Pacchetti che servono:

1. Tomcat8
2. JDK8
3. CAS Overlay Template

1.) **Prima di procedere con tutte le configurazioni si deve generare una chiave per il server CAS.**

Eseguire il seguente comando per generare la chiave:

`keytool -keystore /opt/jdk1.8.0_101/jre/lib/security/cacerts -genkey -alias cas -keyalg RSA`

Importante inserire nel nome e cognome il nome del server(hostname) oppure localhost

2.) **Attivare SSL su tomcat. Modifica server.xml:**

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
             maxThreads="150" scheme="https" secure="true"
             clientAuth="false" sslProtocol="TLS"
             keystoreFile="/opt/jdk1.8.0_101/jre/lib/security/thekeystore"
             keystorePass="changeit"
             truststoreFile="/opt/jdk1.8.0_101/jre/lib/security/cacerts"  />
```

3.) **Installazione CAS Overlay Template**

- Scarica CAS dal: https://github.com/apereo/cas-overlay-template
- Dopo aver scompattato il pacchetto eseguire il commando nella cartella del cas:

`run build.sh package`

- Nella directory cas-overlay-master/target si trova il war file per il tomcat.
- In /etc/cas/config/users.properties modifica in `casuser=notused,ROLE_ADMIN,enabled` nel caso si voglia usera l'utente casuser
- Modifica il /etc/cas/config/cas.properties o /cas/WEB-INF/classes/application.properties:

```
 # CAS Server Context Configuration

cas.server.name=https://localhost:8443
cas.server.prefix=https://localhost:8443/cas

cas.host.name=localhost
server.context-path=/cas
server.port=8443

server.ssl.key-store=file:/opt/jdk1.8.0_101/jre/lib/security/thekeystore
server.ssl.key-store-password=changeit
server.ssl.key-password=changeit


management.contextPath=/status
management.security.enabled=true
management.security.roles=ACTUATOR,ADMIN,ROLE_ADMIN
management.security.sessions=if_required

cas.adminPagesSecurity.ip=127\.0\.0\.1
logging.config=file:/etc/cas/config/log4j2.xml

cas.serviceRegistry.watcherEnabled=true
cas.serviceRegistry.repeatInterval=120000
cas.serviceRegistry.startDelay=15000
cas.serviceRegistry.initFromJson=true
cas.serviceRegistry.config.location=file:/etc/cas/services

#cas.authn.accept.users=casuser::Mellon
cas.authn.accept.users=
#logging.level.org.apereo=DEBUG

cas.authn.file.separator=::
```

```
cas.authn.file.filename=file:///home/utente/users.txt
```

- Per autentificare tramite una lista file TXT, si deve mettere la dependency nel file pom.xml.
- Scaricare nel cas/WEB-INF/lib il jar cas-server-support-generic-5.2.0-RC4.jar dal maven repository. https://mvnrepository.com/
- Ricorda di copiare il codice della dependecy come suggerito nel sito maven

```
<dependency>
    <groupId>org.apereo.cas</groupId>
    <artifactId>cas-server-support-generic</artifactId>
    <version>5.2.0-RC4</version>
    <scope>test</scope>
</dependency>
```

- Crea file json in /cas/WEB-INF/classes/services con il nome allservices-101.json con il contenuto

```
{
  "@class" : "org.apereo.cas.services.RegexRegisteredService",
  "serviceId" : "^(http|https)://.*",
  "name" : "allservices",
  "id" : 101,
  "accessStrategy" : {
    "@class" : "org.apereo.cas.services.DefaultRegisteredServiceAccessStrategy",
    "enabled" : true,
    "ssoEnabled" : true
  }
}
```

Attenzione! *Il nome del file deve essere name-id.json come specificato nello script.*