Desarrollo Seguro de Aplicaciones Web con OWASP

Lab: Encrypt Sensitive Data – JBoss EAP

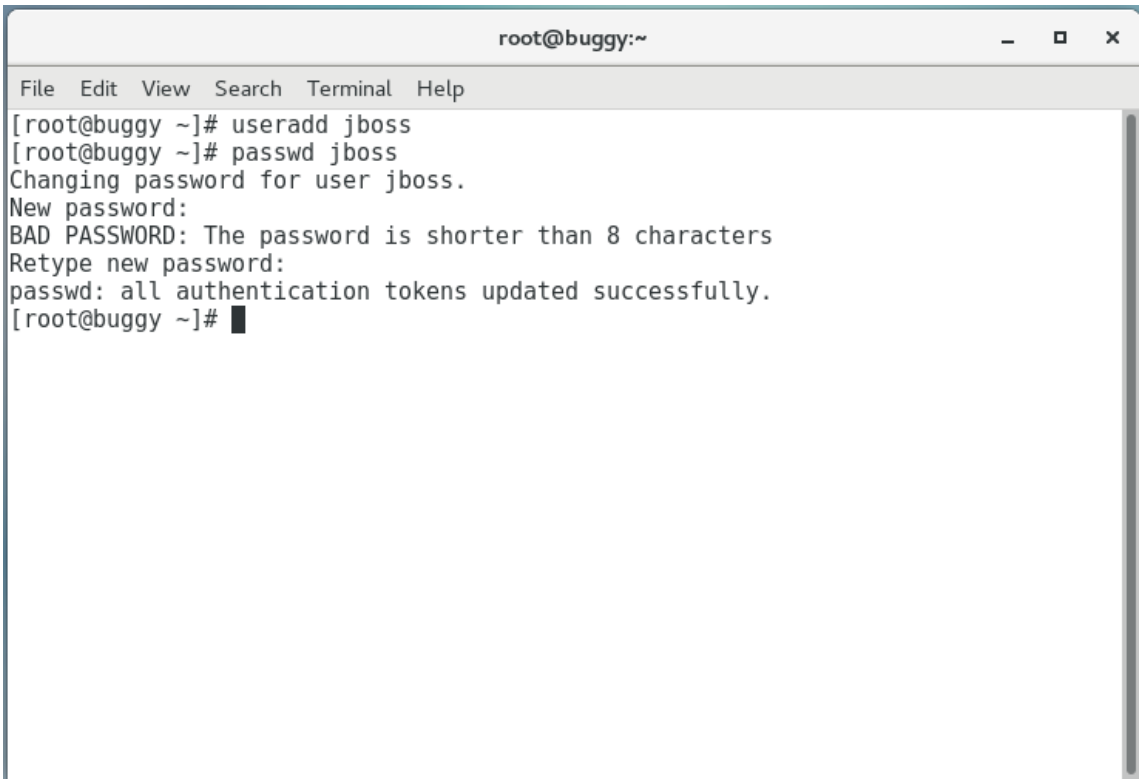
Objetivo

- Encriptar los datos sensibles en JBoss EAP

Procedimiento

1. Instalar y configurar JBoss EAP

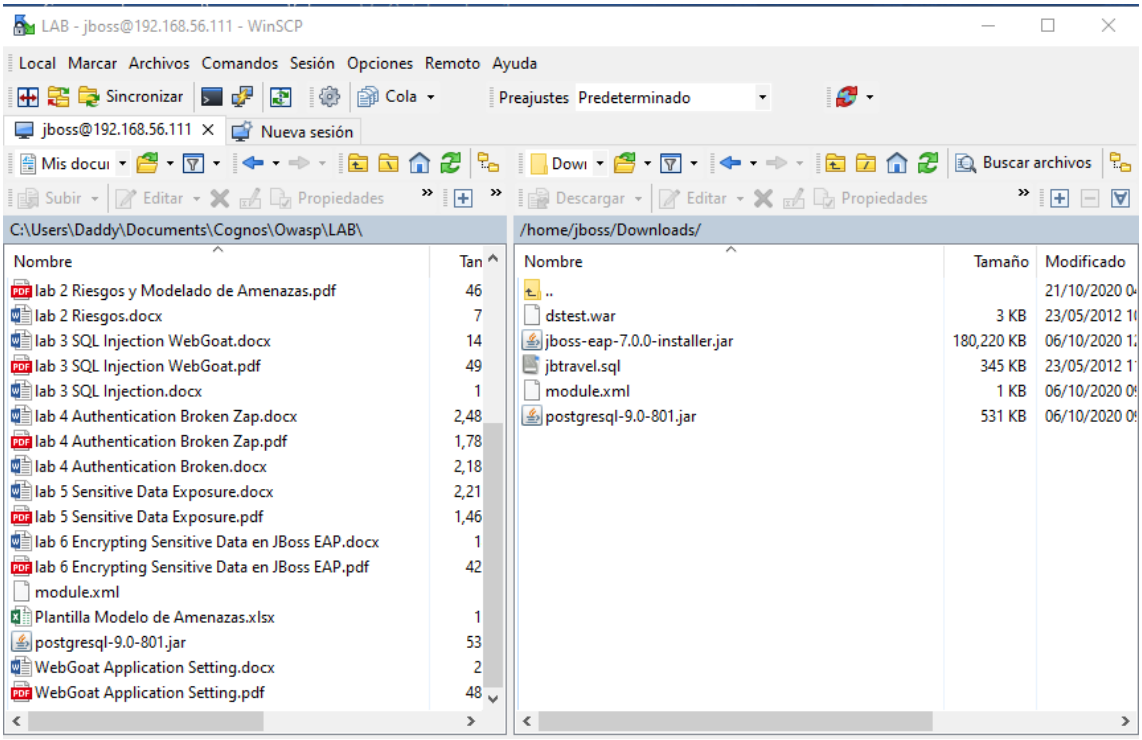
   Crear el usuario jboss



   Ingresar con el usuario jboss, verificar la siguiente estructura.

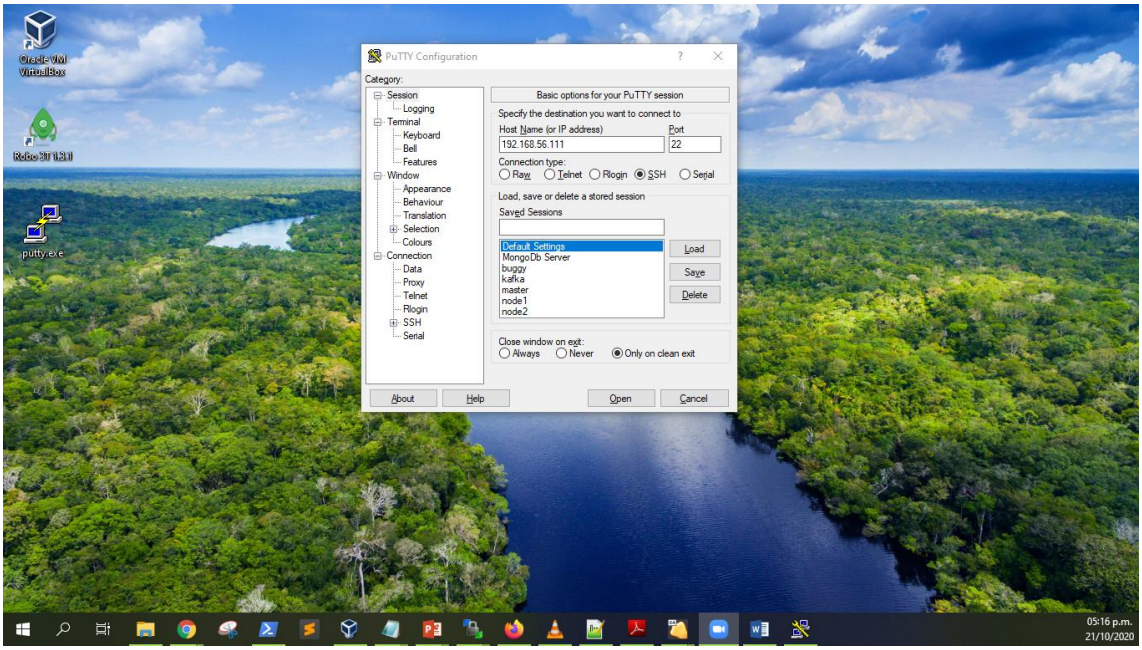
```
jboss@buggy:~
File  Edit  View  Search  Terminal  Help
[jboss@buggy ~]$ ll
total 0
drwxr-xr-x 2 jboss jboss 6 Oct 21 16:51 Desktop
drwxr-xr-x 2 jboss jboss 6 Oct 21 16:51 Documents
drwxr-xr-x 2 jboss jboss 6 Oct 21 16:51 Downloads
drwxr-xr-x 2 jboss jboss 6 Oct 21 16:51 Music
drwxr-xr-x 2 jboss jboss 6 Oct 21 16:51 Pictures
drwxr-xr-x 2 jboss jboss 6 Oct 21 16:51 Public
drwxr-xr-x 2 jboss jboss 6 Oct 21 16:51 Templates
drwxr-xr-x 2 jboss jboss 6 Oct 21 16:51 Videos
[jboss@buggy ~]$ pwd
/home/jboss
[jboss@buggy ~]$
```

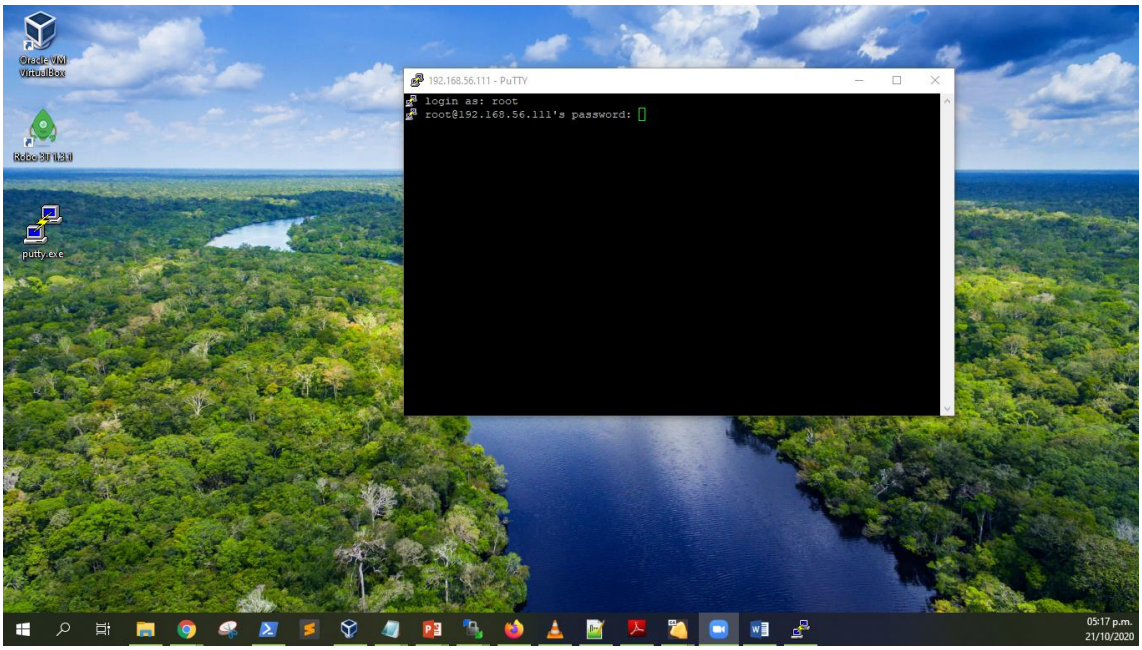
Con winscp copiar los archivos de trabajo al directorio Downloads del usuario jboss.



2. Instalar postgresql y configurar el archivo de acceso

Ingresa con putty.exe y con la cuenta root al servidor.





En la sesión root con putty.exe ejecuta los siguientes comandos:

yum install https://download.postgresql.org/pub/repos/yum/9.6/redhat/rhel-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm -y

yum install postgresql96 postgresql96-server postgresql96-contrib postgresql96-libs -y

/usr/pgsql-9.6/bin/postgresql96-setup initdb

systemctl enable postgresql-9.6.service

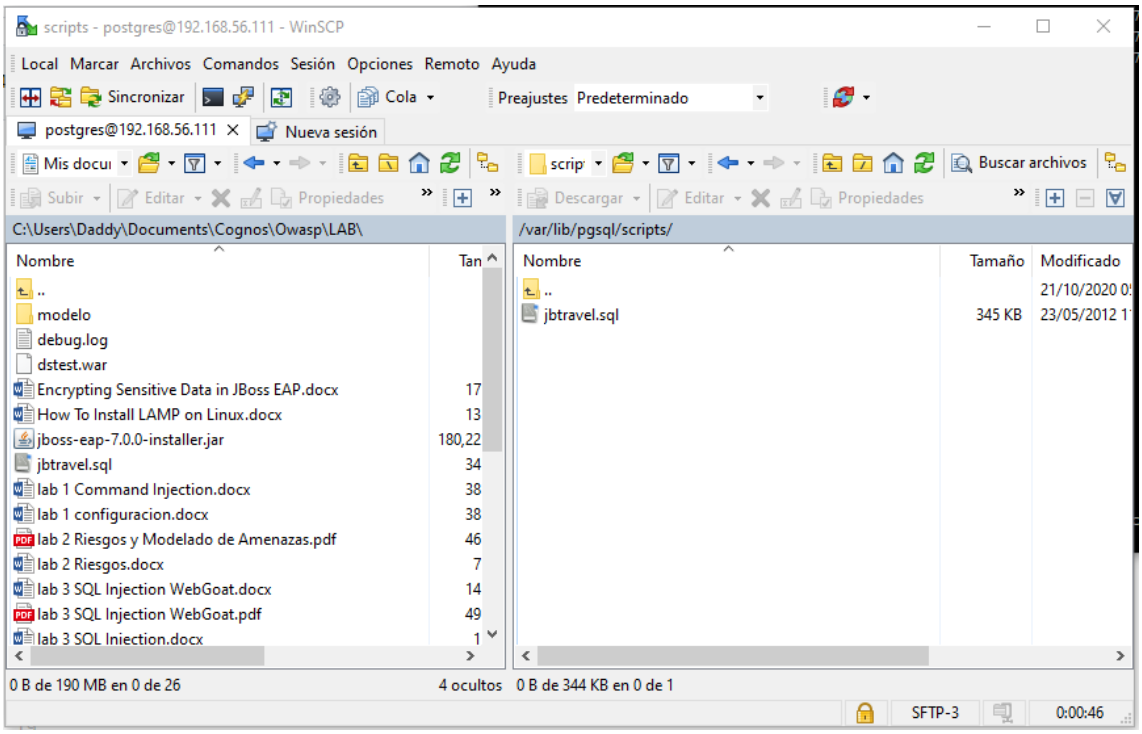
systemctl start postgresql-9.6.service

Asigna la clave postgres al usuario postgres.

[root@buggy ~]# hostname
buggy.example.com
[root@buggy ~]# **cat /etc/hosts**
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
192.168.56.111 buggy buggy.example.com
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
[root@buggy ~]# **passwd postgres**
Changing password for user postgres.
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.
[root@buggy ~]#

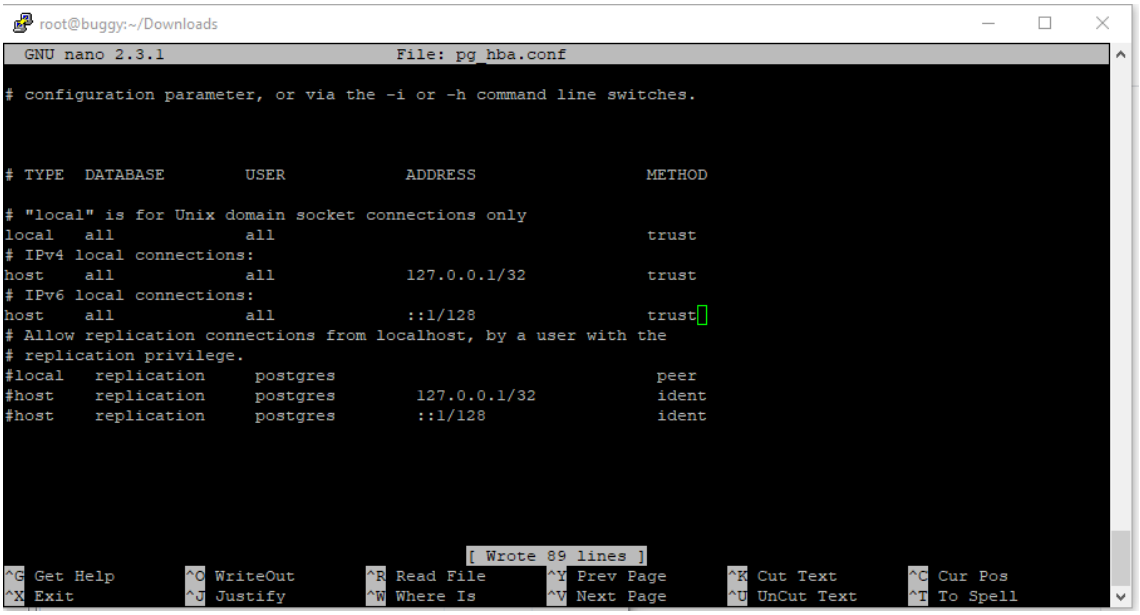
[root@buggy ~]# **su - postgres**
Last login: Wed Oct 21 17:34:31 -05 2020 on pts/1
-bash-4.2$ **mkdir scripts**
-bash-4.2$ **cd scripts**
-bash-4.2$ **pwd**
/var/lib/pgsql/scripts

Copia con winscp y usando la cuenta postgres el archivo jbtravel.sql al directorio /var/lib/pgsql/scripts



Cambiar la configuración de host.

-bash-4.2$ ls
9.6 scripts
-bash-4.2$ **cd 9.6/**
-bash-4.2$ **ls**
backups data initdb.log
-bash-4.2$ **cd data/**
-bash-4.2$ ls
base pg_commit_ts pg_log pg_replslot pg_stat_tmp PG_VERSION postmaster.opts
global pg_dynshmem pg_logical pg_serial pg_subtrans pg_xlog postmaster.pid
log pg_hba.conf pg_multixact pg_snapshots pg_tblspc postgresql.auto.conf
pg_clog pg_ident.conf pg_notify pg_stat pg_twophase postgresql.conf
-bash-4.2$ **pwd**
/var/lib/pgsql/9.6/data
-bash-4.2$ **nano pg_hba.conf**



Reiniciar el servidor con la cuenta root.

[root@buggy Downloads]# systemctl stop postgresql-9.6.service

[root@buggy Downloads]# systemctl start postgresql-9.6.service

3. Crear el modelo de base de datos JBTravel

Inicia con postgres y ejecuta el siguiente comando:

-bash-4.2$ psql -f scripts/jbtravel.sql

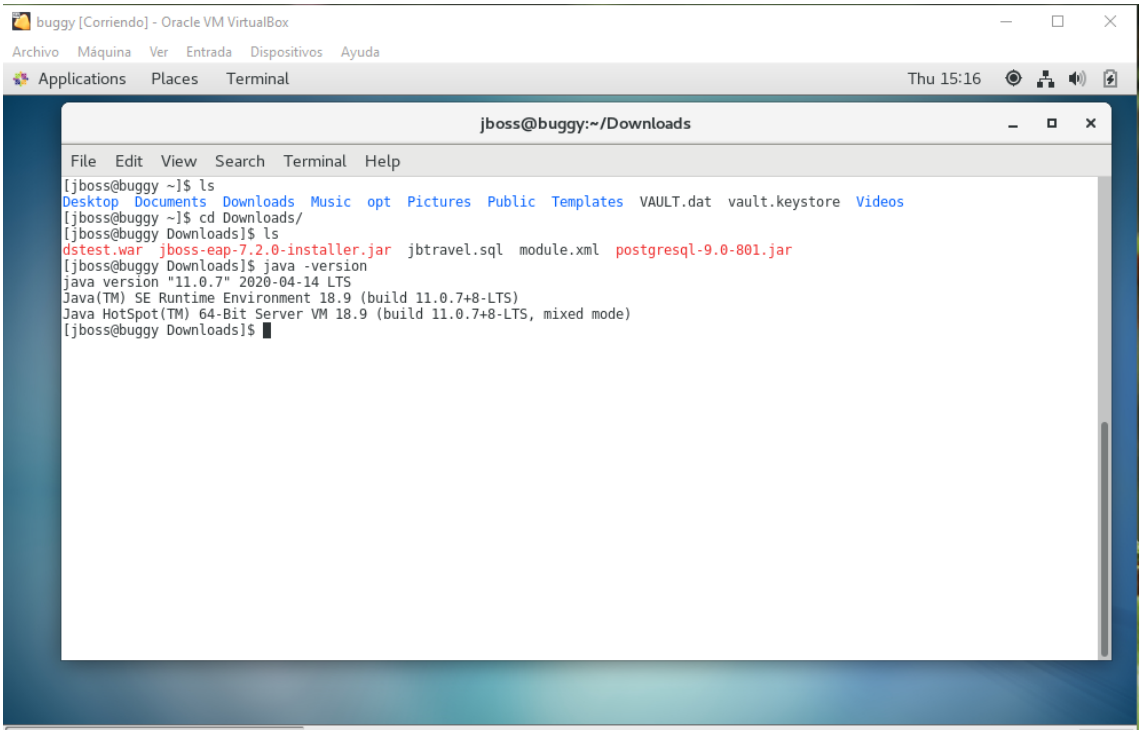
Comprobamos

```
-bash-4.2$ psql
psql (9.6.19)
Type "help" for help.

postgres=# \dt jbtravel.*
            List of relations
  Schema  |      Name       | Type  |  Owner
----------+-----------------+-------+----------
 jbtravel | airport         | table | postgres
 jbtravel | flight          | table | postgres
 jbtravel | plane           | table | postgres
 jbtravel | reservation     | table | postgres
 jbtravel | route           | table | postgres
 jbtravel | seat            | table | postgres
 jbtravel | user            | table | postgres
 jbtravel | val_billingtype | table | postgres
 jbtravel | val_mealtype    | table | postgres
 jbtravel | val_seatclass   | table | postgres
 jbtravel | val_seattype    | table | postgres
(11 rows)

postgres=# select username, password from jbtravel.user;
  username  | password
------------+----------
 mobius     | jboss
 duchess    | jboss
 starbuck   | jboss
 chosen1    | jboss
 hankinator | jboss
 doctor_o   | jboss
 capt_mal   | jboss
 yyyup      | jboss
 avg_joe    | jboss
 stirfryday | jboss
 the_major  | jboss
 watchtower | jboss
 goodintel  | jboss
 lantern    | jboss
 fullmetal  | jboss
 iq187      | jboss
 ironman    | jboss
 smooth     | jboss
 bride      | jboss
 student    | jboss
 admin      | admin
```

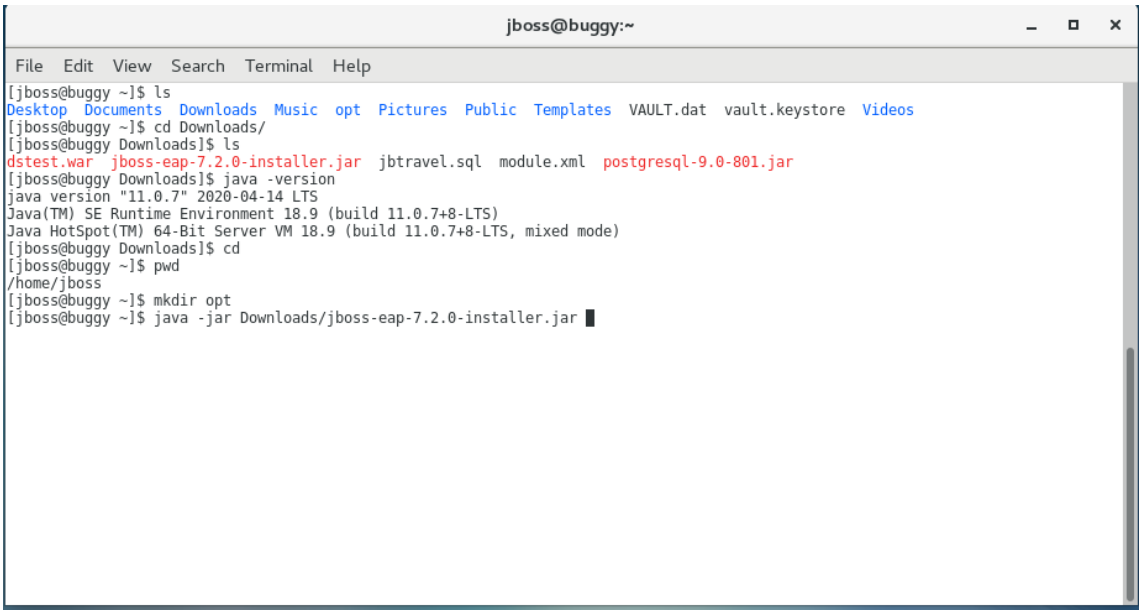
(21 rows)
postgres=# \q
-bash-4.2$

4. Instalar JBoss EAP 7.2

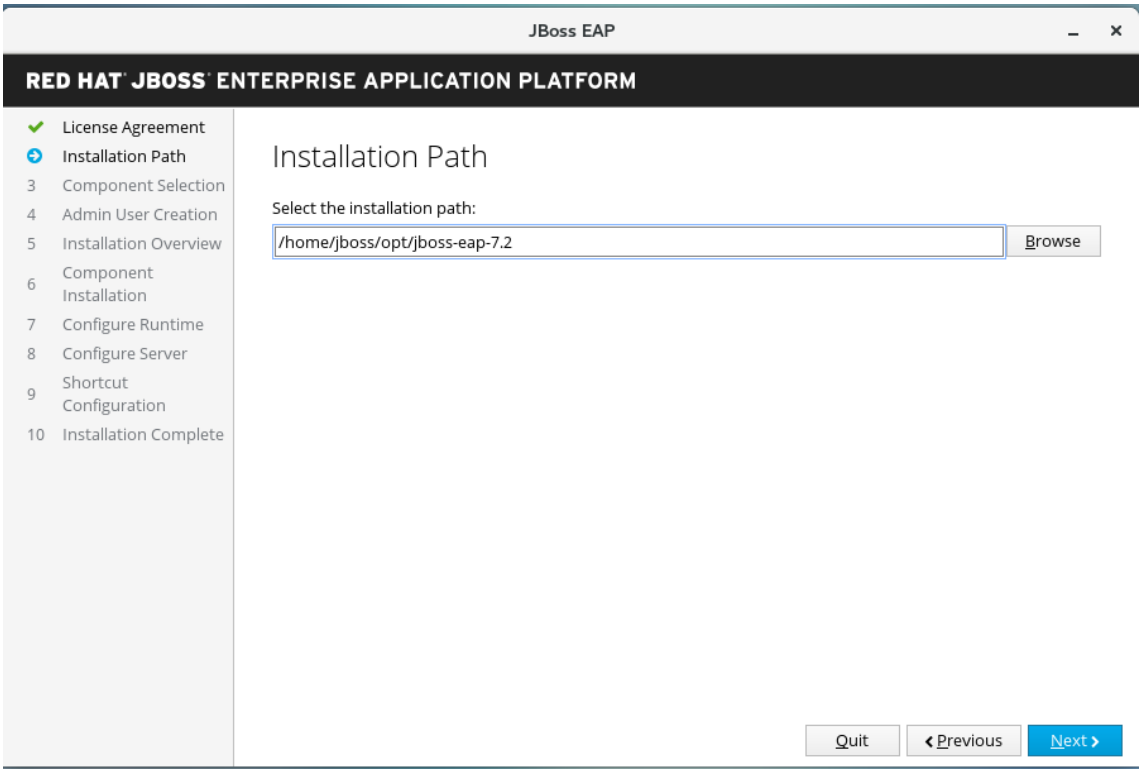
Verificar la versión de Java, debe ser 8 o superior.



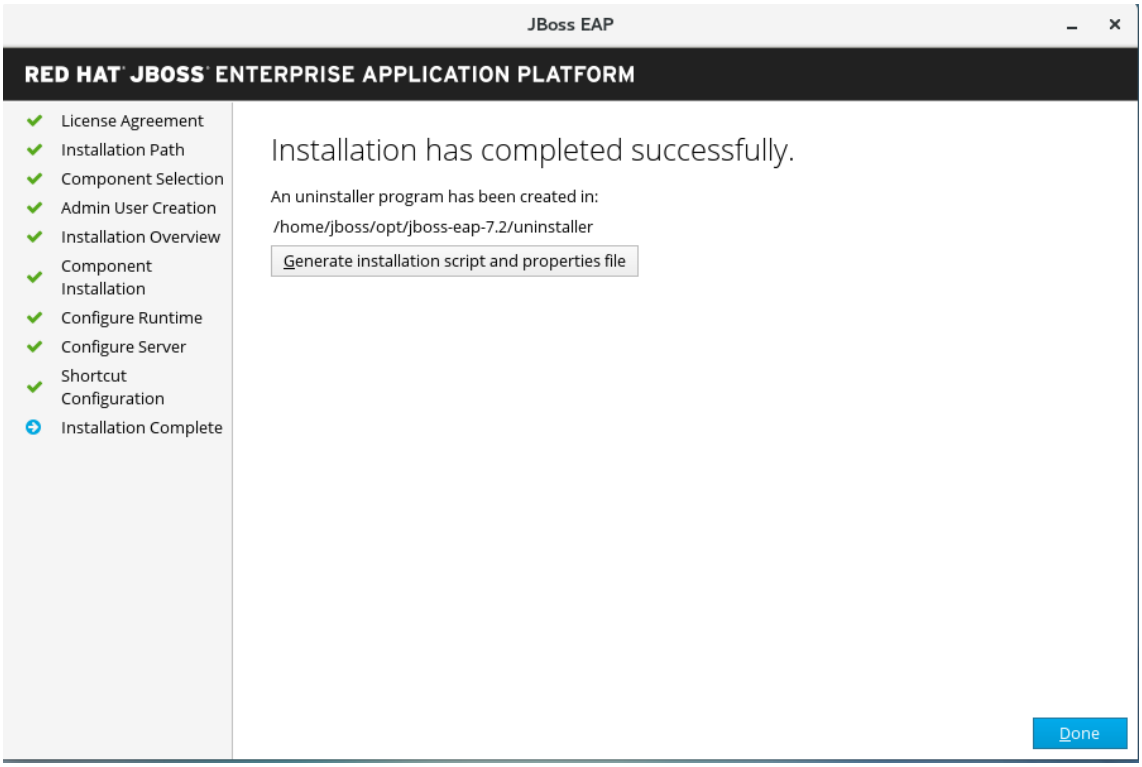
Crea la carpeta opt en el home de jboss y ejecuta el instalador



Seguir los pasos del asistente. Instalar el software en /home/jboss/opt/jboss-eap-7.2



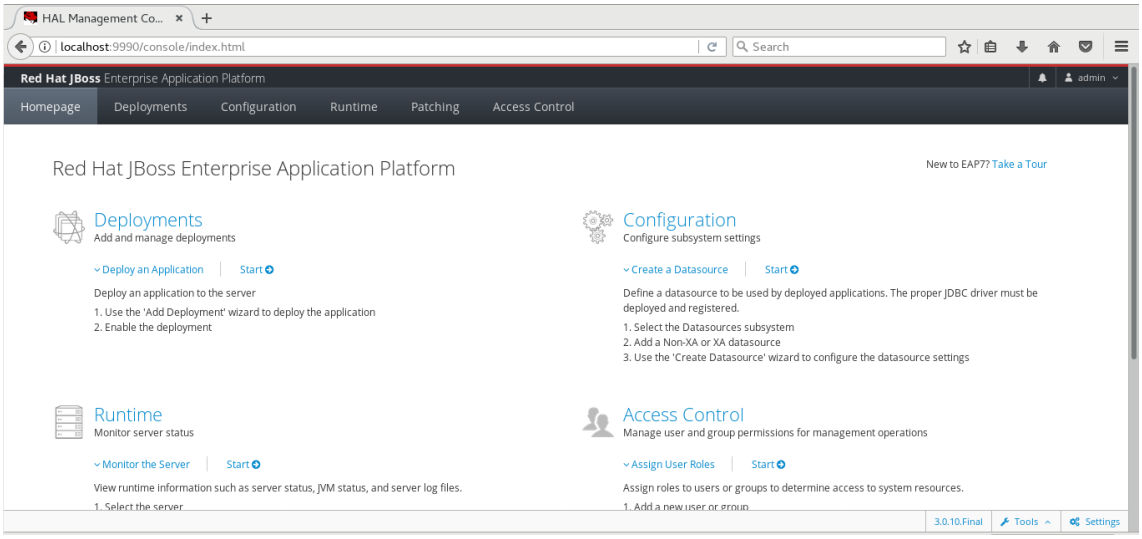
Crea el usuario admin con clave jboss#1!



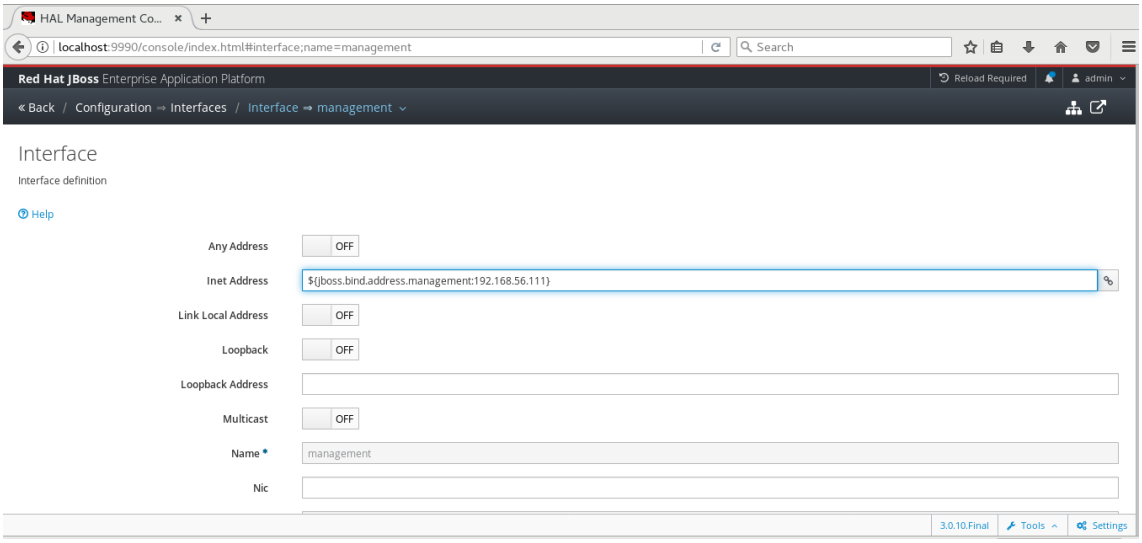
Iniciar el servidor JBoss EAP en modo Standalone.

```
jboss@buggy:~/opt/jboss-eap-7.2/bin
File  Edit  View  Search  Terminal  Help
[jboss@buggy ~]$ cd opt/
[jboss@buggy opt]$ ls
jboss-eap-7.2
[jboss@buggy opt]$ cd jboss-eap-7.2/
[jboss@buggy jboss-eap-7.2]$ ls
appclient  docs    installation   jboss-modules.jar  migration  standalone   version.txt
bin        domain  JBossEULA.txt  LICENSE.txt        modules    uninstaller  welcome-content
[jboss@buggy jboss-eap-7.2]$ cd bin
[jboss@buggy bin]$ ls
add-user.bat         common.ps1        jboss-cli.bat                jdr.sh              vault.sh
add-user.properties  common.sh         jboss-cli-logging.properties launcher.jar        wildfly-elytron-tool.jar
add-user.ps1         domain.bat        jboss-cli.ps1                product.conf        wsconsume.bat
add-user.sh          domain.conf       jboss-cli.sh                 service.bat         wsconsume.ps1
appclient.bat        domain.conf.bat   jboss-cli.xml                standalone.bat      wsconsume.sh
appclient.conf       domain.conf.ps1   jboss-server-migration.bat   standalone.conf     wsprovide.bat
appclient.conf.bat   domain.ps1        jboss-server-migration.sh    standalone.conf.bat wsprovide.ps1
appclient.conf.ps1   domain.sh         jconsole.bat                 standalone.conf.ps1 wsprovide.sh
appclient.ps1        elytron-tool.bat  jconsole.ps1                 standalone.ps1
appclient.sh         elytron-tool.ps1  jconsole.sh                  standalone.sh
client               elytron-tool.sh   jdr.bat                      vault.bat
common.bat           init.d            jdr.ps1                      vault.ps1
[jboss@buggy bin]$ pwd
/home/jboss/opt/jboss-eap-7.2/bin
[jboss@buggy bin]$ ./standalone.sh
=========================================================================

  JBoss Bootstrap Environment

  JBOSS_HOME: /home/jboss/opt/jboss-eap-7.2
```

Actualizar la configuración de red de JBoss EAP para que se enlace a la ip de la red de solo anfitrión. Abrimos la consola de administración e ingresamos con el usuario admin



Actualizar la ip de la interfaz public y la management deben estar enlazadas a la ip de la red solo anfitrión.



5. Configurar un Datasource en JBoss EAP para acceder a la base de datos JBTravel

   Desplegar el driver de la base de datos postgresql.

   [jboss@buggy Downloads]$ **mkdir -p ~/opt/jboss-eap-7.2/modules/system/layers/base/org/postgresql/main**
   [jboss@buggy Downloads]$ **cp module.xml ~/opt/jboss-eap-7.2/modules/system/layers/base/org/postgresql/main**
   [jboss@buggy Downloads]$ **cp postgresql-9.0-801.jar ~/opt/jboss-eap-7.2/modules/system/layers/base/org/postgresql/main**
   [jboss@buggy Downloads]$ **ls ~/opt/jboss-eap-7.2/modules/system/layers/base/org/postgresql/main**
   module.xml postgresql-9.0-801.jar
   [jboss@buggy Downloads]$

   Registra el driver de postgresql

   [jboss@buggy bin]$ **./jboss-cli.sh -c --controller=192.168.56.111**
   [standalone@192.168.56.111:9990 /] /subsystem=datasources/jdbc-driver=postgresql:add(driver-name=postgresql,driver-m
   driver-major-version driver-minor-version driver-module-name*

   [standalone@192.168.56.111:9990 /] **/subsystem=datasources/jdbc-driver=postgresql:add(driver-name=postgresql,driver-module-name=org.postgresql)**
   {"outcome" => "success"}

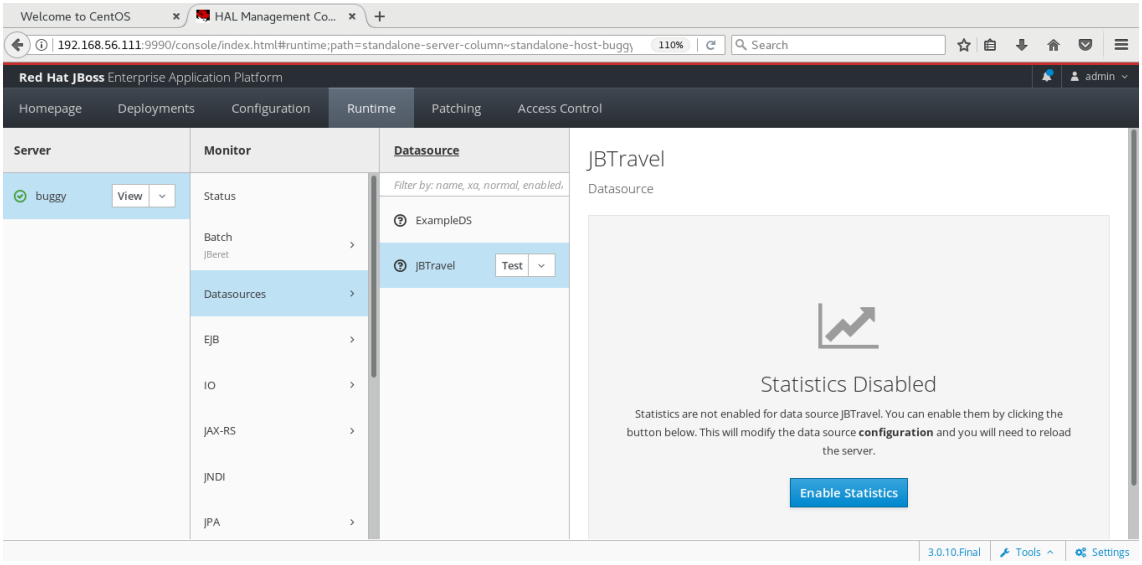
   [standalone@192.168.56.111:9990 /]

   Creacion del Datasource

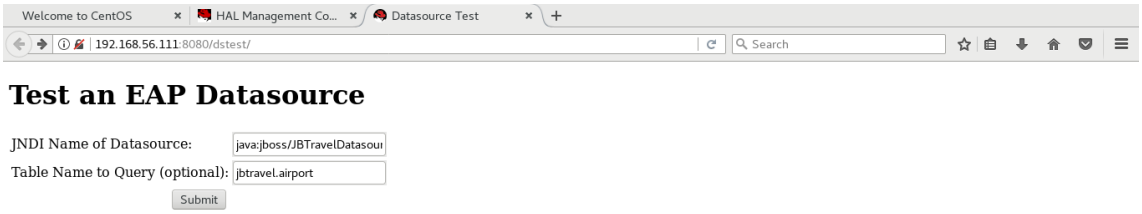
```
<datasource jta="true" jndi-name="java:jboss/JBTravelDatasource" pool-name="JBTravel" enabled="true" use-ccm="true">
   <connection-url>jdbc:postgresql://localhost:5432/postgres</connection-url>
   <driver>postgresql</driver>
   <pool>
      <min-pool-size>5</min-pool-size>
      <max-pool-size>20</max-pool-size>
   </pool>
   <security>
      <user-name>postgres</user-name>
      <password>password</password>
   </security>
   <validation>
      <valid-connection-checker class-name="org.jboss.jca.adapters.jdbc.extensions.postgres.PostgreSQLValidConnectionChecker"/>
      <background-validation>true</background-validation>
      <exception-sorter class-name="org.jboss.jca.adapters.jdbc.extensions.postgres.PostgreSQLExceptionSorter"/>
   </validation>
</datasource>
```

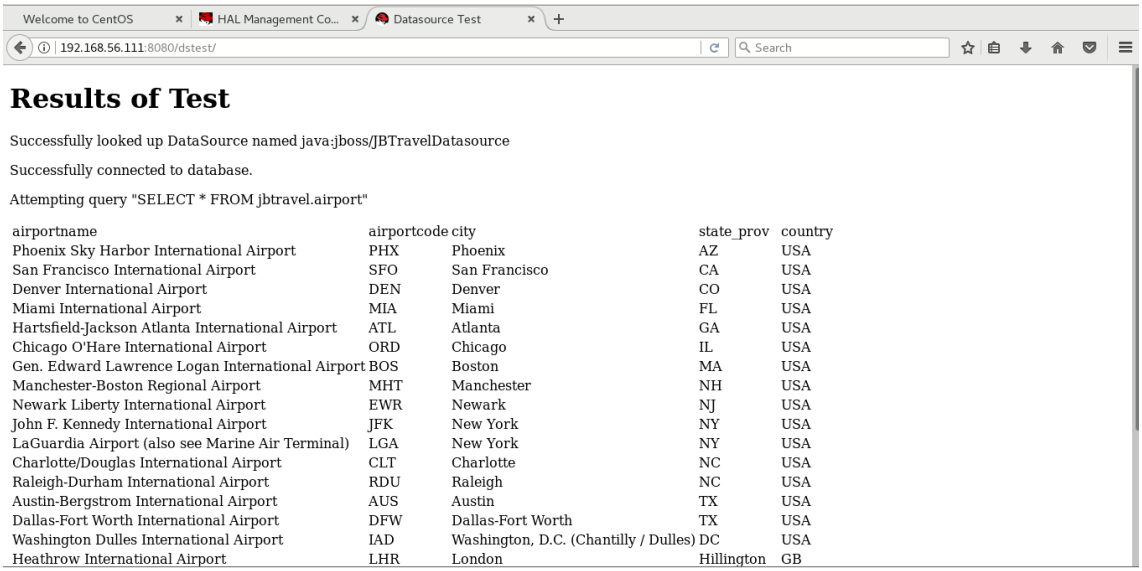
Reinicia el servidor

Prueba el datasource mediante un test en la consola de administración grafica



Desplegar la aplicación dstest





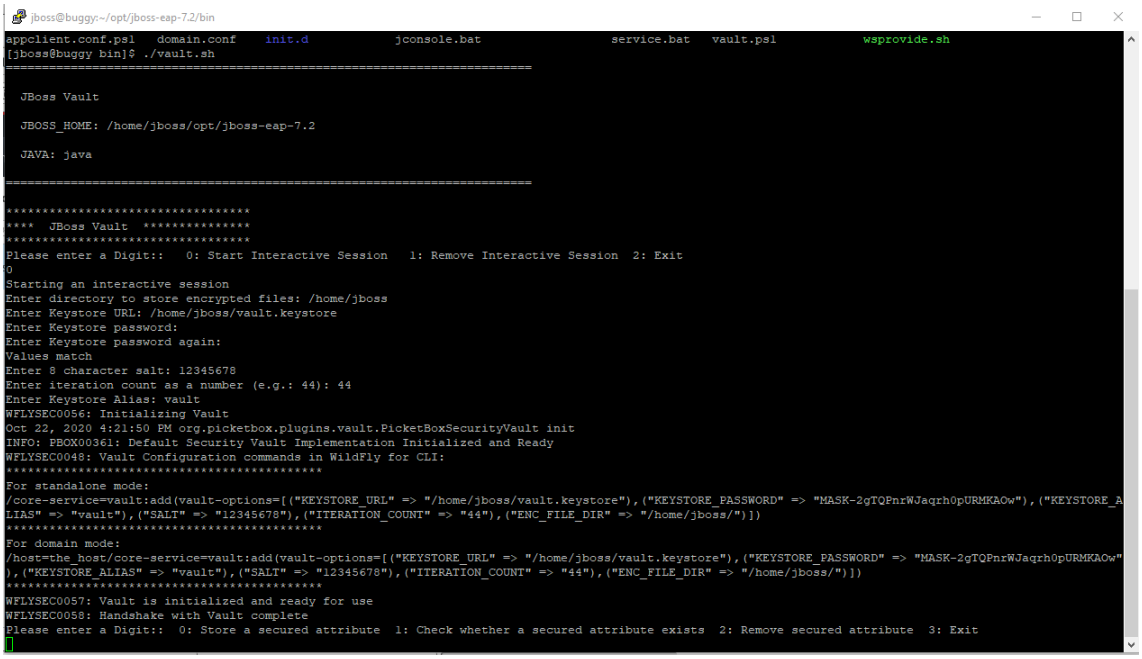
airportname	airportcode	city	state_prov	country
Phoenix Sky Harbor International Airport	PHX	Phoenix	AZ	USA
San Francisco International Airport	SFO	San Francisco	CA	USA
Denver International Airport	DEN	Denver	CO	USA
Miami International Airport	MIA	Miami	FL	USA
Hartsfield-Jackson Atlanta International Airport	ATL	Atlanta	GA	USA
Chicago O'Hare International Airport	ORD	Chicago	IL	USA
Gen. Edward Lawrence Logan International Airport	BOS	Boston	MA	USA
Manchester-Boston Regional Airport	MHT	Manchester	NH	USA
Newark Liberty International Airport	EWR	Newark	NJ	USA
John F. Kennedy International Airport	JFK	New York	NY	USA
LaGuardia Airport (also see Marine Air Terminal)	LGA	New York	NY	USA
Charlotte/Douglas International Airport	CLT	Charlotte	NC	USA
Raleigh-Durham International Airport	RDU	Raleigh	NC	USA
Austin-Bergstrom International Airport	AUS	Austin	TX	USA
Dallas-Fort Worth International Airport	DFW	Dallas-Fort Worth	TX	USA
Washington Dulles International Airport	IAD	Washington, D.C. (Chantilly / Dulles)	DC	USA
Heathrow International Airport	LHR	London	Hillington	GB

6. Cree un almacén de claves de Java

   [jboss@buggy ~]$ keytool -genseckey -alias vault -keyalg AES -storetype jceks -keysize 128 -keystore /home/jboss/vault.keystore
   Enter keystore password:
   Re-enter new password:
   Enter key password for <vault>
   (RETURN if same as keystore password):

   Warning:
   The JCEKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore /home/jboss/vault.keystore -destkeystore /home/jboss/vault.keystore -deststoretype pkcs12".
   [jboss@buggy ~]$ cd opt/jboss-eap-7.2/bin/

7. Ejecute Vault Script para cifrar una contraseña.



8. Configurar la bóveda

   [jboss@buggy bin]$ ./jboss-cli.sh -c --controller=192.168.56.111
   [standalone@192.168.56.111:9990 /] /core-service=vault:add(vault-options=[("KEYSTORE_URL" => "/home/jboss/vault.keystore"),("KEYSTORE_PASSWORD" => "MASK-

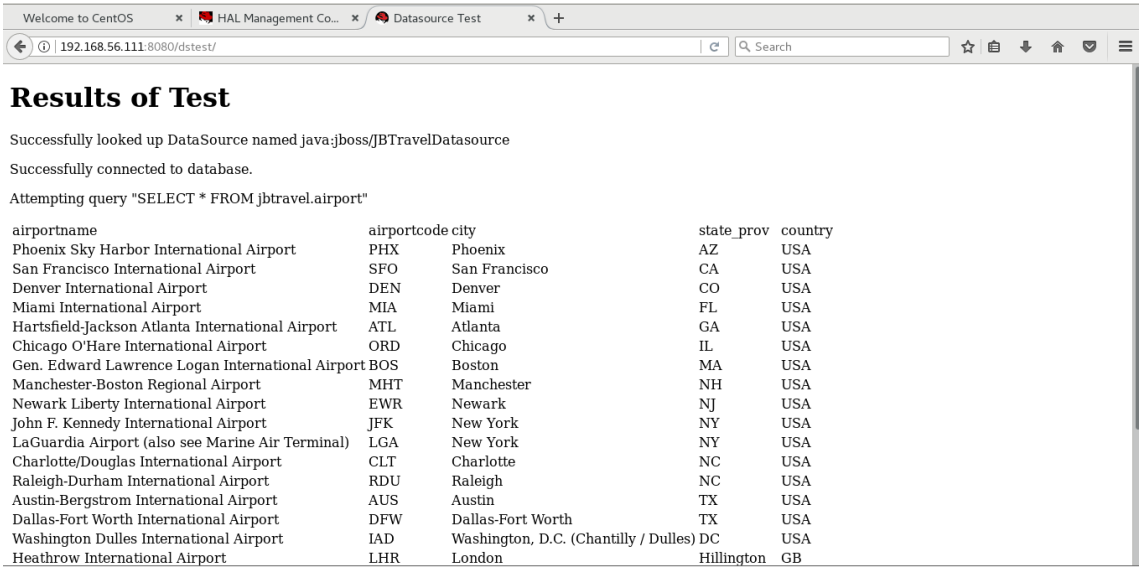
2gTQPnrWJaqrh0pURMKAOw"),("KEYSTORE_ALIAS" => "vault"),("SALT" => "12345678"),("ITERATION_COUNT" => "44"),("ENC_FILE_DIR" => "/home/jboss/")])
{"outcome" => "success"}

[standalone@192.168.56.111:9990 /] exit

9. Configure la fuente de datos

```
<datasource jta="true" jndi-name="java:jboss/JBTravelDatasource" pool-name="JBTravel" enabled="true" use-ccm="true">
  <connection-url>jdbc:postgresql://localhost:5432/postgres</connection-url>
  <driver>postgresql</driver>
  <pool>
    <min-pool-size>5</min-pool-size>
    <max-pool-size>20</max-pool-size>
  </pool>
  <security>
    <user-name>postgres</user-name>
    <password>${VAULT::jbtravel::password::1}</password>
  </security>
  <validation>
    <valid-connection-checker class-name="org.jboss.jca.adapters.jdbc.extensions.postgres.PostgreSQLValidConnectionChecker"/>
    <background-validation>true</background-validation>
    <exception-sorter class-name="org.jboss.jca.adapters.jdbc.extensions.postgres.PostgreSQLExceptionSorter"/>
  </validation>
</datasource>
```

10. Verifique la fuente de datos



airportname	airportcode	city	state_prov	country
Phoenix Sky Harbor International Airport	PHX	Phoenix	AZ	USA
San Francisco International Airport	SFO	San Francisco	CA	USA
Denver International Airport	DEN	Denver	CO	USA
Miami International Airport	MIA	Miami	FL	USA
Hartsfield-Jackson Atlanta International Airport	ATL	Atlanta	GA	USA
Chicago O'Hare International Airport	ORD	Chicago	IL	USA
Gen. Edward Lawrence Logan International Airport	BOS	Boston	MA	USA
Manchester-Boston Regional Airport	MHT	Manchester	NH	USA
Newark Liberty International Airport	EWR	Newark	NJ	USA
John F. Kennedy International Airport	JFK	New York	NY	USA
LaGuardia Airport (also see Marine Air Terminal)	LGA	New York	NY	USA
Charlotte/Douglas International Airport	CLT	Charlotte	NC	USA
Raleigh-Durham International Airport	RDU	Raleigh	NC	USA
Austin-Bergstrom International Airport	AUS	Austin	TX	USA
Dallas-Fort Worth International Airport	DFW	Dallas-Fort Worth	TX	USA
Washington Dulles International Airport	IAD	Washington, D.C. (Chantilly / Dulles)	DC	USA
Heathrow International Airport	LHR	London	Hillington	GB