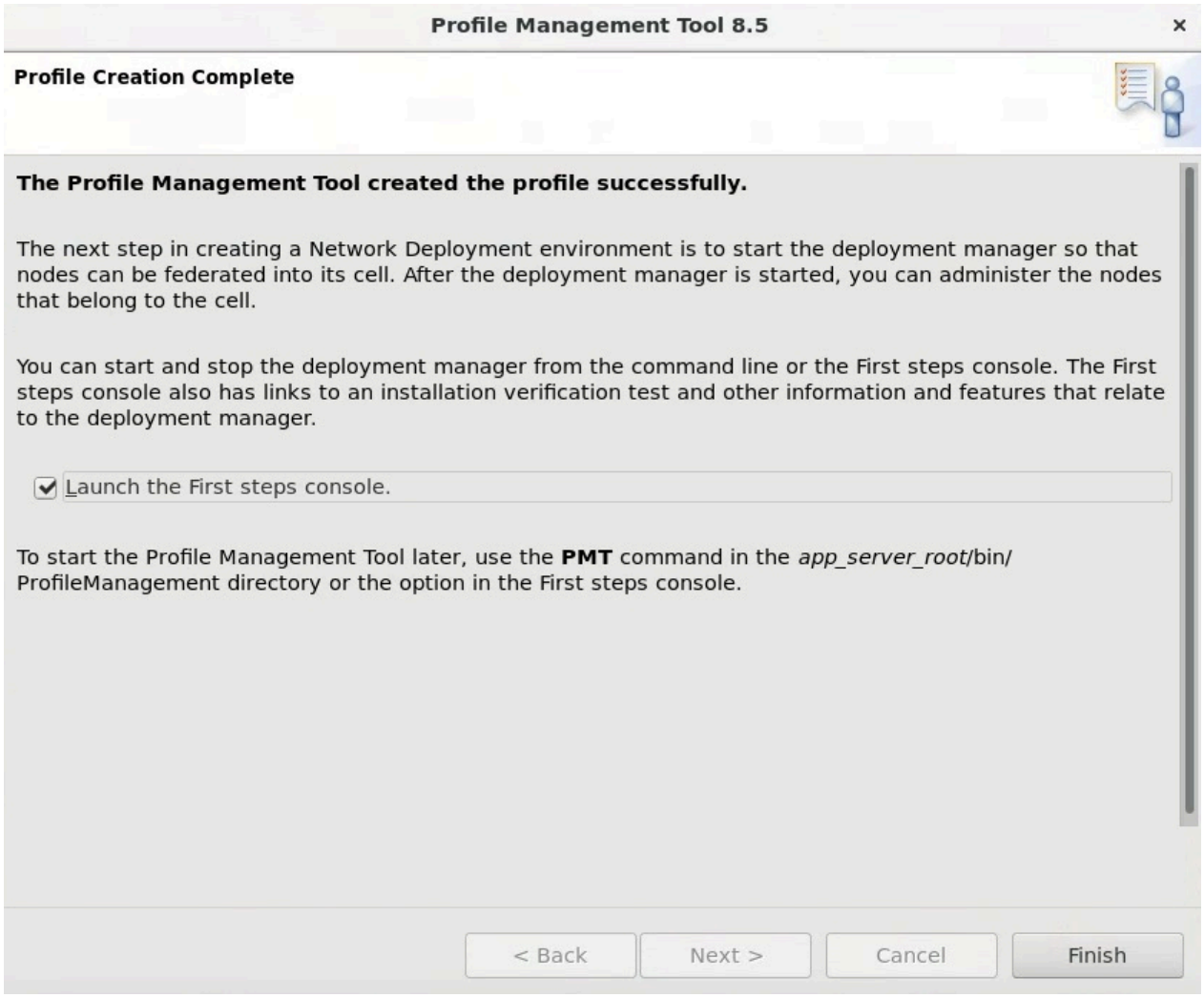
< Back | Next > | Cancel | Finish

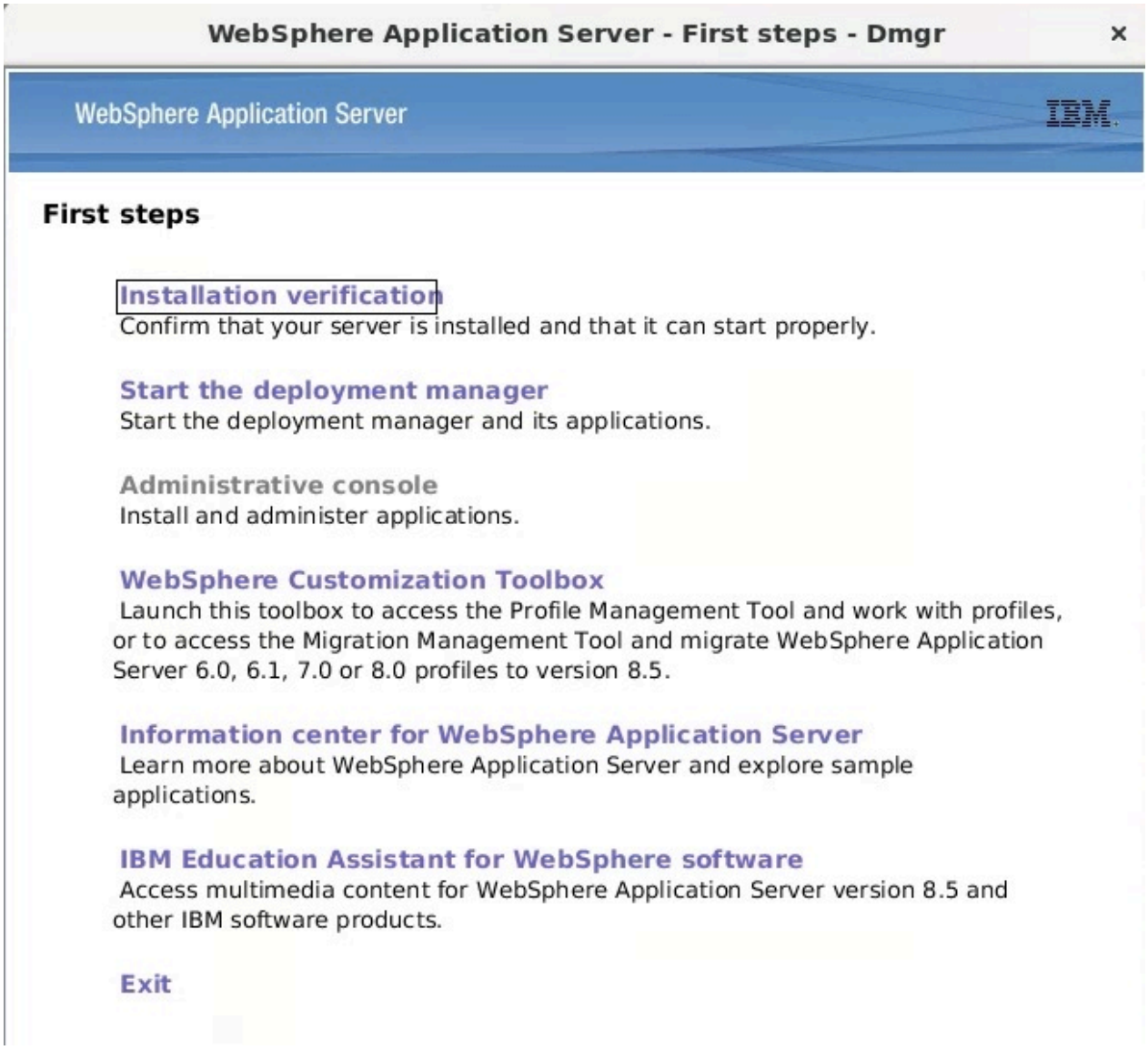

Profile Management Tool 8.5
Security Certificate (Part 2)
Modify the certificate information to create new certificates during profile creation. If you are importing existir
whether the selected certificates contain the appropriate information. If the selected certificates do not, click
Restore Defaults
Default personal certificate (a personal certificate for this profile, public and private key):
Issued to distinguished name:
cn=wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal,ou=wasnd-node01Cell01,ou=was
Issued by distinguished name:
cn=wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal,ou=Root Certificate,ou=wasnd-nc
Expiration period in years:
1
Root signing certificate (personal certificate for signing other certificates, public and private key):
Expiration period in years:
15
< Back
Next >
Cancel
Finish

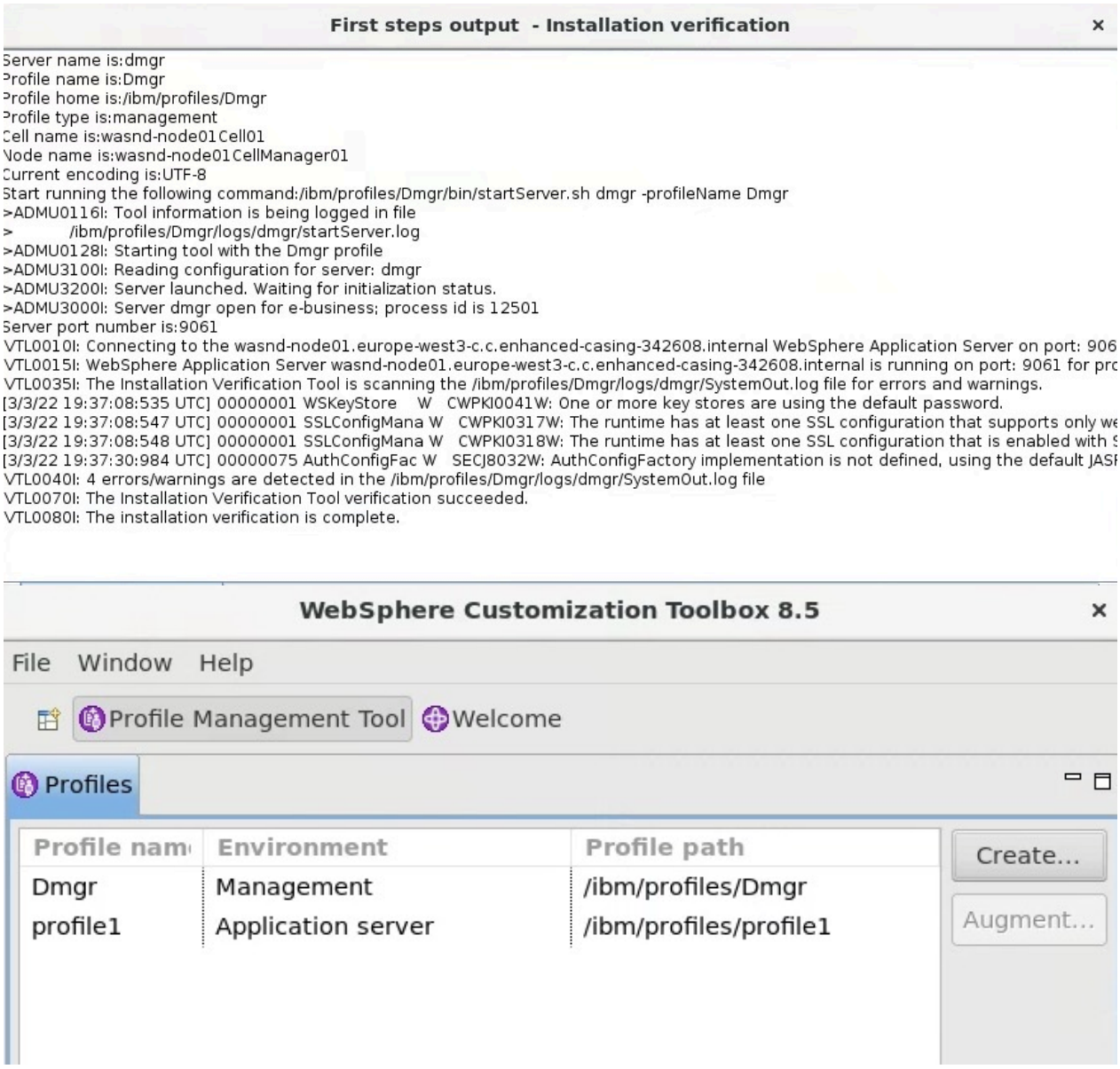

Profile Management Tool 8.5
Port Values Assignment
The values in the following fields define the ports for the deployment manager and do not conflict with other profiles in this installation. Another installation of WebSphere Application Server or other programs might use the same ports. To avoid run-time port conflicts, verify that each port value is unique.
Default Port Values
Recommended Port Values
Administrative console port (Default 9060):
9061
Administrative console secure port (Default 9043):
9044
Bootstrap port (Default 9809):
9809
SOAP connector port (Default 8879):
8879
Administrative interprocess communication port (Default 9632)(X):
9632
SAS SSL ServerAuth port (Default 9401):
9405
CSIV2 ServerAuth listener port (Default 9403):
9404
CSIV2 MultiAuth listener port (Default 9402):
9406
ORB listener port (Default 9100):
9101
< Back
Next >
Cancel
Finish


Profile Management Tool 8.5
Profile Creation Summary
Review the information in the summary for correctness. If the information is correct, click Create to start creating a new profile. Click Back to change values on the previous panels.
Application server environment to create: Management
Server type: Deployment manager
Location: /ibm/profiles/Dmgr
Disk space required: 30 MB
Profile name: Dmgr
Make this profile the default: False
Cell name: wasnd-node01Cell01
Node name: wasnd-node01CellManager01
Host name: wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal
Deploy the administrative console (recommended): True
Enable administrative security (recommended): True
Administrative console port: 9061
< Back
Create
Cancel
Finish


Profile Management Tool 8.5
Profile Creation Progress
Running configuration command: importConfigArchive_Management
< Back
Next >
Cancel
Finish

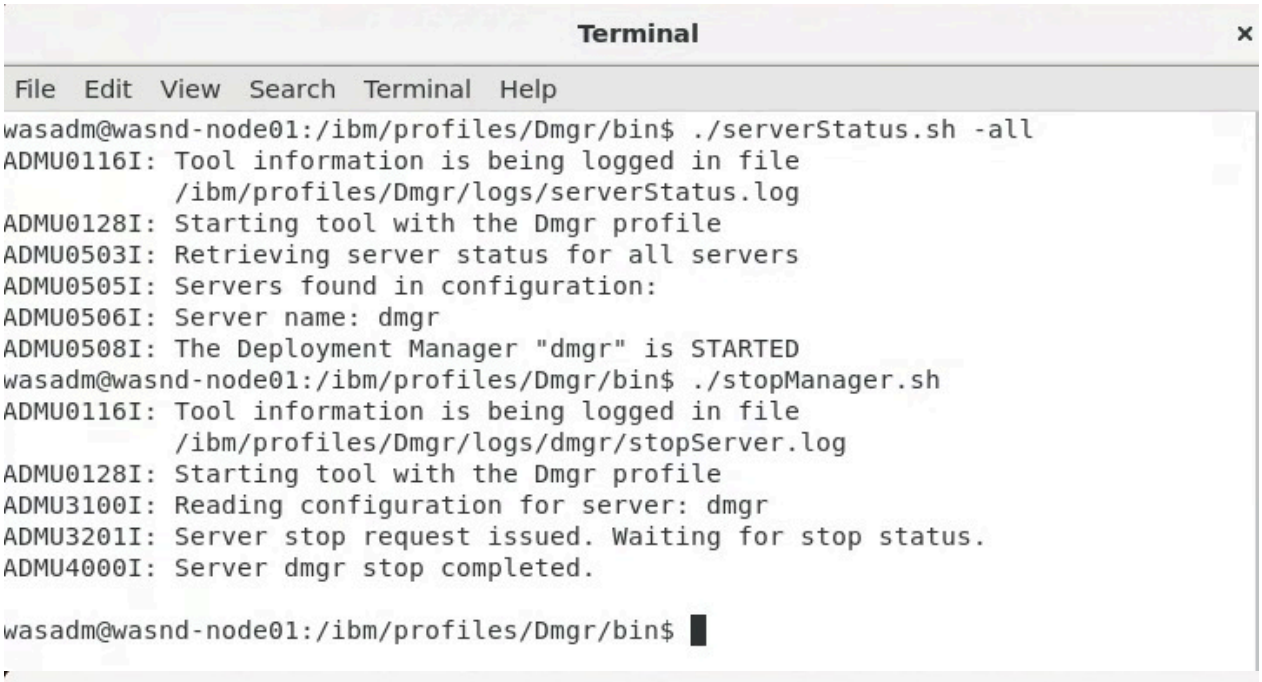

Profile Management Tool 8.5
Profile Creation Complete
The Profile Management Tool created the profile successfully.
The next step in creating a Network Deployment environment is to start the deployment manager so that nodes can be federated into its cell. After the deployment manager is started, you can administer the nodes that belong to the cell.
You can start and stop the deployment manager from the command line or the First steps console. The First steps console also has links to an installation verification test and other information and features that relate to the deployment manager.
Launch the First steps console.
To start the Profile Management Tool later, use the PMT command in the app_server_root/bin/ ProfileManagement directory or the option in the First steps console.
< Back
Next >
Cancel
Finish

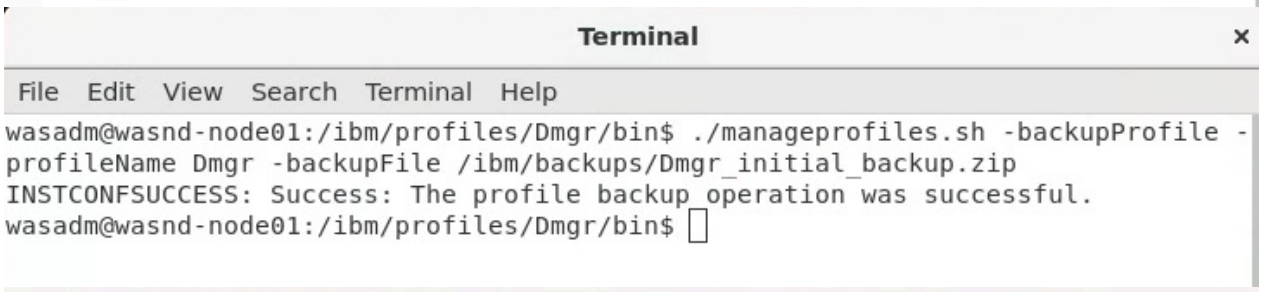

WebSphere Application Server - First steps - Dmgr
WebSphere Application Server
IBM
First steps
Installation verification
Confirm that your server is installed and that it can start properly.
Start the deployment manager
Start the deployment manager and its applications.
Administrative console
Install and administer applications.
WebSphere Customization Toolbox
Launch this toolbox to access the Profile Management Tool and work with profiles, or to access the Migration Management Tool and migrate WebSphere Application Server 6.0, 6.1, 7.0 or 8.0 profiles to version 8.5.
Information center for WebSphere Application Server
Learn more about WebSphere Application Server and explore sample applications.
IBM Education Assistant for WebSphere software
Access multimedia content for WebSphere Application Server version 8.5 and other IBM software products.
Exit

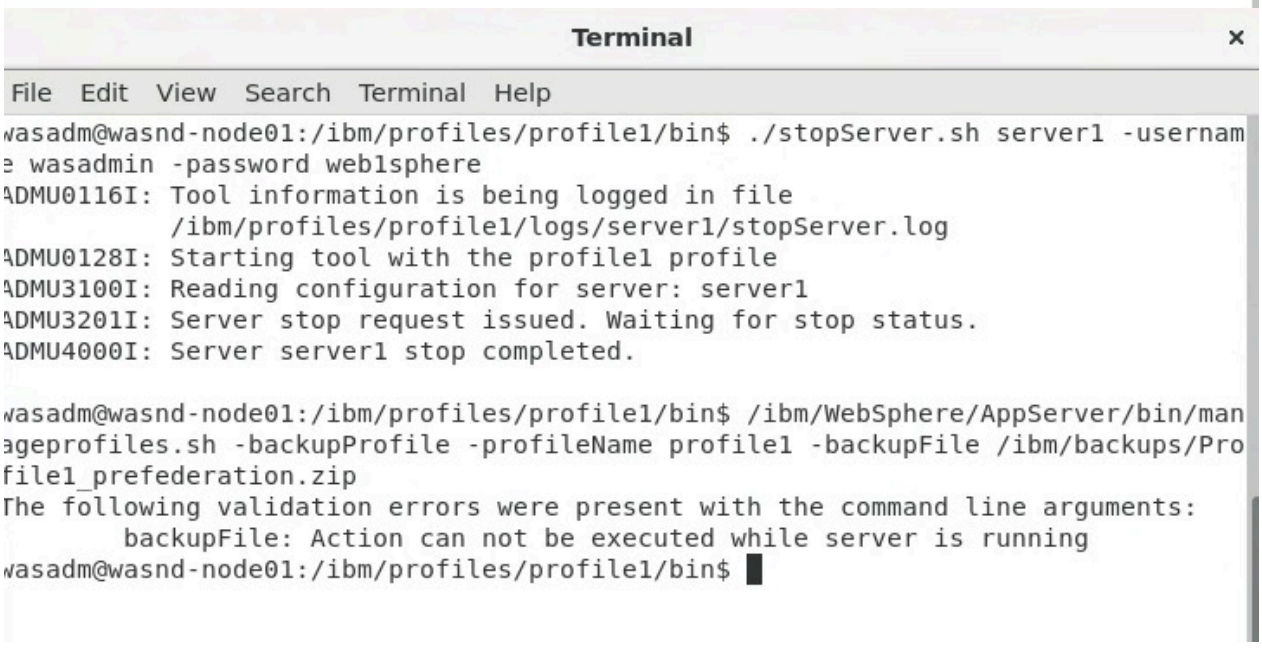


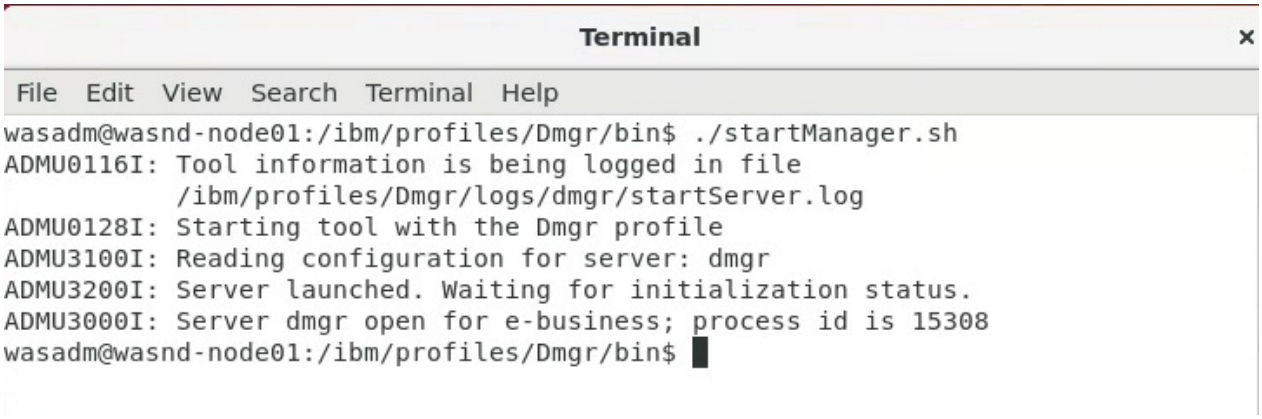
Section 2: Back up the Dmgr profile configuration

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


Terminal
File Edit View Search Terminal Help
wasadm@wasnd-node01:/ibm/profiles/Dmgr/bin$ ./serverStatus.sh -all
ADMU0116I: Tool information is being logged in file
/ibm/profiles/Dmgr/logs/serverStatus.log
ADMU0128I: Starting tool with the Dmgr profile
ADMU0503I: Retrieving server status for all servers
ADMU0505I: Servers found in configuration:
ADMU0506I: Server name: dmgr
ADMU0508I: The Deployment Manager "dmgr" is STARTED
wasadm@wasnd-node01:/ibm/profiles/Dmgr/bin$ ./stopManager.sh
ADMU0116I: Tool information is being logged in file
/ibm/profiles/Dmgr/logs/dmgr/stopServer.log
ADMU0128I: Starting tool with the Dmgr profile
ADMU3100I: Reading configuration for server: dmgr
ADMU3201I: Server stop request issued. Waiting for stop status.
ADMU4000I: Server dmgr stop completed.
wasadm@wasnd-node01:/ibm/profiles/Dmgr/bin$

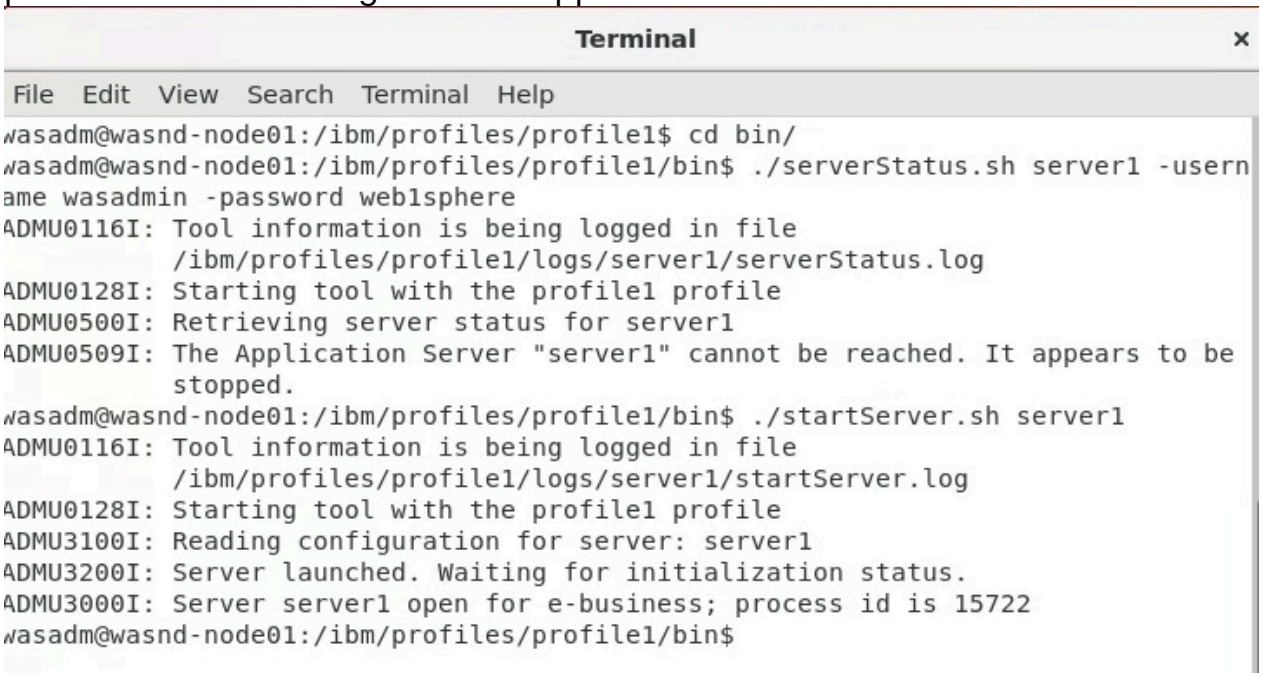

Terminal
File Edit View Search Terminal Help
wasadm@wasnd-node01:/ibm/profiles/Dmgr/bin$ ./manageprofiles.sh -backupProfile -
profileName Dmgr -backupFile /ibm/backups/Dmgr_initial_backup.zip
INSTCONFSUCCESS: Success: The profile backup operation was successful.
wasadm@wasnd-node01:/ibm/profiles/Dmgr/bin$

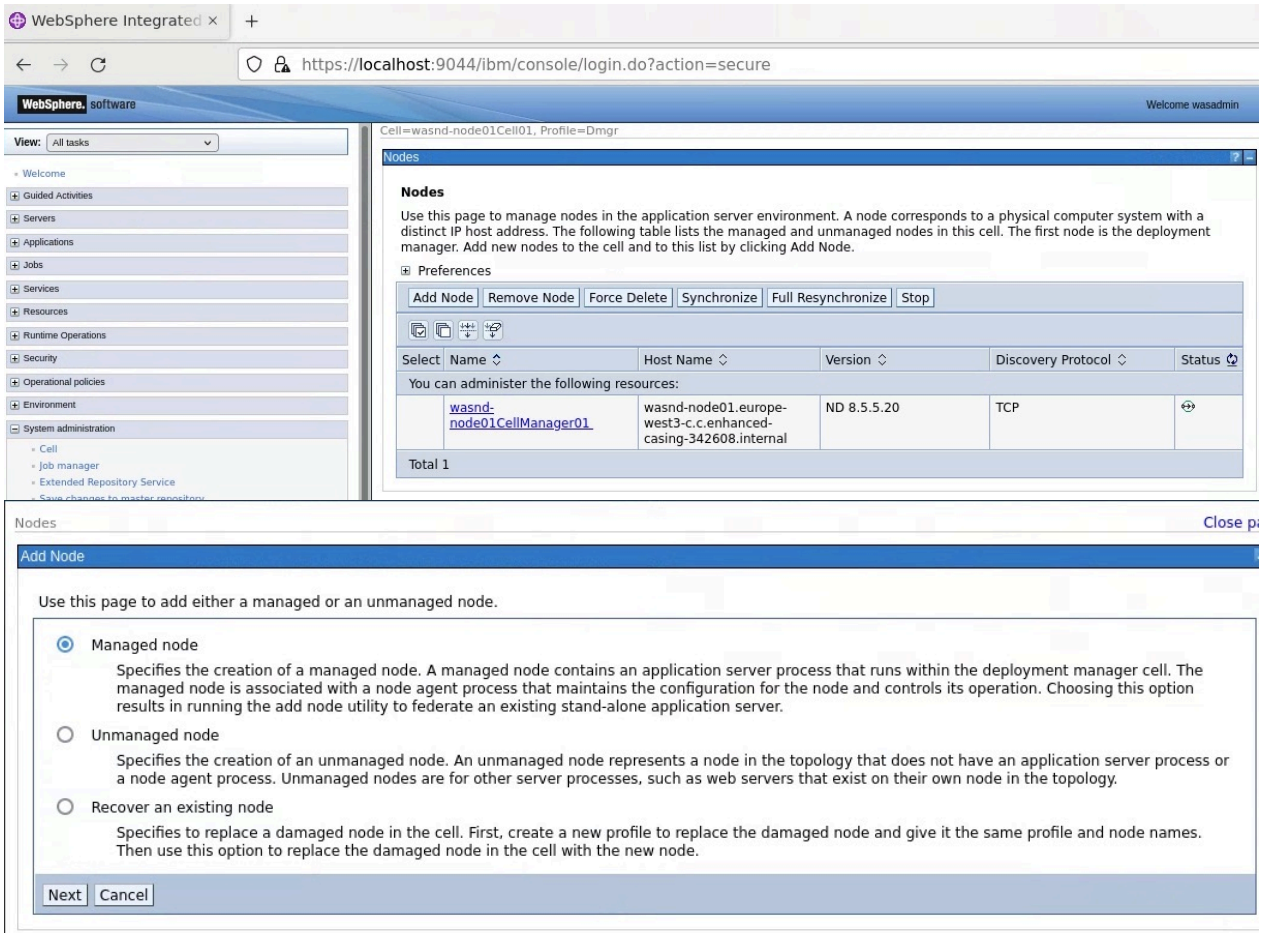

Terminal
File Edit View Search Terminal Help
wasadm@wasnd-node01:/ibm/profiles/profile1/bin$ ./stopServer.sh server1 -usernam
e wasadmin -password web1sphere
ADMU0116I: Tool information is being logged in file
/ibm/profiles/profile1/logs/server1/stopServer.log
ADMU0128I: Starting tool with the profile1 profile
ADMU3100I: Reading configuration for server: server1
ADMU3201I: Server stop request issued. Waiting for stop status.
ADMU4000I: Server server1 stop completed.
wasadm@wasnd-node01:/ibm/profiles/profile1/bin$ /ibm/WebSphere/AppServer/bin/man
ageprofiles.sh -backupProfile -profileName profile1 -backupFile /ibm/backups/Pro
file1_prefederation.zip
The following validation errors were present with the command line arguments:
backupFile: Action can not be executed while server is running
wasadm@wasnd-node01:/ibm/profiles/profile1/bin$



Section 3: Federate 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 was85hostNode01), into the cell named was85hostCell01, which the deployment manager profile defines. The federation process adds a node agent to the application server node.




WebSphere Integrated
https://localhost:9044/ibm/console/login.do?action=secure
WebSphere. software
Welcome wasadmin
View: All tasks
Welcome
Guided Activities
Servers
Applications
Jobs
Services
Resources
Runtime Operations
Security
Operational policies
Environment
System administration
Cell
Job manager
Extended Repository Service
Cell=wasnd-node01Cell01, Profile=Dmgr
Nodes
Nodes
Use this page to manage nodes in the application server environment. A node corresponds to a physical computer system with a distinct IP host address. The following table lists the managed and unmanaged nodes in this cell. The first node is the deployment manager. Add new nodes to the cell and to this list by clicking Add Node.
Preferences
Add Node
Remove Node
Force Delete
Synchronize
Full Resynchronize
Stop
Select
Name
Host Name
Version
Discovery Protocol
Status
You can administer the following resources:
wasnd-node01CellManager01
wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal
ND 8.5.5.20
TCP
Total 1
Nodes
Close p
Add Node
Use this page to add either a managed or an unmanaged node.
Managed node
Specifies the creation of a managed node. A managed node contains an application server process that runs within the deployment manager cell. The managed node is associated with a node agent process that maintains the configuration for the node and controls its operation. Choosing this option results in running the add node utility to federate an existing stand-alone application server.
Unmanaged node
Specifies the creation of an unmanaged node. An unmanaged node represents a node in the topology that does not have an application server process or a node agent process. Unmanaged nodes are for other server processes, such as web servers that exist on their own node in the topology.
Recover an existing node
Specifies to replace a damaged node in the cell. First, create a new profile to replace the damaged node and give it the same profile and node names. Then use this option to replace the damaged node in the cell with the new node.
Next
Cancel

Nodes

Add Managed Node

Use this page to identify a stand-alone application server process that is running. Start the application server, if necessary, or add the node from the command line by running the addNode command from the bin directory of the stopped application server profile.

Node connection

* Host
st3-c.c.enhanced-casing-342608.internal

* JMX connector type
SOAP

* JMX connector port
8880

Application server user name
wasdmin

Application server password
●●●●●●

* Deployment manager user name
wasdmin

* Deployment manager password
●●●●●●

Config URL
file:/${USER_INSTALL_ROOT}/properties/sas.client.props

Options

☑ Include applications

☑ Include b[illegible]ses

Adding node

ADMU0001I: Begin federation of node wasnd-node01Node01 with Deployment Manager at wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal:8879.

ADMU0009I: Successfully connected to Deployment Manager Server: wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal:8879

ADMU0505I: Servers found in configuration:

ADMU0506I: Server name: webserver1

ADMU0506I: Server name: server1

ADMU2010I: Stopping all server processes for node wasnd-node01Node01

ADMU0510I: Server server1 is now STOPPED

ADMU0024I: Deleting the old backup dir

Please Wait...

ADMU0015I: Backing up the original cell

ADMU0012I: Creating Node Agent configuration for node: wasnd-node01Node01

ADMU0120I: isclite.ear will not be uploaded since it already exists in the target repository.

ADMU0120I: WebSphereWSDM.ear will not be uploaded since it already exists in the target repository.

ADMU0014I: Adding node wasnd-node01Node01 configuration to cell: wasnd-node01Cell01

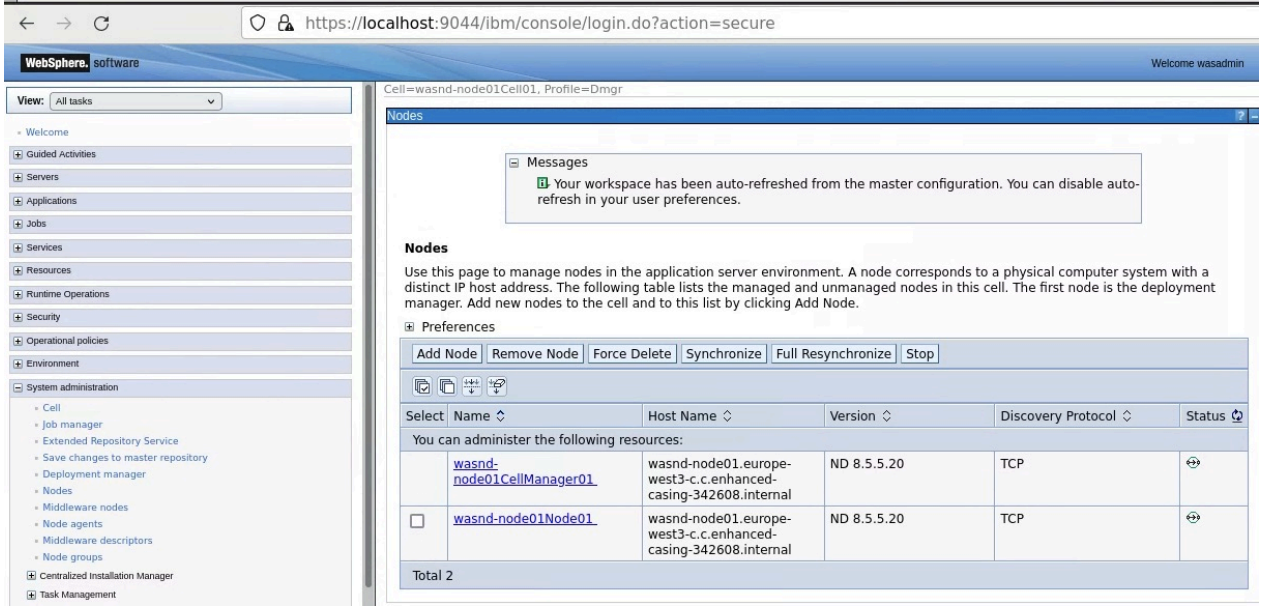
ADMU0120I: isclite on CU will not be uploaded since it already exists in the target repository.

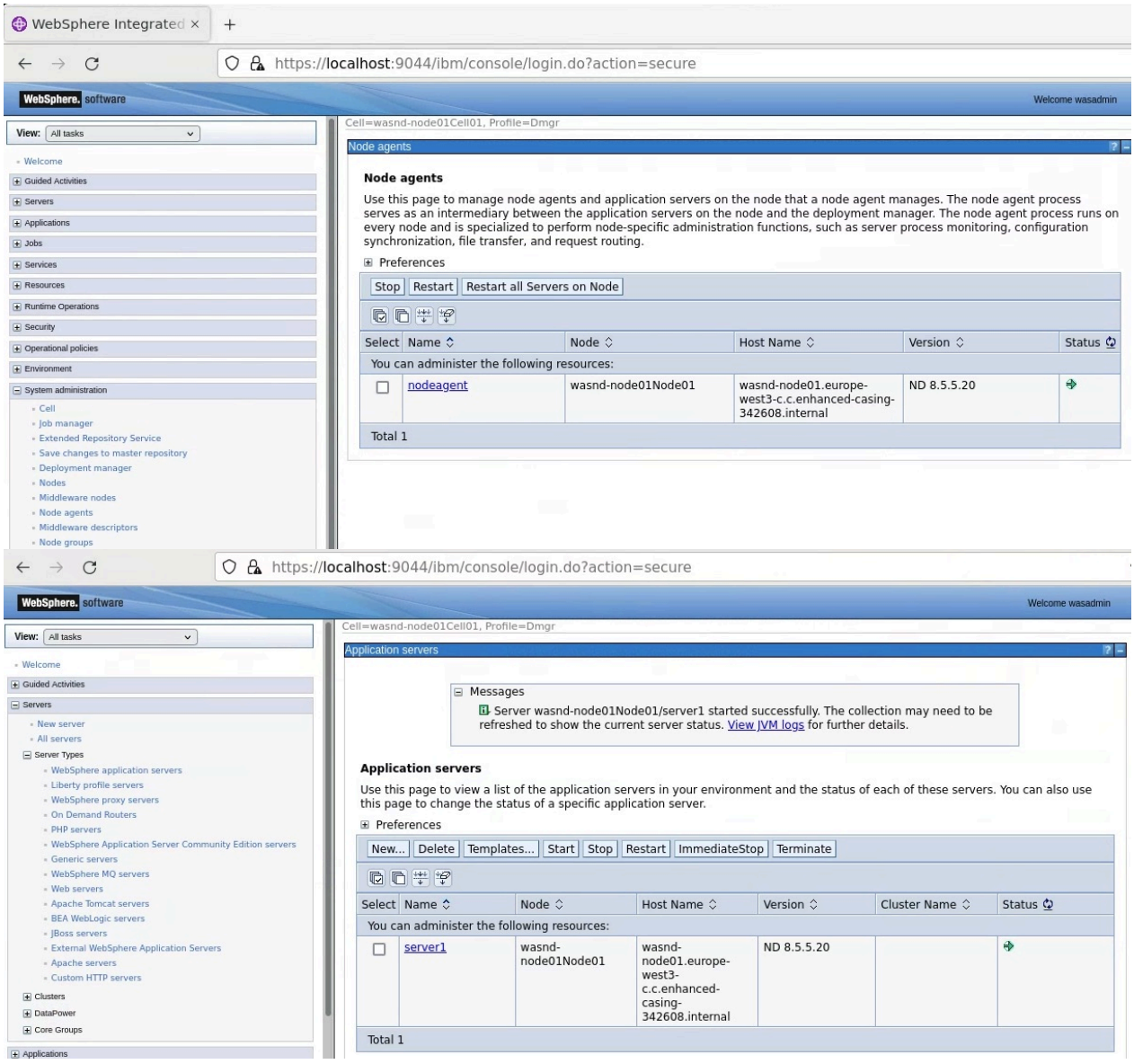
ADMU0120I: WebSphereWSDM on CU will not be uploaded since it already exists in the target repository.

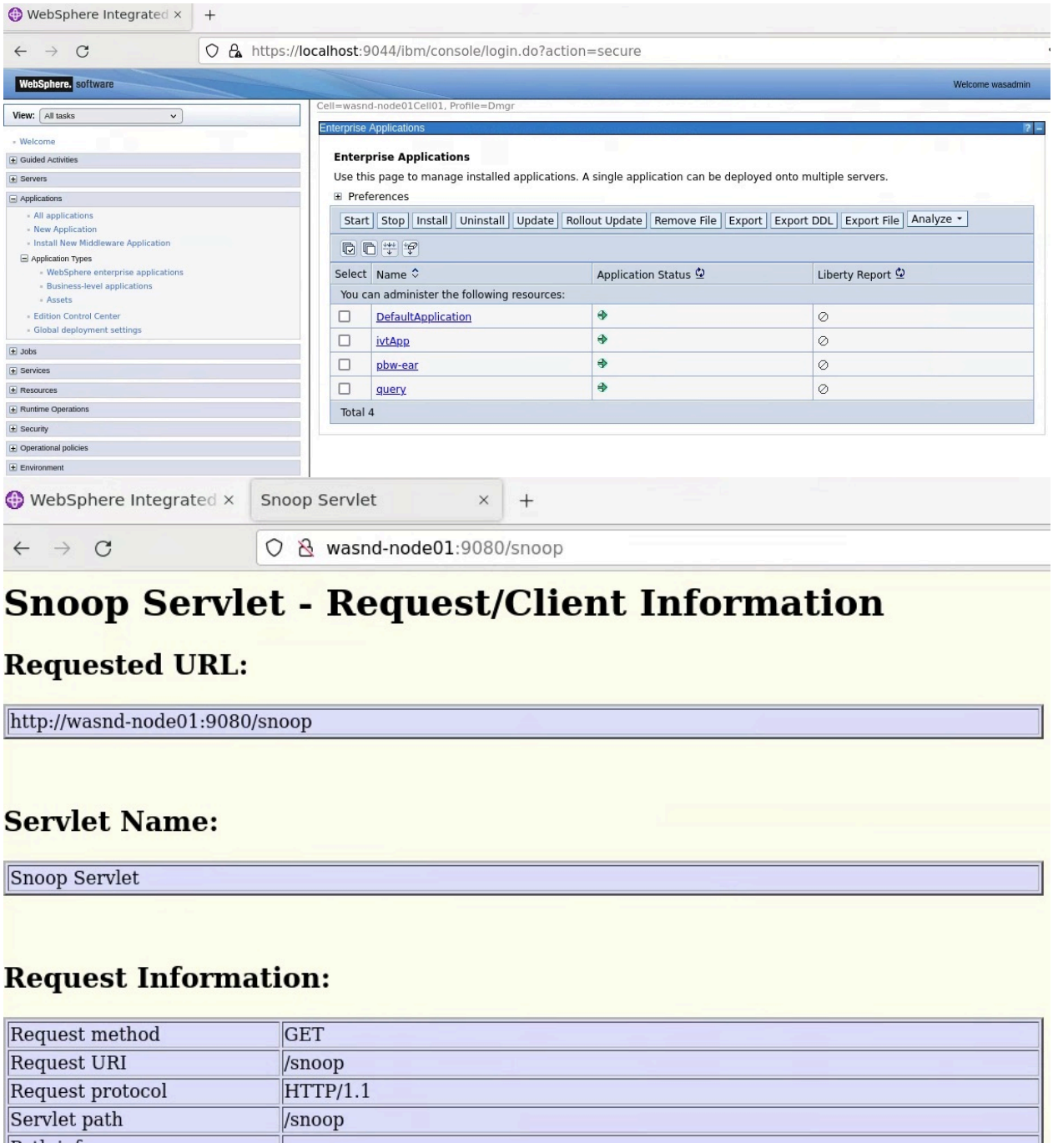
ADMU0120I: isclite on BLA will not be uploaded since it already exists in the target repository.

ADMU0120I: WebSphereWSDM on BLA will not be uploaded since it already exists in the target repository.

```
ADMU0510I: Server server1 is now STOPPED
ADMU0024I: Deleting the old backup directory.
ADMU0015I: Backing up the original cell repository.
ADMU0012I: Creating Node Agent configuration for node: wasnd-node01Node01
ADMU0120I: isclite.ear will not be uploaded since it already exists in the target repository.
ADMU0120I: WebSphereWSDM.ear will not be uploaded since it already exists in the target repository.
ADMU0014I: Adding node wasnd-node01Node01 configuration to cell: wasnd-node01Cell01
ADMU0120I: isclite on CU will not be uploaded since it already exists in the target repository.
ADMU0120I: WebSphereWSDM on CU will not be uploaded since it already exists in the target repository.
ADMU0120I: isclite on BLA will not be uploaded since it already exists in the target repository.
ADMU0120I: WebSphereWSDM on BLA will not be uploaded since it already exists in the target repository.
ADMU0016I: Synchronizing configuration between node and cell.
ADMU0018I: Launching Node Agent process for node: wasnd-node01Node01
ADMU0020I: Reading configuration for Node Agent process: nodeagent
ADMU0022I: Node Agent launched. Waiting for initialization status.
ADMU0030I: Node Agent initialization completed successfully. Process id is: 16593
ADMU0308I: The node wasnd-node01Node01 and associated applications were successfully added to the wasnd-node01Cell01 cell.
ADMU0306I: Note:
ADMU0302I: Any cell-level documents from the standalone wasnd-node01Cell01 configuration have not been migrated to the new cell.
ADMU0307I: You might want to:
ADMU0303I: Update the configuration on the wasnd-node01Cell01 Deployment Manager with values from the old cell-level documents.
ADMU0003I: Node wasnd-node01Node01 has been successfully federated.
View the available nodes.
```



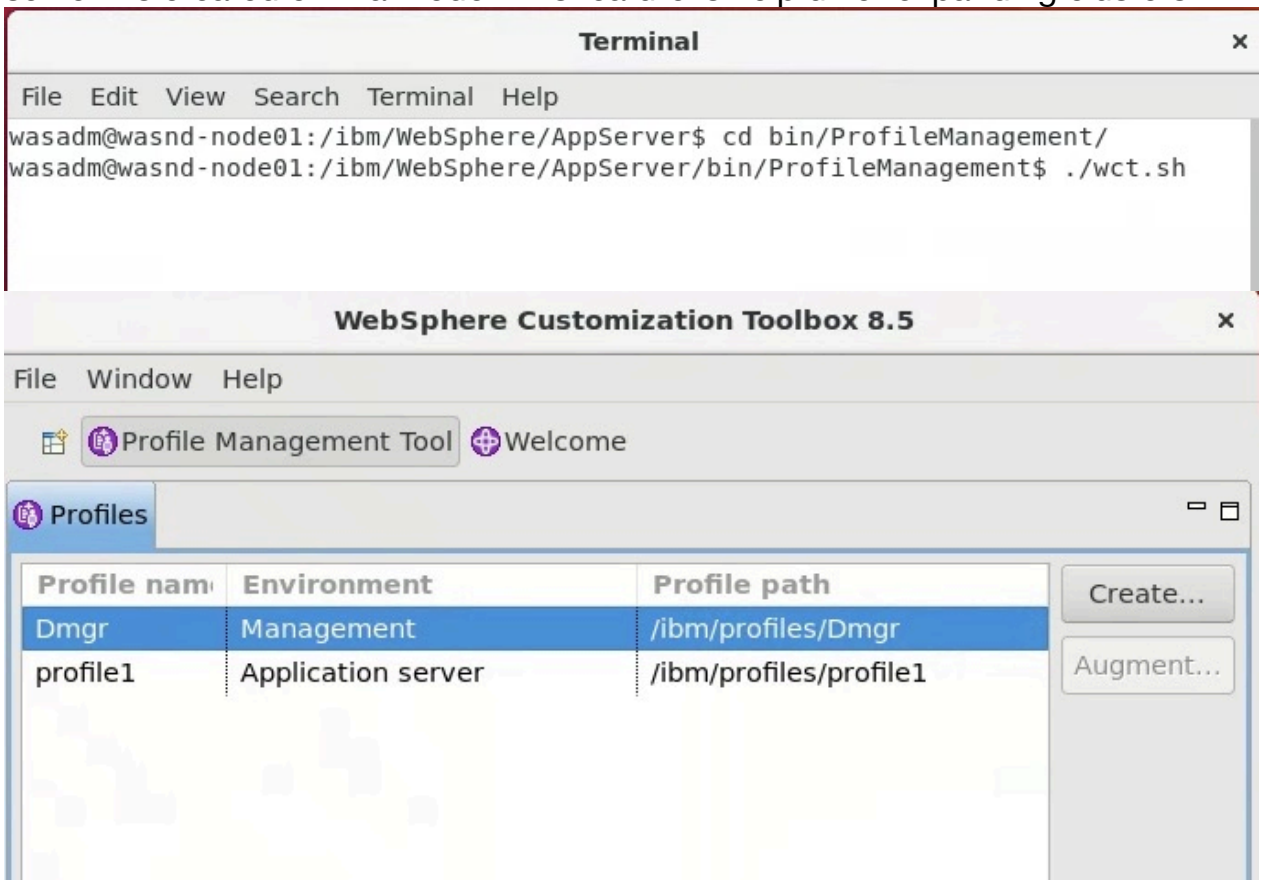

WebSphere Integrated
https://localhost:9044/ibm/console/login.do?action=secure
WebSphere. software
Welcome wasadmin
View: All tasks
Welcome
Guided Activities
Servers
Applications
Jobs
Services
Resources
Runtime Operations
Security
Operational policies
Environment
System administration
Cell
Job manager
Extended Repository Service
Save changes to master repository
Deployment manager
Nodes
Middleware nodes
Node agents
Middleware descriptors
Node groups
Cell=wasnd-node01Cell01, Profile=Dmgr
Node agents
Node agents
Use this page to manage node agents and application servers on the node that a node agent manages. The node agent process serves as an intermediary between the application servers on the node and the deployment manager. The node agent process runs on every node and is specialized to perform node-specific administration functions, such as server process monitoring, configuration synchronization, file transfer, and request routing.
Preferences
Stop
Restart
Restart all Servers on Node
Select
Name
Node
Host Name
Version
Status
You can administer the following resources:
nodeagent
wasnd-node01Node01
wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal
ND 8.5.5.20
Total 1
https://localhost:9044/ibm/console/login.do?action=secure
WebSphere. software
Welcome wasadmin
View: All tasks
Welcome
Guided Activities
Servers
New server
All servers
Server Types
WebSphere application servers
Liberty profile servers
WebSphere proxy servers
On Demand Routers
PHP servers
WebSphere Application Server Community Edition servers
Generic servers
WebSphere MQ servers
Web servers
Apache Tomcat servers
BEA WebLogic servers
JBoss servers
External WebSphere Application Servers
Apache servers
Custom HTTP servers
Clusters
DataPower
Core Groups
Applications
Cell=wasnd-node01Cell01, Profile=Dmgr
Application servers
Messages
Server wasnd-node01Node01/server1 started successfully. The collection may need to be refreshed to show the current server status. View JVM logs for further details.
Application servers
Use this page to view a list of the application servers in your environment and the status of each of these servers. You can also use this page to change the status of a specific application server.
Preferences
New...
Delete
Templates...
Start
Stop
Restart
ImmediateStop
Terminate
Select
Name
Node
Host Name
Version
Cluster Name
Status
You can administer the following resources:
server1
wasnd-node01Node01
wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal
ND 8.5.5.20
Total 1

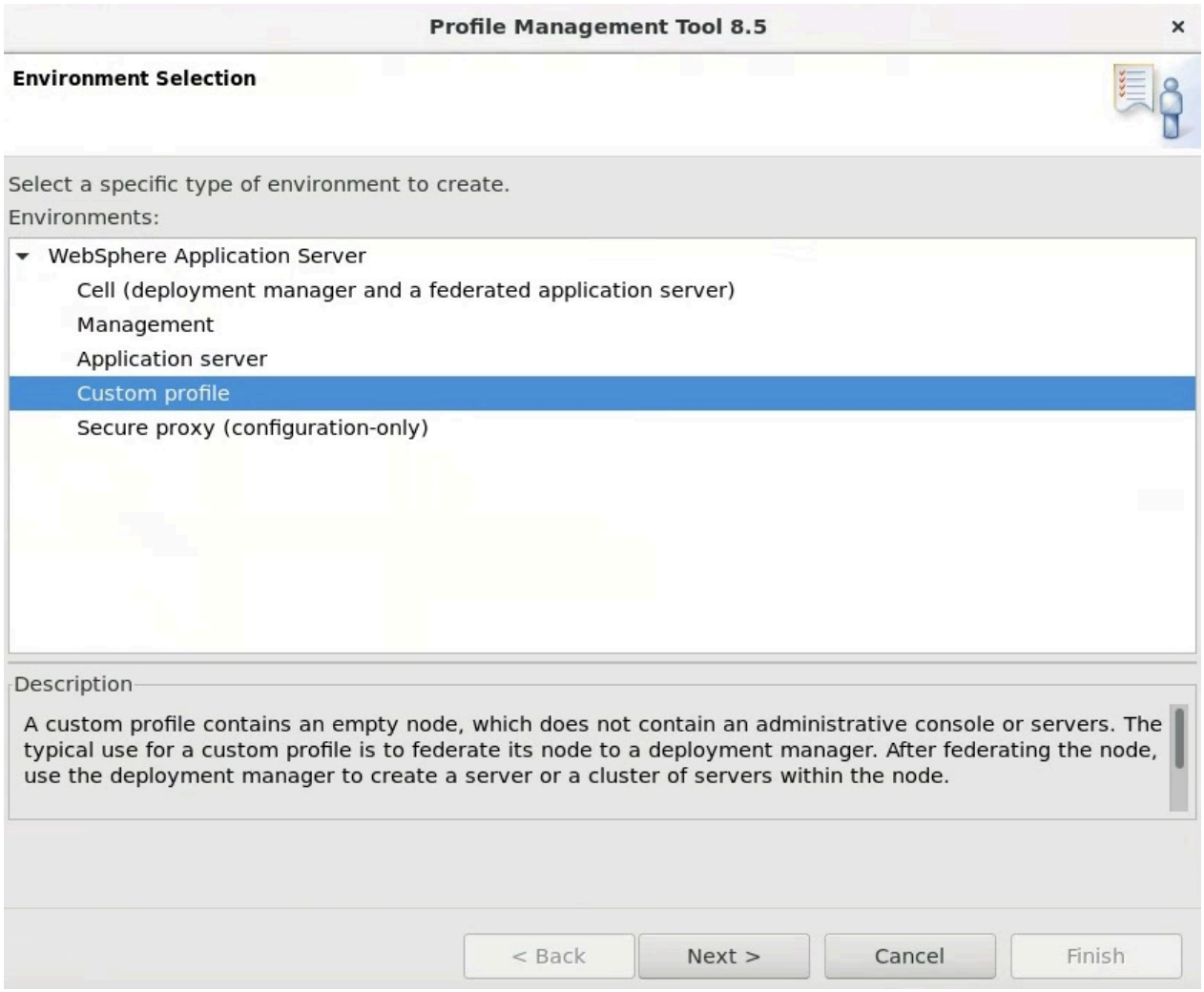


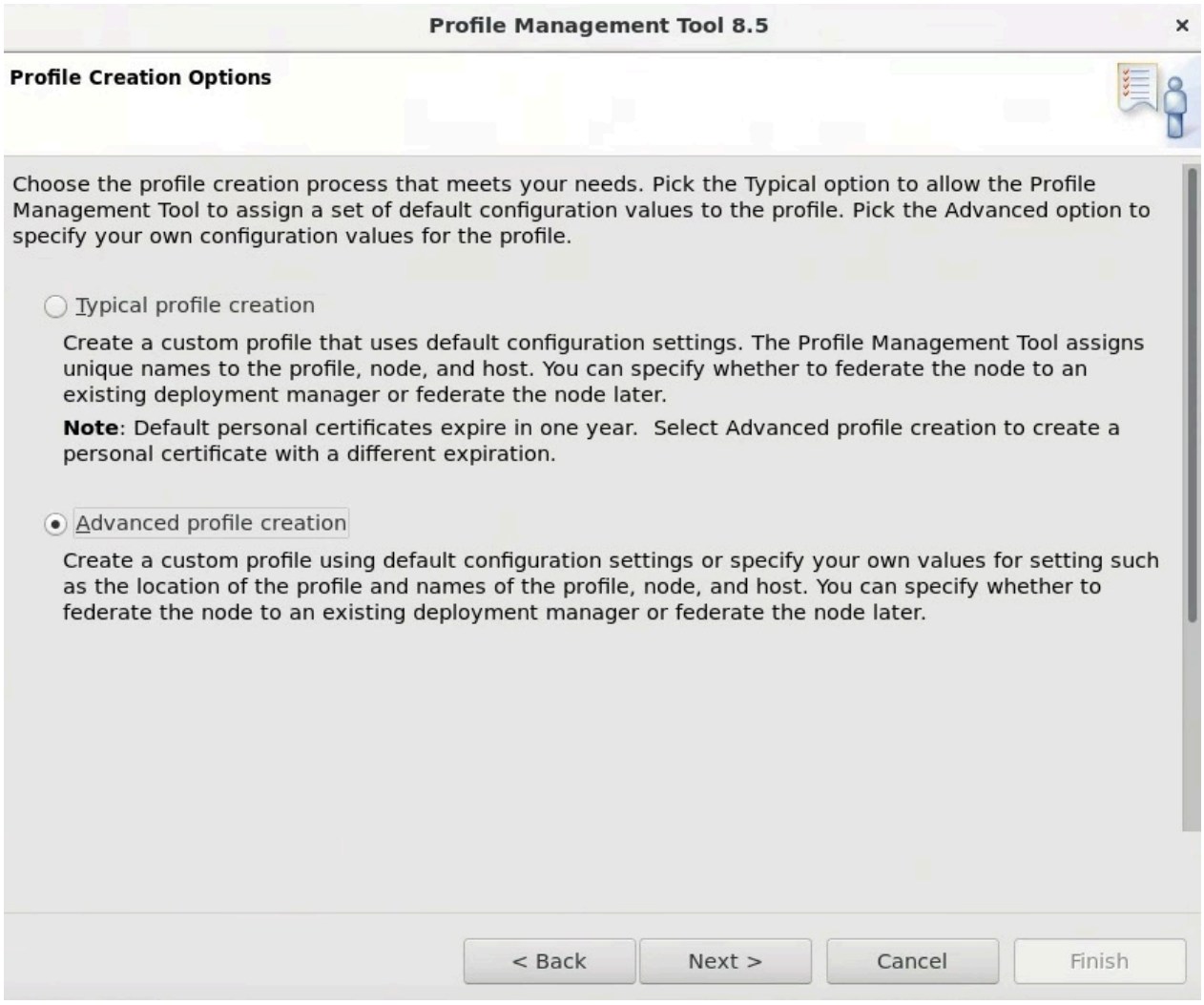
Section 4: Create a custom profile and federate it into the deployment manager cell

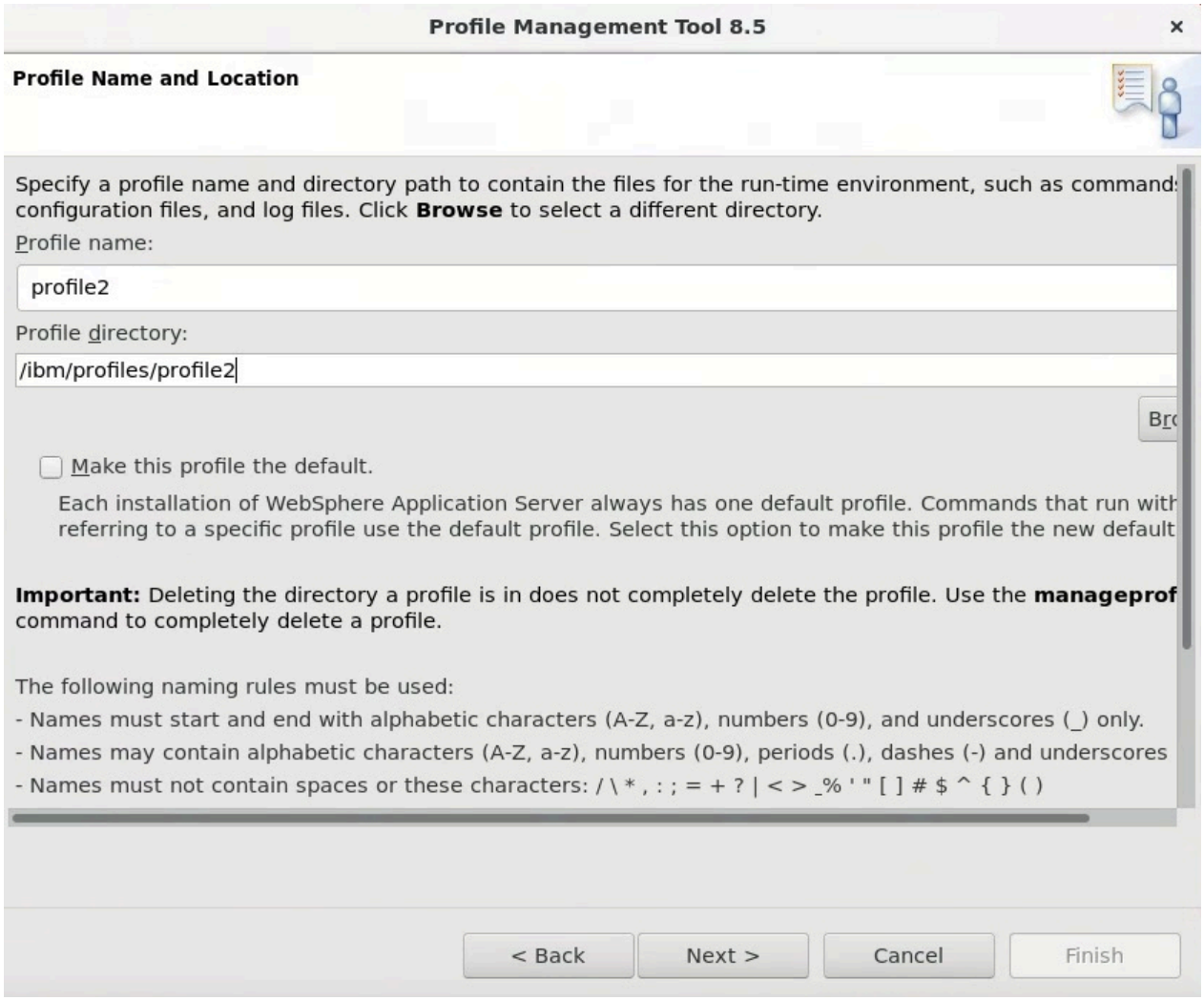
During this section of the exercise, you are going to create a custom profile, profile2, that defines a node, named was85hostNode02. The custom profile is automatically federated into the cell was85hostCell01.

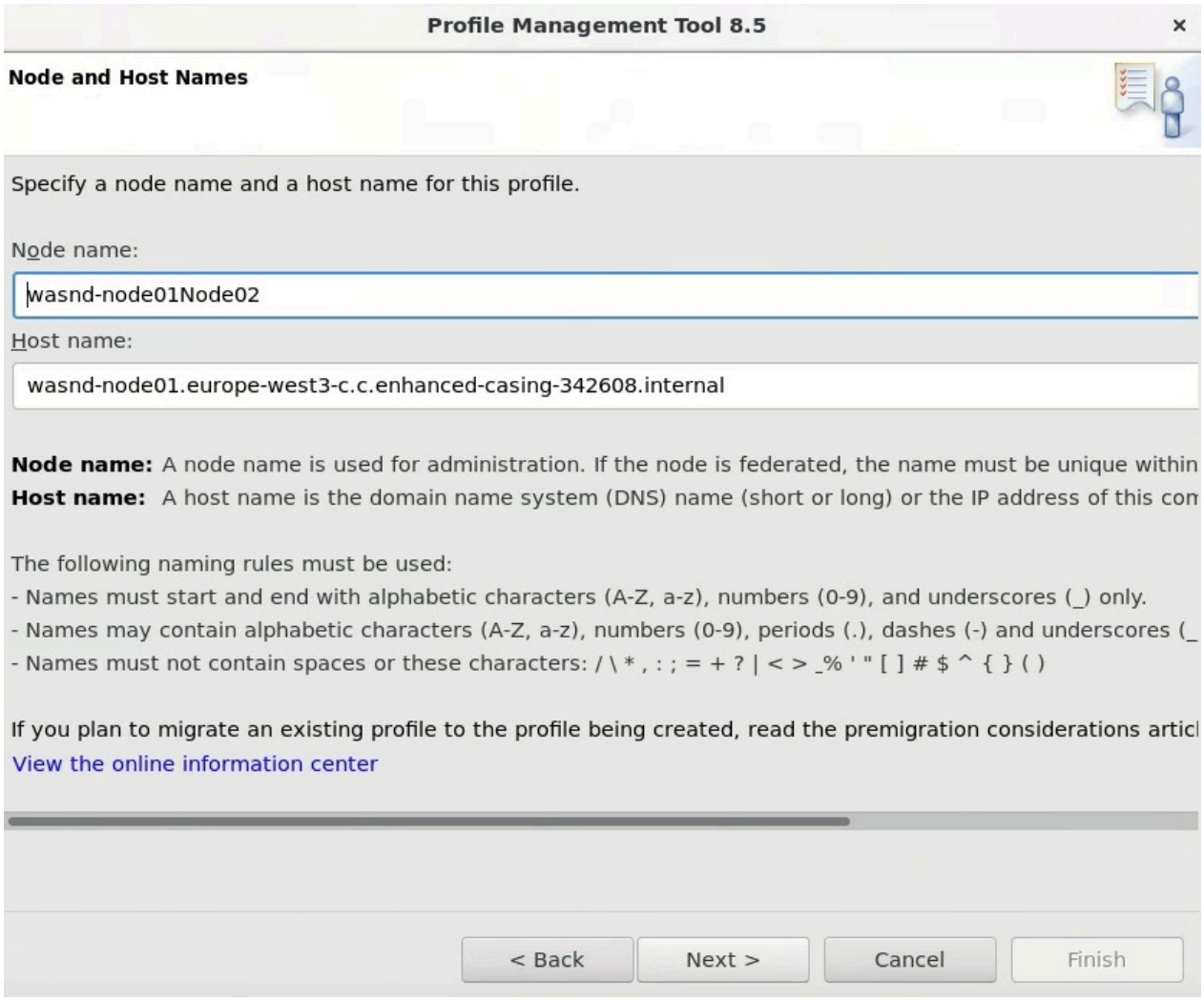
A custom profile is useful because it does not create any application servers on the node; it creates the configuration and the node agent only. Consequently, no server1 is created on that node. This feature is helpful for expanding clusters.

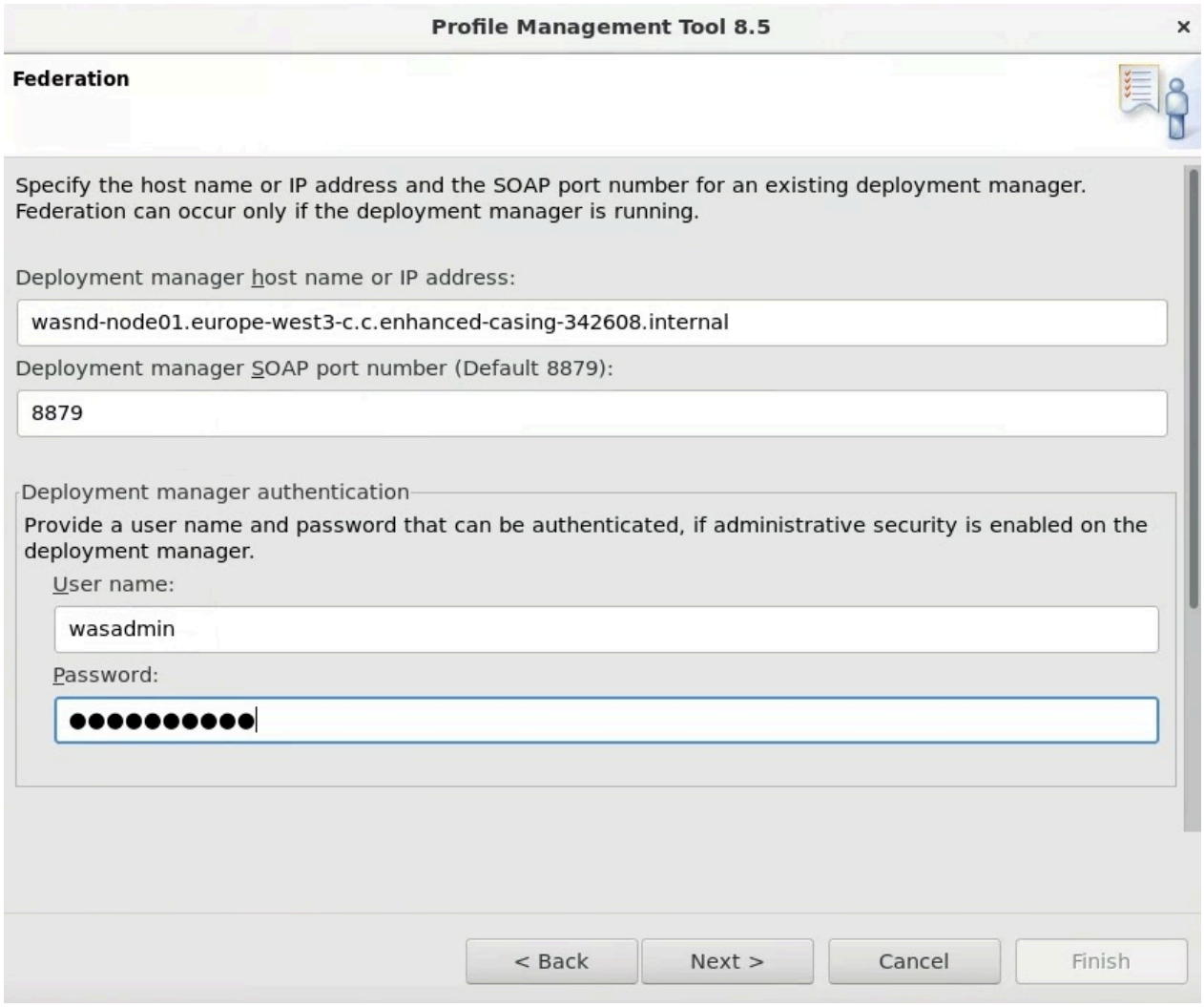



Profile Management Tool 8.5
Environment Selection
Select a specific type of environment to create.
Environments:
WebSphere Application Server
Cell (deployment manager and a federated application server)
Management
Application server
Custom profile
Secure proxy (configuration-only)
Description
A custom profile contains an empty node, which does not contain an administrative console or servers. The typical use for a custom profile is to federate its node to a deployment manager. After federating the node, use the deployment manager to create a server or a cluster of servers within the node.
< Back
Next >
Cancel
Finish

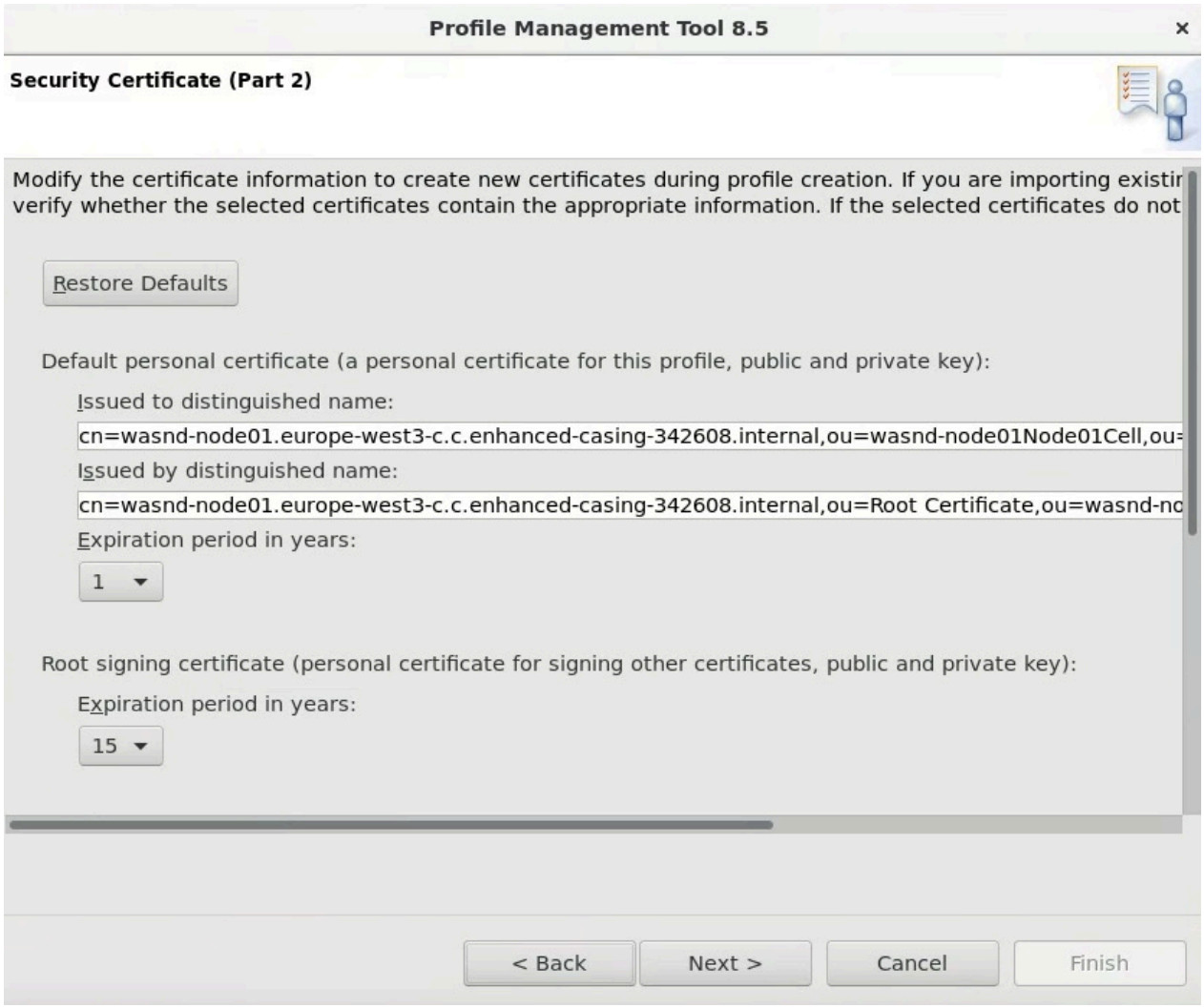

Profile Management Tool 8.5
Profile Creation Options
Choose the profile creation process that meets your needs. Pick the Typical option to allow the Profile Management Tool to assign a set of default configuration values to the profile. Pick the Advanced option to specify your own configuration values for the profile.
Typical profile creation
Create a custom profile that uses default configuration settings. The Profile Management Tool assigns unique names to the profile, node, and host. You can specify whether to federate the node to an existing deployment manager or federate the node later.
Note: Default personal certificates expire in one year. Select Advanced profile creation to create a personal certificate with a different expiration.
Advanced profile creation
Create a custom profile using default configuration settings or specify your own values for setting such as the location of the profile and names of the profile, node, and host. You can specify whether to federate the node to an existing deployment manager or federate the node later.
< Back
Next >
Cancel
Finish

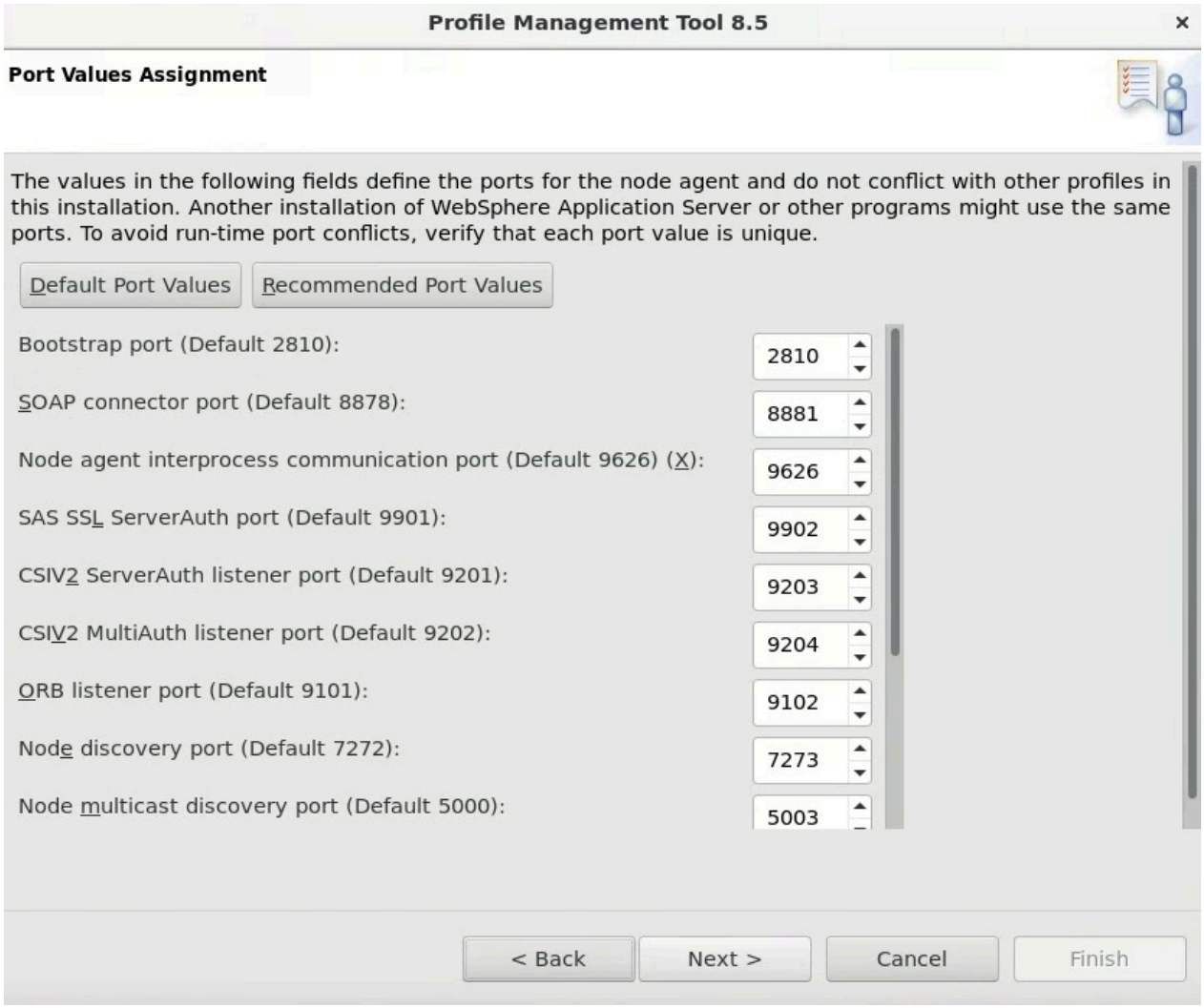

Profile Management Tool 8.5
Profile Name and Location
Specify a profile name and directory path to contain the files for the run-time environment, such as command
configuration files, and log files. Click Browse to select a different directory.
Profile name:
profile2
Profile directory:
/ibm/profiles/profile2
Br
Make this profile the default.
Each installation of WebSphere Application Server always has one default profile. Commands that run with
referring to a specific profile use the default profile. Select this option to make this profile the new default
Important: Deleting the directory a profile is in does not completely delete the profile. Use the manageprof
command to completely delete a profile.
The following naming rules must be used:
- Names must start and end with alphabetic characters (A-Z, a-z), numbers (0-9), and underscores (_) only.
- Names may contain alphabetic characters (A-Z, a-z), numbers (0-9), periods (.), dashes (-) and underscores
- Names must not contain spaces or these characters: / \ * , : ; = + ? | < > _% ' " [ ] # $ ^ { } ( )
< Back
Next >
Cancel
Finish

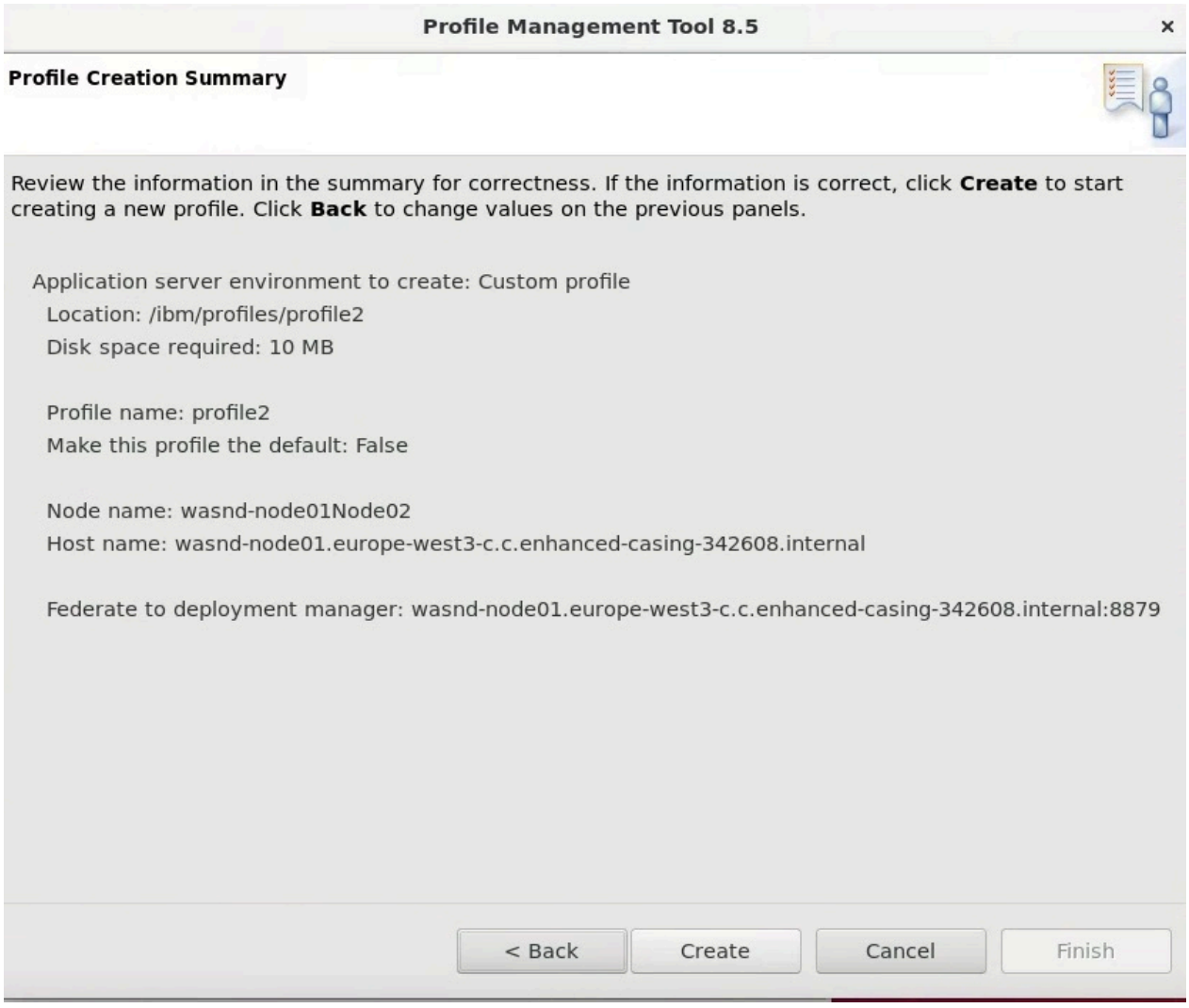

Profile Management Tool 8.5
Node and Host Names
Specify a node name and a host name for this profile.
Node name:
wasnd-node01Node02
Host name:
wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal
Node name: A node name is used for administration. If the node is federated, the name must be unique within
Host name: A host name is the domain name system (DNS) name (short or long) or the IP address of this com
The following naming rules must be used:
- Names must start and end with alphabetic characters (A-Z, a-z), numbers (0-9), and underscores (_) only.
- Names may contain alphabetic characters (A-Z, a-z), numbers (0-9), periods (.), dashes (-) and underscores (_
- Names must not contain spaces or these characters: / \ * , : ; = + ? | < > _% ' " [ ] # $ ^ { } ( )
If you plan to migrate an existing profile to the profile being created, read the premigration considerations artic
View the online information center
< Back
Next >
Cancel
Finish

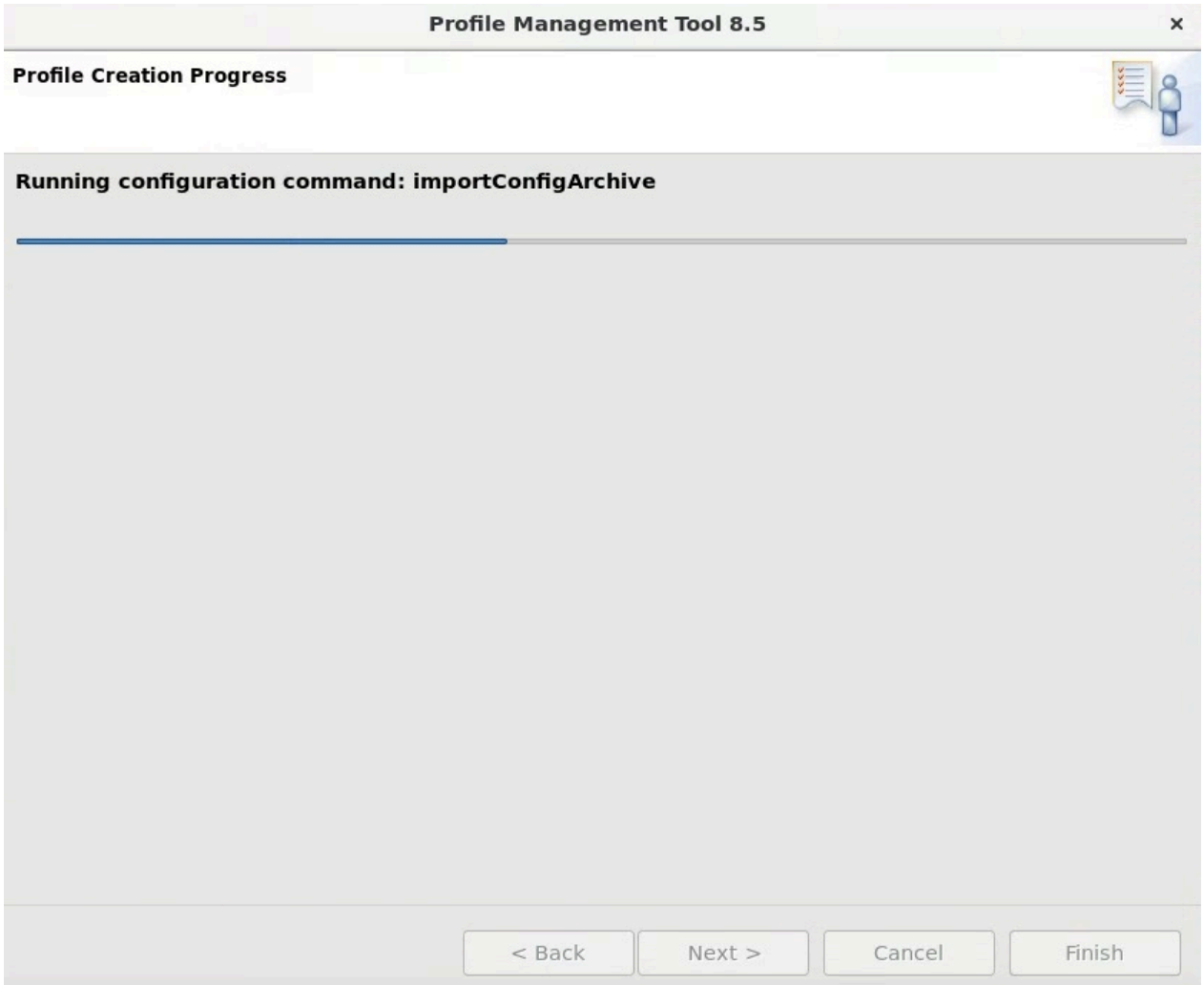

Profile Management Tool 8.5
Federation
Specify the host name or IP address and the SOAP port number for an existing deployment manager.
Federation can occur only if the deployment manager is running.
Deployment manager host name or IP address:
wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal
Deployment manager SOAP port number (Default 8879):
8879
Deployment manager authentication
Provide a user name and password that can be authenticated, if administrative security is enabled on the deployment manager.
User name:
wasadmin
Password:
< Back
Next >
Cancel
Finish

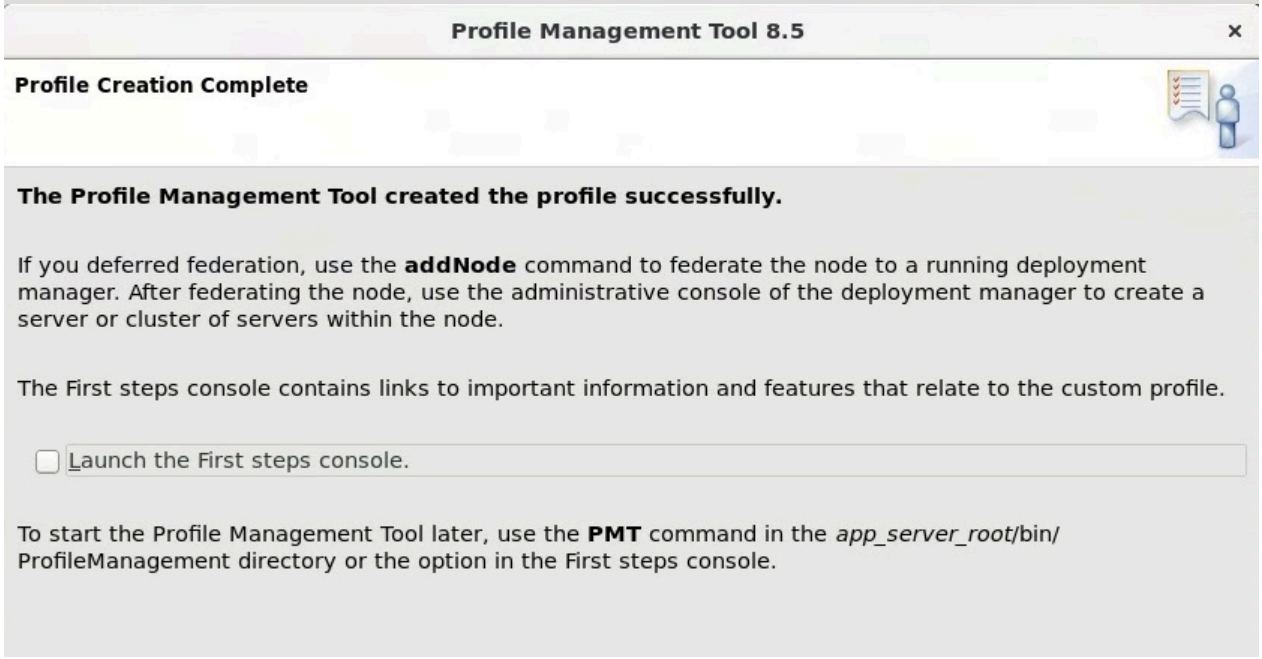

Profile Management Tool 8.5
Security Certificate (Part 1)
Choose whether to create a default personal certificate and root signing certificate, or import them from keystores. To create new certificates, proceed to Part 2 and provide the certificate information. To import existing certificates from keystores, locate the certificates then proceed to Part 2 and verify the certificate information.
Create a new default personal certificate.
Import an existing default personal certificat
Default personal certificate
Path:
Browse...
Password:
Keystore type:
Keystore alias:
Create a new root signing certificate.
Import an existing root signing certificate.
Root signing certificate
< Back
Next >
Cancel
Finish

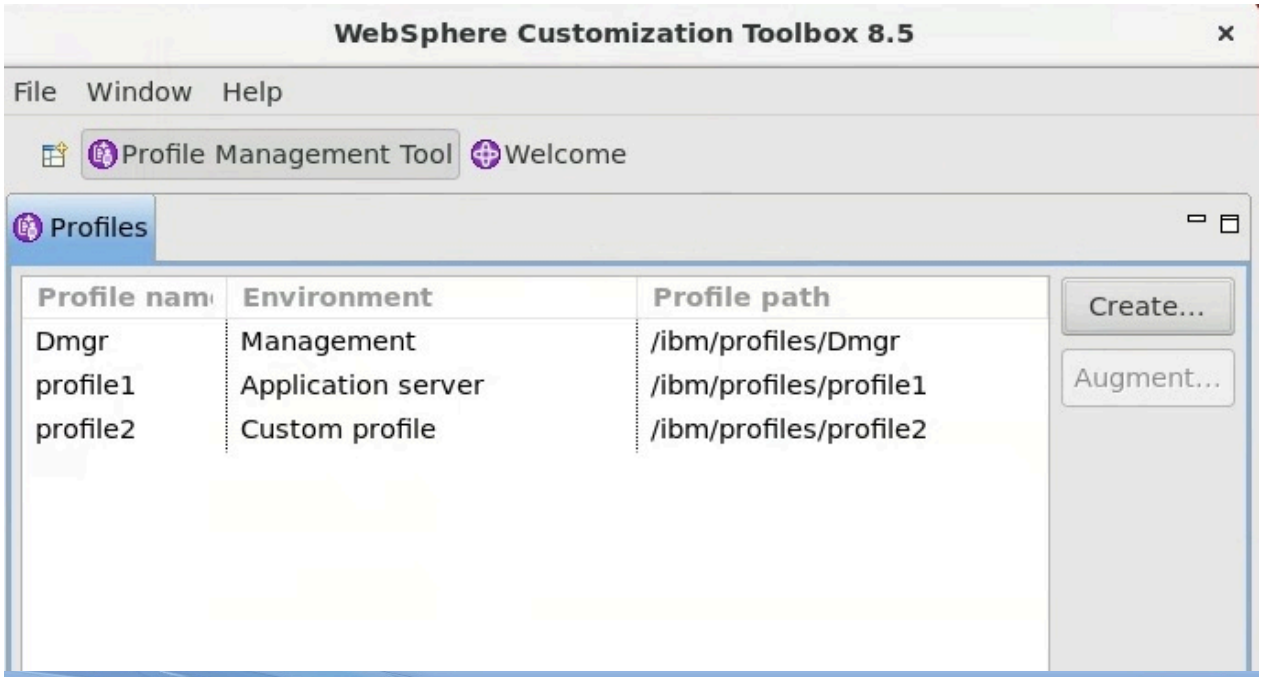

Profile Management Tool 8.5
Security Certificate (Part 2)
Modify the certificate information to create new certificates during profile creation. If you are importing existir
verify whether the selected certificates contain the appropriate information. If the selected certificates do not
Restore Defaults
Default personal certificate (a personal certificate for this profile, public and private key):
Issued to distinguished name:
cn=wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal,ou=wasnd-node01Node01Cell,ou=
Issued by distinguished name:
cn=wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal,ou=Root Certificate,ou=wasnd-no
Expiration period in years:
1
Root signing certificate (personal certificate for signing other certificates, public and private key):
Expiration period in years:
15
< Back
Next >
Cancel
Finish

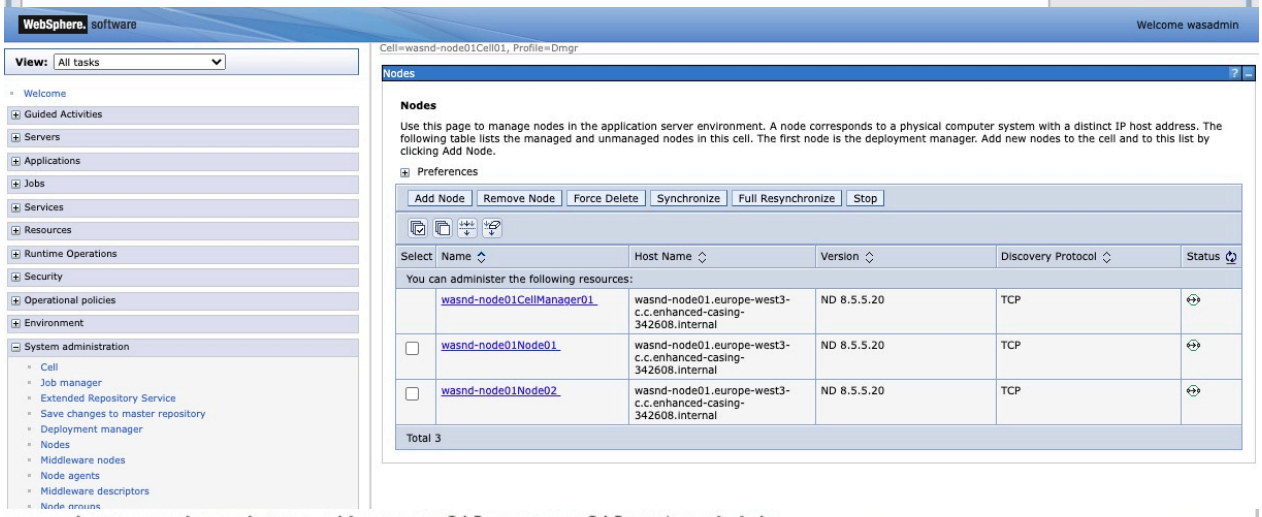

Profile Management Tool 8.5
Port Values Assignment
The values in the following fields define the ports for the node agent and do not conflict with other profiles in this installation. Another installation of WebSphere Application Server or other programs might use the same ports. To avoid run-time port conflicts, verify that each port value is unique.
Default Port Values
Recommended Port Values
Bootstrap port (Default 2810):
2810
SOAP connector port (Default 8878):
8881
Node agent interprocess communication port (Default 9626) (X):
9626
SAS SSL ServerAuth port (Default 9901):
9902
CSIV2 ServerAuth listener port (Default 9201):
9203
CSIV2 MultiAuth listener port (Default 9202):
9204
ORB listener port (Default 9101):
9102
Node discovery port (Default 7272):
7273
Node multicast discovery port (Default 5000):
5003
< Back
Next >
Cancel
Finish


Profile Management Tool 8.5
Profile Creation Summary
Review the information in the summary for correctness. If the information is correct, click Create to start creating a new profile. Click Back to change values on the previous panels.
Application server environment to create: Custom profile
Location: /ibm/profiles/profile2
Disk space required: 10 MB
Profile name: profile2
Make this profile the default: False
Node name: wasnd-node01Node02
Host name: wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal
Federate to deployment manager: wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal:8879
< Back
Create
Cancel
Finish

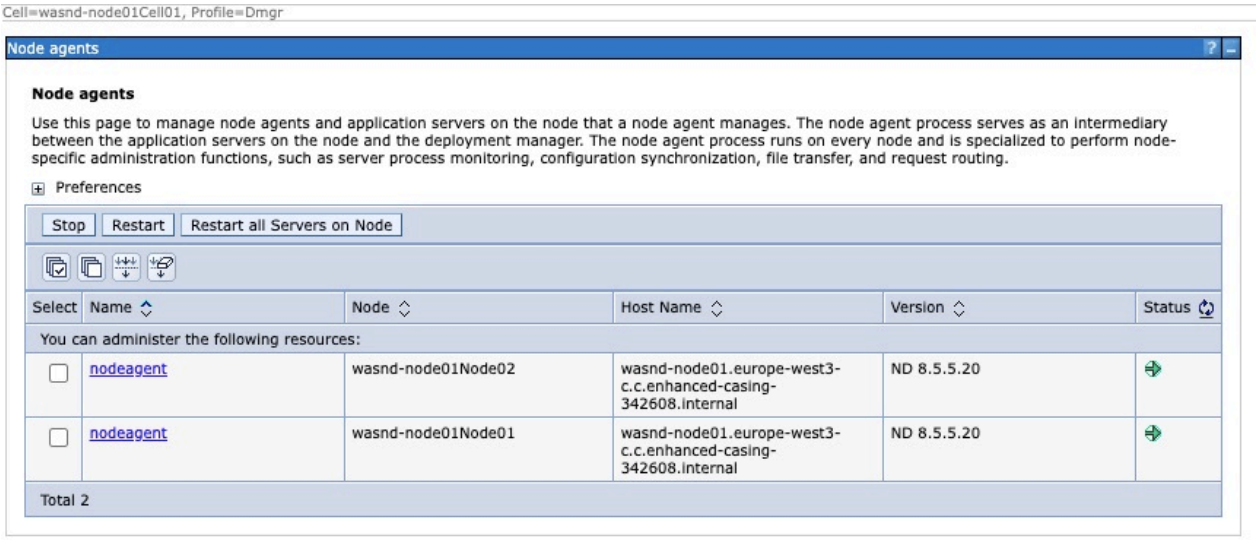

Profile Management Tool 8.5
Profile Creation Progress
Running configuration command: importConfigArchive
< Back
Next >
Cancel
Finish


Profile Management Tool 8.5
Profile Creation Complete
The Profile Management Tool created the profile successfully.
If you deferred federation, use the addNode command to federate the node to a running deployment manager. After federating the node, use the administrative console of the deployment manager to create a server or cluster of servers within the node.
The First steps console contains links to important information and features that relate to the custom profile.
Launch the First steps console.
To start the Profile Management Tool later, use the PMT command in the app_server_root/bin/ ProfileManagement directory or the option in the First steps console.



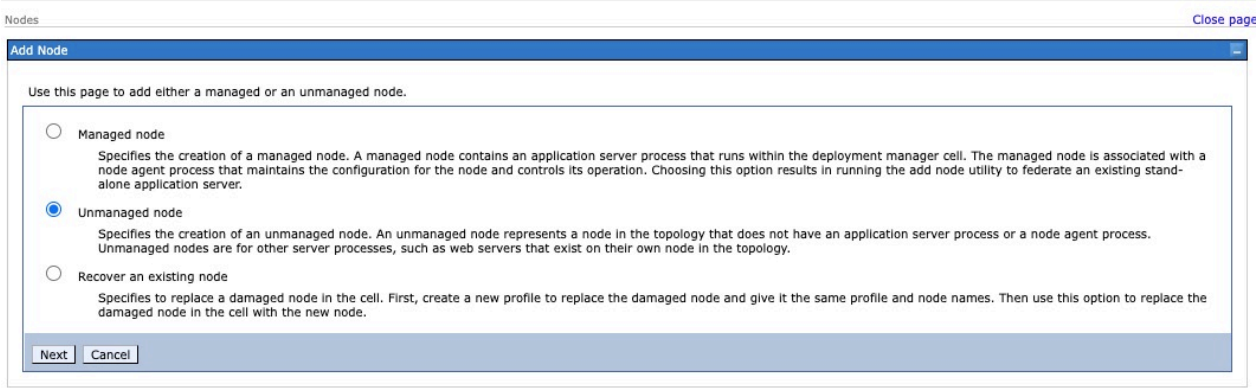


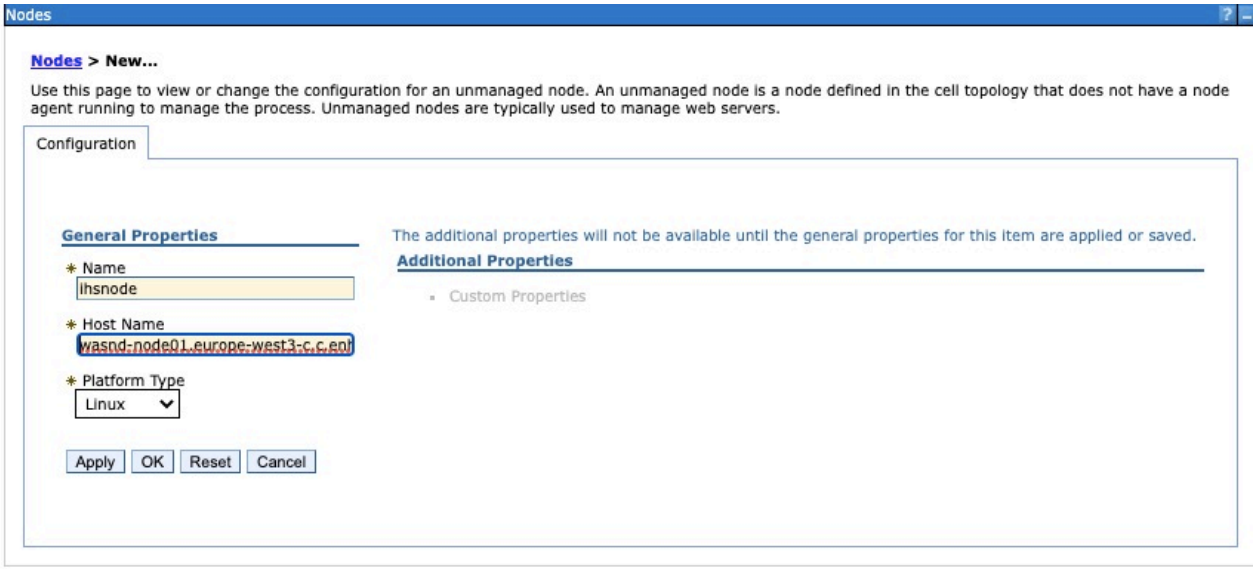

```
wasadm@wasnd-node01:/ibm/profiles/profile2$ cd bin
wasadm@wasnd-node01:/ibm/profiles/profile2/bin$ ./startNode.sh
ADMU0116I: Tool information is being logged in file
           /ibm/profiles/profile2/logs/nodeagent/startServer.log
ADMU0128I: Starting tool with the profile2 profile
ADMU3100I: Reading configuration for server: nodeagent
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server nodeagent open for e-business; process id is 19532
wasadm@wasnd-node01:/ibm/profiles/profile2/bin$
```

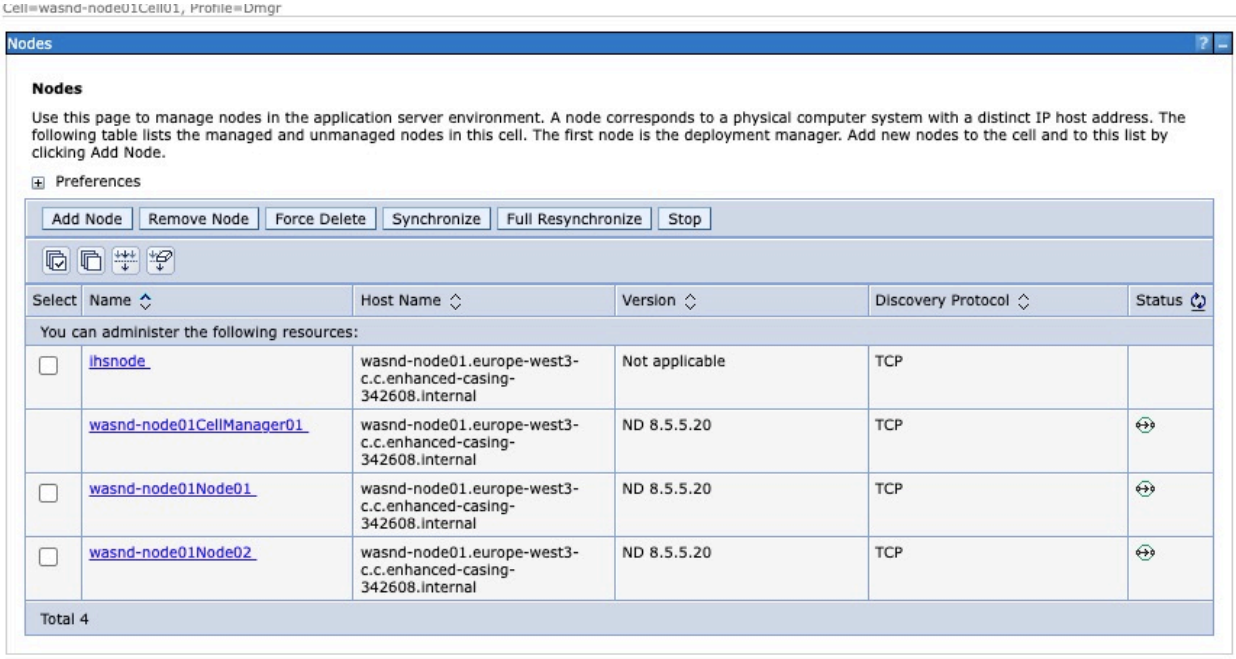


Section 5: Add the IBM HTTP Server to the cell

During this section of the exercise, you add an unmanaged node, ihsnode, to the cell was85hostCell01. 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.



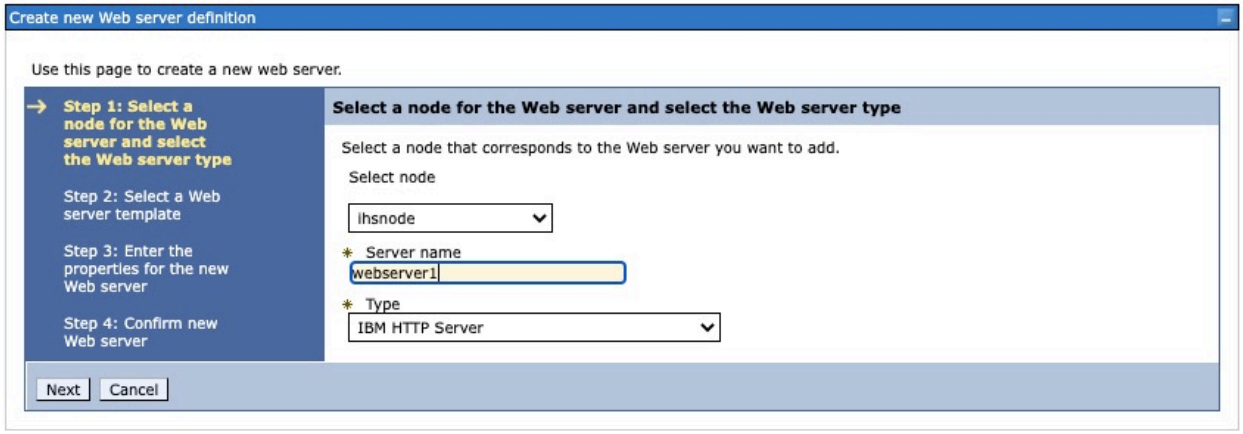




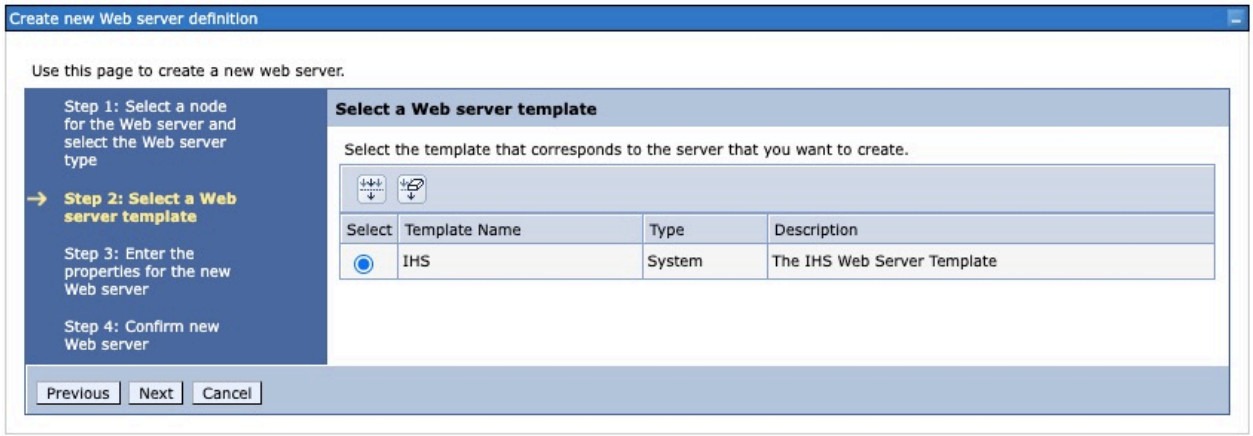
Section 6: Add the web server to the configuration

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

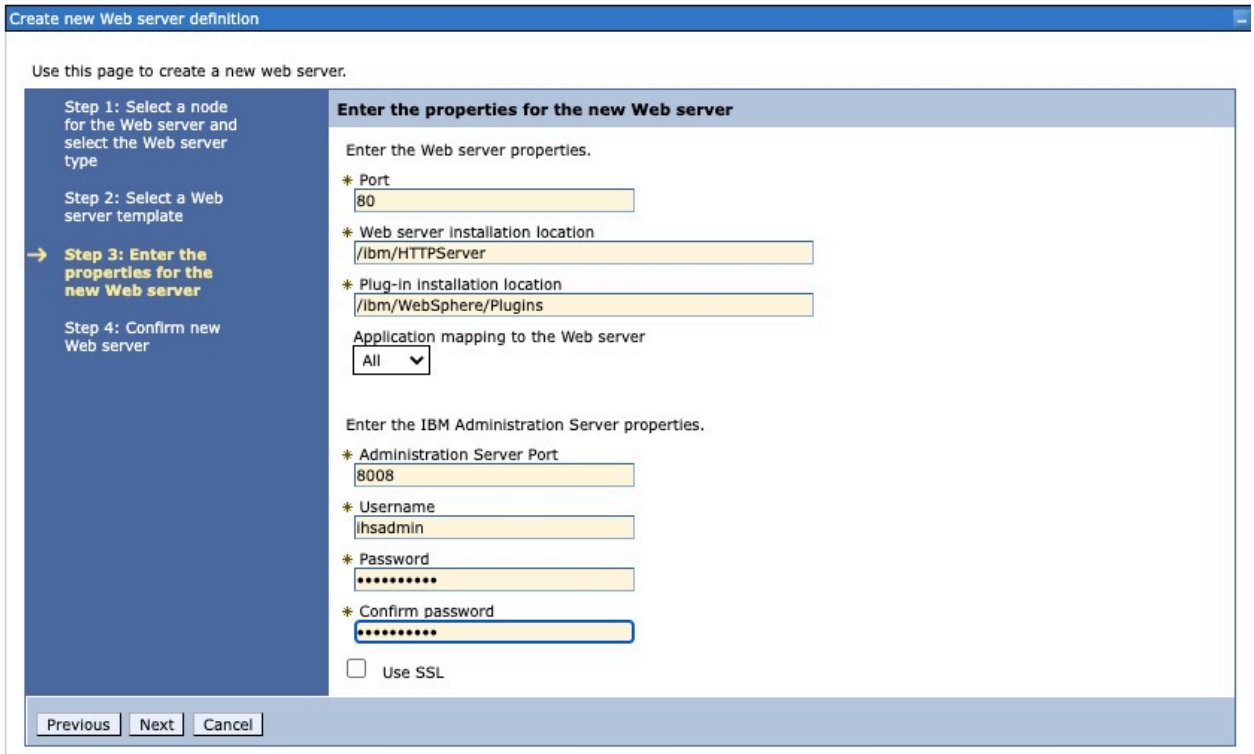
Cell=wasnd-node01Cell01, Profile=Dmgr

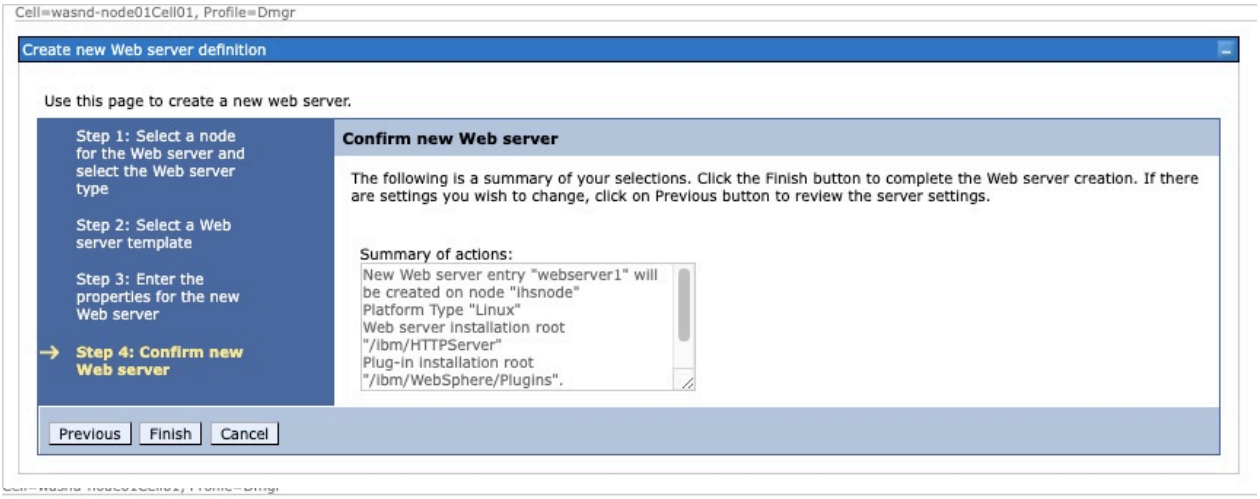


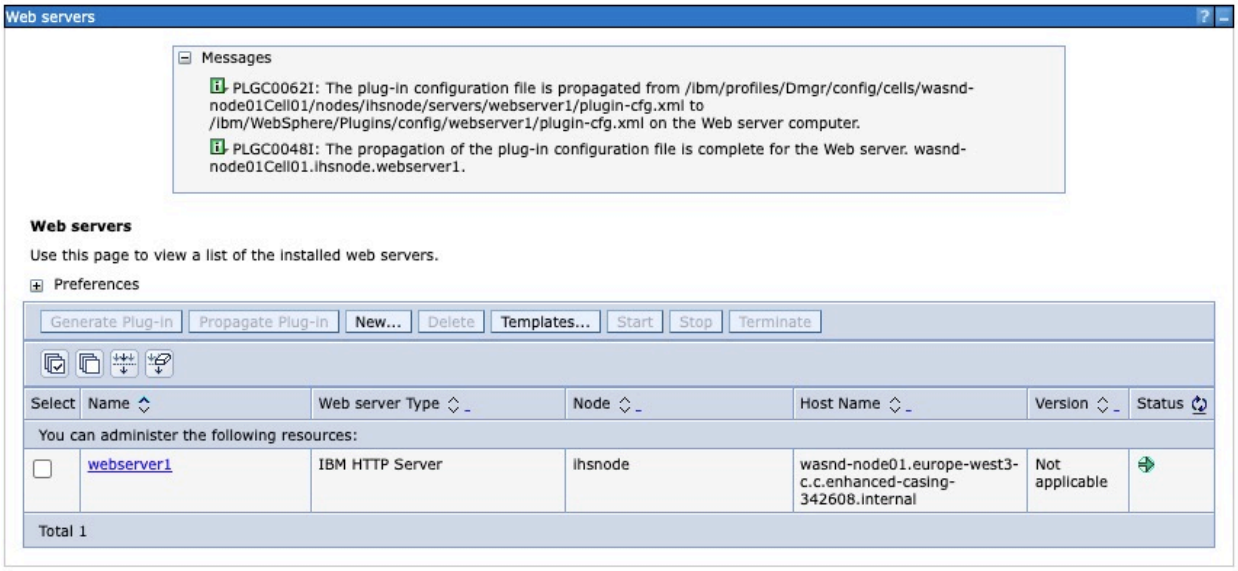
Cell=wasnd-node01Cell01, Profile=Dmgr



Cell=wasnd-node01Cell01, Profile=Dmgr



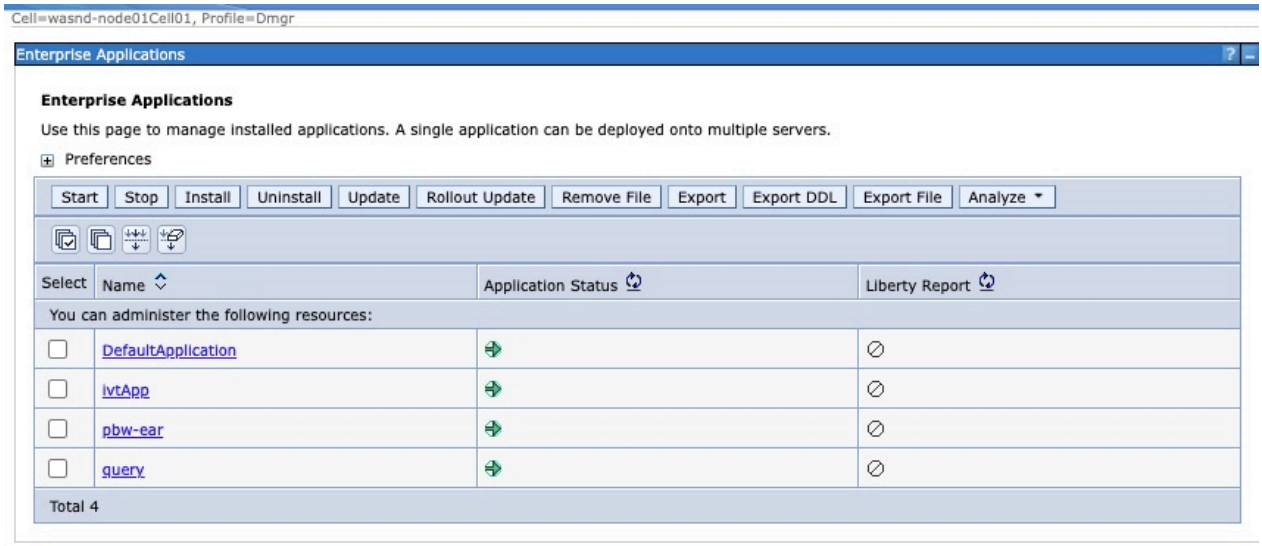


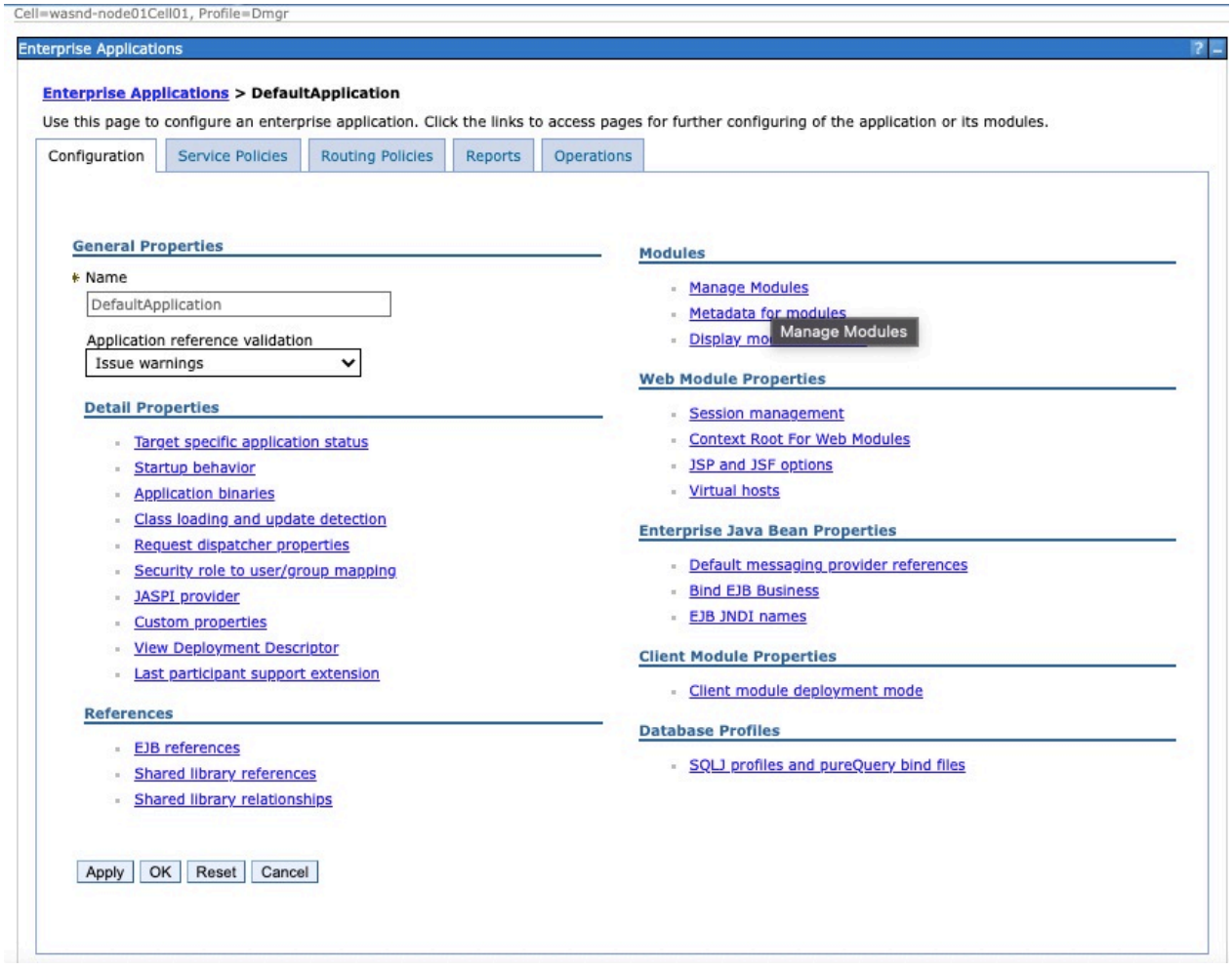


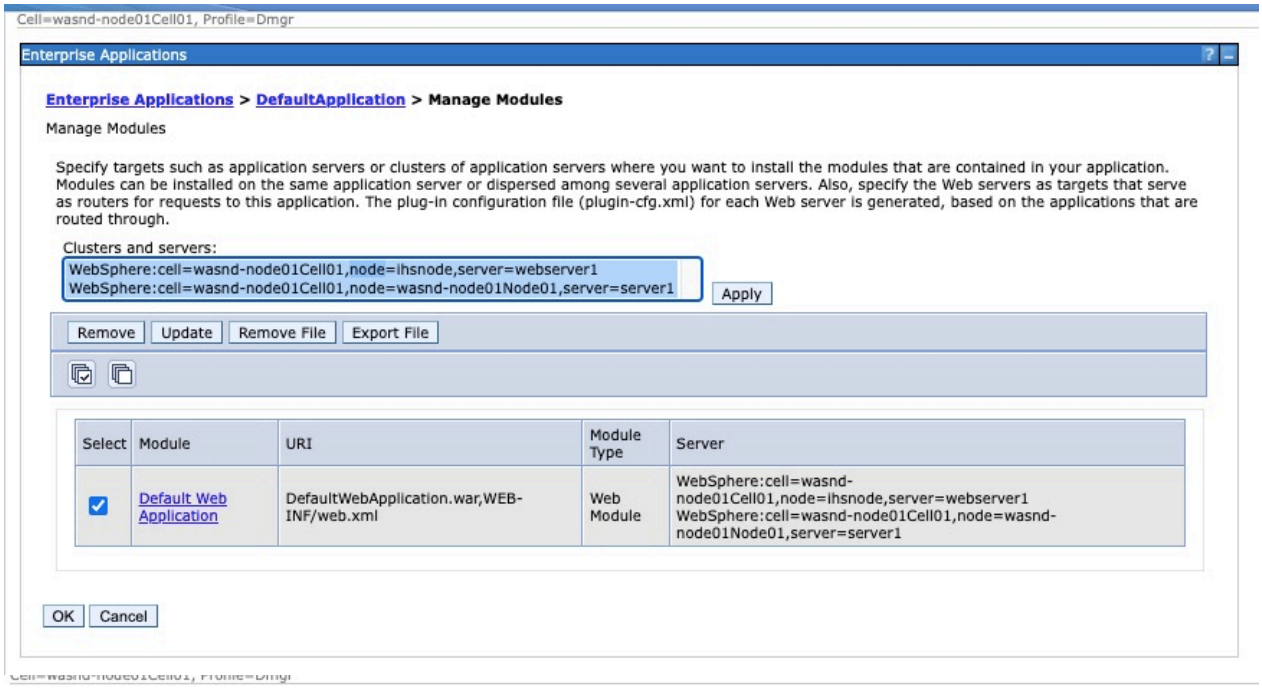
Section 7: Mapping modules to servers

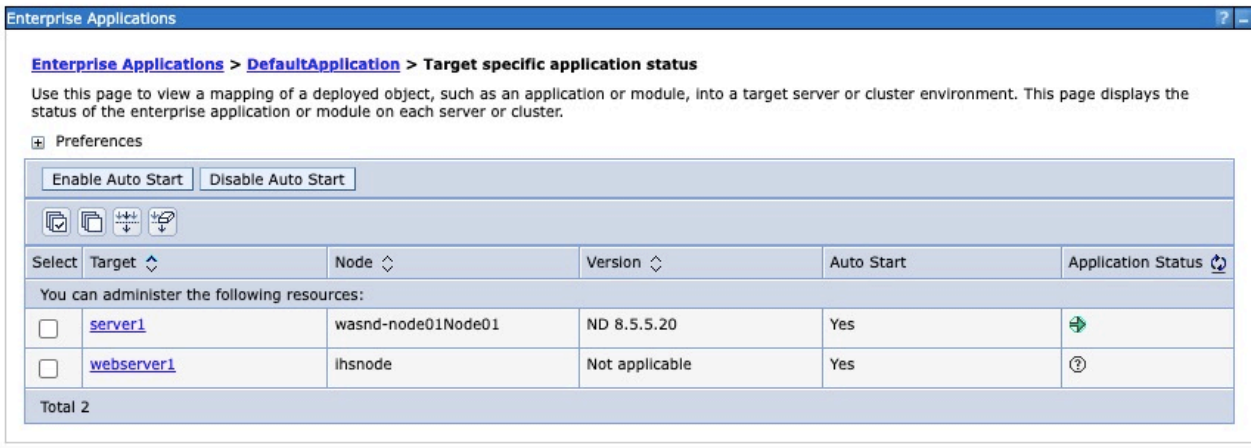
Each module of an application is mapped to one or more target servers. The target server can be an application server, a cluster of application servers, or a web server. Web servers that are specified as targets have the routing information for the application, which is generated in their plug-in configuration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


Cell=wasnd-node01Cell01, Profile=Dmgr
Enterprise Applications
Enterprise Applications
Use this page to manage installed applications. A single application can be deployed onto multiple servers.
Preferences
Start
Stop
Install
Uninstall
Update
Rollout Update
Remove File
Export
Export DDL
Export File
Analyze
Select
Name
Application Status
Liberty Report
You can administer the following resources:
DefaultApplication
ivtApp
pbw-ear
query
Total 4

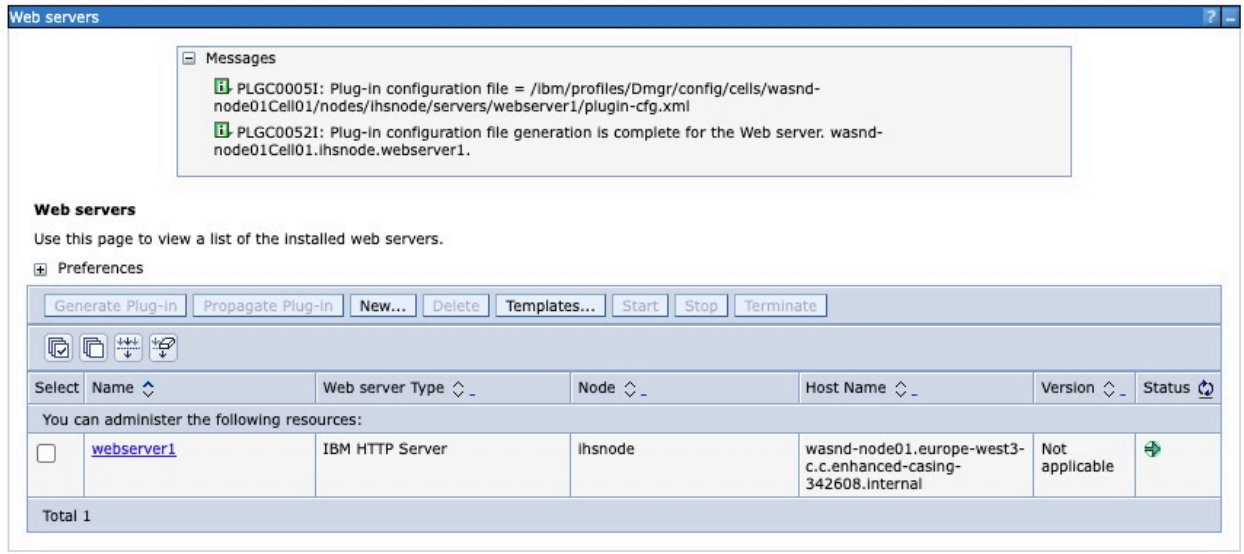

Cell=wasnd-node01Cell01, Profile=Dmgr
Enterprise Applications
Enterprise Applications > DefaultApplication
Use this page to configure an enterprise application. Click the links to access pages for further configuring of the application or its modules.
Configuration
Service Policies
Routing Policies
Reports
Operations
General Properties
Name
DefaultApplication
Application reference validation
Issue warnings
Detail Properties
Target specific application status
Startup behavior
Application binaries
Class loading and update detection
Request dispatcher properties
Security role to user/group mapping
JASPI provider
Custom properties
View Deployment Descriptor
Last participant support extension
References
EJB references
Shared library references
Shared library relationships
Modules
Manage Modules
Metadata for modules
Display mo
Manage Modules
Web Module Properties
Session management
Context Root For Web Modules
JSP and JSF options
Virtual hosts
Enterprise Java Bean Properties
Default messaging provider references
Bind EJB Business
EJB JNDI names
Client Module Properties
Client module deployment mode
Database Profiles
SQLJ profiles and pureQuery bind files
Apply
OK
Reset
Cancel

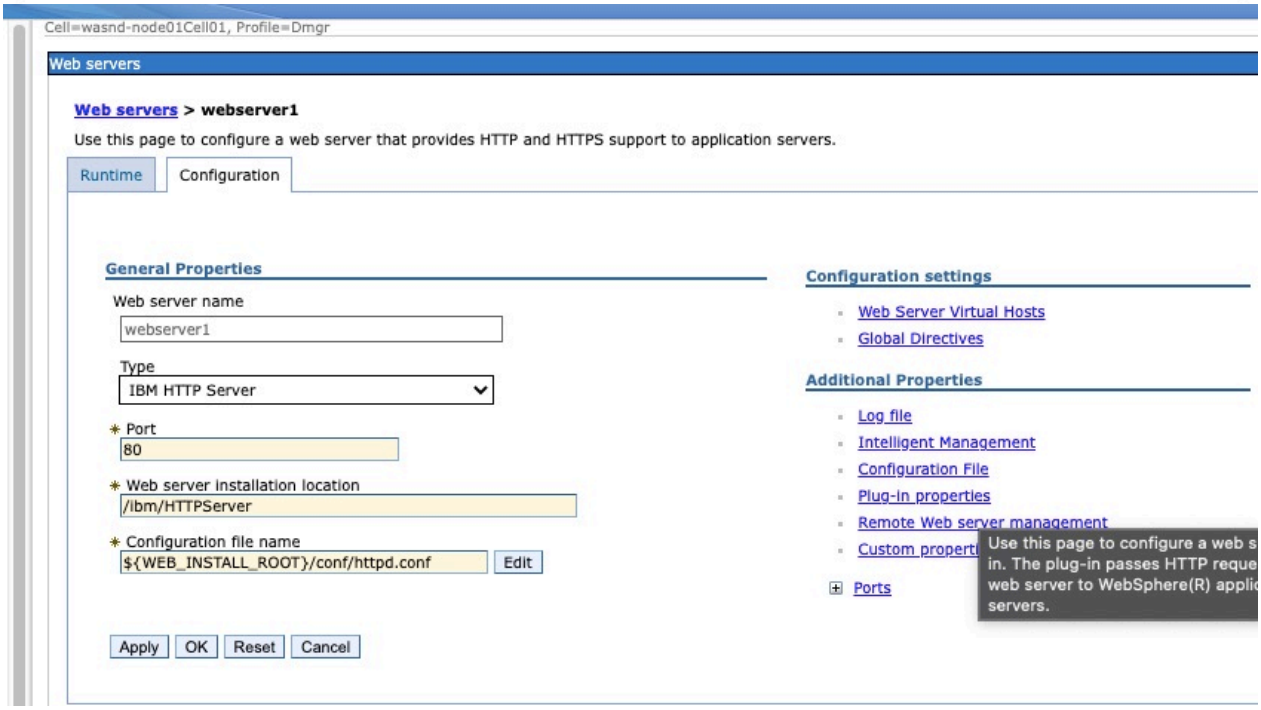


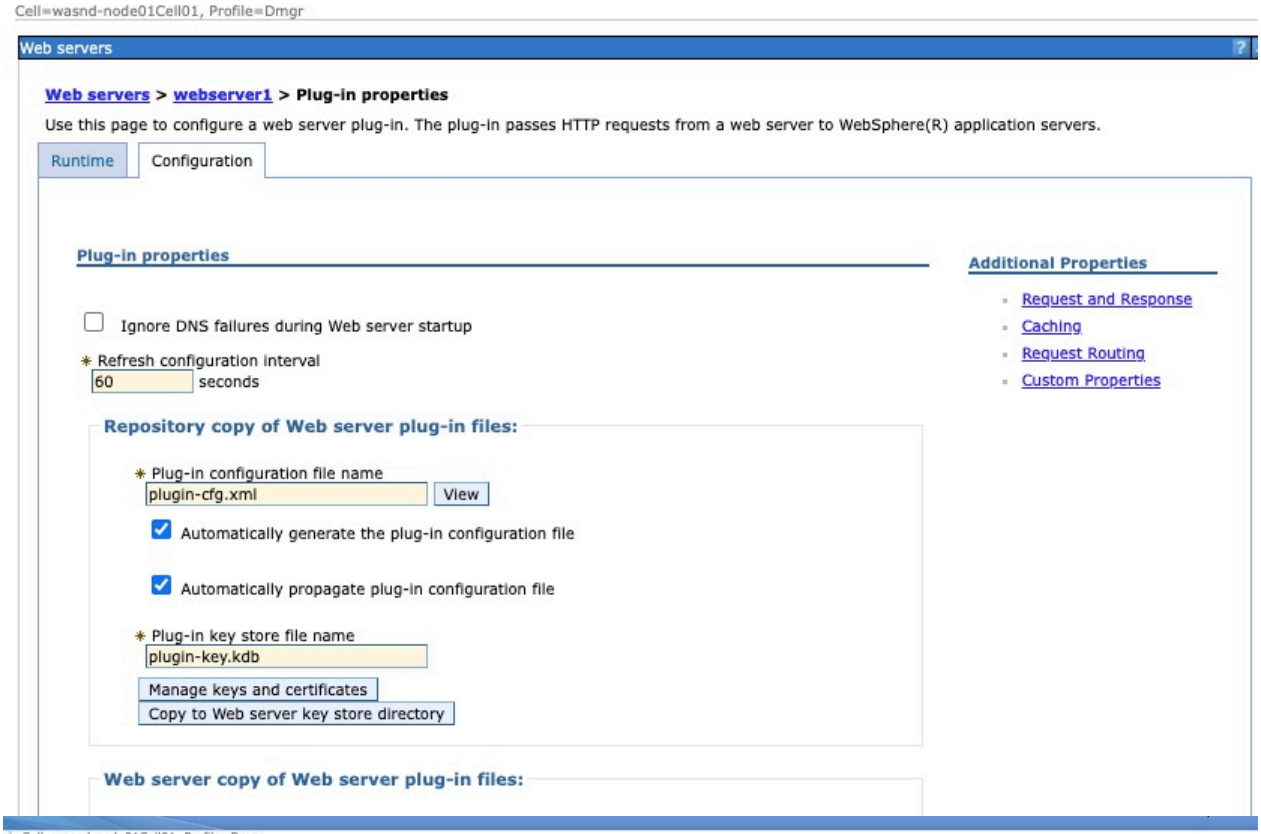


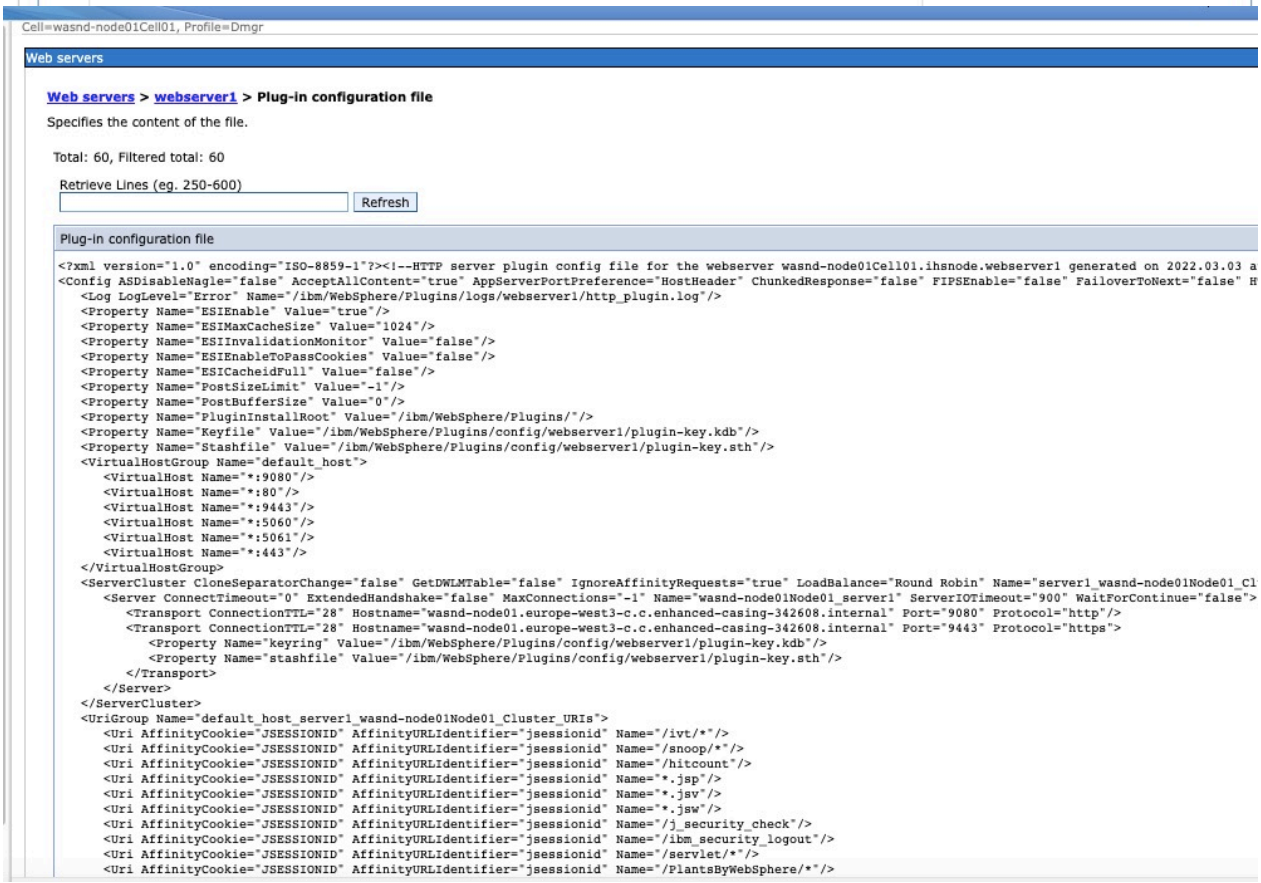
Section 8: Working with the plug-in configuration file

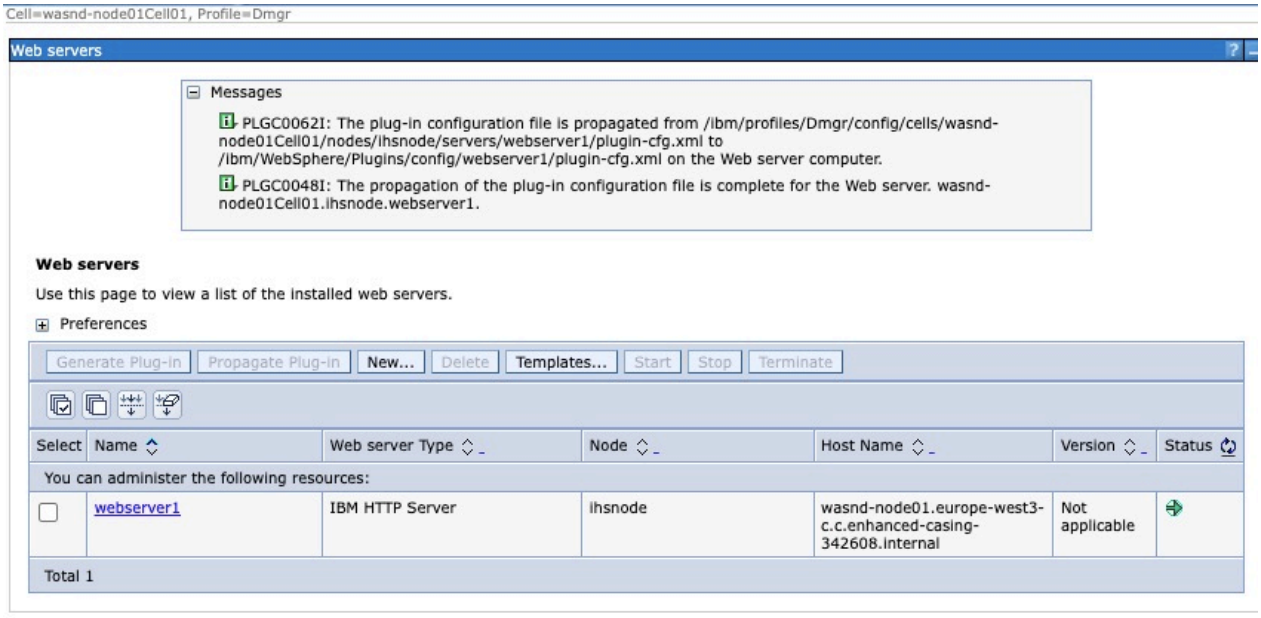
The plug-in configuration file contains routing information for all applications that are mapped to the web server. The plug-in configuration file must be regenerated and propagated to the web server whenever changes that are made to the WebSphere configuration affect how requests are routed from the web server to the application server.


Web servers
Messages
PLGC0005I: Plug-in configuration file = /ibm/profiles/Dmgr/config/cells/wasnd-node01Cell01/nodes/ihsnode/servers/webserver1/plugin-cfg.xml
PLGC0052I: Plug-in configuration file generation is complete for the Web server. wasnd-node01Cell01.ihsnode.webserver1.
Web servers
Use this page to view a list of the installed web servers.
Preferences
Generate Plug-in
Propagate Plug-in
New...
Delete
Templates...
Start
Stop
Terminate
Select
Name
Web server Type
Node
Host Name
Version
Status
You can administer the following resources:
webserver1
IBM HTTP Server
ihsnode
wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal
Not applicable
Total 1


Cell=wasnd-node01Cell01, Profile=Dmgr
Web servers
Web servers > webserver1
Use this page to configure a web server that provides HTTP and HTTPS support to application servers.
Runtime
Configuration
General Properties
Web server name
webserver1
Type
IBM HTTP Server
Port
80
Web server installation location
/ibm/HTTPServer
Configuration file name
${WEB_INSTALL_ROOT}/conf/httpd.conf
Edit
Apply
OK
Reset
Cancel
Configuration settings
Web Server Virtual Hosts
Global Directives
Additional Properties
Log file
Intelligent Management
Configuration File
Plug-in properties
Remote Web server management
Custom properti
Ports
Use this page to configure a web s
in. The plug-in passes HTTP reque
web server to WebSphere(R) appli
servers.

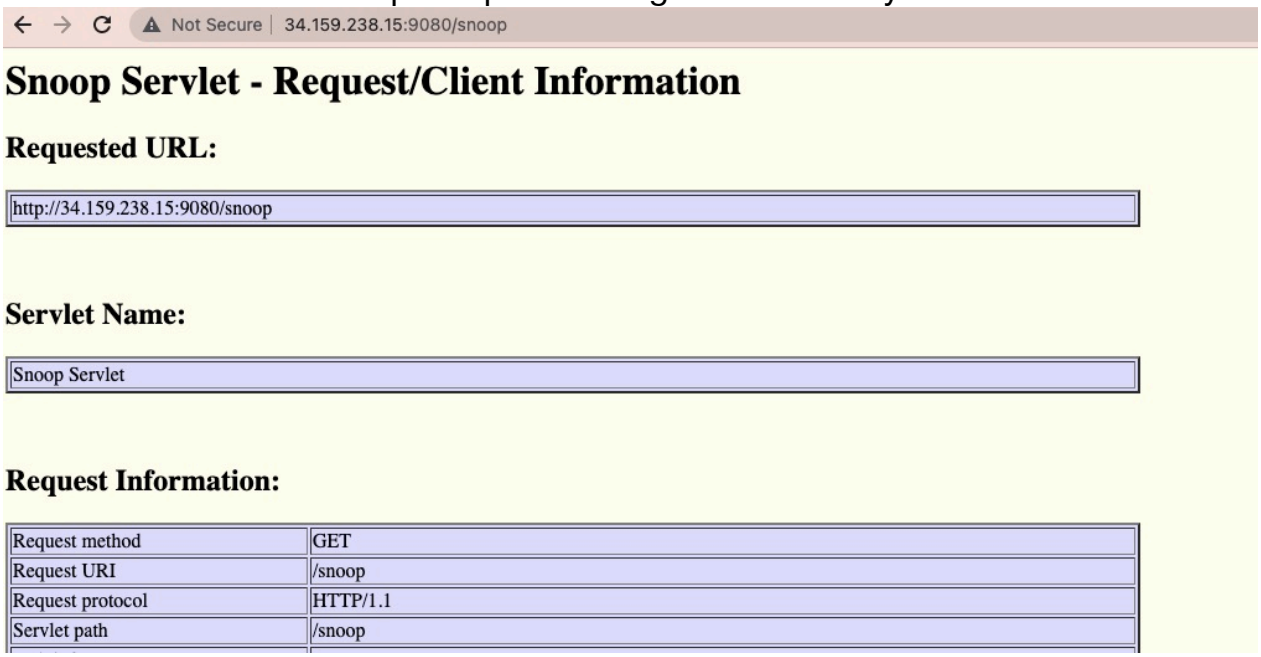

Cell=wasnd-node01Cell01, Profile=Dmgr
Web servers
Web servers > webserver1 > Plug-in properties
Use this page to configure a web server plug-in. The plug-in passes HTTP requests from a web server to WebSphere(R) application servers.
Runtime
Configuration
Plug-in properties
Additional Properties
Request and Response
Caching
Request Routing
Custom Properties
Ignore DNS failures during Web server startup
Refresh configuration interval
60
seconds
Repository copy of Web server plug-in files:
Plug-in configuration file name
plugin-cfg.xml
View
Automatically generate the plug-in configuration file
Automatically propagate plug-in configuration file
Plug-in key store file name
plugin-key.kdb
Manage keys and certificates
Copy to Web server key store directory
Web server copy of Web server plug-in files:


Cell=wasnd-node01Cell01, Profile=Dmgr
Web servers
Web servers > webserver1 > Plug-in configuration file
Specifies the content of the file.
Total: 60, Filtered total: 60
Retrieve Lines (eg. 250-600)
Refresh
Plug-in configuration file
<?xml version="1.0" encoding="ISO-8859-1"?><!--HTTP server plugin config file for the webserver wasnd-node01Cell01.ihsnode.webserver1 generated on 2022.03.03 a
<Config ASDisableNagle="false" AcceptAllContent="true" AppServerPortPreference="HostHeader" ChunkedResponse="false" FIPSEnable="false" FailoverToNext="false" H
<Log LogLevel="Error" Name="/ibm/WebSphere/Plugins/logs/webserver1/http_plugin.log"/>
<Property Name="ESIEnable" Value="true"/>
<Property Name="ESIMaxCacheSize" Value="1024"/>
<Property Name="ESIInvalidationMonitor" Value="false"/>
<Property Name="ESIEnableToPassCookies" Value="false"/>
<Property Name="ESICacheidFull" Value="false"/>
<Property Name="PostSizeLimit" Value="-1"/>
<Property Name="PostBufferSize" Value="0"/>
<Property Name="PluginInstallRoot" Value="/ibm/WebSphere/Plugins/"/>
<Property Name="Keyfile" Value="/ibm/WebSphere/Plugins/config/webserver1/plugin-key.kdb"/>
<Property Name="Stashfile" Value="/ibm/WebSphere/Plugins/config/webserver1/plugin-key.sth"/>
<VirtualHostGroup Name="default_host">
<VirtualHost Name="*:9080"/>
<VirtualHost Name="*:80"/>
<VirtualHost Name="*:9443"/>
<VirtualHost Name="*:5060"/>
<VirtualHost Name="*:5061"/>
<VirtualHost Name="*:443"/>
</VirtualHostGroup>
<ServerCluster CloneSeparatorChange="false" GetDWLMTable="false" IgnoreAffinityRequests="true" LoadBalance="Round Robin" Name="server1_wasnd-node01Node01_Cl
<Server ConnectTimeout="0" ExtendedHandshake="false" MaxConnections="-1" Name="wasnd-node01Node01_server1" ServerIOTimeout="900" WaitForContinue="false">
<Transport ConnectionTTL="28" Hostname="wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal" Port="9080" Protocol="http"/>
<Transport ConnectionTTL="28" Hostname="wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal" Port="9443" Protocol="https">
<Property Name="keyring" Value="/ibm/WebSphere/Plugins/config/webserver1/plugin-key.kdb"/>
<Property Name="stashfile" Value="/ibm/WebSphere/Plugins/config/webserver1/plugin-key.sth"/>
</Transport>
</Server>
</ServerCluster>
<UriGroup Name="default_host_server1_wasnd-node01Node01_Cluster_URIs">
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/ivt/*"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/snoop/*"/>
<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/*"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/PlantsByWebSphere/*"/>



Section 9:Test 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.



Snoop Servlet - Request/Client Information

Requested URL:

http://34.159.238.15/snoop

Servlet Name:

Snoop Servlet

Request Information:

Request method	GET
Request URI	/snoop
Request protocol	HTTP/1.1
Servlet path	/snoop