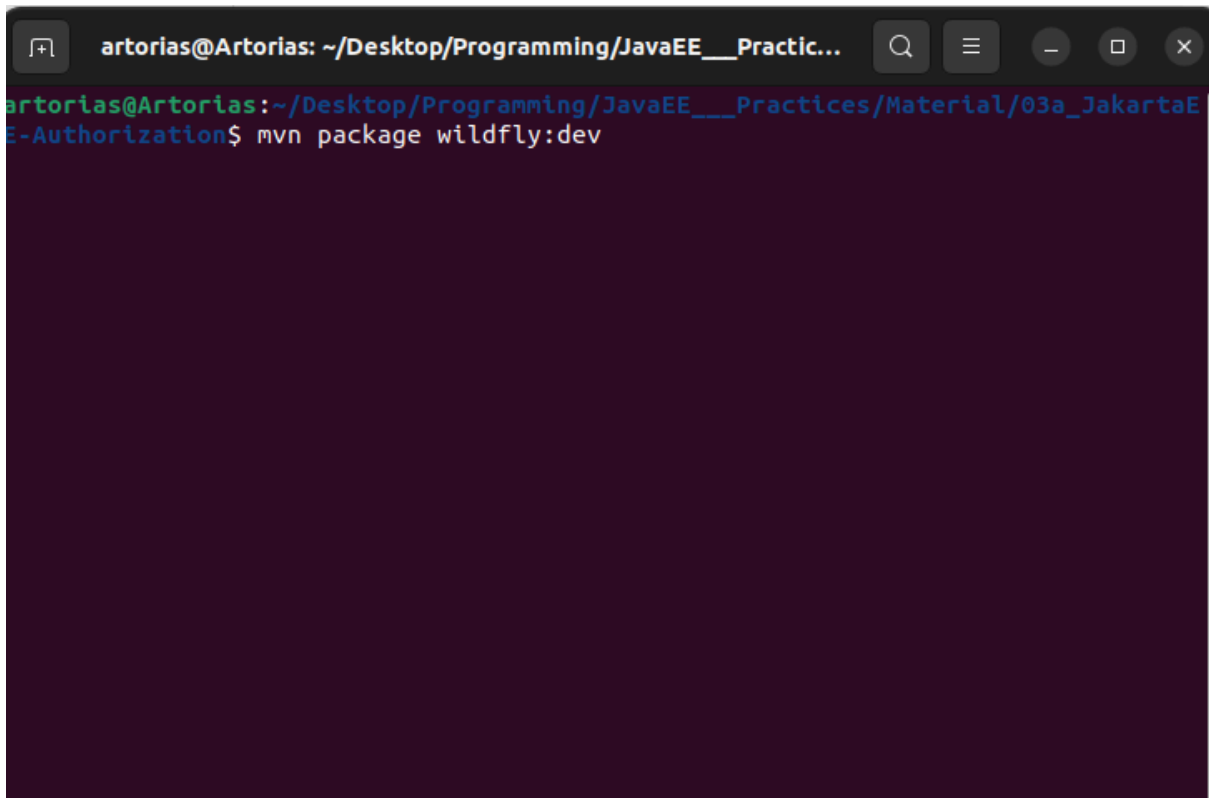


Ejercicio 4

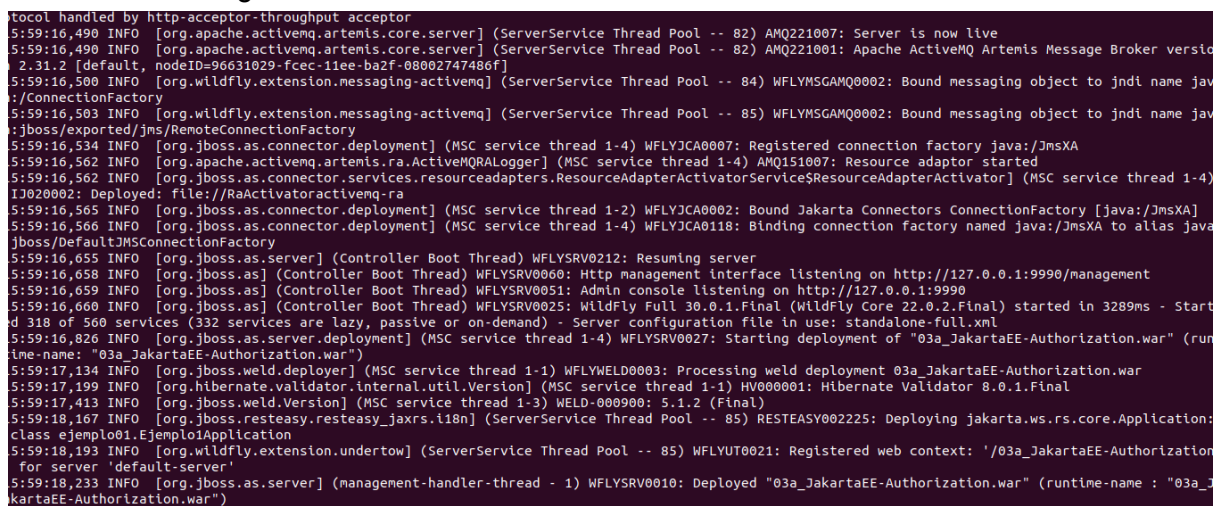
Jakarta Security

1) Primero debemos bajar el código que el docente nos provee.
Una vez bajado, podemos proceder a levantar el servidor.
Debemos ejecutar el comando `mvn package wildfly:dev`.



```
artorias@Artorias: ~/Desktop/Programming/JavaEE__Practic...
artorias@Artorias:~/Desktop/Programming/JavaEE__Practices/Material/03a_JakartaE
E-Authorization$ mvn package wildfly:dev
```

Podemos ver lo siguiente:



```
Protocol handled by http-acceptor-throughput-acceptor
5:59:16,490 INFO [org.apache.activemq.artemis.core.server] (ServerService Thread Pool -- 82) AMQ221007: Server is now live
5:59:16,490 INFO [org.apache.activemq.artemis.core.server] (ServerService Thread Pool -- 82) AMQ221001: Apache ActiveMQ Artemis Message Broker version 2.31.2 [default, nodeID=96631029-fcec-11ee-ba2f-08002747486f]
5:59:16,500 INFO [org.wildfly.extension.messaging-activemq] (ServerService Thread Pool -- 84) WFLYMSGAMQ0002: Bound messaging object to jndi name java:/ConnectionFactory
5:59:16,503 INFO [org.wildfly.extension.messaging-activemq] (ServerService Thread Pool -- 85) WFLYMSGAMQ0002: Bound messaging object to jndi name java:/jboss/exported/jms/RemoteConnectionFactory
5:59:16,534 INFO [org.jboss.as.connector.deployment] (MSC service thread 1-4) WFLYJCA0007: Registered connection factory java:/JmsXA
5:59:16,562 INFO [org.apache.activemq.artemis.ra.ActiveMQRALogger] (MSC service thread 1-4) AMQ151007: Resource adaptor started
5:59:16,562 INFO [org.jboss.as.connector.services.resourceadapters.ResourceAdapterActivatorService$ResourceAdapterActivator] (MSC service thread 1-4) WFLYJCA0011: Deployed: file://RaActivatoractivemq-ra
5:59:16,565 INFO [org.jboss.as.connector.deployment] (MSC service thread 1-2) WFLYJCA0002: Bound Jakarta Connectors ConnectionFactory [java:/JmsXA]
5:59:16,566 INFO [org.jboss.as.connector.deployment] (MSC service thread 1-4) WFLYJCA0118: Binding connection factory named java:/JmsXA to alias java:/jboss/DefaultJMSConnectionFactory
5:59:16,655 INFO [org.jboss.as.server] (Controller Boot Thread) WFLYSRV0212: Resuming server
5:59:16,658 INFO [org.jboss.as] (Controller Boot Thread) WFLYSRV0060: Http management interface listening on http://127.0.0.1:9990/management
5:59:16,659 INFO [org.jboss.as] (Controller Boot Thread) WFLYSRV0051: Admin console listening on http://127.0.0.1:9990
5:59:16,660 INFO [org.jboss.as] (Controller Boot Thread) WFLYSRV0025: WildFly Full 30.0.1.Final (WildFly Core 22.0.2.Final) started in 3289ms - Start
d 318 of 560 services (332 services are lazy, passive or on-demand) - Server configuration file in use: standalone-full.xml
5:59:16,826 INFO [org.jboss.as.server.deployment] (MSC service thread 1-4) WFLYSRV0027: Starting deployment of "03a_JakartaEE-Authorization.war" (run
time-name: "03a_JakartaEE-Authorization.war")
5:59:17,134 INFO [org.jboss.weld.deployer] (MSC service thread 1-1) WFLYWELD0003: Processing weld deployment 03a_JakartaEE-Authorization.war
5:59:17,199 INFO [org.hibernate.validator.internal.util.Version] (MSC service thread 1-1) HV000001: Hibernate Validator 8.0.1.Final
5:59:17,413 INFO [org.jboss.weld.Version] (MSC service thread 1-3) WELD-000900: 5.1.2 (Final)
5:59:18,167 INFO [org.jboss.resteasy.resteasy_jaxrs.i18n] (ServerService Thread Pool -- 85) RESTEASY002225: Deploying jakarta.ws.rs.core.Application:
class ejemplo01.Ejemplo1Application
5:59:18,193 INFO [org.wildfly.extension.undertow] (ServerService Thread Pool -- 85) WFLYUT0021: Registered web context: '/03a_JakartaEE-Authorization
for server 'default-server'
5:59:18,233 INFO [org.jboss.as.server] (management-handler-thread - 1) WFLYSRV0010: Deployed "03a_JakartaEE-Authorization.war" (runtime-name : "03a_J
akartaEE-Authorization.war")
```

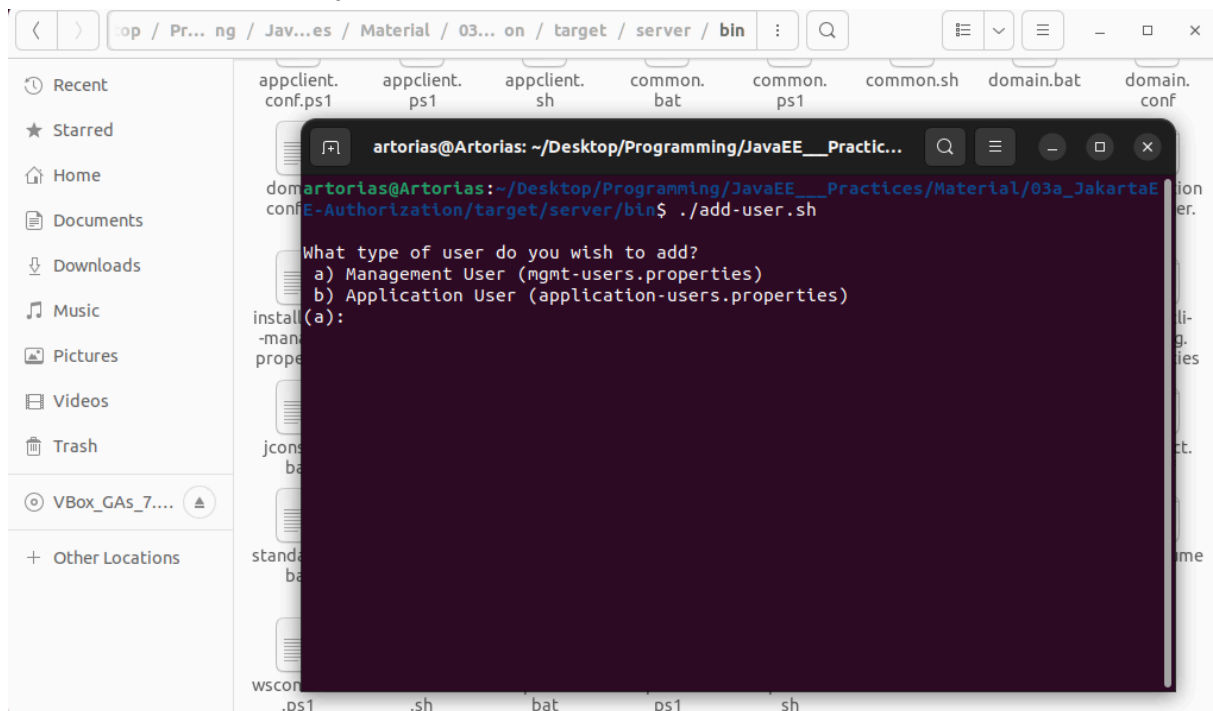
Dentro del código del servidor deployado, se puede ver como estan los usuarios y sus respectivos roles o grupos de roles, ejemplo usr1 tiene grupo1 y usr4 tiene grupo admin.

```
root@Artorias: /home/artorias/Desktop/Programming/JavaEE_PRACTICES/Material/03b_JakartaEESecurity
14:40:53,479 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: create table Usuario_Grupo (Usuario_username varchar(255) not null, grupos_nombre varchar(255) not null)
14:40:53,479 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: alter table if exists Usuario_Grupo add constraint FK0ucyb42b80naql12wg8idjs foreign key (grupos_nombre) references Grupo
14:40:53,491 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: alter table if exists Usuario_Grupo add constraint FK1e8rgo566f9ctjh1nvoc9e4xe foreign key (Usuario_username) references Usuario
14:40:53,496 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Usuario (username,passwordHash) values ('usr1','355d3dbbc5c19e36d4d5e7d2c1b78db0d28881d942a5bf90deddc3aa6789960')
14:40:53,498 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Usuario (username,passwordHash) values ('usr2','e5b0c292403177468df0a1cc8e2fe9d48d905507b12491fa95195f8765723808')
14:40:53,498 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Usuario (username,passwordHash) values ('usr3','0807ae093e07b9aaa3ae75f4ec5a8c5323b8a5550007093e4edf45e85a02f71e')
14:40:53,499 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Usuario (username,passwordHash) values ('usr4','0af6d47d5944b3fdfecc60c23a9b83224a989605633102aee8bf9cb0e6e48ea6')
14:40:53,499 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Grupo (nombre) values ('grupo1')
14:40:53,500 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Grupo (nombre) values ('grupo2')
14:40:53,500 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Grupo (nombre) values ('admin')
14:40:53,501 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Usuario_Grupo (Usuario_username, grupos_nombre) values ('usr1','grupo1')
14:40:53,501 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Usuario_Grupo (Usuario_username, grupos_nombre) values ('usr2','grupo2')
14:40:53,502 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Usuario_Grupo (Usuario_username, grupos_nombre) values ('usr3','grupo1')
14:40:53,502 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Usuario_Grupo (Usuario_username, grupos_nombre) values ('usr3','grupo2')
14:40:53,503 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Usuario_Grupo (Usuario_username, grupos_nombre) values ('usr4','admin')
14:40:53,825 INFO [org.wildfly.security.soteria.original.CdiExtension] (MSC service thread 1-8) Activating jakarta.security.enterprise.authentication.mechanism.http.BasicAuthenticationMechanismDefinition authentication mechanism from ejemplo00.infraestructura.seguridad.SeguridadConfiguracion class
14:40:53,999 INFO [org.wildfly.security.soteria.original.SamlRegistrationInstaller] (ServerService Thread Pool -- 18) Initializing Soteria 3.0.3.Final for context '/03b_JakartaEESecurity'
14:40:54,037 INFO [org.wildfly.extension.undertow] (ServerService Thread Pool -- 18) WFLYUT0021: Registered web context: '/03b_JakartaEESecurity' for server 'default-server'
14:40:54,060 INFO [org.jboss.as.server] (management-handler-thread - 1) WFLYSRV0010: Deployed "03b_JakartaEESecurity.war" (runtime-name : "03b_JakartaEESecurity.war")
```

2) Ahora debemos modificar los usuarios y sus respectivos grupos.

Para esto, debemos irnos a la carpeta /target/server/bin/ y de ahí ejecutar el archivo que nos dejara modificar los mismos, llamado add-user.sh.

Ya dentro del directorio, ejecutaremos el comando add-user.sh.



Seguido de eso nos preguntara que tipo de user queremos agregar, al cual le daremos application user.

```
root@Artorias: /home/artorias/Desktop/Programming/JavaE...
root@Artorias:/home/artorias/Desktop/Programming/JavaEE___Practices/Material/03a
_JakartaEE-Authorization/target/server/bin# ./add-user.sh

What type of user do you wish to add?
a) Management User (mgmt-users.properties)
b) Application User (application-users.properties)
(a): b

Enter the details of the new user to add.
Using realm 'ApplicationRealm' as discovered from the existing property files.
Username : 
```

Aca nos pide user name, y luego nos va a pedir password, para agregarlo al ApplicationRealm.

```
root@Artorias: /home/artorias/Desktop/Programming/JavaE...
root@Artorias:/home/artorias/Desktop/Programming/JavaEE___Practices/Material/03a
_JakartaEE-Authorization/target/server/bin# ./add-user.sh

What type of user do you wish to add?
a) Management User (mgmt-users.properties)
b) Application User (application-users.properties)
(a): b

Enter the details of the new user to add.
Using realm 'ApplicationRealm' as discovered from the existing property files.
Username : Juan
Password recommendations are listed below. To modify these restrictions edit the
add-user.properties configuration file.
- The password should be different from the username
- The password should not be one of the following restricted values {root, adm
n, administrator}
- The password should contain at least 8 characters, 1 alphabetic character(s),
1 digit(s), 1 non-alphanumeric symbol(s)
Password : WFLYDM0099: Password should have at least 8 characters!
Are you sure you want to use the password entered yes/no? 
```

En este caso, queremos agregar el usuario al grupo gerente, pero estaremos realizando lo demas pedido en la propuesta, de igual manera.

```
root@Artorias: /home/artorias/Desktop/Programming/JavaE...
What type of user do you wish to add?
a) Management User (mgmt-users.properties)
b) Application User (application-users.properties)
(a): b
Enter the details of the new user to add.
Using realm 'ApplicationRealm' as discovered from the existing property files.
Username : Juan
Password recommendations are listed below. To modify these restrictions edit the
add-user.properties configuration file.
- The password should be different from the username
- The password should not be one of the following restricted values {root, admin, administrator}
- The password should contain at least 8 characters, 1 alphabetic character(s), 1 digit(s), 1 non-alphanumeric symbol(s)
Password :
WFLYDM0099: Password should have at least 8 characters!
Are you sure you want to use the password entered yes/no? yes
Re-enter Password :
What groups do you want this user to belong to? (Please enter a comma separated list, or leave blank for none)[ ]: gerente
About to add user 'Juan' for realm 'ApplicationRealm'
Is this correct yes/no? y
```

De esta manera quedo agregado el usuario Juan al rol gerente.

```
root@Artorias: /home/artorias/Desktop/Programming/JavaE...
- The password should contain at least 8 characters, 1 alphabetic character(s), 1 digit(s), 1 non-alphanumeric symbol(s)
Password :
WFLYDM0099: Password should have at least 8 characters!
Are you sure you want to use the password entered yes/no? yes
Re-enter Password :
What groups do you want this user to belong to? (Please enter a comma separated list, or leave blank for none)[ ]: gerente
About to add user 'Juan' for realm 'ApplicationRealm'
Is this correct yes/no? y
Added user 'Juan' to file '/home/artorias/Desktop/Programming/JavaEE___Practices/Material/03a_JakartaEE-Authorization/target/server/standalone/configuration/application-users.properties'
Added user 'Juan' to file '/home/artorias/Desktop/Programming/JavaEE___Practices/Material/03a_JakartaEE-Authorization/target/server/domain/configuration/application-users.properties'
Added user 'Juan' with groups gerente to file '/home/artorias/Desktop/Programming/JavaEE___Practices/Material/03a_JakartaEE-Authorization/target/server/standalone/configuration/application-roles.properties'
Added user 'Juan' with groups gerente to file '/home/artorias/Desktop/Programming/JavaEE___Practices/Material/03a_JakartaEE-Authorization/target/server/domain/configuration/application-roles.properties'
root@Artorias: /home/artorias/Desktop/Programming/JavaEE___Practices/Material/03a_JakartaEE-Authorization/target/server/bin#
```

Siguientemente, podemos intentar lo mismo, pero esta vez, agregando el us1 al grupo empleado.

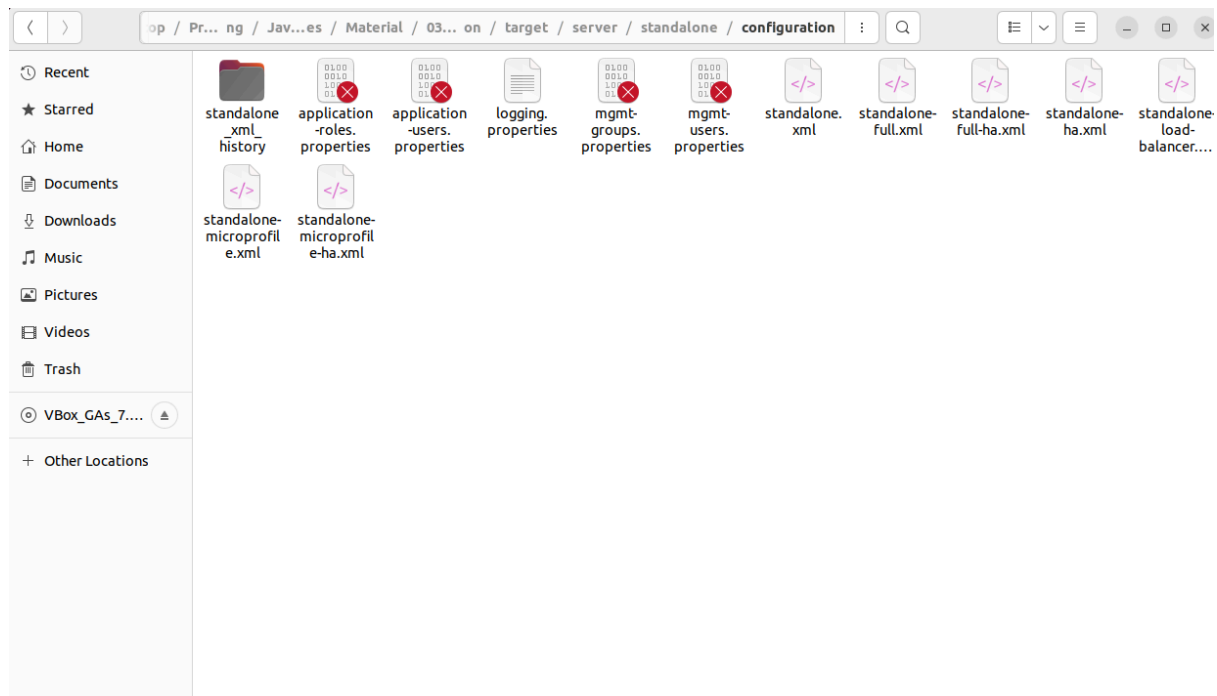
```
root@Artorias: /home/artorias/Desktop/Programming/JavaE...
root@Artorias:/home/artorias/Desktop/Programming/JavaEE___Practices/Material/03a
JakartaEE-Authorization/target/server/bin# ./add-user.sh

What type of user do you wish to add?
a) Management User (mgmt-users.properties)
b) Application User (application-users.properties)
(a): b






Enter the details of the new user to add.
Using realm 'ApplicationRealm' as discovered from the existing property files.
Username : usr1
Password recommendations are listed below. To modify these restrictions edit the
add-user.properties configuration file.
- The password should be different from the username
- The password should not be one of the following restricted values {root, admini
n, administrator}
- The password should contain at least 8 characters, 1 alphabetic character(s),
1 digit(s), 1 non-alphanumeric symbol(s)
Password :
WFLYDM0099: Password should have at least 8 characters!
Are you sure you want to use the password entered yes/no? yes
Re-enter Password :
What groups do you want this user to belong to? (Please enter a comma separated
list, or leave blank for none)[ ]: empleado
```

Y así replicaremos con los demás solicitados.

Una vez hecho esto, nos dirigiremos a la carpeta /server/standalone/configuration para chequear los archivos application-roles.properties y el archivo application-users.properties.



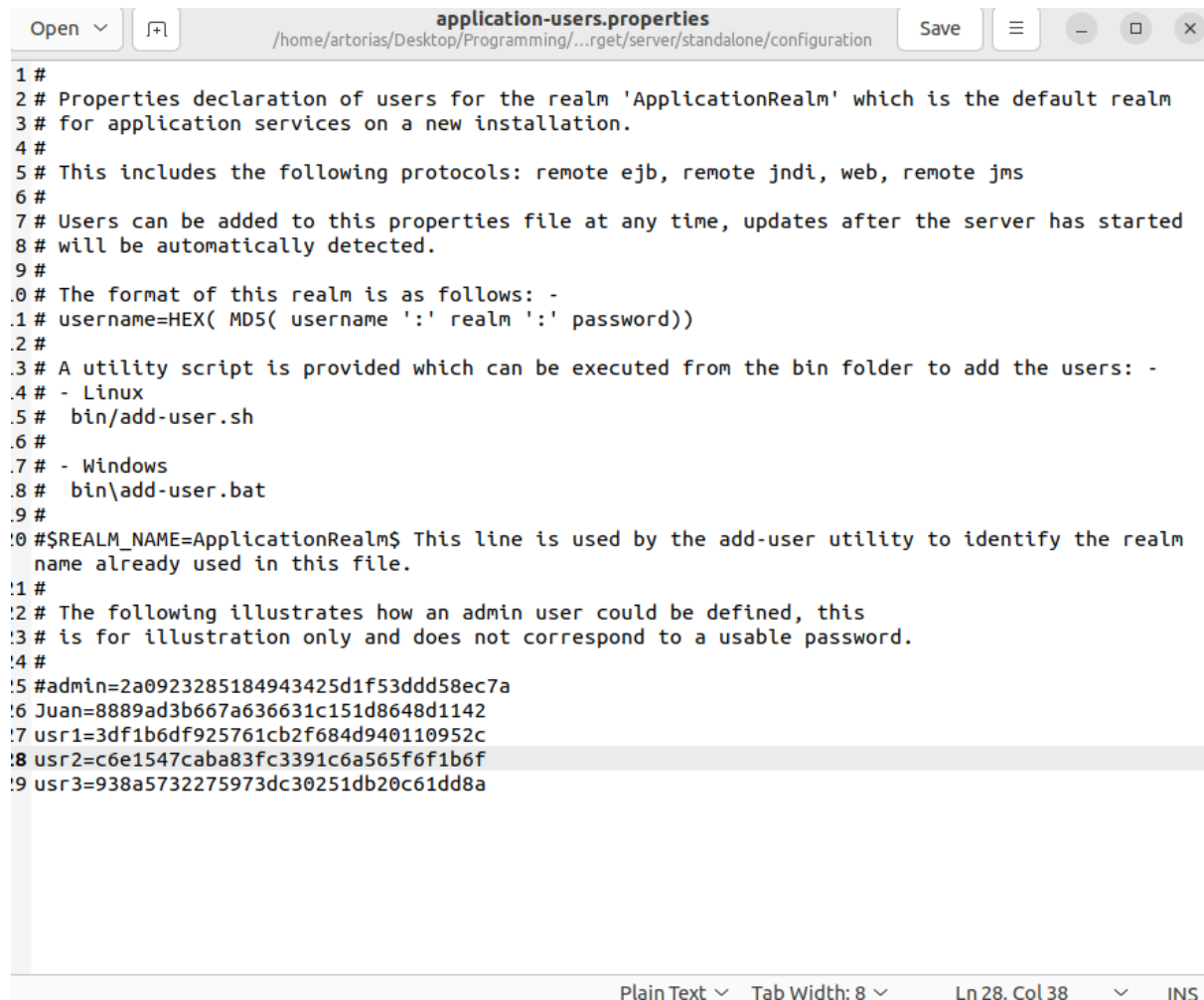
Aquí podemos ver los usuarios y sus respectivos roles

Open ▾  application-roles.properties Save    

/home/artorias/Desktop/Programming/...rget/server/standalone/configuration

```
1 #
2 # Properties declaration of users roles for the realm 'ApplicationRealm' which is the default
  realm
3 # for application services on a new installation.
4 #
5 # This includes the following protocols: remote ejb, remote jndi, web, remote jms
6 #
7 # Users can be added to this properties file at any time, updates after the server has started
8 # will be automatically detected.
9 #
10 # The format of this file is as follows: -
11 # username=role1,role2,role3
12 #
13 # A utility script is provided which can be executed from the bin folder to add the users: -
14 # - Linux
15 #   bin/add-user.sh
16 #
17 # - Windows
18 #   bin\add-user.bat
19 #
20 # The following illustrates how an admin user could be defined.
21 #
22 #admin=PowerUser,BillingAdmin,
23 #guest=guest
24 Juan=gerente
25 usr1=empleado
26 usr2=empleado
27 usr3=gerente
```

Plain Text ▾ Tab Width: 8 ▾ Ln 23, Col 13 ▾ INS



```
1 #
2 # Properties declaration of users for the realm 'ApplicationRealm' which is the default realm
3 # for application services on a new installation.
4 #
5 # This includes the following protocols: remote ejb, remote jndi, web, remote jms
6 #
7 # Users can be added to this properties file at any time, updates after the server has started
8 # will be automatically detected.
9 #
10 # The format of this realm is as follows: -
11 # username=HEX( MD5( username ':' realm ':' password))
12 #
13 # A utility script is provided which can be executed from the bin folder to add the users: -
14 # - Linux
15 #   bin/add-user.sh
16 #
17 # - Windows
18 #   bin\add-user.bat
19 #
20 # $REALM_NAME=ApplicationRealm$ This line is used by the add-user utility to identify the realm
21 # name already used in this file.
22 #
23 # The following illustrates how an admin user could be defined, this
24 # is for illustration only and does not correspond to a usable password.
25 #
26 #admin=2a0923285184943425d1f53ddd58ec7a
27 # Juan=8889ad3b667a636631c151d8648d1142
28 #usr1=3df1b6df925761cb2f684d940110952c
29 #usr2=c6e1547caba83fc3391c6a565f6f1b6f
30 #usr3=938a5732275973dc30251db20c61dd8a
```

Y aqui en el user properties, podemos ver lo que seria el password hasheado, para cada user respectivo.

3) Para el siguiente punto debemos utilizar un curl sin credenciales e invocar el endpoint gerente/enviarMensaje?mensaje=hola.
Para esto invocamos el endpoint con un curl curl -v
http://localhost:8080/03a_JakartaEE-Authorization/mensajes/gerente/enviarMensaje?mensaje=hola
Obtendremos la siguiente respuesta.

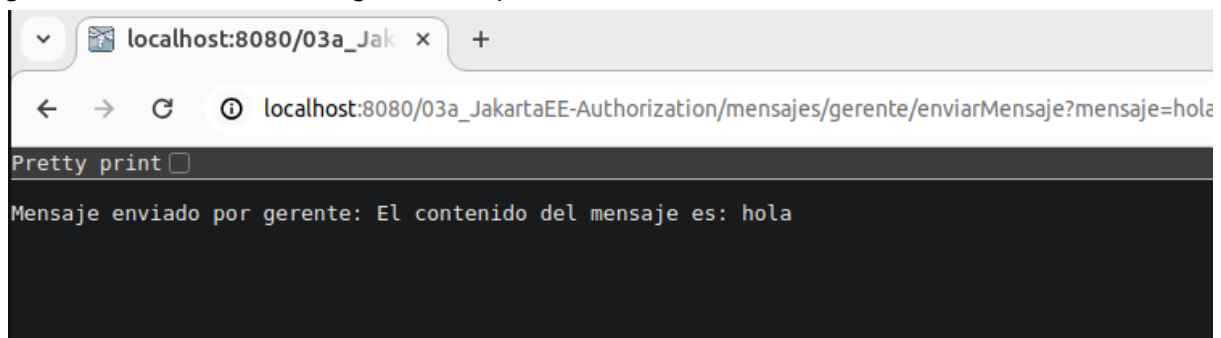
```
root@Artorias: /home/artorias/Desktop/Programming/JavaEE__Practices/Material/03a_JakartaEE-Authorization
JakartaEE-Authorization# curl -v http://localhost:8080/03a_JakartaEE-Authorization/mensajes/gerente/enviarMensaje?mensaje=hol
* Trying 127.0.0.1:8080...
* Connected to localhost (127.0.0.1) port 8080 (#0)
> GET /03a_JakartaEE-Authorization/mensajes/gerente/enviarMensaje?mensaje=hol HTTP/1.1
Host: localhost:8080
User-Agent: curl/7.81.0
Accept: */*

< HTTP/1.1 401 Unauthorized
Expires: 0
Connection: keep-alive
WWW-Authenticate: Basic realm="ApplicationRealm"
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Content-Type: text/html;charset=UTF-8
Content-Length: 71
Date: Wed, 17 Apr 2024 20:05:31 GMT

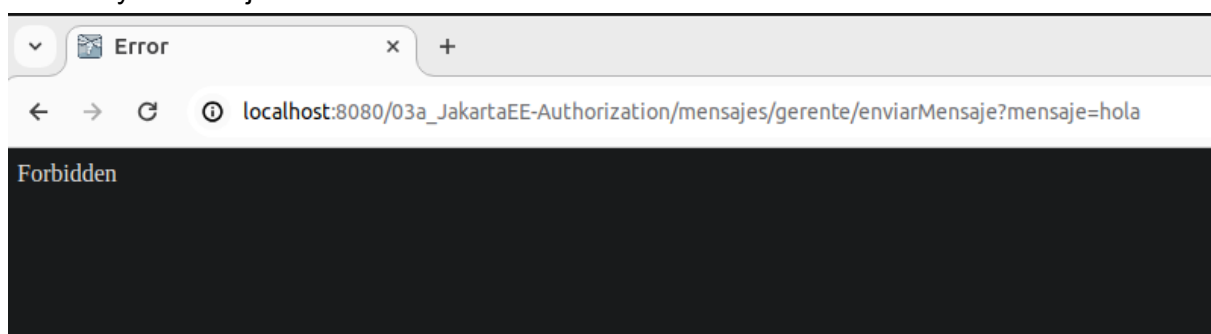
* Connection #0 to host localhost left intact
<html><head><title>Error</title></head><body>Unauthorized</body></html>root@Artorroroorooroot@Aroot@Artoriasroot@Aroot@roororr
root@Artorias: /home/artorias/Desktop/Programming/JavaEE__Practices/Material/03a_JakartaEE-Authorization#
```

Como se puede ver, nos arroja 401 Unauthorized, esto es, por el grupo al que intentamos acceder, que es gerente, no tenemos los permisos.

4) Intentamos nuevamente tomar ese endpoint pero esta vez en el browser. En este momento nos sale una pantalla de login, la cual usaremos la del us3 que era gerente, obtendremos la siguiente respuesta.

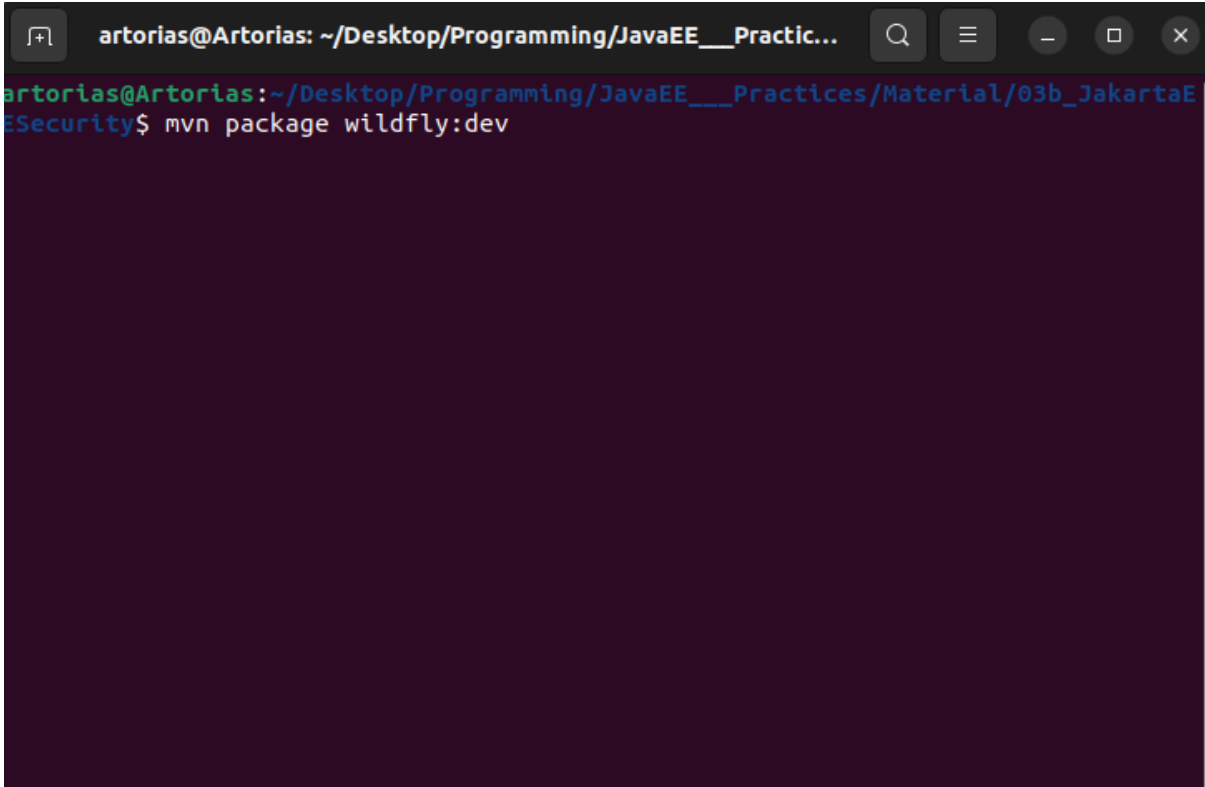


5) En el siguiente punto haremos lo mismo, pero con credenciales de `usr1` y `usr2`. Para ambos casos, vemos que esos grupos de usuarios no tienen permisos para poder acceder y nos arroja un `Forbidden`.



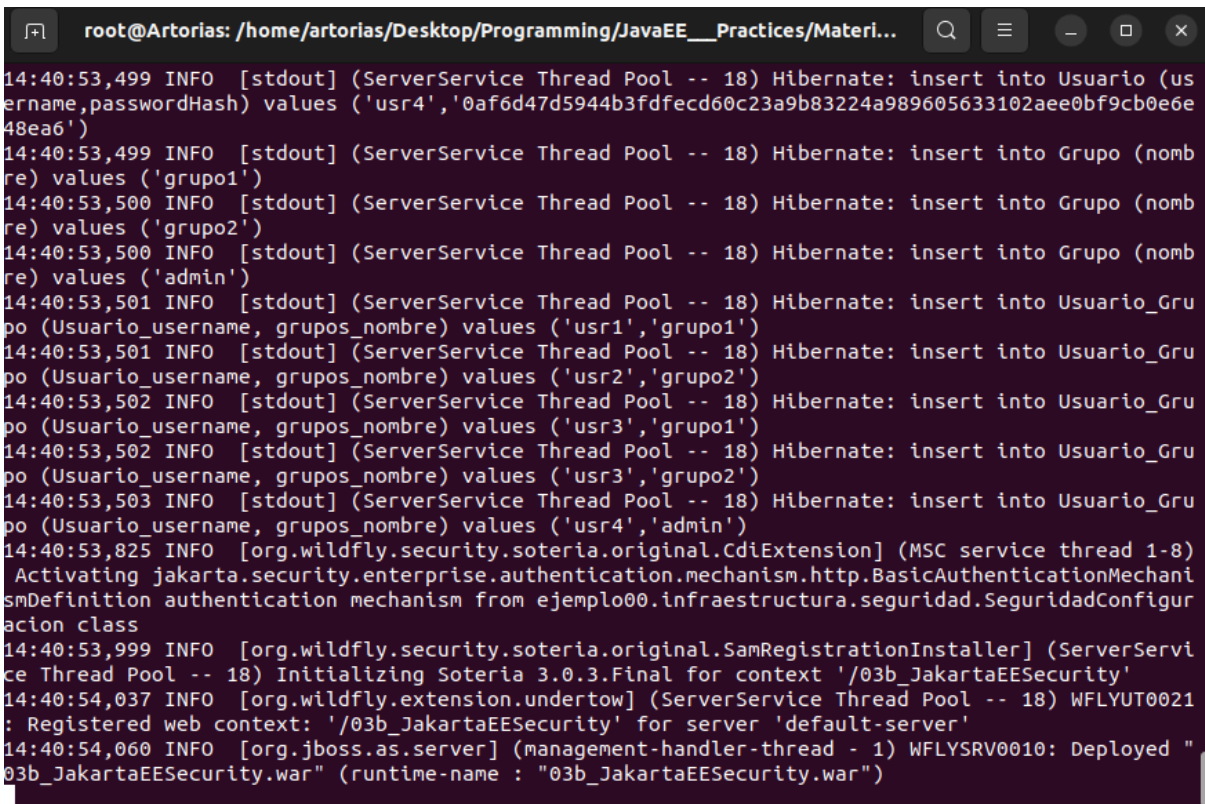
6) Primero debemos bajar el código que el docente nos provee. Una vez bajado, podemos proceder a levantar el servidor.

Debemos ejecutar el comando `mvn package wildfly:dev`.
Podemos ver lo siguiente:



```
artorias@Artorias: ~/Desktop/Programming/JavaEE__Practic...
artorias@Artorias:~/Desktop/Programming/JavaEE__Practices/Material/03b_JakartaEESecurity$ mvn package wildfly:dev
```

Y al deployar se vería lo siguiente:



```
root@Artorias: /home/artorias/Desktop/Programming/JavaEE__Practices/Materi...
14:40:53,499 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Usuario (username,passwordHash) values ('usr4','0af6d47d5944b3dfd60c23a9b83224a989605633102aee0bf9cb0e6e48ea6')
14:40:53,499 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Grupo (nombre) values ('grupo1')
14:40:53,500 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Grupo (nombre) values ('grupo2')
14:40:53,500 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Grupo (nombre) values ('admin')
14:40:53,501 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Usuario_Grupo (Usuario_username, grupos_nombre) values ('usr1','grupo1')
14:40:53,501 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Usuario_Grupo (Usuario_username, grupos_nombre) values ('usr2','grupo2')
14:40:53,502 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Usuario_Grupo (Usuario_username, grupos_nombre) values ('usr3','grupo1')
14:40:53,502 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Usuario_Grupo (Usuario_username, grupos_nombre) values ('usr3','grupo2')
14:40:53,503 INFO [stdout] (ServerService Thread Pool -- 18) Hibernate: insert into Usuario_Grupo (Usuario_username, grupos_nombre) values ('usr4','admin')
14:40:53,825 INFO [org.wildfly.security.soteria.original.CdiExtension] (MSC service thread 1-8) Activating jakarta.security.enterprise.authentication.mechanism.http.BasicAuthenticationMechanismDefinition authentication mechanism from ejemplo00.infraestructura.seguridad.SeguridadConfiguracion class
14:40:53,999 INFO [org.wildfly.security.soteria.original.SamRegistrationInstaller] (ServerService Thread Pool -- 18) Initializing Soteria 3.0.3.Final for context '/03b_JakartaEESecurity'
14:40:54,037 INFO [org.wildfly.extension.undertow] (ServerService Thread Pool -- 18) WFLYUT0021: Registered web context: '/03b_JakartaEESecurity' for server 'default-server'
14:40:54,060 INFO [org.jboss.as.server] (management-handler-thread - 1) WFLYSRV0010: Deployed "03b_JakartaEESecurity.war" (runtime-name : "03b_JakartaEESecurity.war")
```