SSL and How to Use it in JBoss and WAS

What is SSL?

SSL (Secure Sockets Layer) is a protocol that encrypts data between a client and a server. It provides encryption, authentication, and integrity.

How SSL Works:

- Handshake: The server and client exchange keys and certificates to establish a secure session.
- Data Encryption: Data is then encrypted for the session.

Using SSL in JBoss (WildFly):

1. Generate a keystore:

keytool -genkey -keyalg RSA -alias server -keystore keystore.jks -storepass password -validity 3650 -keysize 2048

2. Configure SSL:

Edit standalone.xml:

<connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" secure="true">

<ssl name="my-ssl" key-alias="server" password="password" certificate-key-file="/path/to/keystore.jks" protocol="TLSv1.2" />

</connector>

3. Configure socket binding:

<socket-binding name="https" port="8443"/>

4. Restart JBoss and access: https://<hostname>:8443

Using SSL in WebSphere (WAS):

1. Generate keystore:

keytool -genkey -keyalg RSA -alias server -keystore keystore.jks -storepass password -validity 3650

2. In WAS Admin Console:

- Security > SSL certificate and key management > Key stores and certificates

- Create keystore and certificate.

- Configure server SSL ports (e.g., 9443).

3. Access: https://<hostname>:9443

SSL secures your server communication for sensitive data.