IBM WebSphere Configuration

Configuring Jenkins

1) Copy required admin & optional orb jars to Jenkins classpath (Clicking 'Test Connection' will show the correct path)
2) Enter the IP/DNS of WebSphere Application Server
3) Enter the Port to connect on
4) Select SOAP as the connect type (only supported type)

WebSphere Global Security

5) Enter the Username associated with WebSphere's Admin Console
6) Enter the Password associated with WebSphere's Admin Console

Connecting Remotely (ONLY if WebSphere is using the default untrusted SSL cert)

There are additional steps required for connecting to WebSphere remotely. Since WebSphere ships with an untrusted SSL cert(which the WebSphere Admin Console uses), you must tell the JRE that Jenkins is using to trust the "untrusted" cert. You do this by importing the untrusted SSL cert provided by WebSphere into your "cacerts" file. ** **Please be sure to backup your cacerts file before proceeding with these steps ****

1) By default the WebSphere Admin Console uses an untrusted cert, this cert must be trusted before connecting remotely by either importing it into cacerts for the JRE jenkins uses.

a) point Google Chrome to the WebSphere Admin Console using https

b) Click the https lock icon in the URL address bar of your browser (a dialog window will pop up)

c) Click on the "Connection" tab

d) Click on "Certificate Information" link (another dialog window will pop up)

e) Click on "Details" tab

f) Click "Export..." button and save the certificate to your computer.

g) Import the certificate into <JRE_HOME>/lib/security/cacerts using either the "keytool" command or IKeyMan provided by IBM

example) keytool -keystore <path to jre>/lib/security/cacerts -importcert -alias WebSphereServer -file admin_console.cer

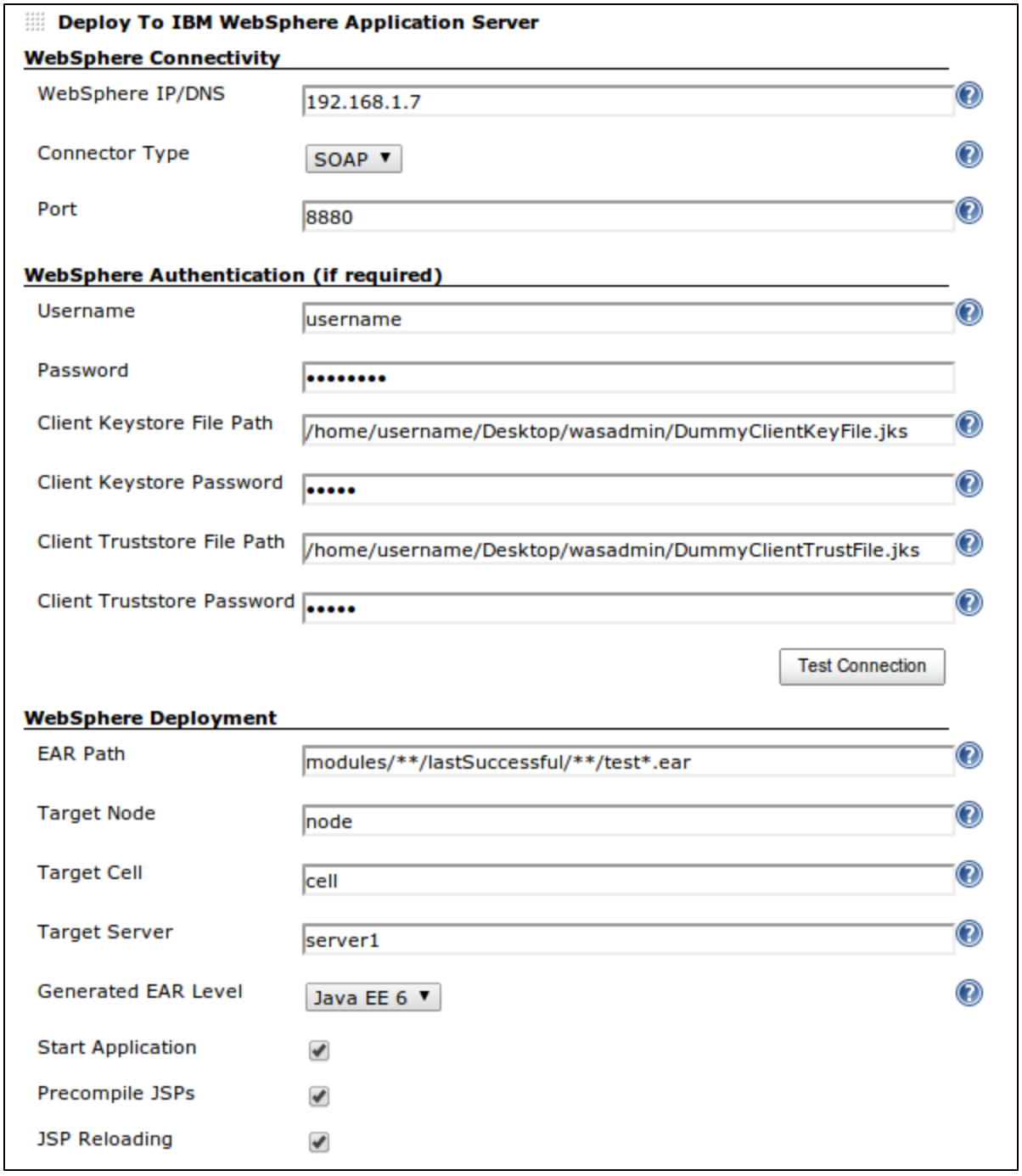
-or-

Download and execute InstallCert.java with "java InstallCert <websphere:9043>", select option 1 then re-execute and select option 2 and copy the created keystore file to the jre/lib/security folder that jenkins is running against.
2) If you cannot ping the short DNS name of the server that's hosting WebSphere, you'll need to add it to etc/hosts on the Jenkins server

Wrapping WAR Deployments

WAR deployments will automatically be wrapped in an EAR based on the EE Level specified in the configuration.

Example Configuration


Deploy To IBM WebSphere Application Server
WebSphere Connectivity
WebSphere IP/DNS
192.168.1.7
Connector Type
SOAP
Port
8880
WebSphere Authentication (if required)
Username
username
Password
Client Keystore File Path
/home/username/Desktop/wasadmin/DummyClientKeyFile.jks
Client Keystore Password
Client Truststore File Path
/home/username/Desktop/wasadmin/DummyClientTrustFile.jks
Client Truststore Password
Test Connection
WebSphere Deployment
EAR Path
modules/**/lastSuccessful/**/test*.ear
Target Node
node
Target Cell
cell
Target Server
server1
Generated EAR Level
Java EE 6
Start Application
Precompile JSPs
JSP Reloading