

Apache Tomcat SSL Kullanımı

Apache Tomcat ile HTTPS protokolü kullanarak çalışmak için;

1.Bir keystore üretilmesi gerekmektedir. Bunun için Java' nın kurulu olduğu dizin içerisinde

```
keytool -genkey -alias tomcat -keyalg RSA
```

komutu çalıştırılır. Bu işlem sonucu üretilen dosya Kullanıcının Ana Dizinde **.keystore** olarak bulunmaktadır.

2.Tomcat kurulumunda conf dizininde bulunan server.xml açılır. Dosya içerisinde 8443 portunu tanımlayan Connector tomcat kurulumunda kapalı gelmektedir. Bu tanım yorumlar silinerek aşağıdaki şekilde düzenlenir :

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11Nio2Protocol"
scheme="https" secure="true" SSLEnabled="true"
keystoreFile="{user.home}/.keystore" keystorePass="xxxx"
clientAuth="false" sslProtocol="TLS"/>
```

Bu işlemlerden sonra Tomcat hem HTTP (8080), hem de HTTPS (443) protokol/port üzerinden çalışmaktadır. Veya mevcut bir sertifika var ise aşağıdaki gibi düzenleme yapılabilir,

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11Nio2Protocol"
scheme="https" secure="true" keystoreFile="conf/logo.com.tr_pfx.pfx" keystorePass="XXXX"
keystoreType="PKCS12" SSLEnabled="true" clientAuth="false"
sslEnabledProtocols = "TLSv1.1,TLSv1.2" />
```

Not : Uygulama sunucusunda yapılacak bu ayarların dışında J-Platform/J-Hr ürünleri için ürünlerimiz üzerinde veya konfigürasyonunda yapılması gereken ek bir ayar veya tanım yoktur. Apache Tomcat'in SSL çalışması ürününde SSL çalışması için yeterlidir.

Load balancer üzerinden kullanılacak farklı SSL OffLoad yöntemleri için Logo Yazılım sistem ekiplerine danışabilirsiniz.