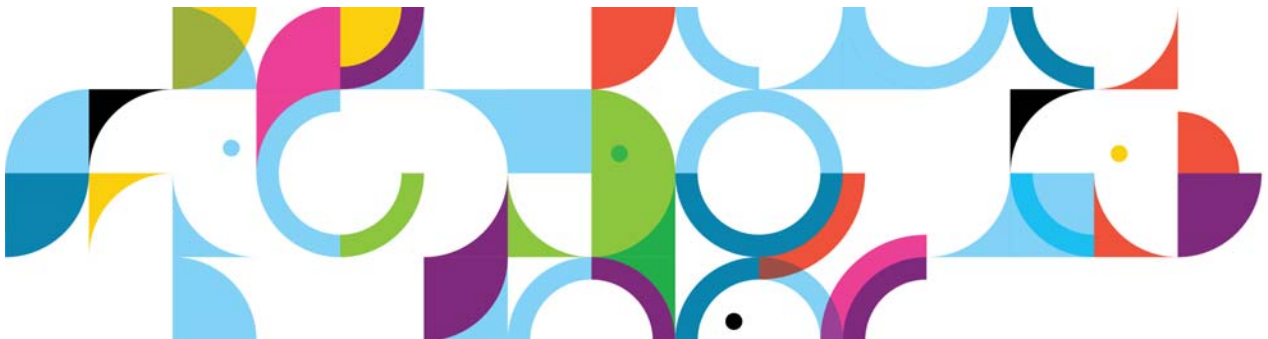




*IBM Connections 4 Public
Deployment Scenarios*

Deployment Scenarios

ERC 1.0



Trademarks

IBM® and the IBM logo are registered trademarks of International Business Machines Corporation. The following are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide:

AIX®	Cognos®	DB™
DB2 Universal Database™	DB2®	Domino®
Lotus®	LotusScript®	Notes®
Power®	Quickr®	Rational®
Sametime®	System z®	Tivoli®
WebSphere®	400®	

Intel and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Microsoft, Windows and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

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

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

January 2013 edition

The information contained in this document has not been submitted to any formal IBM test and is distributed on an “as is” basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer’s ability to evaluate and integrate them into the customer’s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will result elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

© Copyright International Business Machines Corporation 2013.

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

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

IBM Connections 4: PDS Red Hat upgrade for DB2

About the author

Srinivas Allampally is a software engineer for IBM Collaboration Solutions.

Abstract

The objective of this document is to detail the experiences of the IBM System Verification Test (SVT) team Upgrading Connections 4.0 in-place upgrade with SPNEGO. The goal of testing was to ensure that data that was migrated from IBM Connection 3.0.1.x to Connections 4.0 performed as expected when integrated with SPNEGO.

Overview

The components that are required to install and configure in this scenario are Lotus Connections 3.0.x Medium deployment, SPNEGO Domain. All Domains are configured to share LDAP and SPNEGO Domain, and SSO is implemented with a common LTPA token. The operating system used this environment is RHEL 6.2 on a VM.

The environment includes the following assumptions to migrate for the in-place upgrade:

Lotus Connections 3.0.x Medium Cluster deployment

LDAP server: Microsoft Active Directory 2008

Domain: SPNEGO

Database: DB2 9.7

In-place upgrade

The in-place upgrade can be installing a new Deployment Manager, Appserver1, Appserver2, on the Same hardware, but to use the same database to upgrade from Lotus Connections 3.0.x to Connections 4.0.



Reminder

1. Lotus Connections 3.0.x should be up and running when installing WebSphere Application Server, Appserver on nodes on the same hardware to overcome the port conflicts.
2. Double-check Capital K in LCC.xml for custom authenticator, that is, KerberosAuthentication (because Connections 4.0 uses Default Authenticator, and use of small letter k does not migrate properly).

Contents

1. OS tuning on DB2
2. Upgrade existing 3.0.x databases with Connections 4.0 wizard
3. Export applications from Lotus Connections 3.0.1.x: Ensure that Lotus Connections 3.0.1.x is up and running
4. Install WebSphere Application Server, Application Server1, Application Server2, HTTP Server on the same computers as for 3.0.1.x
5. Create shared content directory/content store
6. Reuse content store/copy content store from 3.0.x shared data to IBM Connections 4.0 shared data
7. Backing up IBM Connections before installing Connections 4.0
8. Uninstalling a deployment before migration
9. Install IBM Connections 4.0
10. Import applications that are exported from Lotus Connections 3.0.x
11. Post-installation steps
12. Take a full backup

Infrastructure diagram

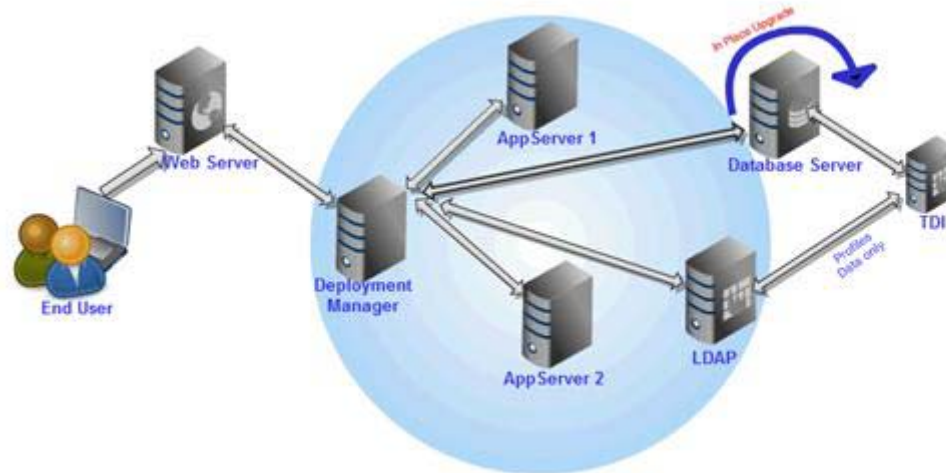


Figure 1. Infrastructure diagram

Migration scenario

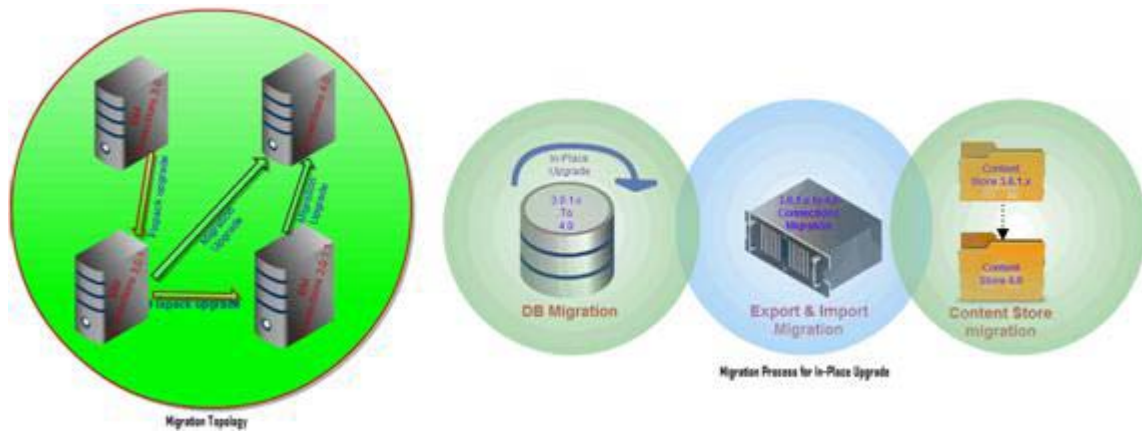


Figure 2. Migration scenario

Specification

Computer	Operating system	Software	Specs
Active Directory	Windows Enterprise 2008 server	Microsoft Active Directory	
Database Server	RedHat Enterprise Linux 6.2	IBM DB2 9.7 fix pack 6	
SPNEGO	RedHat Enterprise Linux 6.2	SPNEGO Domain	
Connection Server	RedHat Enterprise Linux 6.2	WebSphere Application Server 7.0	
DM+Appserver1+Appserver2+HttpServer		Fix pack 21 Connections 4.0 IBM HTTP Server V7.0 fix pack 21	

Assumptions

Prior doing migration Lotus Connections 3.0.1.x is configured up and running with a SPNEGO domain.

Migration process



Note

It is highly recommended to take backups where necessary before attempting any of the following steps.

1. OS tuning on DB2

- ___ 1. Find DB2 release as DB2 instance owner (following is DB2 9.7 fp6).

```
$ db2level
DB21085I  Instance db2inst1 uses 64 bits and DB2 code release SQL09076 with
level identifier 08070107.
Informational tokens are DB2 v9.7.0.6, s120516, IP23328, and Fix Pack 6.
Product is installed at /opt/ibm/db2/V9.7.
```

- ___ 2. Get cpu info (for performance comparison).

```
cat /proc/cpuinfo
...
model name: Intel(R) Xeon(R) CPU X7560 @ 2.27GHz
```

- ___ 3. Get the OS release.

```
$ cat /etc/redhat-release
Red Hat Enterprise Linux Server release 6.2 (Santiago)
```

- ___ 4. Get amount of physical memory installed (following is 8 G).

```
# free
```

	total	used	free	shared	buffers	cached
Mem:	8062104	7255640	806464	0	325372	5831620
-/+ buffers/cache:		1098648	6963456			
Swap:	8388600	336	8388264			

- ___ 5. Check DB2 suggested kernel settings.



Information

For more information about how to check DB2 suggested kernel setting, see <http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/index.jsp?topic=%2Fcom.ibm.db2.luw.q.b.server.doc%2Fdoc%2Fc0057140.html>.

```
# sysctl -a | grep aio
fs.aio-nr = 0
fs.aio-max-nr = 65536 ( Wrong, use 1048576 )

# sysctl -a | grep swappiness
vm.swappiness = 60 ( Wrong, use 0 )

# sysctl -a | grep randomize
kernel.randomize_va_space = 2 ( Wrong, use 0 )

# sysctl -a | grep overcommit
vm.overcommit_memory = 0 (OK )
vm.overcommit_ratio = 50
vm.nr_overcommit_hugepages = 0

# sysctl -a | grep file
fs.file-nr = 7840 0 793843
fs.file-max = 793843 ( OK )

# sysctl -a | grep file
fs.file-nr = 4864 0 793812
fs.file-max = 793812
```

___ 6. Check requirements for the OS and version of DB2.



Information

For more information about how to check requirements for the OS and version of DB2, see <https://www.ibm.com/developerworks/wikis/display/im/Red+Hat+Enterprise+Linux+%28RHEL%29+6+-+DB2+9.7>.

___ 7. For DB2 9.7 on RHEL 6, base kernel level is 2.6.32 (following is OK).

```
$ uname -r
2.6.32-220.23.1.el6.x86_64
```


___ 8. Check required libraries (libstdc++.so.6 is present).

```
# find / -name libstdc++.so.6 -print
/usr/lib64/libstdc++.so.6
/usr/lib/libstdc++.so.6
/usr/lib/vmware-tools/lib64/libstdc++.so.6
/usr/lib/vmware-tools/lib64/libstdc++.so.6/libstdc++.so.6
/usr/lib/vmware-tools/lib32/libstdc++.so.6
/usr/lib/vmware-tools/lib32/libstdc++.so.6/libstdc++.so.6
/root/vmware-tools-distrib/lib/lib64/libstdc++.so.6
/root/vmware-tools-distrib/lib/lib64/libstdc++.so.6/libstdc++.so.6
/root/vmware-tools-distrib/lib/lib32/libstdc++.so.6
/root/vmware-tools-distrib/lib/lib32/libstdc++.so.6/libstdc++.so.6
```

___ 9. Technote is applied to fix autostart? NO.



Information

For RHEL 6, see this technote: "21497220 Autostart of DB2 instance on restart does not work on RHEL6 systems" in <http://www-01.ibm.com/support/docview.wss?uid=swg21497220>.

To apply the previous autostart technote:

```
vi /etc/init/fmcd.conf
add the contents below...
```

```
# ---- select from line below
# DB2 fault monitor
#
# Starts fmcd
```

```
description "Fault Monitor is the DB2 database facility that monitors DB2
database manager instances, and restarting any instance that exits
prematurely."
version "9.7.0.6"
```

```
start on runlevel [2345]
stop on runlevel [016]
```

```
console output
respawn
respawn limit 10 120
```

```
exec /opt/ibm/db2/V9.7/bin/db2fmcd
# ---- stop selecting at line above
```

___ 10. Check kernel settings that relate to shared memory.

```
kernel.shmmax = 8255594496    ( 7.68G OK )
kernel.shmall = 4031052 ( 15.7G... wrong )  should be 2015526 to match above
kernel.shmmni = 4096
kernel.msgmax = 65536
kernel.msgmni = 15738
kernel.msgmnb = 65536
kernel.sem = 250 256000 32 2048
kernel.auto_msgmni = 1
```

```
kernel.shmmax = 8255483904
kernel.shmall = 4030998
kernel.shmmni = 4096
kernel.shm_rmid_forced = 0
kernel.msgmax = 65536
kernel.msgmni = 15738
kernel.msgmnb = 65536
kernel.sem = 250 256000 32 2048
kernel.auto_msgmni = 1
```



Note

DONE on Database.

To correct previously referenced kernel settings:

```
vi sysctl.conf
```

At the bottom of the file, add these lines, and then comment out any previous lines that refer to these kernel settings with #:

```
#DB2 tuning for linux and 8Gb memory
fs.aio-max-nr = 1048576
vm.swappiness = 0
kernel.randomize_va_space = 0
kernel.shmall = 2015526
kernel.sem = 250 256000 32 2048
```

___ 11. Check OS user limits as root.



Information

For more information about how to check OS user limits as root, see

<http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/index.jsp?topic=%2Fcom.ibm.db2.luw.qb.server.doc%2Fdoc%2Fr0052441.html>.

```
# ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited ( OK )
scheduling priority     (-e) 0
file size               (blocks, -f) unlimited ( OK )
pending signals         (-i) 62835
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files              (-n) 1024 ( wrong, for 64-bit Linux must be
65536, and then fs.file-max must be greater than 65536, from above it is )
pipe size               (512 bytes, -p) 8
POSIX message queues    (bytes, -q) 819200
real-time priority      (-r) 0
stack size              (kbytes, -s) 10240
cpu time                (seconds, -t) unlimited
max user processes      (-u) 1024
virtual memory          (kbytes, -v) unlimited
file locks              (-x) unlimited
```

___ 12. Check OS user limits as the DB2 instance owner (in this case dbinst1).



Information

For more information about how to check IS user limits as the DB2 instance owner, see <http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/index.jsp?topic=%2Fcom.ibm.db2.luw.qb.server.doc%2Fdoc%2Fr0052441.html>.

```
# ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited ( OK )
scheduling priority     (-e) 0
file size               (blocks, -f) unlimited ( OK )
pending signals         (-i) 62835
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files              (-n) 1024 ( wrong, for 64-bit Linux must be
65536, and then fs.file-max must be greater than 65536, from above it is )
pipe size               (512 bytes, -p) 8
POSIX message queues    (bytes, -q) 819200
real-time priority      (-r) 0
stack size              (kbytes, -s) 10240
cpu time                (seconds, -t) unlimited
max user processes      (-u) 1024
virtual memory          (kbytes, -v) unlimited
file locks              (-x) unlimited
```

```
ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority     (-e) 0
file size               (blocks, -f) unlimited
pending signals         (-i) 62833
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files              (-n) 65536
pipe size               (512 bytes, -p) 8
POSIX message queues    (bytes, -q) 819200
real-time priority      (-r) 0
stack size              (kbytes, -s) 10240
cpu time                (seconds, -t) unlimited
max user processes      (-u) 1024
virtual memory          (kbytes, -v) unlimited
file locks              (-x) unlimited
```

___ 13. To fix the OS user limits on RHEL:

- ___ a. In `/etc/security/limits.conf`, add the following to cover root and the DB2 instance owner:

```
root hard nofile 65536
root soft nofile 65536
* hard nofile 65536
* soft nofile 65536
```

- ___ b. Add this line to the bottom of `/etc/pam.d/login`:

```
session required pam_limits.so
db2set
db2set DB2CODEPAGE=1208
```

2. Upgrade existing 3.0.x databases with Connections 4.0 wizard

- ___ 1. Copy Connections 4.0 build wizard to the DB2 computer, and change permission 755 and owner to db2inst1. Run the wizard as instance owner.
- ___ 2. Start the db wizard from the wizard folder.



Figure 3. Database wizard for IBM Connections 4.0: Welcome

- ___ 3. Choose **Update operation only for IBM Connections databases 3.0.1.x to 4.0.**



Figure 4. Database wizard for IBM Connections 4.0: Database task selection

- ___ 4. Choose DB2 as database type.

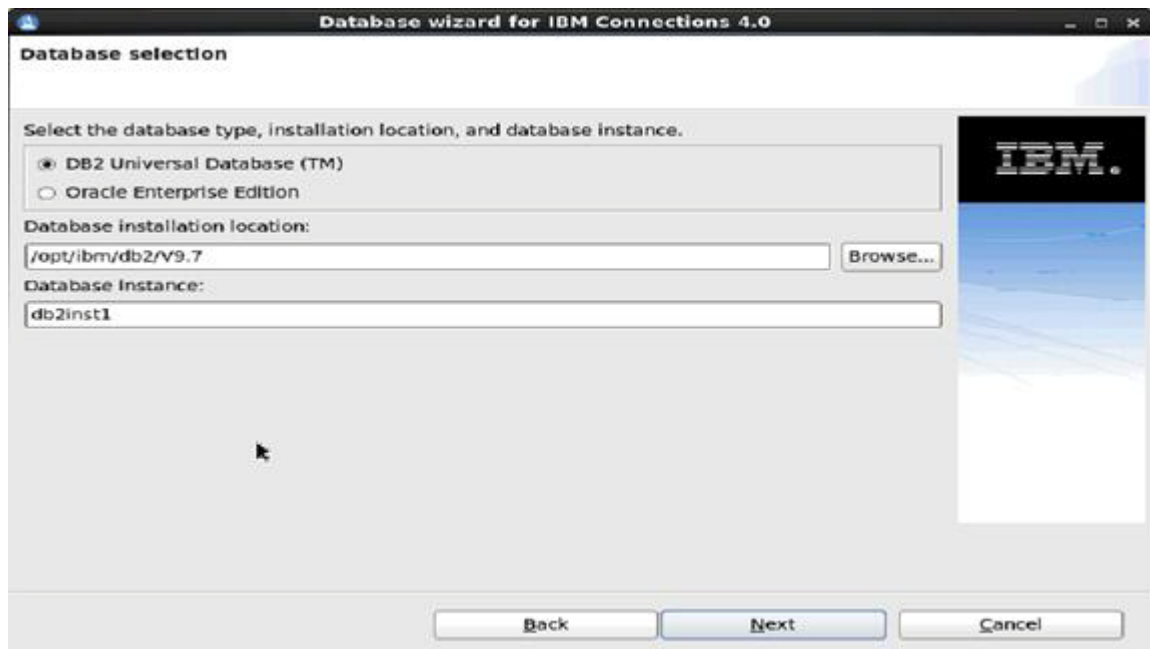


Figure 5. Database wizard for IBM Connections 4.0: Database selection

___ 5. Select all applications for Application Selection.

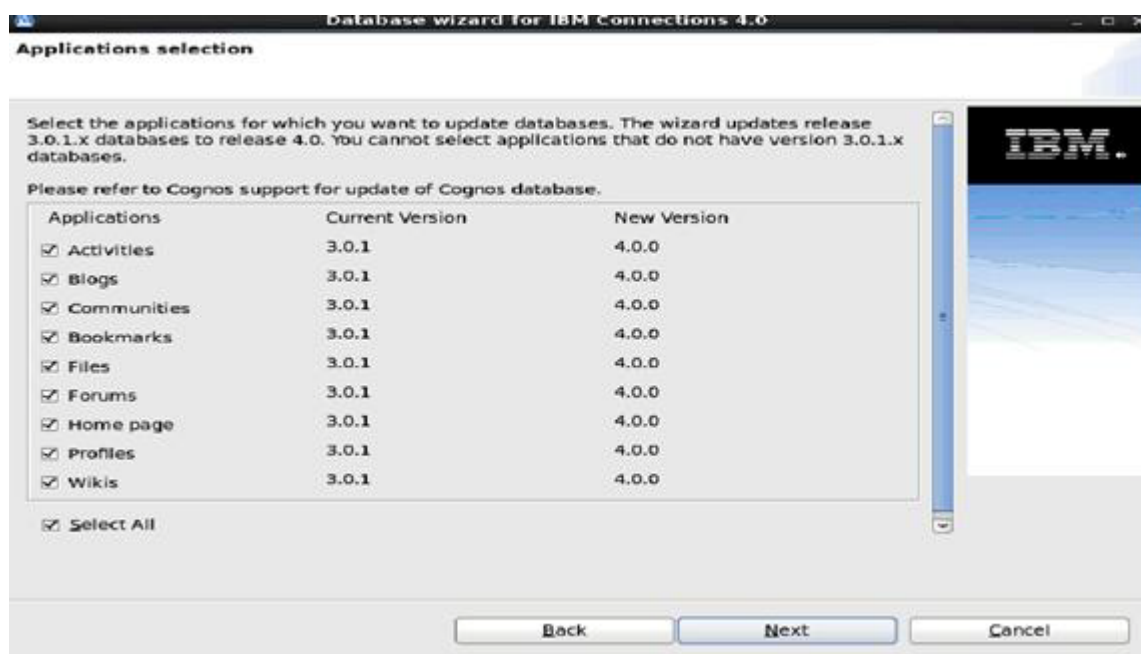


Figure 6. Database wizard for IBM Connections 4.0: Application selection

___ 6. Type **30** from the pop-up storyLifetimeInDays.

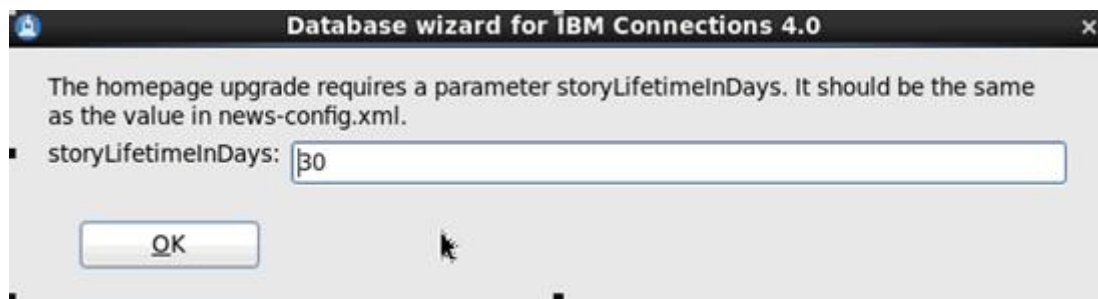
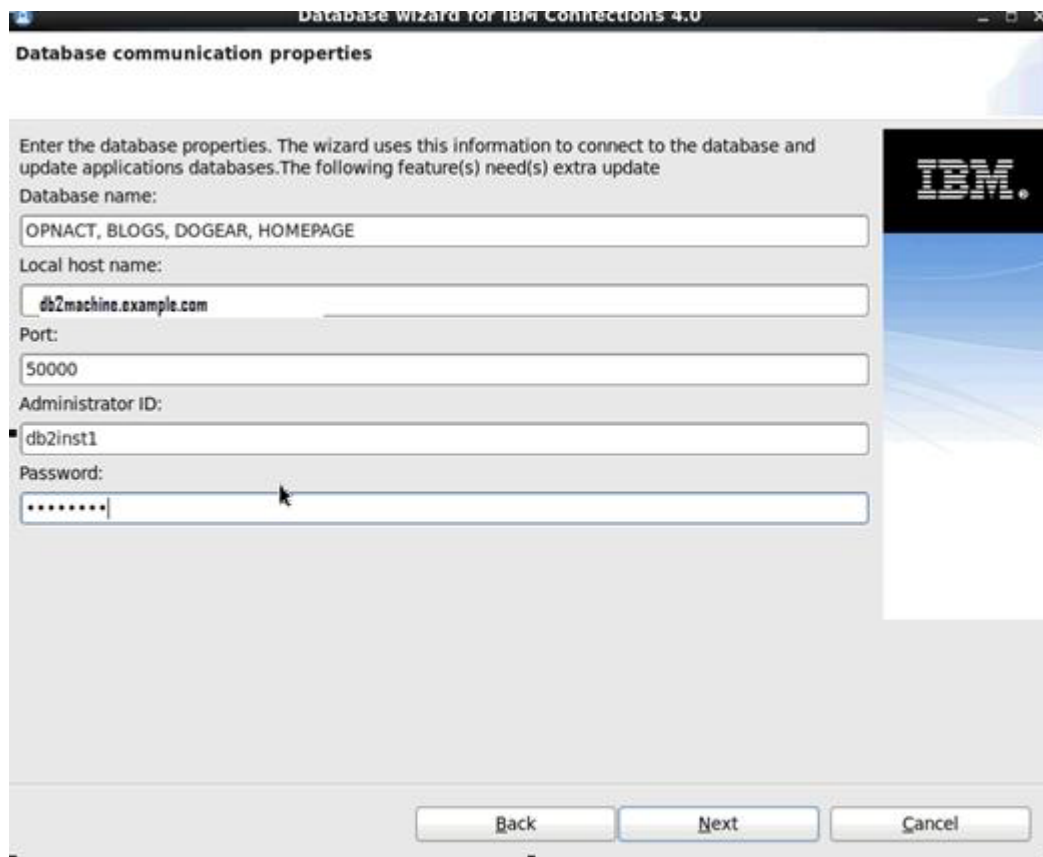


Figure 7. Database wizard for IBM Connections 4.0: Life time in Days

___ 7. Enter the database communication properties.



The screenshot shows a window titled "Database Wizard for IBM Connections 4.0" with a sub-header "Database communication properties". The main text reads: "Enter the database properties. The wizard uses this information to connect to the database and update applications databases. The following feature(s) need(s) extra update". Below this, there are several input fields: "Database name:" with the value "OPNACT, BLOGS, DOGEAR, HOMEPAGE"; "Local host name:" with the value "db2machine.example.com"; "Port:" with the value "50000"; "Administrator ID:" with the value "db2inst1"; and "Password:" with a masked field of seven asterisks. At the bottom right, there is an IBM logo. At the bottom of the window, there are three buttons: "Back", "Next", and "Cancel".

Figure 8. Database wizard for IBM Connections 4.0: Database communication properties

___ 8. Enter the values for profiles database connection.

The screenshot shows a window titled "Database wizard for IBM Connections 4.0" with a sub-header "Profiles database connection". The main text reads: "Enter the Profiles database properties. The wizard uses this information to transfer data from Profiles database to HomePage database." Below this are five input fields: "Database name:" with the value "PEOPLED8", "Database host name:" with the value "db2machine.example.com", "Port:" with the value "50000", "Administrator ID:" with the value "ib2inst1", and "Password:" with masked characters "*****". To the right of the input fields is a vertical bar with the IBM logo. At the bottom of the window are three buttons: "Back", "Next", and "Cancel".

Figure 9. Database wizard for IBM Connections 4.0: Profiles database connection

- ___ 9. Check the pre-configuration task summary and click **Update**.

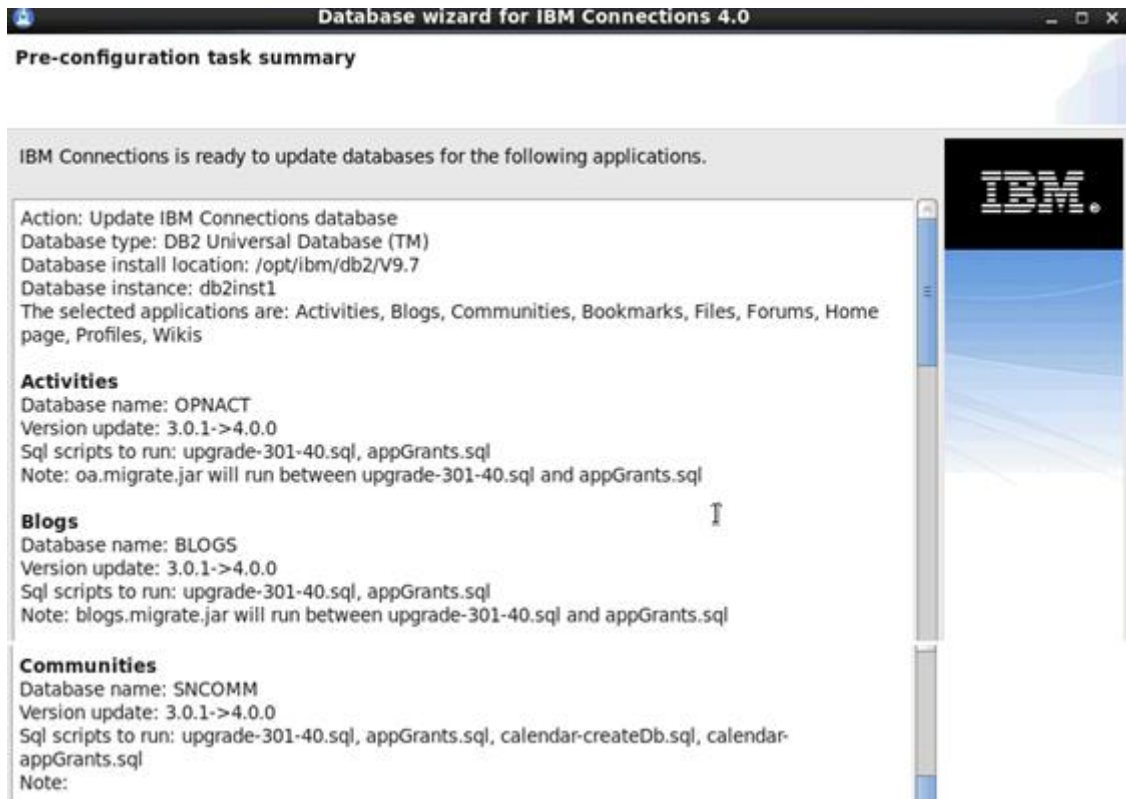


Figure 10. Database wizard for IBM Connections 4.0: Pre-configuration task summary (1 of 3)

Bookmarks
 Database name: DOGEAR
 Version update: 3.0.1->4.0.0
 Sql scripts to run: upgrade-301-40.sql, appGrants.sql
 Note: dogear.migrate.jar will run between upgrade-301-40.sql and appGrants.sql

Files
 Database name: FILES
 Version update: 3.0.1->4.0.0
 Sql scripts to run: upgrade-301-40.sql, appGrants.sql
 Note:

Forums
 Database name: FORUM
 Version update: 3.0.1->4.0.0
 Sql scripts to run: upgrade-301-40.sql, appGrants.sql
 Note:

Home page
 Database name: HOMEPAGE
 Version update: 3.0.1->4.0.0
 Sql scripts to run: upgrade-301-40.sql, appGrants.sql, post-java-migration-301-40.sql, reorg.sql, updateStats.sql
 Note: news.migrate.jar will run between upgrade-301-40.sql and appGrants.sql

Profiles
 Database name: PEOPLEDB
 Version update: 3.0.1->4.0.0
 Sql scripts to run: upgrade-301-40.sql, appGrants.sql
 Note:

Wikis
 Database name: WIKIS
 Version update: 3.0.1->4.0.0
 Sql scripts to run: upgrade-301-40.sql, appGrants.sql
 Note:

Figure 11. Database wizard for IBM Connections 4.0: Pre-configuration task summary (2 of 3)

Database host name: db2machine.example.com
 Database port: 50000
 Administrator ID: db2inst1

To change any settings, click Back. To begin the task, click Update.

☒ Show the detailed database commands.

Back Update Cancel

Figure 12. Database wizard for IBM Connections 4.0: Pre-configuration task summary (3 of 3)

- ___ 10. Click **Next** and then **Execute**.
- ___ 11. Review the Post Configuration Task Summary. Click **Finish** to exit the wizard.

3. Export applications from Lotus Connections 3.0.1.x: Ensure that Lotus Connections 3.0.1.x is up and running

- ___ 1. Download Lotus_Connections_Install Build.
- ___ 2. For LC export copied migration_4.0.0.0_Date_.zip from Build, that is Lotus_Connections_Install/LotusConnections/native/migration_Date.zip and extract.
- ___ 3. Copy the extracted migration folder to the deployment manager where IBM Connections 3.0.1.x, that is /opt/IBM/LotusConnections/.
- ___ 4. Change permission to **777 for migrate.sh** script which is inside Lotus Connections.
- ___ 5. Run the Export command from /opt/IBM/LotusConnections/migration/ that is, **./migrate.sh lc-export**.
- ___ 6. Verify the logs. (The logs are stored in two places, one in /root/lc_migration-<Date>.log, and the second one in /opt/IBM/LotusConnections/migration/**work**/migration-latest.log).
- ___ 7. Backup Migration Folder, that is /opt/IBM/Lotusconnections to a safe place.



Note

The lc-export command exports the following data:

- Configuration files in the LotusConnections-config directory. You can find this directory in the following location: `profile_root/config/cells/DM_cell_name>/LotusConnections-config`.
- Properties files in the `connections` root directory.

- ___ 8. The exported data is stored in the migration directory. Check the log file to validate the export. The log file is stored in the system user's home directory and uses the following naming format: `lc-migration-yyyyMMdd_HHmm_ss.log`.

4. Install WebSphere Application Server, Application Server1, Application Server2, HTTP Server on the same computers as for 3.0.1.x

ULimits

___ 1. Open /etc/profile. Search ulimit -n 8192 and type ulimit -n on #.

```
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
file size               (blocks, -f) unlimited
pending signals         (-i) 31582
max locked memory       (kbytes, -l) 32
max memory size         (kbytes, -m) unlimited
open files              (-n) 8192
pipe size               (512 bytes, -p) 8
POSIX message queues    (bytes, -q) 819200
stack size              (kbytes, -s) 8192
cpu time                (seconds, -t) unlimited
max user processes      (-u) 31582
virtual memory          (kbytes, -v) unlimited
file locks              (-x) unlimited
```

Figure 13. /etc/profile

WebSphere Application Server installation

1. Start IBM WebSphere Application Server Network Deployment installation wizard and click **Next**.

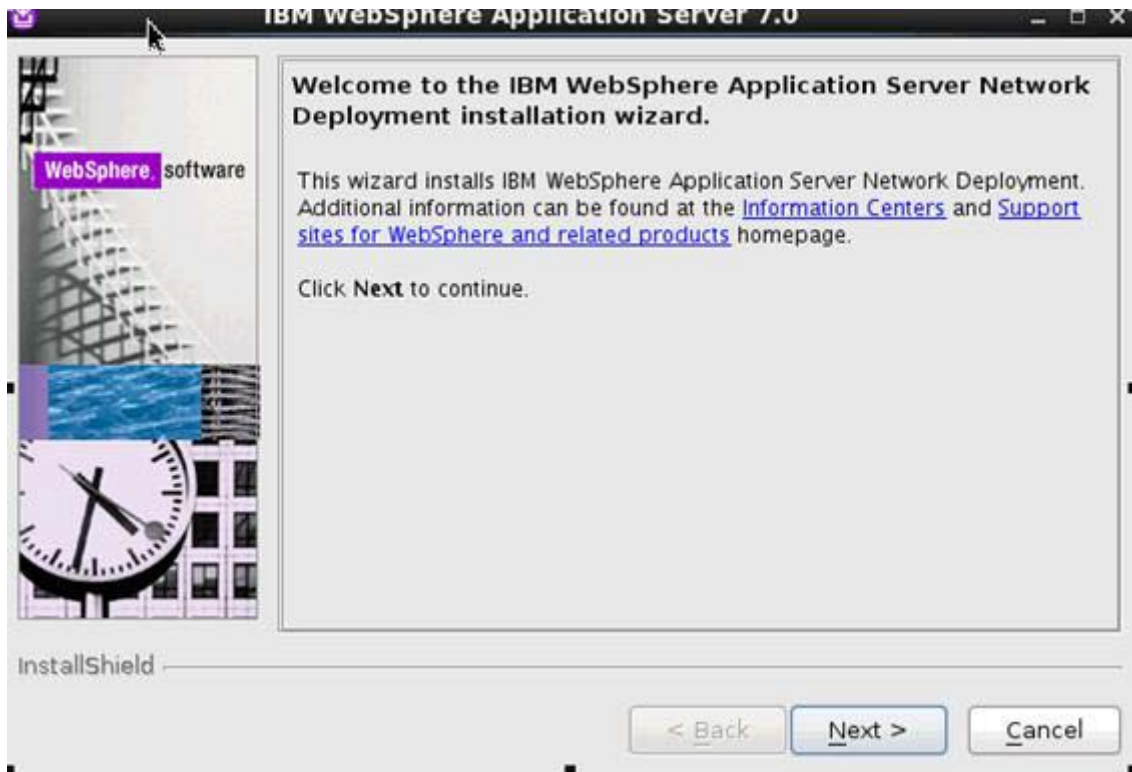


Figure 14. IBM WebSphere Application Server Network Deployment installation wizard: Welcome

___ 2. Accept the license agreement and click **Next**.



Figure 15. IBM WebSphere Application Server Network Deployment installation wizard: Software License Agreement

___ 3. Click **Next** to continue.



Figure 16. IBM WebSphere Application Server Network Deployment installation wizard: Warning screen

- ___ 4. Choose "Install a new copy of IBM WebSphere Application Server Network Deployment" and click **Next**.

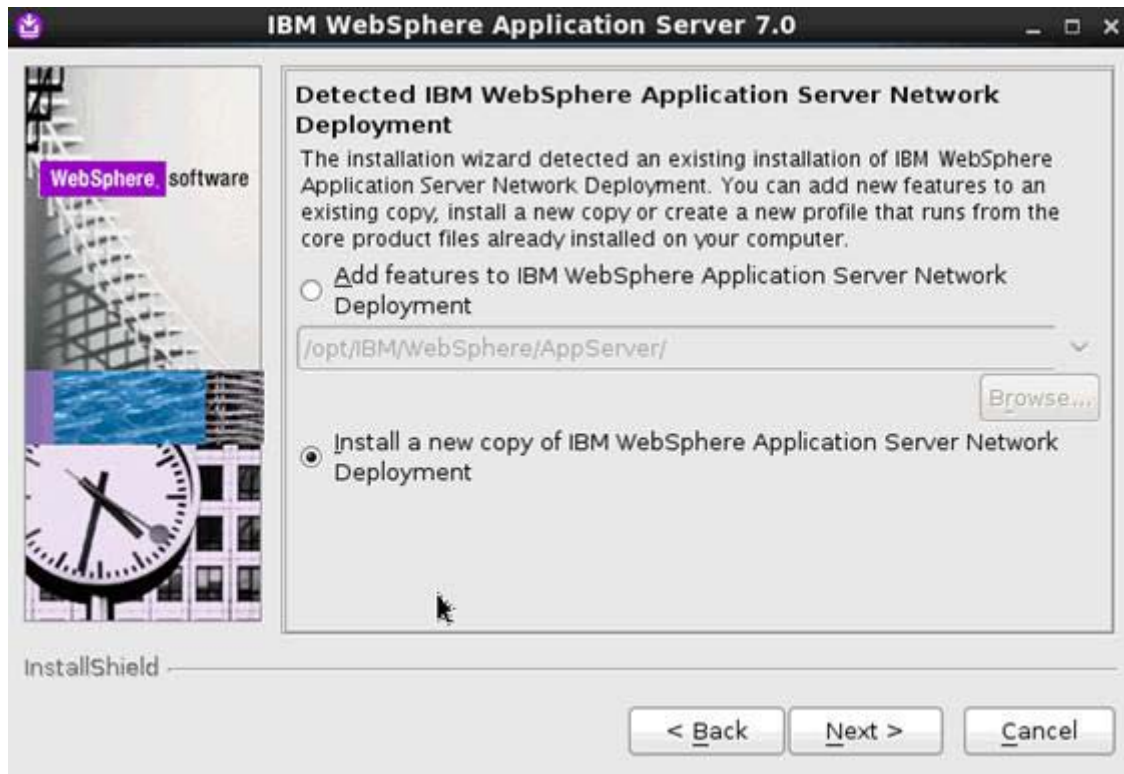


Figure 17. IBM WebSphere Application Server Network Deployment installation wizard: Detected IBM WebSphere Application Server Network Deployment

- ___ 5. Leave the optional features installation as default and click **Next**.



Figure 18. IBM WebSphere Application Server Network Deployment installation wizard: Optional Features Installation

- ___ 6. Choose a different path to install IBM WebSphere Application Server, for example /opt2, and click **Next**.



Figure 19. IBM WebSphere Application Server Network Deployment installation wizard: Installation Directory

___ 7. Select **Management** and click **Next**.



Figure 20. IBM WebSphere Application Server Network Deployment installation wizard: WebSphere Application Server Environments

___ 8. Select **Deployment manager** and click **Next**.



Figure 21. IBM WebSphere Application Server Network Deployment installation wizard: Server Type Selection

- ___ 9. Select **Enable administrative security**, enter the user name and password, and click **Next**.



Figure 22. IBM WebSphere Application Server Network Deployment installation wizard: Enable Administrative Security

___ 10. Do not select a repository for centralized installation managers and click **Next** to continue.

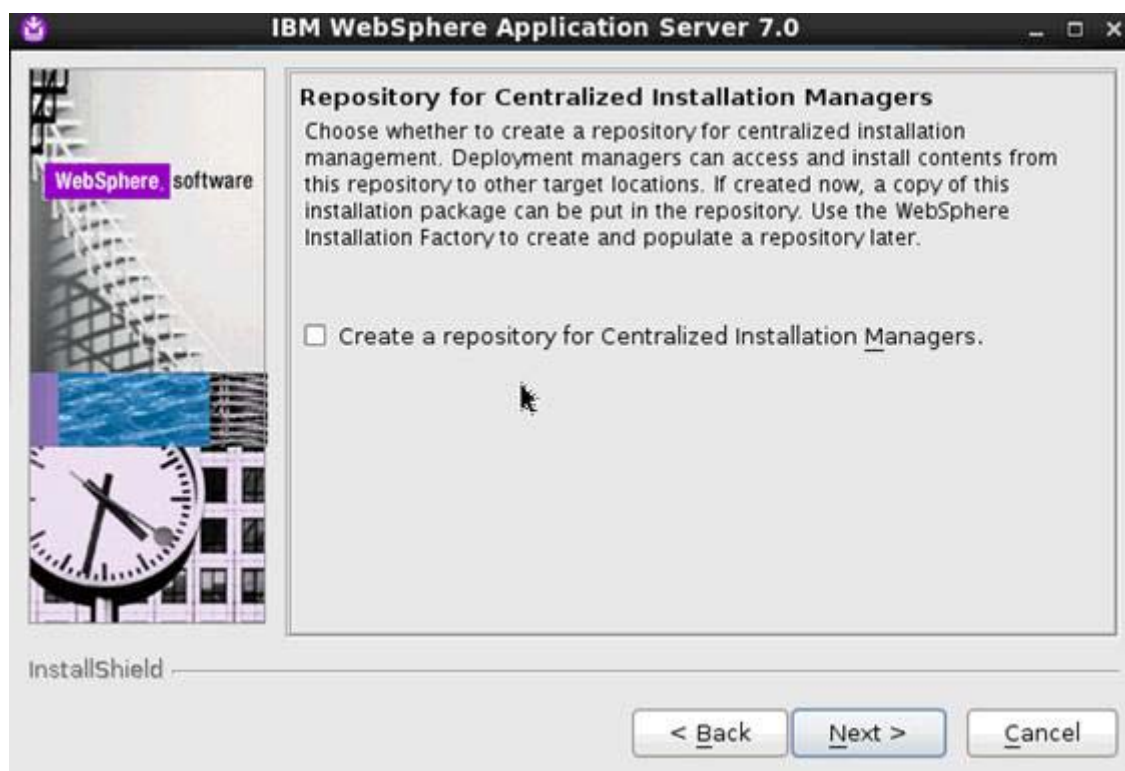


Figure 23. IBM WebSphere Application Server Network Deployment installation wizard: Repository for Centralized Installation Managers

The wizard starts to search for uninstalleable interim fixes.



Figure 24. IBM WebSphere Application Server Network Deployment installation wizard: Searching for uninstalleable interim fixes

___ 11. Check the installation summary and click **Next** to continue.

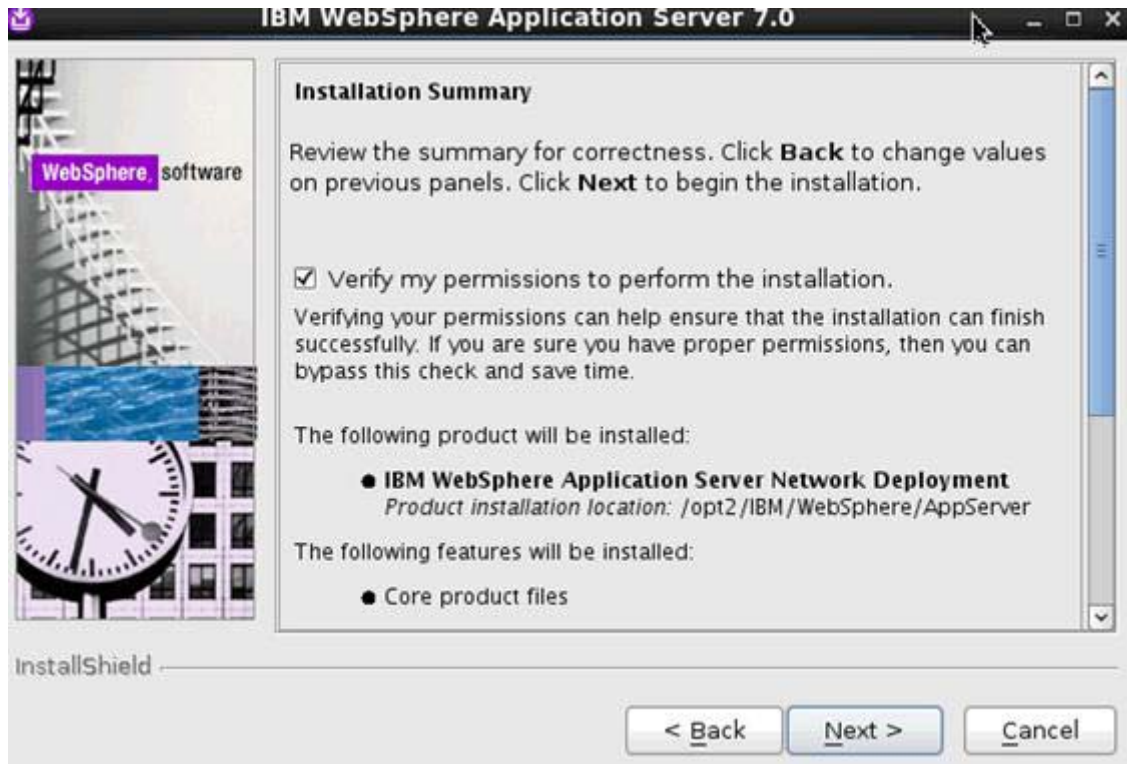


Figure 25. IBM WebSphere Application Server Network Deployment installation wizard: Installation Summary (1 of 3)



Figure 26. IBM WebSphere Application Server Network Deployment installation wizard: Installation Summary (2 of 3)

- ___ 12. Ensure that you have sufficient permissions for the installation and click **Next** to continue.



Figure 27. IBM WebSphere Application Server Network Deployment installation wizard: Installation Summary (3 of 3)

The installation begins.

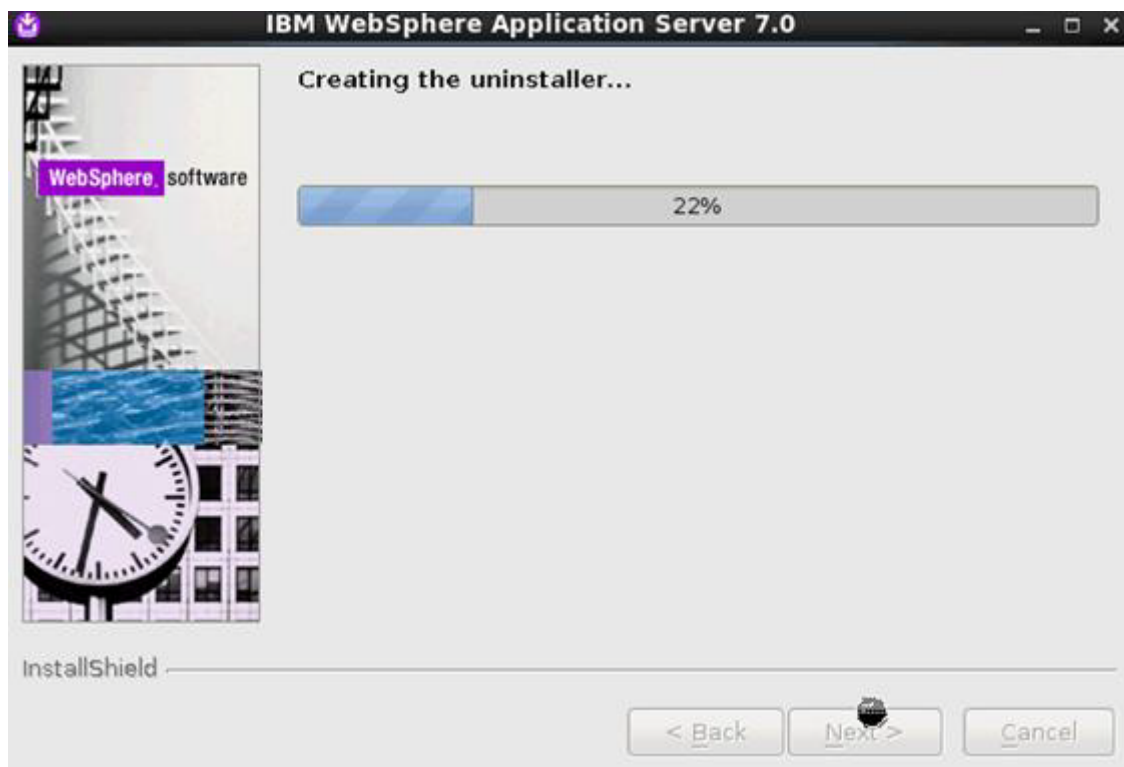


Figure 28. IBM WebSphere Application Server Network Deployment installation wizard: Installation in progress

- ___ 13. The installation is successful. Select **Launch the First steps console** and click **Finish**.

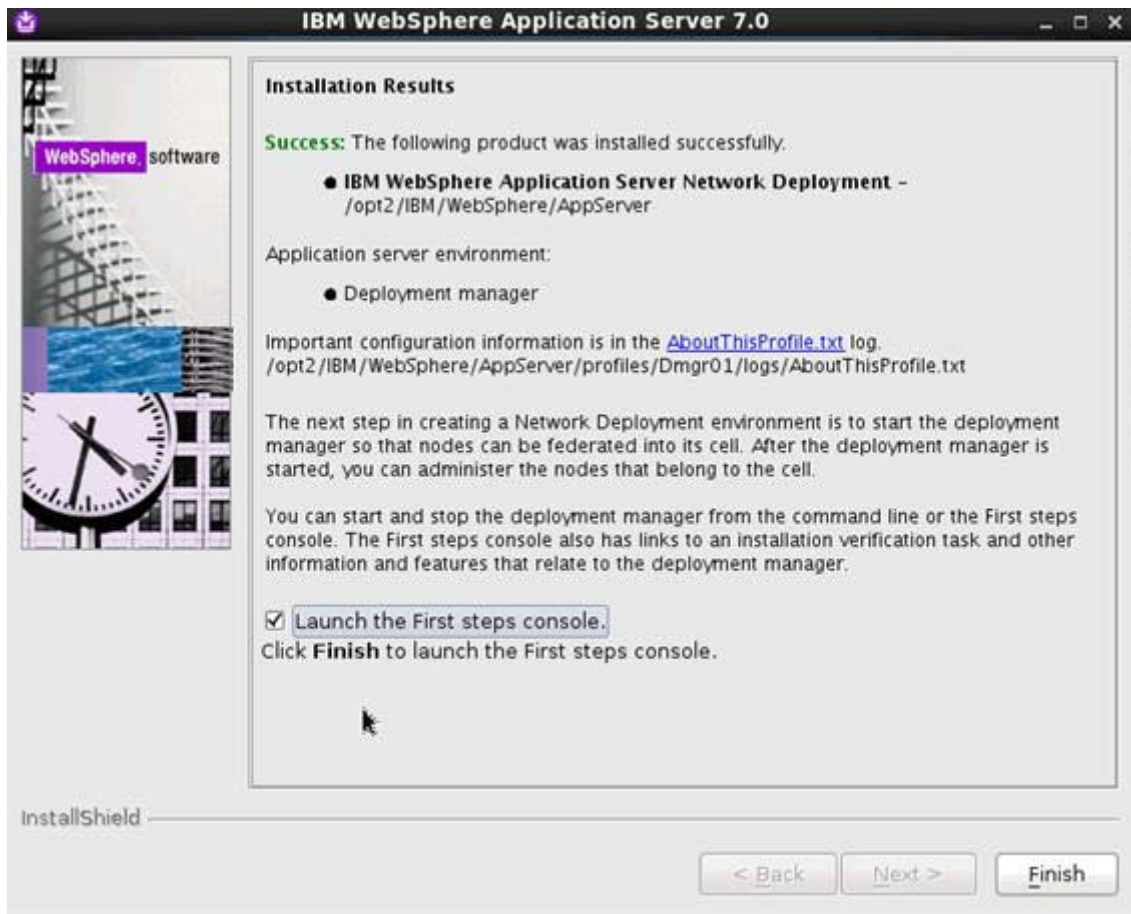


Figure 29. IBM WebSphere Application Server Network Deployment installation wizard: Installation Results

___ 14. Click **Installation verification**.



Figure 30. WebSphere Application Server: First steps: Dmgr01

- ___ 15. In the verification screen, check the profile home and the port, as shown in the following figure.

```

First steps output - Installation verification
Server name is dmgr
Profile name is Dmgr01
Profile home is /opt2/IBM/WebSphere/AppServer/profiles/Dmgr01
Profile type is management
Cell name is: dm Cell02
Node name is: dm CellManager02
Current encoding is UTF-8
Start running the following command: /opt2/IBM/WebSphere/AppServer/profiles/Dmgr01/bin/startServer.sh dmgr -profileName Dmgr01
>ADMU0116I: Tool information is being logged in file
> /opt2/IBM/WebSphere/AppServer/profiles/Dmgr01/logs/dmgr/startServer.log
>ADMU0128I: Starting tool with the Dmgr01 profile
>ADMU3100I: Reading configuration for server: dmgr
>ADMU3200I: Server launched. Waiting for initialization status.
>ADMU3000I: Server dmgr open for e-business; process id is 7219
Server port number is 9061
NTL0010I: Connecting to the DM.example.com WebSphere Application Server on port: 9061
NTL0015I: WebSphere Application Server DM.example.com is running on port: 9061 for profile Dmgr01
NTL0035I: The Installation Verification Tool is running on port: 9044 for profile Dmgr01
[6/26/12 14:03:52:078 IST] 00000000 WSKyStore W CWPJ0041W: One or more key stores are using the default password.
[6/26/12 14:03:56:829 IST] 00000000 ThreadPoolsMgr W WSVR0626W: The ThreadPool setting on the ObjectRequestBroker service is deprecated.
NTL0040I: 2 errors/warnings are detected in the /opt2/IBM/WebSphere/AppServer/profiles/Dmgr01/logs/dmgr/SystemOut.log file
NTL0070I: The Installation Verification Tool verification succeeded.
NTL0080I: The installation verification is complete.
  
```

Figure 31. First steps output: Installation verification

AboutThisProfile.txt

Application server environment to create: Management

Location: /opt2/IBM/WebSphere/AppServer/profiles/Dmgr01

Disk space required: 30 MB

Profile name: Dmgr01

Make this profile the default: True

Node name: DM.machineCellManager02

Cell name: DM.machine1Cell02

Host name: dm.machine.example.com

Enable administrative security (recommended): True

Administrative console port: 9061

Administrative console secure port: 9044

Management bootstrap port: 9810

Management SOAP connector port: 8880

Run Management as a service: False

Application servers on both nodes

1. Start the IBM WebSphere Application Server Network Deployment installation wizard and click **Next**.

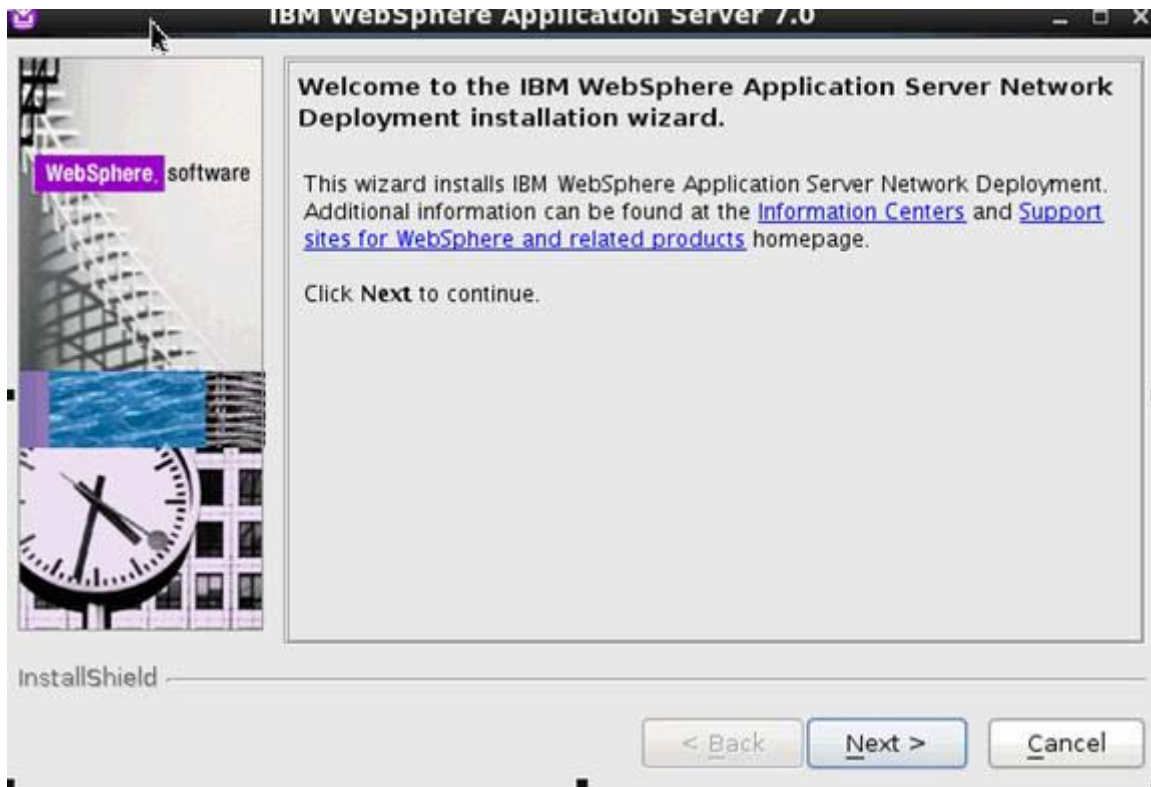


Figure 32. IBM WebSphere Application Server Network Deployment installation wizard: Welcome

- ___ 2. Accept the license agreement and click **Next**.



Figure 33. IBM WebSphere Application Server Network Deployment installation wizard: Software License Agreement

___ 3. Click **Next** to continue.



Figure 34. IBM WebSphere Application Server Network Deployment installation wizard: Warning screen

- ___ 4. Choose "Install a new copy of IBM WebSphere Application Server Network Deployment" and click **Next**.



Figure 35. IBM WebSphere Application Server Network Deployment installation wizard: Detected IBM WebSphere Application Server Network Deployment

___ 5. Leave the optional features installation as default and click **Next**.



Figure 36. IBM WebSphere Application Server Network Deployment installation wizard: Optional Features Installation

- ___ 6. Choose a different path to install IBM WebSphere Application Server, for example `/opt2`, and click **Next**.



Figure 37. IBM WebSphere Application Server Network Deployment installation wizard: Installation Directory

___ 7. Select **Application server** and click **Next**.



Figure 38. IBM WebSphere Application Server Network Deployment installation wizard: WebSphere Application Server Environments

- ___ 8. Select **Enable administrative security**, enter the user name and password, and click **Next**.



Figure 39. IBM WebSphere Application Server Network Deployment installation wizard: Enable Administrative Security

- ___ 9. Do not select a repository for centralized installation managers and click **Next** to continue.

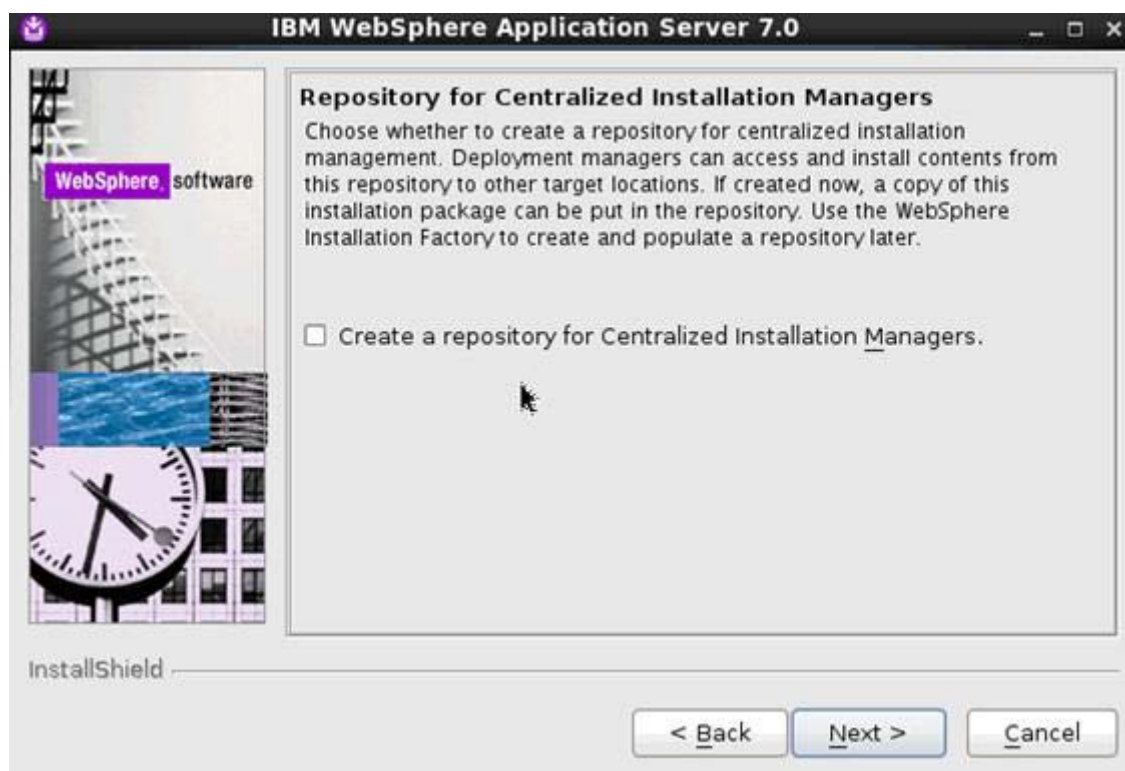


Figure 40. IBM WebSphere Application Server Network Deployment installation wizard: Repository for Centralized Installation Managers

The wizard starts to search for uninstalleable interim fixes.



Figure 41. IBM WebSphere Application Server Network Deployment installation wizard: Searching for uninstalleable interim fixes

___ 10. Check the installation summary and click **Next** to continue.

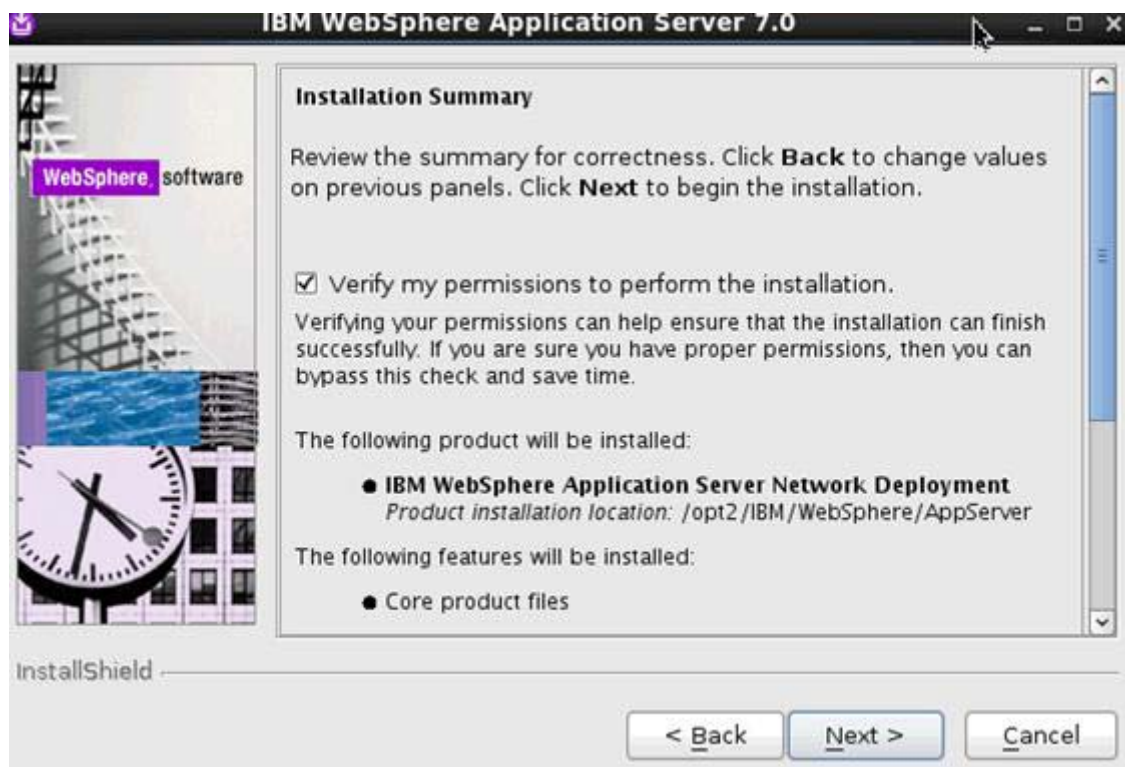


Figure 42. IBM WebSphere Application Server Network Deployment installation wizard: Installation Summary

The component prerequisites installation begins.

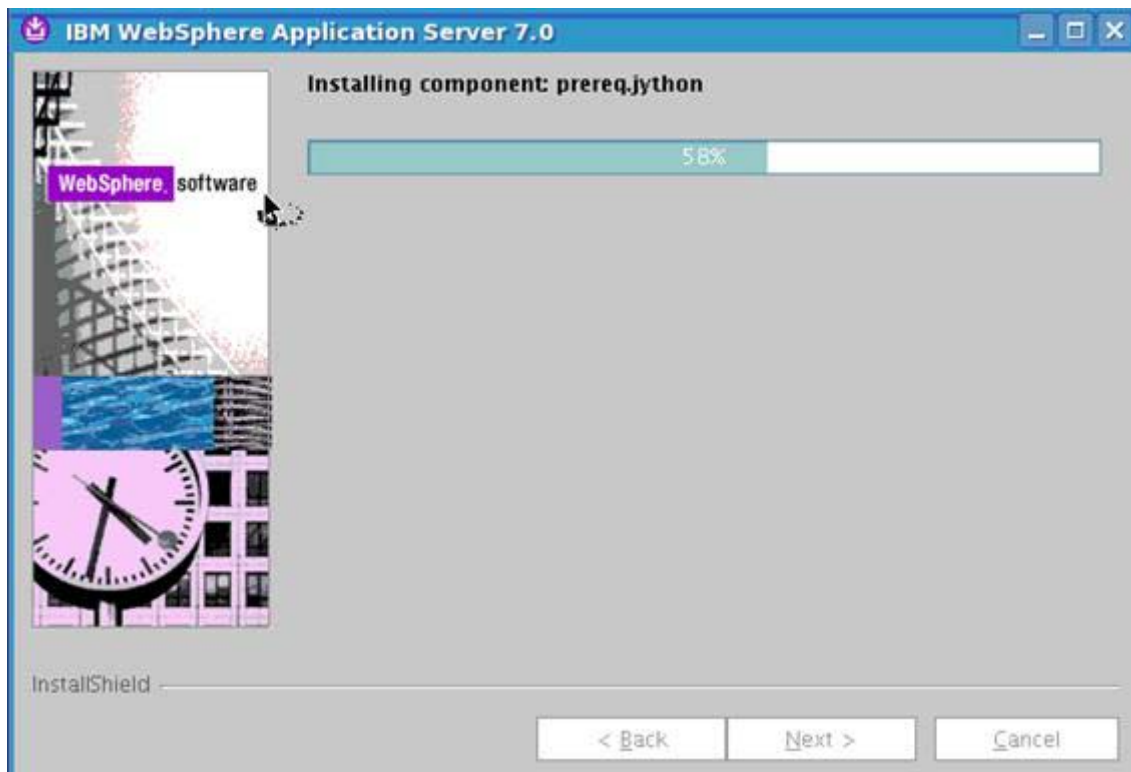


Figure 43. IBM WebSphere Application Server Network Deployment installation wizard: Component prerequisites installation in progress

The installation begins.

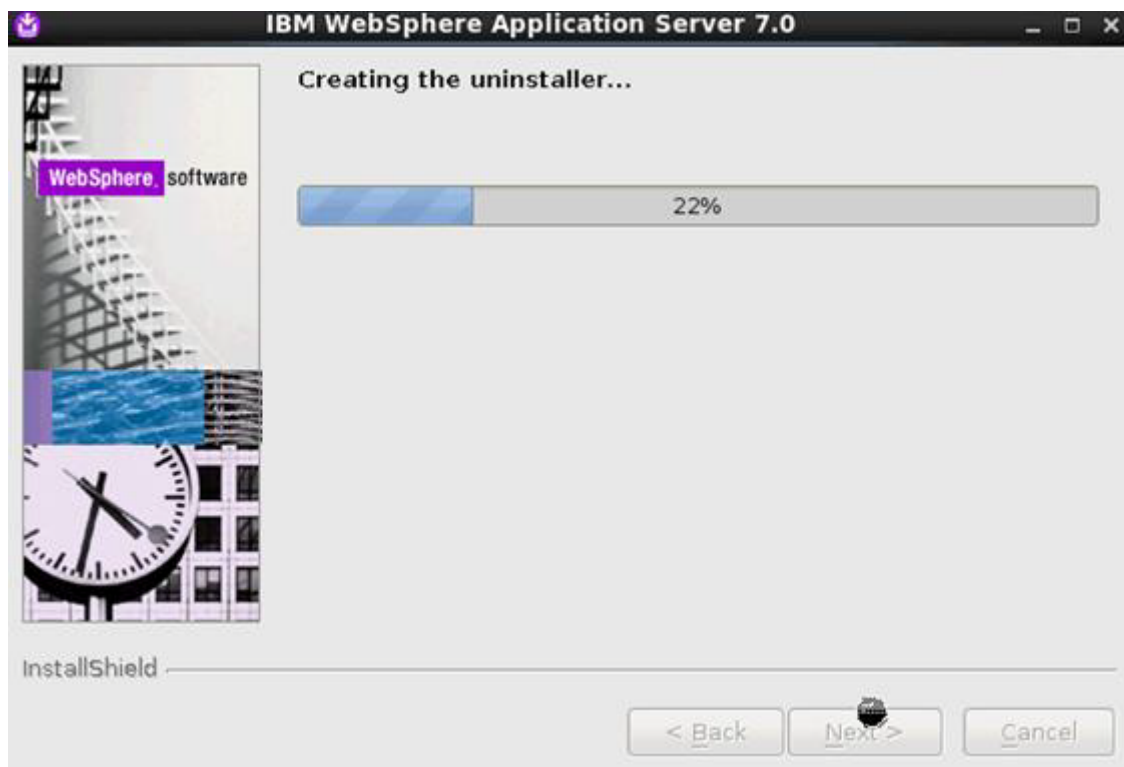


Figure 44. IBM WebSphere Application Server Network Deployment installation wizard: Installation in progress

- ___ 11. The installation is successful. Select **Launch the First steps console** and click **Finish**.

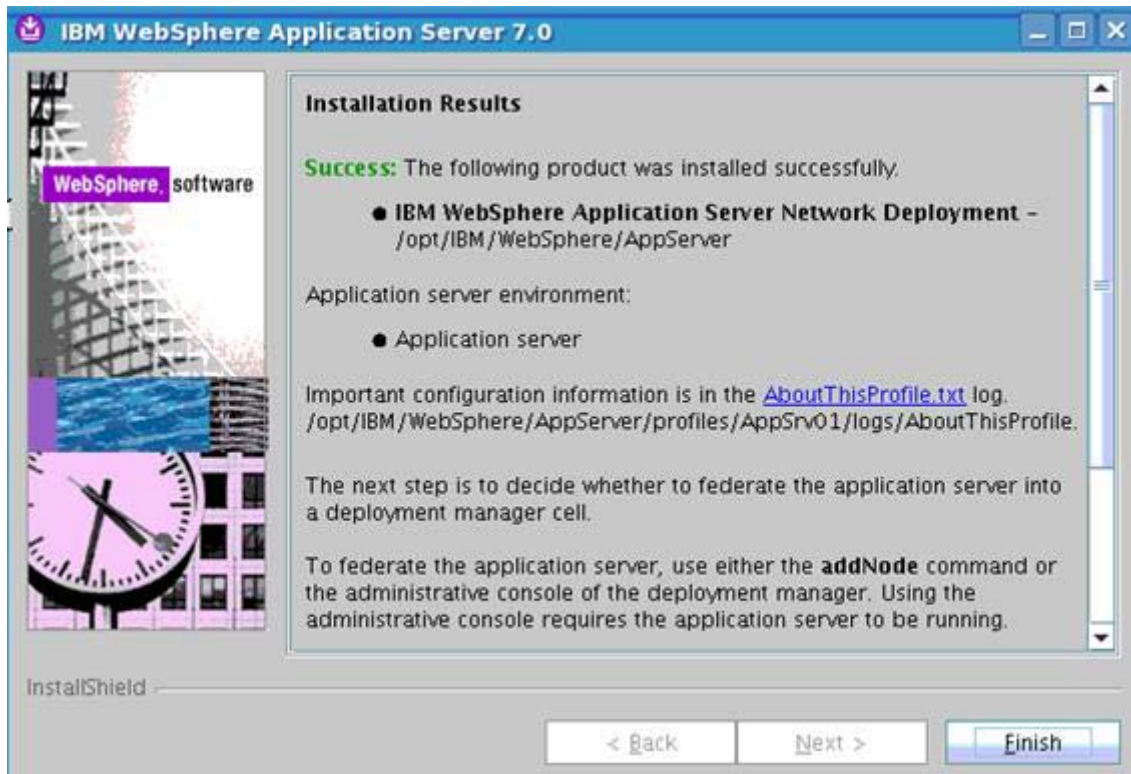


Figure 45. IBM WebSphere Application Server Network Deployment installation wizard: Installation Results

___ 12. Click **Installation verification**.

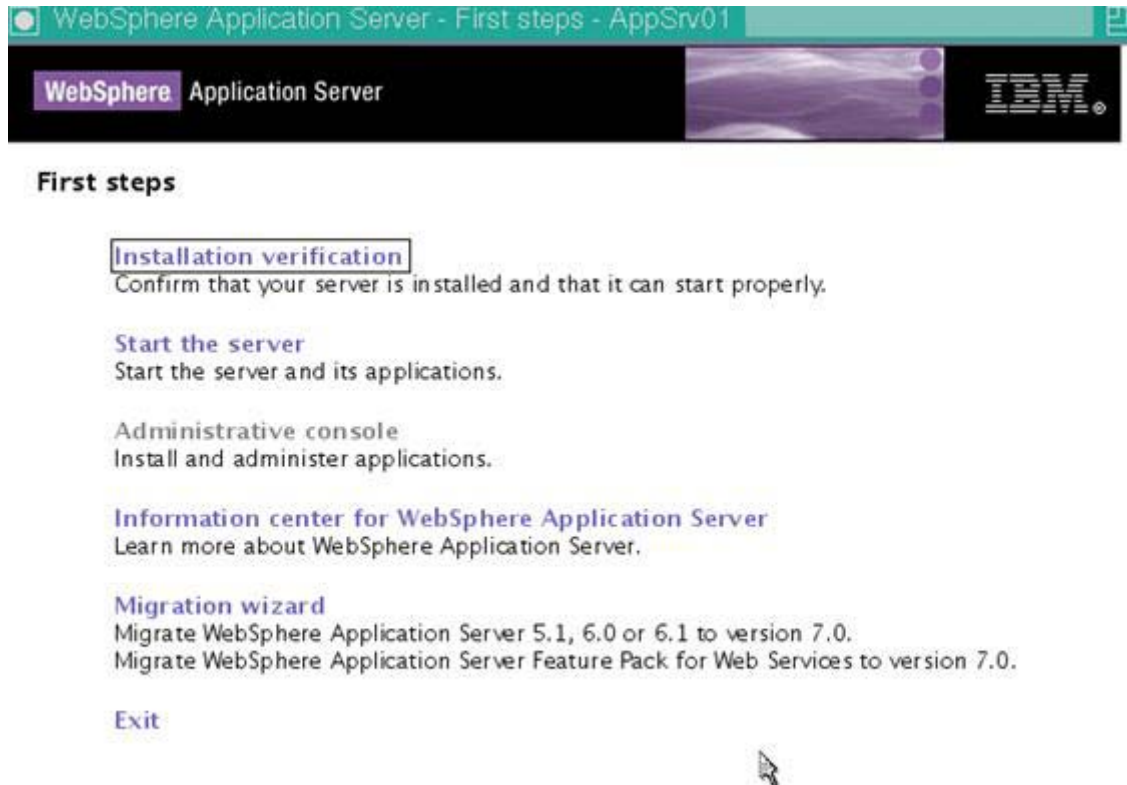


Figure 46. WebSphere Application Server: First steps: AppSrv01

___ 13. Check the installation verification summary, as shown in the following figure.



Figure 47. First steps output: Installation verification

Federate Nodes to Deployment Manager

1. From AppServer 1, run the following command to federate to Deployment Manager.

```

./addNode.sh 8880 -user -password
ADMU0116I: Tool information is being logged in file
/opt2/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/addNode.log
ADMU0128I: Starting tool with the AppSrv01 profile
CWPKI0308I: Adding signer alias "CN=" to local
keystore "ClientDefaultTrustStore" with the following SHA digest:
27:AD:12:C2:2D:91:AD:7C:05:08:3A:2D:DD:70:DC:11:72:1E:59:91
CWPKI0308I: Adding signer alias "datapower" to local keystore
"ClientDefaultTrustStore" with the following SHA digest:
A9:BA:A4:B5:BC:26:2F:5D:2A:BA:F4:31:05:F2:54:14:17
ADMU0001I: Begin federation of node Appserver1 Node02 with Deployment Manager
at DM.machine.example com:8880.
ADMU0009I: Successfully connected to dep Manager Server:
DM.machine.example-com:8880
ADMU0505I: Servers found in co
ADMU0506I: Server name: server.
ADMU2010I: Stopping all server processes for node Node02
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: Node02
ADMU0014I: Adding node Node02 configuration to cell:
Cell02
ADMU0016I: Synchronizing configuration between node and cell.
ADMU0018I: Launching Node Agent process for node: Node02
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:
3074

ADMU0300I: The node Node02 was successfully added to the

```

Figure 48. Command that is used to federate to Deployment Manager from AppServer 1

2. From AppServer 2, run the following command to federate to Deployment Manager.

```

./addNode.sh 8880 -user -password
ADMU0116I: Tool information is being logged in file
/opt2/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/addNode.log
ADMU0128I: Starting tool with the AppSrv01 profile
CWPKI0308I: Adding signer alias "CN=" to local
keystore "ClientDefaultTrustStore" with the following SHA digest:
27:AD:12:C2:2D:91:AD:7C:05:08:3A:2D:DD:70:DC:11:72:1E:59:91
CWPKI0308I: Adding signer alias "datapower" to local keystore
"ClientDefaultTrustStore" with the following SHA digest:
A9:BA:A4:B5:BC:26:2F:5D:2A:BA:F4:31:05:F2:54:14:17
ADMU0001I: Begin federation of node Appserver2 Node02 with Deployment Manager
at DM.machine.example com:8880.
ADMU0009I: Successfully connected to dep Manager Server:
DM.machine.example-com:8880
ADMU0505I: Servers found in co
ADMU0506I: Server name: server.
ADMU2010I: Stopping all server processes for node Node02
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: Node02
ADMU0014I: Adding node Node02 configuration to cell:
Cell02
ADMU0016I: Synchronizing configuration between node and cell.
ADMU0018I: Launching Node Agent process for node: Node02
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:
3074

ADMU0300I: The node Node02 was successfully added to the

```

Figure 49. Command that is used to federate to Deployment Manager from AppServer 2

General Settings

- ___ 4. Go to **Security > Global security > Web and SIP Security: General Settings**, and ensure that the “Use available authentication data when an unprotected URI is accessed” check box is selected.

Global security

Global security > Web security - General settings

Specifies the settings for Web authentication.

General Properties

Web authentication behavior

☒ Authenticate only when the URI is protected

☒ Use available authentication data when an unprotected URI is accessed

☐ Authenticate when any URI is accessed

☐ Default to basic authentication when certificate authentication for the HTTPS client fails

Figure 51. Web authentication behavior

- ___ 5. Select **Apply** and **Save**.
- ___ 6. Go to **Security > Global security > Web and SIP Security: Single sign-on (SSO)** and ensure that Interoperability Mode is selected, and enter the domain name.

Global security

Global security > Single sign-on (SSO)

Specifies the configuration values for single sign-on.

General Properties

☒ Enabled

☐ Requires SSL

Domain name

☒ Interoperability Mode

☒ Web inbound security attribute propagation

Figure 52. Global security: Single sign-on (SSO)

- ___ 7. Select **Apply** and **Save**.

Federate LDAP repositories

- ___ 1. Log in to your admin console `http://DM.machine.example.com:9061/admin`. Use `wasadmin` user and password.
- ___ 2. Select **Security > Global security > Configure....** for Federated repositories.



The dialog titled "User account repository" shows the "Current realm definition" as "Federated repositories". Under "Available realm definitions", "Federated repositories" is selected in a dropdown menu. To the right are two buttons: "Configure..." and "Set as current".

Figure 53. User account repository

- ___ 3. Select **Add Base entry to Realm...**

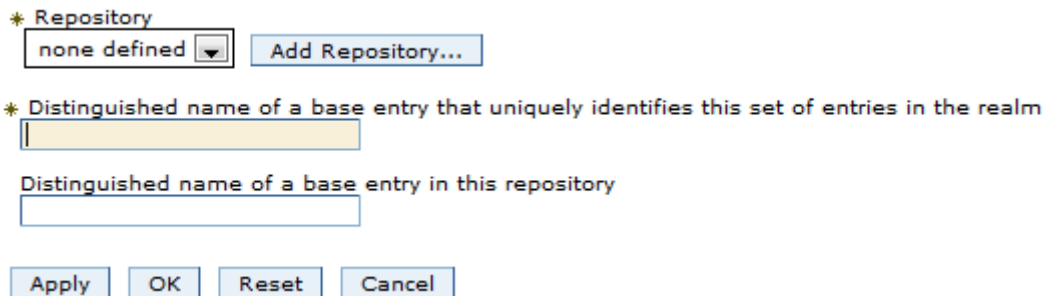


A table titled "Repositories in the realm:" with buttons "Add Base entry to Realm...", "Use built-in repository", and "Remove". The table has columns "Select", "Base Entry", "Repository Identifier", and "Repository Type". Below the table, it says "You can administer the following resources:".

Select	Base Entry	Repository Identifier	Repository Type
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File

Figure 54. Repositories in the realm

- ___ 4. Then, select **Add Repository...**



The "Add Repository" dialog has a dropdown menu for "Repository" currently set to "none defined", with an "Add Repository..." button next to it. Below is a section for "Distinguished name of a base entry that uniquely identifies this set of entries in the realm" with an empty text field. Underneath is another text field labeled "Distinguished name of a base entry in this repository". At the bottom are four buttons: "Apply", "OK", "Reset", and "Cancel".

Figure 55. Adding repository

- ___ 5. Enter the following:
- ___ a. Repository identifier,
 - ___ b. Primary host name,
 - ___ c. Bind distinguished name:
 - ___ d. Bind password:
 - ___ e. Login properties...

General Properties

* Repository identifier
MSAD-LDAP

LDAP server

* Directory type
Microsoft Windows Active Directory

* Primary host name
LDAPserver.example.com

Port
389

Fallover server used when primary is not available:

Select	Fallover Host Name	Port
None		

Add

Support referrals to other LDAP servers
ignore

Security

Bind distinguished name
CN=XXX

Bind password

Login properties
uid

LDAP attribute for Kerberos principal name
userprincipalname

Certificate mapping
EXACT_DN

Certificate filter

☐ Require SSL communications

☒ Centrally managed

[Manage endpoint security configurations](#)

☐ Use specific SSL alias

CellDefaultSSLSettings [SSL configurations](#)

Additional Properties

- [Performance](#)
- [LDAP entity types](#)

Figure 56. General properties

- ___ 6. Select **OK**. Enter the base entry when prompted.



Figure 57. Global security: Federated repositories

- ___ 7. Select **Apply** and **Save**.
- ___ 8. Restart your Deployment Manager and Node Agents.

Add Aamir_001_077 as an administrator

This is a good test, because you then know whether security is enabled correctly. In this task, you add the Aamir_001_077 user from the LDAP as an admin on your console.

- ___ 1. Log in to your admin console <http://DM.machine.example.com:9061/admin>.
- ___ 2. Select **Users and Groups > Administrative user roles**.

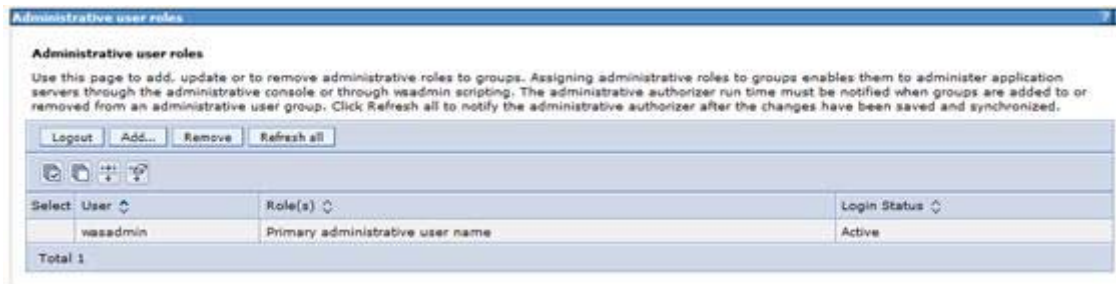


Figure 58. Administrative user roles

- ___ 3. Select **Add...** Then, select the role **Administrator**. Search for `Aamir_001_077` and add that user to the Mapped to Role.

Cell=dslvm1007Cell01, Profile=Dmgr01

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:

Maximum results to display:

Available

Select All Deselect All

Mapped to role

Select All Deselect All

Figure 59. Searching and selecting users

- ___ 4. Select **OK**.

Cell=dslvm1007Cell01, Profile=Dmgr01

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 run time must be notified when groups are added to or removed from an administrative user group. The administrative authorizer after the changes have been saved and synchronized.

☐ ☐ ☐ ☐

Select	User	Role(s)
<input type="checkbox"/>	Aamir_001_077	Administrator
	wasadmin	Primary administrative user name

Total 2

Figure 60. Selected user is added as administrator

- ___ 5. Log out and then log back in again as `Aamir_001_077` to ensure that it is working.

Check that the nodes are synchronized

- ___ 1. Logged in as Aamir_001_077, select **System Administration > Nodes**.
- ___ 2. Check whether the nodes are synchronized. The following figure shows the nodes in synchronization.

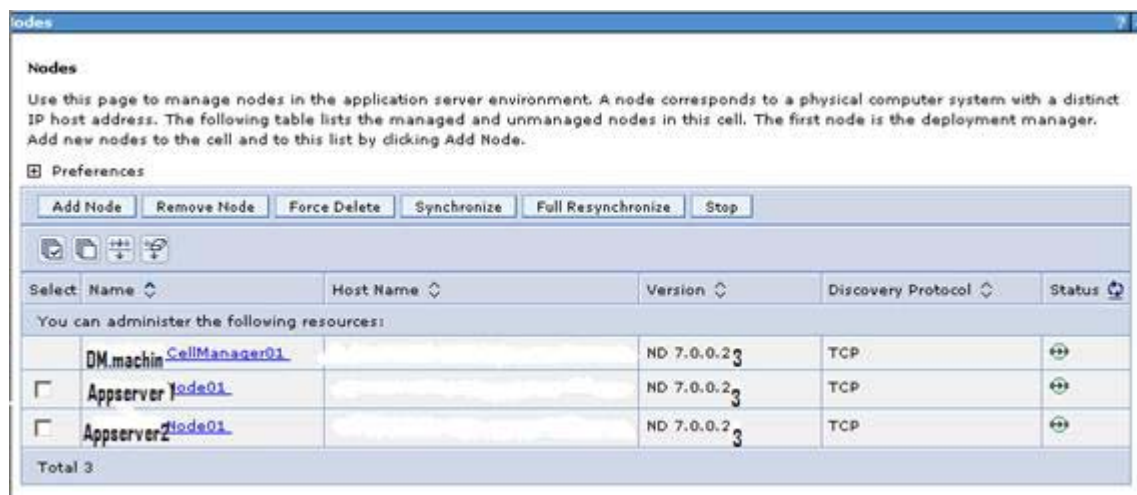


Figure 61. Synchronizes nodes

- ___ 3. If nodes are not synchronized, then do the following on each node to synchronize them.

Steps	Commands
The Node agents: Stop	./stopNode.sh
./syncNode.sh: Run	./syncNode.sh DM.Machine.example.com8880 -username Aamir_001_077 -password password
The Node agents: Restart	./startNode.sh

- ___ 4. Recheck System Administration > Nodes. The nodes should now be in synchronization as in Figure 61, "Synchronizes nodes," on page 60.

Install Update Installer on Deployment Manager, Appnode1, Appnode2

1. Start the installation wizard for the Update Installer and click **Next**.



Figure 62. Installation wizard for the Update Installer: Welcome

- ___ 2. Accept the license agreement and click **Next**.



Figure 63. Installation wizard for the Update Installer: Software License Agreement

- ___ 3. The system prerequisites check is passed. Click **Next** to continue.



Figure 64. Installation wizard for the Update Installer: System Prerequisites Check

- ___ 4. Select the installation directory, for example, `opt2`.

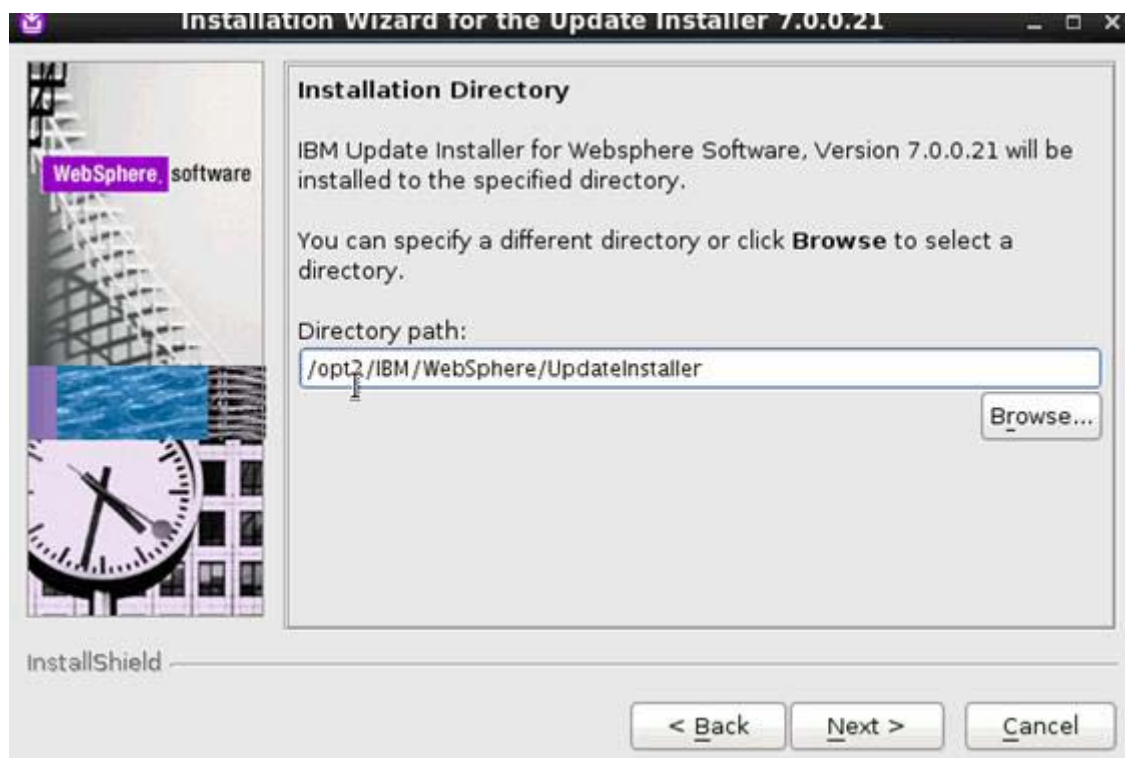


Figure 65. Installation wizard for the Update Installer: Installation Directory

- ___ 5. Check the installation summary and click **Next**.

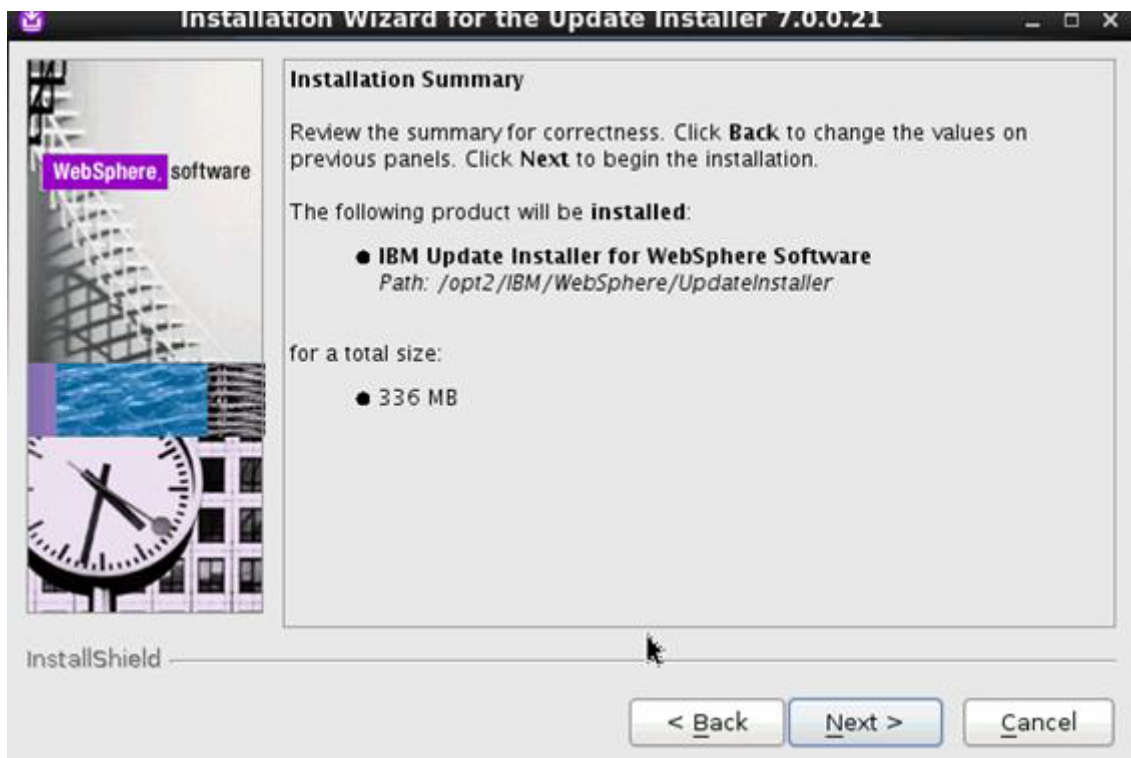


Figure 66. Installation wizard for the Update Installer: Installation Summary

___ 6. The installation completes successfully. Click **Finish** to exit the wizard.



Figure 67. Installation wizard for the Update Installer: Installation Complete

Install IBM HTTP Server

1. Start the IBM HTTP Server 7.0 installation wizard and click **Next**.

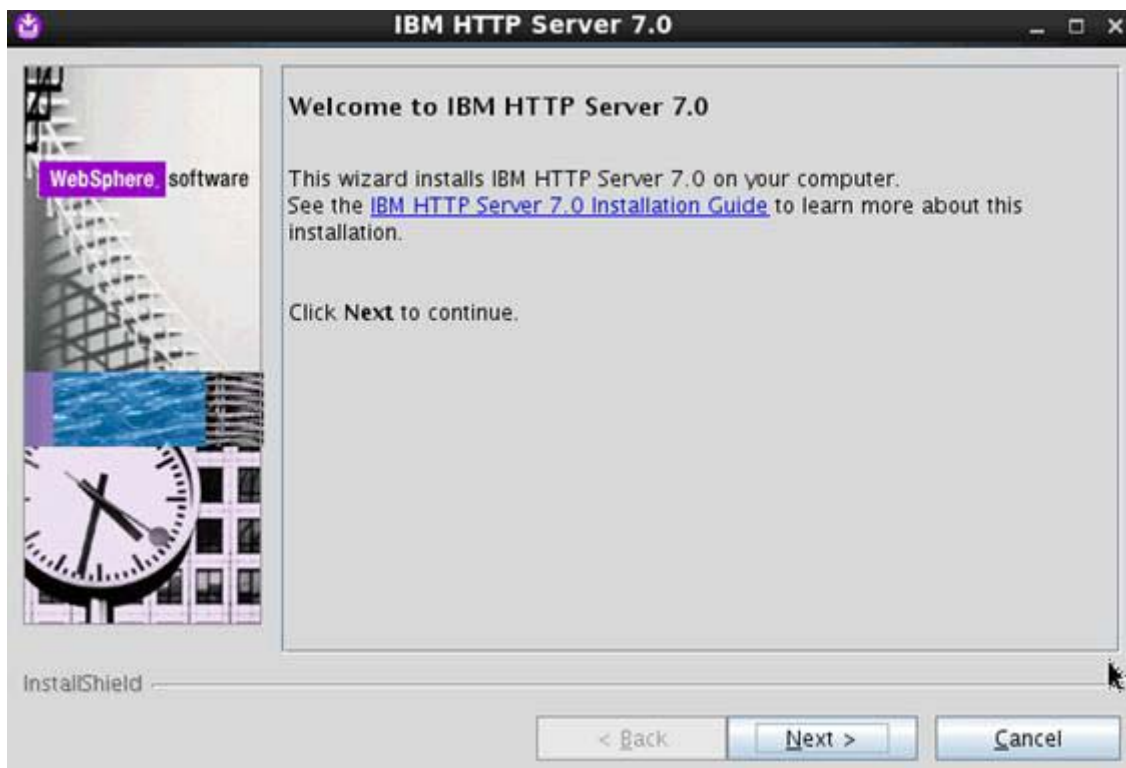


Figure 68. IBM HTTP Server 7.0 installation wizard: Welcome

- ___ 2. Accept the license agreement and click **Next**.



Figure 69. IBM HTTP Server 7.0 installation wizard: Software License Agreement

- ___ 3. Click **Next** to continue.

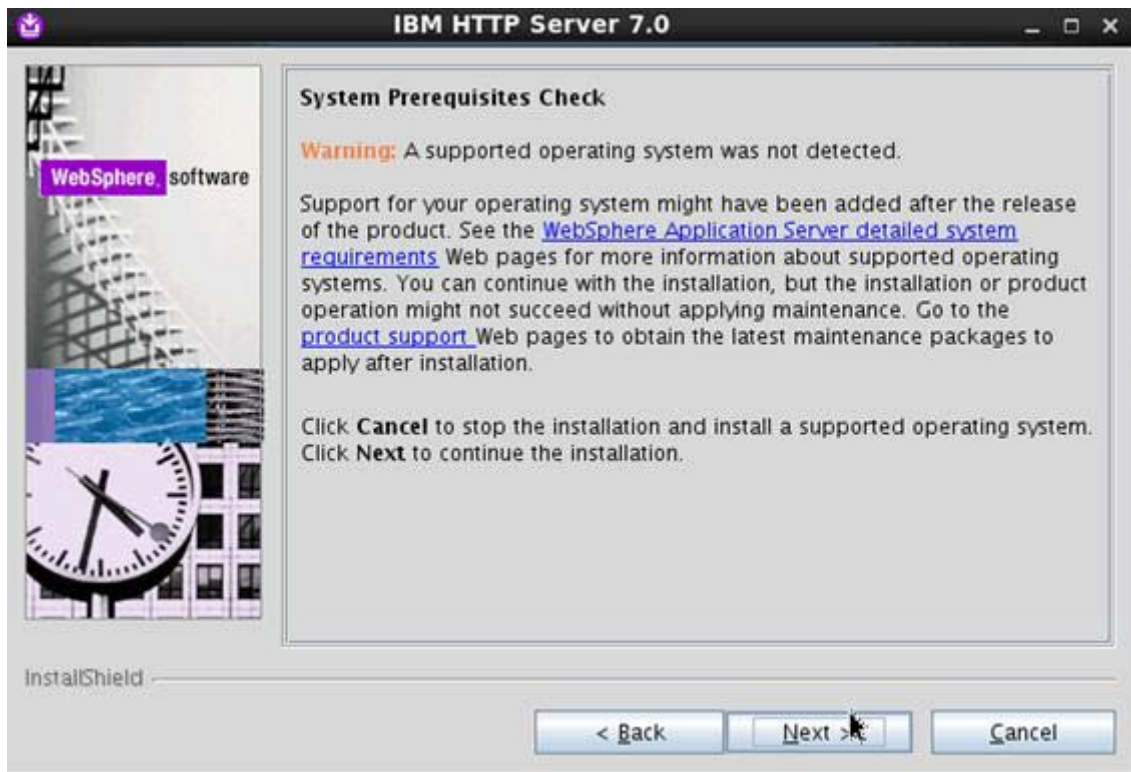


Figure 70. IBM HTTP Server 7.0 installation wizard: System Prerequisites Check

- ___ 4. Enter the installation location, for example, `opt2`, and click **Next**.

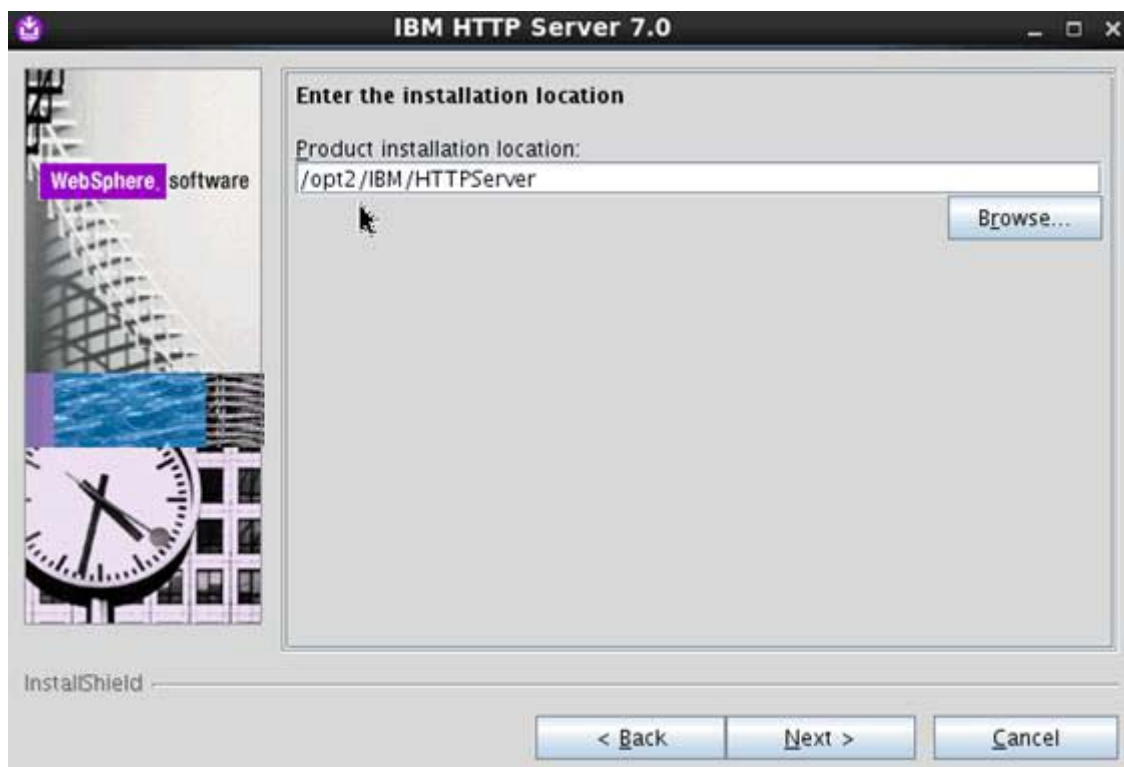


Figure 71. IBM HTTP Server 7.0 installation wizard: Installation location

- ___ 5. Assign the port values and click **Next**.

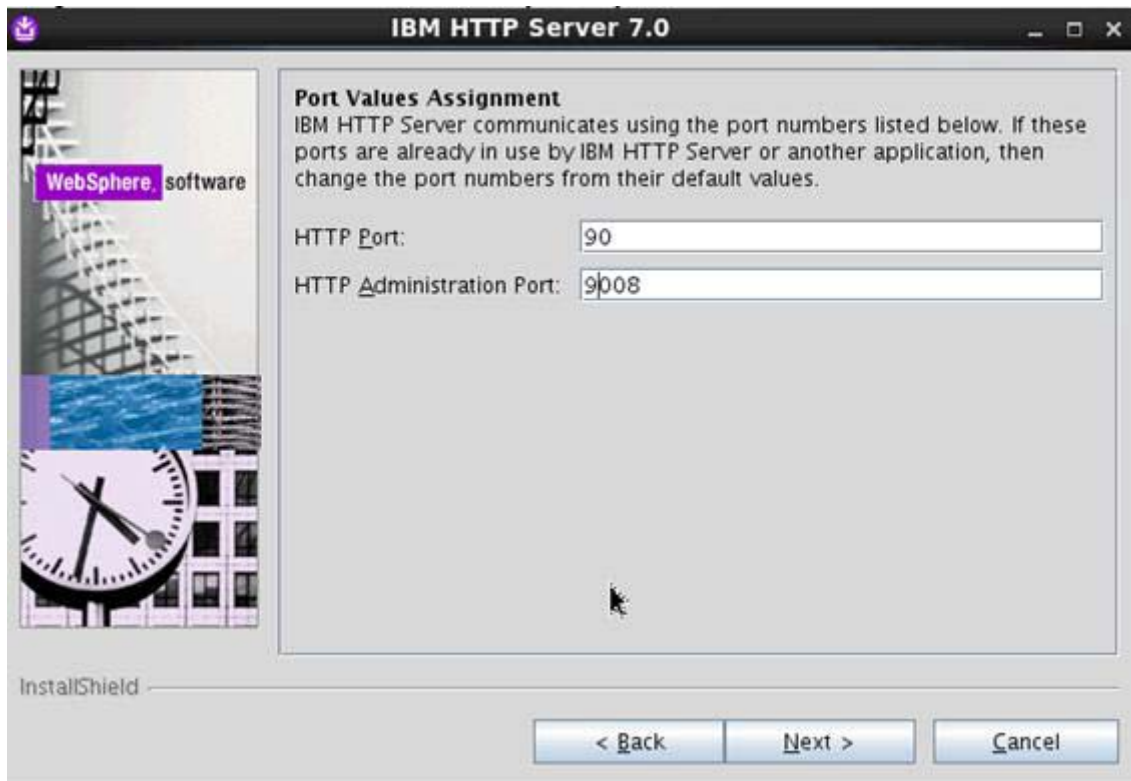


Figure 72. IBM HTTP Server 7.0 installation wizard: Port Values Assignment

- ___ 6. Enter a user ID and password and click **Next**.



Figure 73. IBM HTTP Server 7.0 installation wizard: HTTP Administration Server Authentication

- ___ 7. Enter a user ID and group for IBM HTTP Server Administration files and click **Next**.

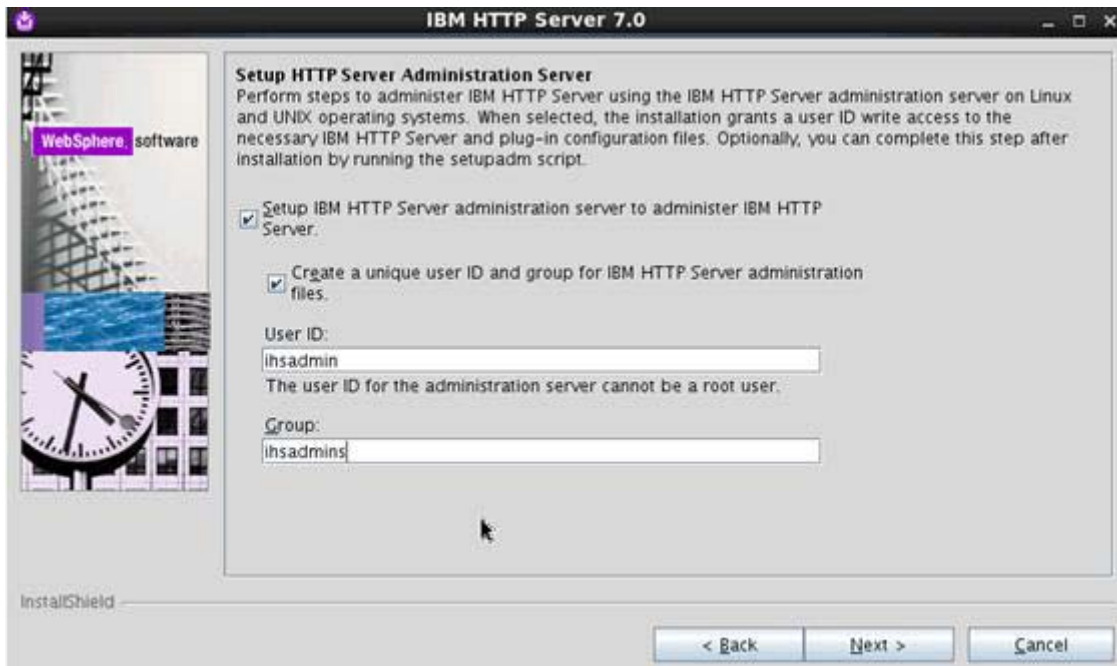


Figure 74. IBM HTTP Server 7.0 installation wizard: Setup HTTP Server Administration Server

- ___ 8. Enter the host name or IP address for the Application Server to install the HTTP Server plug-in.



Figure 75. IBM HTTP Server 7.0 installation wizard: IBM HTTP Server plug-in for IBM WebSphere Application Server

- ___ 9. Check the installation summary and click **Next**.

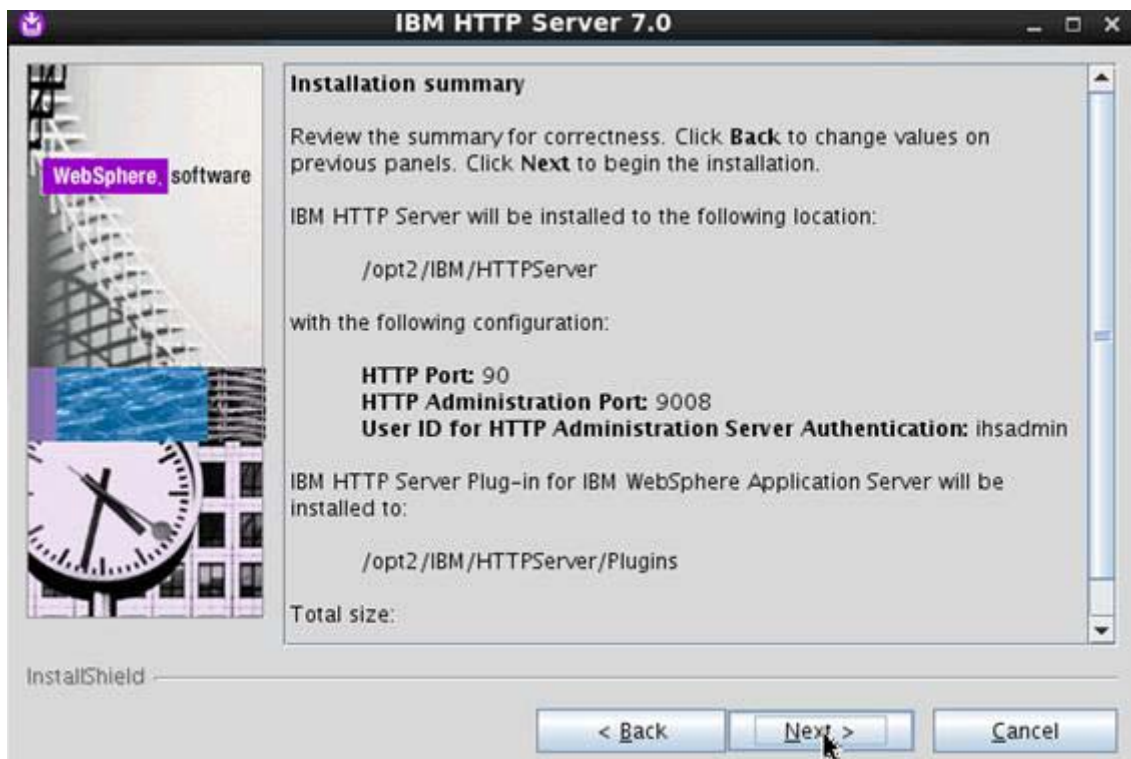


Figure 76. IBM HTTP Server 7.0 installation wizard: Installation Summary

The uninstaller creation begins.

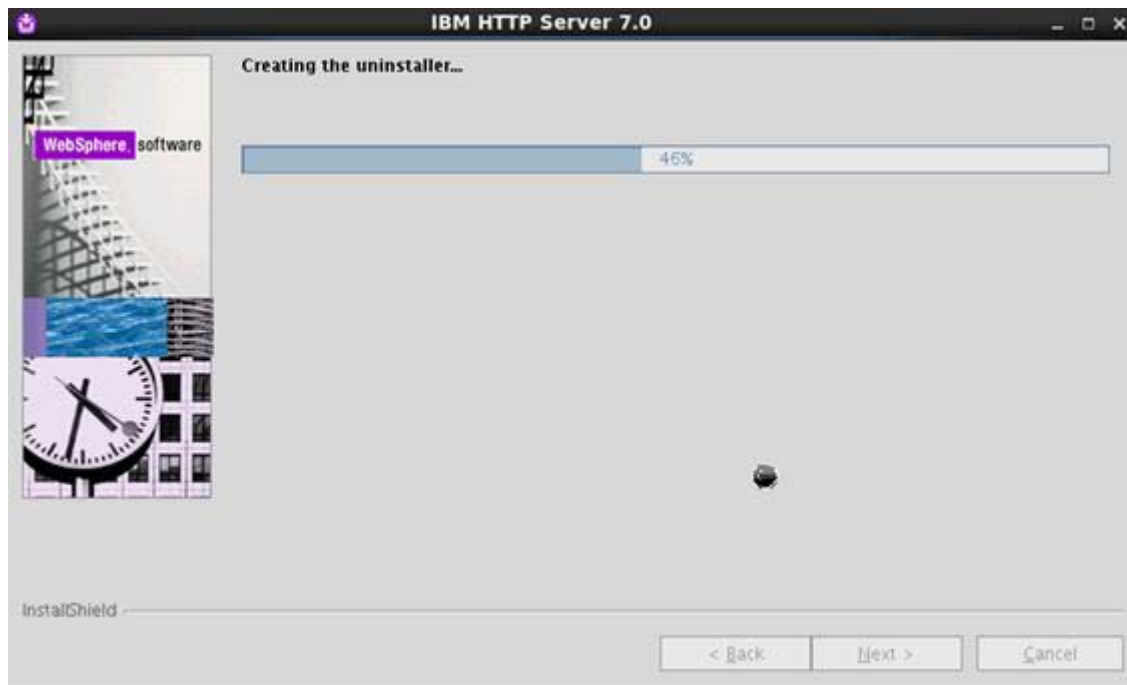


Figure 77. IBM HTTP Server 7.0 installation wizard: Uninstaller creation in progress

The plug-in installation begins.



Figure 78. IBM HTTP Server 7.0 installation wizard: Plug-in installation in progress

- ___ 10. Click **Finish**.
- ___ 11. Verify the logs at `/opt2/IBM/HTTPServer/logs/install/log.txt`.

Update Deployment Manager, AppServer, IBM HTTP Server, IBM HTTP Server plug-ins, SDKs to Fixpack 21

- ___ 1. Copy 7.0.0-WS-WAS-LinuxX64-FP0000021.pak, 7.0.0-WS-WASSDK-LinuxX64-FP0000021.pak, 7.0.0-WS-IHS-LinuxX64-FP0000021.pak and 7.0.0-WS-PLG-LinuxX64-FP0000021.pak to some location on your Deployment Manager, AppServer, and IBM HTTP Server server.
- ___ 2. Stop your Deployment Manager, NodeAgent, AppServer, and IBM HTTP Server servers.
- ___ 3. Start the WebSphere Application Server Update Installer by running `./update.sh` from under `/opt2/IBM/WebSphere/UpdateInstaller/`.
- ___ 4. In the welcome screen of the installation wizard, click **Next** to continue.

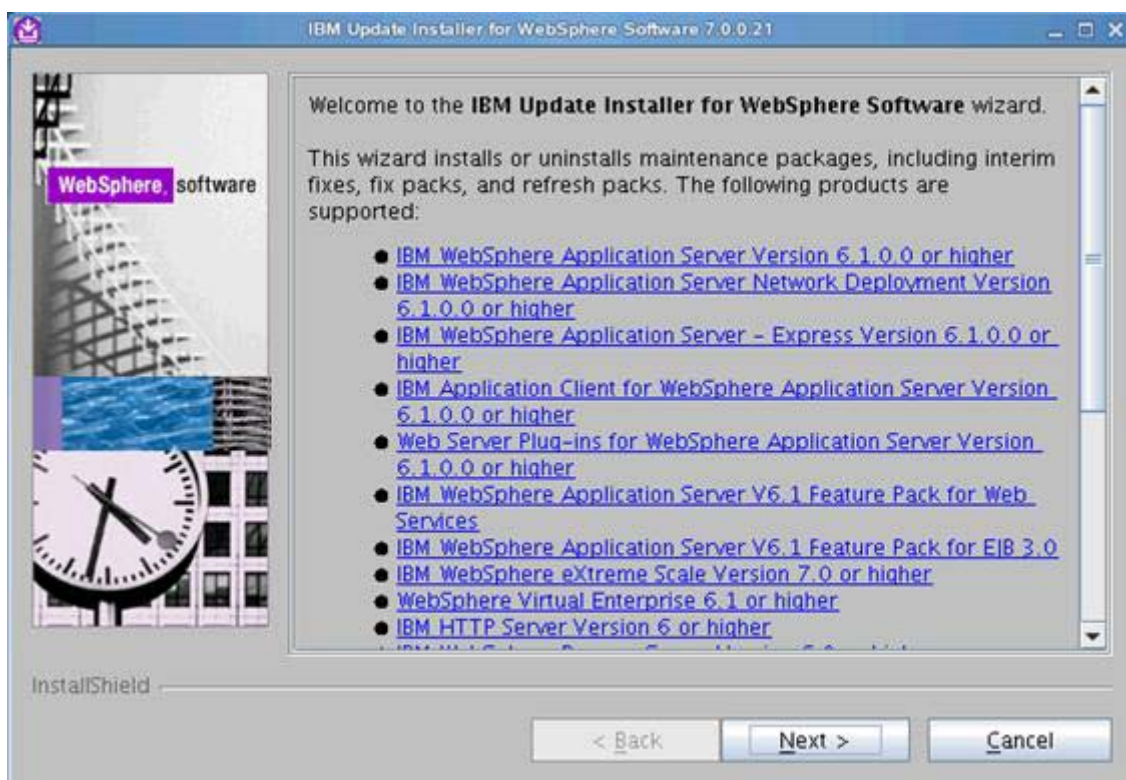


Figure 79. IBM Update Installer for WebSphere Software 7.0.0.21: Welcome

- ___ 5. Browse to the path of your Deployment Manager and select **Next**.



Figure 80. IBM Update Installer for WebSphere Software 7.0.0.21: Product selection

- ___ 6. Select **Install maintenance package** and click **Next**.



Figure 81. IBM Update Installer for WebSphere Software 7.0.0.21: Maintenance Operation Selection

___ 7. Browse to the path of your fix pack 21 files and click **Next**.

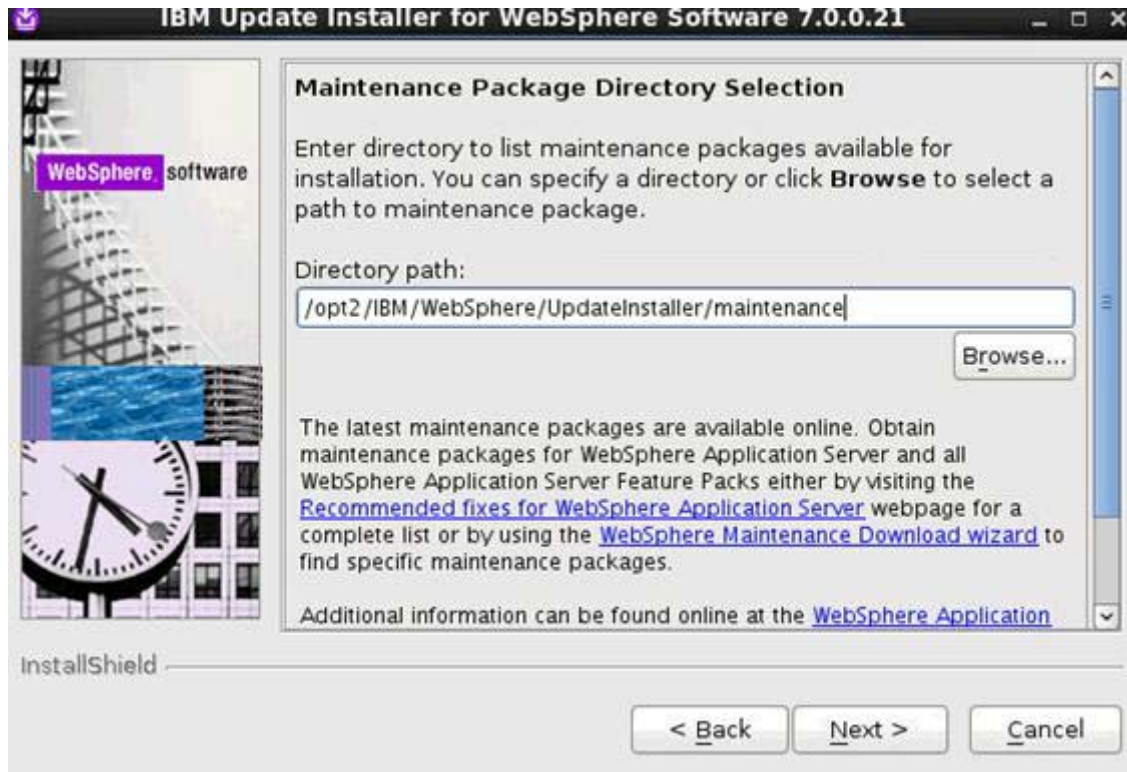


Figure 82. IBM Update Installer for WebSphere Software 7.0.0.21: Maintenance Package Directory Selection

- ___ 8. The installation picks up those two packages to be installed. Click **Next**.

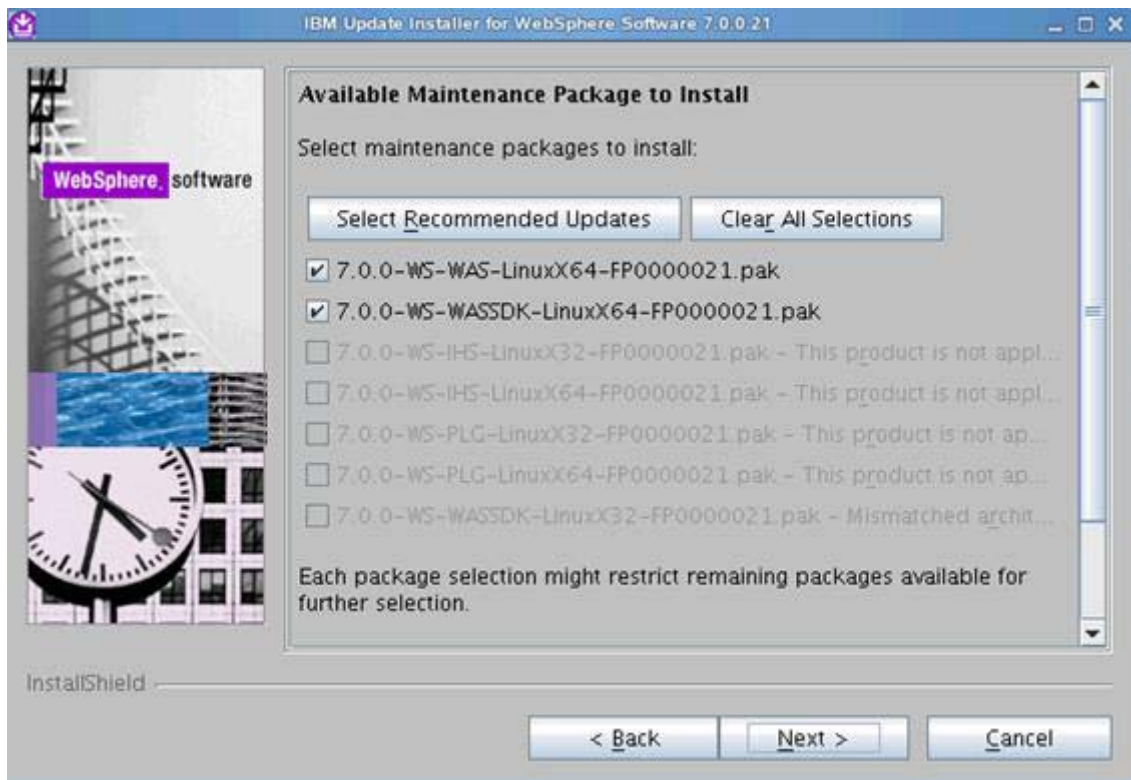


Figure 83. IBM Update Installer for WebSphere Software 7.0.0.21: Available Maintenance Package to Install

- ___ 9. Check the installation summary, select **Verify my permissions to perform the installation**, and click **Next** to continue.

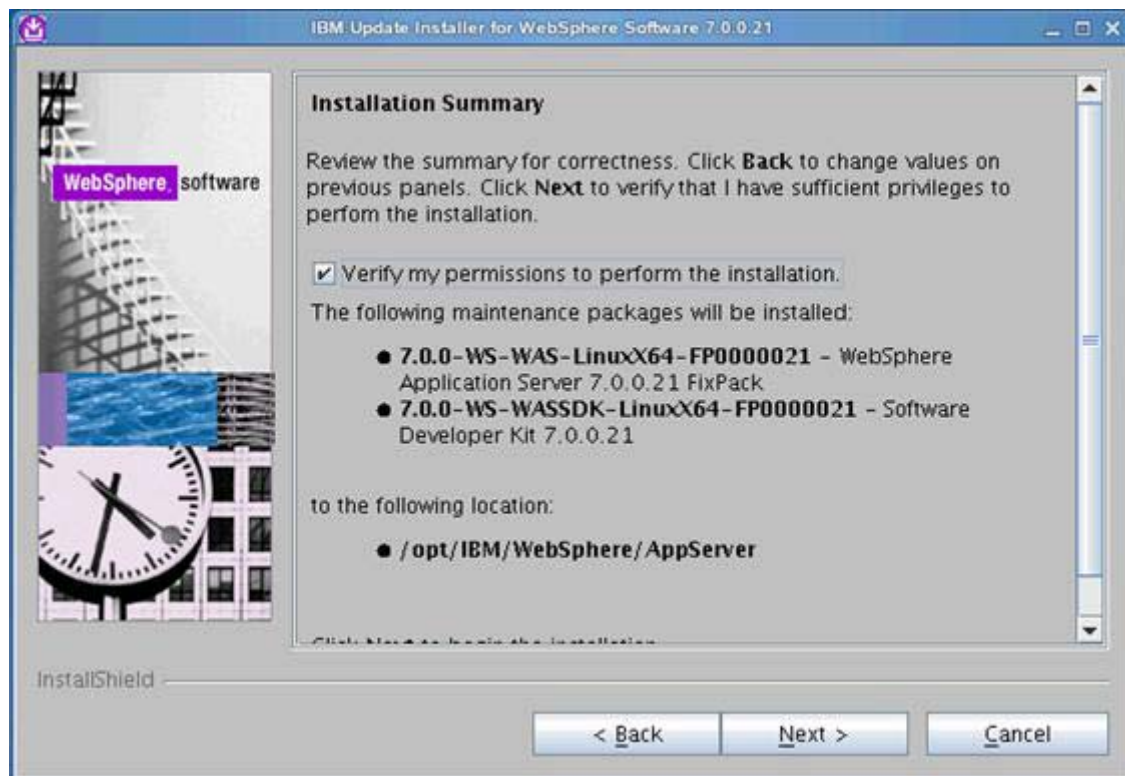


Figure 84. IBM Update Installer for WebSphere Software 7.0.0.21: Installation Summary

- ___ 10. The permissions verification begins. Click **Next** to continue when it completes.

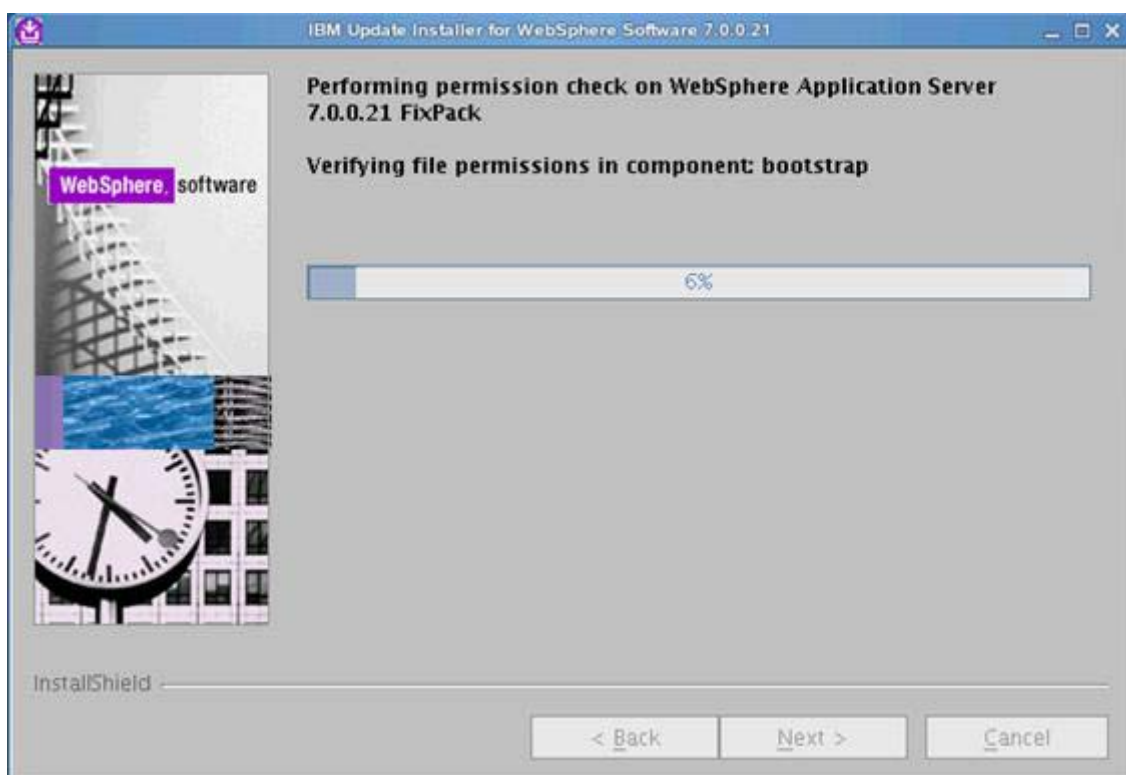


Figure 85. IBM Update Installer for WebSphere Software 7.0.0.21: Permissions verification in progress

___ 11. Click **Next** to begin the Installation.

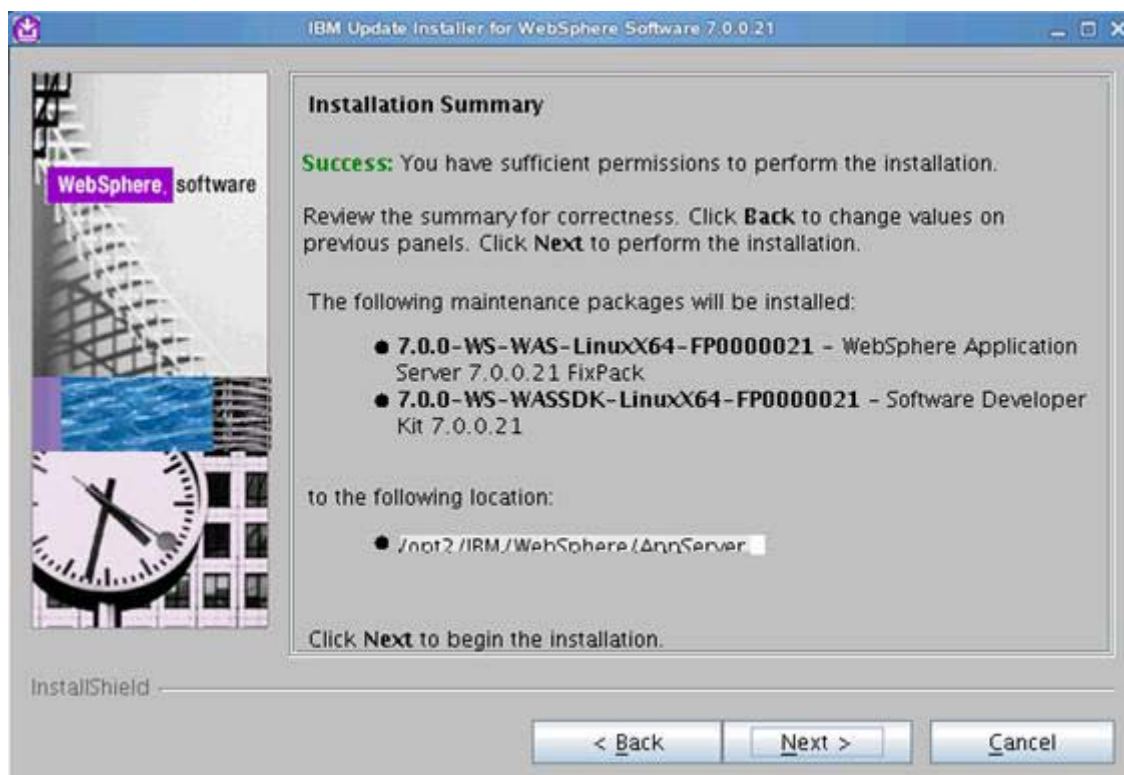


Figure 86. IBM Update Installer for WebSphere Software 7.0.0.21: Installation Summary

The installation begins.

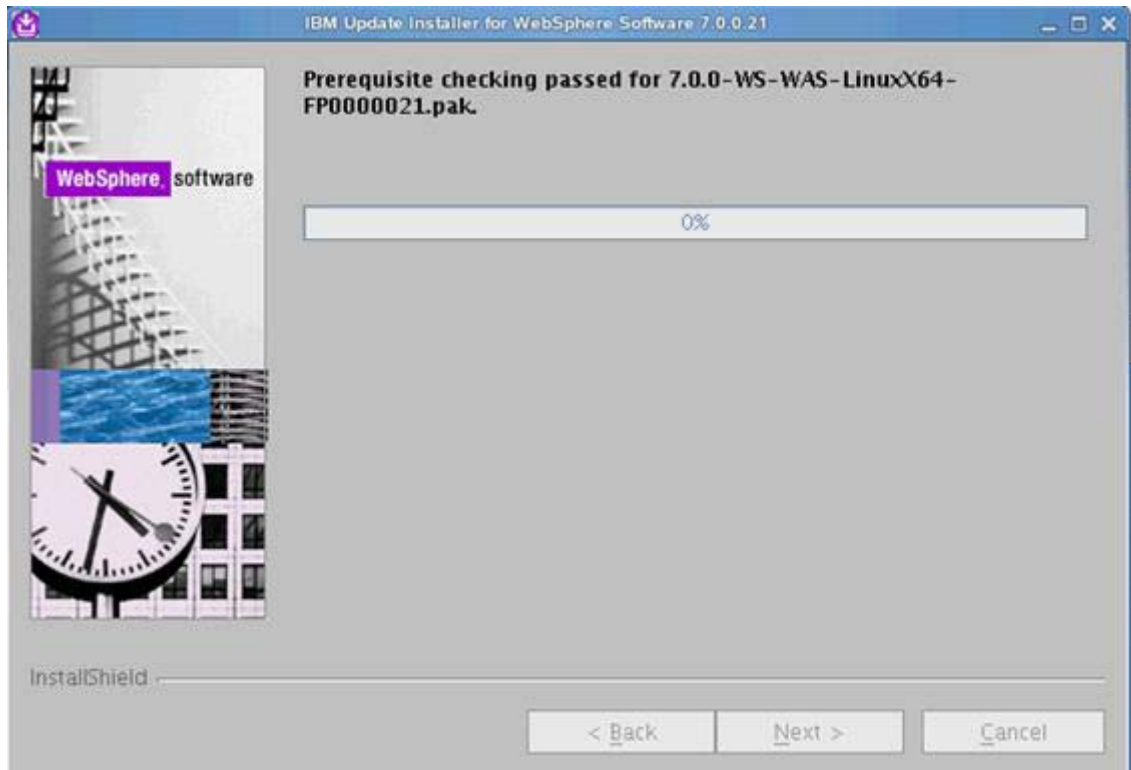


Figure 87. IBM Update Installer for WebSphere Software 7.0.0.21: Installation in progress

___ 12. Click **Finish** to exit the wizard when the installation completes.



Note

Now you must install the AppServers, IBM HTTP Server and IBM HTTP Server plug-ins. Follow the same steps. Just specify the location of each installed service.

5. Create shared content directory/content store

- ___ 1. Created a Folder `IC_Share` on Deployment Manager Appnodes, and share `IC_Share` folder from Deployment manager `/opt2/IBM/IC_Share` on Deployment Manager Appnodes.
- ___ 2. Update `/etc/fstab` `DM.Machine.example.com:/opt2/IBM/IC_Share/
/opt2/IBM/IC_Share nfs4` on Appnodes.
- ___ 3. Created exports on Deployment Manager:
`/opt2/IBM/IC_Share AppServer1.example.com(rw)`
`/opt2/IBM/IC_Share AppServer2.example.com(rw)`
- ___ 4. Server `nfs` restart on Deployment Manager, Appnodes.

6. Reuse content store/copy content store from 3.0.x shared data to IBM Connections 4.0 shared data

- ___ 1. Locate the content stores in your IBM Connections 3.0.1 deployment.
- ___ 2. Copy the 3.0.1 data to the corresponding content store in your IBM Connections 4.0 deployment.
- ___ 3. Use the following table as a guide to organizing the content stores.



Optional

The table excludes content that the Search application generates, such as indexes and statistics.

If you created more content stores, copy those content stores and the default content stores in the table. For Activities, for example, the content stores that you must copy are defined in the `objectStore` element of the `oa-config.xml` file.

Content store location
shared_content_store/audit
shared_content_store/activities/content
shared_content_store/blogs/upload
shared_content_store/customization
shared_content_store/dogear/favorite
shared_content_store/files/upload
shared_content_store/forums/content
shared_content_store/wikis/upload

7. Backing up IBM Connections before installing Connections 4.0

- ___ 1. Stop the IBM WebSphere® Application Server instances that are hosting IBM Connections.
- ___ 2. Using native database tools, back up the databases. If the update or migration fails, use this backup to restore the databases.



Information

For more information about backing up IBM Connections data, see the Backing up and restoring data topic.

- ___ 3. Back up the WebSphere Application Server Deployment Manager profile directory: [profile_root/Dmgr01](#). For example: \WebSphere\AppServer\profiles\dmgr.
- ___ 4. Back up your IBM Connections deployment.
 - ___ a. Create a backup of the IBM Connections installation directory: [connections_root](#).
 - ___ b. Create a backup of the WebSphere Application Server profile directory: [profile_root](#)



Note

If IBM Connections applications are deployed on separate profiles, archive each profile.

- ___ c. Create a backup of the `profileRegistry.xml` file, which is under [app_server_root/properties](#).
- ___ d. Back up the local and shared data directories:
 - [local_data_directory_root](#)
 - [shared_data_directory_root](#)
- ___ e. Back up the Shared Resources directory:
 - Linux: [shared_resources_root](#)



Optional

Back up the IBM Installation Manager data directory.

**Note**

This step is necessary only if you are planning an **in-place migration** of IBM Connections; that is, where you use the same systems to host the new deployment.

- Linux: `/var/ibm/InstallationManager`.
- AIX or Linux (non-root user): `/home/user/var/ibm/Installation Manager`.

8. Uninstalling a deployment before migration

1. Start the IBM Installation Manager.



Figure 88. IBM Installation Manager

___ 2. Click **Uninstall**.



Figure 89. IBM Installation Manager: Uninstall

___ 3. Select **Lotus Connections** and click **Next**.



Figure 90. IBM Installation Manager: Uninstall: Lotus Connections

- ___ 4. Check the summary information and click **Uninstall**.

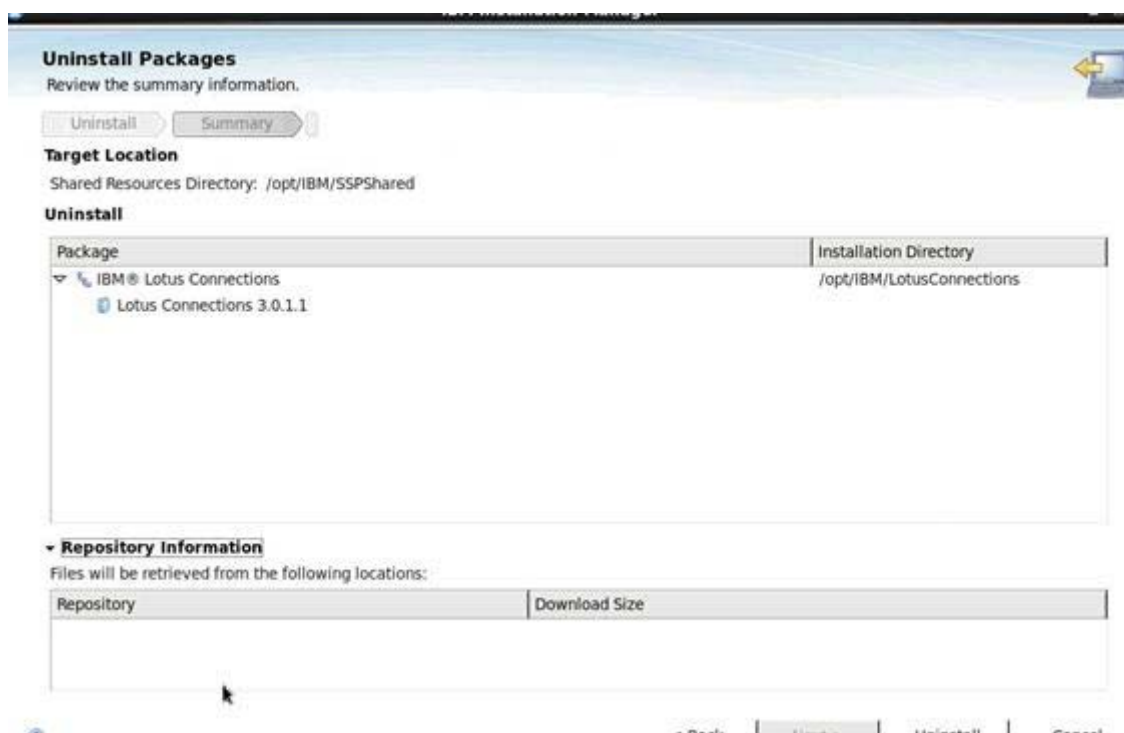


Figure 91. IBM Installation Manager: Uninstall: Summary information

The component unistall begins.



Figure 92. IBM Installation Manager: Uninstalling component

- ___ 5. When the uninstall completes, click **Finish** to exit the uninstaller.

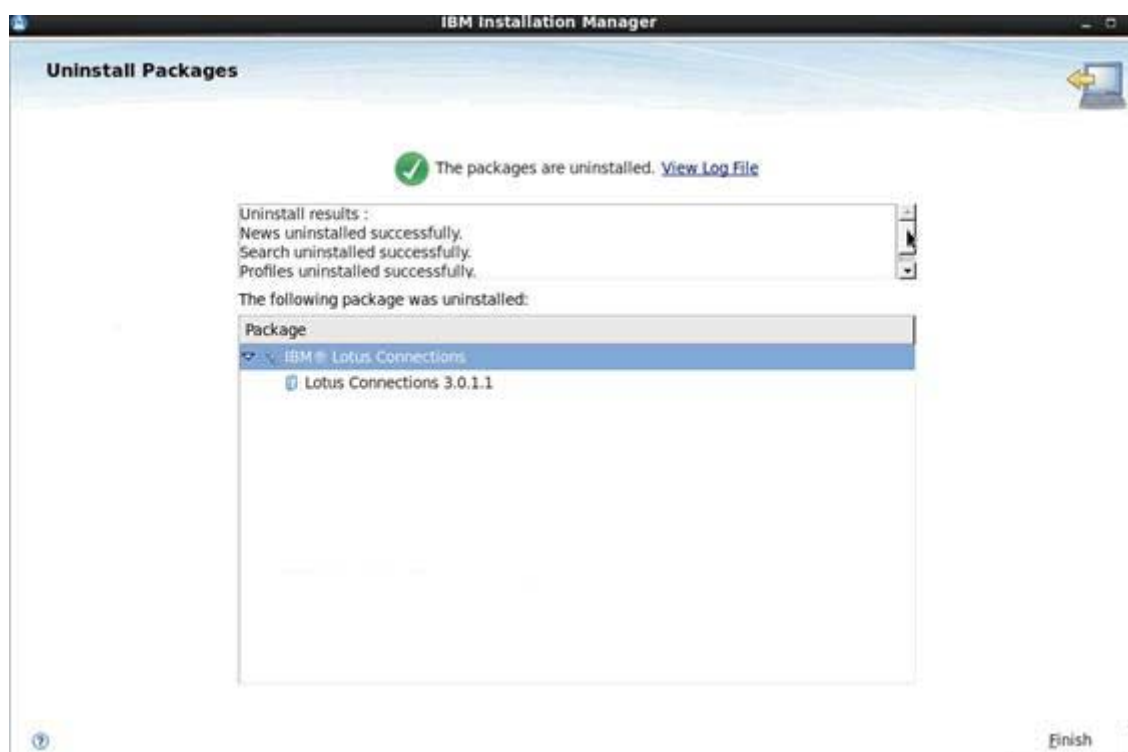


Figure 93. IBM Installation Manager: Uninstall complete

9. Install IBM Connections 4.0

- ___ 1. On each node, stop any running instances of WebSphere Application Server and WebSphere node agents.
- ___ 2. Start WebSphere Application Server Network Deployment Manager.
- ___ 3. Copy the installation files to the system that hosts the Deployment Manager.



Note

Ensure that the directory path that you enter contains no spaces.

- ___ 4. From the Connections setup directory, run the file to start the IBM Connections launchpad:
 - ___ a. Linux: `Connections set-up/launchpad.sh`.



Note

The launchpad needs a web browser to run. If your system does not have a web browser, install one.

Install a web browser

1. Click **Install IBM Connections 4.0.0**.



Figure 94. IBM Connections 4.0.0: Welcome

___ 2. Click **Launch the IBM connection 4.0.0 install wizard**.

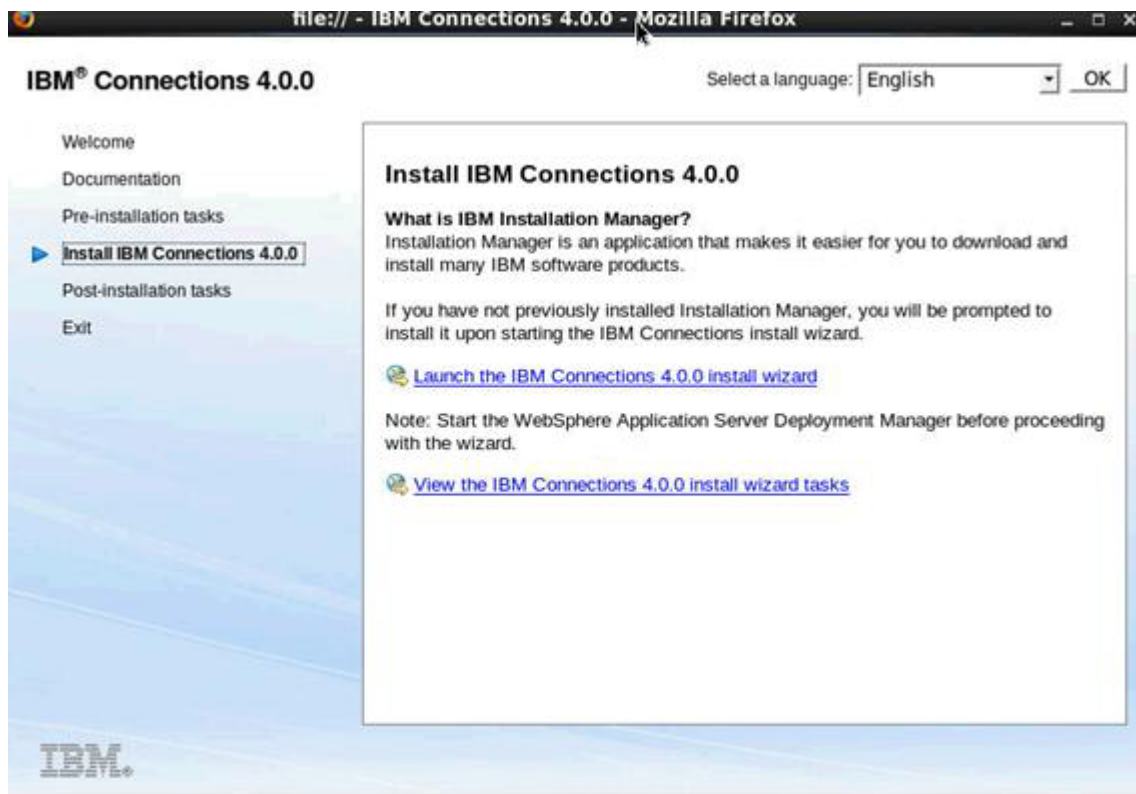


Figure 95. IBM Connections 4.0.0: Launch the IBM connection 4.0.0 installation wizard

The IBM Installation Manager opens.

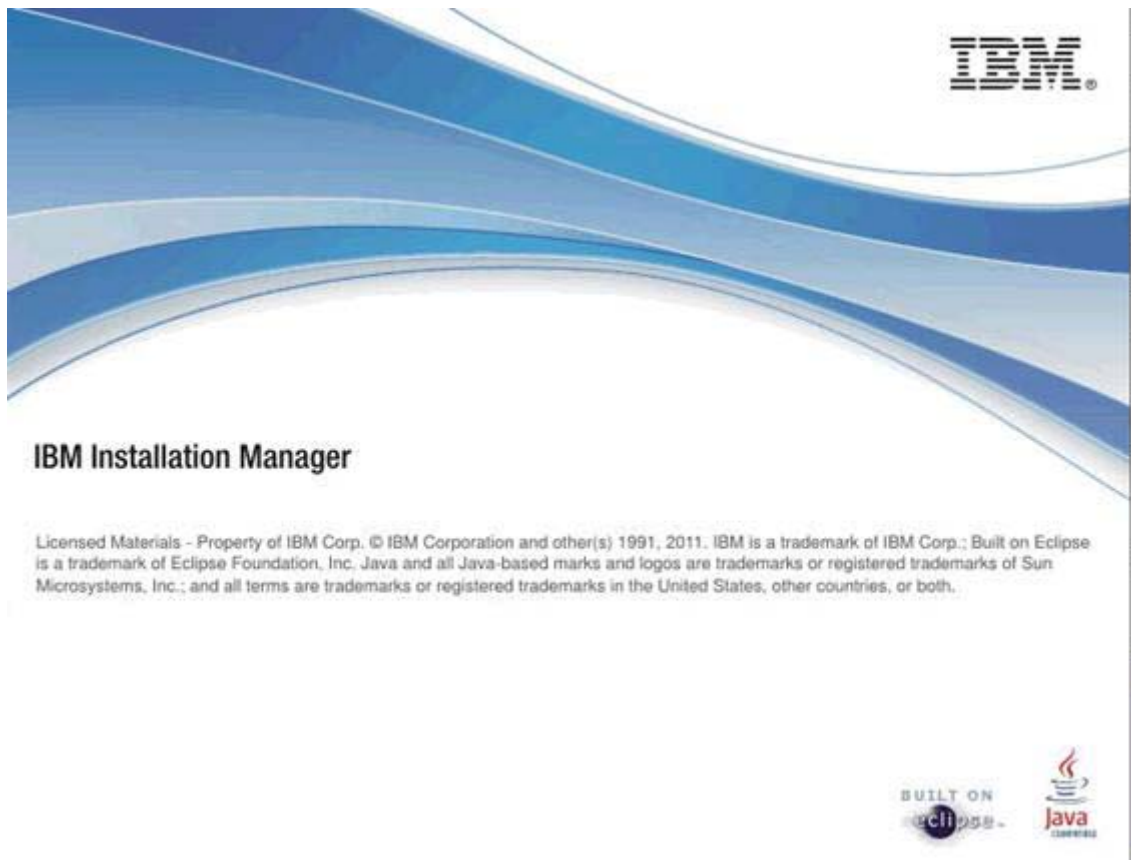


Figure 96. IBM Installation Manager

- ___ 3. A warning message is displayed. Package IBM Connections is already installed. Click **Continue**.



Figure 97. Warning message: Installed Packages

- ___ 4. Select the packages to install and click **Next**.



Figure 98. IBM Installation Manager: Install Packages

- ___ 5. Accept the license agreement and click **Next**.

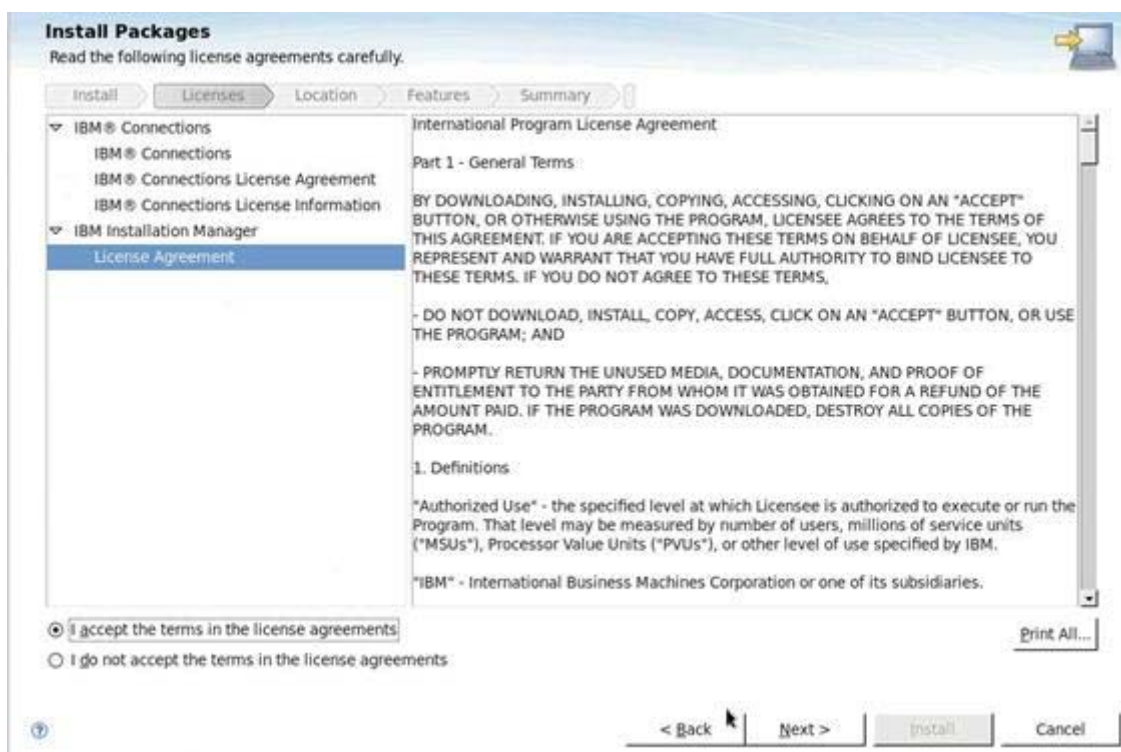


Figure 99. IBM Installation Manager: International Program License Agreement

- ___ 6. Select **Create a new package group** and change the default directory installation of IBM Connections 4.0 to `/opt2/IBM/Connections`. Then, click **Next**.

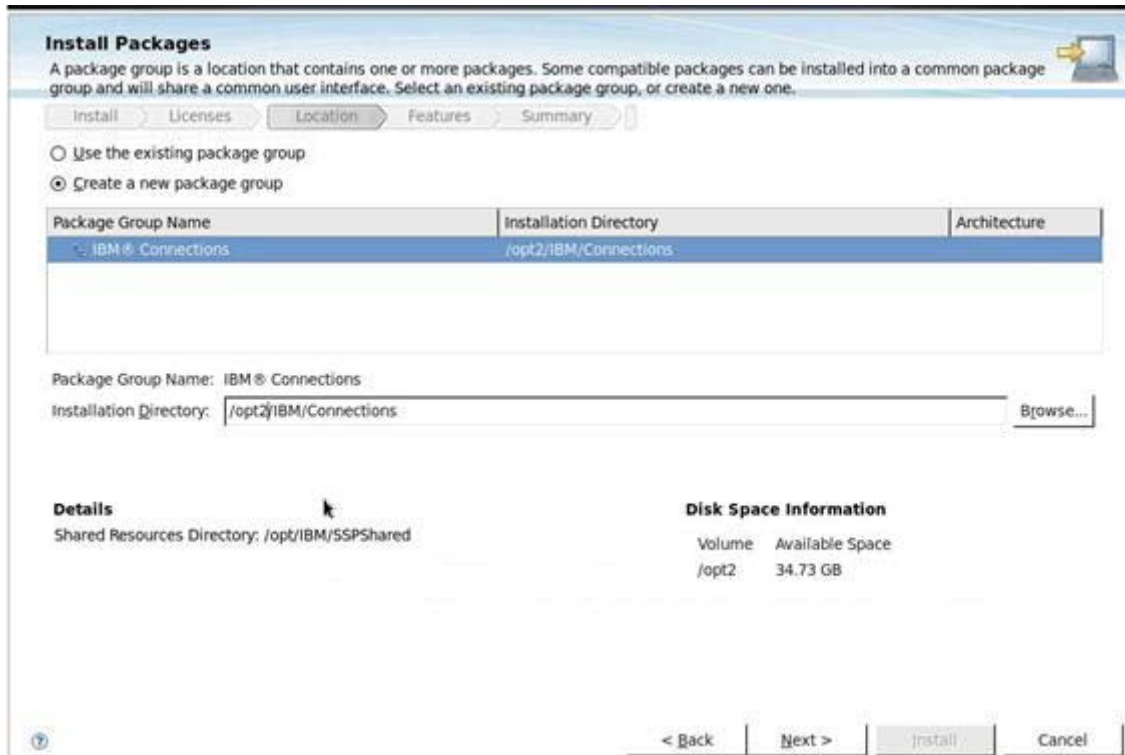


Figure 100. IBM Installation Manager: Installation Directory

- ___ 7. In the features to install, clear **Mobile** and **Metrics**.

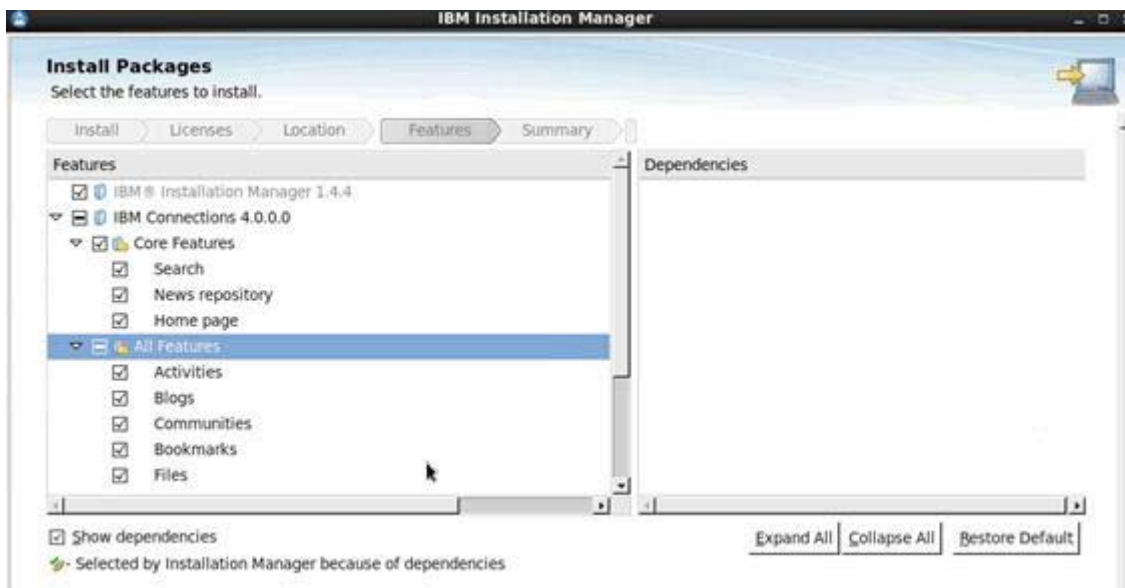


Figure 101. IBM Installation Manager: Features to install

- ___ 8. Enter the host name and the deployment manager credentials and click **Validate**.

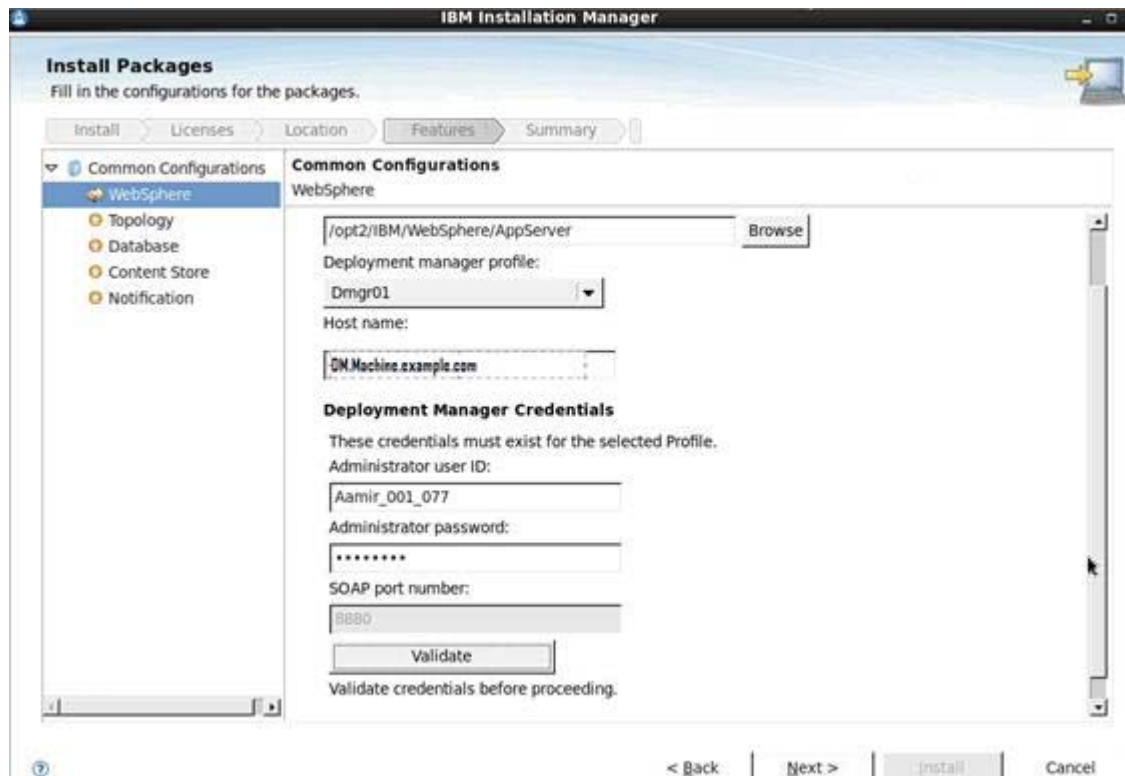


Figure 102. IBM Installation Manager: Common Configurations

- ___ 9. The validation is successful. Click **OK** to continue.



Figure 103. Validation information dialog

___ 10. Select **Medium: Applications grouped in several clusters** and click **Next**.



Figure 104. IBM Installation Manager: Topology

___ 11. The applications are grouped in several clusters. Click **Next** to continue.

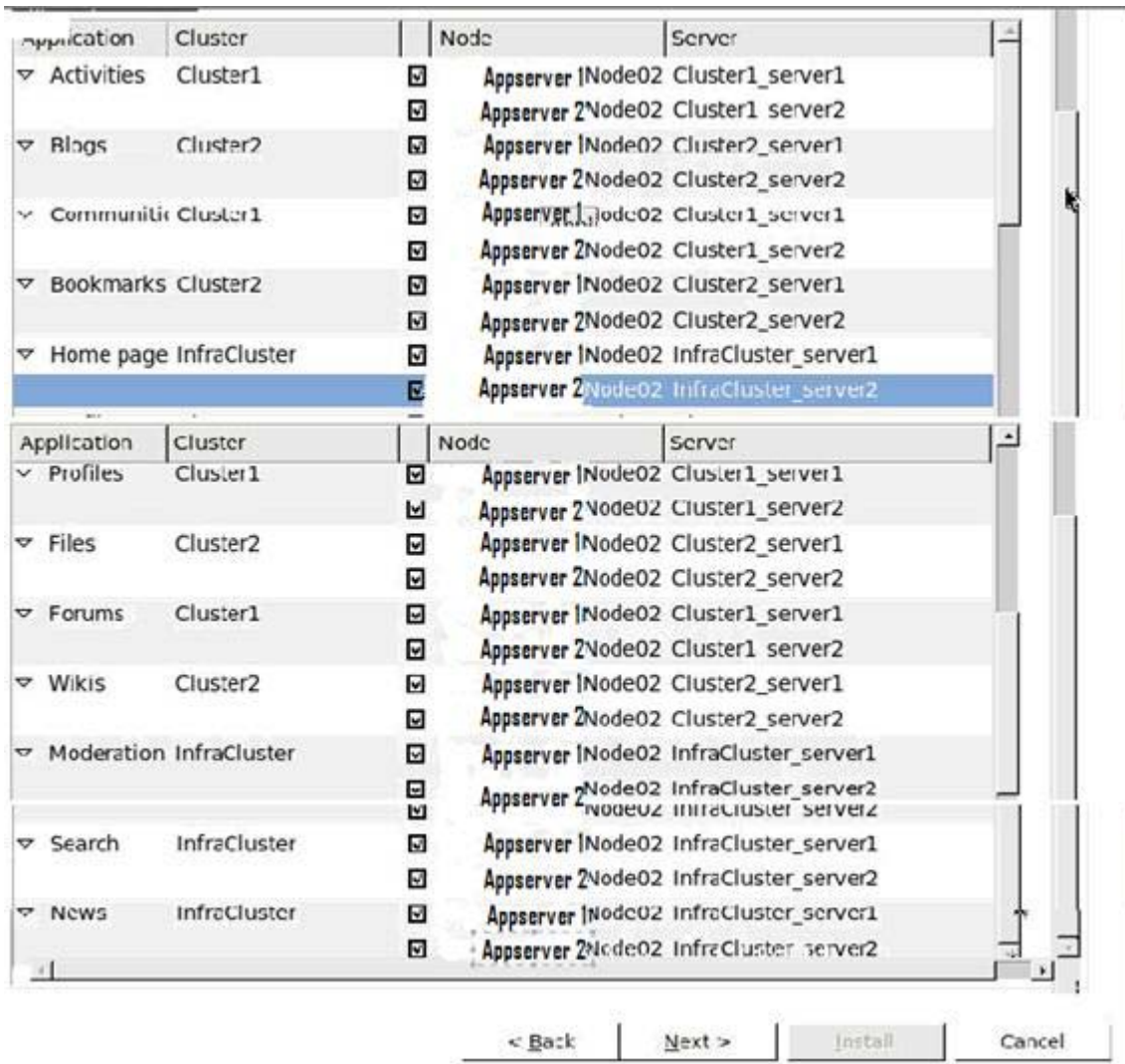


Figure 105. IBM Installation Manager: Applications grouped in several clusters

- ___ 12. Select **Yes, the applications are on the same database instance** and click **Next** to continue.

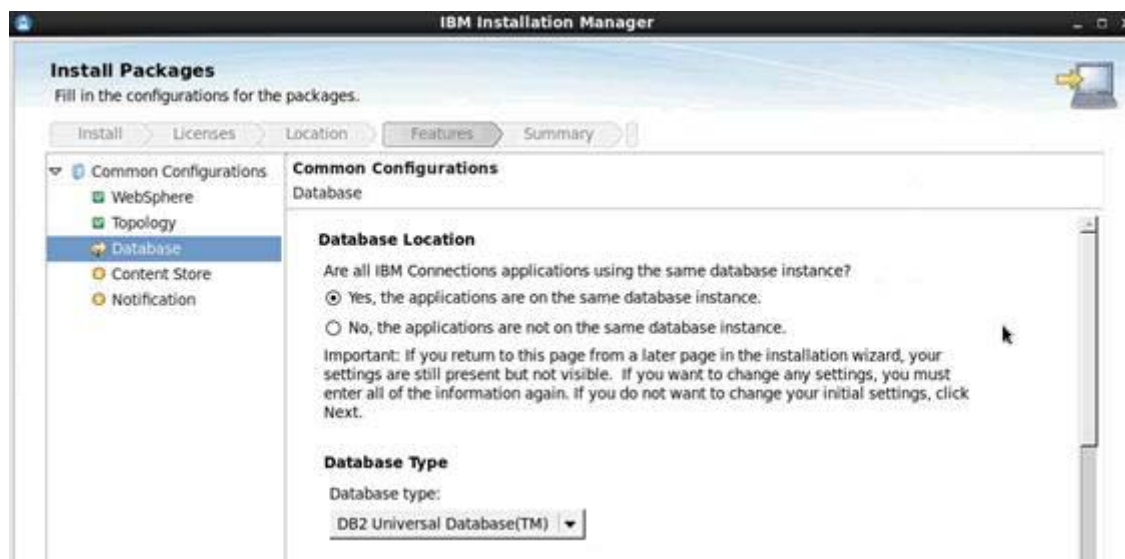


Figure 106. IBM Installation Manager: Database Location

- ___ 13. A database server information summary is displayed. Click **Validate**.

Database Server Information

Database server host name:

Port:

JDBC driver location:

Application Database Information

☒ Use the same password for all applications.

Application	Database Name	User ID	Password
Activities	OPNACT	LCUSER	*****
Blogs	BLOGS	LCUSER	*****
Communities	SNCOMM	LCUSER	*****
Bookmarks	DOGEAR	LCUSER	*****
Files	FILES	LCUSER	*****
Forums	FORUM	LCUSER	*****
Home page	HOMEPAGE	LCUSER	*****
Profiles	PEOPLEDDB	LCUSER	*****
Wikis	WIKIS	LCUSER	*****

< Back Next > [Install] Cancel

Figure 107. IBM Installation Manager: Validating the application database information

___ 14. The database server information starts to validate. Click **OK** when the validation finishes.

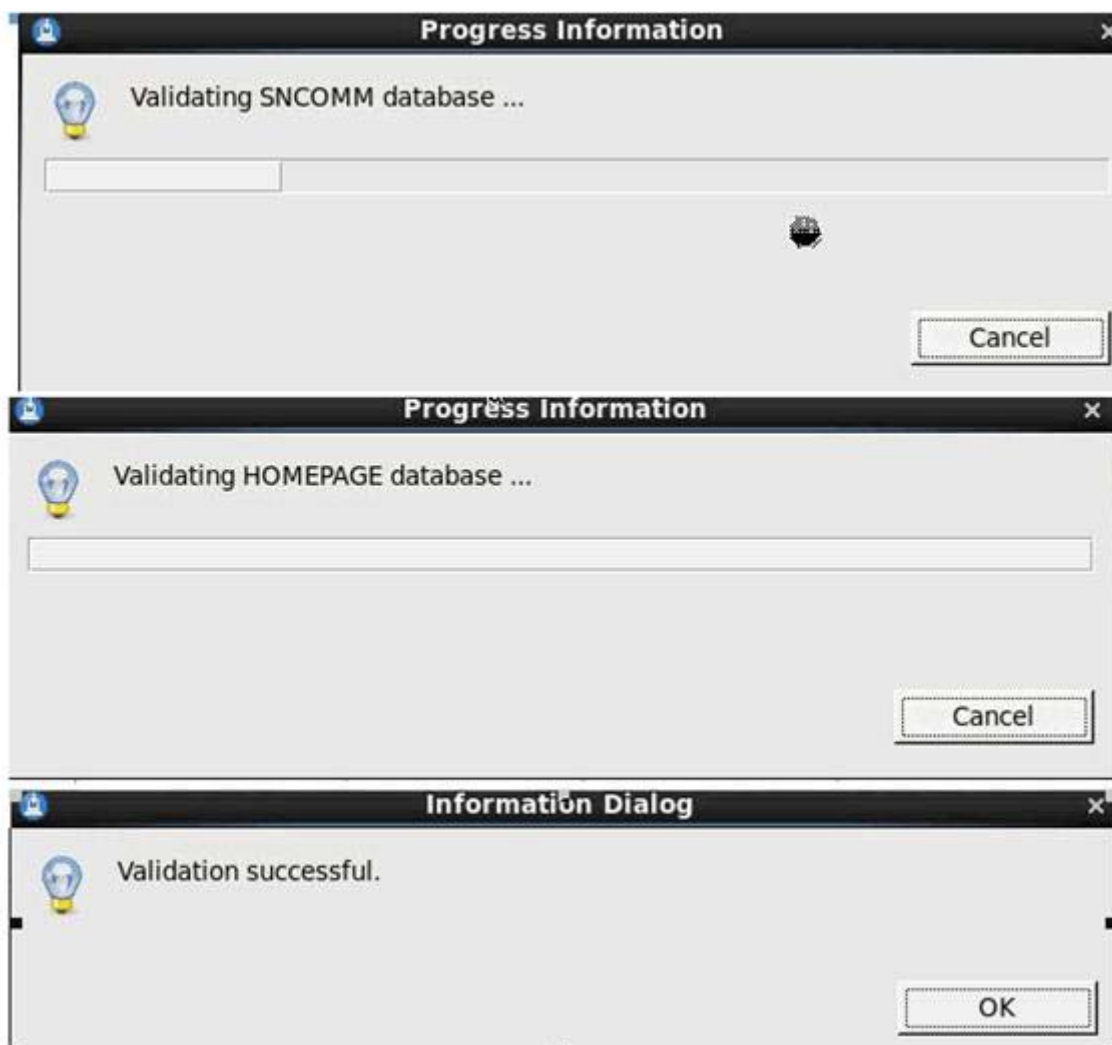


Figure 108. IBM Installation Manager: Application database information validation

- ___ 15. Select a network shared location and a local location. Then, click **Validate**.

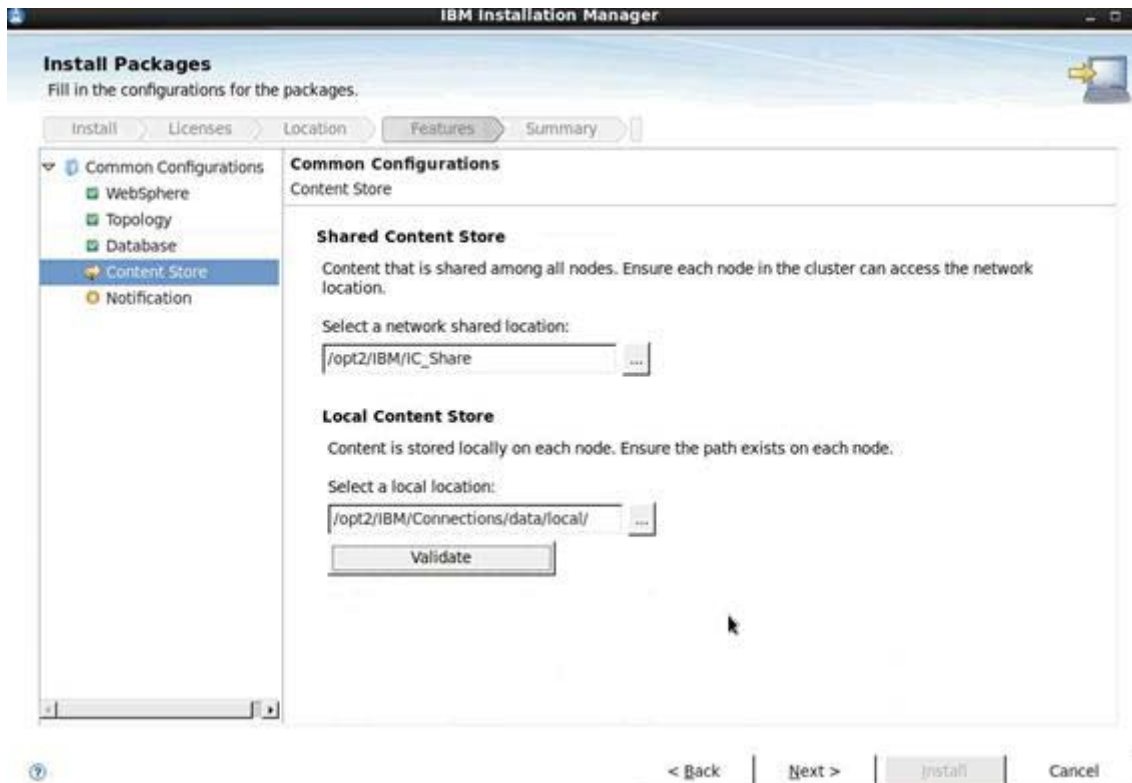


Figure 109. IBM Installation Manager: Shared location and local location

- ___ 16. The validation is successful. Click **OK** to continue.



Figure 110. Validation information dialog

___ 17. Do not enable any type of notification. Select **None** and click **Next**.

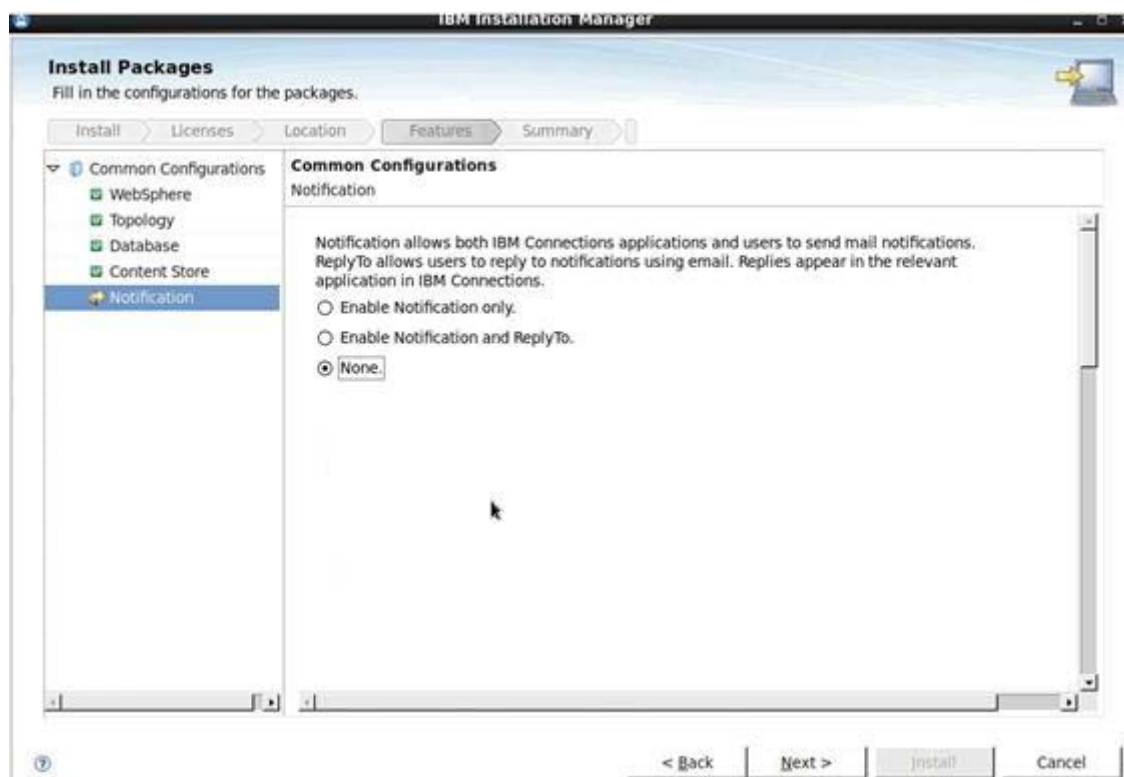


Figure 111. IBM Installation Manager: Notification

___ 18. Review the installation summary information and click **Install**.



Figure 112. IBM Installation Manager: Summary information (1 of 3)



Figure 113. IBM Installation Manager: Summary information (2 of 3)

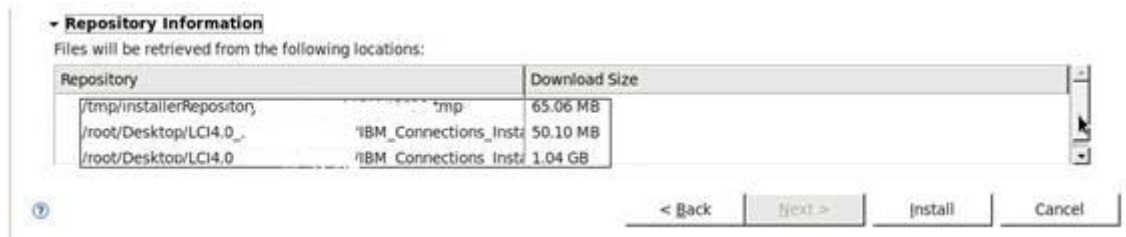


Figure 114. IBM Installation Manager: Summary information (3 of 3)

The installation begins.

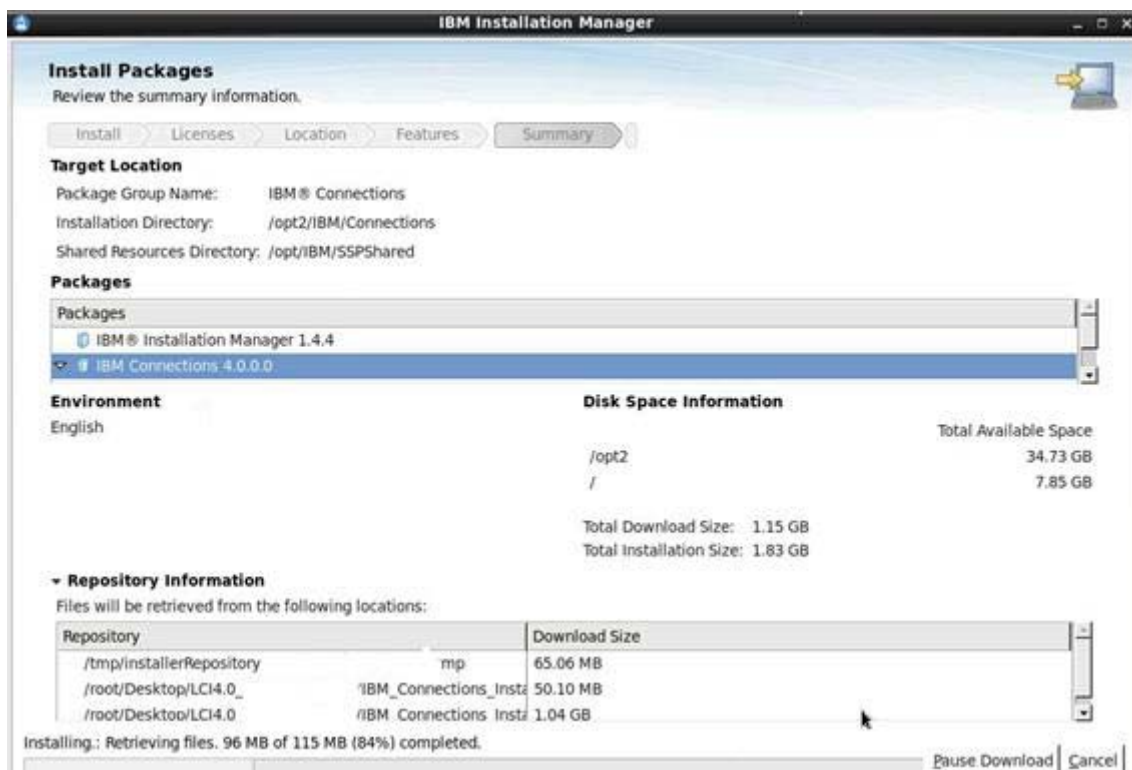


Figure 115. IBM Installation Manager: Installation in progress

___ 19. On installation completion, click **Finish** to exit the wizard.



Figure 116. IBM Installation Manager: Installation completed

10. Import applications that are exported from Lotus Connections 3.0.x

- ___ 1. Start the Deployment Manager in your IBM Connections 4.0 deployment.
- ___ 2. Copy the migration directory that you backed up from your 3.0.1 deployment to the [connections_root](#) directory in your 4.0 deployment.
- ___ 3. Import your 3.0.1 data. Open a command prompt, change to the migration directory on the Deployment Manager node in your 4.0 deployment, and run the following command:
 - ___ a. Linux: `./migration.sh lc-import -DDMuserid=dm_admin -DDMPasswd=dm_password`, where `dm_admin` is the administrative user ID for WebSphere® Application Server Deployment Manager and `dm_password` is the user password.



Note

Check the log file to validate the import. The log file is stored in the system user's home directory, and uses the following naming format: `lc-migration-yyyyMMdd_HHmm_ss.log`.

For example: `/root/lc-migration-20110215_1534_26.log`.

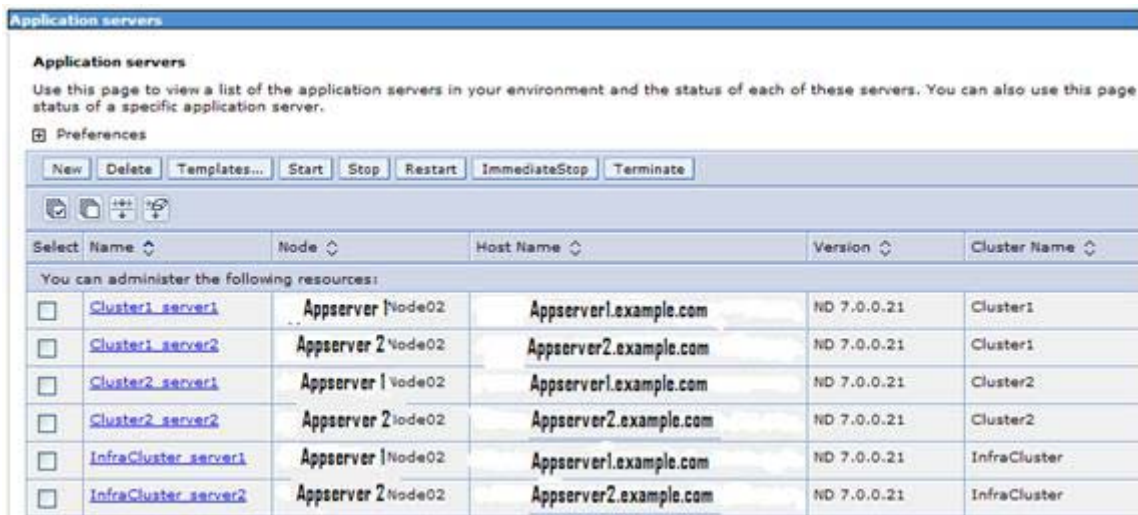
- ___ 4. If your deployment uses multiple nodes, synchronize the nodes.
- ___ 5. Verify `nodeagent SystemOut.log` on both nodes:

```
tail -f /opt2/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/nodeagent/SystemOut.log
00000156 AppBinaryProc I ADMA7021I: Distribution of application Dogear completed
successfully.
00000156 AppBinaryProc I ADMA7021I: Distribution of application Homepage completed
successfully.
00000156 AppBinaryProc I ADMA7021I: Distribution of application Common completed
successfully.
00000156 AppBinaryProc I ADMA7021I: Distribution of application Profiles completed
successfully.
00000156 AppBinaryProc I ADMA7021I: Distribution of application ibmasyncrsp
completed successfully.
00000156 AppBinaryProc I ADMA7021I: Distribution of application Help completed
successfully.
00000156 AppBinaryProc I ADMA7021I: Distribution of application Wikis completed
successfully.
00000156 AppBinaryProc I ADMA7021I: Distribution of application WidgetContainer
completed successfully.
00000157 NodeSyncTask A ADMS0003I: The configuration synchronization completed
successfully.
00000156 AppBinaryProc I ADMA7021I: Distribution of application Files completed
successfully.
```

11. Post-installation steps

Update JVM settings

- ___ 1. Log in to the WebSphere® Application Server Integrated Solutions Console and select **Servers > Server Type > WebSphere application servers**.
- ___ 2. Click <server>, where <server> is the name of an IBM Connections server. You might have several servers in your deployment, so you might need to repeat these steps for each server.
- ___ 3. In the Server Infrastructure area, click **Java and Process Management** and then click **Process Definition > Java Virtual Machine**.



Select	Name	Node	Host Name	Version	Cluster Name
<input type="checkbox"/>	Cluster1_server1	Appserver 1 Node02	Appserver1.example.com	ND 7.0.0.21	Cluster1
<input type="checkbox"/>	Cluster1_server2	Appserver 2 Node02	Appserver2.example.com	ND 7.0.0.21	Cluster1
<input type="checkbox"/>	Cluster2_server1	Appserver 1 Node02	Appserver1.example.com	ND 7.0.0.21	Cluster2
<input type="checkbox"/>	Cluster2_server2	Appserver 2 Node02	Appserver2.example.com	ND 7.0.0.21	Cluster2
<input type="checkbox"/>	InfraCluster_server1	Appserver 1 Node02	Appserver1.example.com	ND 7.0.0.21	InfraCluster
<input type="checkbox"/>	InfraCluster_server2	Appserver 2 Node02	Appserver2.example.com	ND 7.0.0.21	InfraCluster

Figure 117. Application servers

- ___ 4. Review the maximum heap size. IBM Installation Manager sets the following values for Small and Medium deployments. Make sure that the maximum heap size is set to 2048.



Note

Ensure that you are not allocating more memory than the physical capacity of the system where the JVM is installed.

- ___ 5. Adjust the current values of the heap size up or down to suit the needs of your deployment and your hardware capabilities.



Figure 118. Configuring Java Virtual Machine

- ___ 6. Click **OK** and then click **Save**.

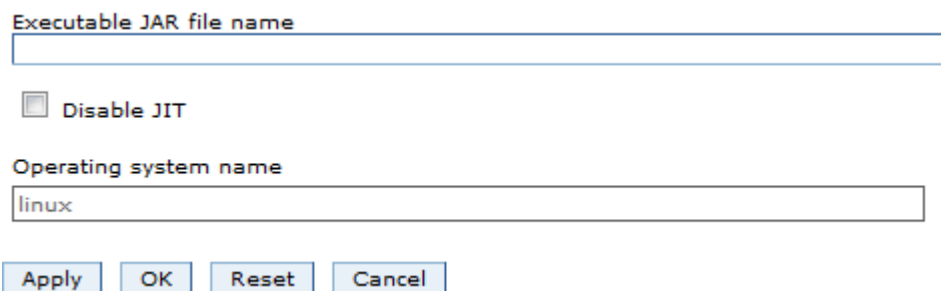


Figure 119. Saving the changes applied

- ___ 7. Repeat these steps for any additional servers in your deployment.

Setting path variables for search



Note

This task is needed only for non-Windows platforms.

During the installation, you set `/opt2/IBM/LC_Share` which then set `/opt2/IBM/LC_Share/search/stellent/dcs/oiexport` as the location for the stellent converters.

In a multi-node cluster, it is recommended to run this on the nodes themselves and not the shared area.

- ___ 1. Create a copy of the folder `/opt2/IBM/LC_Share/search/stellent` to `/opt2/IBM/Connections/stellent` on both nodes in your cluster. Change the rights on the folder to 777.
- ___ 2. Set up that share and then go to **Environment > WebSphere Variables** and `FILE_CONTENT_CONVERSION`. Change the path from the shared area to the local area on your nodes. This path should be the same across both nodes.

You can administer the following resources:

<input type="checkbox"/>	FILES_CONTENT_DIR	/opt2/IBM/LC_Share/files/upload	Cell= DM.Machine Cell02
<input type="checkbox"/>	FILES_EVENT_CONTENT_DIR	\${FILES_CONTENT_DIR}	Cell= DM.Machine Cell02
<input type="checkbox"/>	FILE_CONTENT_CONVERSION	/opt2/IBM/Connections/stellent/dcs/oiexport/exporter	Cell= DM.MachineCell02

Total 3 Filtered total: 3

Figure 120. File content conversion

- ___ 3. Then, add `/opt2/IBM/Connections/stellent/dcs/oiexport` to your `PATH` variable in the `.bash_profile` for the root user.
- ___ 4. Add export `LD_LIBRARY_PATH=/opt/IBM/LotusConnections/stellent/dcs/oiexport` to `/opt/IBM/WebSphere/AppServer/bin/setupCmdLine.sh`.
- ___ 5. Run `./setupCmdLine.sh` before you start the nodes.
- ___ 6. To check that `LD_LIBRARY_PATH` is checked, enter `echo $LD_LIBRARY_PATH`.



Note

This must be done on all nodes of your cluster.

- ___ 7. Restart the computer to make sure that the variables take effect.

**Information**

For more information about this topic, see

http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Copying_Search_conversion_tools_to_local_nodes_ic40&content=pdcontent.

Configuring the HTTP server

The next section is about HTTP configuration and must be completed as HTTP is required for Login by default on Connections.



Important

Before beginning this task, ensure that the IBM HTTP Administration server is started. The admin server must be started to synchronize configuration files between the HTTP Server and the Deployment Manager.



Linux

Go to the HTTPServer/bin directory and issue the command `./adminctl start`.

Add web server as unmanaged node

- ___ 1. After the administration server is started, open the Deployment Manager and add the web server to the cell as an unmanaged node. Open the administrative console at `https://DM.Machine.example.com:9044/admin`.
- ___ 2. Go to **System administration > Nodes** and click **Add Node**.

Nodes

Use this page to manage nodes in the application server environment. A node corresponds to a physical computer. The following table lists the managed and unmanaged nodes in this cell. The first node is the deployment manager. Clicking Add Node.

Preferences

Add Node				Remove Node		Force Delete		Synchronize		Full Resynchronize		Stop	
Select	Name	Host Name		Version									
You can administer the following resources:													

Figure 121. System administration > Nodes: Add Node

- ___ 3. Select **Unmanaged node** and click **Next**.

Use this page to add either a managed or an unmanaged node.

☐ Managed node
Specifies the creation of a managed node. A managed node contains an application server process that runs within the deployment manager cell. The managed node is associated with a node agent process that maintains the configuration for the node and controls its operation. Choosing this option results in running the add node utility to federate an existing standalone application server.

☒ Unmanaged node
Specifies the creation of an unmanaged node. An unmanaged node represents a node in the topology that does not have an application server process or a node agent process. Unmanaged nodes are for other server processes, such as Web servers that exist on their own node in the topology.

Next Cancel

Figure 122. Unmanaged node

- ___ 4. Provide a name and host name for the HTTP server and click **OK**.

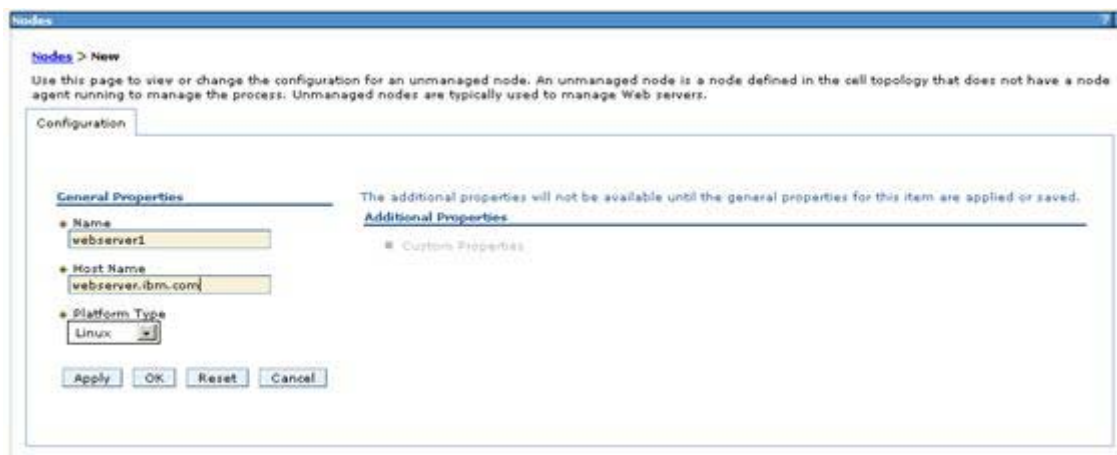


Figure 123. Entering a name and host name for the HTTP server

- ___ 5. Click **Save**.

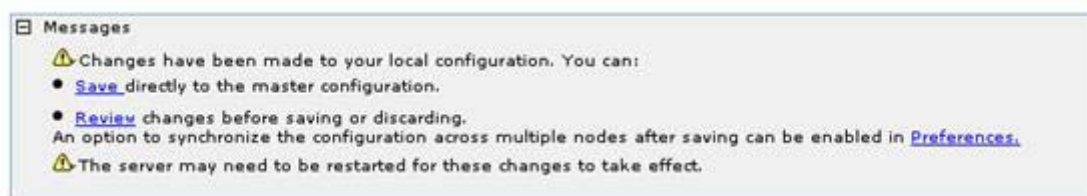


Figure 124. Messages: Save

On the Nodes panel, the web server is displayed in the list.

<input type="checkbox"/>	webserver1	DM.Machine.example.com	Not applicable	TCP
--------------------------	----------------------------	------------------------	----------------	-----

Figure 125. Node panel

Add web server as a server

1. Next, go to **Servers > Server Types > Web servers** add the web server as a server in the configuration and click **New**.

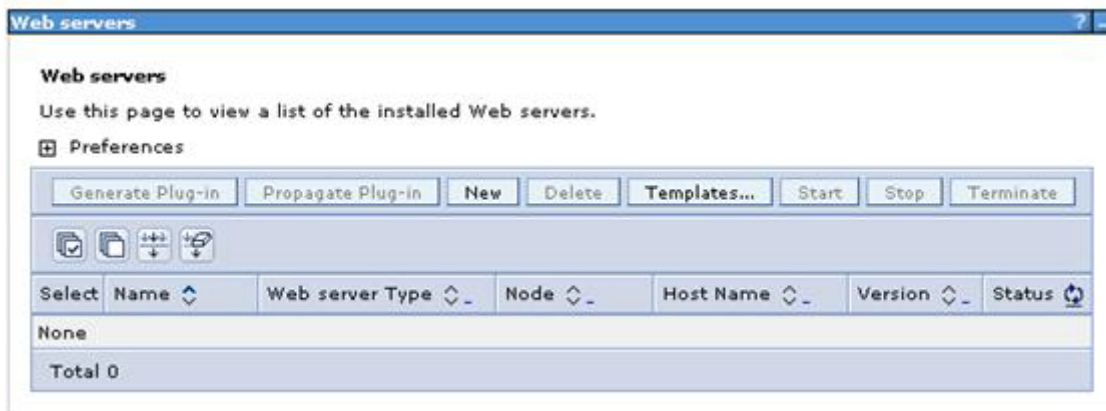


Figure 126. Web servers

2. Select the web server node and provide the name of this server as `webserver1`. This name is the same name that is provided during the plug-ins installation on the web server. Select **IBM HTTP Server** as the type. Click **Next** to continue.

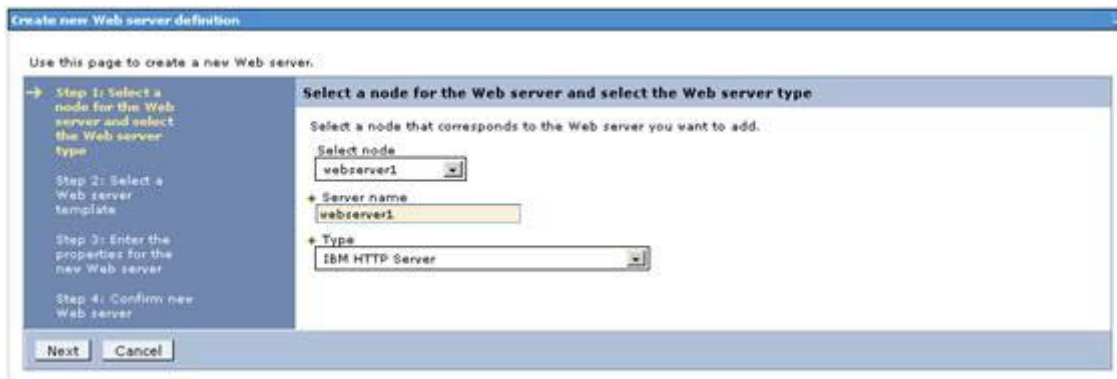


Figure 127. Defining the new web server

- ___ 3. Leave the web server template as default and click **Next**.

Use this page to create a new Web server.

Step 1: Select a node for the Web server and select the Web server type

→ Step 2: Select a Web server template

Step 3: Enter the properties for the new Web server

Step 4: Confirm new Web server

Select a Web server template

Select the template that corresponds to the server that you want to create.

Select	Template Name	Type	Description
<input checked="" type="radio"/>	IHS	System	The IHS Web Server Template

Previous Next Cancel

Figure 128. Web server template

- ___ 4. Enter the web server properties and click **Next**.

Use this page to create a new Web server.

Step 1: Select a node for the Web server and select the Web server type

Step 2: Select a Web server template

→ Step 3: Enter the properties for the new Web server

Step 4: Confirm new Web server

Enter the properties for the new Web server

Enter the Web server properties.

- Port: 90
- Web server installation location: /opt2/IBM/HTTPServer
- Plug-in installation location: /opt2/IBM/HTTPServer/Plugins
- Application mapping to the Web server: All

Enter the IBM Administration Server properties.

- Administration Server Port: 9008
- Username: ihadmin
- Password: *****
- Confirm password: *****
- ☐ Use SSL

Previous Next Cancel

Figure 129. Web server properties

___ 5. Click **Finish** to confirm the new web server.



Figure 130. Confirming new web server

___ 6. Click **Save**.

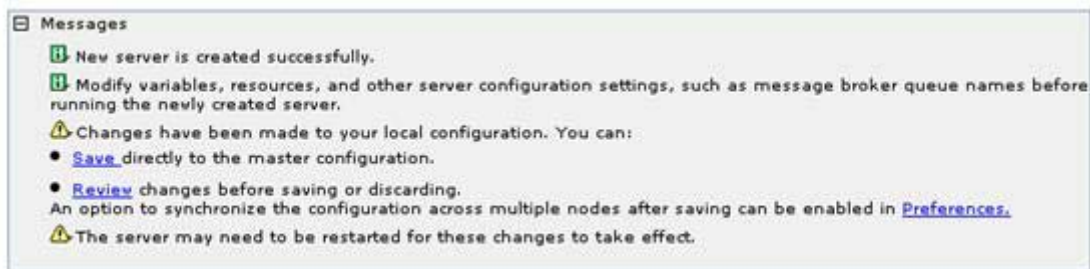


Figure 131. Messages: Save

The following screen is displayed again.



Figure 132. Web servers

___ 7. Perform a **Full Resynchronize** between nodes in the deployment.

- ___ 8. Return to **Servers: Server Types: Web Servers**. Select the box next to `webserver1` and click **Generate Plug-in**.



Figure 133. Web servers

- ___ 9. Click **webserver1**.



Figure 134. Administering the web server

___ 10. Then, click **Plug-in properties**.

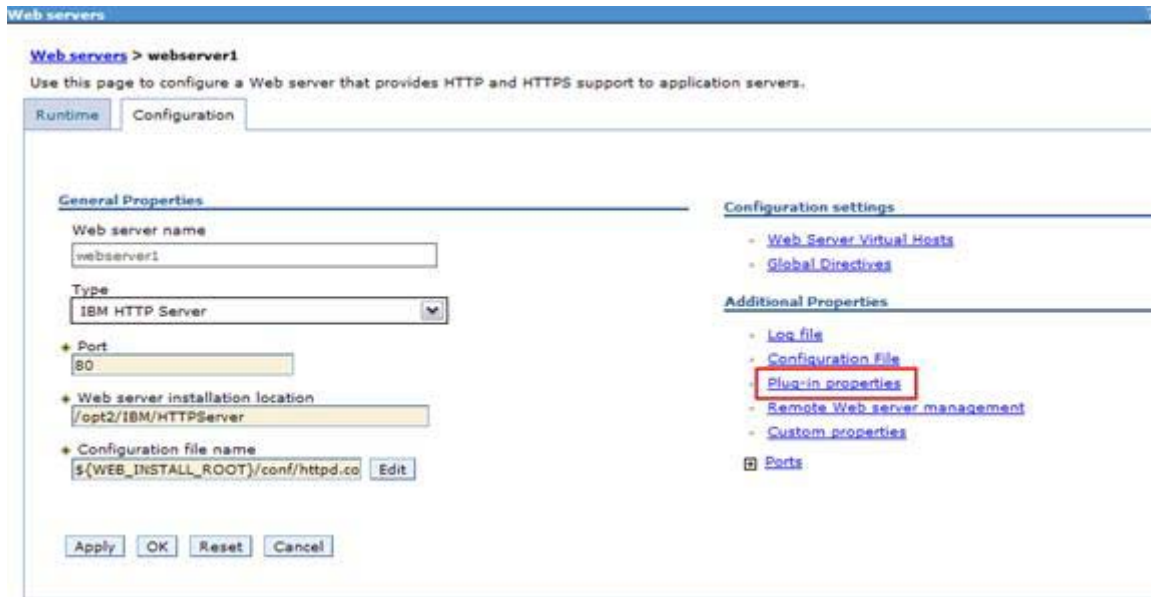


Figure 135. Additional Properties: Plug-in properties

___ 11. Click **Copy to Web server key store directory**.



Figure 136. Repository copy of web server plug-in file

___ 12. The following message is displayed to indicate the successful copy of these keys. Again, restart the web server for the plug-in changes to take effect.



Figure 137. Message: Successful copy of the keys

Configuring IBM HTTP Server for SSL

To support SSL, create a self-signed certificate and then configure IBM HTTP Server for SSL traffic. If you use this certificate in production, users might receive warning messages from their browsers. In a typical production deployment, you would use a certificate from a trusted certificate authority.

- ___ 1. The first step is to create a key file. Start the iKeyman utility by double-clicking the file `ikeyman.sh` (default directory for this file is `/opt2/IBM/HTTPServer/bin`). The following panel is displayed when you run this utility

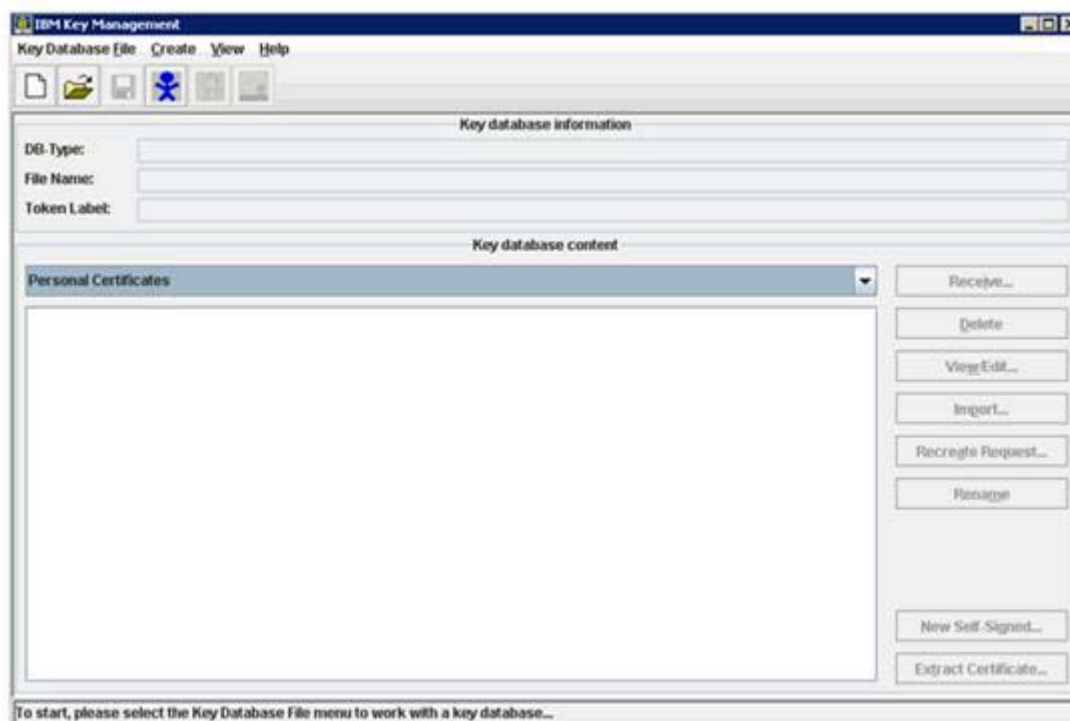


Figure 138. Starting IBM Key Management

- ___ 2. Select **Key Database File: New...**

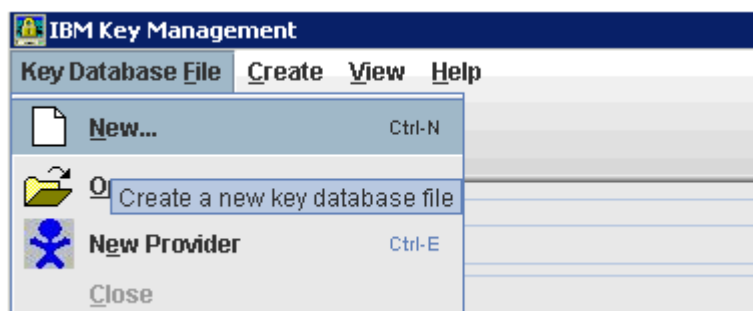


Figure 139. Creating a database file

- ___ 3. Ensure that the key database type is selected as CMS. Input a name for the key file and location to store it.

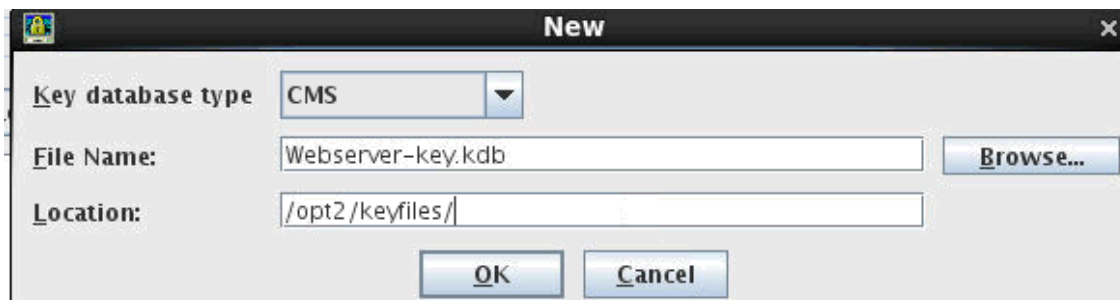


Figure 140. Key database type, file name, and location

- ___ 4. Enter a password and select **Stash password to a file**.

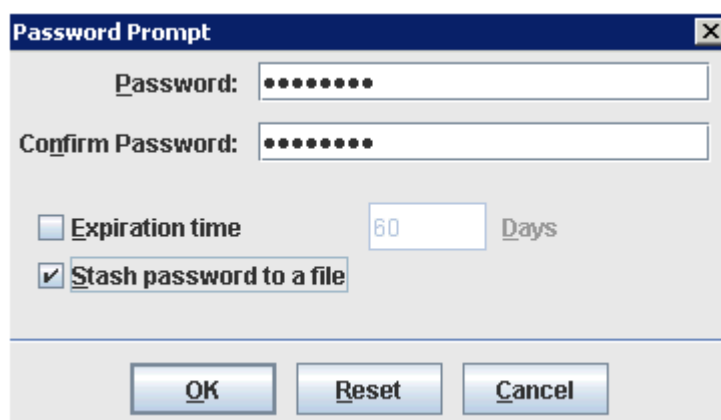


Figure 141. Password prompt

You turn back to the iKeyman panel with the `webserver-key.kdb` opened.



Figure 142. IBM Key Management

- ___ 5. Now create a self-signed certificate by using **Create > New Self-Signed Certificate...**

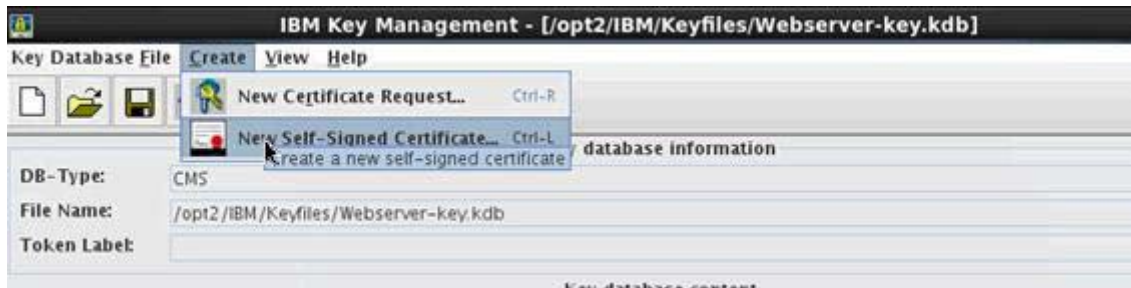


Figure 143. Creating a self-signed certificate

- ___ 6. Input the label and other details as appropriate. Click **OK** to save the certificate.

 The screenshot shows the 'Create New Self-Signed Certificate' dialog box. It contains the following fields and options:

- Key Label:** Text field containing 'SelfSignedCertificate'.
- Version:** Dropdown menu set to 'X509 V3'.
- Key Size:** Dropdown menu set to '1024'.
- Signature Algorithm:** Dropdown menu set to 'SHA1WithRSA'.
- Common Name (optional):** Text field containing 'DM.Machine.example.com'.
- Organization (optional):** Empty text field.
- Organizational Unit (optional):** Empty text field.
- Locality (optional):** Empty text field.
- State/Province (optional):** Empty text field.
- Zipcode (optional):** Empty text field.
- Country or region (optional):** Dropdown menu with a small flag icon.
- Validity Period:** Text field containing '365' followed by 'Days'.

 At the bottom are three buttons: 'OK', 'Reset', and 'Cancel'.

Figure 144. Providing label and other details to the self-signed certificate

Configure the web server for SSL

1. Stop the IBM HTTP Server, if started. When you verified that it is stopped, log in to the administrative console and configure the web server for SSL.

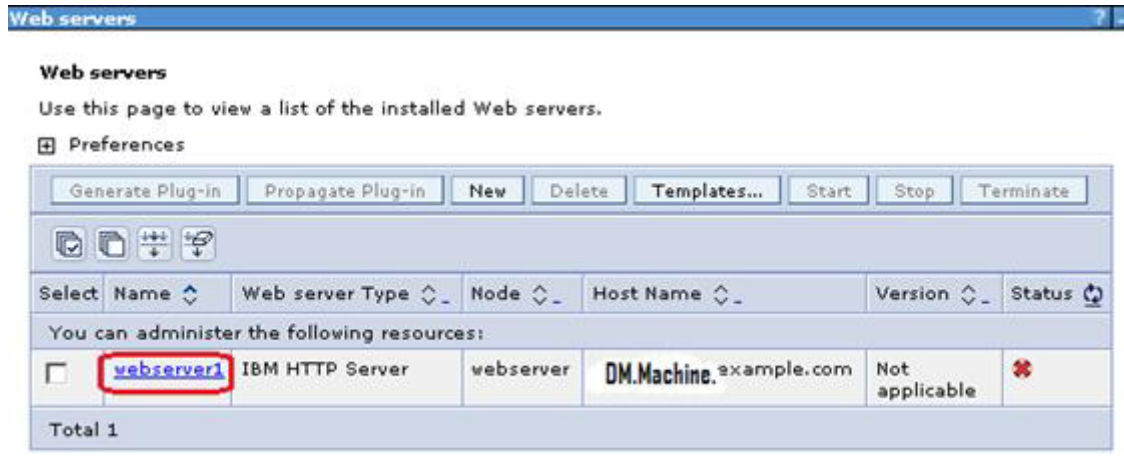


Figure 145. Starting the web server configuration for SSL

2. From the web servers panel, select **webserver1**.

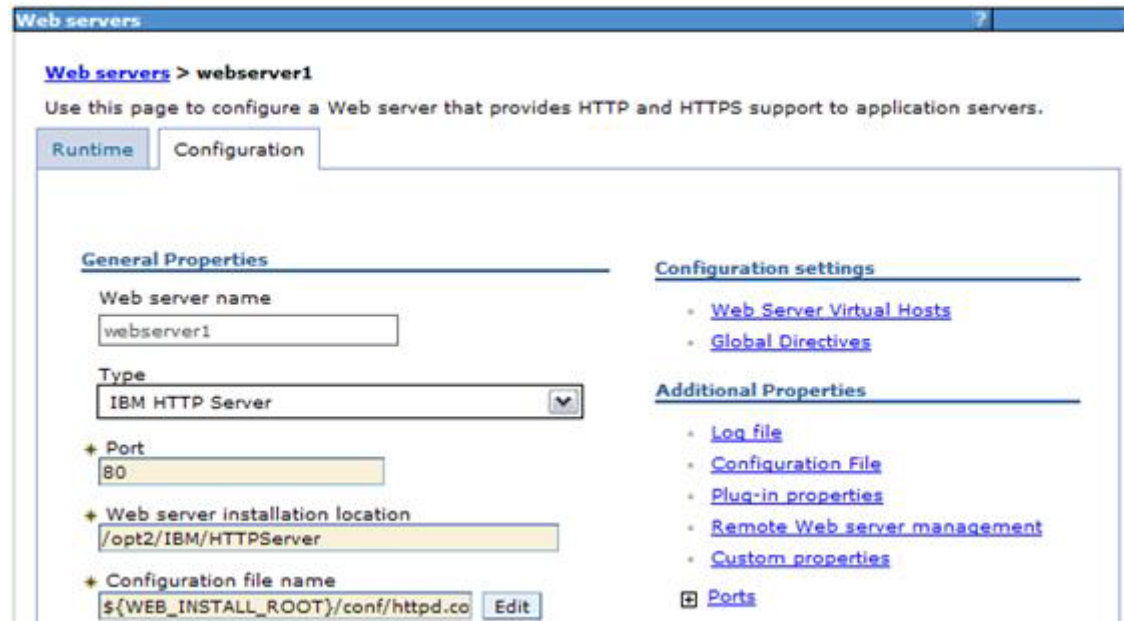


Figure 146. Configuring webserver1

- ___ 3. Click the configuration file option to open the `httpd.conf` from the administrative console.

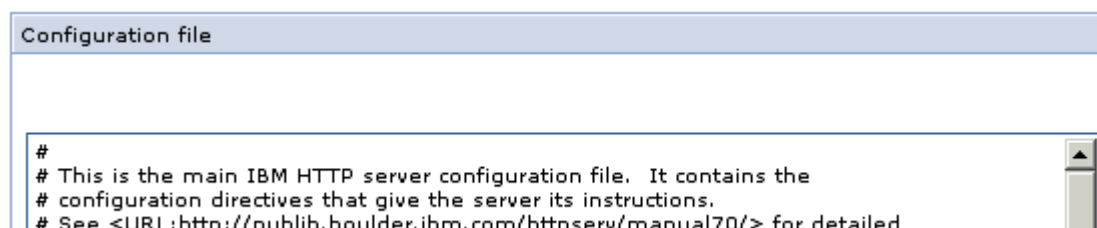


Figure 147. Configuration file

- ___ 4. The `httpd.conf` opens in the browser as previously shown. At the bottom of the configuration, add the following lines to the `http.conf` file:

```
SLoadModule ibm_ssl_module modules/mod_ibm_ssl.so
<IfModule mod_ibm_ssl.c>
Listen 0.0.0.0:443
<VirtualHost *:443>
ServerName DM.Machine.example.com
SSLEnable
</VirtualHost>
</IfModule>
SSLDisable
Keyfile "/opt2/keyfiles/webserver-key.kdb"
SSLStashFile "/opt2/keyfiles/webserver-key.sth"
```

- ___ 5. Click **OK** to save this change.

- ___ 6. Next, start the IBM HTTP Server. To verify that the SSL settings took effect correctly, type <https://DM.machine.example.com> into a browser. If the IBM HTTP Server page appears over https, then this step was successful. You might need to accept the certificate to your browser as it is not signed.

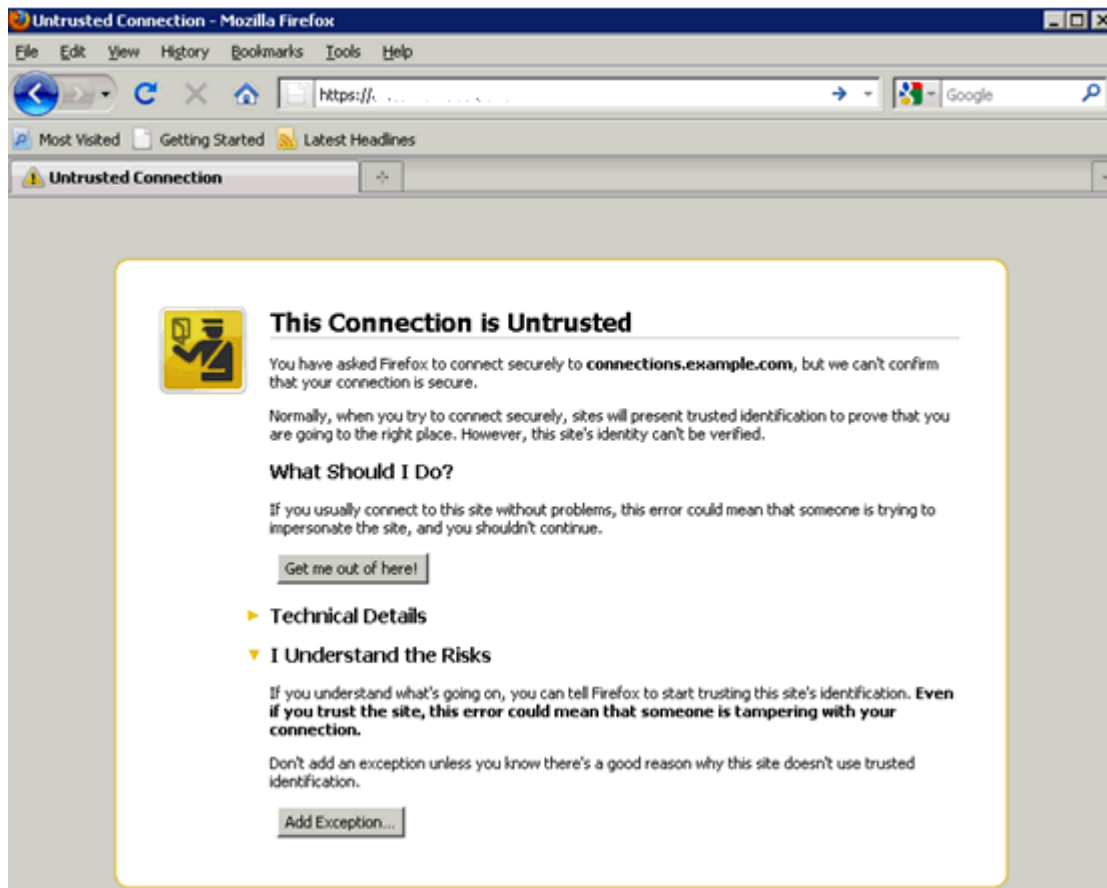


Figure 148. Browser certificate

- ___ 7. Add a security exception and click **Confirm Security Exception**.

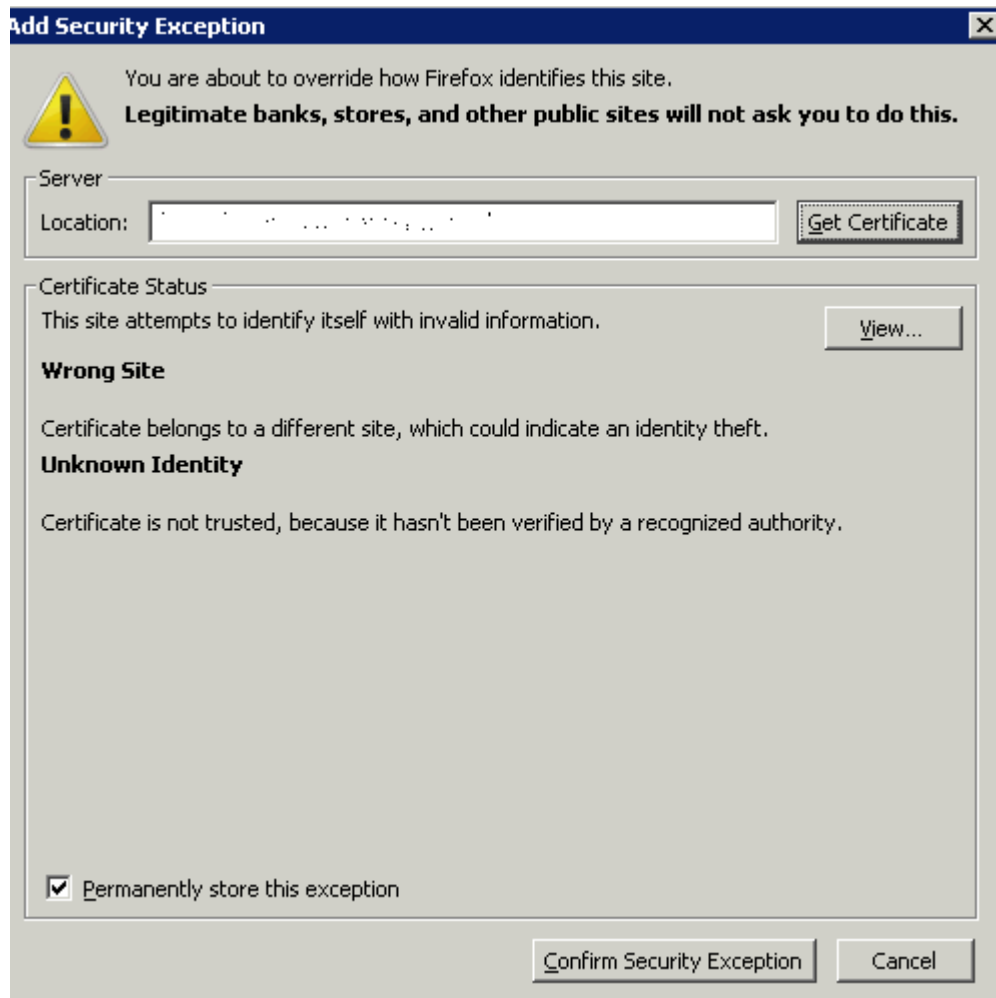


Figure 149. Adding a security exception

IBM HTTP Server Version 7.0 is successfully displayed on your browser.

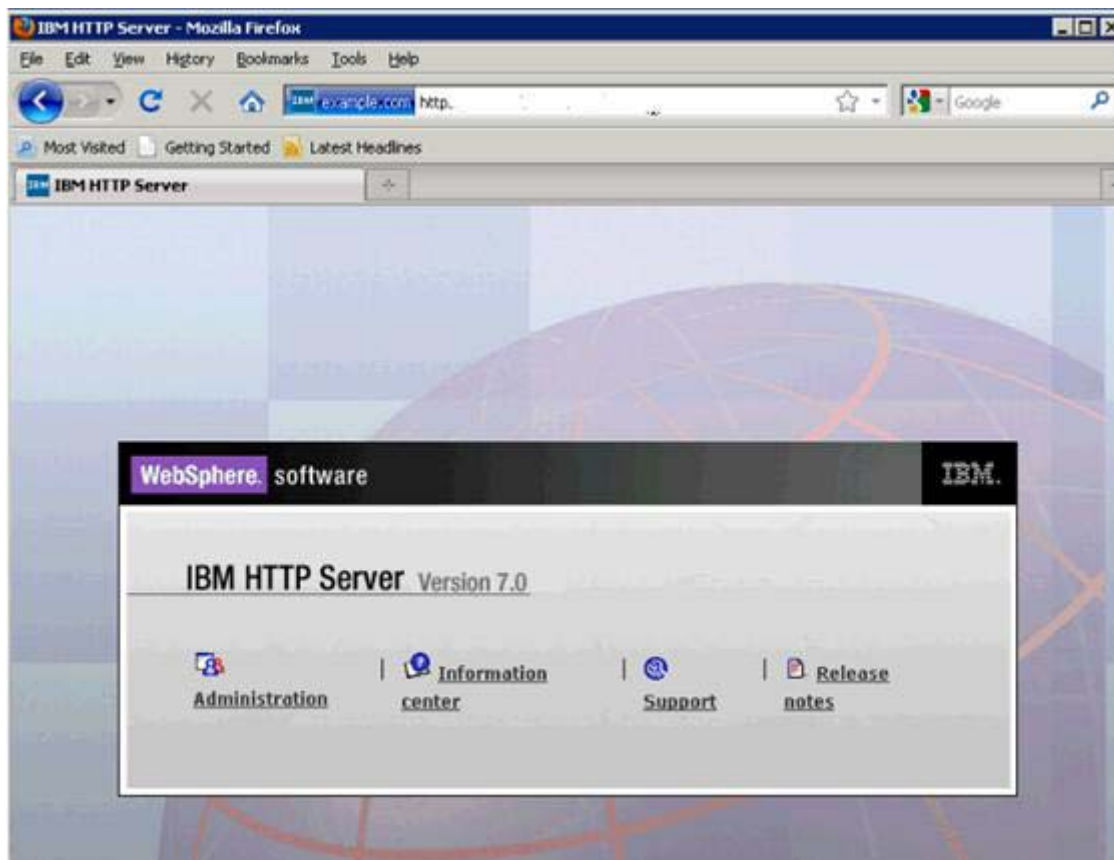


Figure 150. IBM HTTP Server Version 7.0

Adding certificates to the WebSphere truststore

- ___ 1. On the administrative console, go to **Security > SSL Certificate and Key Management > Key stores and certificates**. Click **CellDefaultTrustStore**.

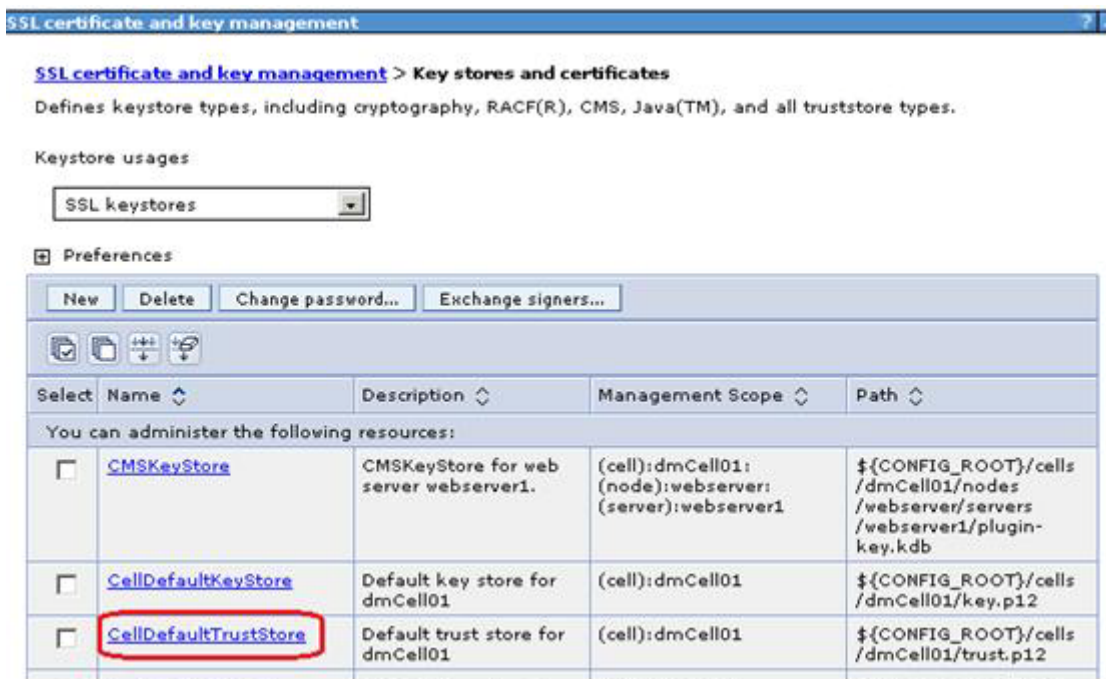


Figure 151. Key stores and certificates

- ___ 2. Within CellDefaultTrustStore, click **Signer Certificates** from the right side.



Figure 152. Signer certificates

- ___ 3. To add the webservers signer to the truststore, click **Retrieve from Port**.



Figure 153. Retrieving certificate from port

- ___ 4. Enter the host name of the web server and its SSL port (typically 443) and an Alias.
- ___ 5. Click **Retrieve signer information**, which retrieves the information that is shown at the bottom of the screen capture.
- ___ 6. Click **OK** to add this certificate to the list of signers.
- ___ 7. Click **Save** to save this change and restart the HTTP server to apply the changes.

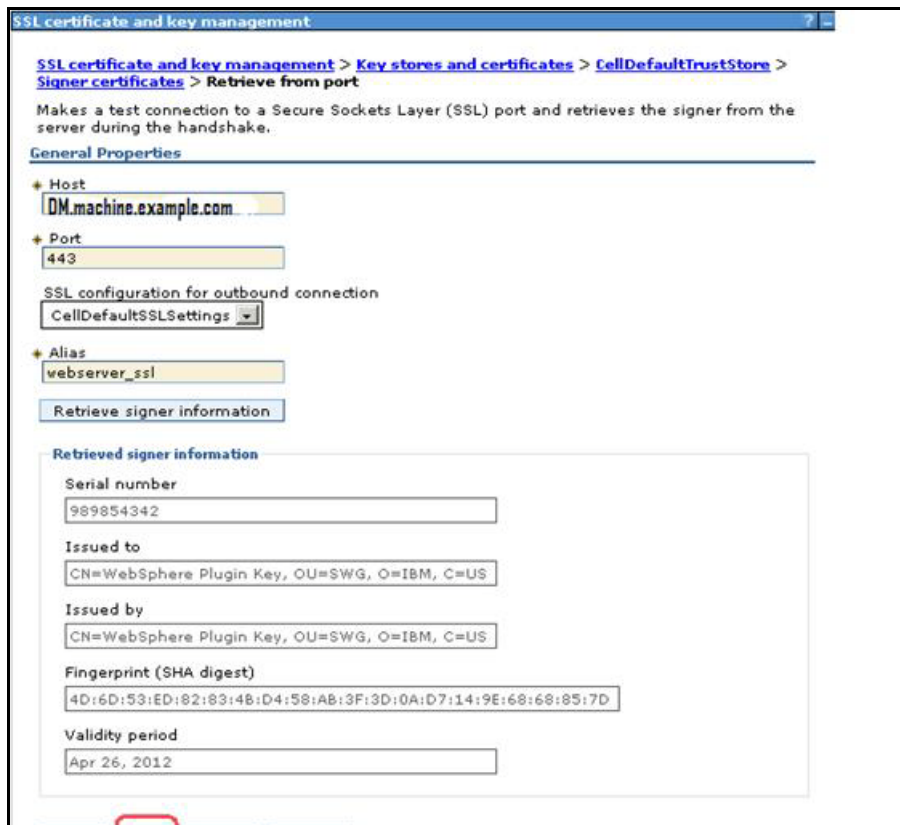


Figure 154. SSL certificate and key management: General properties

Update web addresses used by IBM Connections to access content

- ___ 1. Using the wsadmin client, check out the LotusConnections-config.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 host name of the HTTP Server and do not include any port numbers. An example 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>
```

Figure 155. LotusConnections-config.xml file

- ___ 2. Convert the following original values of the hrefs ssl_hrefs from their previous default values to their new values. In this case, all that is done is to drop the port numbers 9081 and 9044 from these URLs.

```
<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>
```

Figure 156. LotusConnections-config.xml file: Dropping the port numbers

- ___ 3. Repeat this process for all href and ssl_hrefs that are currently set to dm.example.com: .

After this process is complete, 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 web server, 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 do all of the above are shown in the following figure (the previous updates take place after the check out command).

```

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 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>synchAllNodes()
Nodes synchronized
wsadmin>exit

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

```

Figure 157. Administrator: Command Prompt

- ___ 4. The following list provides the previous commands in a test format so that they can be copied and used again in your own deployment.

```

1: wsadmin.bat -lang jython -username wasadmin -password wasadmin -port 8879
2: execfile("C:\IBM\WebSphere\AppServer\profiles\Dmgr01\config\bin_lc_admin\connectionsConfig.py")
3: LCConfigService.checkOutConfig("C:/temp","connectionsCell01")
<Make changes to the checked out file>
4: LCConfigService.checkInConfig()
5: synchAllNodes()

```

Figure 158. Commands in text format

Configuring an administrator user for blogs

Next, you add an admin user for blogs.

- ___ 1. Log in to your admin console <https://DM.Machine.example.com:9044/admin> (use wasadmin user and password).
- ___ 2. Select **Application > Application Types > WebSphere Enterprise Applications** and then select **Blogs**.
- ___ 3. Select **Security role to user/group mapping**.

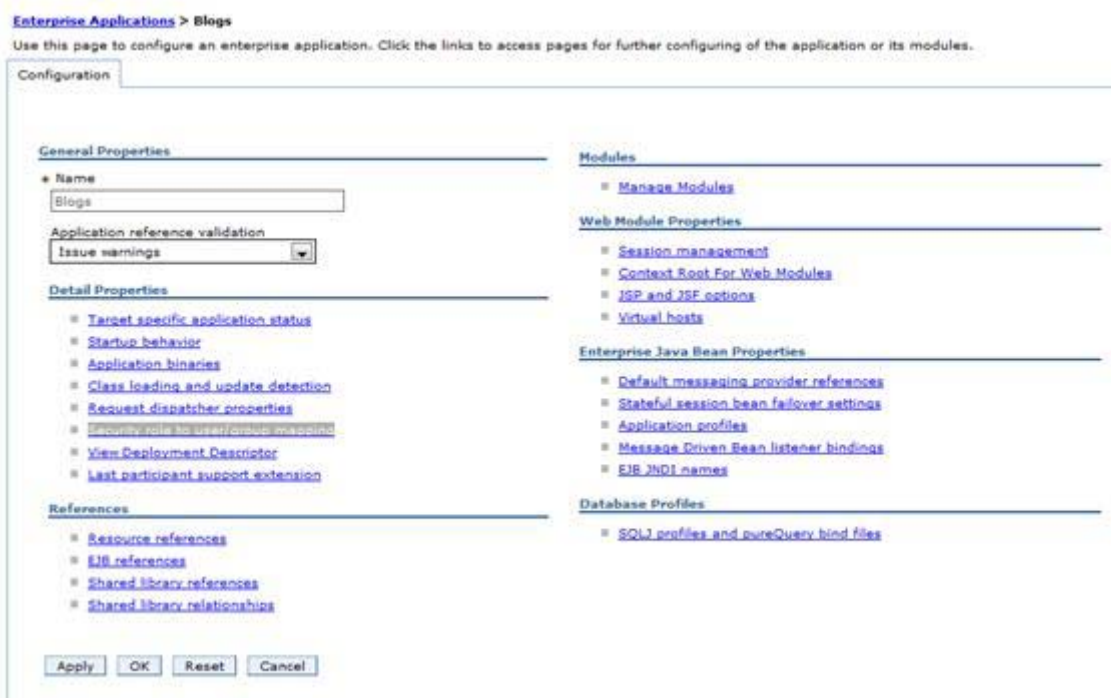


Figure 159. Selecting Security role to user/group mapping

- ___ 4. Select the admin role and then **Map Users...**

___ 5. Search for the user, Aamir_001_077 in the example, and add it.



Figure 160. Searching for the user and adding it

___ 6. Select **OK** and **Save**.

___ 7. For home page, repeat for the home page component.

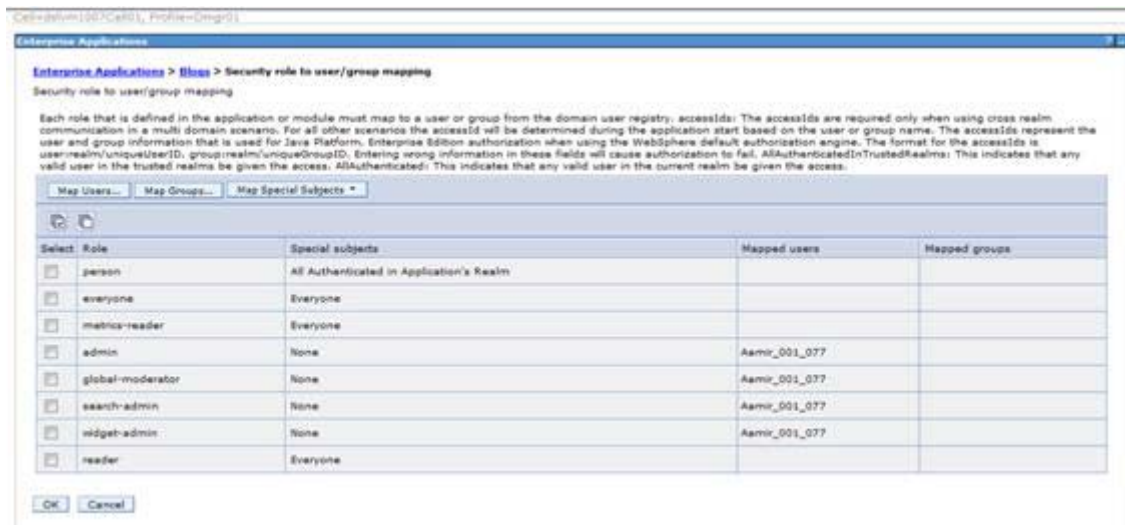


Figure 161. Home page component

- ___ 8. Make sure to synchronize your changes with the other nodes in the cluster.

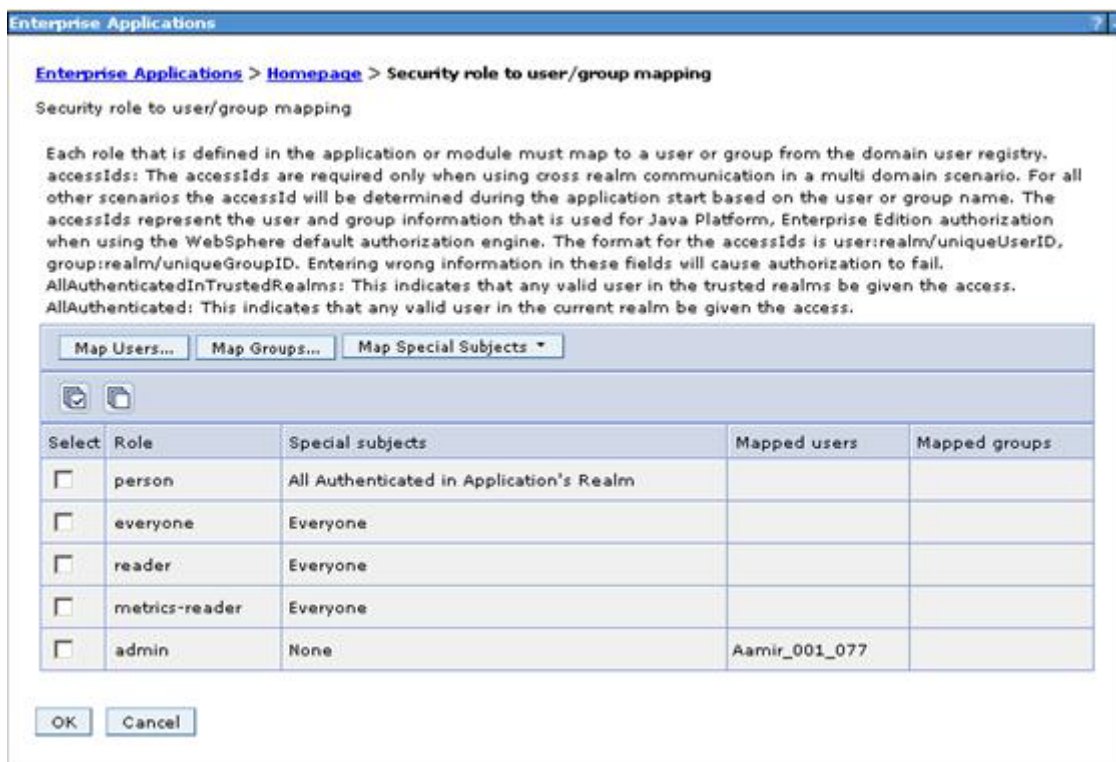


Figure 162. Synchronizing changes with the other nodes in the cluster

Double-check the Connections LDAP admin user to the Connections bus



Note

If you installed connections as wasadmin, you must do these steps. If you installed as the admin user from the LDAP when you enabled security on your LDAP, you do not need to do them.

- ___ 1. Base in this URL <http://www-01.ibm.com/support/docview.wss?uid=swg21293752> to resolve the problem. You can fix this problem in the administrative console by assigning a user to the bus connector.
- ___ 2. Go to **Service integration > Buses > ConnectionsBus > Security > Users and groups** in the bus connector role.



Note

You might have to enter `Aamir*` and find the user.

- ___ 3. Add a user name to the bus connector role.

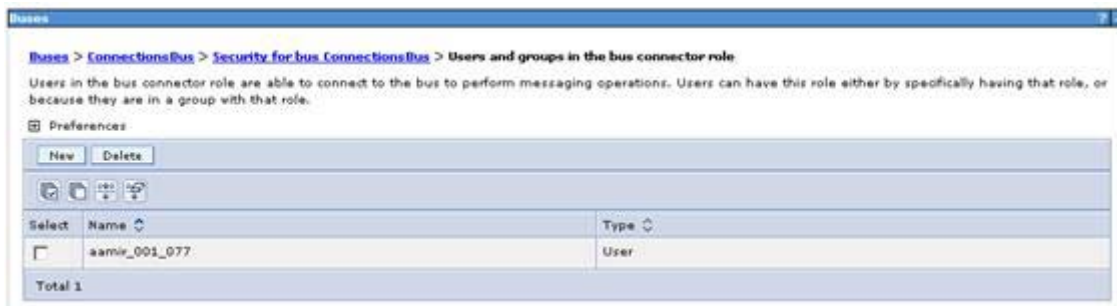


Figure 163. Users and groups in the bus connector role

Synchronizing the application member tables and corporate directory



Note

Run Tivoli Directory Integrator (`populationwizard.sh`) to synch between LDAP and profile database.

Synchronize all of the application member table databases, except News and Profiles, with the corporate directory by running `thesyncAllMembersByExtId()` administrative command for each application.

- ___ 1. Open a command prompt and then do the following step:
 - ___ a. Change to the following directory of the system on which you installed the deployment manager: `WAS_HOME\profiles\DMGR\bin`



Information

You must run the following command to start the wsadmin client from this specific directory because the Python files for the product are stored here. If you try to start the client from a different directory, then the `execfile()` command that you later call to initialize the administration environment for an IBM Connections component does not work properly.

- ___ 2. Enter the following command to start the wsadmin client:



Linux

```
./wsadmin.sh -lang jython -user admin_user_id -password
admin_password -port SOAP_CONNECTOR_ADDRESS Port
```

For example:

```
./wsadmin.sh -lang jython -username jsmith -password mypassword -port 8879
```

- ___ 3. Use following command to access the application configuration files:

```
execfile("application_py_file")
```

Where `application_py_file` is one of the following items:

- Activities: `activitiesAdmin.py`
- Blogs: `blogsAdmin.py`
- Bookmarks: `dogearAdmin.py`
- Communities: `communitiesAdmin.py`
- Files: `filesAdmin.py`

- Forums: forumsAdmin.py
- News: newsAdmin.py
- Wikis: wikisAdmin.py

You do not need to synchronize the News repository, Profiles, and Search now.

___ 4. Enter the following command to synchronize user data:

```
application_nameMemberService.syncAllMembersByExtId({ "updateOnEmailLoginMatch": "false" })
```

Where `application_name` is the name of the application. Specify one of the following items:

- Activities
- Blogs
- Dogear (Bookmarks)
- Communities
- Files
- Forums
- News



Note

The Home page, News repository, and Search applications share a database, so running the synchronization command against News applies to all three areas.

- Wikis



Example

```
DogearMemberService.syncAllMembersByExtId({ "updateOnEmailLoginMatch": "false" })
```

The logs are in Appserver1

The log `application_nameULcSyncCmd.log` is generated in the `application_cluster` path, for example `.profiles/AppSrv01/logs/Cluster1_server1/`.

SPNEGO configuration

Mapping an Active Directory account to administrative roles

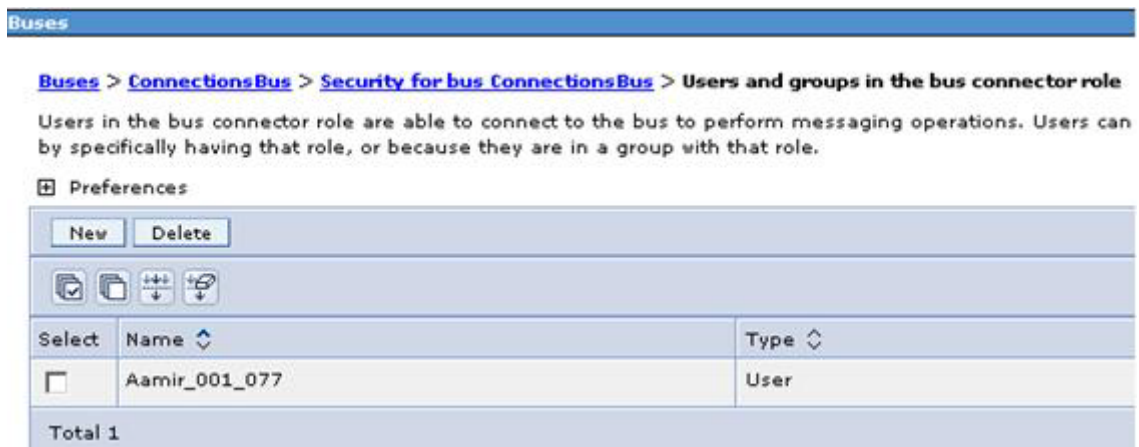


Figure 164. Mapping an Active Directory account to administrative roles

Creating a service principal name and keytab file

```
Hostnames( DM.machine, Appserver1, Appserver2) SPNEGO config
C:\keyfiles>ktpass -out c:\keyfiles\Appserver1http.keytab -princ
HTTP/Appserver1.example.com@EXAMPLE.COM -pass passwd -mapUser dub
xpcvm923http -mapOp add -pType KRB5_NT_PRINCIPAL
Targeting domain controller: MSADLDAP.example.com
Successfully mapped HTTP/Appserver1.example.com to Appserver1HTTP .
Password successfully set!
Key created.
Output keytab to c:\keyfiles\Appserver1http.keytab:
Keytab version: 0x502
keysize 101 HTTP/Appserver1.example.com@EXAMPLE.COM p
type 1 (KRB5_NT_PRINCIPAL) vno 4 etype 0x17 (RC4-HMAC) keylength 16
(0xb9f917853
e3dbf6e6831ecce60725930)
C:\keyfiles>ktpass -out c:\keyfiles\Appserver2http.keytab -princ
HTTP/Appserver2.example.com@EXAMPLE.COM -pass passwd -mapUser dub
xpcvm922http -mapOp add -pType KRB5_NT_PRINCIPAL
Targeting domain controller: MSADLDAP.example.com
Successfully mapped HTTP/Appserver2.example.com to Appserver2HTTP .
Password successfully set!
Key created.
Output keytab to c:\keyfiles\Appserver2http.keytab:
Keytab version: 0x502
keysize 101 HTTP/Appserver2.example.com@EXAMPLE.COM p
type 1 (KRB5_NT_PRINCIPAL) vno 4 etype 0x17 (RC4-HMAC) keylength 16
(0xb9f917853
e3dbf6e6831ecce60725930)
C:\keyfiles>ktpass -out c:\keyfiles\DM.machinehttp.keytab -princ
HTTP/DM.machine.example.com@EXAMPLE.COM -pass passwd -mapUser dub
xpcvm922http -mapOp add -pType KRB5_NT_PRINCIPAL
Targeting domain controller: MSADLDAP.example.com
Successfully mapped HTTP/DM.machine.example.com to DM.MachineHTTP.
Password successfully set!
Key created.
Output keytab to c:\keyfiles\DM.machinehttp.keytab:
Keytab version: 0x502
keysize 101 HTTP/DM.Machine.example.com@EXAMPLE.COM p
type 1 (KRB5_NT_PRINCIPAL) vno 4 etype 0x17 (RC4-HMAC) keylength 16
(0xb9f917853
e3dbf6e6831ecce60725930)
```

- ___ 1. Merge Appserver1.keytab, Appserver2.keytab to DM.machine.keytab by creating a folder in /opt2/keytab.
 - ___ a. Merge the keytab file on Node A into the keytab file on the Deployment Manager from cd /opt2/IBM/WebSphere/AppServer/java/jre/bin.

```
#/ktab -m /opt2/keytab/Appserver1.keytab /opt2/keytab/DM.machine.keytab
```

- ___ b. Merging keytab files: source=Appserver1.keytab destination=DM.machine.keytab.
Done!

- ___ 2. Merge the keytab file on Node B into the keytab file on the Deployment Manager:

```
# /ktab -m /opt2/keytab/Appserver2.keytab /opt2/keytab/DM.machine.keytab
```

- ___ a. Merging keytab files: source=Appserver2.keytab destination=DM.machine.keytab.
Done!

- ___ 3. Finally, cat /opt2/keytab/DM.Machine.keytab:

```
cd /opt2/IBM/WebSphere/AppServer/profiles/Dmgr01/bin
./wsadmin.sh -lang jacl -user Aamir_001_077 -password password

$AdminTask createKrbConfigFile {-krbPath
/opt2/IBM/WebSphere/AppServer/java/jre/lib/security/krb5.conf -realm
EXAMPLE.COM -kdcHost MSADLDAP.example.com -dns example.com -keytabPath
/opt/keytab/DM.machinehttp.keytab}
```

- ___ 4. Copy krb5.conf to the /opt2/keytab folder (which should also have the merged keytab file (DM.machinehttp.keytab)).
- ___ 5. Copy this folder to same location on appnode1 and appnode2, Deployment manager.

Creating a redirect page for users without SPNEGO support

- ___ 1. `<!DOCTYPE HTML PUBLIC "-//W3C/DTD HTML 4.0 Transitional//EN">`
`<META HTTP-EQUIV="Content-Type" CONTENT="text/html">`
`<!--`



Note

This file should be served from an unprotected website. Alternatively, it can be loaded from the WebSphere Application Server file system.

Any embedded `graphics/javascript/css` must be loaded from an unprotected website.

This file is loaded after WebSphere Application Server is initialized. If changes to this file are necessary, restart WebSphere Application Server.

This file is returned whenever the SPNEGO TAI receives an NTLM token for any application in the cell. In other words, this file is generic for all applications. However, by using the `document.location` JavaScript, you can get the original URL, and redirect to that original URL with the `"?noSPNEGO"` text added: thus forcing the standard application userid/password challenge.

```
-->
<html>
<script language="javascript">
var origUrl="" + document.location;
if (origUrl.indexOf("noSPNEGO") < 0) {
if (origUrl.indexOf('?') >= 0) origUrl += "&noSPNEGO";
else origUrl += "?noSPNEGO";
}
function redirTimer() {
self.setTimeout("self.location.href=origUrl;", 0);
}
</script>
<META HTTP-EQUIV = "Pragma" CONTENT="no-cache">
<script language="javascript">
document.write("<title> Redirect to " + origUrl + " </title>");
</script>
<head>
</head>
<body onLoad="redirTimer()" />
</html>
```

- ___ 2. Save the file as, for example, `NoSpnegoRedirect.html` on a publicly accessible directory on your web server. For example, `IHS_server/htdocs/NoSpnegoRedirect.html`.

Configuring SPNEGO on WebSphere Application Server

- ___ 1. Log on to the WebSphere Application Server Integrated Solutions Console on the Deployment Manager and select **Security > Global Security**.
- ___ 2. In the Authentication area, click **Kerberos configuration** and then enter the following details:
 - **Kerberos service name:** HTTP
 - **Kerberos configuration file:** Full path to your Kerberos configuration file
 - **Kerberos keytab file name:** Full path to your keytab file
 - **Kerberos realm name:** Name of your Kerberos realm

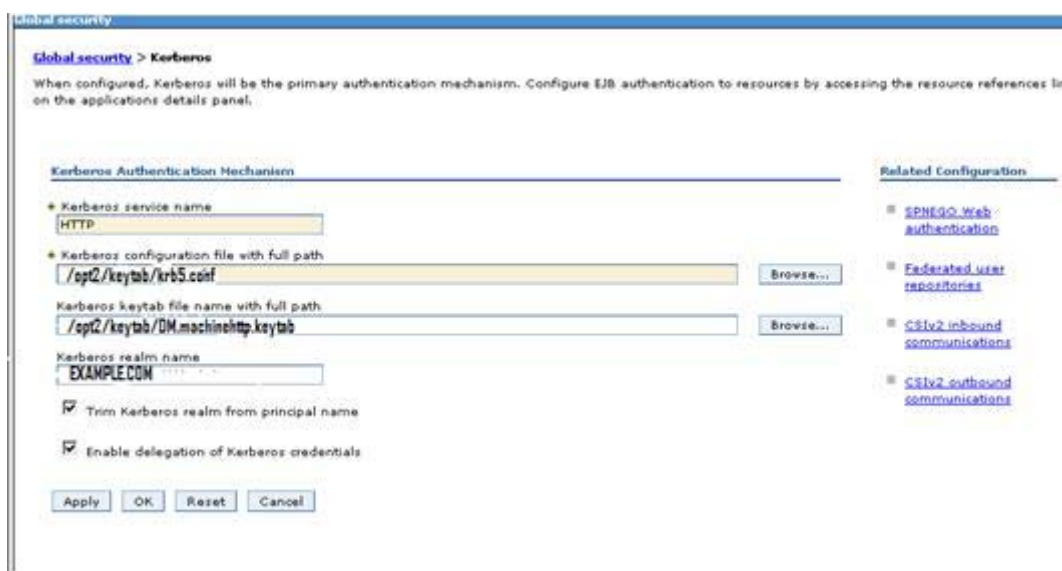


Figure 165. Kerberos Authentication Mechanism

- ___ 3. Select **Trim Kerberos realm from principal name** if it is not already selected.
- ___ 4. Select **Enable delegation of Kerberos credentials** if it is not already selected.
- ___ 5. Click **OK** and then click **Save**.
- ___ 6. Click **Kerberos configuration** and in the Related Configuration area, click **SPNEGO Web authentication**.



Note

SPNEGO web authentication and Kerberos authentication use the same Kerberos client configuration and keytab files.

- ___ 7. Specify the SPNEGO filter.
 - ___ a. In the SPNEGO Filters area, click **New** and enter the following details:

- **Host name:** Enter the host name of the deployment manager
- **Kerberos realm name:** Enter your Kerberos realm name
- **Filter criteria:**

```
request-url!=noSPNEGO;request-url!=/mobile;request-url!=/nav;request-url!=/bundles/js;request-url!=/static;request-url!=/activities/oauth;request-url!=/blogs/oauth;request-url!=/dogear/oauth;request-url!=/communities/calendar/oauth;request-url!=/communities/service/atom/oauth;request-url!=/communities/service/opensocial/oauth;/request-url!=/communities/recomm/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/anonymous/rest;request-url!=/connections/opensocial/common;request-url!=/connections/opensocial/gadgets;request-url!=/connections/opensocial/ic;request-url!=/connections/opensocial/rpc;request-url!=/connections/opensocial/social;request-url!=/connections/opensocial/xrds;request-url!=/connections/opensocial/xpc;request-url!=/connections/resources/web;request-url!=/connections/resources/ic;request-url!=/files/oauth;request-url!=/forums/oauth;request-url!=/homepage/oauth;request-url!=/metrics/service/oauth;request-url!=/moderation/oauth;request-url!=/news/oauth;request-url!=/news/follow/oauth;request-url!=/profiles/oauth;request-url!=/wikis/oauth;request-url!=/search/oauth;request-url!=/connections/core/oauth;/request-url!=/resources;request-url!=/oauth2/endpoint/
```



Note

Ensure that you separate each filter with a semicolon (;). No other character is allowed as a separator.

- **Filter class:** Leave this field blank to allow the system to use the default filter class (`com.ibm.ws.security.spnego.HTTPHeaderFilter`).
- **SPNEGO not supported error page URL:** Enter the URL to the redirect page that you created. For example: `http://webserver/NoSpnegoRedirect.html`.

Where `webserver` is the name of your IBM HTTP Server instance and `NoSpnegoRedirect.html` is the name of the redirect page.

- **NTLM token received error page URL:** Enter the URL to the redirect `http://webserver/NoSpnegoRedirect.html`.



Figure 166. Global security: General properties

- ___ b. Select **Trim Kerberos realm from principal name**.
- ___ c. Select **Enable delegation of Kerberos credentials**.
- ___ d. Click **OK** and then click **Save**.
- ___ 8. On the SPNEGO web authentication page, complete the following steps:
 - ___ a. Select **Dynamically update SPNEGO**.
 - ___ b. Select **Enable SPNEGO**.
 - ___ c. Select **Allow fall back to application authentication mechanism**.
 - ___ d. Enter the path to the Kerberos configuration file in the **Kerberos configuration file with full path** field.
 - ___ e. Enter the path to the Kerberos keytab file in the **Kerberos keytab file name with full path** field.

- ___ f. Click **Apply**.

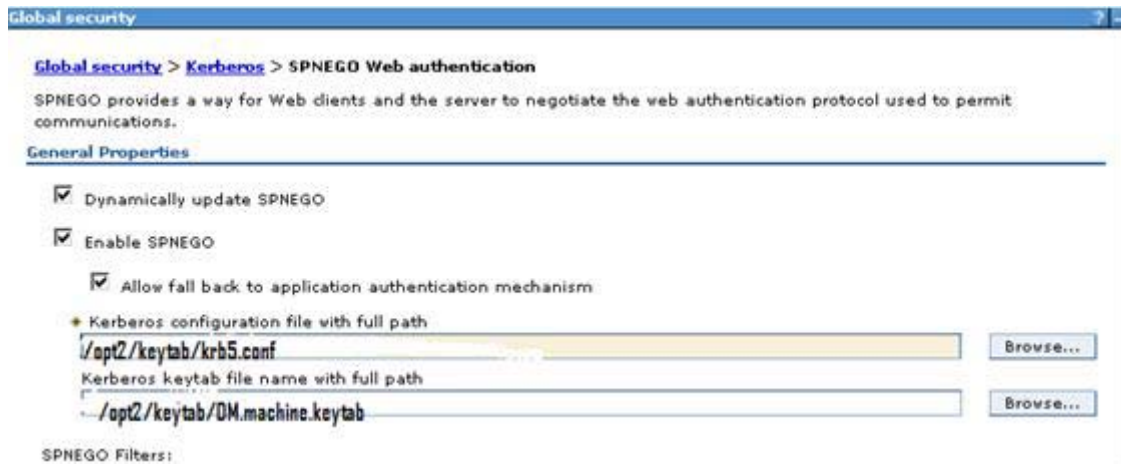


Figure 167. Global > Kerberos > SPNEGO web authentication

- ___ 9. Specify the level of authentication that users must go through to access your IBM Connections deployment. In the following choices, you can force users to always authenticate or allow users to access Blogs, Bookmarks, Communities, Files, Profiles, and Wikis anonymously. These anonymous users must log in only if they try to access a private area. For more information about forcing authentication, see the Forcing users to log in before they can access an application topic.
- ___ a. (default) Allow anonymous access to IBM Connections:
- Select **Applications > Application Types > WebSphere enterprise applications**.
 - Click the link to the first IBM Connections application in the Enterprise Applications table.
 - In the Detail Properties area, click **Security role to user/group mapping**.
 - Select the **reader** Role, click **Map Special Subjects**, and select **Everyone**.
 - Click **OK** and then click **Save**.
 - Repeat these steps for the remaining IBM Connections applications in the Enterprise Applications table.
- ___ b. Force users to log in to access IBM Connections:
- Select **Applications > Application Types > WebSphere enterprise applications**.
 - Click the link to the first IBM Connections application in the Enterprise Applications table.
 - In the Detail Properties area, click **Security role to user/group mapping**.
 - Select the **reader** Role. Then, click **Map Special Subjects** and select **All Authenticated in Application's Realm**.
 - Click **OK** and then click **Save**.
 - Repeat these steps for the remaining IBM Connections applications in the Enterprise Applications table.

- ___ 10. Remove interceptor classes:
 - ___ a. Select **Security > Global Security**.
 - ___ b. Expand **Web and SIP security** and click **Trust association > Interceptors**.
 - ___ c. Select the check boxes for the following two classes:
 - `com.ibm.ws.security.spnego.TrustAssociationInterceptorImpl`
 - `com.ibm.ws.security.TAMTrustAssociationInterceptorPlus`
 - ___ d. Click **Delete** and then click **Save**.



Figure 168. Global security > Trust association > Interceptors

- ___ 11. Disable TAI authentication:



Important

If you are configuring Tivoli® Access Manager with SPNEGO, or SiteMinder with SPNEGO. Those configurations require the default value of true for this parameter.

- ___ a. Select **Security > Global Security > Custom properties > New**.
- ___ b. Enter the following name and value pair:
 - **Name:** `com.ibm.websphere.security.performTAIForUnprotectedURI`
 - **Value:** `false`
- ___ c. Click **OK** and then click **Save**.



Figure 169. TAI authentication

- ___ 12. Click **Global Security**. In the Authentication area, click **LTPA** if it is not already selected. Click **Save**.
- ___ 13. Synchronize all the nodes in your deployment.

- ___ 14. Stop and restart WebSphere Application Server:
 - ___ a. Stop all instances of WebSphere Application Server that host your IBM Connections applications.
 - ___ b. Stop all node agents.
 - ___ c. Restart the Deployment Manager.
 - ___ d. Restart all the node agents.
 - ___ e. Restart all instances of WebSphere Application Server.

Configuring web browsers to support SPNEGO

Do one of the following set of steps depending on your web browser:

- ___ 1. Microsoft Internet Explorer:
 - ___ a. From the Internet Explorer menu, select **Tools > Internet Options** and then click the **Security** tab.
 - ___ b. Click the **Local intranet** icon and then click **Sites**.
 - ___ c. Click **Advanced** and then add the web address of the host name of your IBM Connections server into the **Add this website to the zone** field. For example: `*.enterprise.example.com`. Click **Add**.
 - ___ d. Enter the host name of your IBM HTTP Server into the **Add this website to the zone** field and click **Add**. For example: `http://<IHS_host>` or `https://IHS_host`.
 - ___ e. Click **OK** to save the change and return to the main Security page.
 - ___ f. Click **Custom level**, scroll to find **User Authentication > Logon**, and select **Automatic logon only in Intranet zone**. Click **OK** to save the change and return to the main Security page.
 - ___ g. Click the **Advanced** tab, scroll to find Security, and then select the **Enable Integrated Windows Authentication** check box. Click **OK** to save the change.
 - ___ h. Restart the web browser to apply the configuration changes.
- ___ 2. Mozilla Firefox:
 - ___ a. Open Firefox and type `about:config` into the location bar.
 - ___ b. Type `network.n` into the **Filter** field and double-click `network.negotiate-auth.trusted-uris`.
 - ___ c. Enter the address of the server that hosts IBM Connections. For example: <http://enterprise.example.com> or <https://enterprise.example.com> if you want to use HTTPS. Enter a comma and then enter the address of your IBM HTTP Server.
 - ___ d. Click **OK** to save the change.
 - ___ e. If the deployed SPNEGO solution is using the advanced Kerberos application of Credential Delegation, double-click `network.negotiate-auth.delegation-uris`. This preference defines the sites for which the browser can delegate user authorization to the server. Enter a comma-delimited list of trusted domains or URLs.
 - ___ f. Restart Firefox to apply the configuration change.

12. Take a full backup

When Lotus Connections 4.0 is working:

- ___ 1. Restart Nodeagents, deployment manager, the one installed on 3.0.1.x.
- ___ 2. Verify **NO** references to Connections 3.0.1.x.
- ___ 3. Uninstall Appserver1, Appserver2, HTTP server & Deployment manager which was used for IBM Connections 3.0.1.x.

