**Tomcat listen to 80 and 443**

* **Change the following existing port 8080 to 80 as shown /opt/tomcat/co**

|  |
| --- |
| Existing -  <Connector port="8080" protocol="HTTP/1.1"  connectionTimeout="20000"  redirectPort="8443" /> |

|  |
| --- |
| Change to - <Connector port="80" protocol="HTTP/1.1"  connectionTimeout="20000"  redirectPort="443"  maxParameterCount="1000"  authbind="yes"  /> |

* **Edit the startup.sh file**

|  |
| --- |
| Edit the /opt/tomcat/bin/startup.sh Add this  exec authbind --deep "$PRGDIR"/"$EXECUTABLE" start "$@" |

* **Next to open and allow permission to the port (apt install authbind)**

|  |
| --- |
| Touch /etc/authbind/byport/80 chmod 500 /etc/authbind/byport/80  Chown tomcat /etc/authbind/byport/80 |

**Reference -** [**https://docs.lucee.org/guides/installing-lucee/lucee-server-adminstration-linux/configure-Tomcat-listen-to-port.html**](https://docs.lucee.org/guides/installing-lucee/lucee-server-adminstration-linux/configure-Tomcat-listen-to-port.html)

* **Add the following connector to allow tomcat to run on 443**

|  |
| --- |
| Kshemakeysstore is a certificate generated by keystore <Connector port="443" protocol="org.apache.coyote.http11.Http11Nio2Protocol"  maxThreads="150" SSLEnabled="true"  maxParameterCount="1000"  scheme="https" secure="true"  keystoreFile="/opt/tomcat/conf/kshemakeysstore" keystorePass="@123Kshema"  clientAuth="false" sslProtocol="TLS">  </Connector> |

* **Next to open and allow permission to the port**

|  |
| --- |
| Touch /etc/authbind/byport/443 chmod 500 /etc/authbind/byport/443  Chown tomcat /etc/authbind/byport/443 |

* Import the pfx file

|  |
| --- |
| Keytool –import –alias tomcat –keystore kshemakeysstore –file <pfx\_file> |

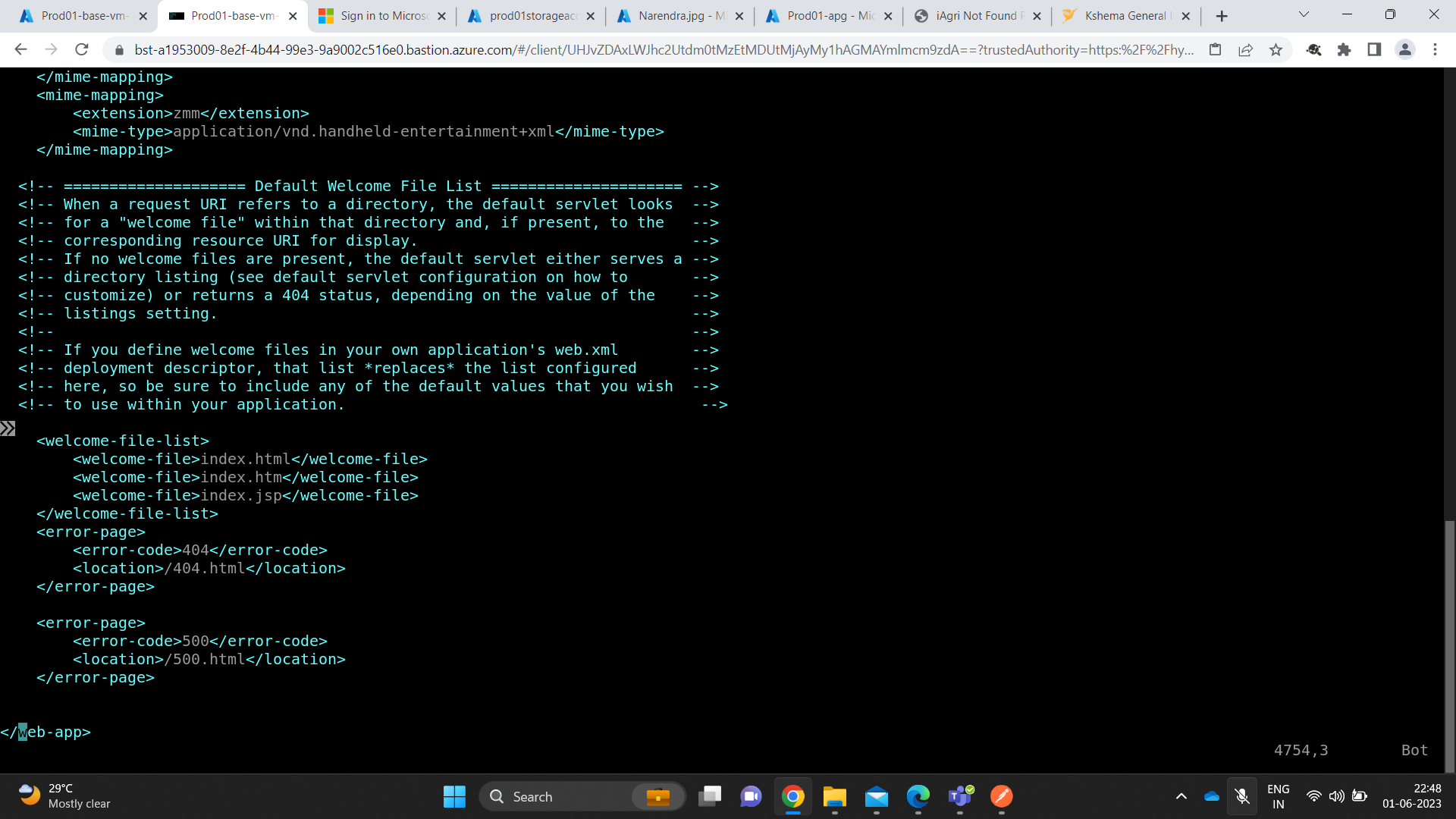
* Command for generating the RSA certificate

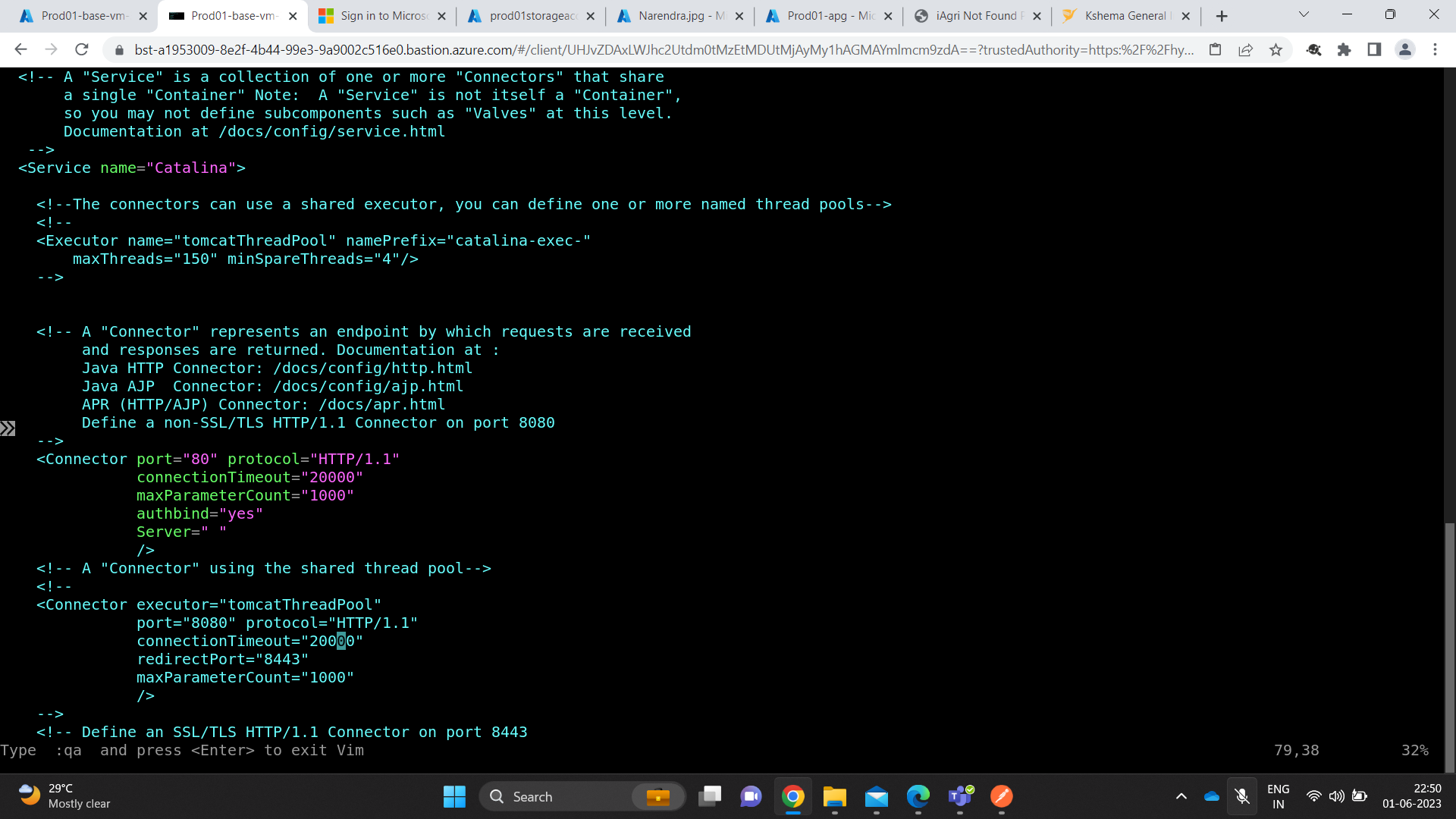
|  |
| --- |
| Keytool –genkey –alias tomcat –keyalg RSA –keystore ./kshemakeysstore |

**Kshema security hardening**

* Set tomcat to auto run on Port 80 (*authbind*) NO HTTPS ACTIVE/REDIRECT in tomcat.
* Change the timezone - sudo timedatectl set-timezone Asia/Kolkata
* Remove unwanted webapps (manager, exampled, doc ...), cleanup ROOT folder and add the following in place of it [link.](https://github.com/sahith-palika-99/Project-codes/blob/main/ROOT.zip)
* Update web.xml and include 404 and 505 error pages.

|  |
| --- |
| <error-page>  <error-code>404</error-code>  <location>/404.html</location>  </error-page>  <error-page>  <error-code>500</error-code>  <location>/500.html</location>  </error-page> |



* Ensure full tomcat sub-directories & files inside are owned by tomcat:tomcat (chown)
* **Add the server=” “ in server.xml file**  
  

**Extras**

* Command to change the tomcat variable to another folder

|  |
| --- |
| ln -s <source\_tomcat> <target\_tomcat> Example – ln –s tomcat9 tomcat  to change it use command: unlink tomcat |

**Rate limiting**

**Rate limiting – APIs – WAF – Kshema shall provide the list and Cloud Angles to implement**

<https://techcommunity.microsoft.com/t5/azure-paas-blog/configure-rate-limits-for-different-api-operations-in-azure-api/ba-p/3789108#:~:text=Rate%20limits%20are%20policies%20that,API%20within%20a%20billing%20period>.

* Unfortunately, Application Gateway WAF does not have a way to rate limit incoming connections.  
  <https://learn.microsoft.com/en-us/answers/questions/771079/rate-limiting-in-azure-application-gateway-waf>
* Rate-limiting, geo-filtering, and Azure managed Default Rule Set rules are supported only with WAF on Azure Front Door.
* Azure Front Door (CloudFront) can be configured on the Application Gateway and waf can be attached on it.