

IBM Connections 4.5: How to Deploy a Two Node Cluster of IBM connections V4.5 on a RedHat (RHEL) Server V6.4 (x86-64bit)

About the author

Patrick (Pat) Cadogan has worked for IBM for over a quarter of a century. Pat initially started working at Lotus Development and focused on the globalization and localization of Lotus products such as Lotus 1-2-3, Freelance, Symphony, Improv and Lotus Notes/Domino. IBM acquired Lotus in 1995. In 1998 Pat moved to the IBM Lotus Lab in Massachusetts, US, where he worked on Lotus Domino for Linux, iSeries and zSeries. After five years in the US Pat returned to the IBM Dublin Lab where he focused on System Verification Testing (SVT) of various IBM products. Pat has worked on the SVT of IBM Connections V2x, 3x, V4 and now V4.5. Pat can be reached at pcadogan@ie.ibm.com.

References

- [IBM Connections System Requirements](#)
- [IBM Connections 4.5 Information Center](#)
- [Tutorial - Installing IBM Connections 4.0 on a Linux RHEL 6.3 64 bit system](#)

See related documents:

- IBM Connections 4.5: How to configure SPNEGO
- IBM Connections 4.5: How to configure TAM

Contents

1. Deployment topology
2. IBM Connections system requirements
3. Middleware installation and configuration
 - 3.1 Install IBM Installation Manager 1.5.3
 - 3.2 Install WAS V8 Deployment Manager (DM)
 - 3.3 Install WAS V8 Applications Server on Node1 and Node2
 - 3.4 Install IBM HTTP Server (IHS) V8
 - 3.5 Update DM, Applications Server and IHS to required Fixpack and iFixes
 - 3.6 Install DB2 10-FP1 Server
 - 3.7 Install Tivoli Directory Integrator (TDI) V7.1 + Fixpack 5
4. Deployment configuration steps
 - 4.1 Enable Security on the Deployment Manager:
 - 4.2 Federate Application Server (Nodes) into the Deployment Manager
 - 4.3 Configure HTTP server to accept SSL connections
5. Creating the Connections databases on DB2 using the dbWizard
6. Populating the profiles database (PEOPLEDDB) with LDAP user information
7. Installation of IBM Connections
8. Post install steps
 - 8.1 Copying Search conversion tools to local nodes
 - 8.2 Configuring the HTTP Server
 - 8.3 Configuring an Administrator User for Homepage
 - 8.4 Enabling Fast Downloads for Files and Wikis
 - 8.5 Configure Notifications

1. Deployment Topology

Installing IBM® Connections in a network deployment to achieve optimum scaling, load balancing, and failover.

A network deployment can consist of a single server with all applications installed, or two or more sets of servers that are grouped to share the workload. You must also configure an additional system with WebSphere® Application Server Network Deployment Manager, which enables you to build, manage, and tune the clustered servers.

A network deployment provides the administrator with a central management facility, and it ensures that users have constant access to data. It balances the workload between servers, improves server performance, and facilitates the maintenance of performance when the number of users increases. The added reliability also requires a larger number of systems and the experienced administrative personnel who can manage them.

Standard Enterprise Network Deployment Architecture

Figure 1 shows the enterprise-level network deployment of IBM Connections without any additional complexity. This topology shows a two-node cluster of IBM Connections, in which the LDAP and database servers communicate with the cell controlled by the Deployment Manager. The Tivoli Directory Integrator server sits between the database and LDAP, maintaining synchronization between both.

IBM Connections is installed on the Deployment Manager machine and from there is pushed out to the nodes in the cell, node01Node and node02Node. The shared data store is a shared space accessible from all nodes in the configuration and the Deployment Manager. In this case the shared space is mounted on the Deployment Manager machine and shared with both nodes, at the same location on those machines.

Sitting in front of the entire configuration is the Web server, from which the end user accesses IBM Connections.

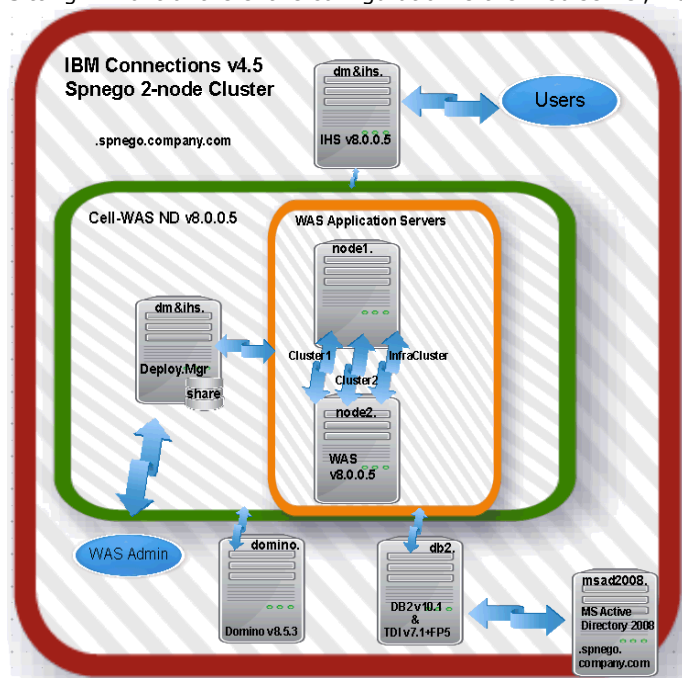


Figure 1

In this Scenario and in the above Topology diagram the following apply:

Cognos/Metric is not installed - Cognos install/configuration is covered in a separate document.

IBM Connections Content Manager (Filenet) is not installed - Filenet install/configuration is covered in a separate document.

the WAS Deployment Manager and the IHS server both co-exist on the same physical machine, but they are depicted (in the diagram) as existing on different machines. This was done to help simplify understanding of this deployment - note the hostname is the same for both.

The Domino Mailin server is not integrated with the MS-AD2008 LDAP so that users are not automatically created as needed on the Domino mail server; instead Domino mailin users were created manually (as needed) and the mapping between IC4 and Domino users was based on the users email address. This is not typically how customers would configure Notifications and Domino mail integration.

When installing IBM Connections there are three deployment options to choose from ie small, medium and large. This deployment uses the Medium topology; see [Deployment options](#) for more details.

Topology: **Medium** deployment

Install a subset of applications in separate clusters. IBM Connections provides three predefined cluster names shared among all 12 applications. Use this option to distribute applications according to your usage expectations. For instance, you might anticipate higher loads for the Profiles application and install it in its own cluster, while other applications could be installed in a different cluster. This option allows you to maximize the use of available hardware and system resources to

suit your needs.

2. IBM Connections 4.5 System Requirements

For IBM Connections V4.5 System requirements see the product documentation: <http://www-01.ibm.com/support/docview.wss?uid=swg27037782>

Systems specification used in this deployment

Machine Hostname	Applications	Version	OS/version	RAM / CPU / HDD
dm&ihs.spnego.company.com	WAS Deployment Manager IBM HTTP Server (IHS)	WAS v8.0.0.5 (64bit) IHS v8.0.0.5 (64bit)	RedHat 6 (64bit) Enterprise	8GB / 2CPUs / 80GB
node1.spnego.company.com	Node1 (WAS Application Server)	WAS v8.0.0.5		
node2.spnego.company.com	Node2 (WAS Application Server)	WAS v8.0.0.5		
db2.spnego.company.com	DB2 Tivoli Directory Integrator (TDI)	DB2 v10.1 TDI v7.1+FP5		
msad2008.spnego.company.com	MS Active Directory 2008	'2008	Win2008 R2 EE Server	
domino.company.com	Domino Mail-in server	Domino 8.5.3	Win2008 R2 EE Server	4GB / 2CPUs / 40GB

All of the above systems are Virtual Machines (VM) running on VMware vSphere V5.0

When installing Connections (in this scenario) we refer to a fictitious user called "**AdminFromLDAP**" - this user must meet the following criteria:

- is a valid user from the LDAP branch
- is populated to the profiles database (PEOPLEDDB) when running the dbPopulation wizard
- is granted Admin access to the DM so that this user can login to the WAS console and can administrate all aspects of Connections
- is selected as the Connections administrator when running the Connections Install wizard

Note: Where possible we will use the default setting throughout this document especially for paths.

Before Installing IBM Connections you must apply the following:

i) Linux RedHat 6 (64bit) OS essential patches: see the IBM Connections InfoCenter for details:

http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.5+documentation#action=openDocument&res_title=Linux_libraries_ic45&content=pdcontent

ii) Install the following additional Redhat libraries

./ibm-yum.sh install <package> - where packages are:

```
ksh*  
compat-db*  
compat-libstdc++-33*  
compat-glibc-2*  
openmotif22-2*  
libXtst*  
libXp*  
libXmu*  
libXtst*  
pam*  
rpm-build*  
elfutils*  
libXft*  
gtk2*
```

iii) WebSphere requirements

a) WAS 8.0.0.5 is the minimum requirement

b) Additional required WebSphere iFixes (for the Deployment Manager) are:

[PM62615 - Here is Fix Central iFix for PM62615](#)

[PM71430 - Here is Fix Central iFix for PM71430](#)

iv) Synchronise the time on all systems in the deployment by running: **ntpdate clock.redhat.com** on each system

v) Configure the Open File Descriptor limit to at least 8192 on all systems (DM, Node1, Node2 and DB2)

```
vi /etc/profile
add ulimit -n 8192
```

verify by running: **ulimit -a**

On none windows platforms ensure that the Open File Descriptor limit is set to at least 8192
ulimit -n 8192

vi) Setup a NFS4 Shared Area for the DM, Node1 and Node2

In a Networked Deployment (multi node clustered environment with several systems) there is the need to set up a shared area which all nodes and the DM can access.

All nodes in the cluster need to have read and write access to this area.

This is used to store indexes which Connections needs.

This area needs to be setup prior to the Connections install as the installation will ask for this location during the setup process.

NOTE: Its highly recommended to use a 'fast reliable networked file system' for both this shared file area and the server were you locate your databases.

When using NFS, use NFS v4 because NFS v3 lacks advanced locking capability.

In this scenario we will set up the NFS share on our Deployment Manager; then share it out to each Nodes system so that each node system can read/write to the share.

These are the steps to do this:

On the DM system (dm&his.spengo.company.com), create a Share folder (using NFS4 Server)

Create a folder on the system you want to share the folder on eg on the DM system create a folder **/opt/IC_Share** eg: **mkdir /opt/IC_Share**

Give full read/write access to this folder, **chmod -R 777 /opt/IC_Share**

With NFS v4 you can export just one file system, so all the folders you need to mount on the clients should be under this one.

Edit the /etc/exports file [ie #vi /etc/exports] and add the following lines

```
/opt/IC_Share node1.company.com(rw)
/opt/IC_Share node2.company.com(rw)
```

Write and Quit [:wq!]

verify nsf service is running - if it is not then enable it via services

```
service nfs restart | stop | start
mount -all
```

You have now shared this folder to systems node1 and node2

Config Node1 and Node2 to access the Shared Folder on the DM system as follows:

Enable the **nfs** service on node1 and node2

create the folder to mount to eg: **mkdir /opt/IC_Share**

Add the following line to

```
vi /etc/fstab
dm&ihs.spnego.company.com:/opt/IC_Share /opt/IC_Share nfs
```

Mount the remote file system: **mount -all**

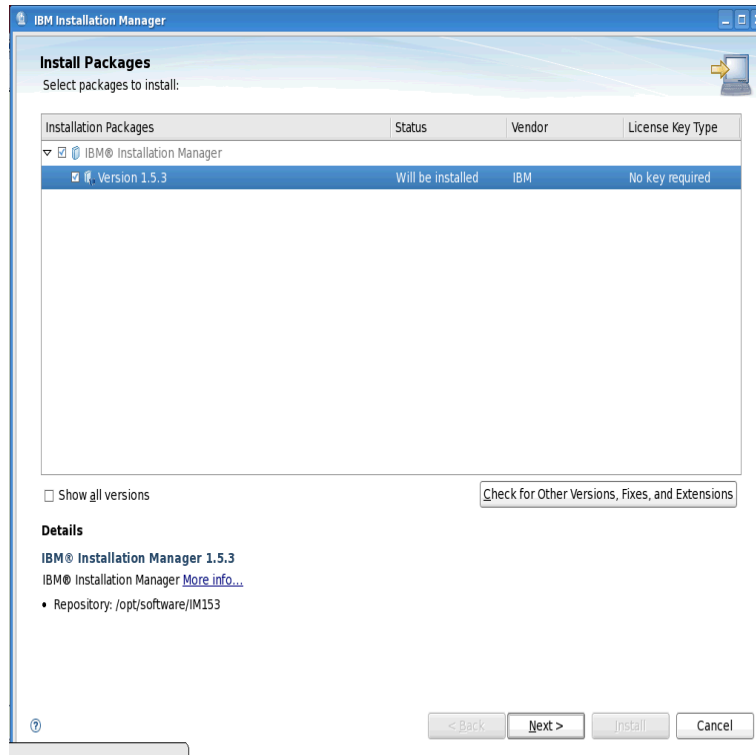
3. Middleware installation and configuration

3.1 IBM Installation Manager 1.5.3:

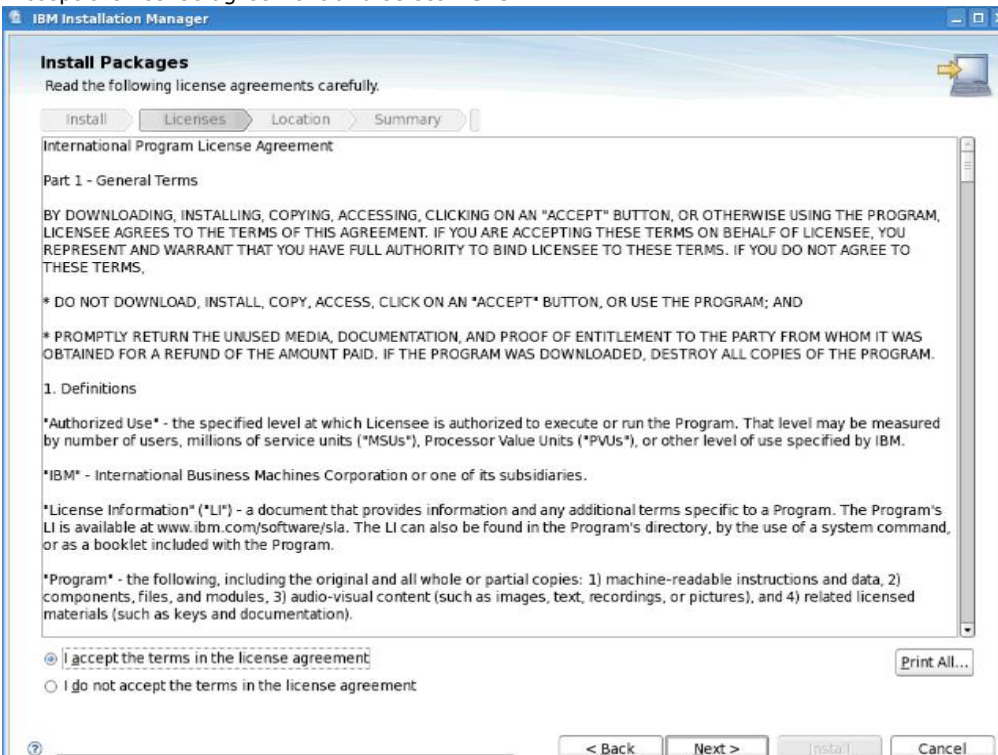
WebSphere V8.0 is installed using the **IBM Installation Manager** (IM) so we must install this first. You can download IM 1.5.3 from <http://www-01.ibm.com/support/docview.wss?uid=swg24032358>.

Unzip locally on your machine and run **install** to begin the IM installation...this will display the following screen.

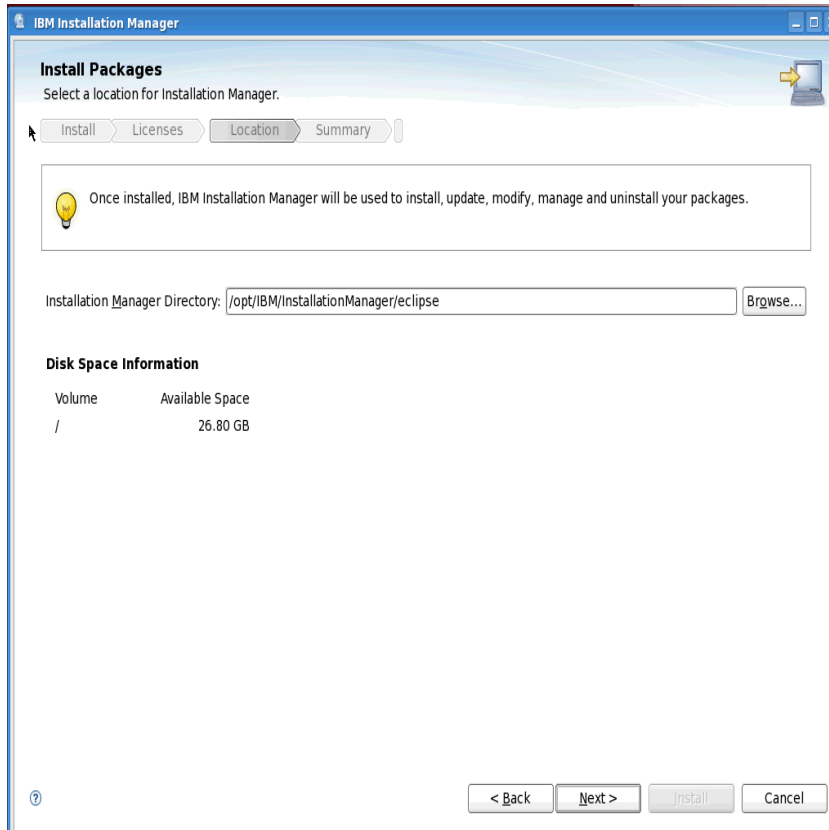
Select **Next** to continue...



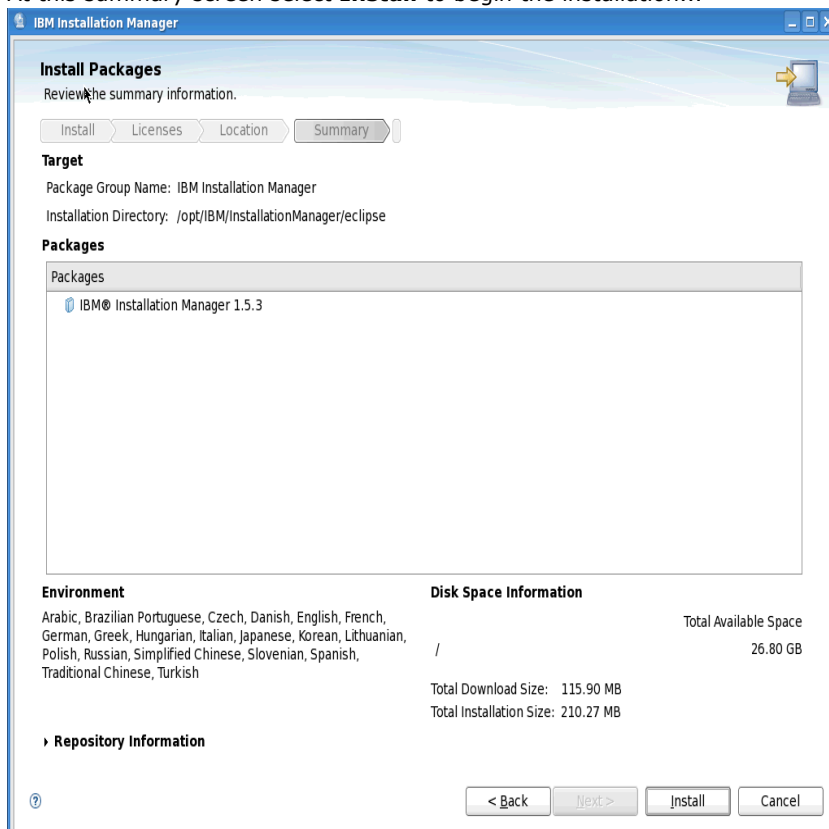
Accept the license agreement and select **Next**



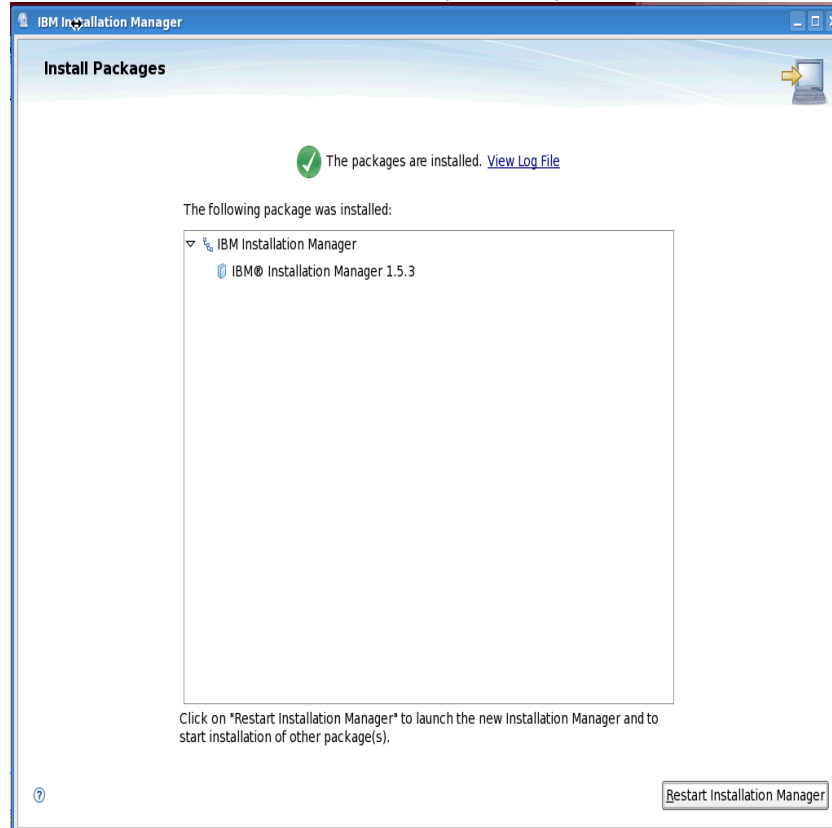
select **Next** to continue...



At this summary screen select **Install** to begin the installation...



After some time the installation will complete and you will see:



That's the IM installed.

Note: You will need to do this on your Deployment Manager, Application Server(s), HTTP Server and Plugin's servers in your deployment.

Tip: How to start the Installation Manager to install WAS; the IHS webserver and updates:

Goto the folder: `/opt/IBM/InstallationManager/eclipse`
Select 'launcher' or from the cmd line enter `"./launcher"`

3.2 WebSphere V8.0 Deployment Manager Installation

Create the following folder: **/opt/software** - we will use this folder to store all download images required to install WAS DM

Download the WAS Network Deployment V8 install images/zip-files into a folder called **/opt/software/WAS80DM** on you designated DM machine. The four images/zip files to download:

CZM9KML.zip
CZM9LML.zip
CZM9MML.zip
CZVG4ML.zip

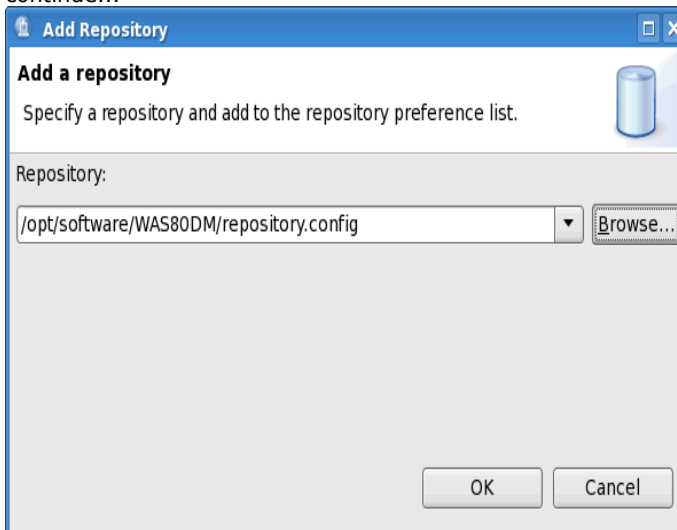
Unzip all four zip files and you will see the following files in the WAS80DM folder:

```
[root@dubxpcvm766 WAS80DM]# ls
Copyright.txt  disk1  disk2  disk3  disk4  lafiles  readme  Remote_Installation_Tool_for_IBM_i  repository.config
[root@dubxpcvm766 WAS80DM]#
```

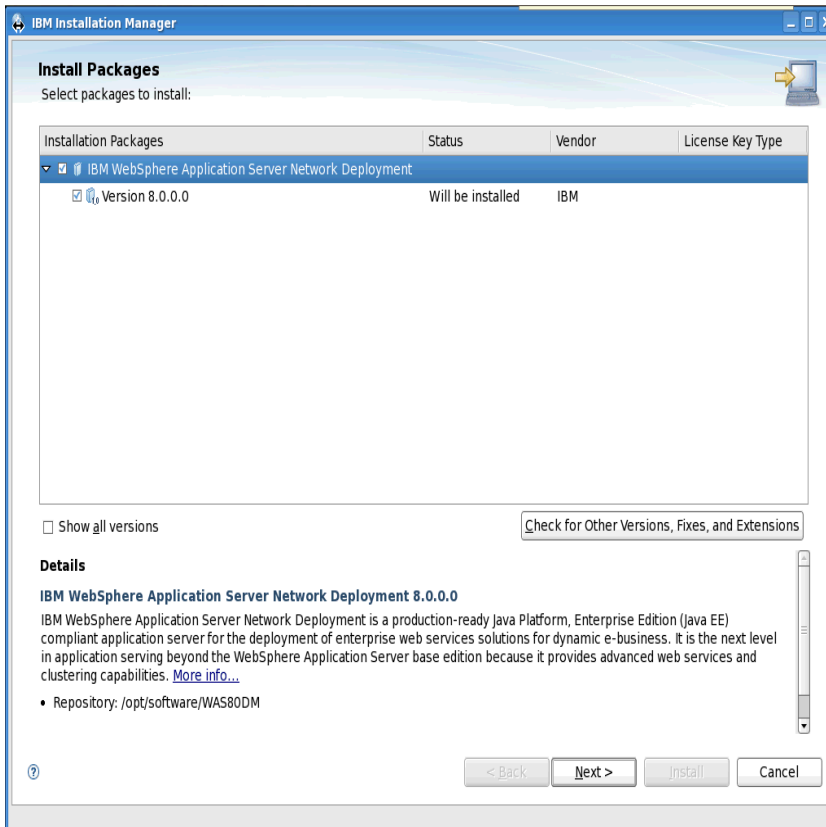
Startup the Installation Manager, which you installed earlier, on your deployment manager system.

Select File then Preferences.

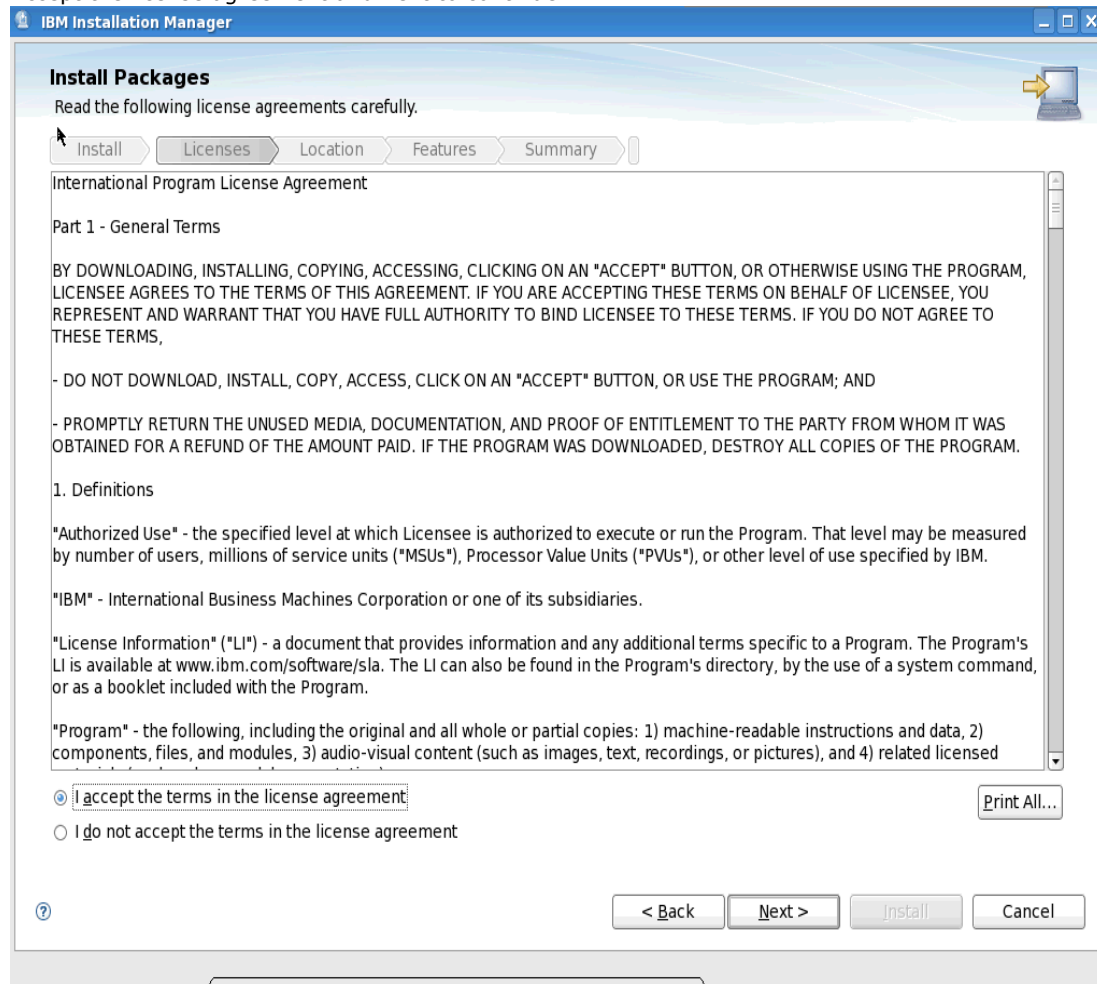
Select the Add Repository... button and enter the details to the path for the DM repository.config file. Select OK to continue...



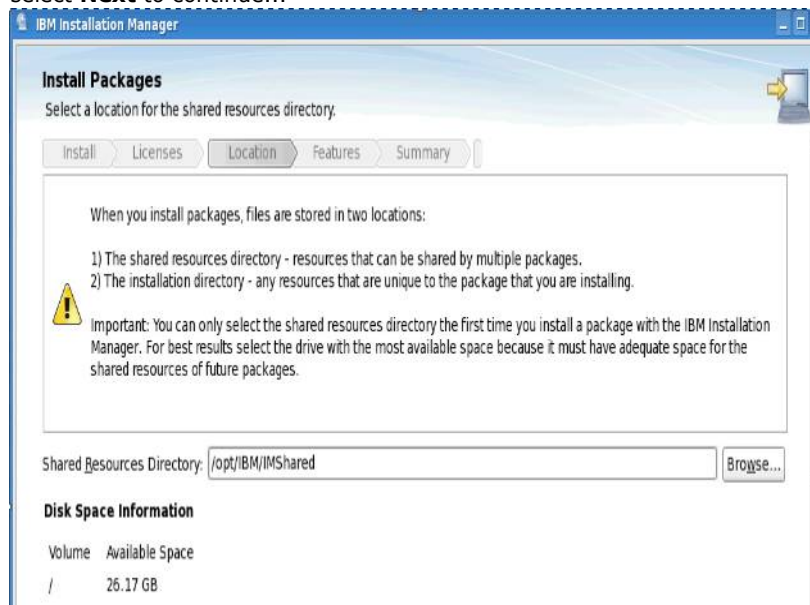
Now select **Install**



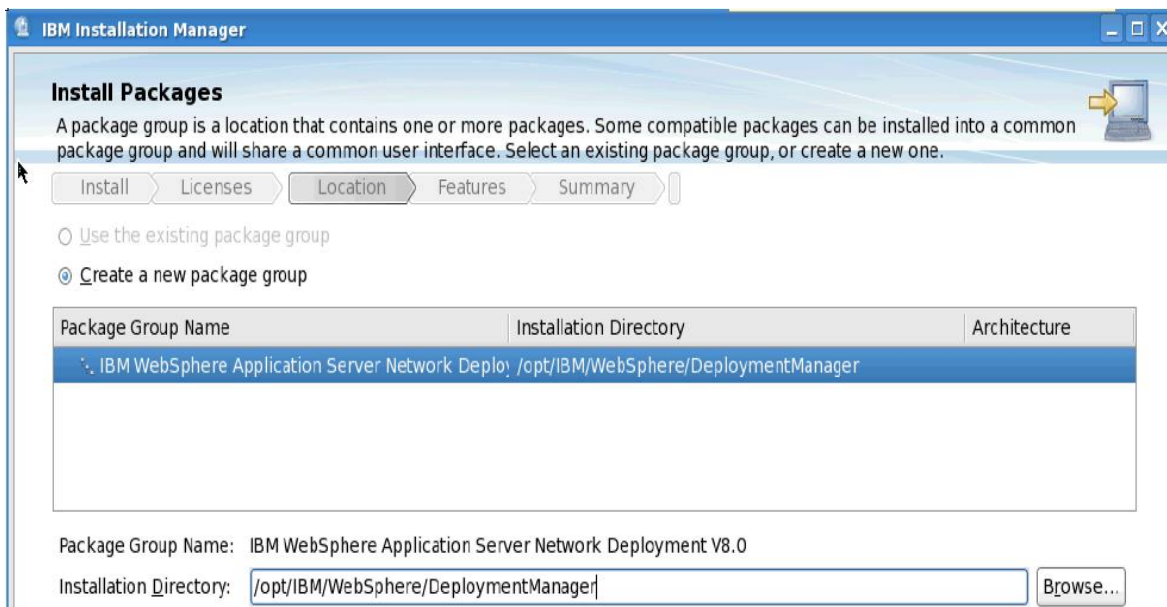
Accept the license agreement and next to continue...



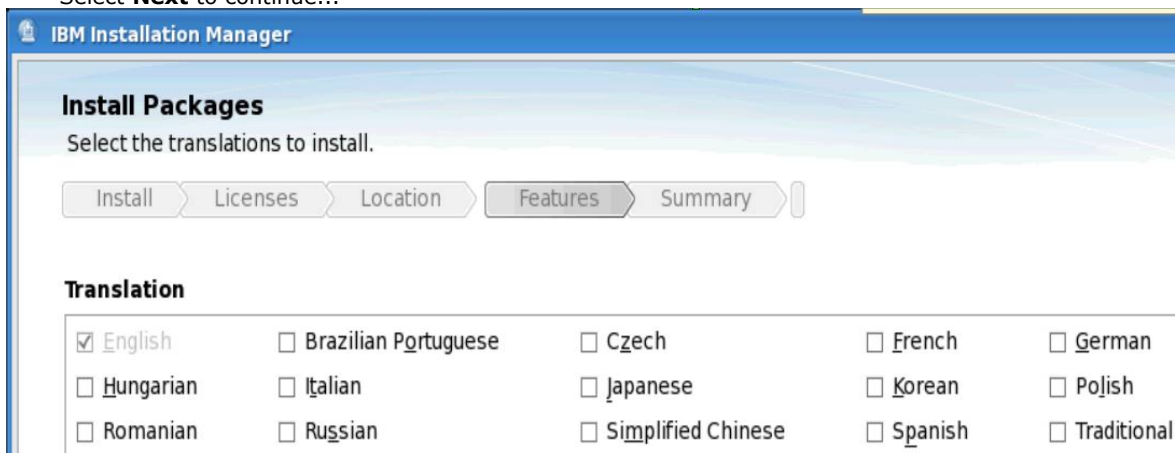
select **Next** to continue...



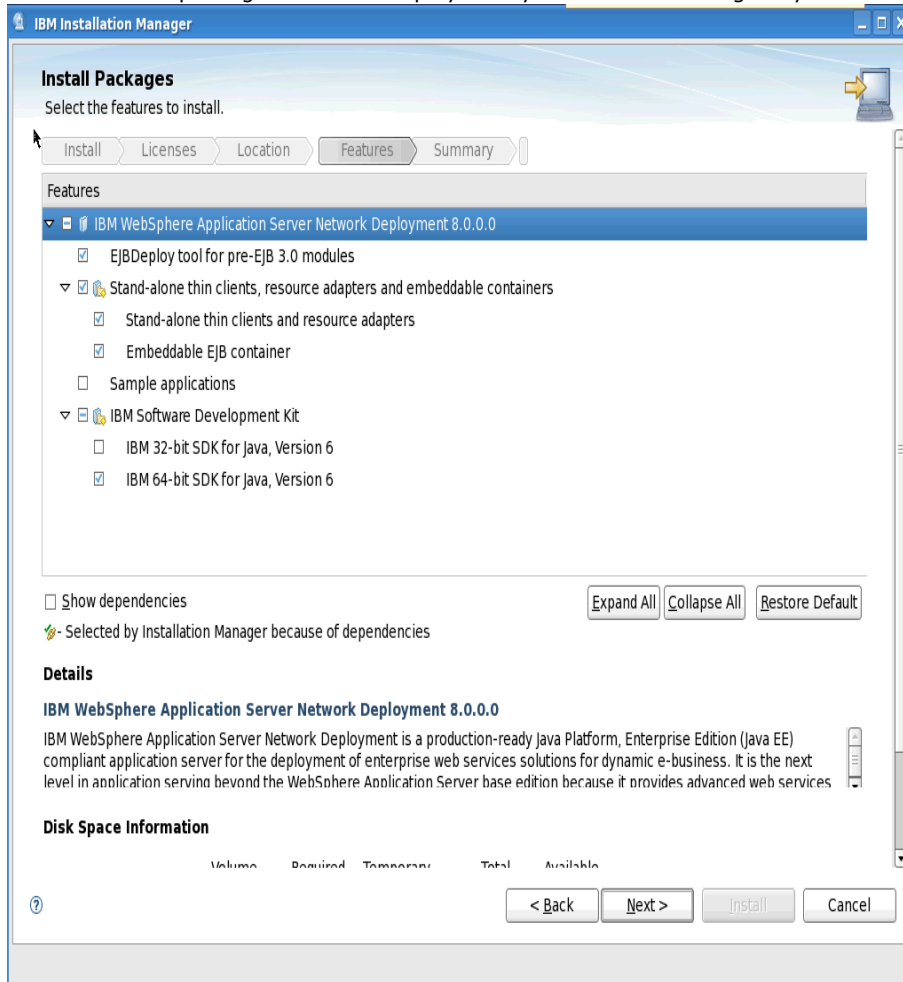
Enter the path to were to install the deployment manager. Select **Next** to continue...



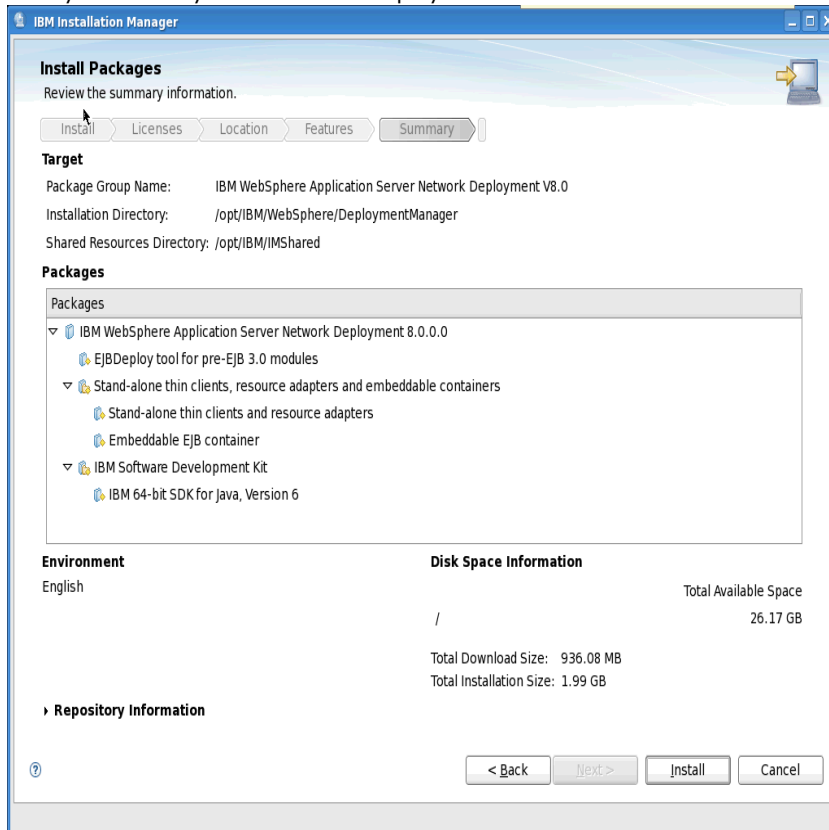
- Select **Next** to continue...



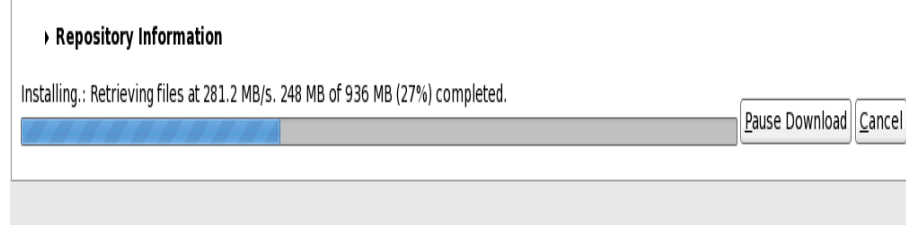
The installation packages are then displayed to you. I did not change any of the defaults here. Select **Next** to continue...



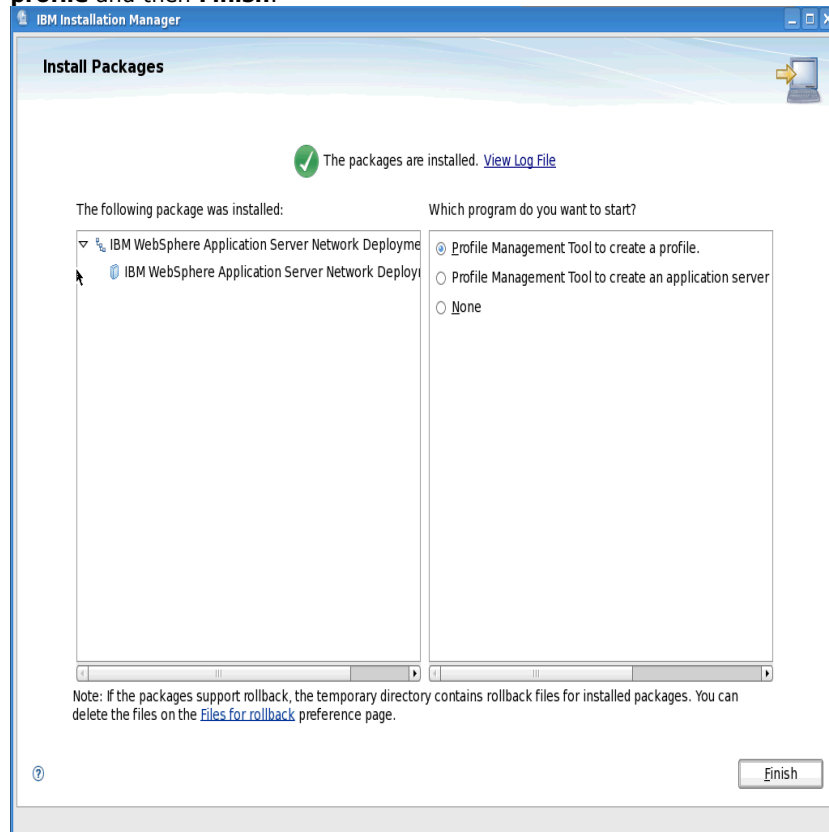
Finally a summary screen will be displayed. Select **Install..**



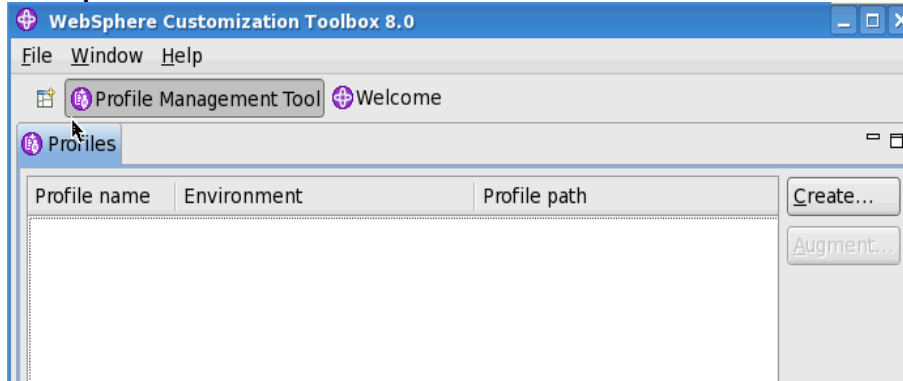
After some time the installation will complete. During the installation you will see stuff like this...



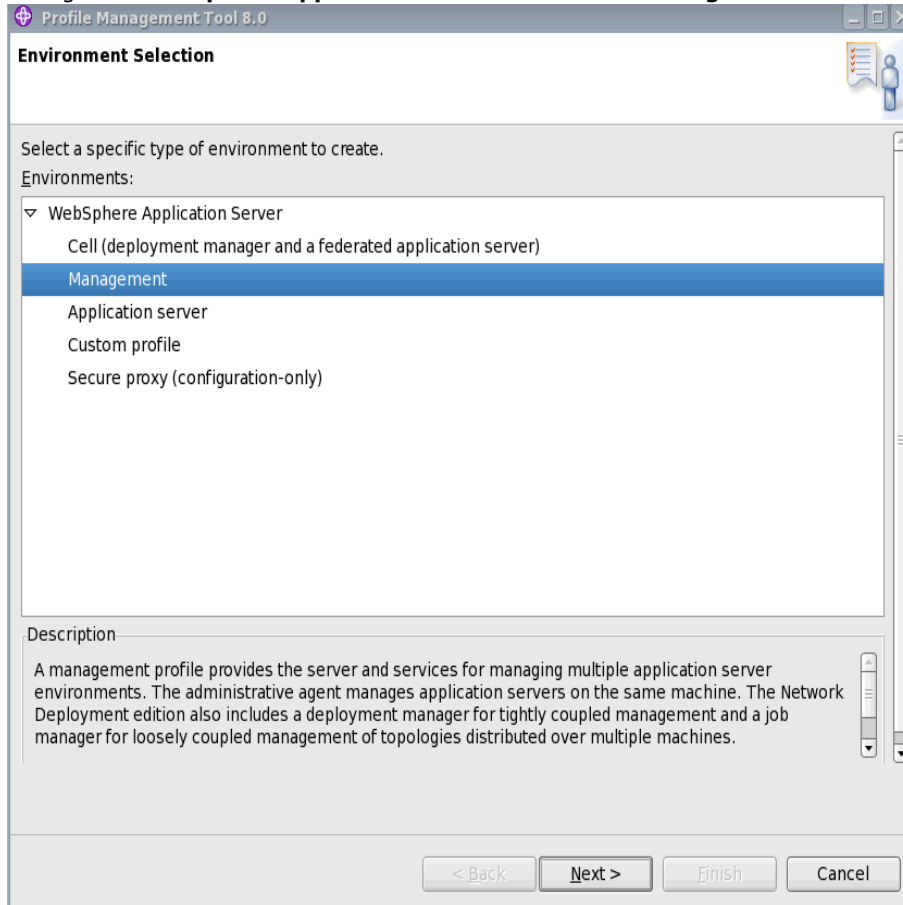
Once complete you are asked to create a Deployment Manager Profile... Select **Profile Management Tool to create a profile** and then **Finish**.



- The **WebSphere Customization Toolbox** starts. Select the **Create...** button



Change the **WebSphere Application Server** selection to **Management** and then **Next**



Select the **Deployment manager** option and then **Next** to continue...

Profile Management Tool 8.0

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 > Finish Cancel

Select the **Typical profile creation** option and then **Next** to continue...

Profile Management Tool 8.0

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 > Finish Cancel

Ensure **Enable administrative security** is checked and enter an admin user name & password.

Select **Next** to continue...

Profile Management Tool 8.0

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:

Password:

Confirm password:

See the information center for more information about administrative security.
[View the online information center](#)

< Back Next > Finish Cancel

At this summary screen select **Create** (to create the profile)...this will take a few minutes...

Profile Management Tool 8.0

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: /opt/IBM/WebSphere/DeploymentManager/profiles/Dmgr01

Disk space required: 30 MB

Profile name: Dmgr01

Make this profile the default: True

Cell name: dubxpcvm766Cell01

Node name: dubxpcvm766CellManager01

Host name: dubxpcvm766.mul.ie.ibm.com

Deploy the administrative console (recommended): True

Enable administrative security (recommended): True

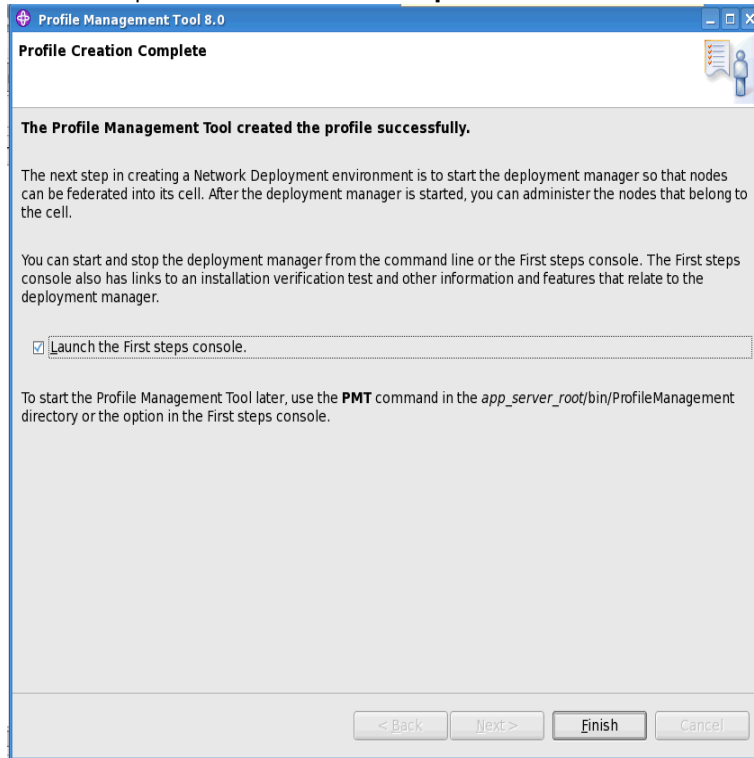
Administrative console port: 9060

Administrative console secure port: 9043

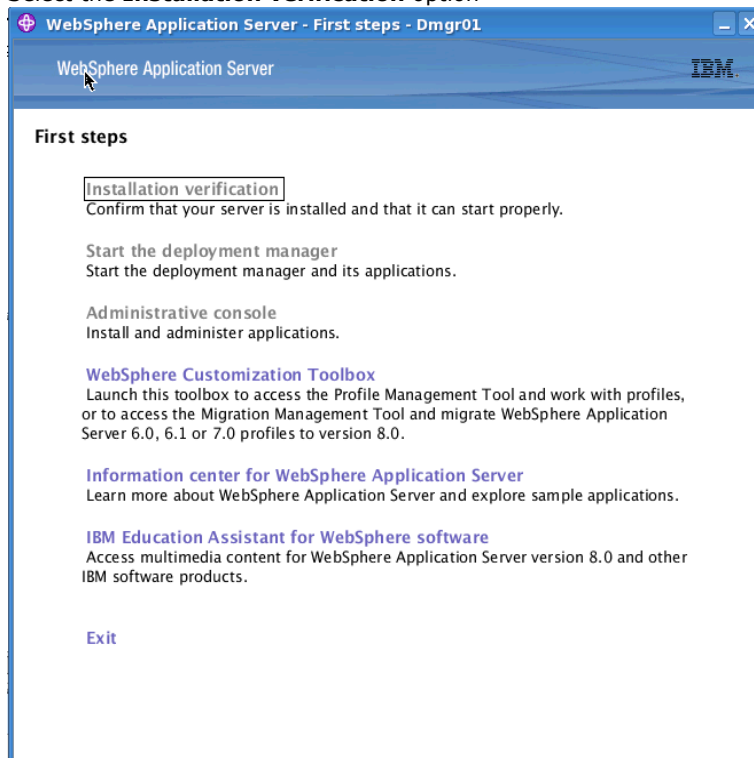
Deployment manager bootstrap path: 6800

< Back Create Finish Cancel

Check the option **Launch the First steps console** and then select **Finish**.



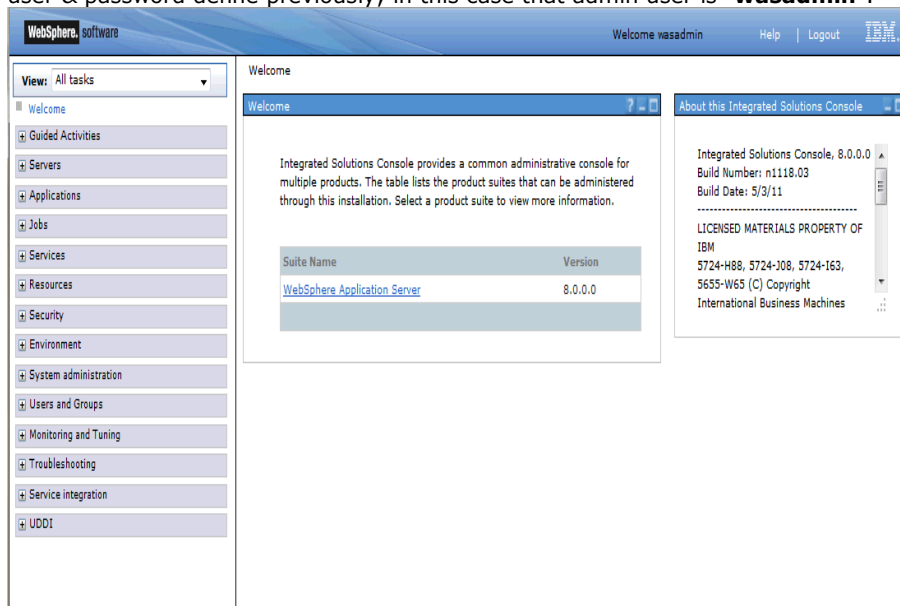
Select the **Installation verification** option



Once complete you should see the following messages...

```
[10/4/12 15:26:27:018 IST] 0000000a wtp W org.eclipse.jst.j2ee.commonarchivcore.internal.strategy.LoadStrategyImpl createFile FileNotFo
[10/4/12 15:26:27:019 IST] 0000000a wtp W org.eclipse.jst.j2ee.commonarchivcore.internal.strategy.LoadStrategyImpl createFile FileNotFo
[10/4/12 15:26:27:021 IST] 0000000a wtp W org.eclipse.jst.j2ee.commonarchivcore.internal.strategy.LoadStrategyImpl createFile FileNotFo
[10/4/12 15:26:27:022 IST] 0000000a wtp W org.eclipse.jst.j2ee.commonarchivcore.internal.strategy.LoadStrategyImpl createFile FileNotFo
[10/4/12 15:26:27:023 IST] 0000000a wtp W org.eclipse.jst.j2ee.commonarchivcore.internal.strategy.LoadStrategyImpl createFile FileNotFo
[10/4/12 15:26:27:025 IST] 0000000a wtp W org.eclipse.jst.j2ee.commonarchivcore.internal.strategy.LoadStrategyImpl createFile FileNotFo
[10/4/12 15:26:28:977 IST] 0000000a wtp W org.eclipse.jst.j2ee.commonarchivcore.internal.strategy.LoadStrategyImpl createFile FileNotFo
[10/4/12 15:26:28:979 IST] 0000000a wtp W org.eclipse.jst.j2ee.commonarchivcore.internal.strategy.LoadStrategyImpl createFile FileNotFo
VTLO040I: 64 errors/warnings are detected in the /opt/IBM/WebSphere/DeploymentManager/profiles/Dmgr01/logs/dmgr/SystemOut.log file
VTLO070I: The Installation Verification Tool verification succeeded.
VTLO080I: The installation verification is complete.
```

Using your Browser check that you login to Websphere Integrated Solutions Console (also known as the WAS Admin Console) via the URL address: "<https://dm&ihs.spnego.company.com:9043/ibm/console/logon.jsp>" using the administrator user & password define previously; in this case that admin user is "**wasadmin**".



Your Deployment Manager is now setup.

3.3 Install WAS V8 Applications Server on Node1 and Node2

In this scenario we have a 2 node cluster deployment so we will repeat these steps on both Node1 and Node2 systems.

Download and unzip the following four WAS V8 images/zip files into the folder **/opt/software/WAS80App**

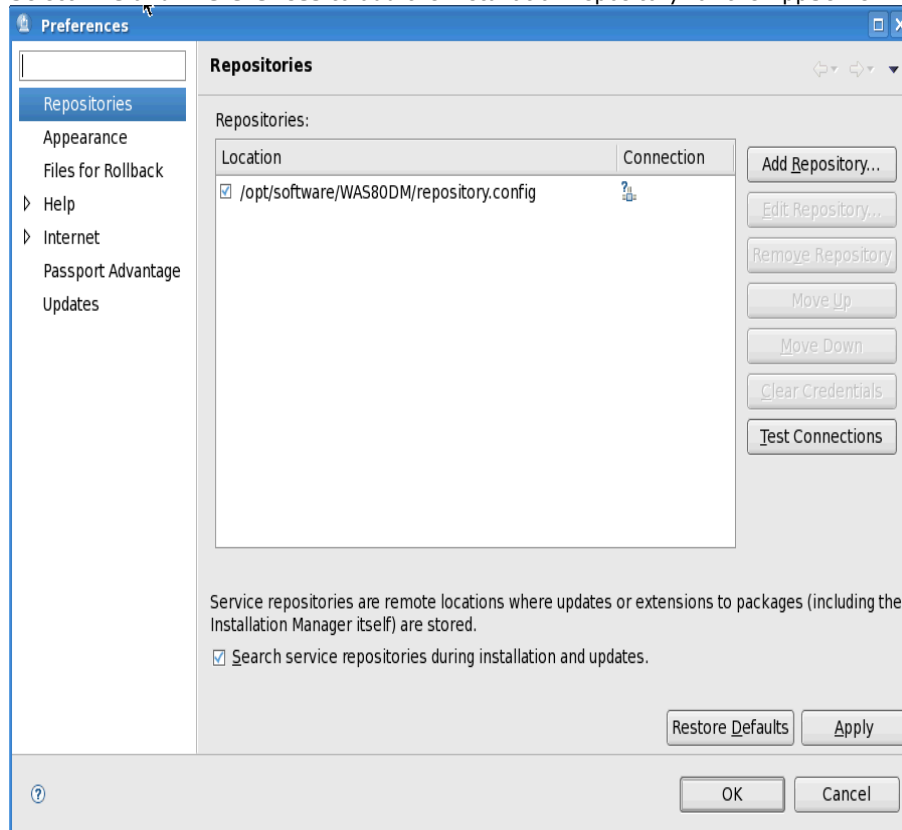
CZM9HML.zip
CZM9IML.zip
CZM9JML.zip
CZVG3ML.zip

After unzipping these files you should see the following files/folder in the WAS80App folder:

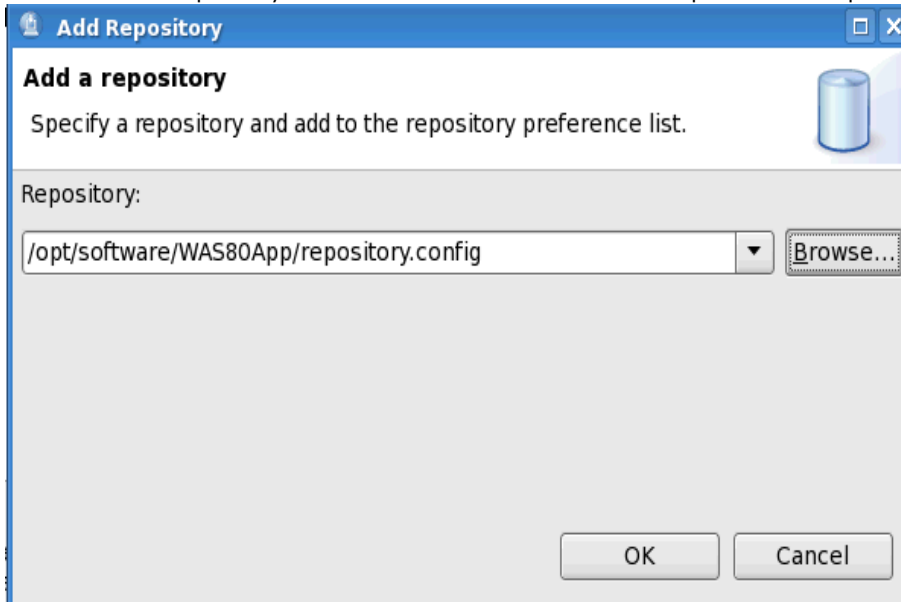
```
[root@dubxpcvm766 WAS80App]# ls
Copyright.txt  disk1  disk2  disk3  disk4  lafiles  readme  Remote_Installation_Tool_for_IBM_i  repository.config
[root@dubxpcvm766 WAS80App]#
```

Start Installation Manager which you installed earlier.

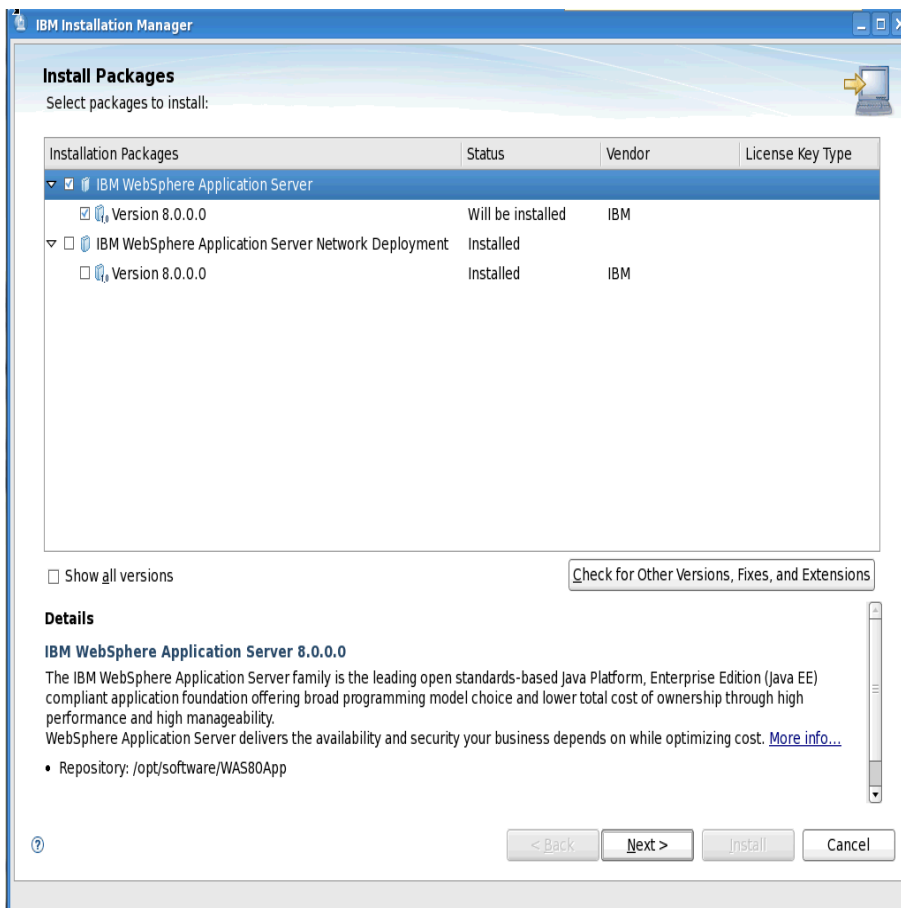
Select **File** and **Preferences** to add the installation repository for the AppServer install.



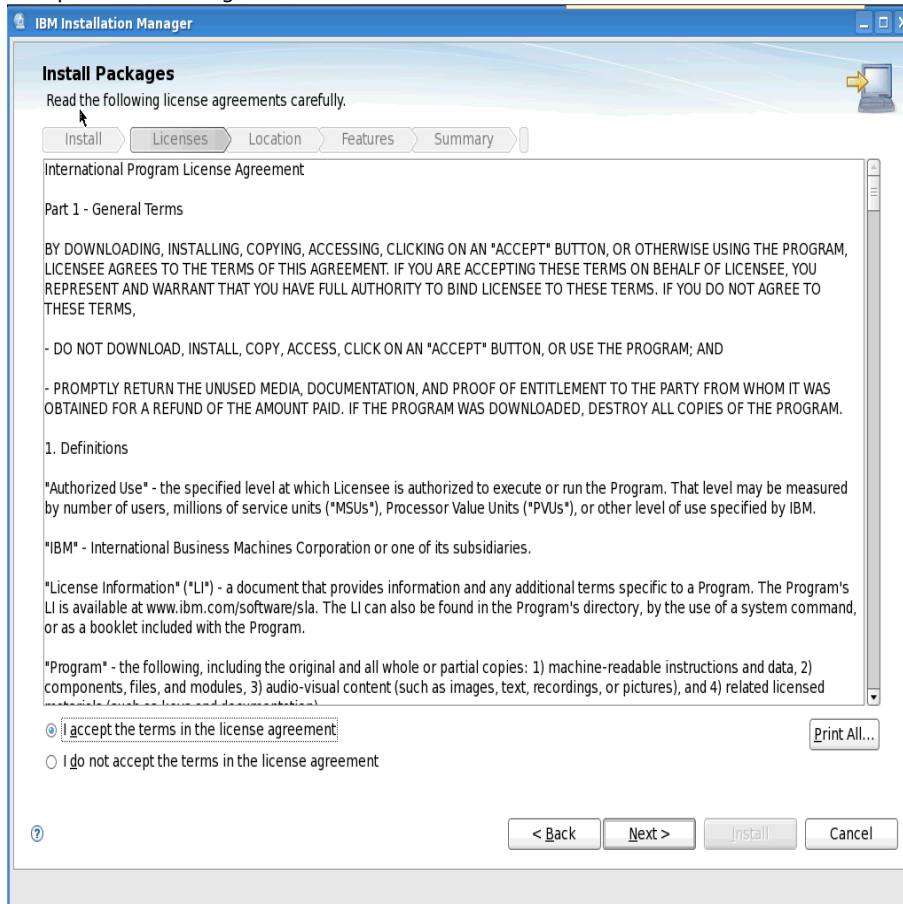
Select the Add Repository... button and enter the details to the path for the repository.config file. Select OK to continue...



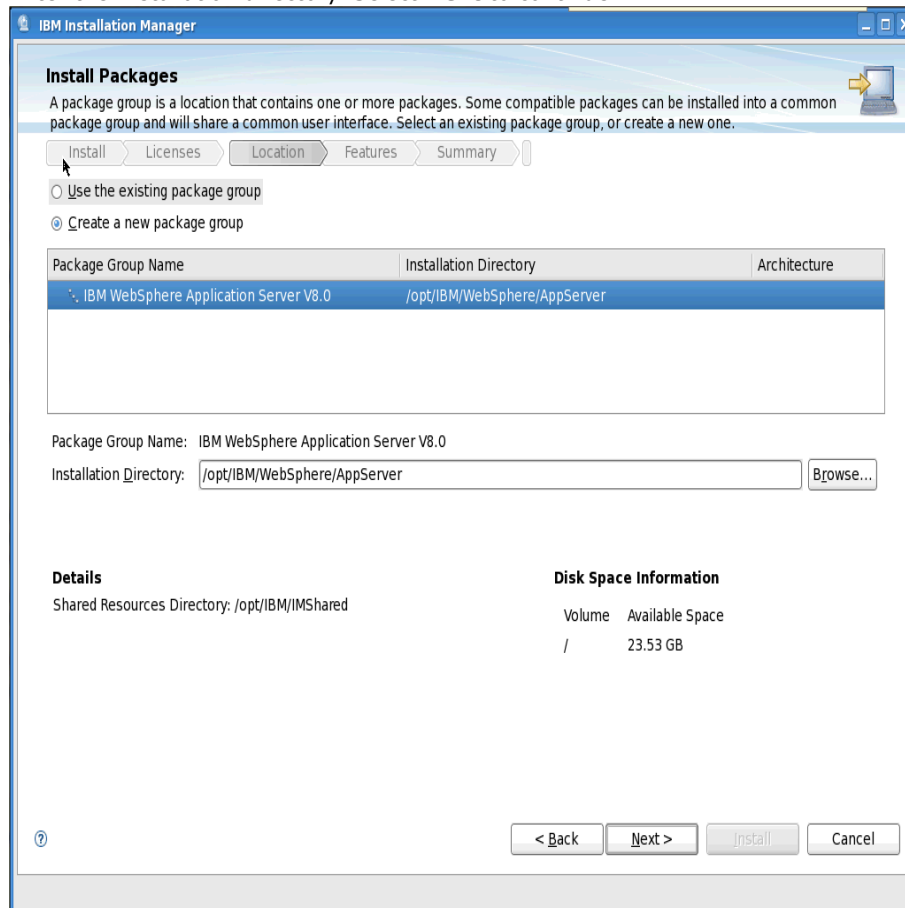
Now select **Install** from the main window on the installation manager.



Accept the license agreement and **Next** to continue...



Enter the Installation directory. Select **Next** to continue...



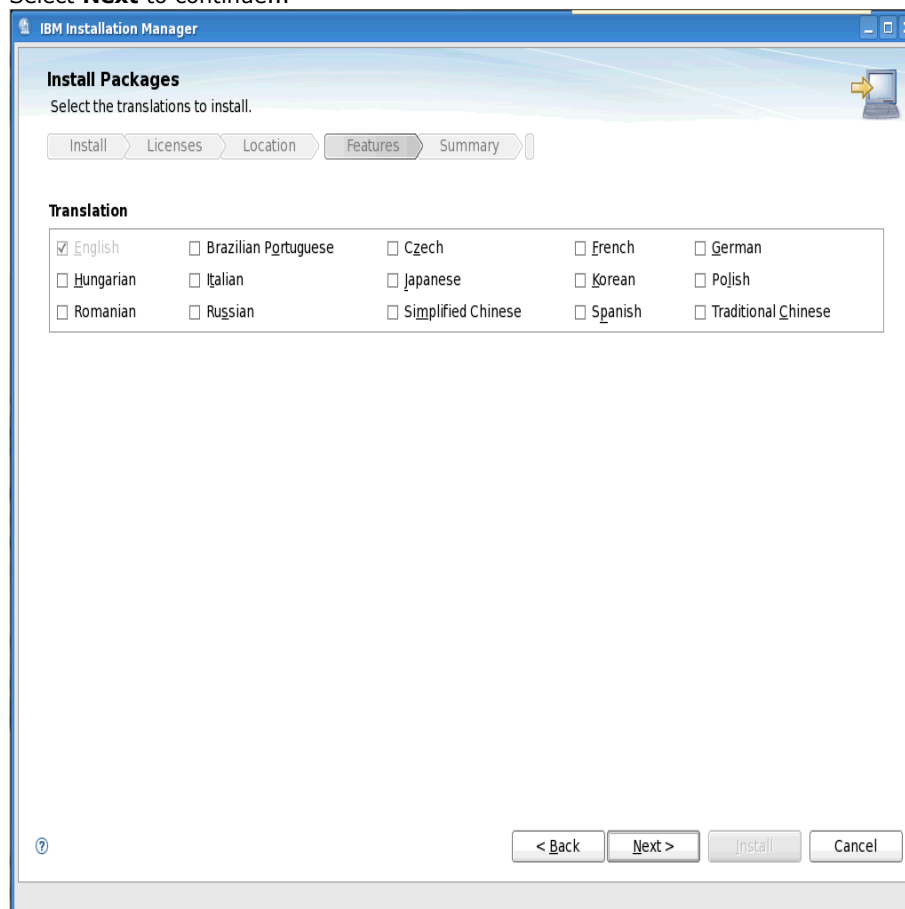
The screenshot shows the 'Install Packages' window in IBM Installation Manager. The 'Location' tab is selected in the top navigation bar. Below the tabs, there are two radio buttons: 'Use the existing package group' (unselected) and 'Create a new package group' (selected). A table lists the package group details:

Package Group Name	Installation Directory	Architecture
IBM WebSphere Application Server V8.0	/opt/IBM/WebSphere/AppServer	

Below the table, the 'Package Group Name' is 'IBM WebSphere Application Server V8.0' and the 'Installation Directory' is '/opt/IBM/WebSphere/AppServer' with a 'Browse...' button. At the bottom, there are buttons for '< Back', 'Next >', 'Install', and 'Cancel'. A 'Details' section shows 'Shared Resources Directory: /opt/IBM/IMShared' and a 'Disk Space Information' table:

Volume	Available Space
/	23.53 GB

Select **Next** to continue...

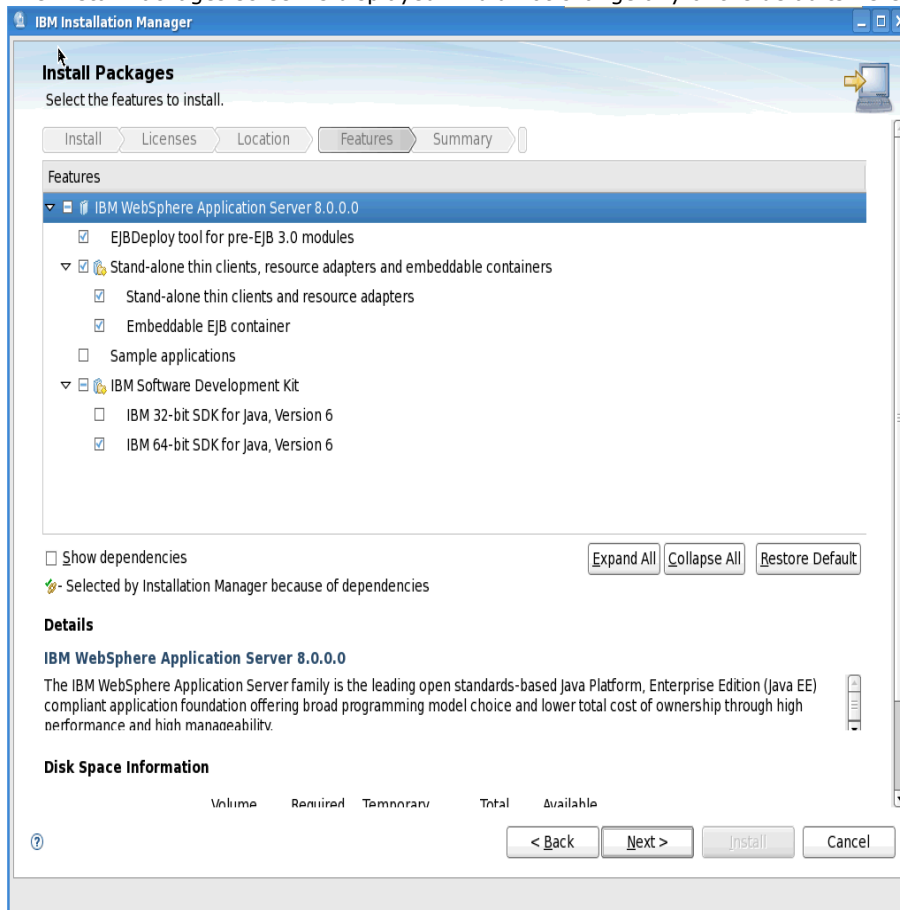


The screenshot shows the 'Install Packages' window in IBM Installation Manager, with the 'Features' tab selected. The 'Translation' section contains a list of languages with checkboxes:

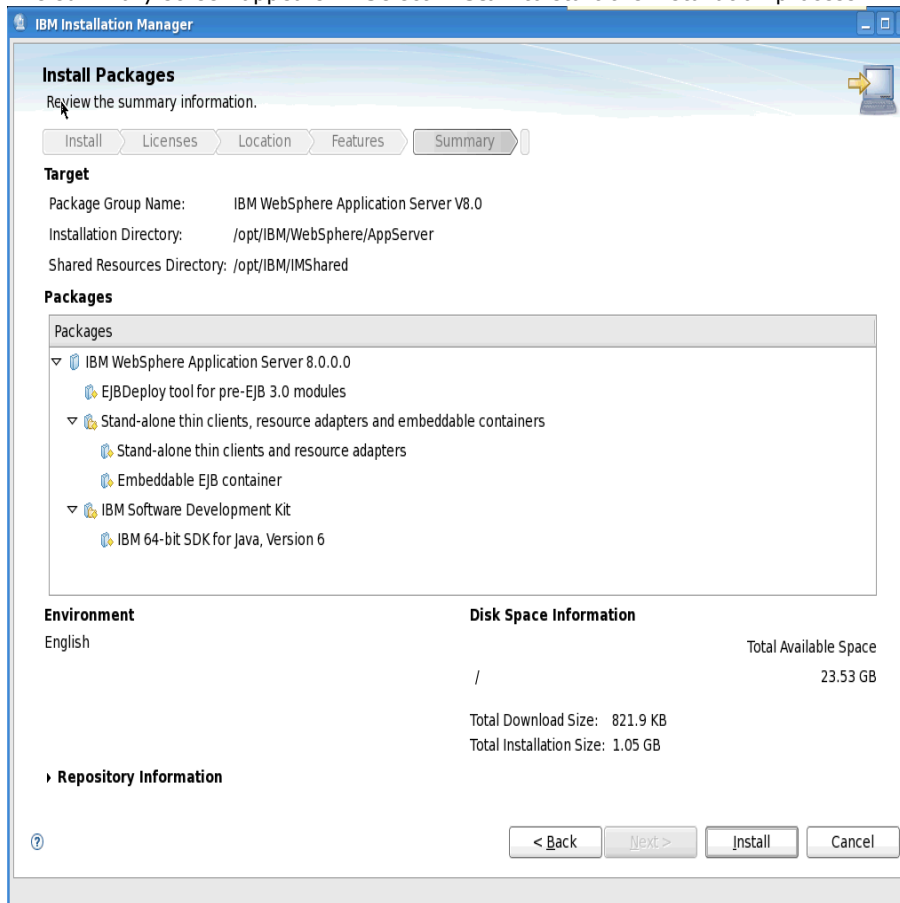
<input checked="" type="checkbox"/> English	<input type="checkbox"/> Brazilian Portuguese	<input type="checkbox"/> Czech	<input type="checkbox"/> French	<input type="checkbox"/> German
<input type="checkbox"/> Hungarian	<input type="checkbox"/> Italian	<input type="checkbox"/> Japanese	<input type="checkbox"/> Korean	<input type="checkbox"/> Polish
<input type="checkbox"/> Romanian	<input type="checkbox"/> Russian	<input type="checkbox"/> Simplified Chinese	<input type="checkbox"/> Spanish	<input type="checkbox"/> Traditional Chinese

At the bottom, there are buttons for '< Back', 'Next >', 'Install', and 'Cancel'.

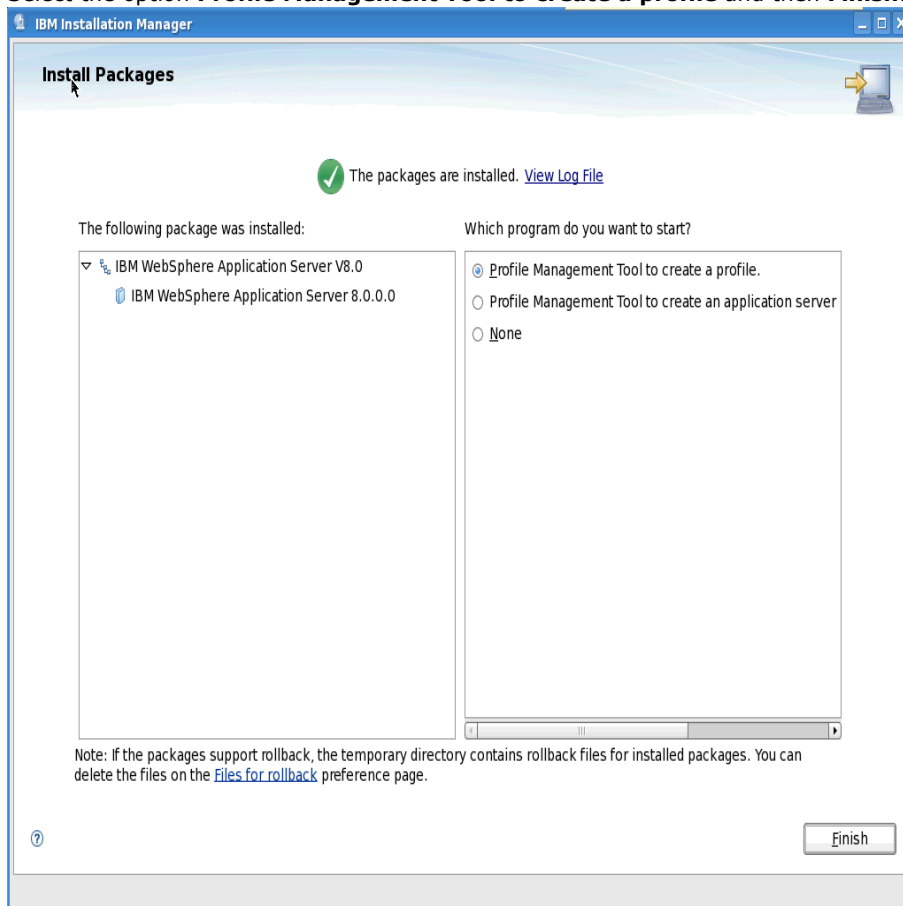
The Install Packages screen is displayed. I did not change any of the defaults here. Select **Next** to continue...



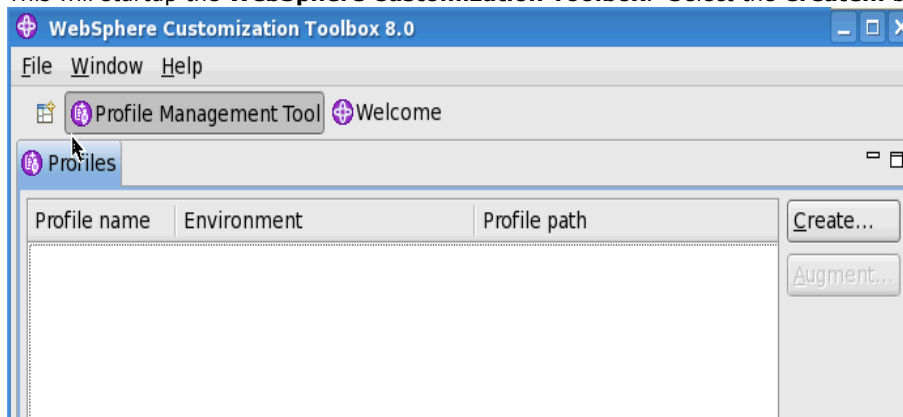
The summary screen appears.... Select **Install** to start the installation process...



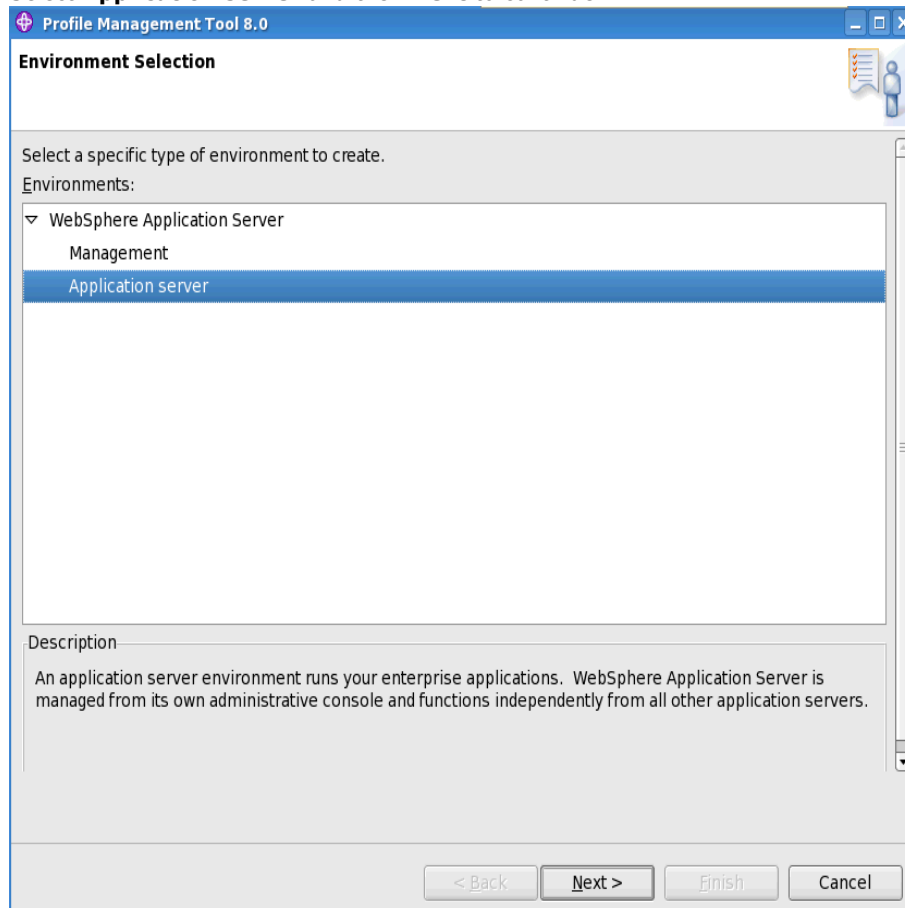
After a few minutes the install will complete and you will see the following screen.
Select the option **Profile Management Tool to create a profile** and then **Finish**.



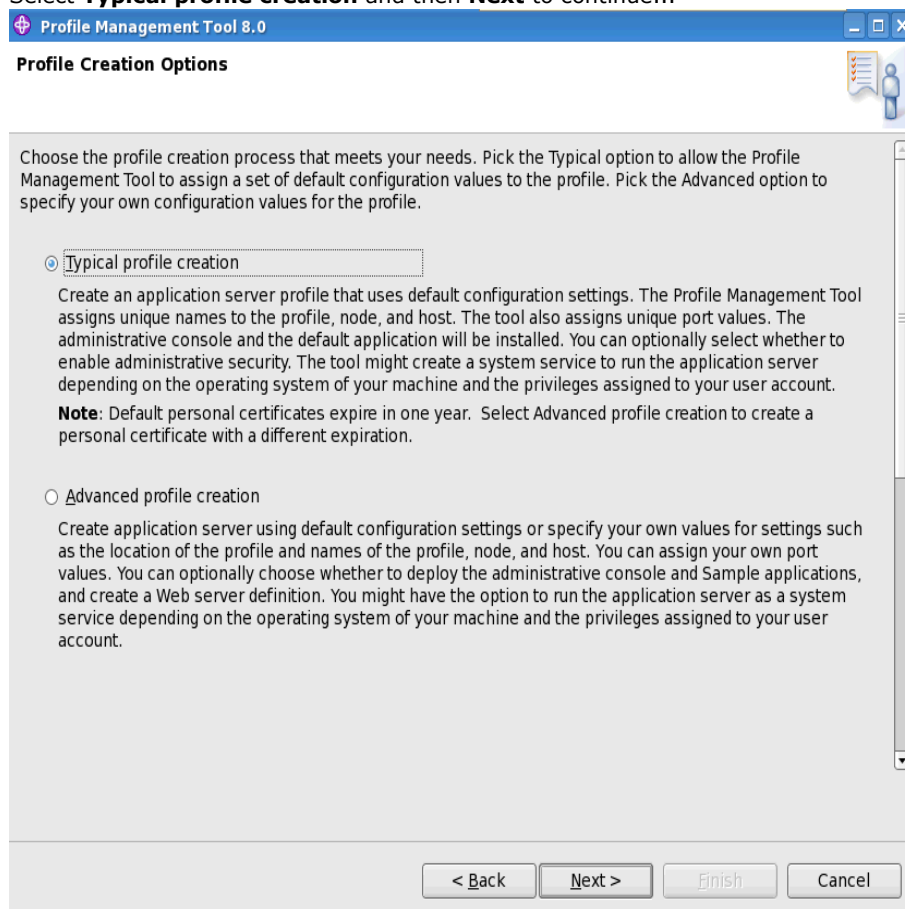
This will startup the **WebSphere Customization Toolbox**. Select the **Create...** button



Select **Application server** and then **Next** to continue...



Select **Typical profile creation** and then **Next** to continue...



Ensure the **Enable administrative security** box is checked and enter a User name and Password for the WAS Admin. I use the same User name and password that I used when setting up the Deployment Manager ie "**wasadmin**"

Select **Next** to continue

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 > Finish Cancel

The summary screen is displayed. Select **Create** to create the profile...

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: Application server
Location: /opt/IBM/WebSphere/AppServer/profiles/AppSrv01
Disk space required: 200 MB

Profile name: AppSrv01
Make this profile the default: True
Performance tuning setting: Standard

Node name: dubxpcvm766Node01
Server name: server1
Host name: dubxpcvm766.mul.ie.ibm.com

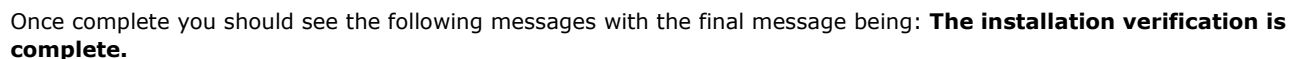
Deploy the administrative console (recommended): True
Deploy the default application: True

Enable administrative security (recommended): True

Administrative console port: 9061
Administrative console secure port: 9044

< Back Create Finish Cancel

Ensure the **Launch the First steps console** option is selected; then click on **Finish**



-
- Redo these steps on Node2.

3.4 Install IBM HTTP Server (IHS) V8

NOTE: In this scenario we install the HTTP Server on the same machine as the DM

Download the following WAS Supplemental images/zip files into the folder **/opt/software/WAS80Sup** on your IHS system; the four image/zip files are:

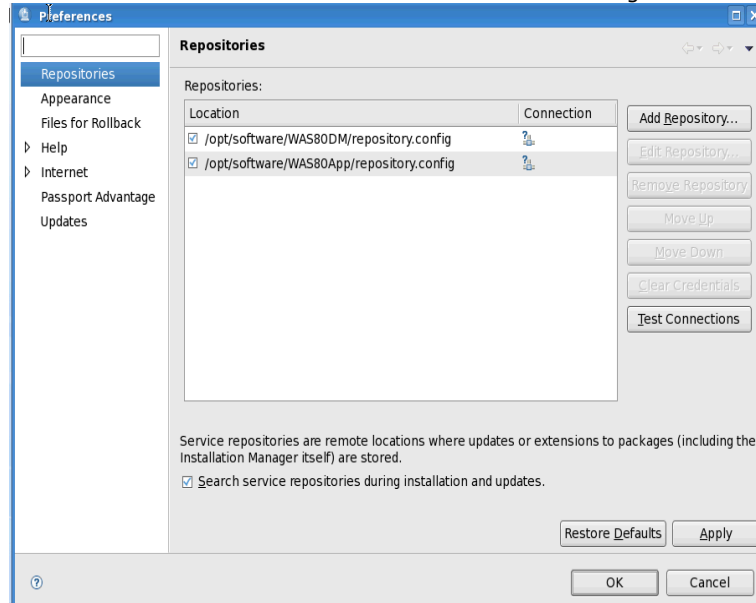
CZM91ML.zip
CZM94ML.zip
CZM95ML.zip
CZXR9ML.zip

Unzip these zip files in the WAS80Sup folder and you should see following folders/files:

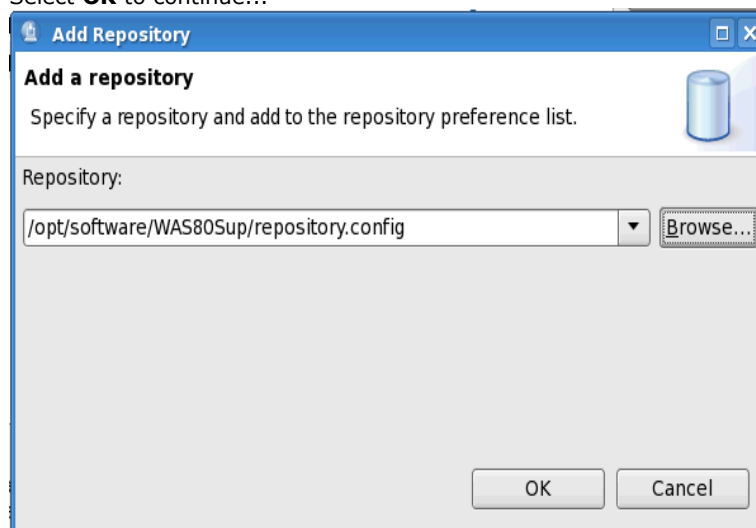
```
[root@dubxpcvm766 WAS80Sup]# ls
Copyright.txt  disk1  disk2  disk3  disk4  lafiles  readme_appclient  readme_ihs  readme_pluginclient  readme_plugins  readme_wct  Remote_Installation_Tool_for_IBM_i  repository.config
[root@dubxpcvm766 WAS80Sup]#
```

Start the Installation Manager which you should have installed earlier.

Select **File** then **Preferences** and in the Preference dialog select **Add Repository...**



Select the **Add Repository...** button and enter the details to the path for the Supplementary **repository.config** file. Select **OK** to continue...



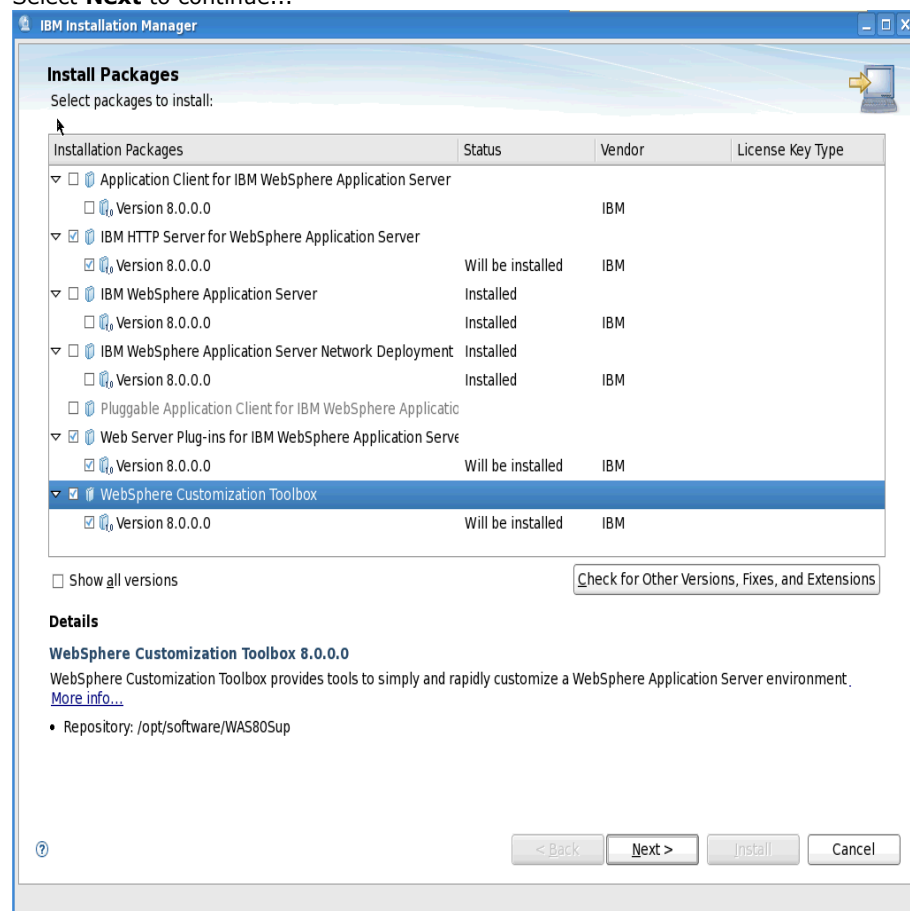
From the Installation Manager main window select **Install**. This will pickup that the HTTP Server, Plugins and Toolbox is now to be installed.

Select the following three options (as in the next screen shot):

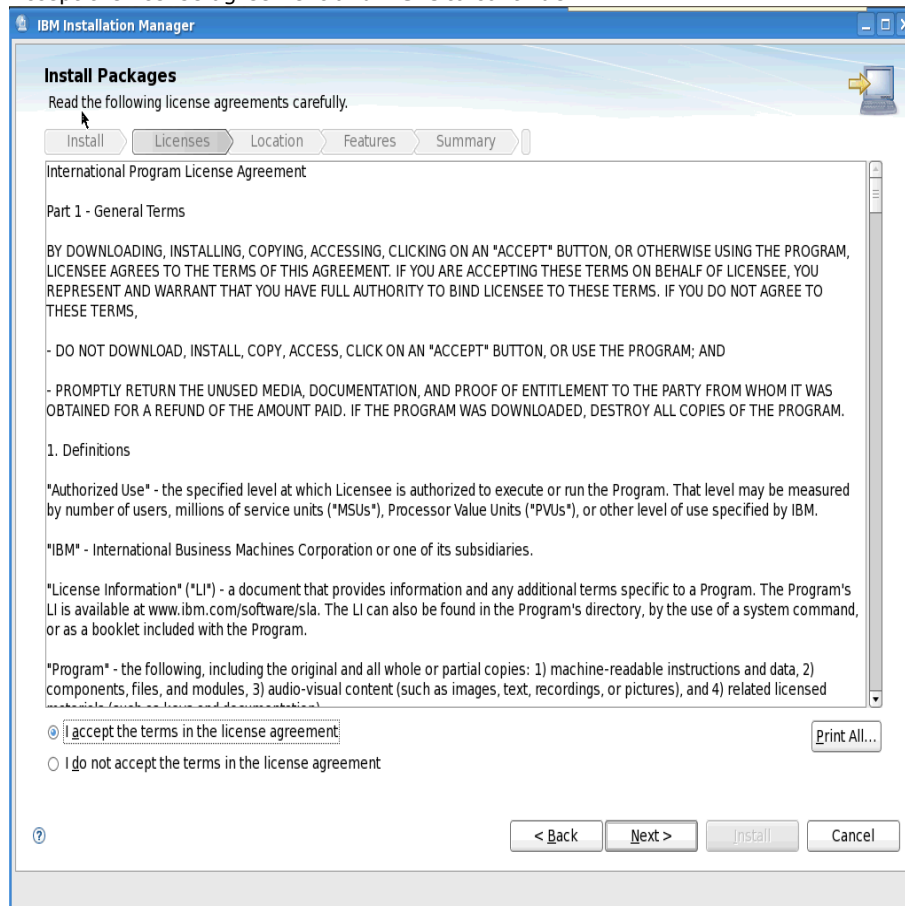
1. IBM HTTPServer for WAS
2. Web Server Plug-ins for IBM WAS
3. WebSphere Customization Toolbox

Do NOT select **Application Client for IBM WAS**

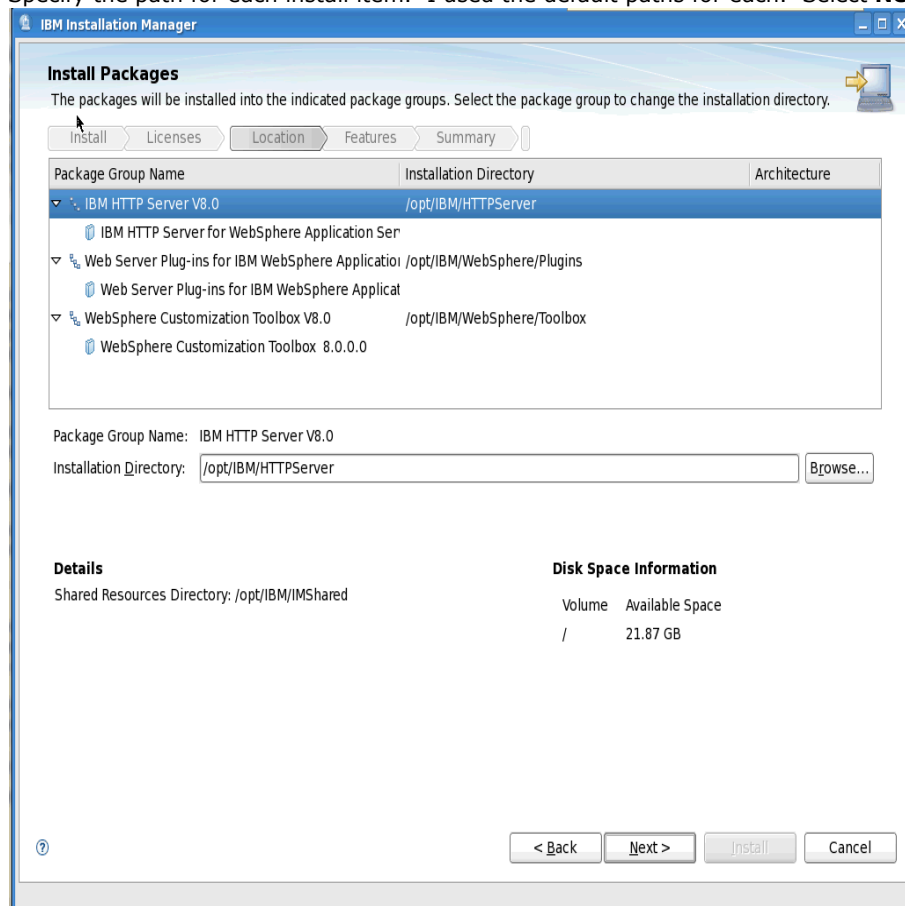
Select **Next** to continue...



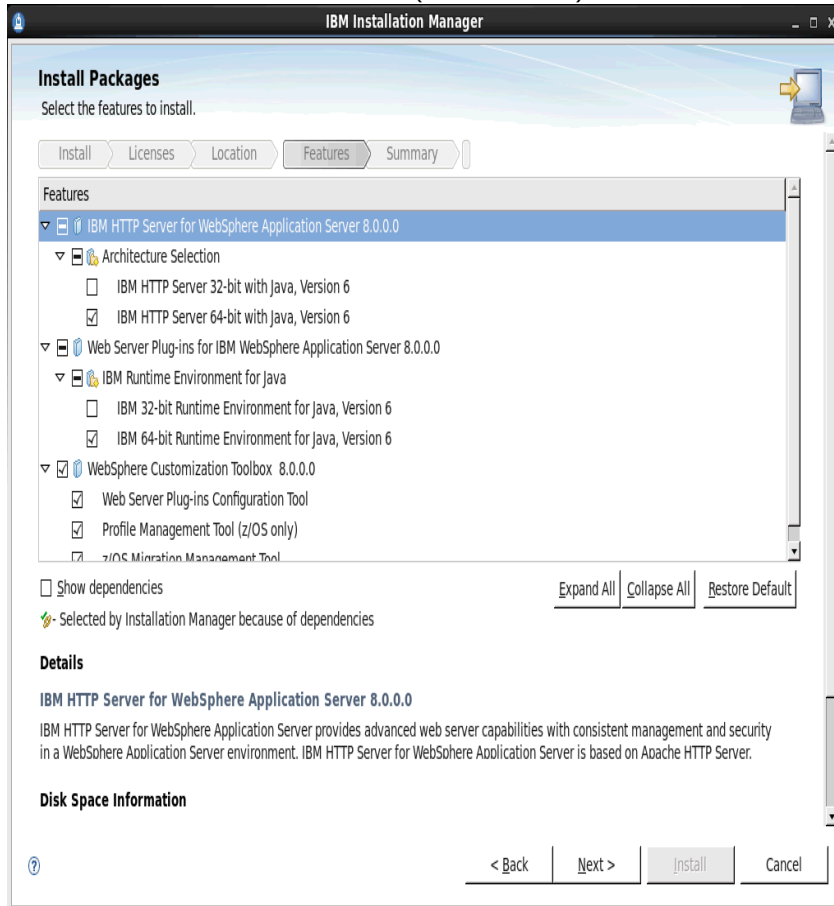
Accept the license agreement and **Next** to continue...



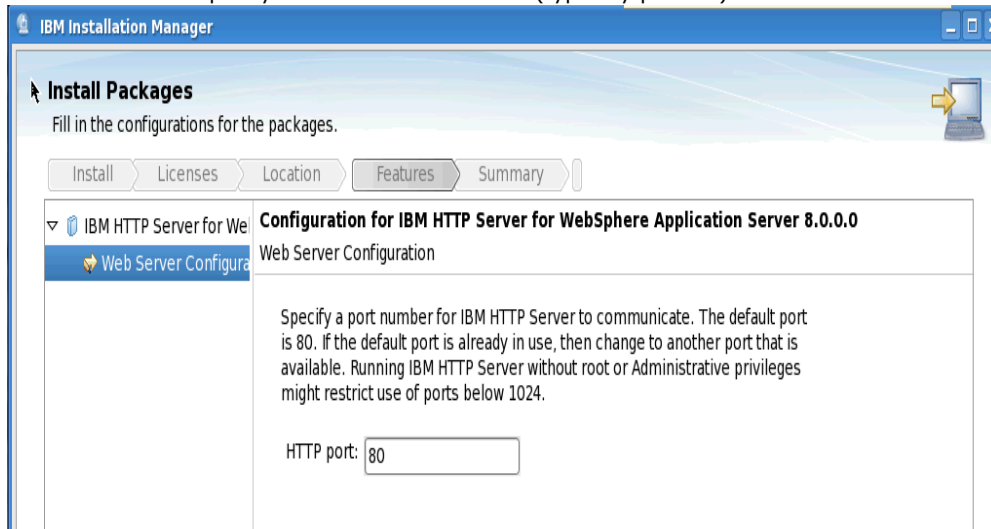
Specify the path for each install item. I used the default paths for each. Select **Next** to continue.



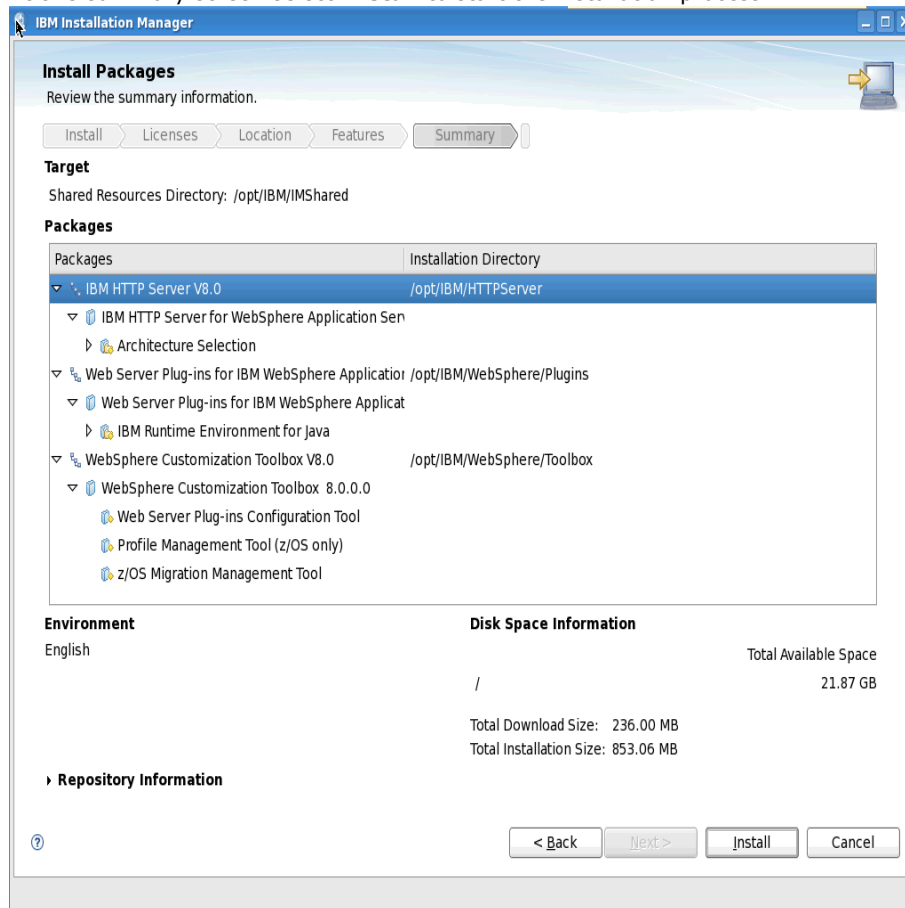
Select the features to install (as seen below) and **Next** to continue...



Enter the port you want HTTP to run on (typically port 80) and **Next** to continue...

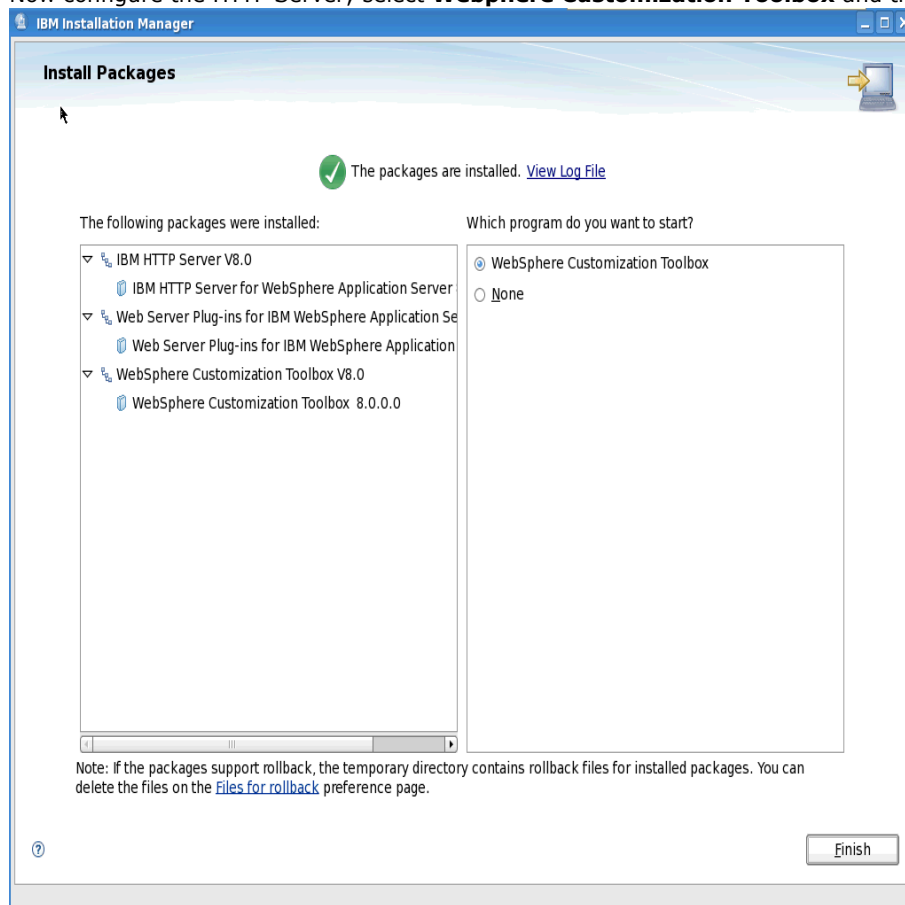


At this summary screen select **Install** to start the installation process...

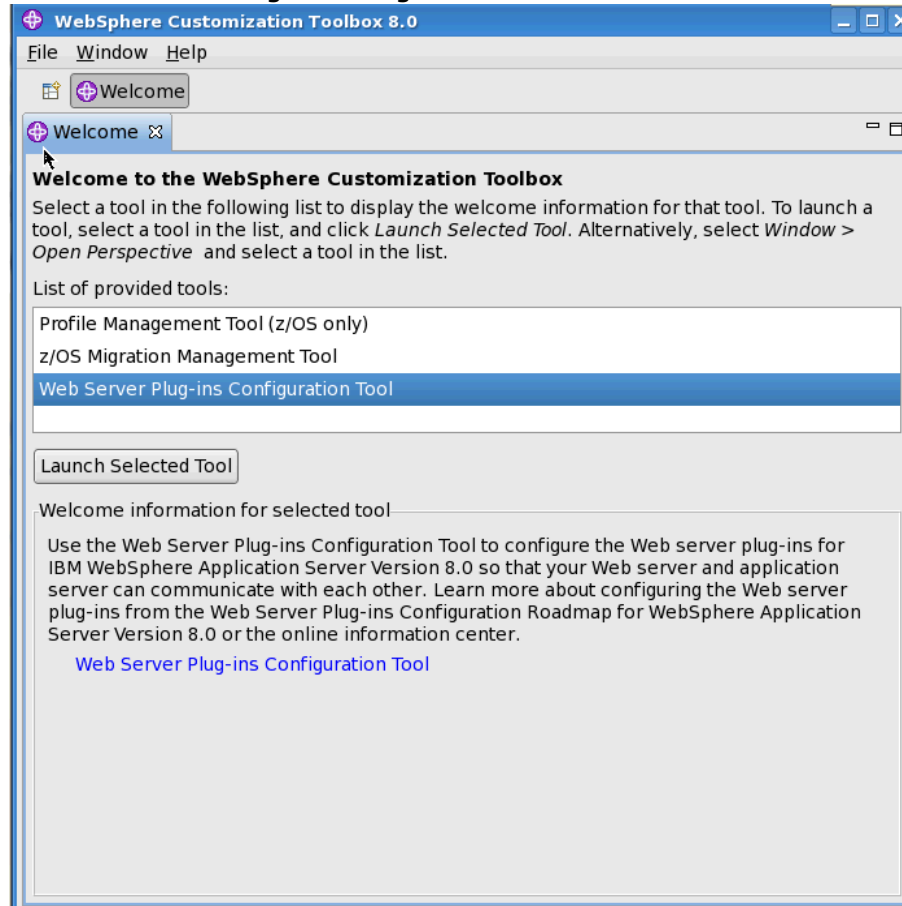


After a few moments the following screen will appear:

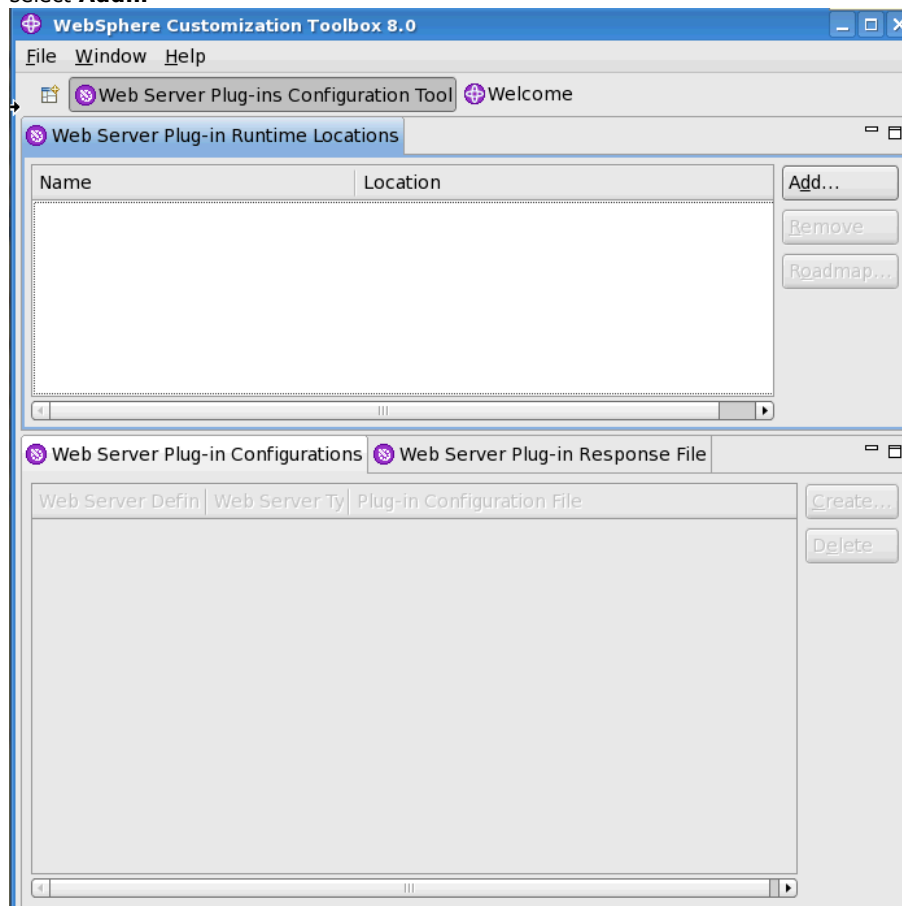
Now configure the HTTP Server; select **Webphere Customization Toolbox** and then **Finish**.



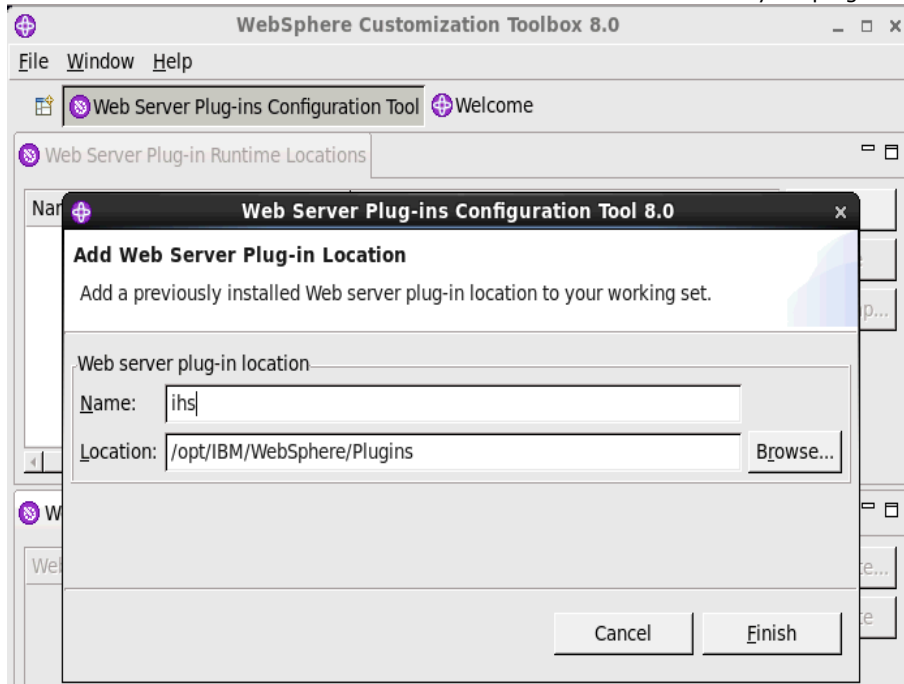
Select **Web Server Plug-ins Configuration Tool** and then select **Launch Selected Tool**



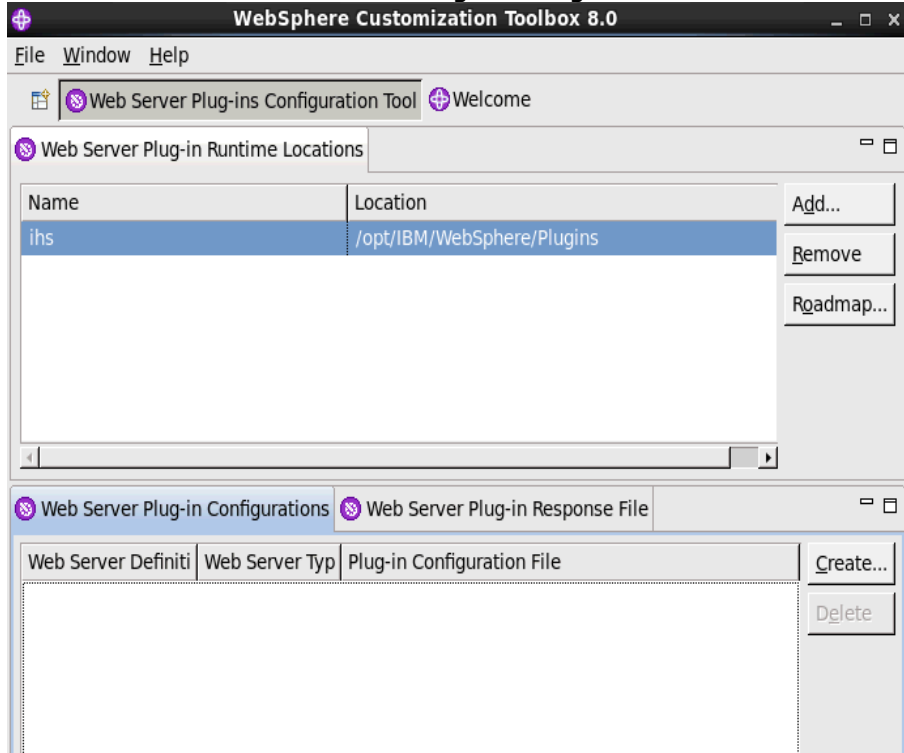
select **Add...**



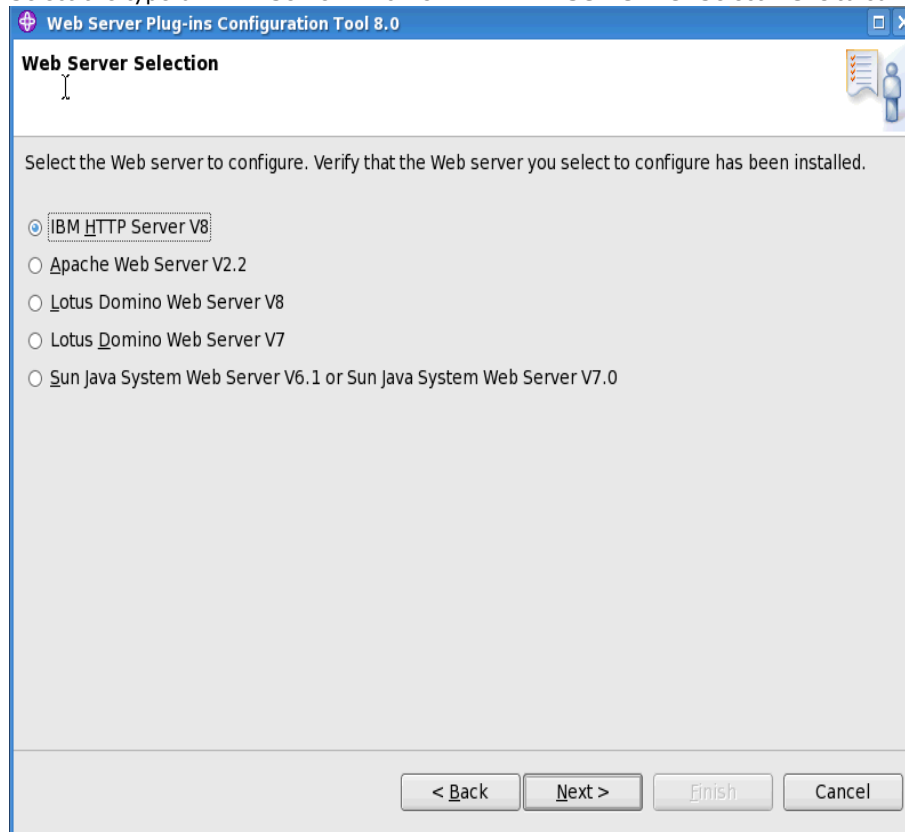
Enter the name of the HTTP Server and the location to where your plugins were installed earlier. Select **Finish** to continue



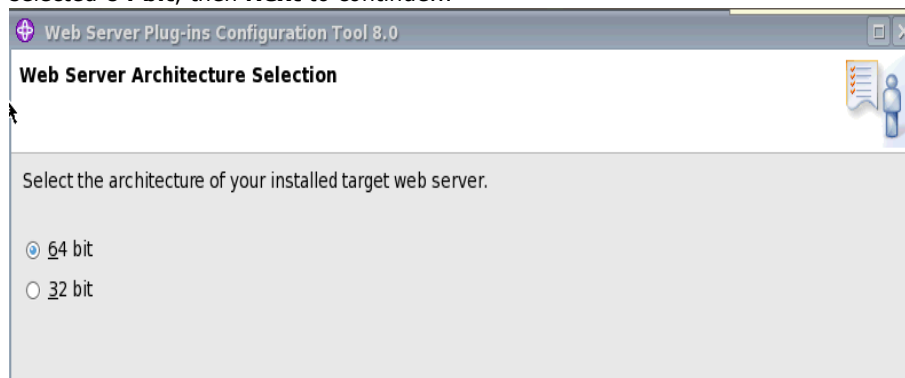
Select **Create...** for the **Web Server Plug-in Configuration**



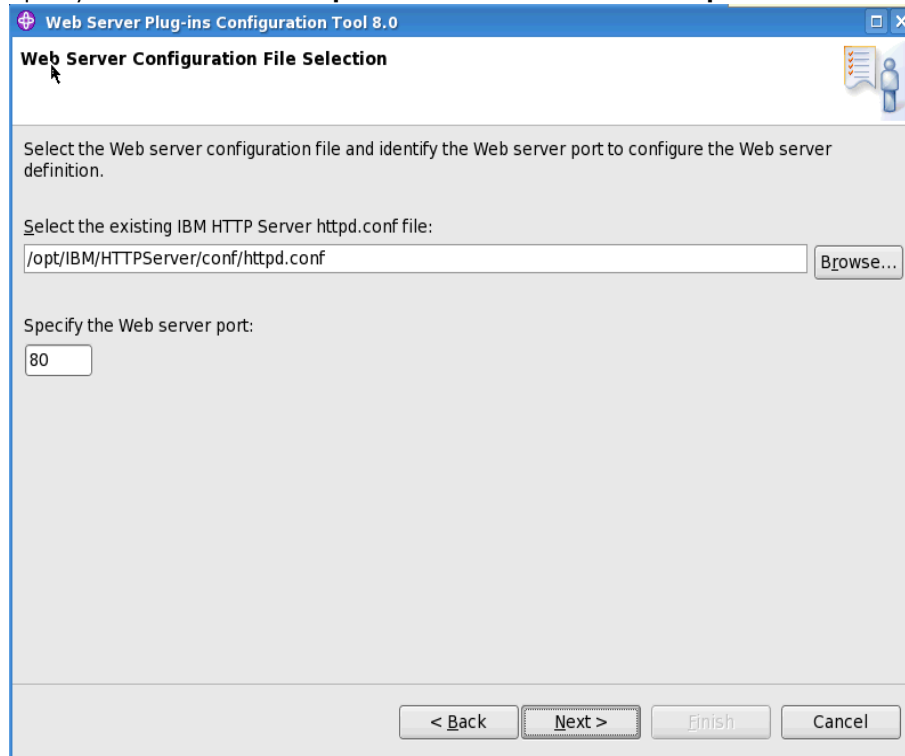
Select the type of HTTP Server which is **IBM HTTP Server V8**. Select **Next** to continue...



selected **64 bit**, then **Next** to continue...



Specify the location of the **httpd.conf** file and set **Web server port=80** and then **Next** to continue



Web Server Plug-ins Configuration Tool 8.0

Web Server Configuration File Selection

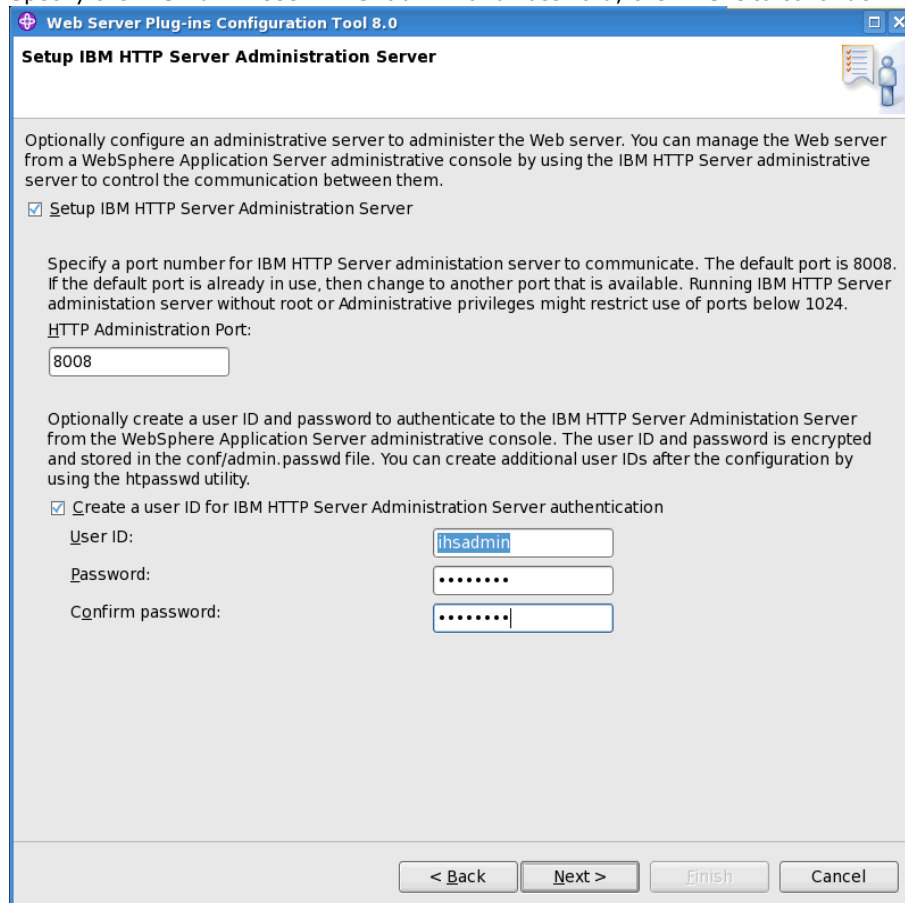
Select the Web server configuration file and identify the Web server port to configure the Web server definition.

Select the existing IBM HTTP Server httpd.conf file:

Specify the Web server port:

< Back Next > Finish Cancel

Specify the IHS Admin UserID=**ishadmin** and Password; then **Next** to continue



Web Server Plug-ins Configuration Tool 8.0

Setup IBM HTTP Server Administration Server

Optionally configure an administrative server to administer the Web server. You can manage the Web server from a WebSphere Application Server administrative console by using the IBM HTTP Server administrative server to control the communication between them.

☒ Setup IBM HTTP Server Administration Server

Specify a port number for IBM HTTP Server administration server to communicate. The default port is 8008. If the default port is already in use, then change to another port that is available. Running IBM HTTP Server administration server without root or Administrative privileges might restrict use of ports below 1024.

HTTP Administration Port:

Optionally create a user ID and password to authenticate to the IBM HTTP Server Administration Server from the WebSphere Application Server administrative console. The user ID and password is encrypted and stored in the conf/admin.passwd file. You can create additional user IDs after the configuration by using the httpasswd utility.

☒ Create a user ID for IBM HTTP Server Administration Server authentication

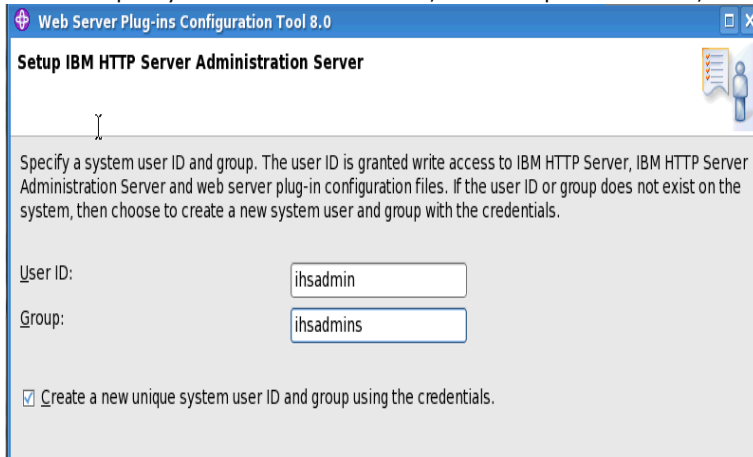
User ID:

Password:

Confirm password:

< Back Next > Finish Cancel

Specify the UserID=**ihsadmin**, and Group=**ihsadmins**, then **Next** to continue



Web Server Plug-ins Configuration Tool 8.0

Setup IBM HTTP Server Administration Server

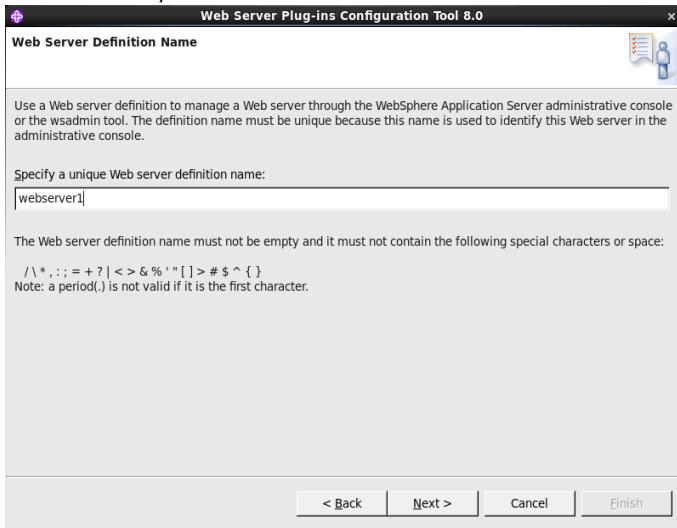
Specify a system user ID and group. The user ID is granted write access to IBM HTTP Server, IBM HTTP Server Administration Server and web server plug-in configuration files. If the user ID or group does not exist on the system, then choose to create a new system user and group with the credentials.

User ID:

Group:

☒ Create a new unique system user ID and group using the credentials.

Give your web server a definition name. Select **Next** to continue...



Web Server Plug-ins Configuration Tool 8.0

Web Server Definition Name

Use a Web server definition to manage a Web server through the WebSphere Application Server administrative console or the wsadmin tool. The definition name must be unique because this name is used to identify this Web server in the administrative console.

Specify a unique Web server definition name:

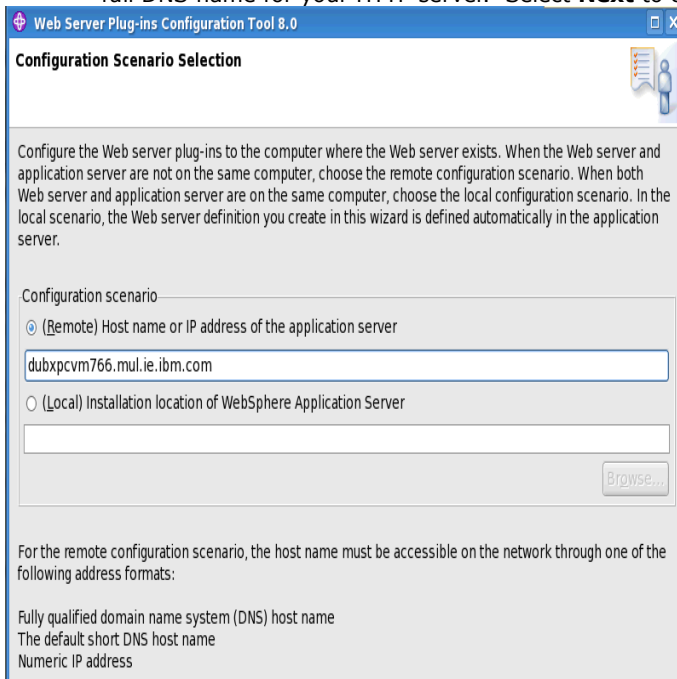
The Web server definition name must not be empty and it must not contain the following special characters or space:

/ \ * . : ; = + ? [< > & % ' " [] > # \$ ^ { }

Note: a period(.) is not valid if it is the first character.

< Back Next > Cancel Finish

Under **Configuration scenario** select "**(Remote) Host name or IP address for the application server**" and enter the full DNS name for your HTTP server. Select **Next** to continue...



Web Server Plug-ins Configuration Tool 8.0

Configuration Scenario Selection

Configure the Web server plug-ins to the computer where the Web server exists. When the Web server and application server are not on the same computer, choose the remote configuration scenario. When both Web server and application server are on the same computer, choose the local configuration scenario. In the local scenario, the Web server definition you create in this wizard is defined automatically in the application server.

Configuration scenario

☒ (Remote) Host name or IP address of the application server

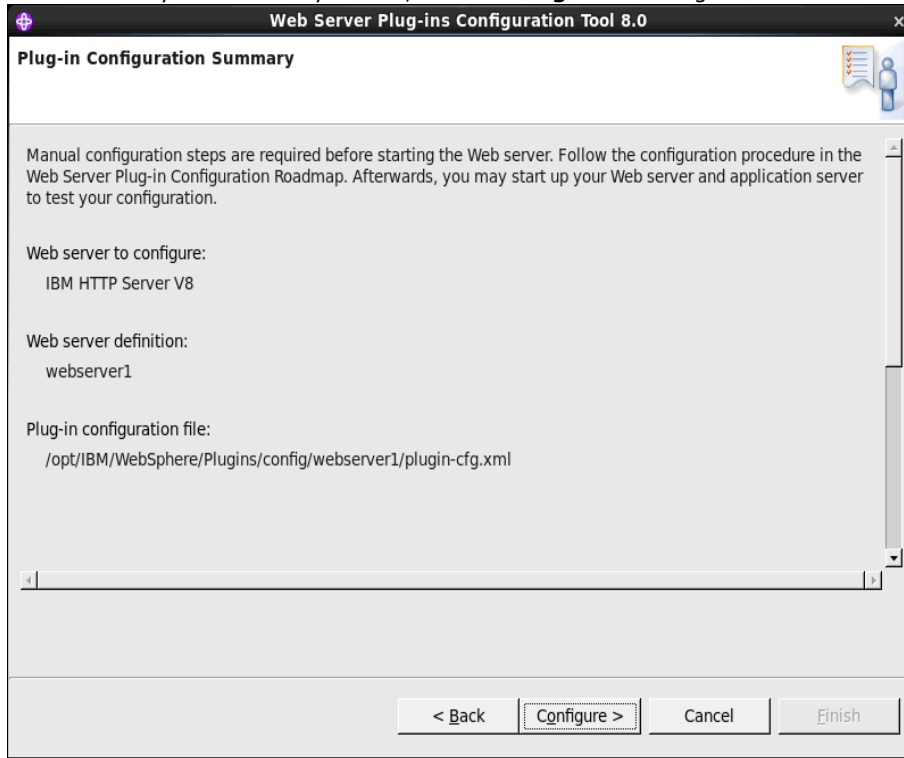
☐ (Local) Installation location of WebSphere Application Server

Browse...

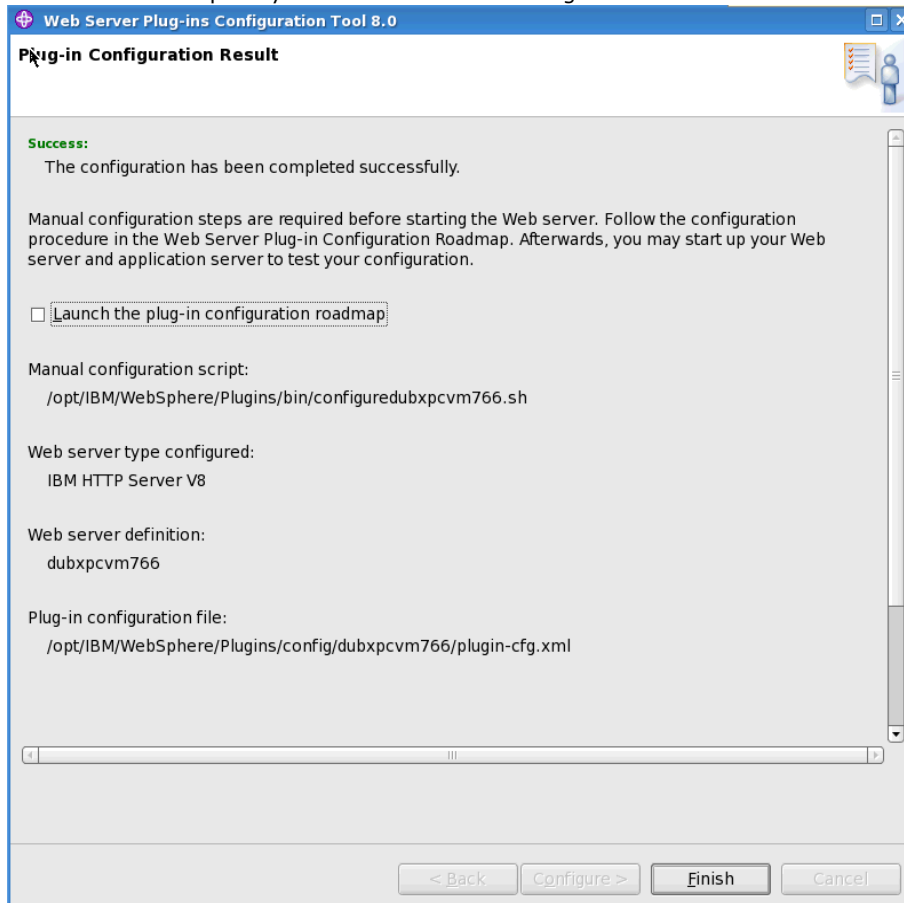
For the remote configuration scenario, the host name must be accessible on the network through one of the following address formats:

Fully qualified domain name system (DNS) host name
The default short DNS host name
Numeric IP address

Finally the Summary screen; select **Configure** to configure the IBM HTTP Server.



Once complete you should see the following... Select **Finish** to close the wizard.



3.5 Update DM, Applications Server and IHS to required Fixpack and iFixes

IBM Connections V4.5 requires the following WAS updated:

1. **WAS V8 Fixpack V8.0.0.5**
2. **Additional WAS V8 iFixes; they are:**
 - [PM62615 - Here is Fix Central iFix for PM62615](#)
 - [PM71430 - Here is Fix Central iFix for PM71430](#)

1. How to update your WAS V8 environment to V8.0.0.5

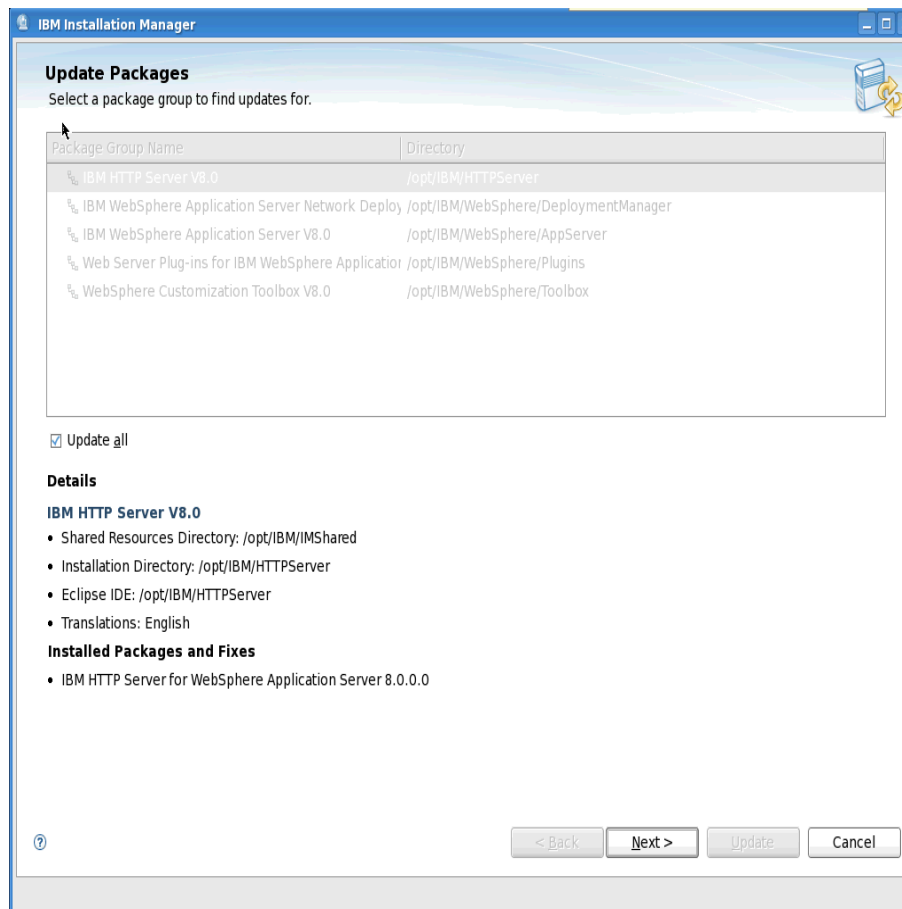
Repeat these Steps for each of the following system: DM, WAS(Application Servers) and the IHS system

Stop all servers (DM, WAS, IHS) before installing the fixpacks

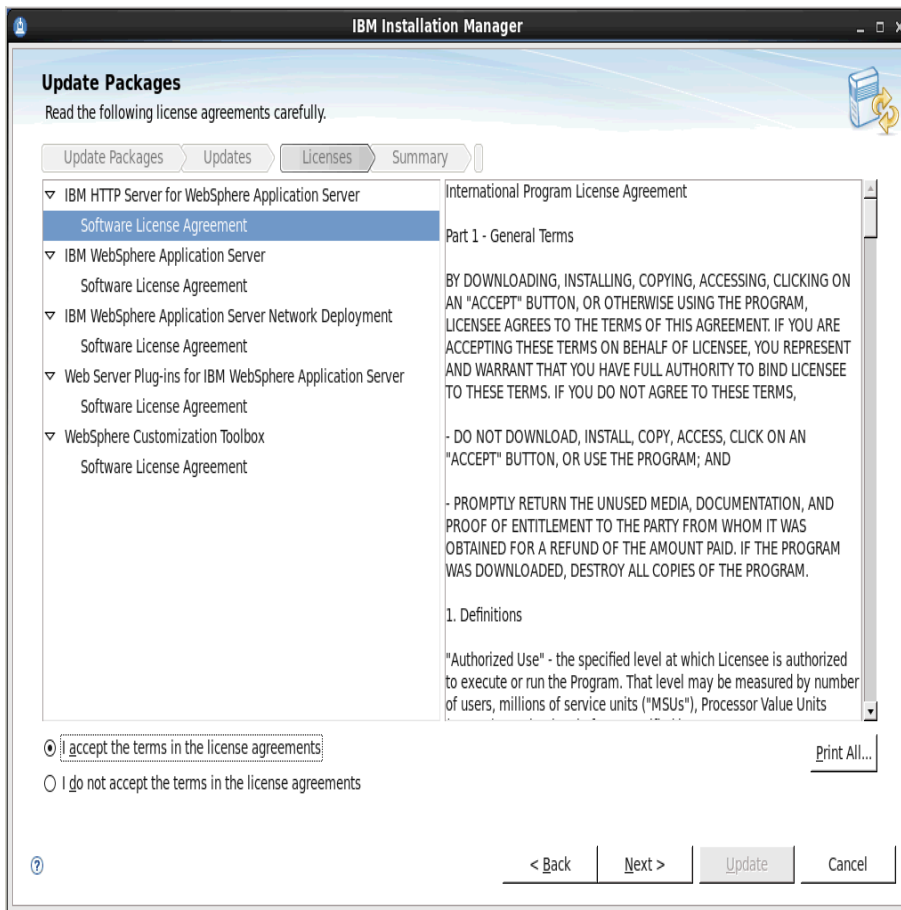
Launch the Installation Manager and select the **Update** link... and on the next screen select the **Update all** check box; You may be requested to enter your IBM registered credentials at this point.

Note: The next screen shown is an example of what you would see if the DM, Application server and IHS co-existed on the same machine

Select **Next** to continue



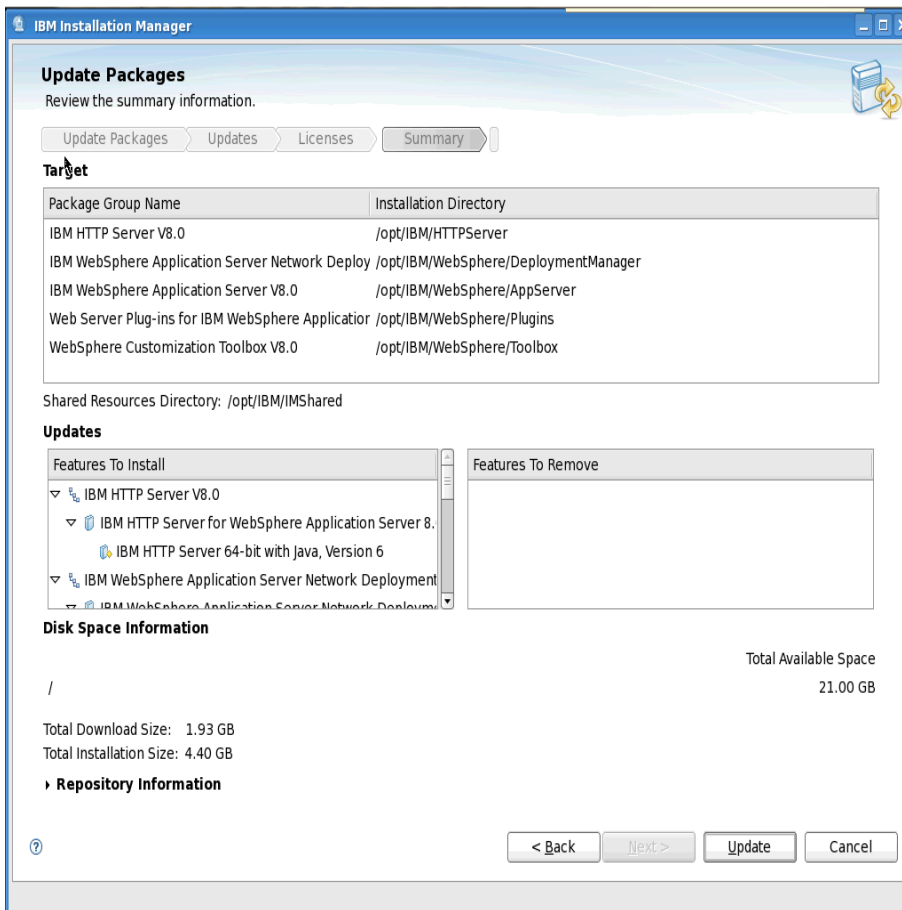
Validation and preparation checks will then happen and after a few minutes you will get this next screen. Accept the licence agreement and then select **Next** to continue...



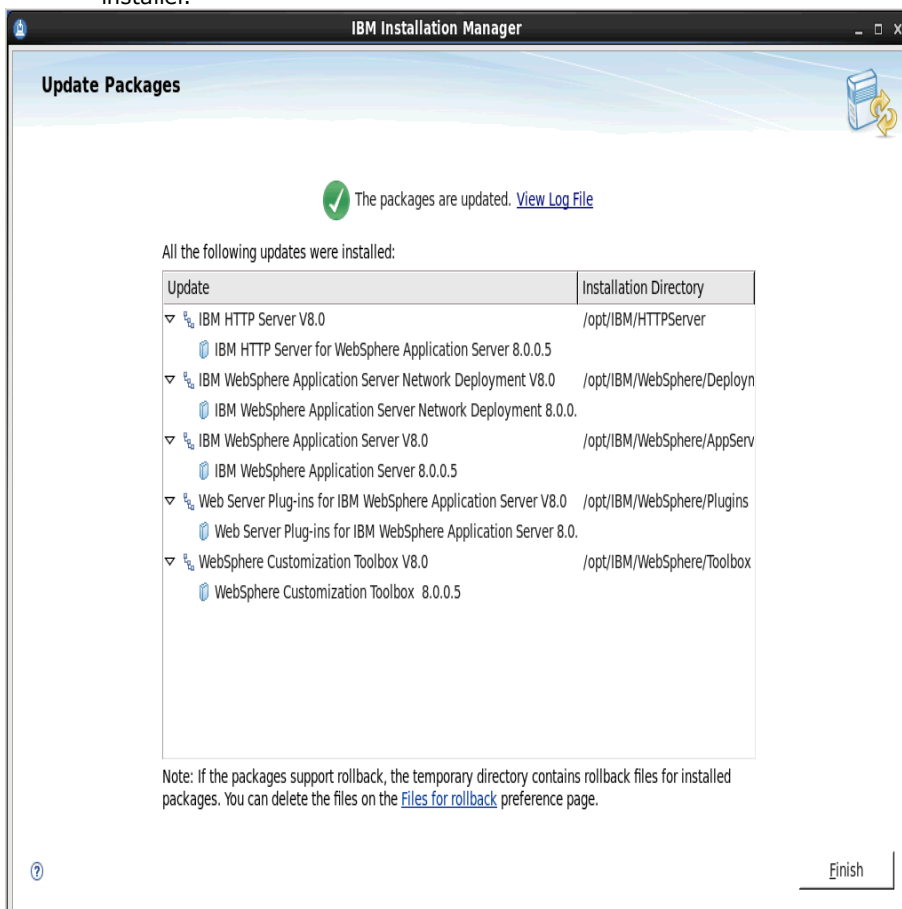
The update installer will now collect the files needed to do the update/install; this will take a few minutes...

Once completed, select the **Update** button. This will update your server to the **latest fixpack** for WAS 8.0 which is (at the time of writing) ie **V8.0.0.5**.

Note: IBM Connections V4.5 at release requires WAS V8 fix pack 8.0.0.5. At the time of writing this was the latest fixpack available. Please check with IBM Connections V4.5 documentation for support for later releases of WAS fixpacks.



After several minutes the update will complete returning the following screen. Now select **Finish** to exit the Update installer.



You have now updated to V8.0.0.5

___2. Additional WAS V8 iFixes required to support IBM Connections V4.5

There are additional iFixes that are required to be installed for IBM Connections V4.5, and these are installed on the Deployment manager; they are:

- [PM62615 - Here is Fix Central iFix for PM62615](#)
- [PM71430 - Here is Fix Central iFix for PM71430](#)

Steps - on the DM system do the following:

download the iFixes into separate folders and unzip them

Load Installation Manager and select **Files**, then **Repositories**

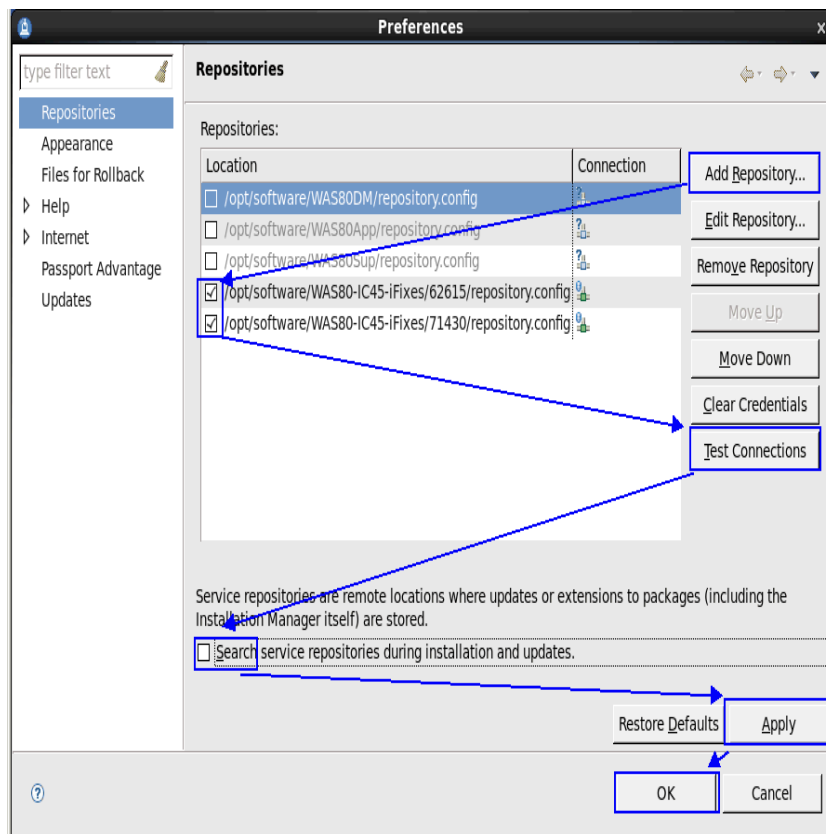
Deselect all existing Repositories; if any such exist

For each iFix select **Add Repositories** and navigate to the folder where the iFix was unzipped and select it's corresponding **repository.config** file as in the example screen shot below:

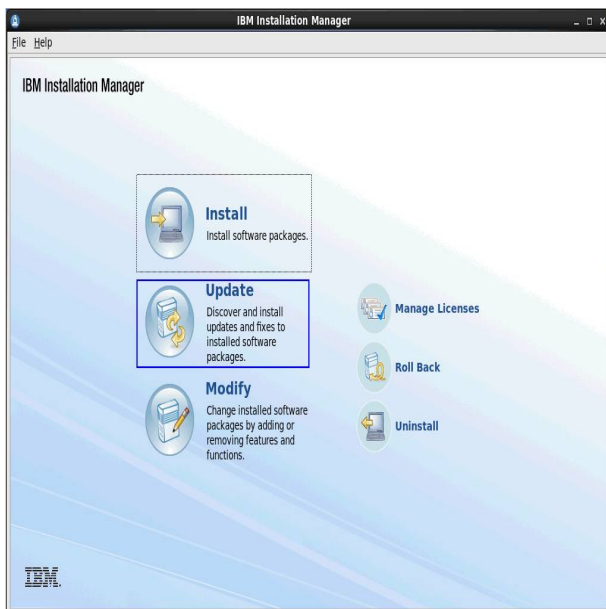
Select the locations of the iFixes and then **Test Connections** to verify

Deselect the option **Search service repositories during installation and updates** and select the **Apply** button

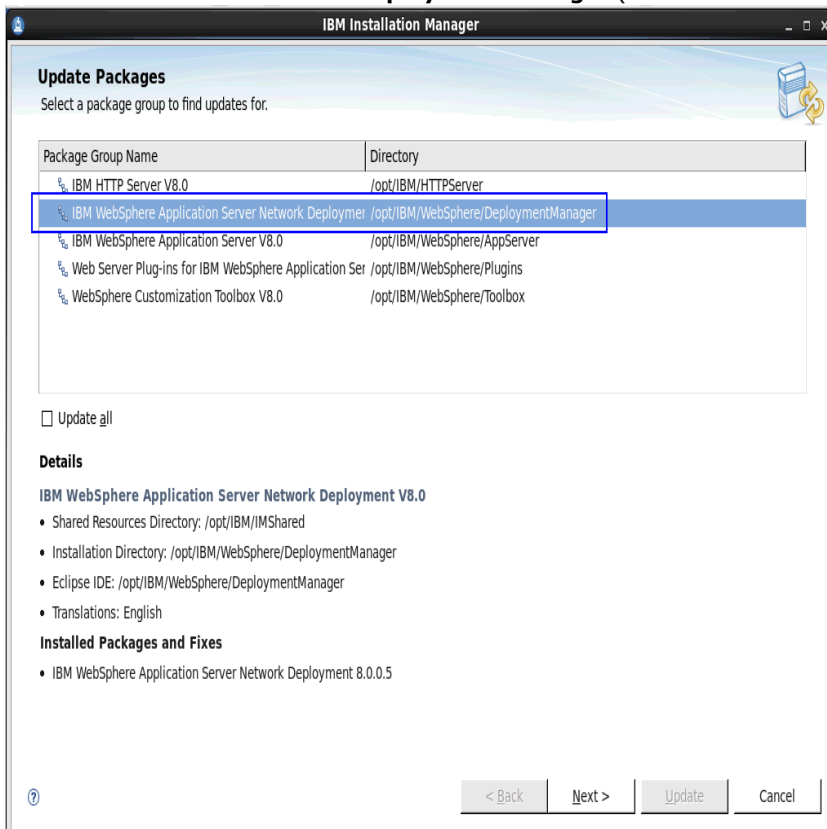
Select **OK** to continue.



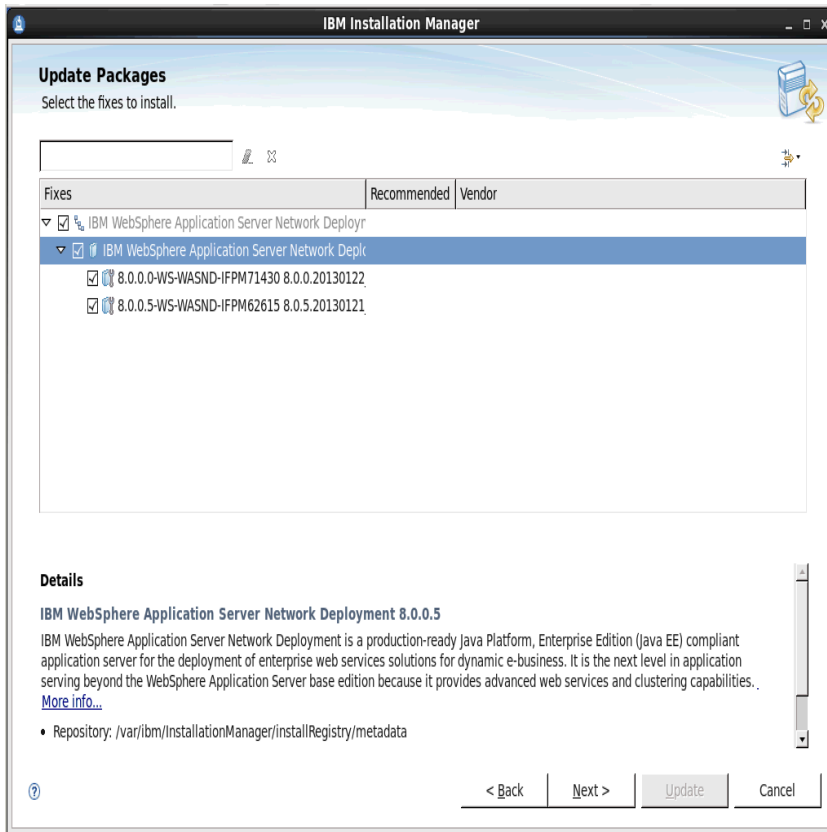
Select **Update** to continue



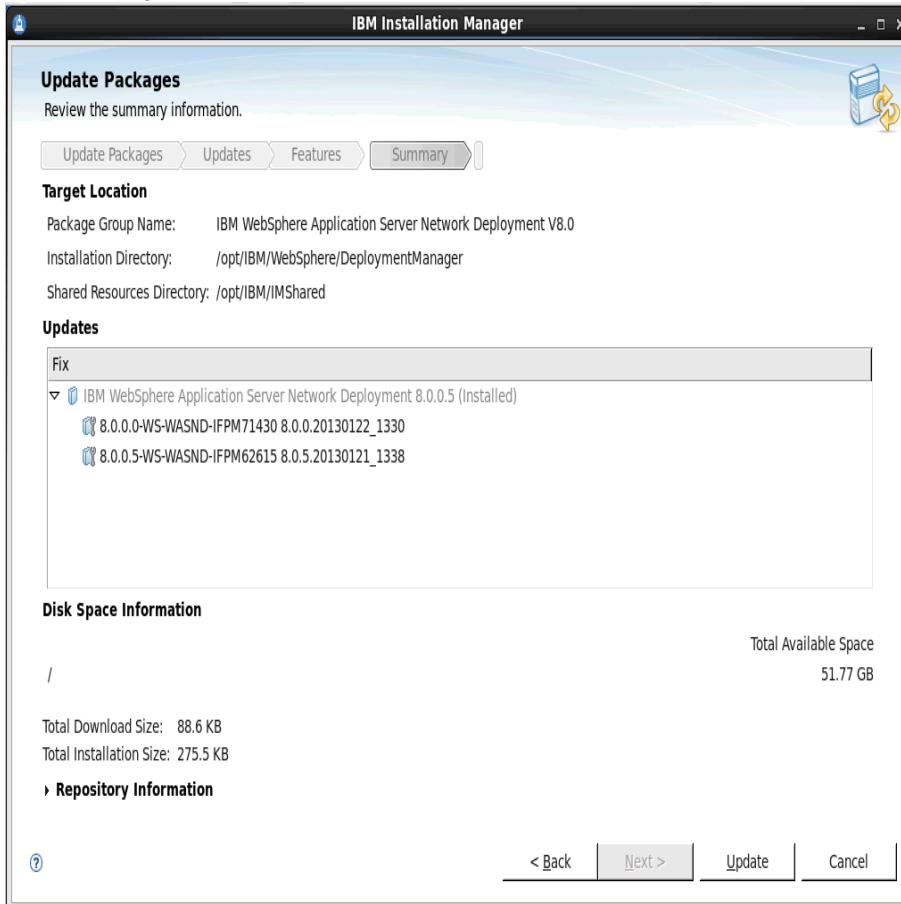
Select **IBM WAS Network Deployment Manager** (as in the screen shot below).. Select **Next** to continue



Select both iFixes, then **Next** to continue

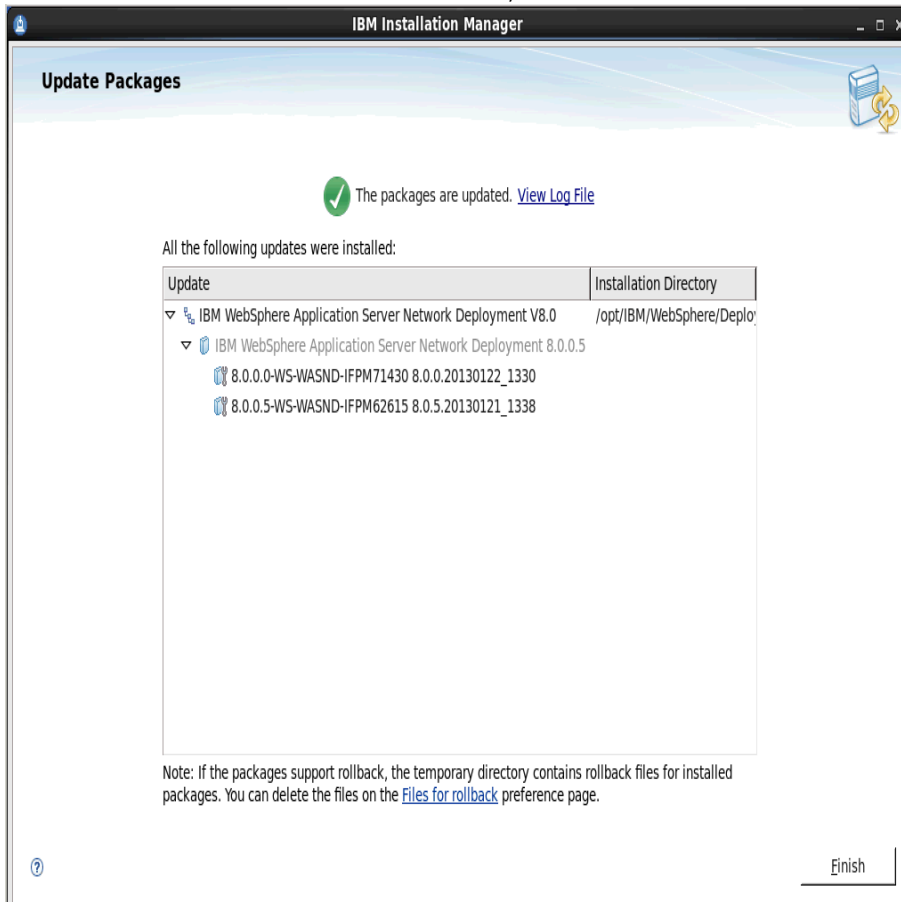


Select **Update** to install the iFixes



And after a few minutes the install will complete.

Select **Finish** to return to the Main screen; then **File > Exit** to exit the Installation Manager.



3.6 Install DB2 10-FP1 Server

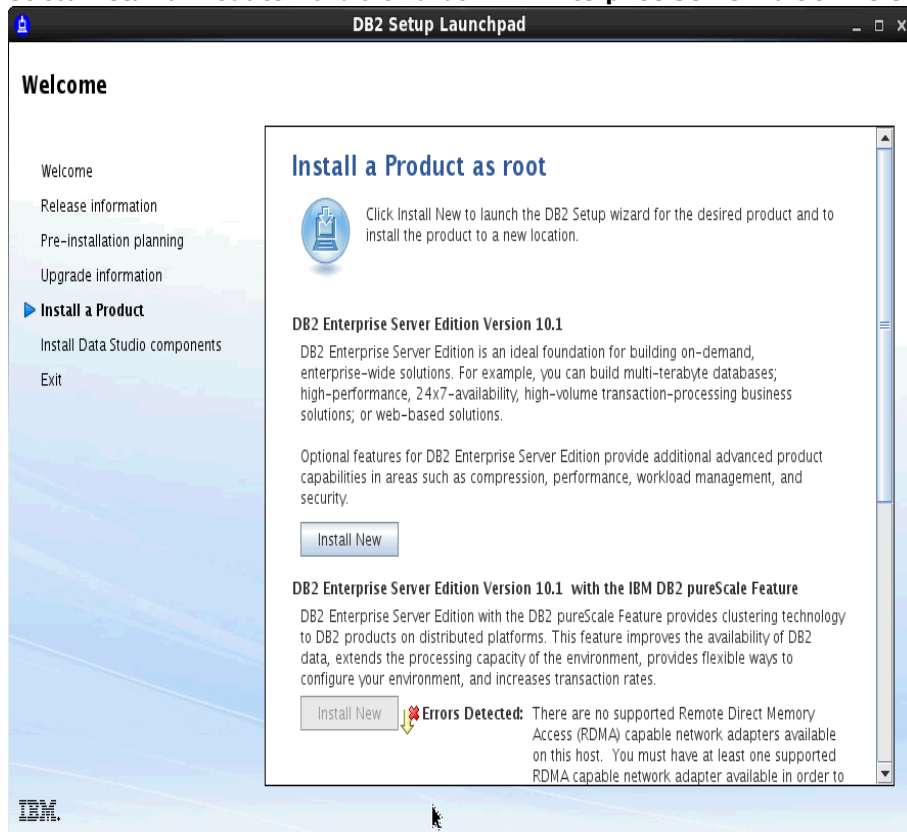
Install Steps for DB2

Copy the DB2 V10.1 install/image file to your machine.

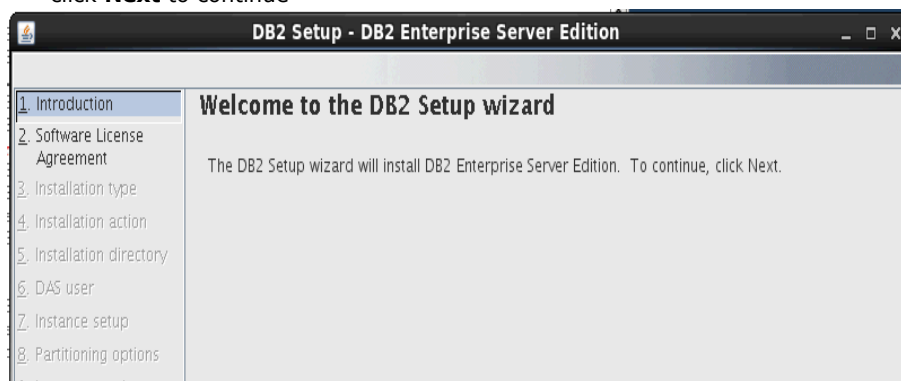
Uncompress the files; then, as root, start the DB2 installer by running **./db2setup**. You will see:



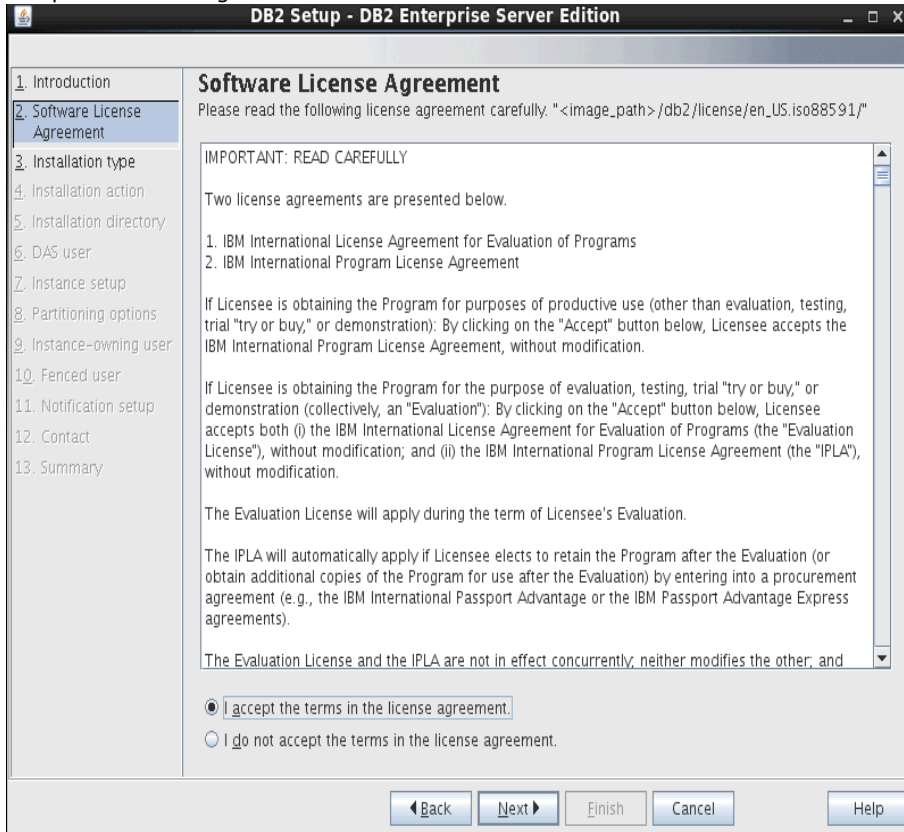
Select **Install a Product...** and then under **DB2 Enterprise Server Edition Version 10.1** select **Install New**



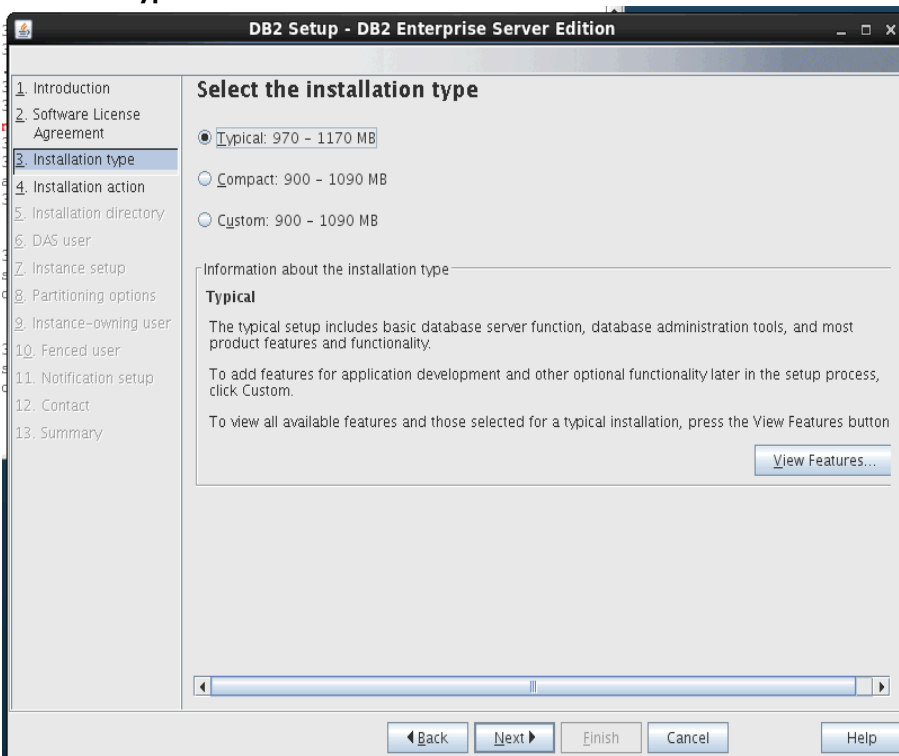
click **Next** to continue



Accept the license agreement... and **Next** to continue...



Select **Typical** and then **Next** to continue...



Select the **Install DB2 Enterprise Server Edition Version on this computer** then **Next** to continue

The screenshot shows the 'DB2 Setup - DB2 Enterprise Server Edition' window. On the left is a navigation pane with steps 1 through 13. Step 4, 'Installation action', is selected and highlighted. The main area is titled 'Select installation, response file creation, or both'. It contains explanatory text about the DB2 Setup wizard and two radio button options. The first option, 'Install DB2 Enterprise Server Edition on this computer', is selected. Below it, there is a text field for 'Response file name' with the value '/root/db2ese.rsp'. At the bottom of the window are five buttons: 'Back', 'Next', 'Finish', 'Cancel', and 'Help'.

DB2 Setup - DB2 Enterprise Server Edition

1. Introduction
2. Software License Agreement
3. Installation type
4. Installation action
5. Installation directory
6. DAS user
7. Instance setup
8. Partitioning options
9. Instance-owning user
10. Fenced user
11. Notification setup
12. Contact
13. Summary

Select installation, response file creation, or both

The DB2 Setup wizard can install DB2 Enterprise Server Edition on this computer, create a response file that you can use to install this product on a computer later, or both.

If you are setting up an Enterprise Server Edition partitioned database environment, you can also create a response file to install DB2 on the other computers that will act as database partition servers.

☒ Install DB2 Enterprise Server Edition on this computer

☐ Save my installation settings in a response file

No software will be installed on this computer.

☐ Install DB2 Enterprise Server Edition on this computer and save my settings in a response file

Response file name: /root/db2ese.rsp

◀ Back Next ▶ Finish Cancel Help

Used the default path for the Directory; select **Next** to continue

The screenshot shows the 'DB2 Setup - DB2 Enterprise Server Edition' window at step 5, 'Installation directory'. The navigation pane on the left has step 5 highlighted. The main area is titled 'Select the installation directory'. It explains that the wizard installs DB2 Enterprise Server Edition in a specific directory and provides instructions on how to change it. A text field for 'Directory' contains the path '/opt/ibm/db2/V10.1'. To the right of the text field, it shows 'Space required: 964 MB' and 'Space available: 18057 MB'. The 'Next' button is the primary action at the bottom.

DB2 Setup - DB2 Enterprise Server Edition

1. Introduction
2. Software License Agreement
3. Installation type
4. Installation action
5. Installation directory
6. DAS user

Select the installation directory

The DB2 Setup wizard installs DB2 Enterprise Server Edition in the following directory. To select a different directory, type the path or click the ellipsis button and select another directory.

Directory: /opt/ibm/db2/V10.1

Space required: 964 MB
Space available: 18057 MB

Next

Use the default names and directory paths and enter a valid password. Select **Next** to continue.

DB2 Setup - DB2 Enterprise Server Edition

1. Introduction
2. Software License Agreement
3. Installation type
4. Installation action
5. Installation directory
6. DAS user
7. Instance setup
8. Partitioning options
9. Instance-owning user
10. Fenced user
11. Notification setup
12. Contact
13. Summary

Set user information for the DB2 Administration Server

The DB2 Administration Server (DAS) runs on your computer to provide support required by the DB2 tools. A user with a minimal set of privileges is required to run the DAS. Specify the required user information for the DAS.

☒ **New user**

User name:

UID: ☒ Use default UID

Group name:

GID: ☒ Use default GID

Password:

Confirm password:

Home directory:

☐ Existing user

User name:

Select **Create a DB2 instance...** select **Next** to continue...

DB2 Setup - DB2 Enterprise Server Edition

1. Introduction
2. Software License Agreement
3. Installation type
4. Installation action
5. Installation directory
6. DAS user
7. Instance setup
8. Partitioning options
9. Instance-owning user
10. Fenced user
11. Notification setup

Set up a DB2 instance

A DB2 instance is an environment in which you store data and run applications. You must have an instance to use this product.

If you would like to add this computer to an existing partitioned database environment, you should not create an instance on this computer. The instance should be created on the instance-owning database partition server.

☒ **Create a DB2 instance**

☐ Do not create a DB2 instance

Select **Single partition instance...** select **Next** to continue...

DB2 Setup - DB2 Enterprise Server Edition

1. Introduction
2. Software License Agreement
3. Installation type
4. Installation action
5. Installation directory
6. DAS user
7. Instance setup
8. **Partitioning options**
9. Instance-owning user
10. Fenced user
11. Notification setup
12. Contact
13. Summary

Set up partitioning options for the DB2 instance

A DB2 instance can have one or more database partitions, which exist on one or more computers. Select the partitioning options for this instance. The number of partitions specified will be reserved in the services file.

☒ **Single partition instance**

The instance will reside only on this computer. Select this option if the instance will not be used in a partitioned database environment.

☐ Multiple partition instance

Selecting this option will create two response files. Refer to the DB2 Information Center to read about the additional steps needed to prepare your DPF environment.

To use this functionality, you must have a Database Partitioning Feature license.

◀ Back Next ▶ Finish Cancel Help

Enter your DB2 instance owner and password; used the default names, and entered a valid password.
Select **Next** to continue.

DB2 Setup - DB2 Enterprise Server Edition

1. Introduction
2. Software License Agreement
3. Installation type
4. Installation action
5. Installation directory
6. DAS user
7. Instance setup
8. Partitioning options
9. **Instance-owning user**
10. Fenced user
11. Notification setup
12. Contact
13. Summary

Set user information for the DB2 instance owner

Specify the instance-owning user information for the DB2 instance. DB2 will use this user to perform instance functions, and will store instance information in the user's home directory. The name of the instance will be the same as the user name.

☒ **New user**

User name: db2inst1

UID: ☒ Use default UID

Group name: db2iadm1

GID: ☒ Use default GID

Password: Password • You must specify a value. ▶

Confirm password:

Home directory: /home/db2inst1

☐ Existing user

User name:

◀ Back Next ▶ Finish Cancel Help

Enter your fenced username and password... I used the default user names... select **Next** to continue.

DB2 Setup - DB2 Enterprise Server Edition

1. Introduction
2. Software License Agreement
3. Installation type
4. Installation action
5. Installation directory
6. DAS user
7. Instance setup
8. Partitioning options
9. Instance-owning user
10. Fenced user
11. Notification setup
12. Contact
13. Summary

Set user information for the fenced user
Specify the required information for the fenced user. Fenced user defined functions (UDFs) and stored procedures will execute under this user and group.

☒ **New user**

User name:

UID:

☒ Use default UID

Group name:

GID:

☒ Use default GID

Password:

Confirm password:

Home directory:

☐ Existing user

User name:

◀ Back Next ▶ Finish Cancel Help

Select **Do not set up your DB2 server to send notifications at this time**, then **Next** to continue.

DB2 Setup - DB2 Enterprise Server Edition

1. Introduction
2. Software License Agreement
3. Installation type
4. Installation action
5. Installation directory
6. DAS user
7. Instance setup
8. Partitioning options
9. Instance-owning user
10. Fenced user
11. Notification setup
12. Summary

Set up notifications
You can set up your DB2 server to automatically send e-mail or pager notifications to alert administrators when a database needs attention. The contact information is stored in the administration contact list. You need an unauthenticated SMTP server to send these notifications.

☐ Set up your DB2 server to send notifications

Notification SMTP server:

Administration contact list location:

☒ Local - Create a contact list on this computer

☐ Remote - Use an existing contact list that resides on another DB2 server

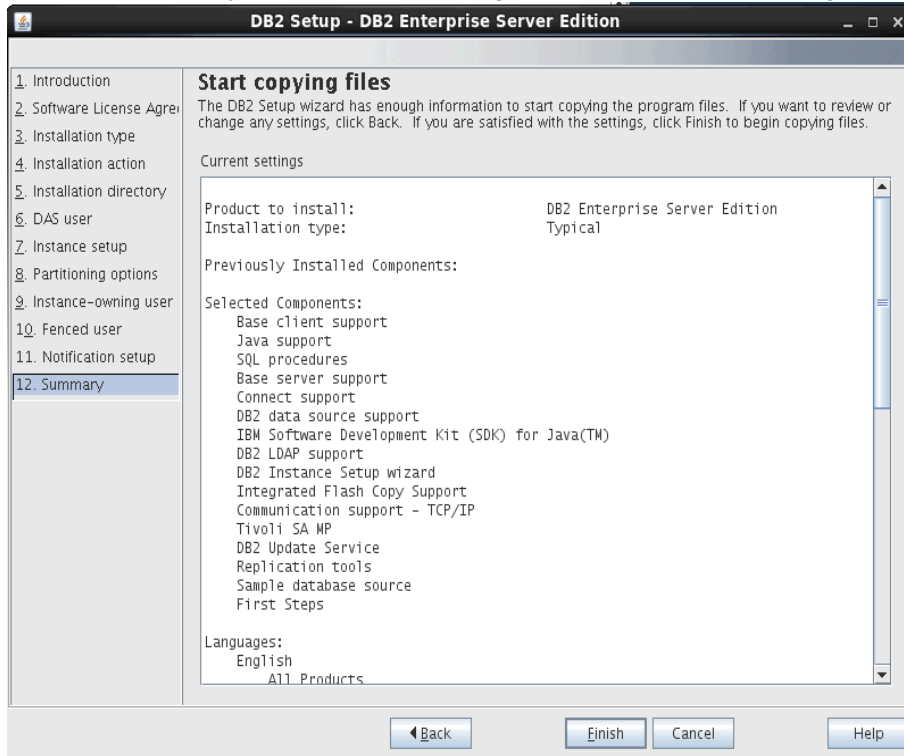
Remote DB2 server:

☒ **Do not set up your DB2 server to send notifications at this time**

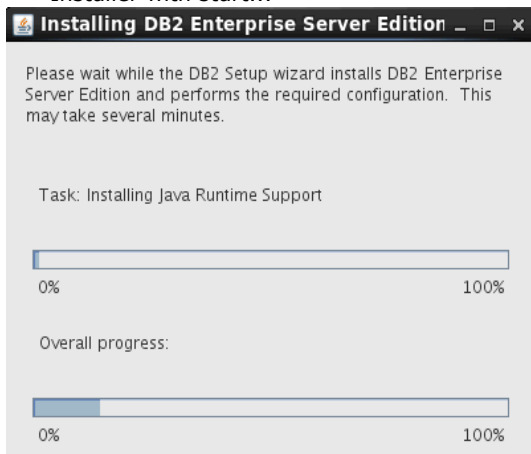
If you do not set up your DB2 server to send notifications, the health alerts are still recorded in the administration notification log.

◀ Back Next ▶ Finish Cancel Help

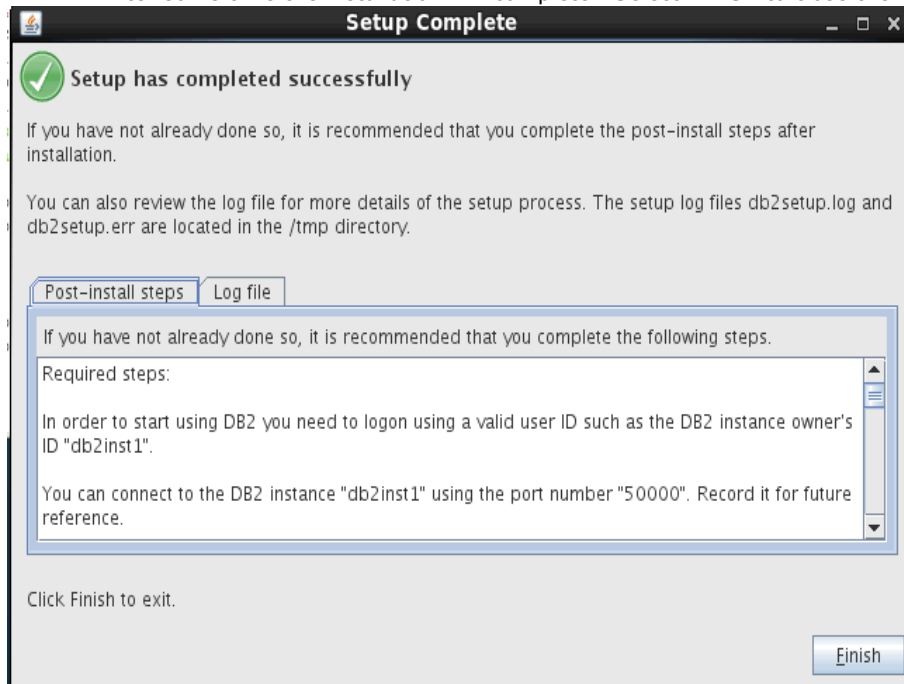
On the Summary screen, check all setting and if OK select **Finish** to begin installing DB2



Installer with start...



After some time the installation will complete...Select **Finish** to close the installer and you are returned to the cmd prompt.



Check the version of DB2 installed as follows:

At the CMD prompt enter the following commands to verify the version of DB2 installed.

```
su - db2inst1  
db2level
```

```
[root@dslvm1037 esel]# su - db2inst1  
[db2inst1@dslvm1037 ~]$ db2level  
DB21085I  Instance "db2inst1" uses "64" bits and DB2 code release "SQL10010"  
with level identifier "0201010E".  
Informational tokens are "DB2 v10.1.0.0", "s120403", "LINUXAMD64101", and Fix  
Pack "0".  
Product is installed at "/opt/ibm/db2/V10.1".  
[db2inst1@dslvm1037 ~]$ █
```

Apply the DB2 License:

Out of the box DB2 comes without a license installed. To check this run the cmd **db2licm -l**

```
[db2inst1@dubxpcvm624 ~]$ db2licm -l  
Product name:          "DB2 Enterprise Server Edition"  
License type:          "License not registered"  
Expiry date:           "License not registered"  
Product identifier:    "db2ese"  
Version information:   "10.1"
```

The **License type** is reported as "**License not unregistered**"

Copy the DB2 license to the DB2 system and install the license by running the cmd **db2licm -a <database license file>**
e.g.

```
[db2inst1@dslvm1037 ~]$ db2licm -a /opt/software/db2ese_u.lic
```

```
LIC1402I  License added successfully.
```





```
LIC1426I  This product is now licensed for use as outlined in your License Agreement.  USE OF THE PRODUCT CONSTITUTES ACCEPT  
ANCE OF THE TERMS OF THE IBM LICENSE AGREEMENT, LOCATED IN THE FOLLOWING DIRECTORY: "/opt/ibm/db2/V10.1/license/en_US.iso885  
91"
```

Verify that the license is installed correctly by re-running the cmd **db2licm -l**

```
[db2inst1@dubxpcvm624 ~]$ db2licm -l
Product name: "DB2 Enterprise Server Edition"
License type: "Authorized User Option"
Expiry date: "Permanent"
Product identifier: "db2ese"
Version information: "10.1"
Enforcement policy: "Soft Stop"
Number of licensed authorized users: "25"
Features:
DB2 Storage Optimization: "Not licensed"
DB2 Advanced Access Control: "Not licensed"
DB2 pureScale: "Not licensed"
```

Copy the DB2 JDBC jars files to the DM and to each of the Application Nodes

On the DM, Node1 and Node1 create the folder: **/opt/DB2-JDBC-jars** and copy the following DB2 files (from /opt/ibm/db2/V10.1/java) to this folder on the DM/Node1 & node2 system

-  db2java.zip
-  db2jcc.jar
-  db2jcc_license_cu.jar
-  db2jcc4.jar

Note: These files must be in exactly the same folder on the DM and the Application servers/nodes

3.7 Install Tivoli Directory Integrator (TDI) V7.1 + Fixpack 5

IBM Tivoli Directory Integrator 7.1 Install:

The install of TDI is needed so the IBM Connections profiles database (PEOPLEDDB) can be populated with LDAP information.

In this scenario the TDI will be installed on the same system as the DB2.

NOTE: The **TDI V7.1 Installer** (launchpad.sh) required the Firefox browser version **3.0.18** to run it's install. You can download and install FF 3.0.18 as follows:

download **firefox-3.0.18** (from: <https://ftp.mozilla.org/pub/mozilla.org/firefox/releases/3.0.18/linux-i686/en-US/>) into the folder: **/opt/software/firefox3**.

decompress **firefox-3.0.18.tar.bz2** using the cmd: **tar -jxvf firefox-3.0.18.tar.bz2** -- Firefox is then extracted into the folder: **/opt/software/firefox3/firefox**

set the following Environment Variable: **export BROWSER=/opt/software/firefox3/firefox/firefox**

Installing TDI V7.1

Copy the TDI V7.1 installer image (CZ9MNM.L.tar) to your machine (/opt/software/TDI71) and decompress it.

Start the TDI V7.1 launchpad by running: **./launchpad.sh...** and then follow these instructions.

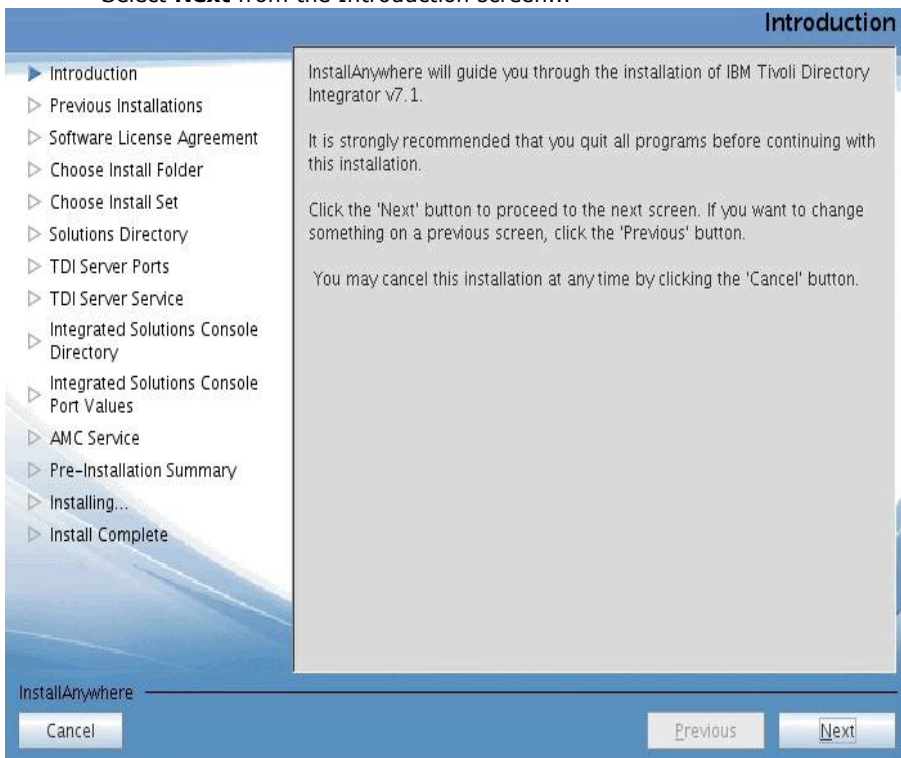
Select **Install IBM Tivoli Directory Integrator** and then **Tivoli Directory Integrator 7.1 Installer**.



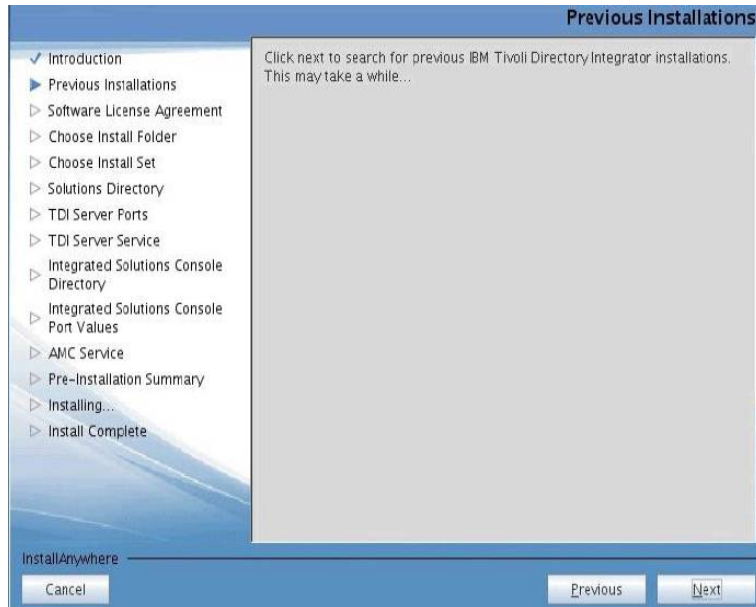
Select **English** and click **OK**



Select **Next** from the Introduction screen...



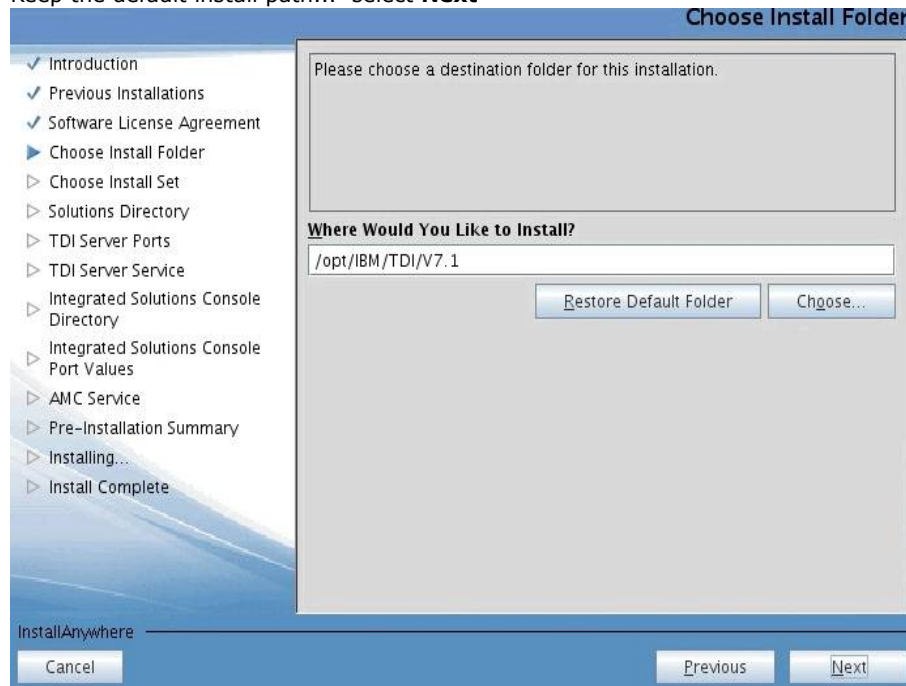
select **Next**



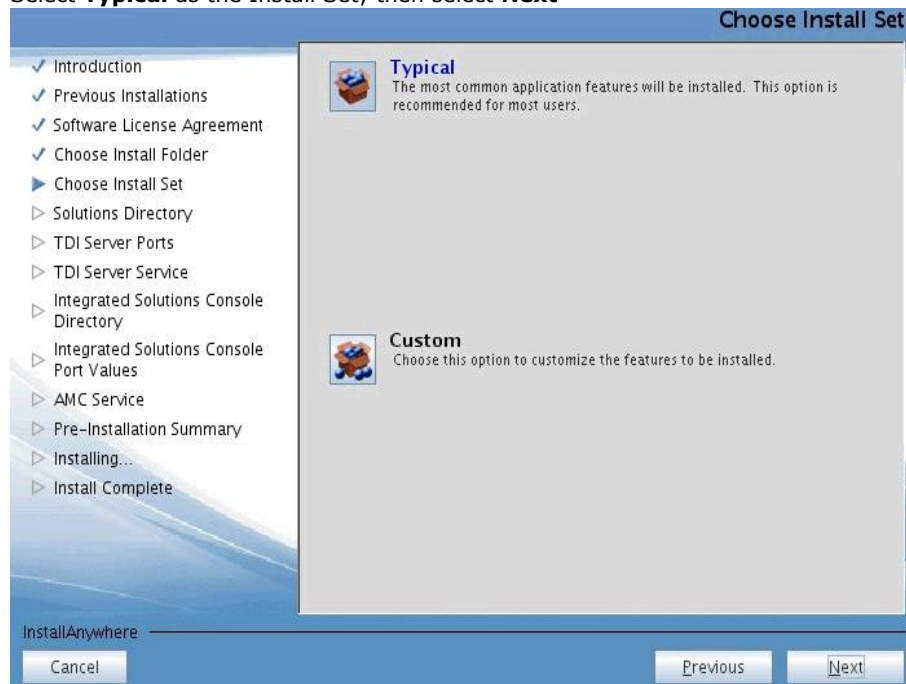
Accept the terms of the license agreement and select **Next**



Keep the default install path... select **Next**



Select **Typical** as the Install Set; then select **Next**



Select **Do not specify - use current working directory at startup time** and then **Next**

The screenshot shows the 'Solutions Directory' window. On the left is a navigation pane with a list of steps: Introduction, Previous Installations, Software License Agreement, Choose Install Folder, Choose Install Set, Solutions Directory (highlighted), TDI Server Ports, TDI Server Service, Integrated Solutions Console Directory, Integrated Solutions Console Port Values, AMC Service, Pre-Installation Summary, Installing..., and Install Complete. The main area contains a text box explaining the purpose of a Solutions Directory, followed by three radio button options: 'Use a subdirectory named TDI under my home directory', 'Use Install Directory', and 'Select a directory to use' (which has a text input field and 'Restore Default' and 'Choose...' buttons). The option 'Do not specify - use current working directory at startup time' is selected with a radio button. At the bottom are 'Cancel', 'Previous', and 'Next' buttons.

Solutions Directory

You have the option of selecting a Solutions Directory. A Solutions Directory is a static directory where the IBM Tivoli Directory Integrator Server and Configuration Editor look for your solutions.

☐ Use a subdirectory named TDI under my home directory

☐ Use Install Directory

☐ Select a directory to use

☒ Do not specify - use current working directory at startup time

InstallAnywhere

Cancel Previous Next

Use the default ports and select **Next**

The screenshot shows the 'Server Port Values' window. The navigation pane on the left is identical to the previous window, with 'Solutions Directory' highlighted. The main area has a text box asking for port values for IBM Tivoli Directory Integrator v7.1 Server. Below are four labeled text input fields: 'Server Port:' (1099), 'System Store Port:' (1527), 'REST API Port:' (1098), and 'System Queue Port:' (41001). At the bottom are 'Cancel', 'Previous', and 'Next' buttons.

Server Port Values

Enter the port values to be used by IBM Tivoli Directory Integrator v7.1 Server.

Server Port:
1099

System Store Port:
1527

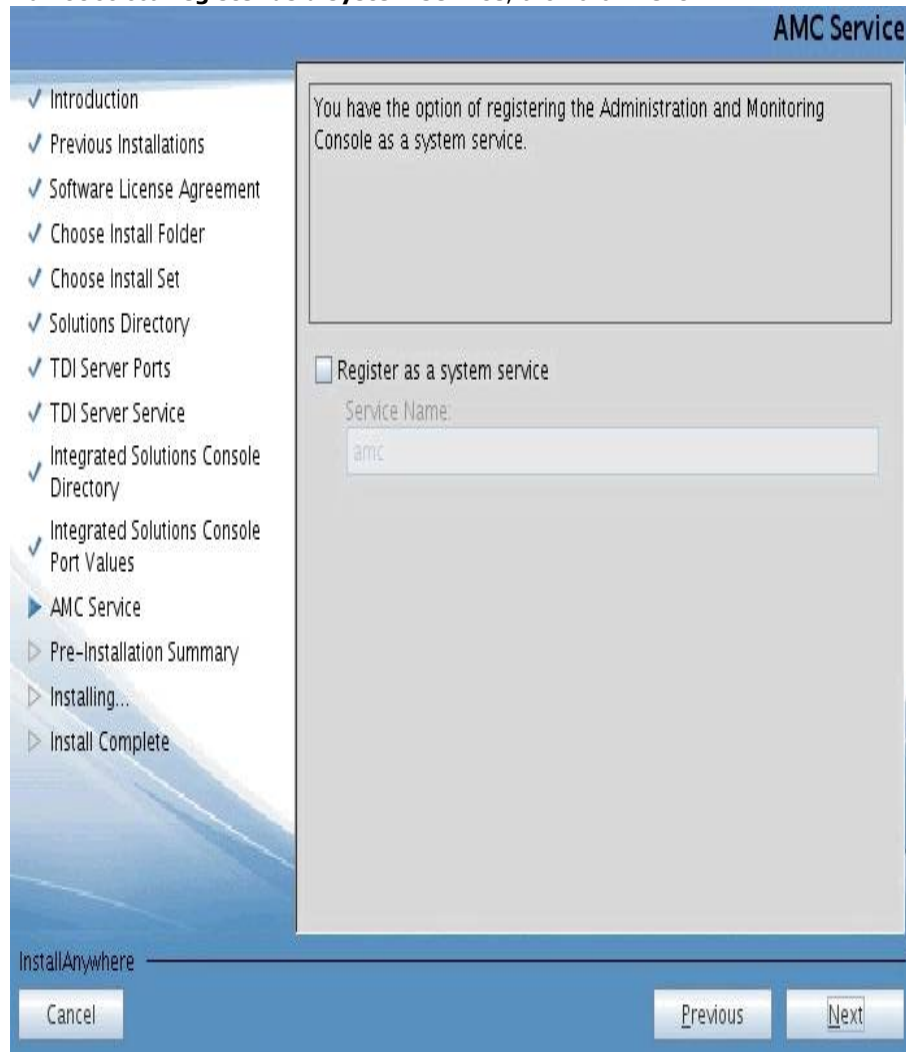
REST API Port:
1098

System Queue Port:
41001

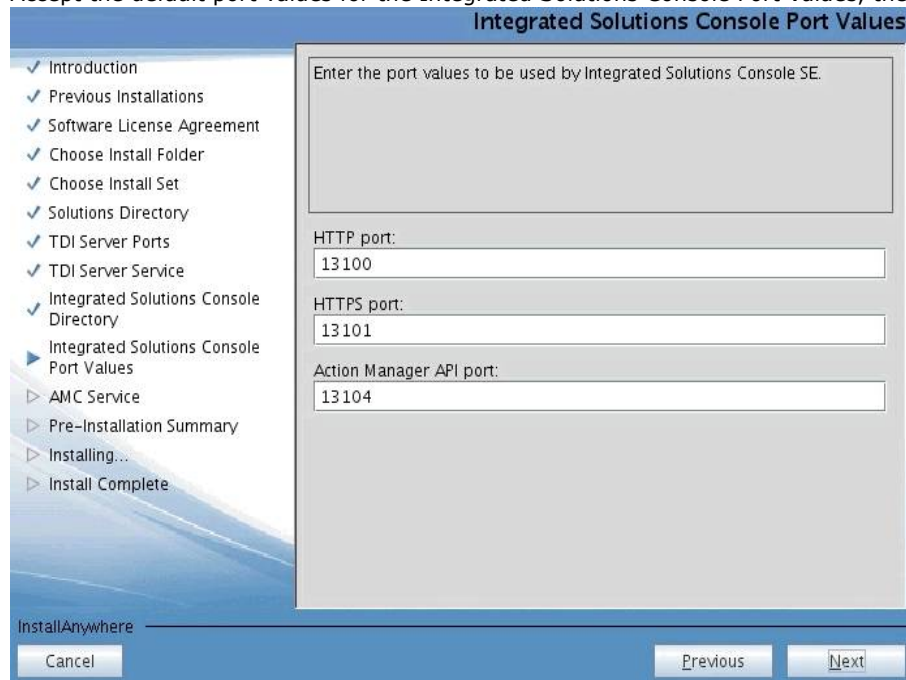
InstallAnywhere

Cancel Previous Next

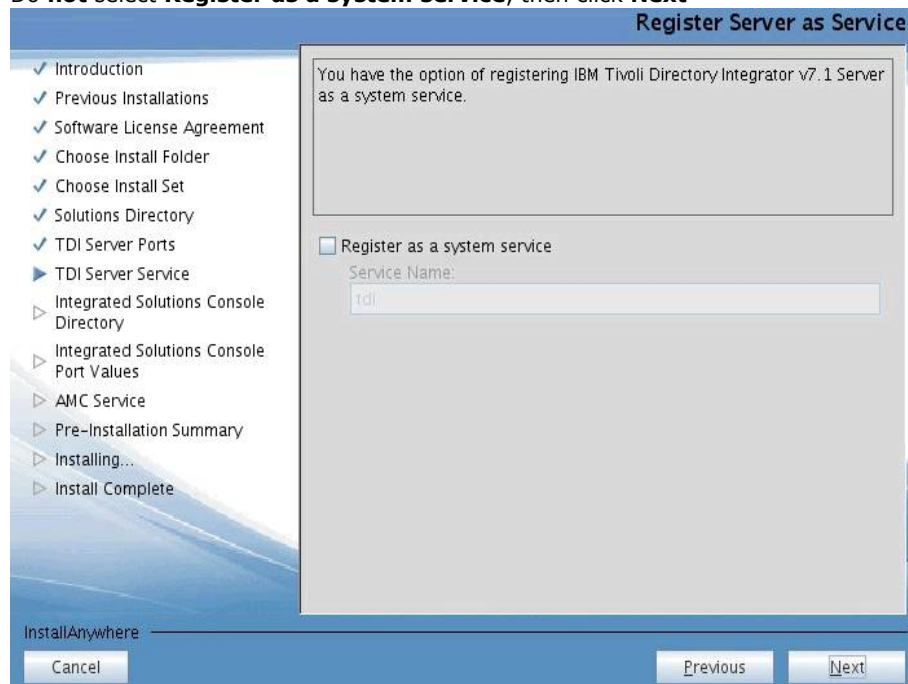
Do **not** select **Register as a system service**, then click **Next**



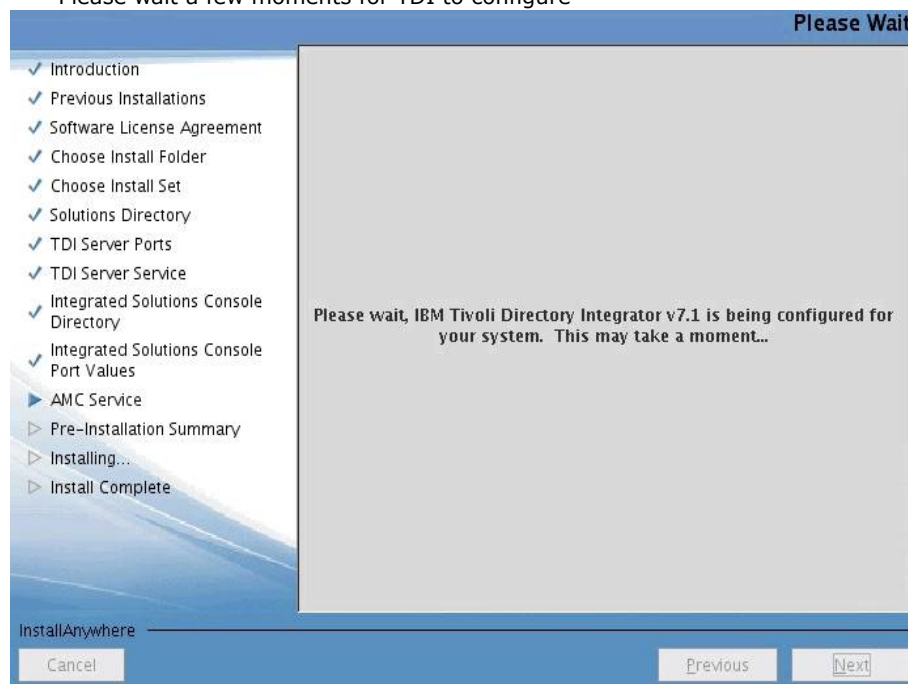
Accept the default port values for the Integrated Solutions Console Port Values, then select **Next**



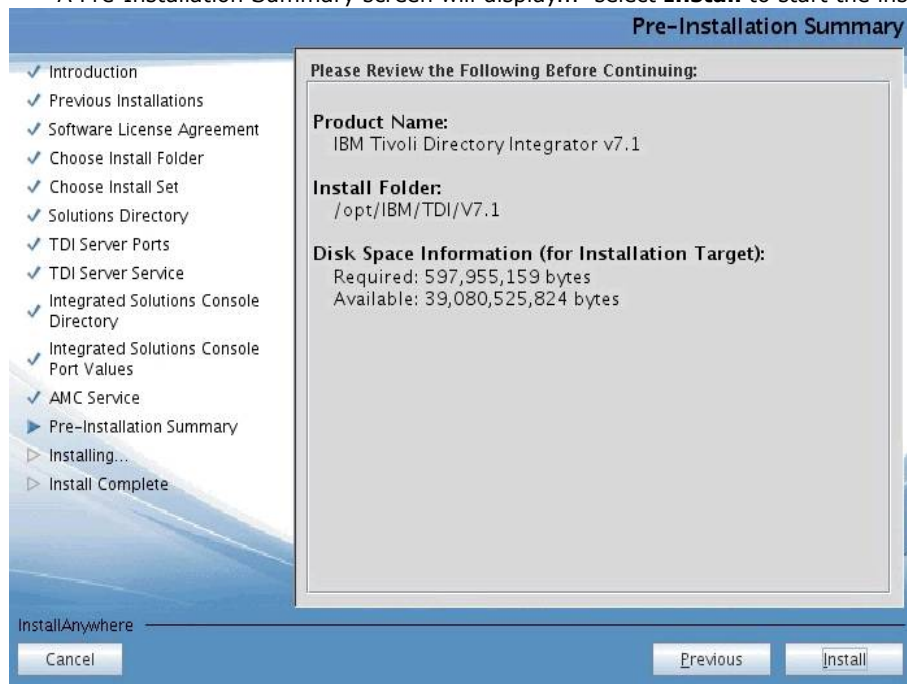
Do **not** select **Register as a system service**, then click **Next**



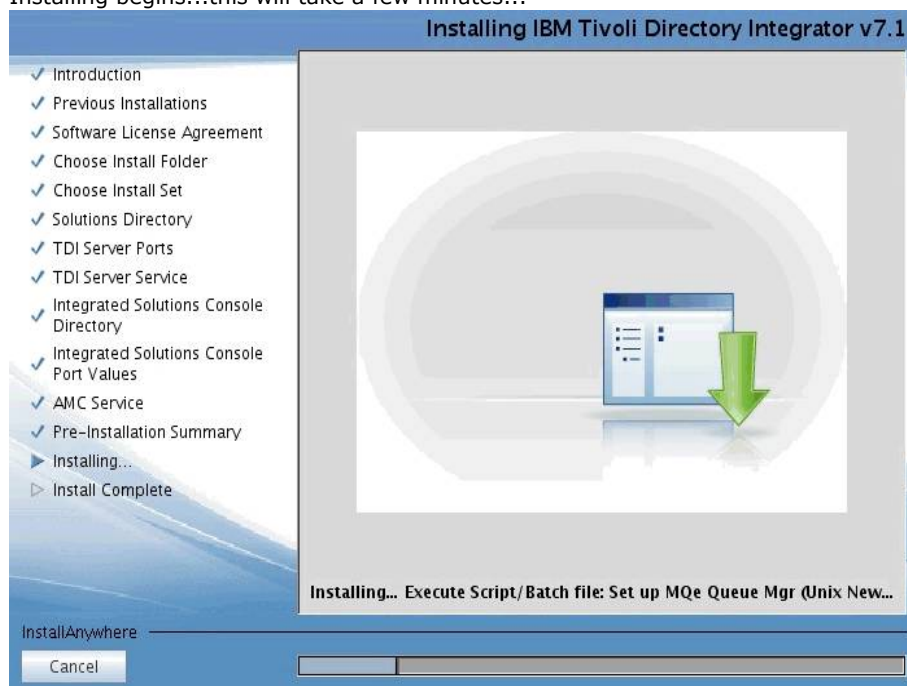
Please wait a few moments for TDI to configure



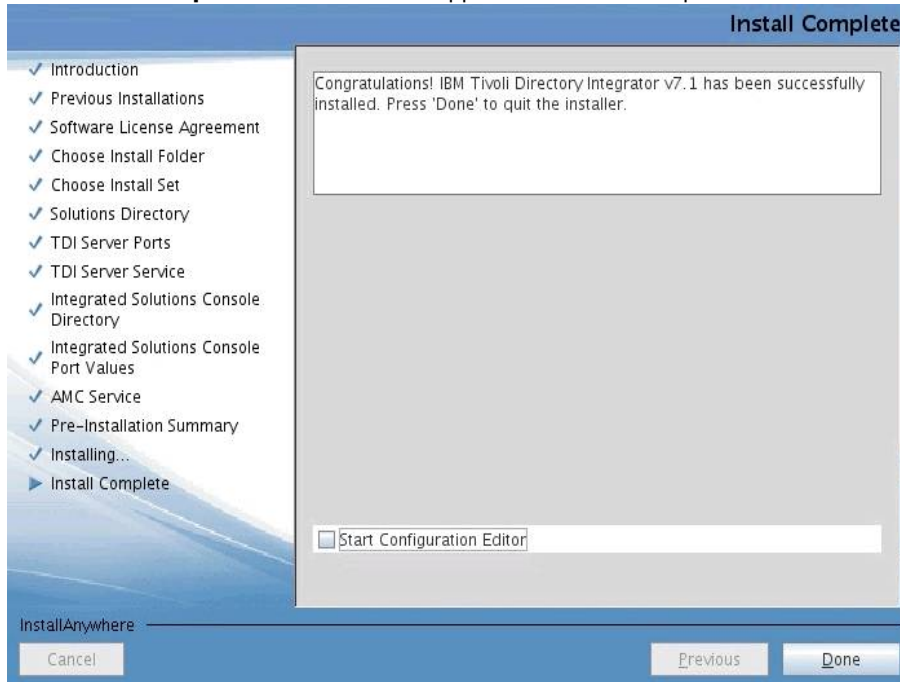
A Pre-Installation Summary screen will display... select **Install** to start the installation...



Installing begins...this will take a few minutes...



The **Install Complete** screen will next appear. Deselect the option to **Start Configuration Editor**; then select **Done**



You can now **Exit** the installer... TDI 7.1 is now installed, but now we need to install FixPack 5.

IBM Tivoli Directory Integrator 7.1 FixPack 5 Install

Copy TDI V7.1 Fixpack 5 (**7.1.0-TIV-TDI-FP0005.zip**) to the folder **/opt/software/TDI7.1-FP5** and unzip it.

Make sure TDI is not running before applying the fixpack.

In the **7.1.0-TIV-TDI-FP0005** folder there is a file called **applyUpdates.sh**; copy this file to **/opt/IBM/TDI/V7.1/bin/** replacing the version that is already there.

Goto **/opt/IBM/TDI/V7.1/bin** and run the following commands: **chmod 755 applyUpdates.sh**

Note: Run the following commands from a VNC session

./applyUpdates.sh -update /opt/software/TDI7.1-FP5/7.1.0-TIV-TDI-FP0005/TDI-7.1-FP0005.zip

The FixPack will then install.

```
[root@dubxpcvm624 bin]# ./applyUpdates.sh -update /opt/software/TDI7.1-FP5/7.1.0-TIV-TDI-FP0005/TDI-7.1-FP0005.zip
CTGDKO023I Applying fix 'TDI-7.1-FP0005' using backup directory '/opt/IBM/TDI/V7.1/maintenance/BACKUP/TDI-7.1-FP0005'.
CTGDKO027I Updating SERVER.
CTGDKO027I Updating CE.
CTGDKO027I Updating EXAMPLES.
```

To check the install was OK run **./applyUpdates.sh -queryreg** it should report that FP5 is installed...

```
[root@dubxpcvm624 bin]# ./applyUpdates.sh -queryreg
Information from .registry file in: /opt/IBM/TDI/V7.1
Edition: Identity
Level: 7.1.0.5
License: None
```

Fixes Applied

=====

TDI-7.1-FP0005(7.1.0.0)

Components Installed

=====

BASE

SERVER

-TDI-7.1-FP0005

CE

-TDI-7.1-FP0005

JAVADOCS

EXAMPLES

-TDI-7.1-FP0005

EMBEDDED WEB PLATFORM

AMC

Deferred: false

```
[root@dubxpcvm624 bin]# █
```

4. Deployment configuration steps

4.1 Enable Security on the Deployment Manager

Next we need to add the LDAP repository to your Configuration...

Login to your WAS admin console -> <https://dm&ihs.spnego.company.com:9043/ibm/console> (use wasadmin user and password).

Enable the following General Settings:

Select: **Security -> Global security.**

Ensure the **Enable administrative security** and **Enable application security** are selected.

Under **User account repository** ensure **Available realm definitions** is set to **Federated repositories**

Select **Apply** and **Save**.

The screenshot shows the 'Global security' configuration page. At the top, there's a title bar 'Global security'. Below it, a description states: 'Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy for user applications. Security domains can be defined to override and customize the security policies for user applications.' There are two buttons: 'Security Configuration Wizard' and 'Security Configuration Report'.

The page is divided into several sections:

- Administrative security:** Contains a checked checkbox 'Enable administrative security' and three links: 'Administrative user roles', 'Administrative group roles', and 'Administrative authentication'.
- Application security:** Contains a checked checkbox 'Enable application security'.
- Java 2 security:** Contains an unchecked checkbox 'Use Java 2 security to restrict application access to local resources' and two sub-options: 'Warn if applications are granted custom permissions' (unchecked) and 'Restrict access to resource authentication data' (unchecked).
- User account repository:** Contains a text field for 'Realm name' with the value 'defaultWIMFileBasedRealm', a text field for 'Current realm definition' with the value 'Federated repositories', and a section for 'Available realm definitions' with a dropdown menu set to 'Federated repositories' and buttons for 'Configure...' and 'Set as current'.
- Authentication:** Contains the heading 'Authentication mechanisms and expiration' and a radio button selected for 'LTPA'. Other options include 'Kerberos and LTPA' (unselected) with links for 'Kerberos configuration' and 'Authentication cache settings', 'Web and SIP security', 'RMI/IIOP security', 'Java Authentication and Authorization Service' (with an unchecked checkbox), 'Enable Java Authentication SPI (JASPI)' (unchecked) with a link for 'Providers', and 'Use realm-qualified user names' (unchecked). At the bottom of this section are links for 'Security domains', 'External authorization providers', 'Programmatic session cookie configuration', and 'Custom properties'.

At the bottom left of the page are 'Apply' and 'Reset' buttons.

Select: **Security -> Global security -> Web and SIP Security -> General Settings.**

Ensure the **Use available authentication data when an unprotected URI is accessed** check box is ticked.

Select Apply and Save.

The screenshot shows the 'Global security' window with the 'Web security - General settings' tab selected. The title bar reads 'Global security'. Below the title bar, the breadcrumb path is 'Global security > Web security - General settings'. A description states: 'Specifies the settings for web authentication.' The 'General Properties' section is expanded, showing 'Web authentication behavior'. There are three radio buttons: 'Authenticate only when the URI is protected' (selected), 'Use available authentication data when an unprotected URI is accessed' (checked with a checkbox), and 'Authenticate when any URI is accessed'. Below these is a checkbox for 'Default to basic authentication when certificate authentication for the HTTPS client fails', which is unchecked. At the bottom are buttons for 'Apply', 'OK', 'Reset', and 'Cancel'.

Select: **Security -> Global security -> Web and SIP Security -> Single sign-on (SSO).**

Enter the **Domain name** - you must prefix it with the dot/period (.) e.g. ".spnego.company.com"

Ensure the **Interoperability mode** is select and enter the domain name.

Ensure the LTPA V1 and V2 Cookie names are spelt and cased correctly as shown ie use "**LtpaToken**" and "**LtpaToken2**"

Ensure **Web inbound security attribute propagation** is checked

Ensure **Set security cookies to HTTPOnly to help prevent cross-site scripting attacks** is checked

Select Apply and Save.

The screenshot shows the 'Global security' window with the 'Single sign-on (SSO)' tab selected. The title bar reads 'Global security'. Below the title bar, the breadcrumb path is 'Global security > Single sign-on (SSO)'. A description states: 'Specifies the configuration values for single sign-on.' The 'General Properties' section is expanded. It contains several checkboxes: 'Enabled' (checked), 'Requires SSL' (unchecked), 'Interoperability mode' (checked), 'Web inbound security attribute propagation' (checked), and 'Set security cookies to HTTPOnly to help prevent cross-site scripting attacks' (checked). There are three text input fields: 'Domain name' with the value '.spnego.company.com', 'LTPA V1 cookie name' with the value 'LtpaToken1', and 'LTPA V2 cookie name' with the value 'LtpaToken2'. At the bottom are buttons for 'Apply', 'OK', 'Reset', and 'Cancel'.

Configure the Federate LDAP Repositories:

Select: **Security -> Global security -> Configure...** opposite **Federated repositories**

Select **Add Base entry to Realm...**

Global security

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

By federating repositories, identities stored in multiple repositories can be managed in a single, virtual realm. The realm can consist of identities in the file-based repository that is built into the system, in one or more external repositories, or in both the built-in repository and one or more external repositories.

General Properties

* Realm name
defaultWIMFileBasedRealm

* Primary administrative user name
wasadmin

Server user identity

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

☒ Ignore case for authorization
☐ Allow operations if some of the repositories are down

Repositories in the realm:

[Add Base entry to Realm...](#) [Use built-in repository](#) [Remove](#)

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

- Then select **Add Repository...** and then **LDAP repository**

Global security

[Global security](#) > [Federated repositories](#) > [Repository reference](#)

Specifies a set of identity entries in a repository that are referenced by a base entry into the directory. It is necessary to define an additional distinguished name that uniquely identifies this set of entries within the repository.

General Properties

* Repository
none defined [Add Repository...](#)
LDAP repository
Custom repository
File repository

* Distinguished name
at uniquely identifies this set of entries in the realm
Distinguished name of a base entry in this repository

[Apply](#) [OK](#) [Reset](#) [Cancel](#)

Enter the Repository information as shown below; then **OK**, then **Save**

Global security

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

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

General Properties

* Repository identifier
msad2008

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

LDAP server

* Directory type
Microsoft Windows Active Directory

* Primary host name
msad2008.spnego.company.com

Port
389

Failover server used when primary is not available:

Delete

Select	Failover Host Name	Port
None		

Add

Support referrals to other LDAP servers
ignore

Support for repository change tracking
none

Custom properties

New Delete

Select	Name	Value
<input type="checkbox"/>		

Security

Bind distinguished name
CN=bind,OU=branch,DC=spnego,DC=company,DC=com

Bind password

Login properties
uid

LDAP attribute for Kerberos principal name

Certificate mapping
EXACT_DN

Certificate filter

☐ Require SSL communications

☒ Centrally managed

[Manage endpoint security configurations](#)

☒ Use specific SSL alias

CellDefaultSSLSettings [SSL configurations](#)

Enter the base entry... select **OK**, then **Save**

Global security

Global security > Federated repositories > Repository reference

Specifies a set of identity entries in a repository that are referenced by a base entry into the directory information tree. If multiple repositories are included in the same realm, it might be necessary to define an additional distinguished name that uniquely identifies this set of entries within the realm.

General Properties

* Repository
msad2008 Add Repository...

* Distinguished name of a base entry that uniquely identifies this set of entries in the realm
OU=branch,DC=spnego,DC=company,D

Distinguished name of a base entry in this repository
OU=branch,DC=spnego,DC=company,D

Apply OK Reset Cancel

Now, restart the Deployment Manager and the Node Agents.

Add an LDAP user as an administrator:

Login to your admin console -> <https://dm&ihs.spnego.company.com:9043/ibm/console>

Select **Users and Groups** -> **Administrative user roles**; select **Add...**

Administrative user roles

Administrative user roles

Use this page to add, update or to remove administrative roles to groups. Assigning administrative roles to groups enables them to administer application servers through the administrative console or through wsadmin scripting. The administrative authorizer run time must be notified when groups are added to or removed from an administrative user group. Click Refresh all to notify the administrative authorizer after the changes have been saved and synchronized.

Logout Add... Remove Refresh all

Select User Role(s) Login Status

wasadmin	Primary administrative user name	Active
----------	----------------------------------	--------

Total 1

select **Administrator** under **Role(s)**; search for the user: **AdminFromLDAP** and add that user to **Mapped to role**. Select **OK**; then **Save**.

Administrative user roles

Administrative user roles > User

Use this page to add, update or to remove administrative roles to users. Assigning administrative roles to users enables them to administer application servers through the administrative console or through wsadmin scripting.

* Role(s)

Admin Security Manager
Administrator
Auditor
Configurator

Search and Select Users

Decide how many results to display, enter a search string (use * for wildcard), and click Search. Select users from the Available list and add them to the Mapped to role list. Users which have already been mapped to a role will not be returned in the search results.

Search string
AdminFromLDAP Search

Maximum results to display 20

Available Mapped to role

Select All Deselect All Select All Deselect All

Administrative user roles

Administrative user roles

Use this page to add, update or to remove administrative roles to groups. Assigning administrative r to administer application servers through the administrative console or through wsadmin scripting. Th run time must be notified when groups are added to or removed from an administrative user group. administrative authorizer after the changes have been saved and synchronized.

Logout Add... Remove Refresh all

Select User Role(s)

<input type="checkbox"/>	AdminFromUser	Administrator
	wasadmin	Primary administrative user name

Total 2

Verification check

Logout of the WAS Console

Now relogin as the user **AdminFromLDAP**. If all went well then you should log in successfully.

4.2 Federate Application Server into Deployment Manager:

Next we federate the AppServers (Nodes) into the Deployment Manager.

Checks:

- Ensure the clocks are in synch between your DM and AppServer. Run **ntpdate clock.redhat.com** to on your DM and AppServer.
- Make sure the DM is started and the AppServers are stopped.

Steps: On each of your Application Servers (Nodes) execute the following:

```
cd /opt/IBM/WebSphere/AppServer/bin
./addNode.sh dubxpcvm603.mul.ie.ibm.com 8879 -user wasadmin -password wasadmin
```

You should see the following

```
[root@dubxpcvm766 bin]# ./addNode.sh dubxpcvm766.mul.ie.ibm.com 8879 -user wasadmin -password wasadmin -localusername wasadmin -localpassword wasadmin
ADMU0116I: Tool information is being logged in file
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/addNode.log
ADMU0128I: Starting tool with the AppSrv01 profile
CWPKI0308I: Adding signer alias "CN=dubxpcvm766.mul.ie.ibm.com, " to local
keystore "ClientDefaultTrustStore" with the following SHA digest:
8B:40:B0:4D:31:D1:7E:22:1A:93:7E:4C:BD:74:59:00:9E:25:75:48
CWPKI0309I: All signers from remote keystore already exist in local keystore.
ADMU0001I: Begin federation of node dubxpcvm766Node01 with Deployment Manager
at dubxpcvm766.mul.ie.ibm.com:8879.
ADMU0009I: Successfully connected to Deployment Manager Server:
dubxpcvm766.mul.ie.ibm.com:8879
ADMU0505I: Servers found in configuration:
ADMU0506I: Server name: server1
ADMU2010I: Stopping all server processes for node dubxpcvm766Node01
ADMU0512I: Server server1 cannot be reached. It appears to be stopped.
ADMU0024I: Deleting the old backup directory.
ADMU0015I: Backing up the original cell repository.
ADMU0012I: Creating Node Agent configuration for node: dubxpcvm766Node01
ADMU0014I: Adding node dubxpcvm766Node01 configuration to cell:
dubxpcvm766Cell01
ADMU0016I: Synchronizing configuration between node and cell.
ADMU0018I: Launching Node Agent process for node: dubxpcvm766Node01
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:
29727

ADMU0300I: The node dubxpcvm766Node01 was successfully added to the
dubxpcvm766Cell01 cell.

ADMU0306I: Note:
ADMU0302I: Any cell-level documents from the standalone dubxpcvm766Cell01
configuration have not been migrated to the new cell.
ADMU0307I: You might want to:
ADMU0303I: Update the configuration on the dubxpcvm766Cell01 Deployment Manager
with values from the old cell-level documents.

ADMU0306I: Note:
ADMU0304I: Because -includeapps was not specified, applications installed on
the standalone node were not installed on the new cell.
ADMU0307I: You might want to:
ADMU0305I: Install applications onto the dubxpcvm766Cell01 cell using wsadmin
$AdminApp or the Administrative Console.

ADMU0003I: Node dubxpcvm766Node01 has been successfully federated.
[root@dubxpcvm766 bin]#
```

Verify the federation has been successful by:

Logging into your DM via: <https://dm&ihs.spnego.company.com:9043/ibm/console>

Then goto **Servers / Server Types / WebSphere Application Servers** you should see something like this...

WebSphere[®] software

Welcome wasadmin

Help | Logout

IBM

View: All tasks

Cell=dubxpcvm766Cell01, Profile=Dmgr01

Close page

Application servers

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	dubxpcvm766Node01	dubxpcvm766.mul.ie.ibm.com	Base	8.0.0.0	
---	---------	-------------------	----------------------------	------	---------	---

Total 1

Field help

For field help information, select a field label or list marker when the help cursor is displayed.

Page help

[More information about this page](#)

Command Assistance

[View administrative scripting command for last action](#)

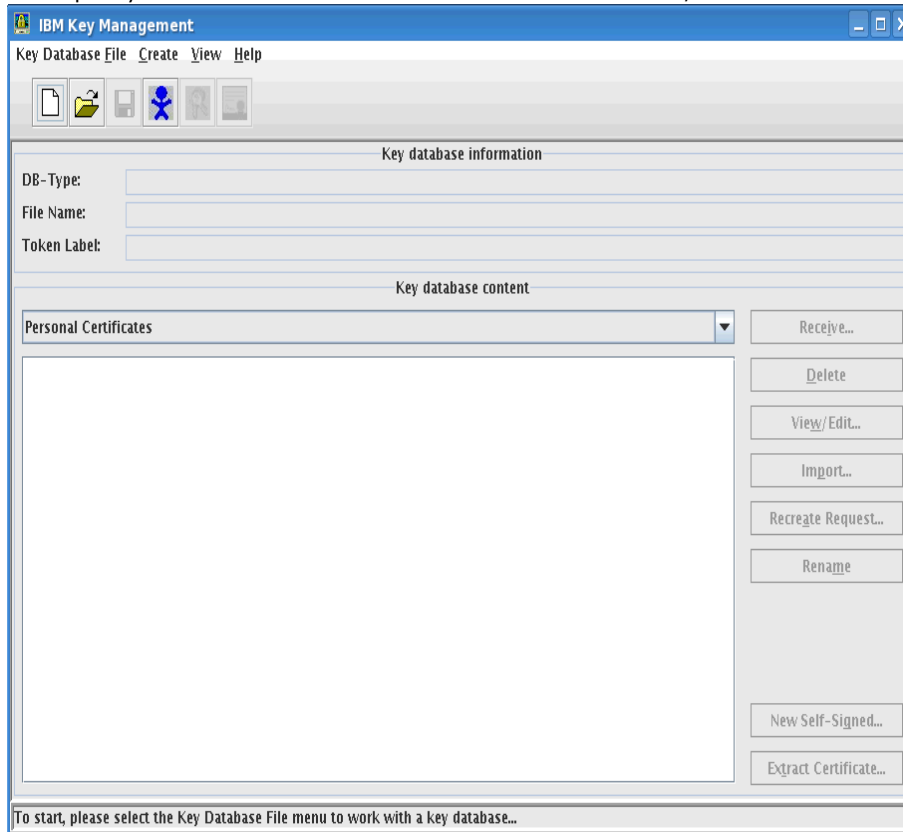
Repeat this for each node in your deployment.

4.3 Configure HTTP server to accept SSL connections

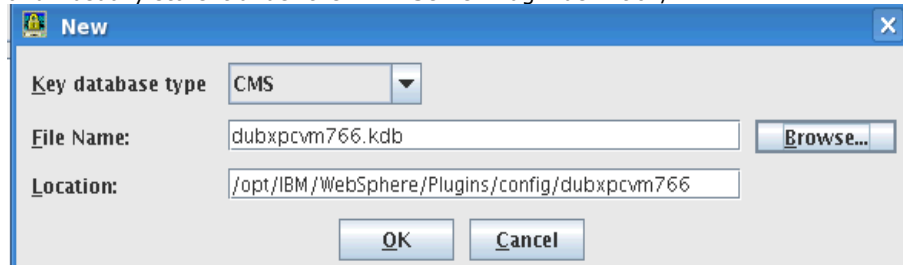
___1. Create Self-Signed SSL Certs for HTTP Server:

Connections supports login only over SSL, so we need to configure the HTTP server to accept SSL connections.

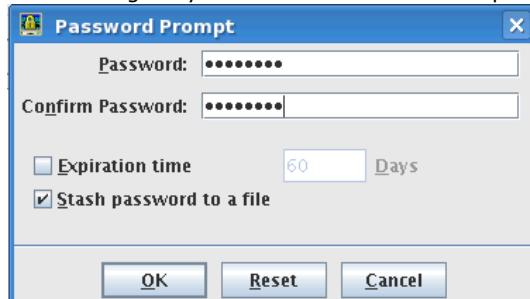
Startup ikeyman. This should be located under the HTTPServer/bin folder.



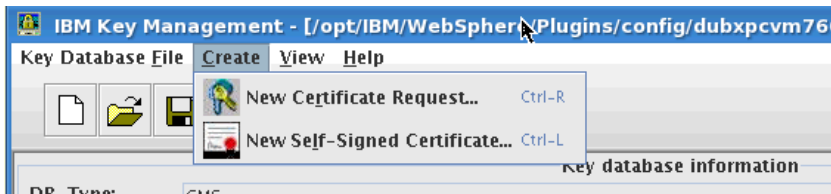
Select Key Database File -> New. Give the key a name, I usually call it the name of the server running the HTTP Server and I usually store it under the HTTP Server Plugin definition/..



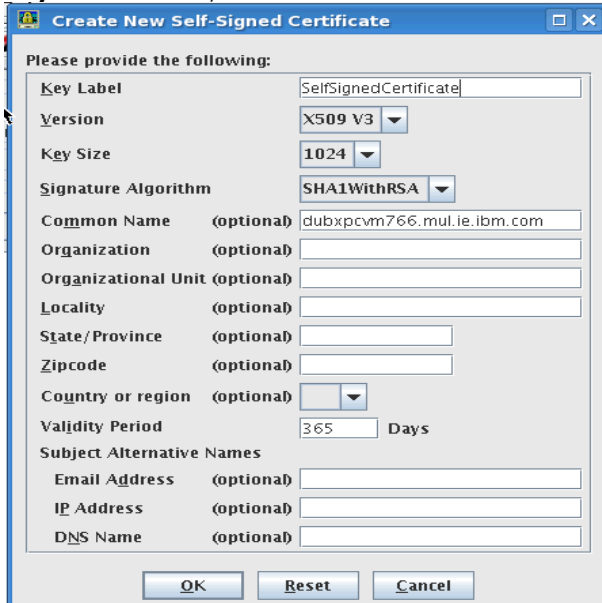
On selecting OK you will be asked to enter a password and make sure to select the **Stash password to a file** check box.



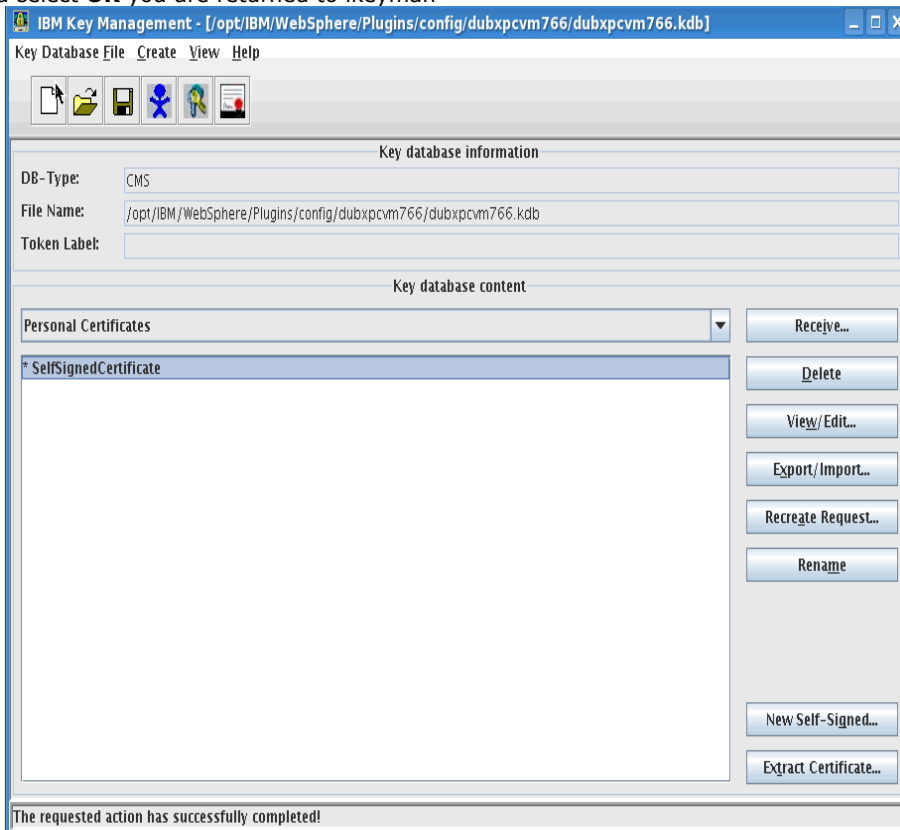
You are returned to the ikeyman panel with the dubxpcvm766.kdb opened. Now select Create and New Self-Signed Certificate...



Give the **Key Label** a name, and set the field **Common Name** to the IHS hostname.



Once you select **OK** you are returned to ikeyman



That's the certificate configured. We now need to configure the HTTP Server to use this certificate.

2. Configure httpd.conf to enable SSL:

In httpd.conf file which is under /opt/IBM/HTTPServer/conf, add the following lines to the end of file before the LoadModule was_ap22_module and WebSpherePluginConfig sections...

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
<IfModule mod_ibm_ssl.c>
    Listen 0.0.0.0:443
    ServerName dm&ihs.mul.ie.ibm.com
    <VirtualHost *:443>
        SSLEnable

        AllowEncodedSlashes On

    </VirtualHost>
</IfModule>
SSLDisable

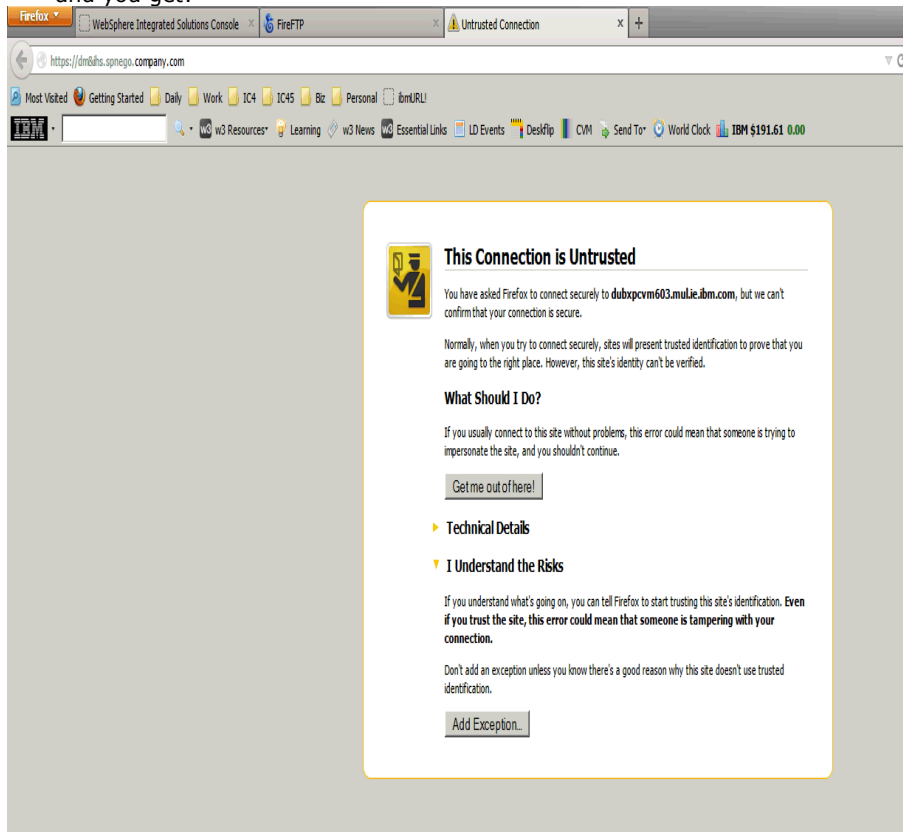
Keyfile " /opt/ihs/key.kdb"
SSLStashFile " /opt/ihs/key.sth"
```

3. Verify IHS is SSL enabled

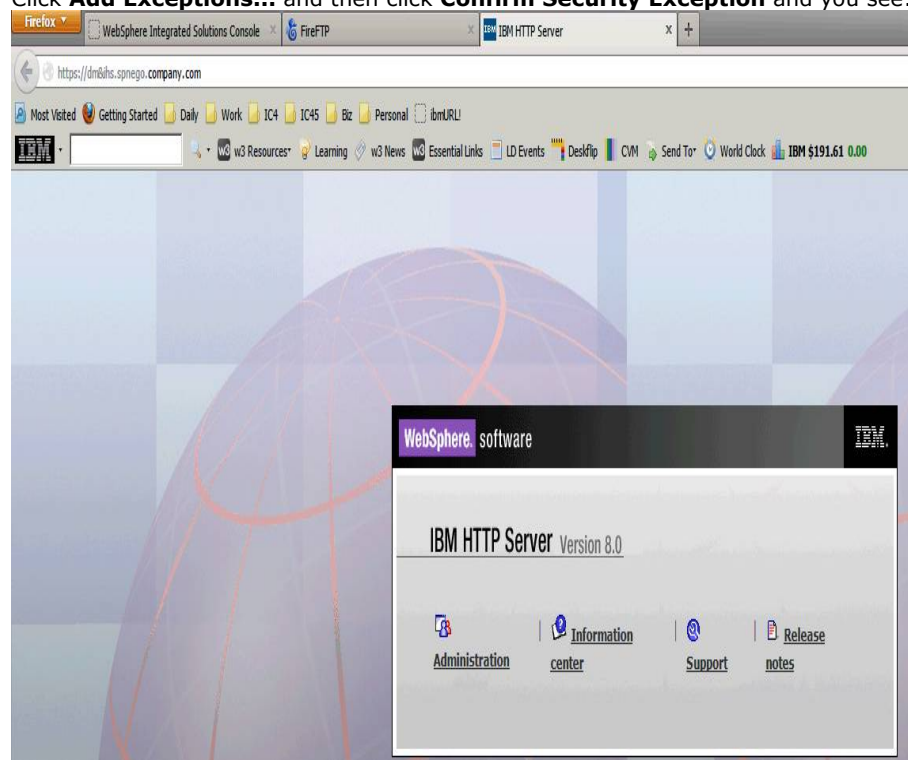
Restart/start IHS and the IHS administrator as follows: from the folder /opt/IBM/HTTPServer/bin enter:

```
./adminctl -k restart | start | stop
./apachectl -k restart | start | stop
```

Enter the IHS server URL (using the https protocol) i.e. <https://dm&ihs.spnego.company.com>, in to your browser's address box and you get:



Click **Add Exceptions...** and then click **Confirm Security Exception** and you see:



5. Create Connections DB2 databases using the dbWizard

- ___1. Log in, using a VNC client, to your database server as the **root** user or system administrator.
- ___2. Grant display authority to all users by running the following commands under the root user or system administrator:
xhost + // Grant display authority to other users
echo \$DISPLAY // Echo the value of DISPLAY under the root user
- ___3. Switch to the db2 instance admin (in this case the db2 admin is **db2inst1**)
su - db2inst1
- ___4. export the DISPLAY; enter: **export DISPLAY=:1.0**
- ___5. Start the Database Instance, by entering: **db2start**
- ___6. As root, download **IBM_Connections_4.5_wizards_lin_aix.tar** to your DB2 system and untar it (I downloaded this file into a folder called **/opt/software/ic45**)

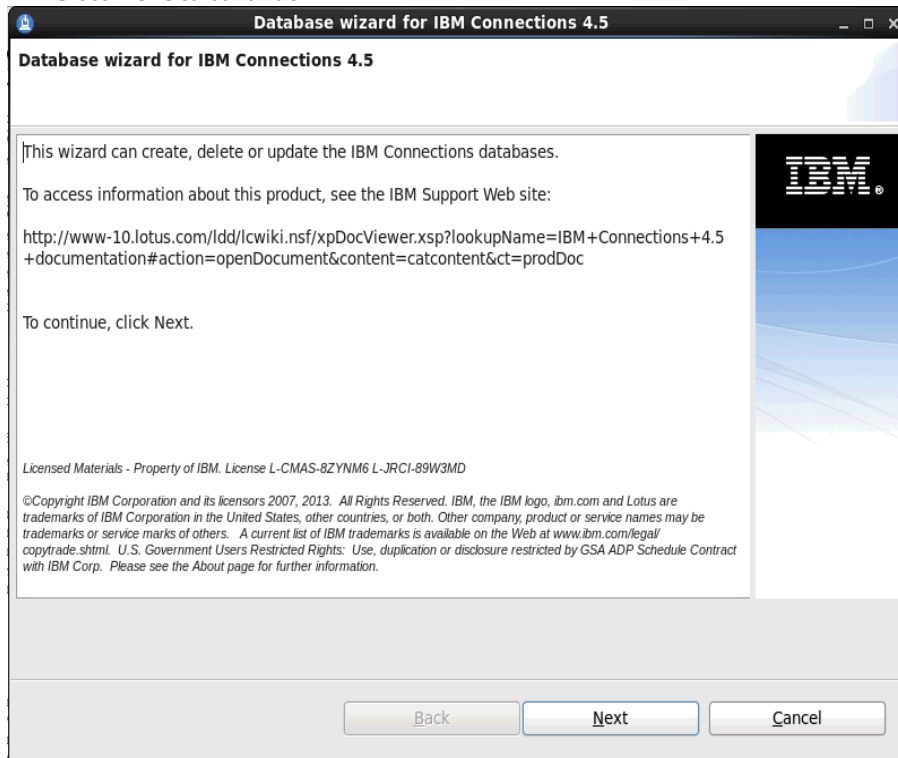
Note: The dbWizard must be run using the DB2 instance user (in this scenario this user is **db2inst1**)

- ___7. Assign the DB2 instance user as the owner for the file **IBM_Connections_4.5_wizards_lin_aix.tar** & it's respective folders.
cd /opt/software
chown db2inst1:db2iadm1 -R IC45/
cd /opt/software/ic45 and enter '**ls -la**' and you should see the file **IBM_Connections_4.5_wizards_lin_aix.tar** has the owner db2inst1:db2iadm1 i.e:

```
-rw-r--r-- 1 db2inst1 db2iadm1 580044800 Apr 22 10:19 IBM_Connections_4.5_wizards_lin_aix.tar
```

- ___8. As db2inst1, run **./dbWizard.sh** , from the folder **/opt/software/ic45/Wizards**, and follow these screens:

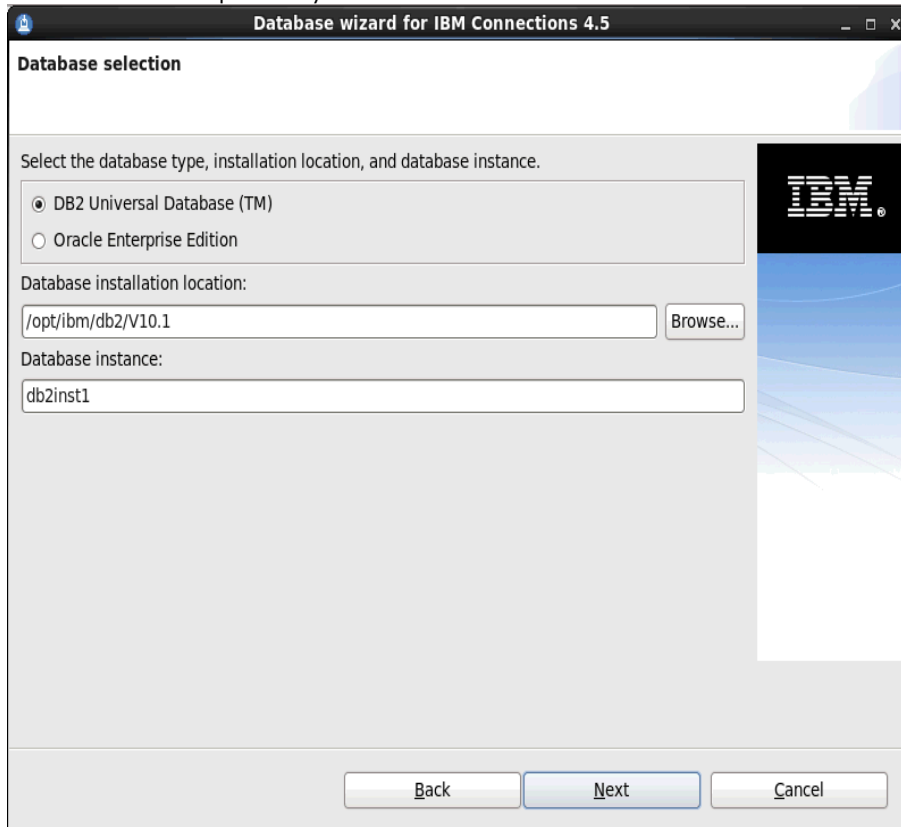
Select **Next** to continue



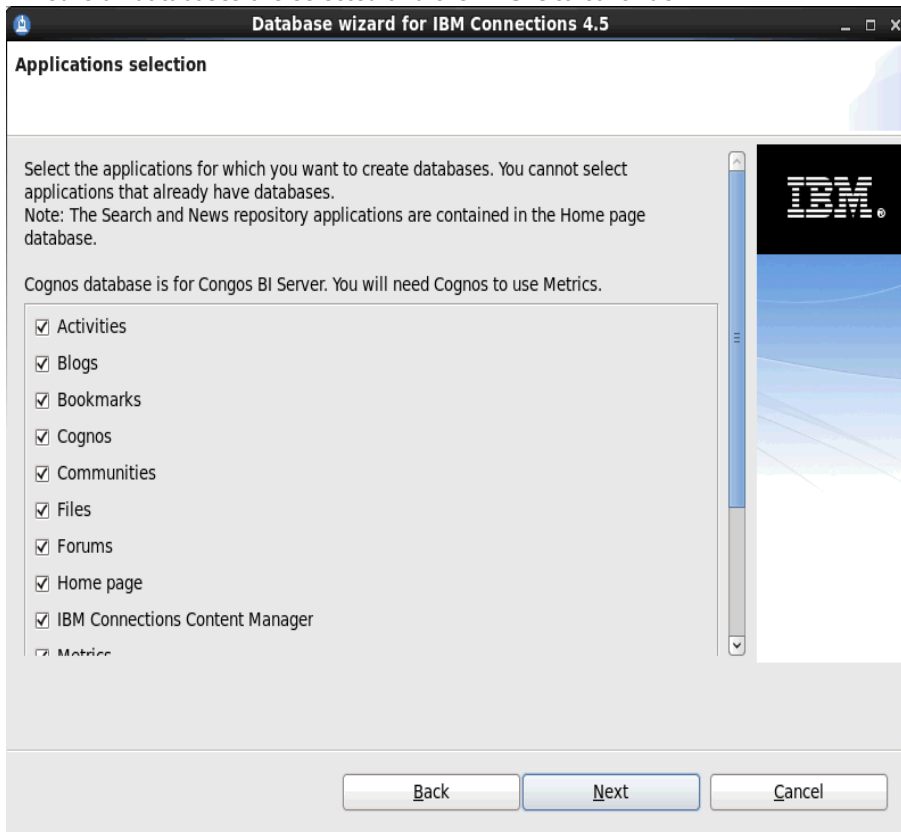
Select **Create** and then **Next**



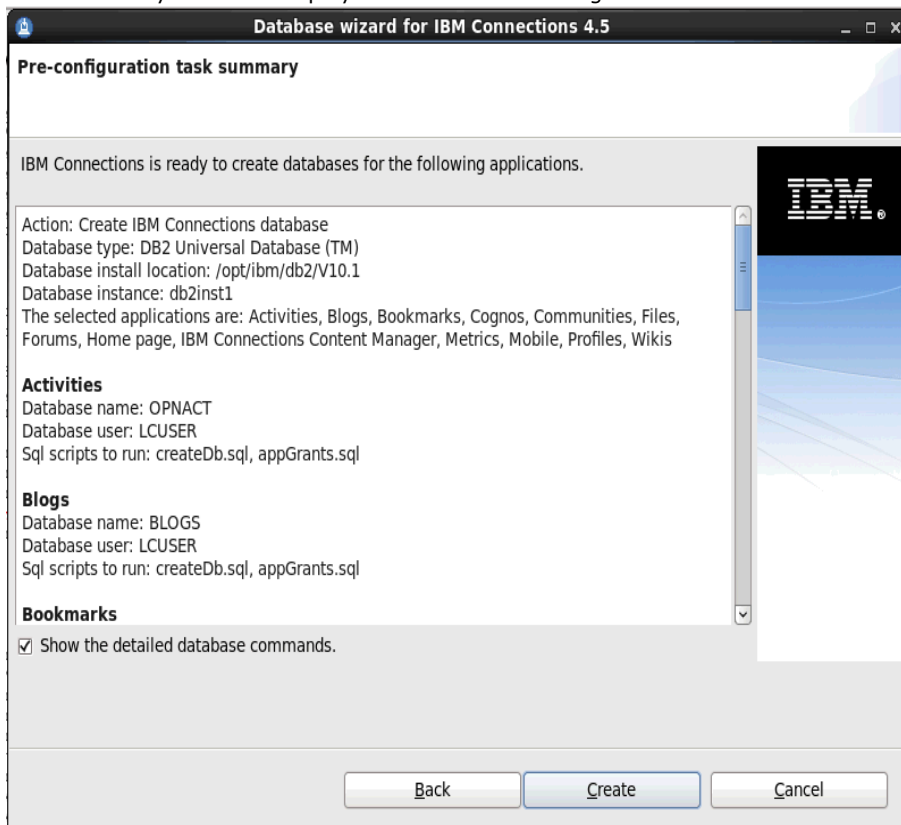
Select the path for your DB2 database installation location and the database instance name... select **Next** to continue...



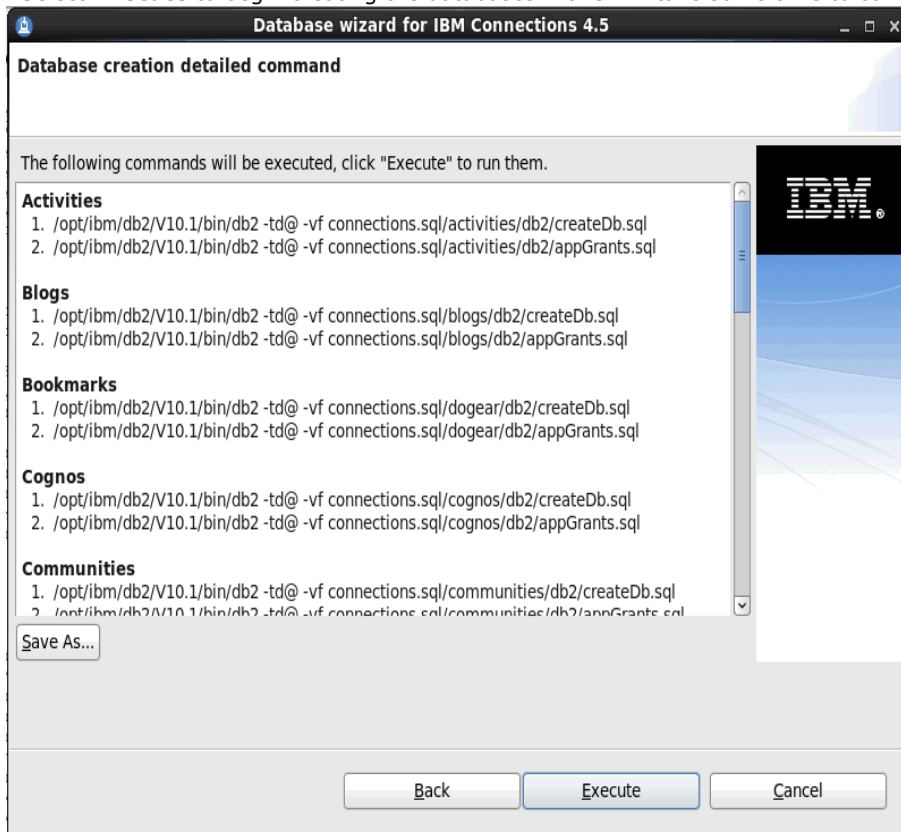
Ensure all databases are selected and then **Next** to continue...



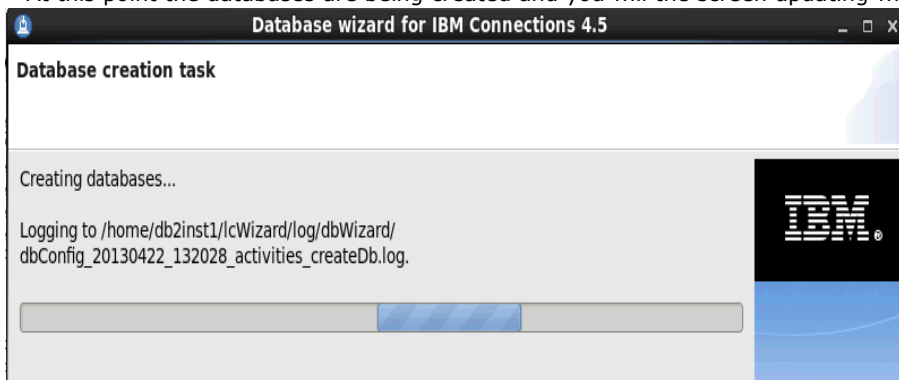
The summary screen is displayed... review the setting and select **Create**



Select **Execute** to begin creating the databases... this will take some time to complete.



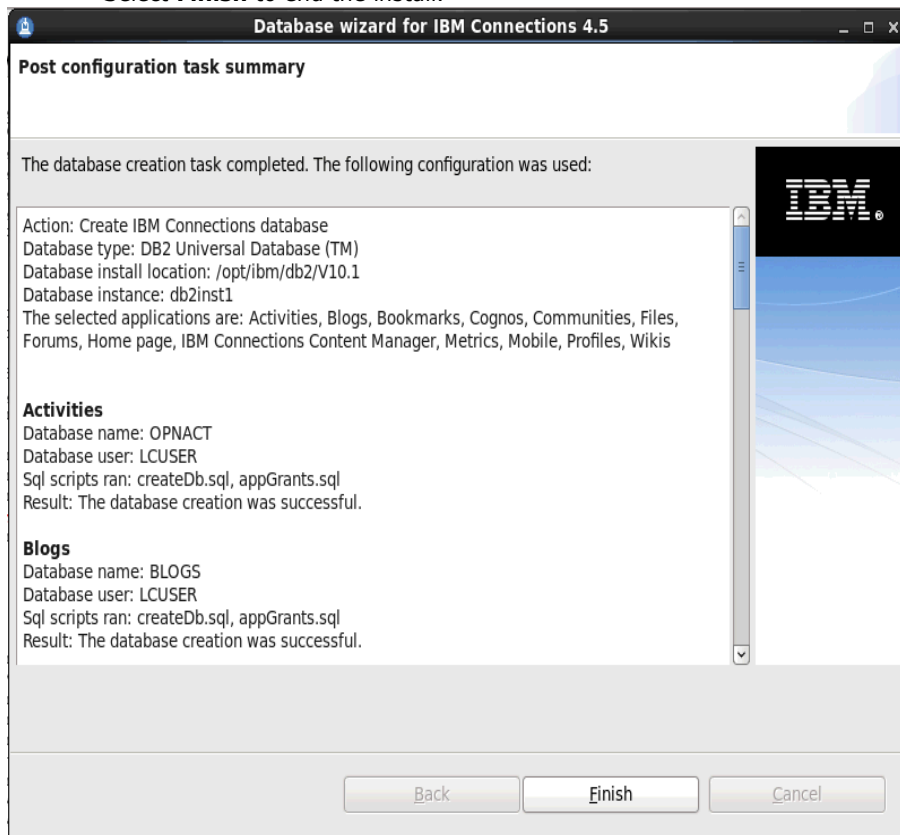
At this point the databases are being created and you will see the screen updating with info like this:



After some time (10+ minutes) the following screen appears:

Check for each database that the **Result:** message is **The database creation was successful.**

Select **Finish** to end the install.



Verify that all databases are created successfully by doing the following:

In the final screen (above) check for each database that the **"Result:"** message is **"The database creation was successful."**

Check the log files for any issues.

As user db2inst1 entering the following DB2 command and verify all Connections' databases are listed:

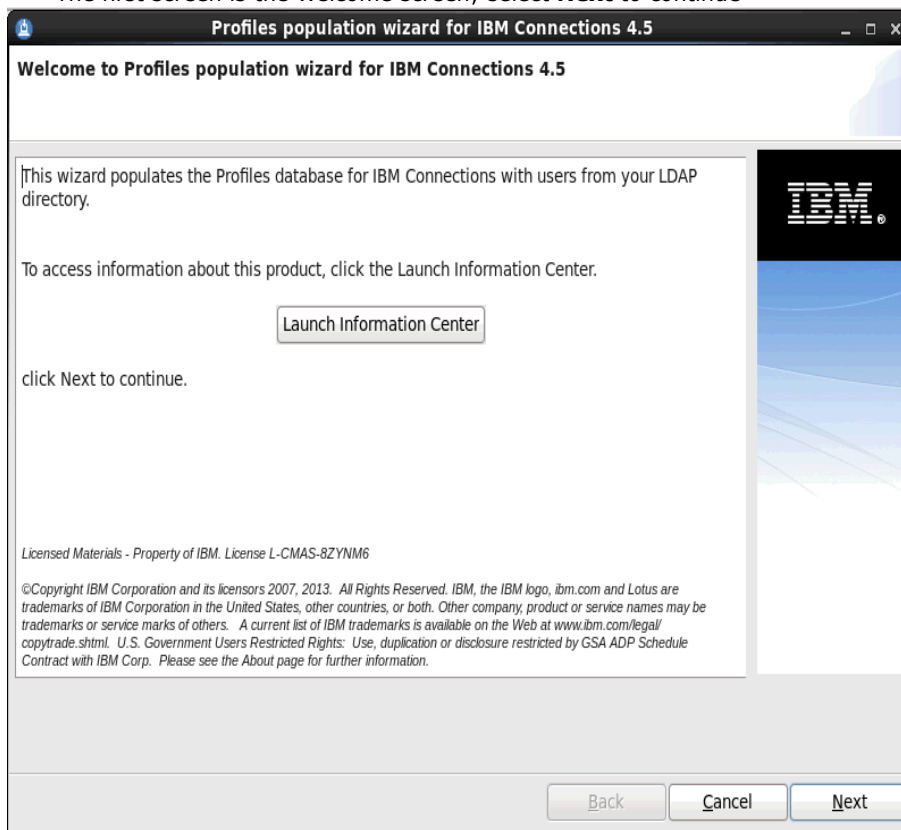
db2 list database directory

Now, as user db2inst1, issue the following DB2 command to set the default for the number of concurrently open DB2 databases to 18:

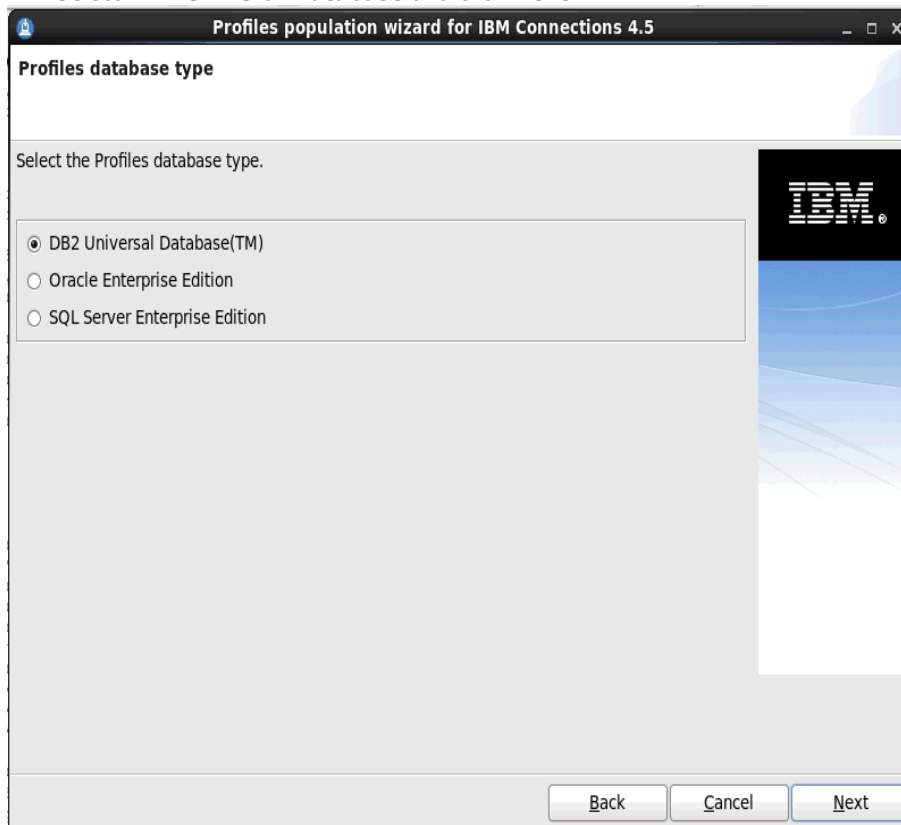
db2 update dbm cfg using numdb 18

6. Populate the Connections profiles (PEOPLEDDB) database with LDAP User Information

On the DB2 server, as root, go to the /Wizard folder and enter **./populationWizard.sh**
The first screen is the Welcome screen; select **Next** to continue



Select **DB2 Universal Database** and click **Next.....**



Next enter the database information for the profiles (PEOPLEDDB) database; select **Next** to continue..

The screenshot shows a window titled "Profiles population wizard for IBM Connections 4.5". The main heading is "Profiles database properties". Below it, a text box says: "Enter the Profiles database properties. The wizard uses this information to access the Profiles database." To the right is an IBM logo. The form contains the following fields and controls:

- Host name:
- Port:
- Database name:
- JDBC driver library path:
- User ID (Account used to write to database):
- Password:

At the bottom right are three buttons: "Back", "Cancel", and "Next".

Enter the LDAP server name and port number and then select Next to continue...

The screenshot shows the same window titled "Profiles population wizard for IBM Connections 4.5". The main heading is "LDAP server connection". Below it, a text box says: "Specify the LDAP host name and port to enable the Profiles population wizard to connect to the LDAP server." To the right is an IBM logo. The form contains the following fields and controls:

- LDAP server name:
- LDAP server port:
- Select to use SSL communication for secured access:
☐ Use SSL communication

At the bottom right are three buttons: "Back", "Cancel", and "Next".

Enter the bind user details and password **CN=bind,OU=branch,DC=spnego,DC=company,DC=com**

LDAP authentication properties

Enter the bind distinguished name and password to allow the wizard to access the LDAP directory.

Bind distinguished name (DN):
CN=bind,OU=branch,DC=spnego,DC=company,DC=com

Bind password:
.....

Back Cancel Next

Enter the search base and search filter... select **Next** to continue...

Base distinguished name and filter for searches

Enter the base distinguished name and filter for this wizard to begin searching for users in the LDAP directory tree.

LDAP user search base:
DC=spnego,DC=company,DC=com

LDAP user search filter:
(&(uid=*)(objectclass=inetOrgPerson))

Back Cancel Next

Use the default database mappings... select **Next** to continue...

The screenshot shows the 'Profiles database mapping' step of the wizard. It contains a table with three columns: 'Database Fields', 'LDAP Attributes or JS Functions', and 'Description'. The table lists various fields and their corresponding LDAP attributes or JavaScript functions. At the bottom, there are 'Back', 'Cancel', and 'Next' buttons.

Database Fields	LDAP Attributes or JS Functions	Description
alternateLastName		Alternate last name
bldgId		Building
blogUrl		Blog link
calendarUrl		Calendar link
countryCode	c	Country code
courtesyTitle		Courtesy title
deptNumber		Department number
description	description	About me
displayName	cn	Name
distinguishedName	\$dn	LDAP distinguished name
email	mail	Office email
employeeNumber	employeenumber	Employee number

Do not select any of the **Optional database tasks**

Select 'Yes' for Do you want to run the task that marks the profiles of each manager?

select Next to continue...

The screenshot shows the 'Optional database tasks' step of the wizard. It contains several checkboxes for optional tasks: 'Countries', 'Departments', 'Organizations', 'Employee types', and 'Work locations'. Each checkbox has a text field and a 'Browse' button. At the bottom, there is a question 'Do you want to run the task that marks the profiles of each manager?' with 'Yes' and 'No' radio buttons. At the very bottom, there are 'Back', 'Cancel', and 'Next' buttons.

☐ Countries
/opt/software/IC45/Wizards/TDIPopulation/linux/TDI/isocc.csv Browse

☐ Departments
/opt/software/IC45/Wizards/TDIPopulation/linux/TDI/deptinfo.csv Browse

☐ Organizations
/opt/software/IC45/Wizards/TDIPopulation/linux/TDI/orginfo.csv Browse

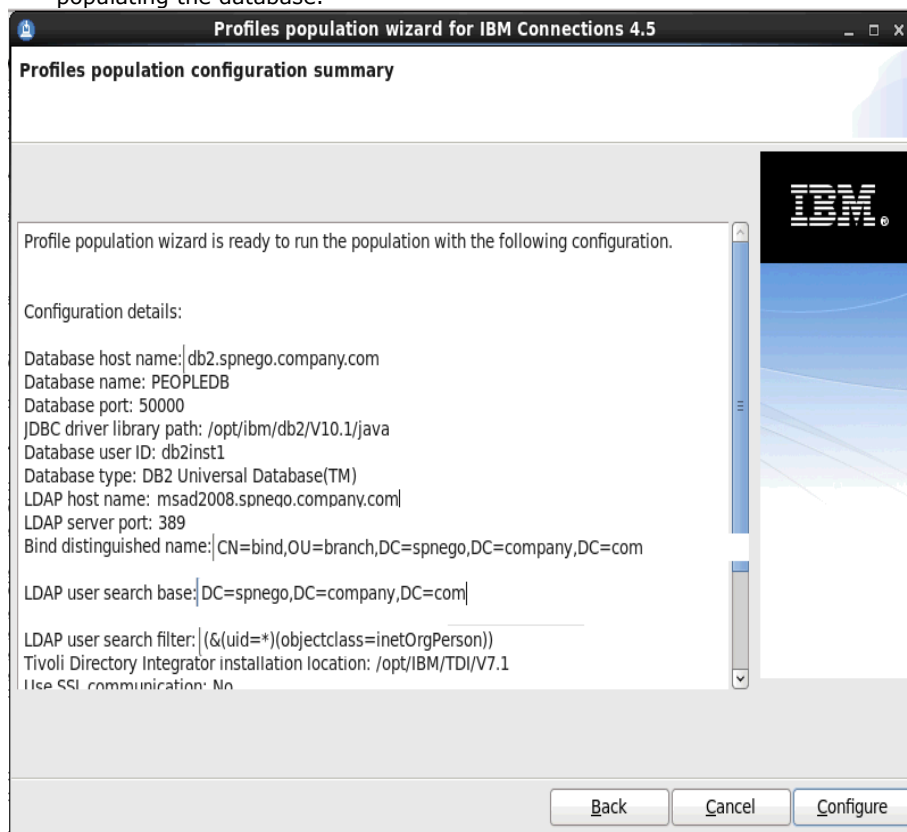
☐ Employee types
/opt/software/IC45/Wizards/TDIPopulation/linux/TDI/emtype.csv Browse

☐ Work locations
/opt/software/IC45/Wizards/TDIPopulation/linux/TDI/workloc.csv Browse

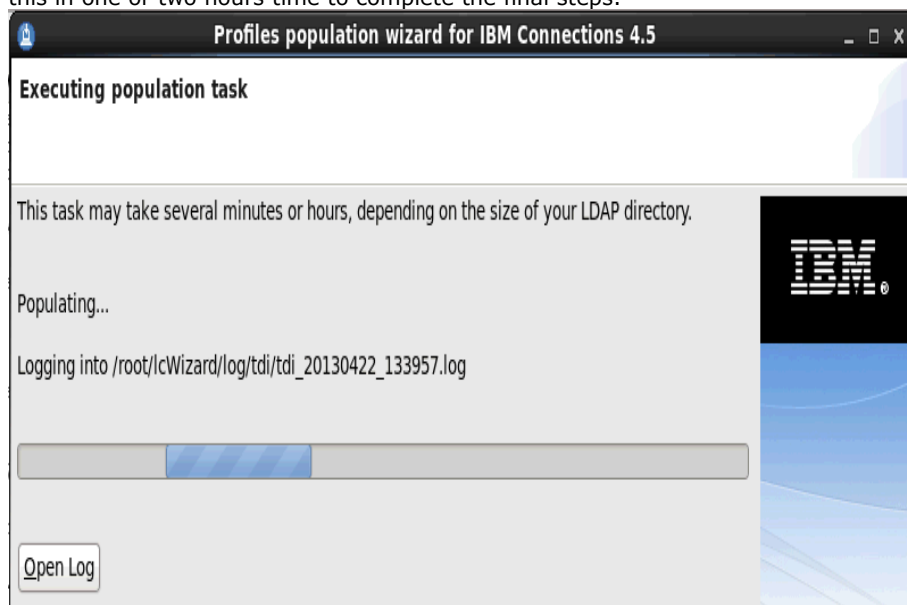
Do you want to run the task that marks the profiles of each manager?
☒ Yes
☐ No

Review the Summary page to ensure that the information you entered in the previous panels is correct.

To make changes, click Back to return to the relevant page and edit the information. Otherwise, click **Configure** to begin populating the database.



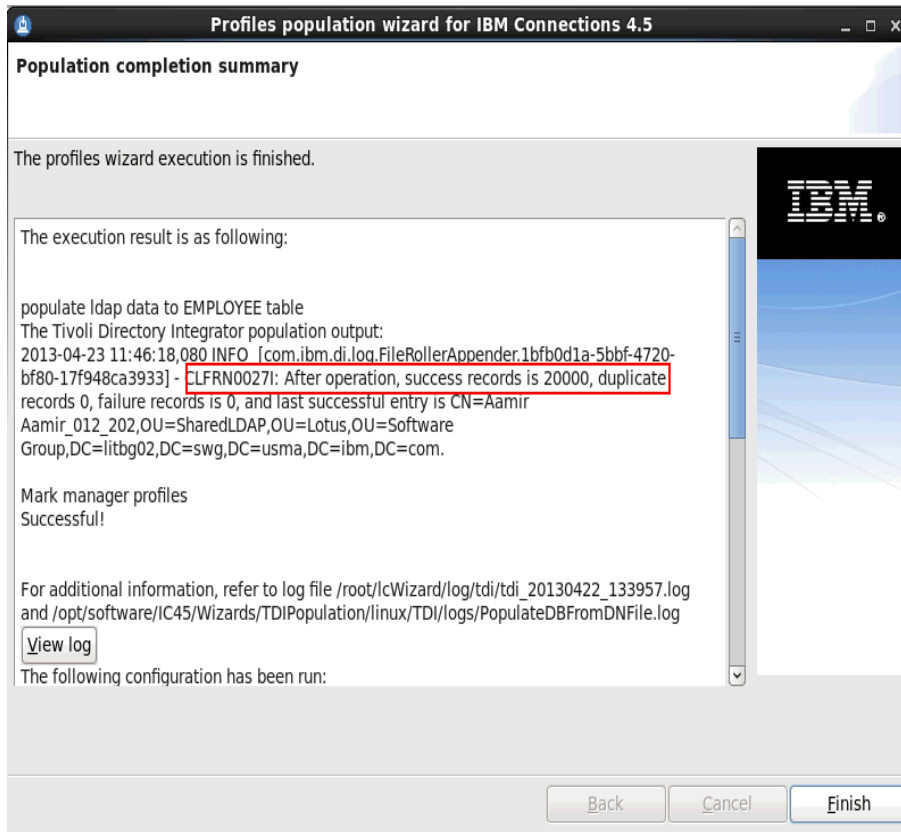
The next screen indicating that Execution of the Population Task is in progress... the population process could take over one hour. Installing IC45 does not require the profiles (PEOPLEDDB) database to be populated so I will turn to installing IC45 now and return to this in one or two hours time to complete the final steps.



Once the population wizard has completed you should get the screen below.

WARNING: There are over 400k users in my LDAP branch but the message below says that it has only successfully populated the first 20k user... this is a limitation of the dbPopulation Wizard; I will need to populate the remaining users manually (see below).

Select **Finish** to exit the wizard.



How to complete the population of the profiles database (PEOPLEDDB) with the full 400K users MANUALLY

NOTE! The `./populationWizard.sh` wizard stopped populating after the first 20k users. To fix this issue I need to manually populate the remaining 400k users using the following steps:

1. From a CMD line change to the folder: `/opt/software/IC45/Wizards/TDIPopulation/linux/TDI`
2. Edit the file **profiles_tdi.properties** and change the value for **source_ldap_page_size=1000** then save the file.
2. Run the following command: `./collect_dns.sh` - Note: this took a few hours to complete.
3. Make a backup copy of this newly created file **collect.dns** i.e. `cp collect.dns backup-collect.dns`
4. Split the file **collect.dns** into chunks of 20k users by running:
split -l 20000 collect.dns collect-split

enter `ls -la collect-split*` and you can see the list of files created each with 20k users; in my case the following files were created:
`collect-splitaa collect-splitab collect-splitac collect-splitad collect-splitae collect-splitaf collect-splitag collect-splitah collect-splitai
collect-splitaj collect-splitak collect-splital collect-splitam collect-splitan collect-splitao collect-splitap collect-splitaq collect-splitar
collect-splitas collect-splitat`
5. Populated the profiles database by running the following command
**for i in collect-splitaa collect-splitab collect-splitac collect-splitad collect-splitae collect-splitaf collect-splitag collect-splitah
collect-splitai collect-splitaj collect-splitak collect-splital collect-splitam collect-splitan collect-splitao collect-splitap collect-splitaq
collect-splitar collect-splitas collect-splitat ; do cp \$i collect.dns ; ./populate_from_dn_file.sh \$i ; rm -rf collect.dns ;
done**

Note: this step took over 24hrs to run to completion and ended with the profiles db populated with all 400+K users.

7. Installation of IBM Connections 4.5 (IC45) :

IC45 is installed over WAS 8.0.0.5.

The install of IC45 is done on the Deployment Manager (DM) machine and then synchronised with the nodes.

Check that the:

1. DM and Nodes are stopped.
2. All directory paths that you created contain no spaces.
3. Open File Descriptor limit is 8192. (ulimit -n 8192).
4. required OS libraries/patches are installed on all systems

Steps:

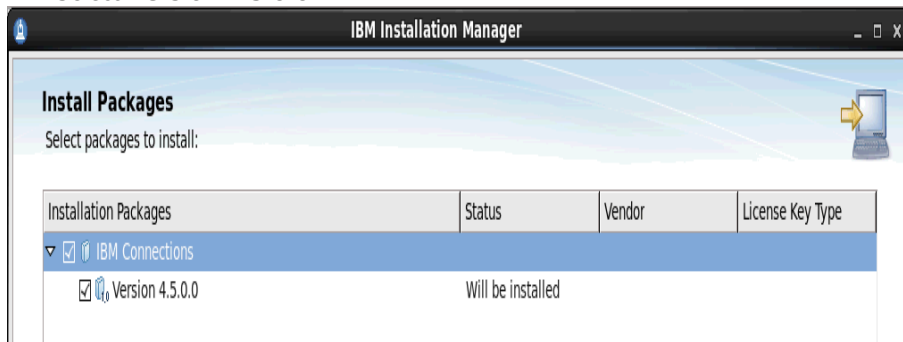
Copy the IC45 install file (IBM_Connections_4.5_lin_aix.tar) to your Deployment Manager and decompress it.

Start the IBM Installation Manager: got to the folder: **/opt/IBM/InstallationManager/eclipse** and start **./launcher**

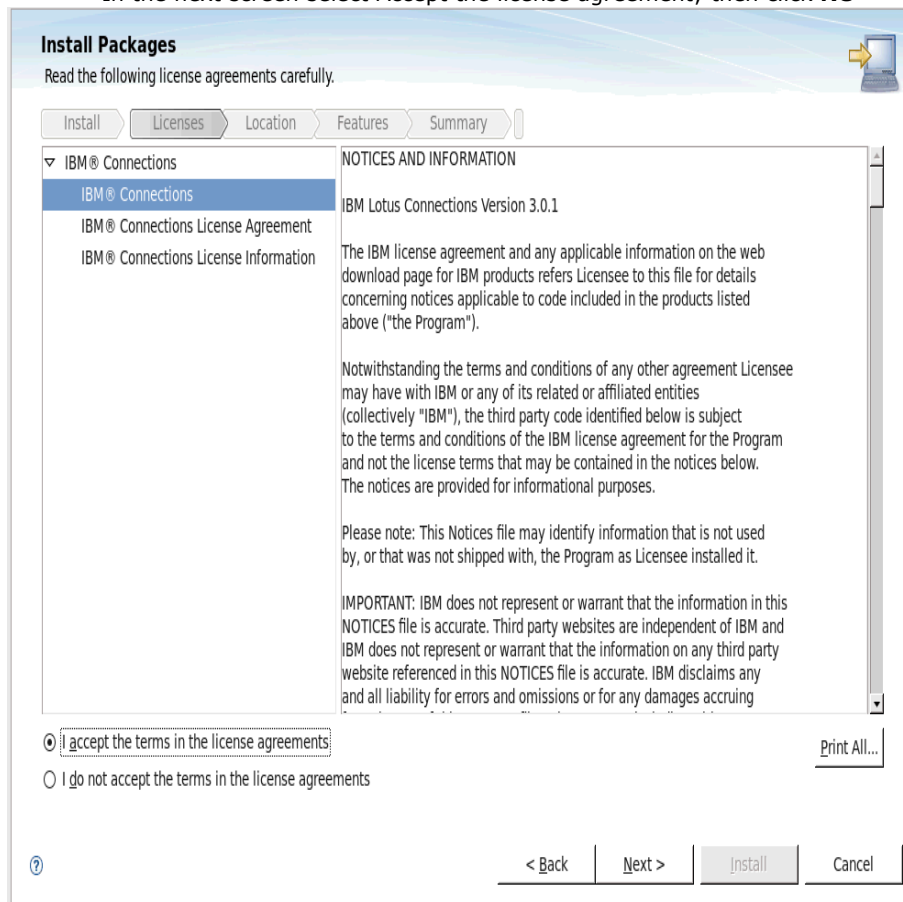
In the IM specify the IC45 repository file.

Select **Install** to start the IC45 install and follows these screen

Select **Version 4.5.0.0**



In the next screen select Accept the license agreement; then click **Ne**



Install Packages

A package group is a location that contains one or more packages. Some compatible packages can be installed into a common package group and will share a common user interface. Select an existing package group, or create a new one.

Install | Licenses | **Location** | Features | Summary

- ☐ Use the existing package group
- ☒ Create a new package group

Package Group Name	Installation Directory	Architecture
IBM® Connections	/opt/IBM/Connections	

Package Group Name: IBM® Connections

Installation Directory: /opt/IBM/Connections

Browse...

Details

Shared Resources Directory: /opt/IBM/IMShared

Disk Space Information

Volume	Available Space
/	12.58 GB



< Back

Next >

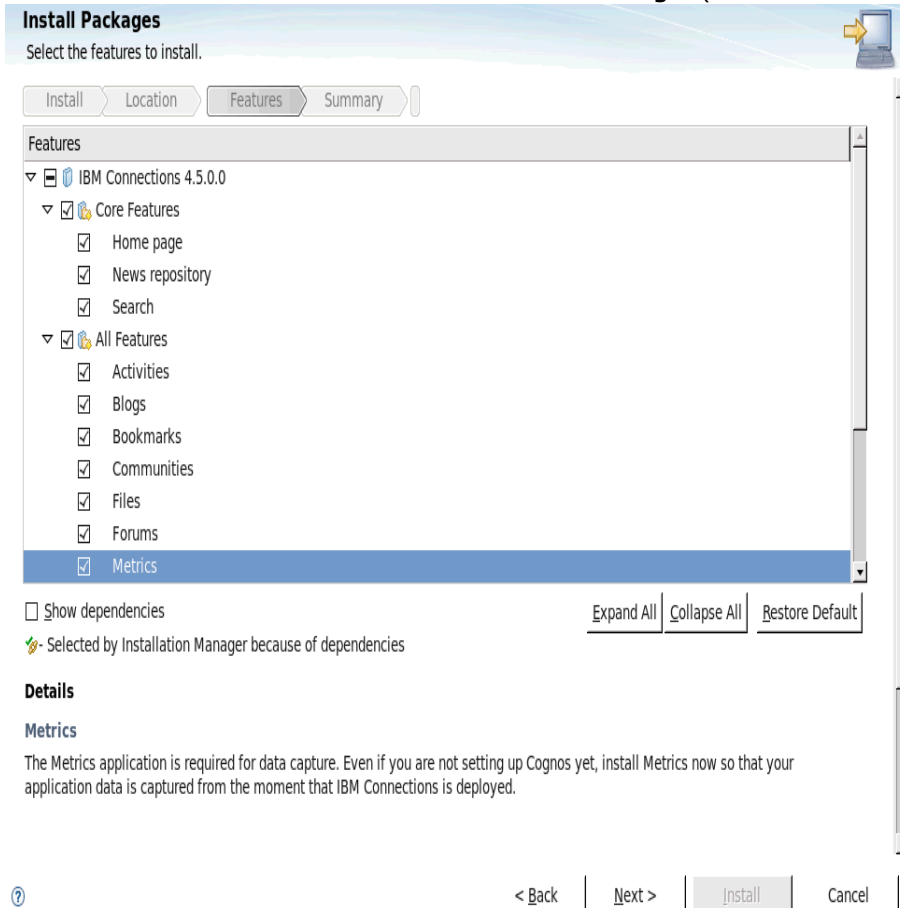
Install

Cancel

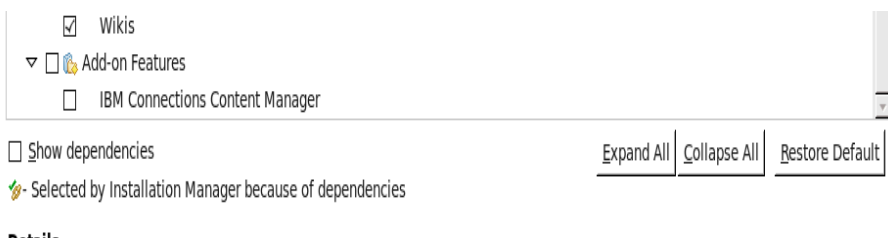
Select what applications to install.

I selected **Metrics** because when I get to the Cognos install screen I can choose **Not to Install Now** and do this later.

I did NOT select **IBM Connections Content Manager** (File)



Note: IBM Connections Content Manager is not selected...

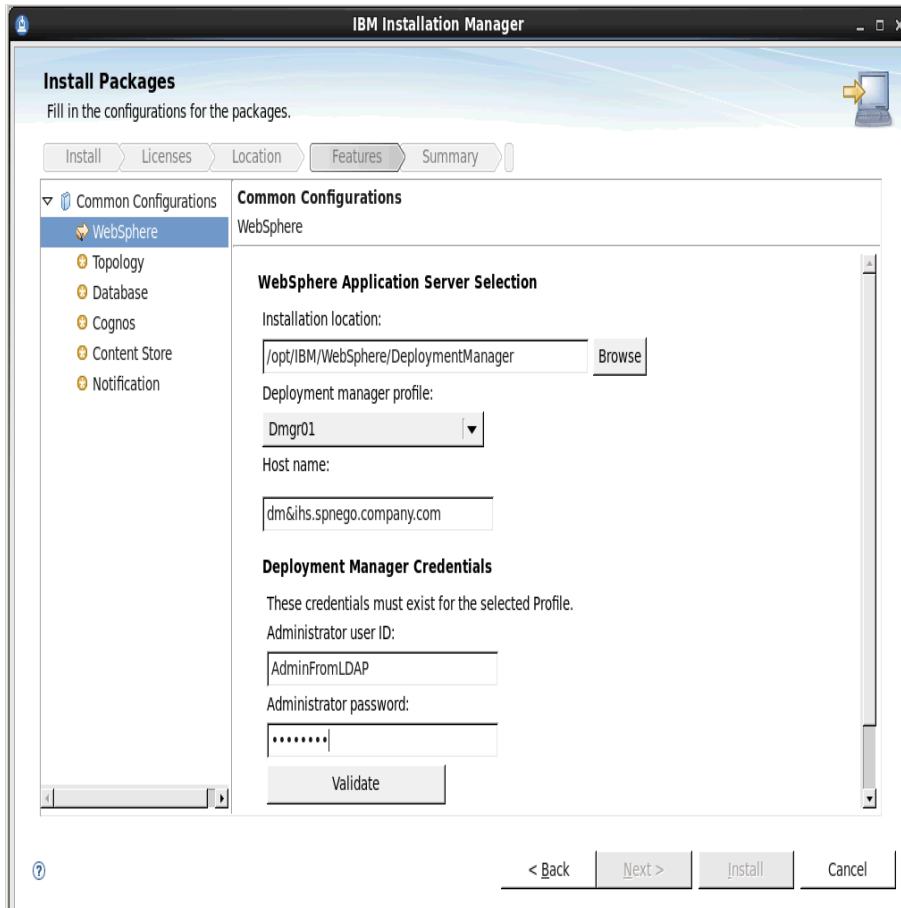


Select the path to the WebSphere Application Server instance running on your deployment manager.

Enter the hostname,

NOTE: the Administration user ID = AdminFromLDAP

Select the **Validate** button at the bottom.



The screenshot shows the 'Install Packages' window in IBM Installation Manager. The 'Location' tab is selected. Under 'Common Configurations', 'WebSphere' is chosen. The 'WebSphere Application Server Selection' section contains the following fields: 'Installation location' with the path '/opt/IBM/WebSphere/DeploymentManager' and a 'Browse' button; 'Deployment manager profile' with a dropdown menu showing 'Dmgr01'; and 'Host name' with the value 'dm&ihs.spnego.company.com'. The 'Deployment Manager Credentials' section includes a note 'These credentials must exist for the selected Profile.', 'Administrator user ID' with the value 'AdminFromLDAP', and 'Administrator password' with masked characters. A 'Validate' button is at the bottom of this section. At the very bottom of the window are navigation buttons: '< Back', 'Next >', 'Install', and 'Cancel'.

The install will then proceed to perform various checks and retrieve info from the DM. After a few moments you should get the prompt: **Validation successful.**

Select **OK**, then **Next** to continue.



The screenshot shows an 'Information Dialog' window with a lightbulb icon and the text 'Validation successful.'. An 'OK' button is located at the bottom right of the dialog.

Selected the **Medium** topology

Select the Nodes as required (I selected all nodes) then **Next**

Install Packages
Fill in the configurations for the packages.

Install | Licenses | Location | **Features** | Summary

Common Configurations

- WebSphere
- Topology**
- Database
- Cognos
- Content Store
- Notification

Common Configurations
Topology

Deployment topology
Select the deployment type:

☐ Small - All applications are grouped in the same cluster.

☒ **Medium - Applications grouped in several clusters.**

☐ Large - Each application is grouped in its own cluster.

If you return to this page during installation, your settings remain but are not visible. To change a settings, you must enter all of the information again. If you do not want to change them, click Next.

Cluster
Enter a cluster name or select an existing cluster name. Then select the nodes for each cluster and enter a server name or accept the default server name.

Restore Defaults

Application	Cluster	Node	Server
▼ Activities	Cluster1	<input checked="" type="checkbox"/> dslvm1035Node01	Cluster1_server1
		<input checked="" type="checkbox"/> dslvm1036Node01	Cluster1_server2

Configure **Database** - (the database server must be started) as shown below; click **Validate**; then **Next**

Install Packages

Fill in the configurations for the packages.

Install Licenses Location Features Summary

Common Configurations

WebSphere

Topology

Database

Cognos

Content Store

Notification

Common Configurations

Database

Database Location

Are all IBM Connections applications using the same database instance?
☒ Yes, the applications are on the same database instance.
☐ No, the applications are not on the same database instance.
If you return to this page during installation, your settings remain but are not visible. To change a settings, you must enter all of the information again. If you do not want to change them, click Next.

Database Type
DB2 Universal Database(TM)

Database Server
Host name:
db2.spnego.company.com
Port:
50000
JDBC driver location:

Notification

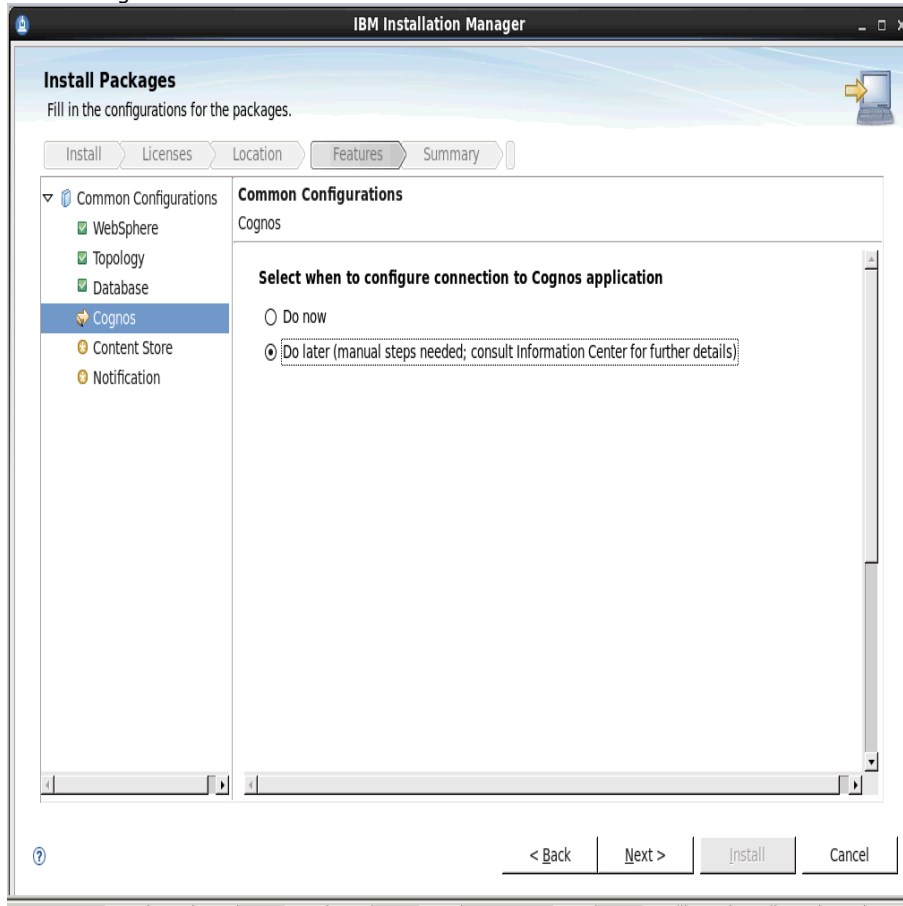
JDBC driver location:
/opt/DB2-JDBC-jars Browse

Database Credentials
☒ Use the same password for all applications.

Application	Database Name	User ID	Password
Activities	OPNACT	db2inst1	*****
Blogs	BLOGS	db2inst1	*****
Bookmarks	DOGEAR	db2inst1	*****
Communities	SNCOMM	db2inst1	*****
Files	FILES	db2inst1	*****

? < Back Next > Install Cancel

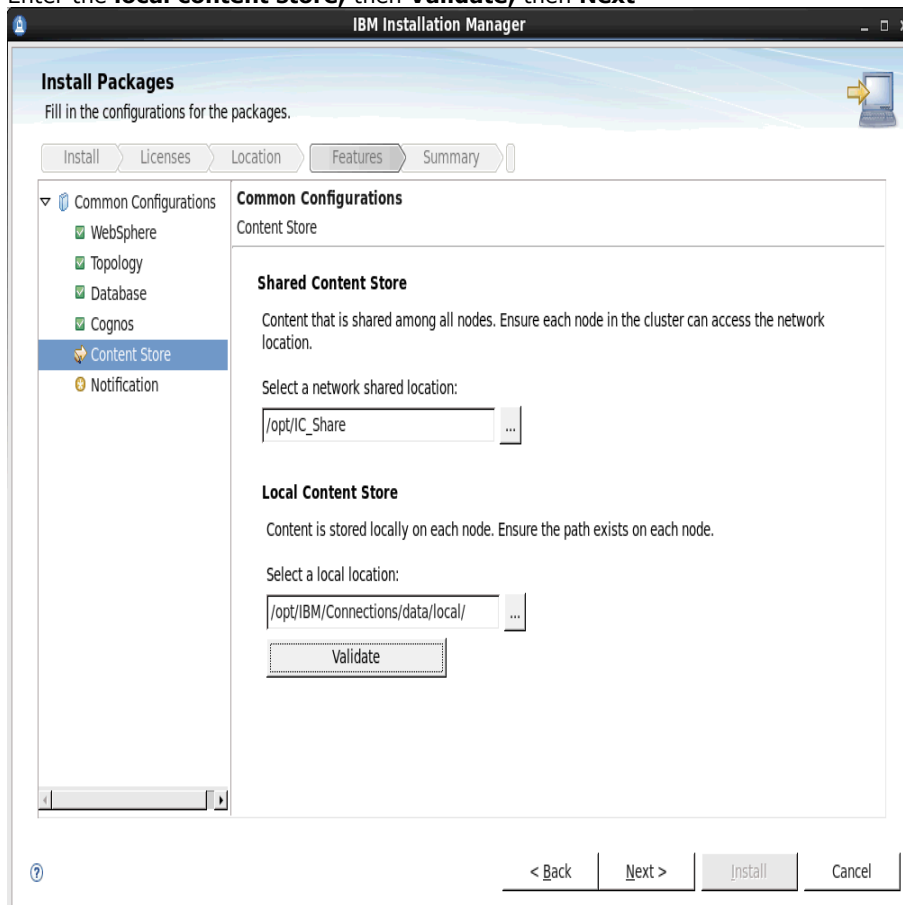
Next is Cognos - select **Do later**



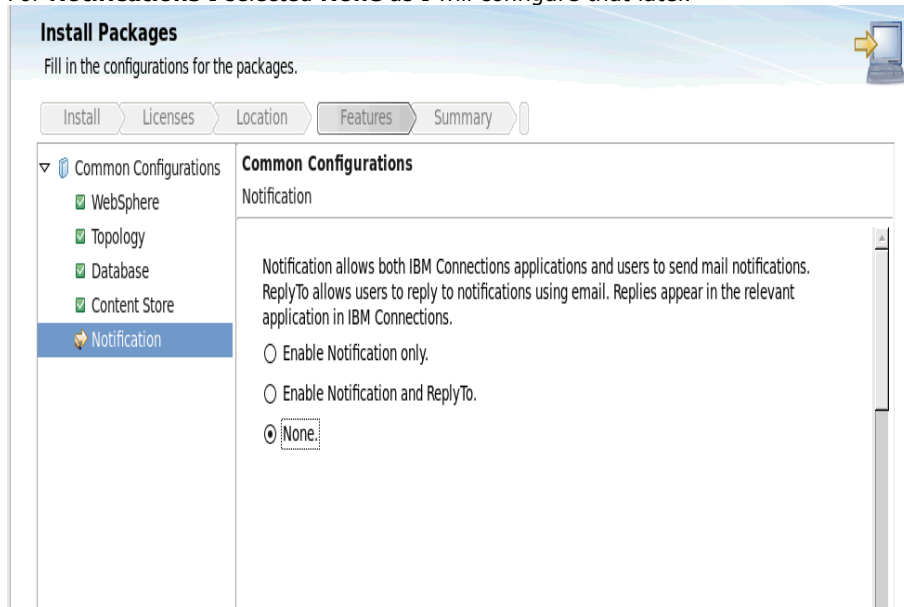
Next **Content Store**

Enter the **network share location** (that will be shared with the Application servers Node1 & Node2)

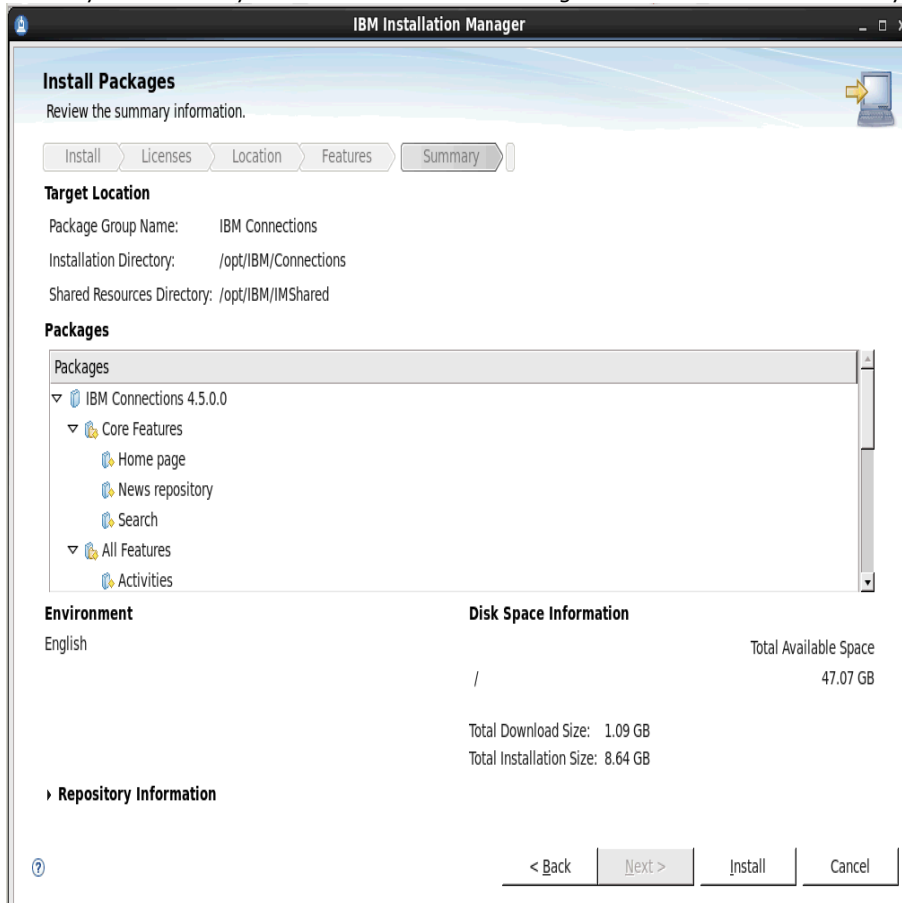
Enter the **local content store**; then **Validate**; then **Next**



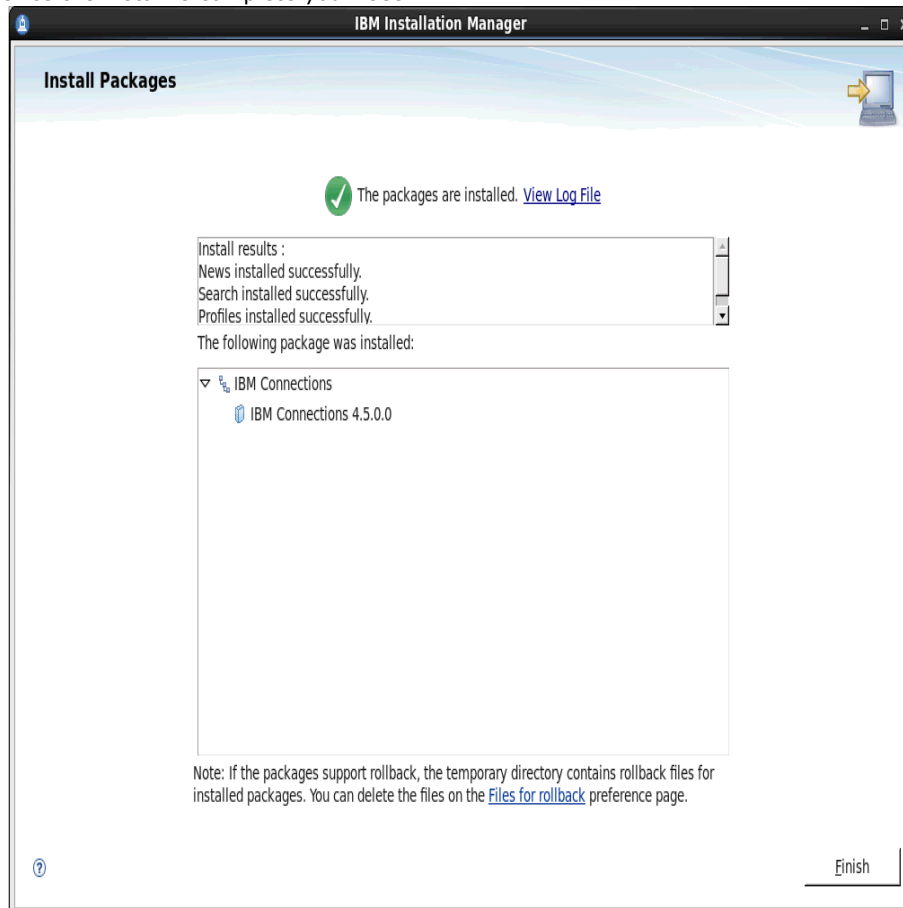
For **Notifications** I selected **None** as I will configure that later.



And finally the summary screen.... click **Install** to begin the install of IC45. This may take over an hour to complete.



Once the install is complete you'll see:



Select **Finish** to exit and return to the Installation Manager, then select **File -> Exit**

8. Post Install steps

8.1 Copying Search conversion tools to local nodes

___1. On each Applications server (node) copy the entire **stellent** folder in the shared drive (under **/opt/IC_Share/search**) to the local **search** folder under **/opt/IBM/Connections/data/local**.

___2. Via the WAS console update the Websphere variable: **FILE_CONTENT_CONVERSION** to point to the **exporter** file in the stellent folder on local drive of each node (that you copied in step 1)
set the variable:

FILE_CONTENT_CONVERSION=/opt/IBM/Connections/data/local/search/stellent/dcs/oiexport/exporter

___3. Edit the file **setupCmdLine.sh** and add the following export statements

vi /opt/IBM/WebSphere/AppServer/bin/setupCmdLine.sh

add

export PATH=\$PATH:/opt/IBM/Connections/data/local/search/stellent/dcs/oiexport

export LD_LIBRARY_PATH=\$LD_LIBRARY_PATH:/opt/IBM/Connections/data/local/search/stellent/dcs/oiexport

___4. Add the following export statements to the **/etc/profile** file

export PATH=\$PATH:/opt/IBM/Connections/data/local/search/stellent/dcs/oiexport

export LD_LIBRARY_PATH=\$LD_LIBRARY_PATH:/opt/IBM/Connections/data/local/search/stellent/dcs/oiexport

8.2 Configuring the HTTP Server

1) Add the Web server as an unmanaged node AND Add Web server as a server

A quick way to do this is to use the special configure file that was created when the IHS was created as follows:

From the IHS server, copy the file **/opt/IBM/WebSphere/Plugins/bin/configurewebserver1.sh** (remember I used the name 'webserver1' when creating the IHS server) to the Deployment Manager system in to the folder:
/opt/IBM/WebSphere/AppServer/bin

NOTE: The above filename and location will vary depending on what values you used to install the IHS and the Deployment Manager

On the DM machines run the **configurewebserver1.sh** file as follows

```
cd /opt/IBM/WebSphere/AppServer/bin
./configurewebserver1.sh
```

You will be prompted to enter WAS credentials and then after a few minutes the creation of the Web server will complete...you should see the following messages appear:

```
[root@dubxpcvm603 bin]# ./configurewebserver1.sh
WASX7209I: Connected to process "dmgr" on node dubxpcvm603CellManager01 using SO
AP connector; The type of process is: DeploymentManager
WASX7303I: The following options are passed to the scripting environment and are
available as arguments that are stored in the argv variable: "[webserver1, IHS,
/opt/IBM/HTTPServer, /opt/IBM/HTTPServer/conf/httpd.conf, 80, MAP_ALL, /opt/IBM
/WebSphere/Plugins, unmanaged, dubxpcvm603.mul.ie.ibm.com-node, dubxpcvm603.mul
.ie.ibm.com, linux, 8008, ihsadmin, passw0rd]"

Input parameters:

Web server name           - webserver1
Web server type           - IHS
Web server install location - /opt/IBM/HTTPServer
Web server config location - /opt/IBM/HTTPServer/conf/httpd.conf
Web server port           - 80
Map Applications          - MAP_ALL
Plugin install location   - /opt/IBM/WebSphere/Plugins
Web server node type      - unmanaged
Web server node name      - dubxpcvm603.mul.ie.ibm.com-node
Web server host name      - dubxpcvm603.mul.ie.ibm.com
Web server operating system - linux
IHS Admin port            - 8008
IHS Admin user ID         - ihsadmin
IHS Admin password        - passw0rd
IHS service name          - ""

Found node with matching hostname. Using existing node dubxpcvm603Node01

Node definition dubxpcvm603Node01 already exists.

Creating the web server definition for webserver1 on node dubxpcvm603Node01.
Parameters for administering IHS web server can also be updated using wsadmin sc
```

And end with...

```
Computed the current target mapping for the application Wikis.
Start updating the target mappings for the application Wikis.
ADMA5075I: Editing of application Wikis started.
ADMA5058I: Application and module versions are validated with versions of deploy
ment targets.
ADMA5005I: The application Wikis is configured in the WebSphere Application Serv
er repository.
ADMA5005I: The application Wikis is configured in the WebSphere Application Serv
er repository.
ADMA5005I: The application Wikis is configured in the WebSphere Application Serv
er repository.
ADMA5005I: The application Wikis is configured in the WebSphere Application Serv
er repository.
ADMA5113I: Activation plan created successfully.
ADMA5011I: The cleanup of the temp directory for application Wikis is complete.
ADMA5076I: Application Wikis edited successfully. The application or its web mod
ules may require a restart when a save is performed.
Target mapping is updated for the application Wikis.

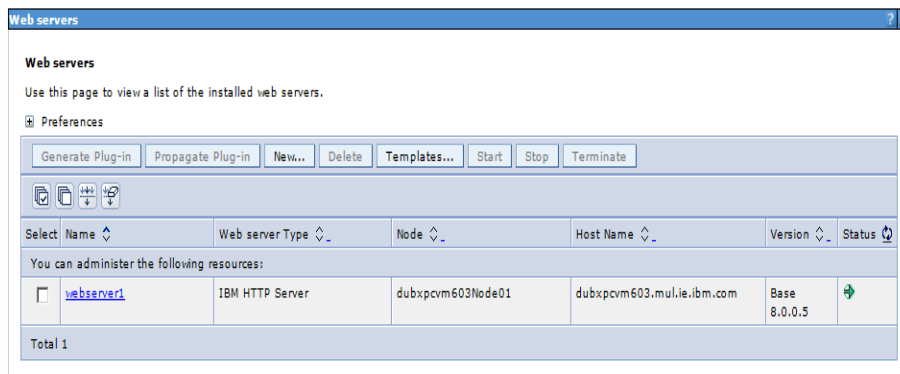
Processing the application connectionsProxy.
Get the current target mapping for the application connectionsProxy.
Computed the current target mapping for the application connectionsProxy.
Start updating the target mappings for the application connectionsProxy.
ADMA5075I: Editing of application connectionsProxy started.
ADMA5058I: Application and module versions are validated with versions of deploy
ment targets.
ADMA5005I: The application connectionsProxy is configured in the WebSphere Appli
cation Server repository.
ADMA5005I: The application connectionsProxy is configured in the WebSphere Appli
cation Server repository.
ADMA5005I: The application connectionsProxy is configured in the WebSphere Appli
cation Server repository.
ADMA5005I: The application connectionsProxy is configured in the WebSphere Appli
cation Server repository.
ADMA5113I: Activation plan created successfully.
ADMA5011I: The cleanup of the temp directory for application connectionsProxy is
complete.
ADMA5076I: Application connectionsProxy edited successfully. The application or
its web modules may require a restart when a save is performed.
Target mapping is updated for the application connectionsProxy.

Start saving the configuration.
Configuration save is complete.
```

Stops and restart the Deployment Manager

Log in to the WAS console and verify that the Web server has been added under **Servers -> Server Types -> Web servers** and you should see:

Try Stop and Start the web server thru the menu options.



Note: The IHS administrator must be running in order to be able to administrate the web server via this Web server panel and to to synchronize configuration files between the HTTP Server and the DM. To do this navigate to **../HTTPServer/bin** directory (on the IHS server) and issue the command: **./adminctl -k start**

___2) Generate and Propagate configuration info to the Plugin-cfg.xml file

Return to **Servers - Server Types - Web Servers**.

Select the check box beside **webserver1** and click the **Generate Plug-in** button.

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:

Select	Name	Web server Type	Node	Host Name	Version	Status
<input type="checkbox"/>	webserver1	IBM HTTP Server	webserver	dm&ihs.spnego.compan	Not applicable	

Total 1

results in...

Web servers

☒ Messages

- PLGC0005I: Plug-in configuration file = C:\IBM\WebSphere\AppServer\profiles\Dmgr02\config\cells\connectionsCell01\nodes\webserver\servers\webserver1\plugin-cfg.xml
- PLGC0052I: Plug-in configuration file generation is complete for the Web server, connectionsCell01.webserver.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:

Select	Name	Web server Type	Node	Host Name	Version	Status
<input type="checkbox"/>	webserver1	IBM HTTP Server	webserver	dm&ihs.spnego.compai	Not applicable	

Total 1

Select the check box again and click **Propagate Plug-in** (which propagates the plugin-cfg.xml file to the webserver)

Web servers

☒ Messages

- PLGC0062I: The plug-in configuration file is propagated from C:\IBM\WebSphere\AppServer\profiles\Dmgr02\config\cells\connectionsCell01\nodes\webserver\servers\webserver1\plugin-cfg.xml to c:\IBM\HTTPServer\Plugins\config\webserver1\plugin-cfg.xml on the Web server computer.
- PLGC0048I: The propagation of the plug-in configuration file is complete for the Web server, connectionsCell01.webserver.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:

Select	Name	Web server Type	Node	Host Name	Version	Status
<input type="checkbox"/>	webserver1	IBM HTTP Server	webserver	dm&ihs.spnego.company	Not applicable	

Total 1

___3) Propagate The plug-in keyring file from the DM to the IHS web server

Click on **webserver1** then click on the link: **Plug-in properties**

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
C:/IBM/HTTPServer

* Configuration file name
\${WEB_INSTALL_ROOT}/conf/httpd.conf Edit

* Service name
IBMHTTPServer7.0

Apply OK Reset Cancel

Configuration settings

- Web Server Virtual Hosts
- Global Directives

Additional Properties

- Log file
- Configuration File
- Plug-in properties**
- Remote Web server management
- Custom properties
- Ports

click on **Copy to Web server key store directory**

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

The following message is displayed to indicate the successful copying of these keys. Once again, restart the webserver for the plug-in changes to take effect.

Messages

PLGC0064I: The plug-in keyring file is propagated from C:\IBM\WebSphere\AppServer\profiles\Dmgr01\config\cells\dmCell01\nodes\webserver\servers\webserver1\plugin-key.kdb to c:\IBM\HTTPServer\Plugins\config\webserver1\plugin-key.kdb on the Web server computer.

PLGC0069I: The propagation of the plug-in keyring is complete for the Web server, dmCell01.webserver.webserver1.

4) Adding Certificates to the WebSphere Trust Store

On the WebSphere Administration Console go to **Security > SSL Certificate and Key Management. > Key stores and certificates**

Click **CellDefaultTrustStore**

SSL certificate and key management

[SSL certificate and key management](#) > **Key stores and certificates**

Defines keystore types, including cryptography, RACF(R), CMS, Java(TM), and all truststore types.

Keystore usages

SSL keystores

Preferences

New Delete Change password... Exchange signers...

Select	Name	Description	Management Scope	Path
<input type="checkbox"/>	CMSKeyStore	CMSKeyStore for web server webserver1.	(cell):dmCell01: (node):webserver: (server):webserver1	\${CONFIG_ROOT}/cells/ dmCell01/nodes/ webserver/servers/ webserver1/plugin- key.kdb
<input type="checkbox"/>	CellDefaultKeyStore	Default key store for dmCell01	(cell):dmCell01	\${CONFIG_ROOT}/cells/ dmCell01/key.p12
<input type="checkbox"/>	CellDefaultTrustStore	Default trust store for dmCell01	(cell):dmCell01	\${CONFIG_ROOT}/cells/ dmCell01/trust.p12

From within **CellDefaultTrustStore**, click the **Signer certificates** link from the right hand side

SSL certificate and key management

[SSL certificate and key management](#) > [Key stores and certificates](#) > **CellDefaultTrustStore**

Defines keystore types, including cryptography, RACF(R), CMS, Java(TM), and all truststore types.

General Properties

Name
CellDefaultTrustStore

Description
Default trust store for dmCell01

Management scope
(cell):dmCell01

Path
\${CONFIG_ROOT}/cells/dmCell01/trust.p12

Additional Properties

- [Signer certificates](#)
- [Personal certificates](#)
- [Personal certificate requests](#)
- [Custom properties](#)

To add the webserver's signer to the trust store, click the **Retrieve from Port** button.

SSL certificate and key management

[SSL certificate and key management](#) > [Key stores and certificates](#) > [CellDefaultTrustStore](#) > **Signer certificates**

Manages signer certificates in key stores.

Preferences

Add Delete Extract **Retrieve from port**

Select	Alias	Issued to	Fingerprint (SHA Digest)
--------	-------	-----------	--------------------------

Enter the hostname of the webserver and its SSL port (typically 443) and an Alias

Click the **Retrieve signer information** button, which retrieves the information shown at the bottom of the screenshot.

Click **OK** to add this certificate to the list of signers.

click **Save** to save this change.

SSL certificate and key management

[SSL certificate and key management](#) > [Key stores and certificates](#) > [CellDefaultTrustStore](#) > [Signer certificates](#) > [Retrieve from port](#)

Makes a test connection to a Secure Sockets Layer (SSL) port and retrieves the signer from the server during the handshake.

General Properties

* Host
dm&ihs.spnego.company.com

* Port
443

SSL configuration for outbound connection
CellDefaultSSLSettings

* Alias
webserver_ssl

Retrieve signer information

Retrieved signer information

Serial number
989854342

Issued to
CN=WebSphere Plugin Key, OU=SWG, O=IBM, C=US

Issued by
CN=WebSphere Plugin Key, OU=SWG, O=IBM, C=US

Fingerprint (SHA digest)
4D:6D:53:ED:82:83:4B:D4:58:AB:3F:3D:0A:D7:14:9E:68:68:85:7D

Validity period
Apr 26, 2012

Apply OK Reset Cancel

results in:

SSL certificate and key management

[SSL certificate and key management](#) > [Key stores and certificates](#) > [CellDefaultTrustStore](#) > [Signer certificates](#)

Manages signer certificates in key stores.

Preferences

Add Delete Extract Retrieve from port

Select	Alias	Issued to	Fingerprint (SHA Digest)	Expiration
<input type="checkbox"/>	datapower	OU=Root CA, O="DataPower Technology, Inc.", C=US	A9:BA:A4:B5:BC:26:2F:5D:2A:80:93:CA:BA:F4:31:05:F2:54:14:17	Valid from Jun 11, 2003 to Jun 6, 2023.
<input type="checkbox"/>	root	CN=dslvm171.litbg02.swg.usma.ibm.com, OU=Root Certificate, OU=dslvm171Cell01, OU=dslvm171CellManager01, O=IBM, C=US	00:A6:16:8B:05:ED:7B:68:60:18:19:ED:78:0E:AA:F1:7E:37:55:F9	Valid from Apr 12, 2012 to Apr 9, 2027.
<input type="checkbox"/>	webserver_ssl	CN=dslvm171.litbg02.swg.usma.ibm.com	9D:FC:07:B7:31:5F:41:86:01:09:F5:FD:53:4B:24:50:CB:72:1D:AC	Valid from Jul 11, 2012 to Jul 11, 2013.

Total 3

___5) Update Web addresses used by IBM Connections to access content

Using the wsadmin client, check out the **LotusConnections-config.xml** (aka lcc.xml) to a temporary directory. From this directory, this file must be edited so that all **href** and **ssl_href** values are updated to reflect the hostname of the HTTP Server and do not include any port numbers.

The file **LotusConnections-config.xml** is located in the folder: **LotusConnections-config** i.e.
/opt/IBM/WebSphere/DeploymentManager/profiles/Dmgr01/config/cells/dubxpcvm603Cell01/LotusConnections-config

An example of what needs to be done is as follows

```
<sloc:serviceReference bootstrapHost="connections.example.com" bootstrapPort="2811" clusterName="LotusConnections">
  <sloc:href>
    <sloc:hrefPathPrefix>/activities</sloc:hrefPathPrefix>
    <sloc:static href="http://connections.example.com:9081" ssl_href="https://connections.example.com:9444"/>
    <sloc:interService href="https://connections.example.com:9444"/>
  </sloc:href>
</sloc:serviceReference>
```

For each Connections applications remove the ":"+port_numbers of the two 'href' entries and also the 'ssl_href' entry

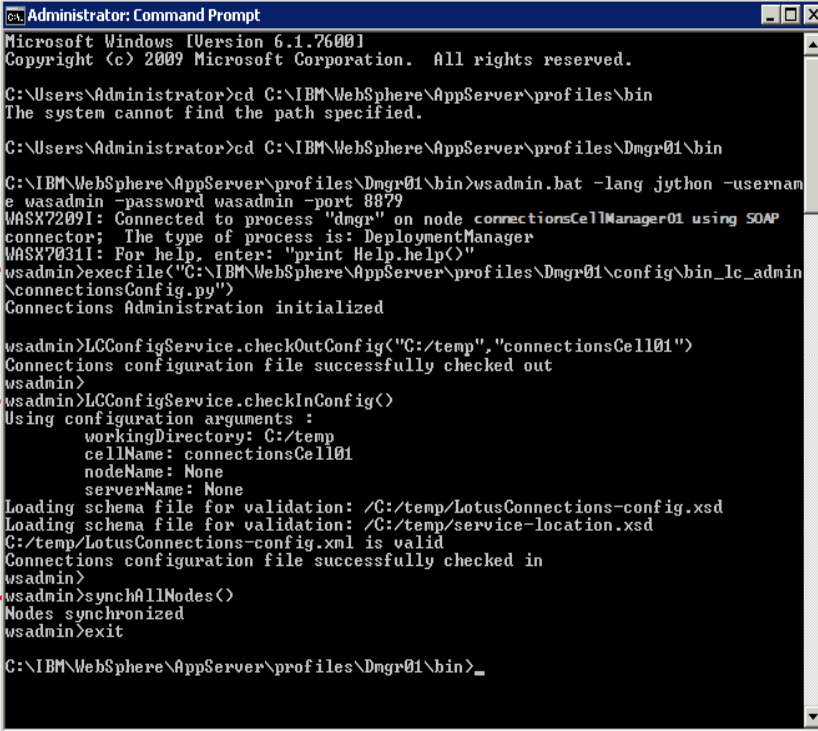
```
<sloc:serviceReference bootstrapHost="connections.example.com" bootstrapPort="2811" clusterName="LotusConnections">
  <sloc:href>
    <sloc:hrefPathPrefix>/activities</sloc:hrefPathPrefix>
    <sloc:static href="http://connections.example.com" ssl_href="https://connections.example.com"/>
    <sloc:interService href="https://connections.example.com"/>
  </sloc:href>
</sloc:serviceReference>
```

Tip: search on "connections.example.com:" and remove the colon (:) and the port number. Once finished you should not be able to find any more occurrences of this string "connections.example.com:" (not the colon at the end of the string; this is most important)

Save the file and check the file back in using the wsadmin client. After the file is checked back in, resynchronize the node so that this change is pushed out.

This completes the webserver, SSL, and certificate configuration for this scenario. Now, when the application is started it can be accessed at <http://connections.example.com/<component>>, where <component> represents any of the Connections applications.

The commands to check-out/ check-in the **lcc.xml** file and sync all nodes are as follows:



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\IBM\WebSphere\AppServer\profiles\bin
The system cannot find the path specified.

C:\Users\Administrator>cd C:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin
C:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin>wsadmin.bat -lang jython -username
e wasadmin -password wasadmin -port 8879
WASX7209I: Connected to process "dmgr" on node connectionsCellManager01 using SOAP
connector; The type of process is: DeploymentManager
WASX7031I: For help, enter: "print Help.help()"
wsadmin>execfile("C:\IBM\WebSphere\AppServer\profiles\Dmgr01\config\bin_lc_admin
\connectionsConfig.py")
Connections Administration initialized

wsadmin>LCConfigService.checkOutConfig("C:/temp","connectionsCell01")
Connections configuration file successfully checked out
wsadmin>
wsadmin>LCConfigService.checkInConfig()
Using configuration arguments :
  workingDirectory: C:/temp
  cellName: connectionsCell01
  nodeName: None
  serverName: None
Loading schema file for validation: /C:/temp/LotusConnections-config.xsd
Loading schema file for validation: /C:/temp/service-location.xsd
C:/temp/LotusConnections-config.xml is valid
Connections configuration file successfully checked in
wsadmin>
wsadmin>syncAllNodes()
Nodes synchronized
wsadmin>exit

C:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin>
```


8.3 Configuring an Administrator User for Homepage

Login to your admin console -> **http://dm&ihs.spnego.company.com:9060/admin** (use wasadmin user and password).

Select **Application -> Application Types -> WebSphere Enterprise Applications** and then select the **Homepage** app.

Select the **Security role to user/group mapping** link...

Select the admin role and then the Map Users... button.

Search for the user, **AdminFromLDAP** in my example, and add them.

Select **OK** then **Save...** the result should be:

Enterprise Applications > Homepage > Security role to user/group mapping

Security role to user/group mapping

Each role that is defined in the application or module must map to a user or group from the domain user registry. accessIds: The accessIds are required only when using cross realm communication in a multi domain scenario. For all other scenarios the accessId will be determined during the application start based on the user or group name. The accessIds represent the user and group information that is used for Java Platform, Enterprise Edition authorization when using the WebSphere default authorization engine. The format for the accessIds is user:realm/uniqueUserID, group:realm/uniqueGroupID. Entering wrong information in these fields will cause authorization to fail. AllAuthenticatedInTrustedRealms: This indicates that any valid user in the trusted realms be given the access. AllAuthenticated: This indicates that any valid user in the current realm be given the access.

Map Users... Map Groups... Map Special Subjects ▾

Select	Role	Special subjects	Mapped users	Mapped groups
<input type="checkbox"/>	person	All Authenticated in Application's Realm		
<input type="checkbox"/>	everyone	Everyone		
<input type="checkbox"/>	reader	Everyone		
<input type="checkbox"/>	metrics-reader	Everyone		
<input type="checkbox"/>	admin	None	AdminFromLDAP	

OK Cancel

Synchronise your changes with the other nodes.

8.4 Enabling Fast Downloads for Files and Wikis

NOTE: Although this is an optional step for customers we do this for all our test systems.

___a) On the Deployment Manager copy the file: **mod_ibm_local_redirect.so** from
/opt/IBM/Connections/plugins/ihs/mod_ibm_local_redirect/linux_x64-ap22/
to the IHS system in to the folder: **/opt/IBM/HTTPServer/modules/**

```
cp /opt/IBM/Connections/plugins/ihs/mod_ibm_local_redirect/linux_x64-ap22/mod_ibm_local_redirect.so  
/opt/IBM/HTTPServer/modules/
```

___b) Edit the **httpd.conf** (/opt/IBM/HTTPServer/conf) and add/edit the following:

```
vi /opt/IBM/HTTPServer/conf/httpd.conf
```

```
LoadModule ibm_local_redirect_module modules/mod_ibm_local_redirect.so // had to add this  
LoadModule env_module modules/mod_env.so // already existed
```

___c) Add the following to the bottom of the **httpd.conf** file... [note: paths will need to change based on installation]

```
Alias /downloadfiles /opt/IC_Share/files/upload/  
Alias /downloadwikis /opt/IC_Share/wikis/upload/  
<Directory /opt/IC_Share/files/upload/>  
Order Deny,Allow  
Deny from all  
Allow from env=REDIRECT_FILES_CONTENT  
</Directory>  
<Directory /opt/IC_Share/wikis/upload/>  
Order Deny,Allow  
Deny from all  
Allow from env=REDIRECT_WIKIS_CONTENT  
</Directory>  
<Location /files>  
IBMLocalRedirect On  
IBMLocalRedirectKeepHeaders X-LConn-Auth,Cache-Control,Content-Type,Content-Disposition,Last-Modified,ETag,Content-  
Language,Set-Cookie  
SetEnv FILES_CONTENT true  
</Location>  
<Location /wikis>  
IBMLocalRedirect On  
IBMLocalRedirectKeepHeadErs X-LConn-Auth,Cache-Control,Content-Type,Content-Disposition,Last-Modified,ETag,Content-  
Language,Set-Cookie  
SetEnv WIKIS_CONTENT true  
</Location>
```

___d) On the Deployment Manager edit the **files-config.xml** and **wikis-config.xml** files that can be found in the
folder: **/opt/IBM/WebSphere/AppServer/profiles/Dmgr01/config/cells/dslvm171Cell01/LotusConnections-config/** and
make the following changes:

files-config: search for "<download>" and set the values of the properties to those shown in blue

```
<download>  
  <modIBMLocalRedirect enabled="true"  
    hrefPathPrefix="/downloadfiles" />  
  <stats>  
    <logging enabled="true" />  
  </stats>  
</download>
```

wikis-config.xml: search for "<download>" and set the values of the properties to those shown in blue

```
<download>  
  <modIBMLocalRedirect enabled="true"  
    hrefPathPrefix="/downloadwikis" />  
  <stats>  
    <logging enabled="false" />  
  </stats>  
</download>
```

___e) **Synchronize and Restart IBM Connections as follows:**

- Do a Full Synchronize on all Nodes
- Stop all Connection's clusters
- Stop and reStart the Deployment manager
- Stop and Restart the HTTP server

Start all Connections Clusters

8.5 Configure Notifications

Machine Hostname	Applications	Version#	OS
dm&ihs.spnego.company.com	WAS Deployment Manager IBM HTTP Server (IHS)	WAS v8.0.0.5 IHS v8.0.0.5	RedHat 6 (64)
domino.company.com	Domino Mail-in server	Domino 8.5.3	Win2008 R2 E

You can configure Notifications by following these steps:

1. In the Domino Mailin server, create a special [ReplyTo](#) user
2. (In Domino) Configure the ReplyTo user for Notifications
3. (In Domino) Configuring Domino for email notification replies
4. (In Connections DM) Configuring WAS DM for email notification replies
5. (In Connections) Configure **news-config.xml** for notification replies
6. (in Connections) Sync and restart Connections

___1. Create a special [ReplyTo](#) user and configure

Open the Domino Admin client, and connect to Domino mail server
 Select **People & Group** view, click **People** tab on the right panel.
 Click **Register**, input the certifier's password for the Domino server.
 Check the **Advanced** box and create a **ReplyTo** user as follows:

Register Person -- ReplyTo

Provide name, password and other basic information for the new person. To view/edit additional registration settings, check the 'Advanced' checkbox below.

Registration Server...

First name: Middle name: Last name: Short name:

Password: Mail system: Explicit policy:

☐ Enable roaming for this person

☒ Create a Notes ID for this person

☒ Advanced

Registration Queue (local):

^	User Name ^	Registration Status ^	Date ^
8	ReplyTo	Ready for registration	07/17/2012

- The **Internet Domain** value could be set to the real domain you use:

Register Person -- ReplyTo

Mail Internet Address Information

Internet address: ReplyTo@us.ibm.com Internet Domain: us.ibm.com

Address name format: FirstName LastName Separator: None

Supply internet address format settings for the selected people or person. The Internet address is created using the person's name, the internet domain and internet address format components. It must be unique in the address book.

☒ Advanced New Person Migrate People... Import Text File...

Registration Queue (local):

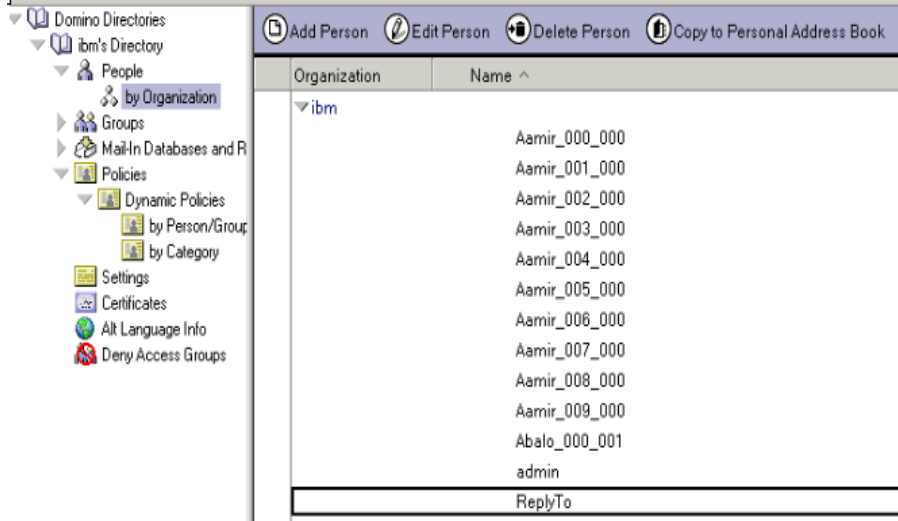
^	User Name ^	Registration Status ^	Date ^
8	ReplyTo	Ready for registration	07/17/2012

Register All Register Delete Options... Views... Done

Click **Register** to complete the registration.

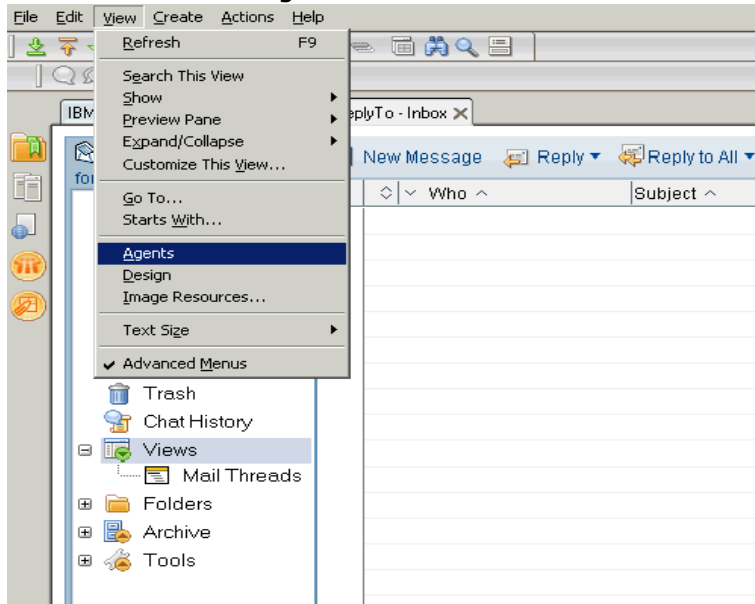
2. Now, configure the ReplyTo user For Notifications

Go back to **People & Groups** tab, expand **People byOrganization**.
Edit the account of the user used to direct reply mail (the **ReplyTo** user)

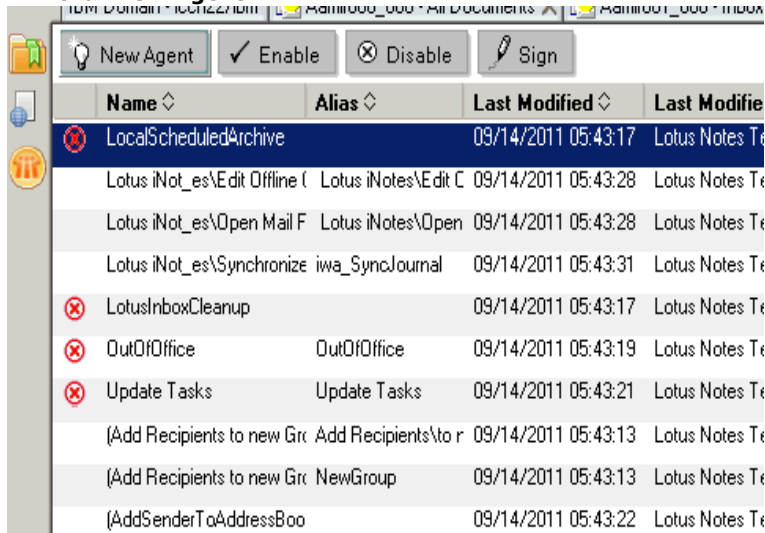


Click Open Mail File for the **ReplyTo** user.

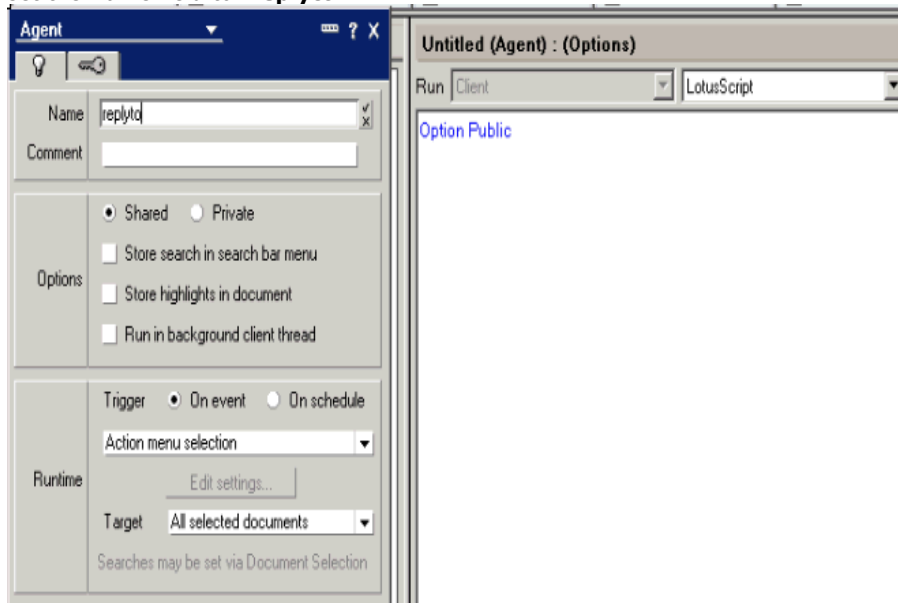
Select the **View > Agents** menu item.



Click **New Agent**.



set the Name field to **"replyto"**



Add the following Lotusscript code to the agent:

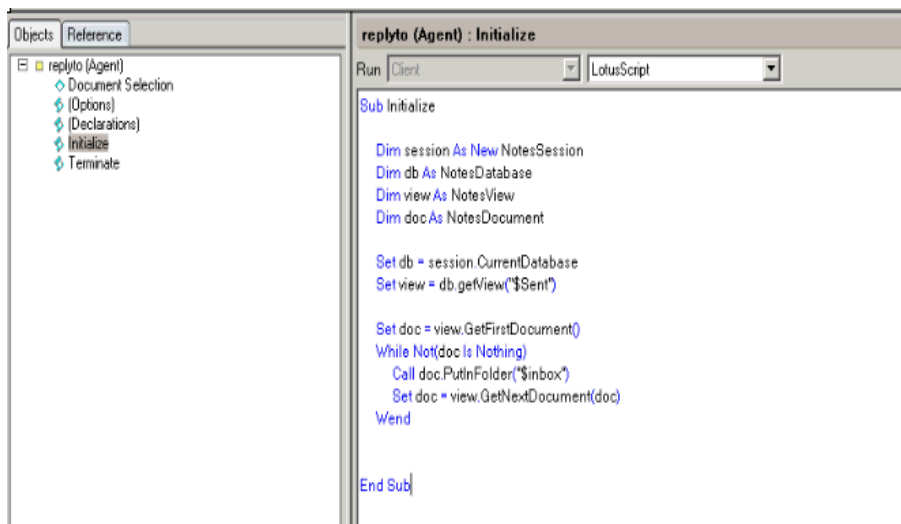
Sub Initialize

```
Dim session As New NotesSession
Dim db As NotesDatabase
Dim view As NotesView
Dim doc As NotesDocument

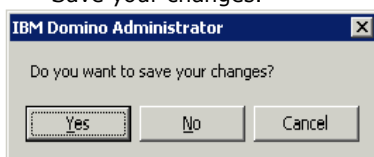
Set db = session.CurrentDatabase
Set view = db.getView("$Sent")

Set doc = view.GetFirstDocument()
While Not(doc Is Nothing)
    Call doc.PutInFolder("$inbox")
    Set doc = view.GetNextDocument(doc)
Wend
```

End Sub



Save your changes.



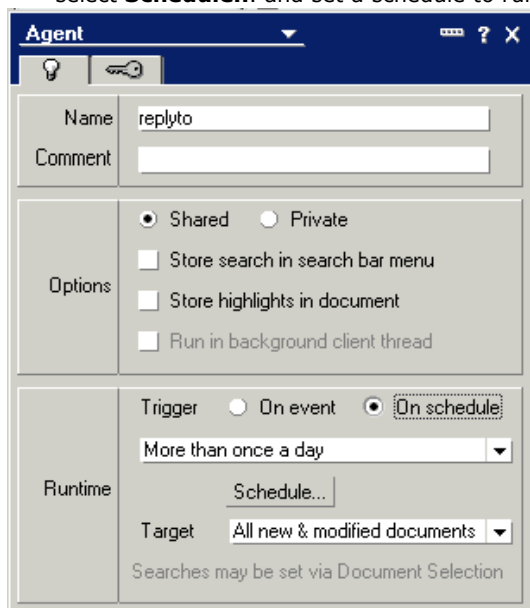
Open the agent again to set the following properties:

in the **Options** section select **Shared**.

in the **Runtime** section select **On schedule**, and then select **More than once a day**.

in the **Target** field select **All new & modified documents**.

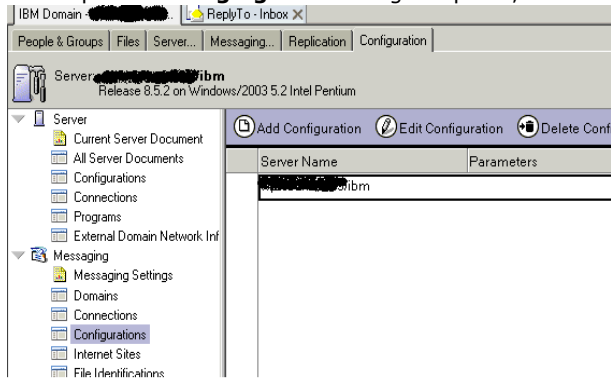
select **Schedule...** and set a schedule to run every 5 minutes, all day.



3. Configuring Domino for email notification replies

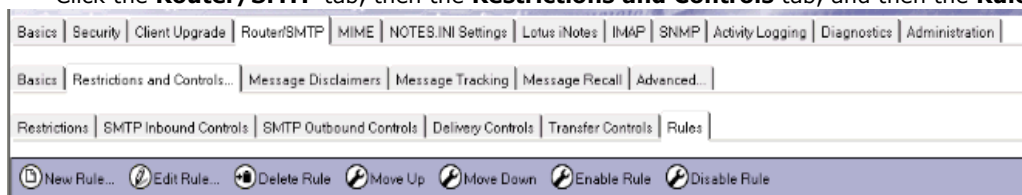
Open Domino Admin client and click on configuration tab.

Expand **Messaging** in the navigator panel, and then click **Configuration**.

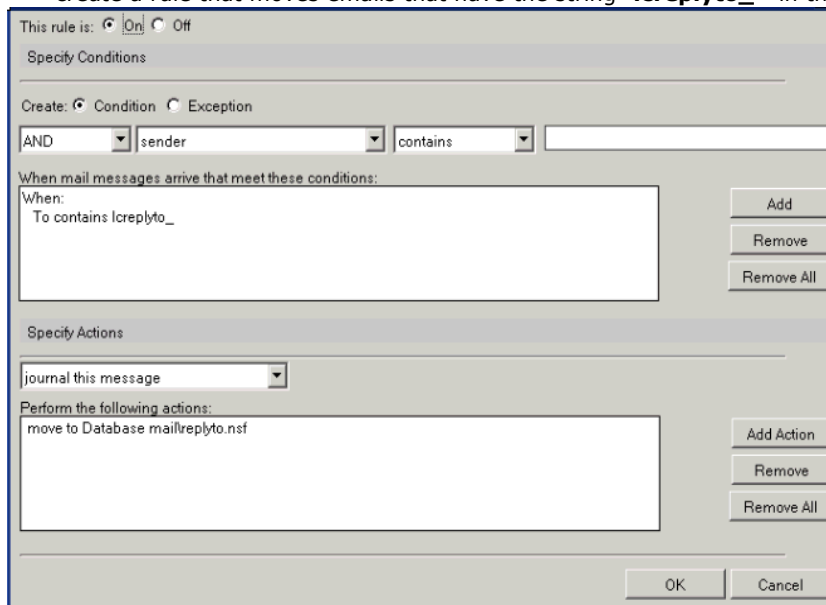


Select the messaging server record and click **Edit Configuration**.

Click the **Router/SMTP** tab, then the **Restrictions and Controls** tab, and then the **Rules** tab...then click **New Rule...**



create a rule that moves emails that have the string "**lcreplyto_**" in the To field to the mailbox as follows



- Save and Close.
- Stop and Restart the Domino server

4. In Connections DM, configuring Notifications

4.1 Create and configure the mail session: "lcnotifications"

login to the WAS Console: <https://dm&ihs.spnego.company.com:9043/ibm/console>

select **Resources > Mail > Mail Sessions**

Mail Sessions

Use this page to create mail sessions, which are collections of properties that define how your application sends mail and accesses the mail store. To create a useful mail session, an outgoing or incoming server and protocol must be provided. Configure mail sessions only after you configure the necessary protocol providers.

Scope: Cell=dubxpcvm603Cell01

☒ Show scope selection drop-down list with the all scopes option

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, [see the scope settings help](#).

Cell=dubxpcvm603Cell01

Preferences

New... Delete

☒ ☐ ☐ ☐

Select	Name	JNDI name	Scope	Provider	Description	Category
None						
Total 0						

Select **Scope = Cell=XXXXCell01**, then select **New...**

Mail Sessions

Use this page to create mail sessions, which are collections of properties that define how your application sends mail and accesses the mail store. To create a useful mail session, an outgoing or incoming server and protocol must be provided. Configure mail sessions only after you configure the necessary protocol providers.

Scope: Cell=dubxpcvm603Cell01

☒ Show scope selection drop-down list with the all scopes option

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, [see the scope settings help](#).

Cell=dubxpcvm603Cell01

Preferences

New... Delete

☒ ☐ ☐ ☐

Select	Name	JNDI name	Scope	Provider	Description	Category
None						
Total 0						

Enter the following information... then **OK**, then **Save**

Messages

Additional Properties for this object will not be available to edit until its general properties are applied by clicking on either Apply or OK.

Mail Sessions > New...

Use this page to create mail sessions, which are collections of properties that define how your application sends mail and accesses the mail store. To create a useful mail session, an outgoing or incoming server and protocol must be provided. Configure mail sessions only after you configure the necessary protocol providers.

Configuration

General Properties

Scope

cells:dubxpcvm603Cell01

Provider

Built-in Mail Provider

Create New Provider

* Name

notification

* JNDI name

mail/notification

Description

The additional properties will not be available until the general properties for this item are applied or saved.

Additional Properties

Custom properties

Category

Enable debug mode

Enable strict Internet address parsing

Outgoing Mail Properties

Server

domino.company.com

* Protocol

smtp

User

Password

Verify Password

Return e-mail address

Incoming Mail Properties

Server

* Protocol

imap

User

Password

Verify Password

Apply OK Reset Cancel

select [Mail Sessions](#) > [Innotification](#) > **Custom properties**
create/verify the following settings:

Mail Sessions

[Mail Sessions](#) > [Innotification](#) > Custom properties

Use this page to specify custom properties that your enterprise information system (EIS) requires for the resource providers and resource factories that you configure. For example, most database vendors require additional custom properties for data sources that access the database.

Preferences

NewDelete

Select

Name

Value

Description

Required

You can administer the following resources:

<input type="checkbox"/>	mail.smtp.connectiontimeout	12000		false
<input type="checkbox"/>	mail.smtp.timeout	12000		false
<input type="checkbox"/>	mail.smtp.port	25		false
<input type="checkbox"/>	mail.smtp.auth	false		false

Total 4

4.2 Create and configuring the Mail Session: "Icreplyto"

select **Resources > Mail > Mail Sessions**

Mail Sessions

Use this page to create mail sessions, which are collections of properties that define how your application sends mail and accesses the mail store. To create a useful mail session, an outgoing or incoming server and protocol must be provided. Configure mail sessions only after you configure the necessary protocol providers.

Scope: Cell=dubxpcvm603Cell01





☒ Show scope selection drop-down list with the all scopes option

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, [see the scope settings help](#).

Cell=dubxpcvm603Cell01

Preferences

New... Delete

Select	Name	JNDI name	Scope	Provider	Description	Category
None						
Total 0						

Select **Scope = Cell=XXXXCell01**, then select **New...**

Mail Sessions

Use this page to create mail sessions, which are collections of properties that define how your application sends mail and accesses the mail store. To create a useful mail session, an outgoing or incoming server and protocol must be provided. Configure mail sessions only after you configure the necessary protocol providers.

Scope: Cell=dubxpcvm603Cell01





☒ Show scope selection drop-down list with the all scopes option

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, [see the scope settings help](#).

Cell=dubxpcvm603Cell01

Preferences

New... Delete

Select	Name	JNDI name	Scope	Provider	Description	Category
You can administer the following resources:						
<input type="checkbox"/>	Inotification	mail/notification	Cell=dubxpcvm603Cell01	Built-in Mail Provider		
Total 1						

Enter the following information... then **OK**, then **Save**

Mail Sessions

Messages

Additional Properties for this object will not be available to edit until its general properties are applied by clicking on either Apply or OK.

Mail Sessions > New...

Use this page to create mail sessions, which are collections of properties that define how your application sends mail and accesses the mail store. To create a useful mail session, an outgoing or incoming server and protocol must be provided. Configure mail sessions only after you configure the necessary protocol providers.

Configuration

General Properties

Scope

cells:idxpcvm603Cell01

Provider

Built-in Mail Provider

Create New Provider

Name

lcreplyto

JNDI name

mail/replyto

Description

Category

The additional properties will not be available until the general properties for this item are applied or saved.

Additional Properties

Custom properties

Enable debug mode

Enable strict Internet address parsing

Outgoing Mail Properties

Server

Protocol

smtp

User

Password

Verify Password

Return e-mail address

Incoming Mail Properties

Server

domino.compnay.com

Protocol

imap

User

ReplyTo

Password

Verify Password

Apply

OK

Reset

Cancel

© Copyright IBM Corp. 2013

126

the end result is:

Mail Sessions

Mail Sessions

Use this page to create mail sessions, which are collections of properties that define how your application sends mail and accesses the mail store. To create a useful mail session, an outgoing or incoming server and protocol must be provided. Configure mail sessions only after you configure the necessary protocol providers.

Scope: Cell=dubxpcvm603Cell01

☒ Show scope selection drop-down list with the all scopes option

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, [see the scope settings help](#).

Cell=dubxpcvm603Cell01

Preferences

New...Delete

Select	Name	JNDI name	Scope	Provider	Description	Category
You can administer the following resources:						
<input type="checkbox"/>	lcnofication	mail/notification	Cell=dubxpcvm603Cell01	Built-in Mail Provider		
<input type="checkbox"/>	lcreplyto	mail/replyto	Cell=dubxpcvm603Cell01	Built-in Mail Provider		
Total 2						

___5. Configure news-config.xml for email notifications

Using **wpadmin** checkout the file **news-config.xml**; open the file and search for the section "**mailin**" and make the following changes in blue:

```
<mailin enabled="true">
  <replyto enabled="true">

    <!-- A special ReplyTo address is added to notifications where
           the user can reply to the notification to respond/comment.
           The domain may be a dedicated domain for connections bound
           mails. Or it could be existing domain, in which case a prefix
           of suffix should be provided also. -->

    <replytoAddressFormat>
      <domain>company.com</domain>
      <!-- A prefix OR suffix (not both) may also be provided.
           This is necessary if an existing domain (with other
           email addresses) is being used.
           There is a 28 character limit for the affix. -->

      <!--
      <affix type="suffix">_lcreplyto</affix>
      <affix type="prefix">lcreplyto_</affix>
      -->
      <affix type="prefix">lcreplyto_</affix> // add this
    </replytoAddressFormat>
  </replyto>
</mailin>
```

Save the file and check it back-in

___6. Sync and Restart Connections

- a) from the WAS console
 - Sync all Nodes
 - Stop all Connections Clusters
- b) Stop and Restart the Deployment Manager
- c) from the WAS console Start all Connections Clusters