

Desarrollo Seguro de Aplicaciones Web con OWASP

Lab: Encrypt Sensitive Data – JBoss EAP

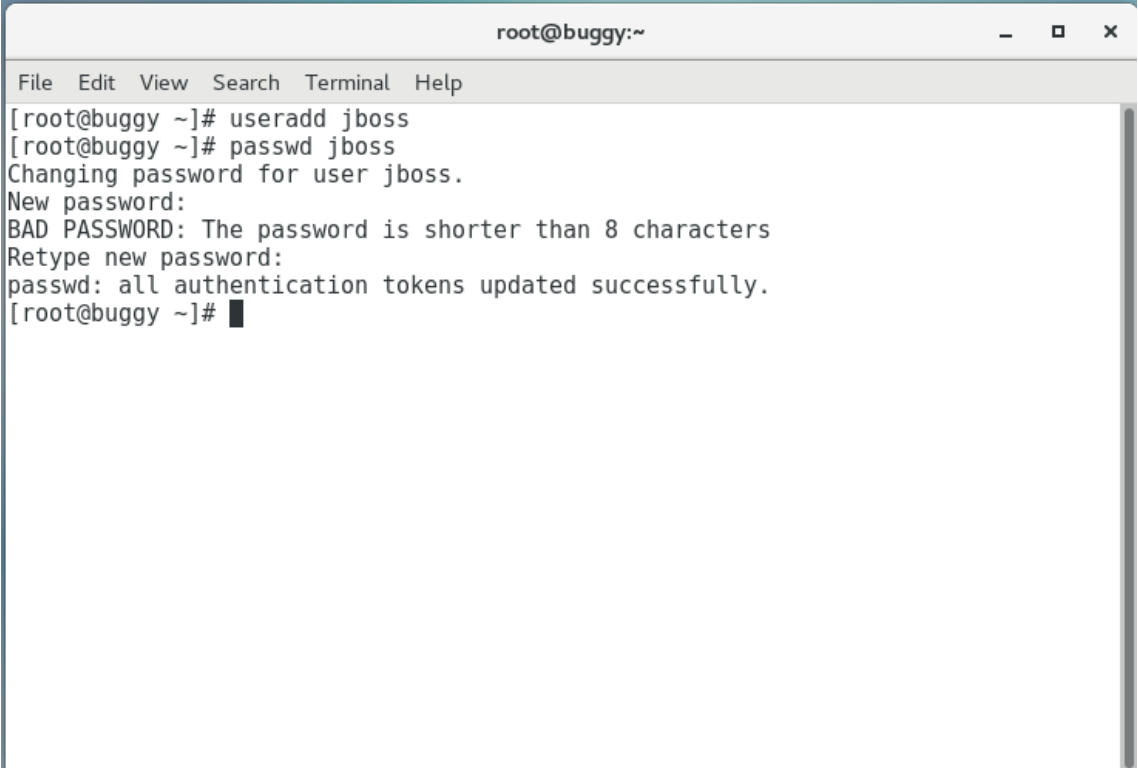
Objetivo

- Encriptar los datos sensibles en JBoss EAP

Procedimiento

1. Instalar y configurar JBoss EAP

Crear el usuario jboss

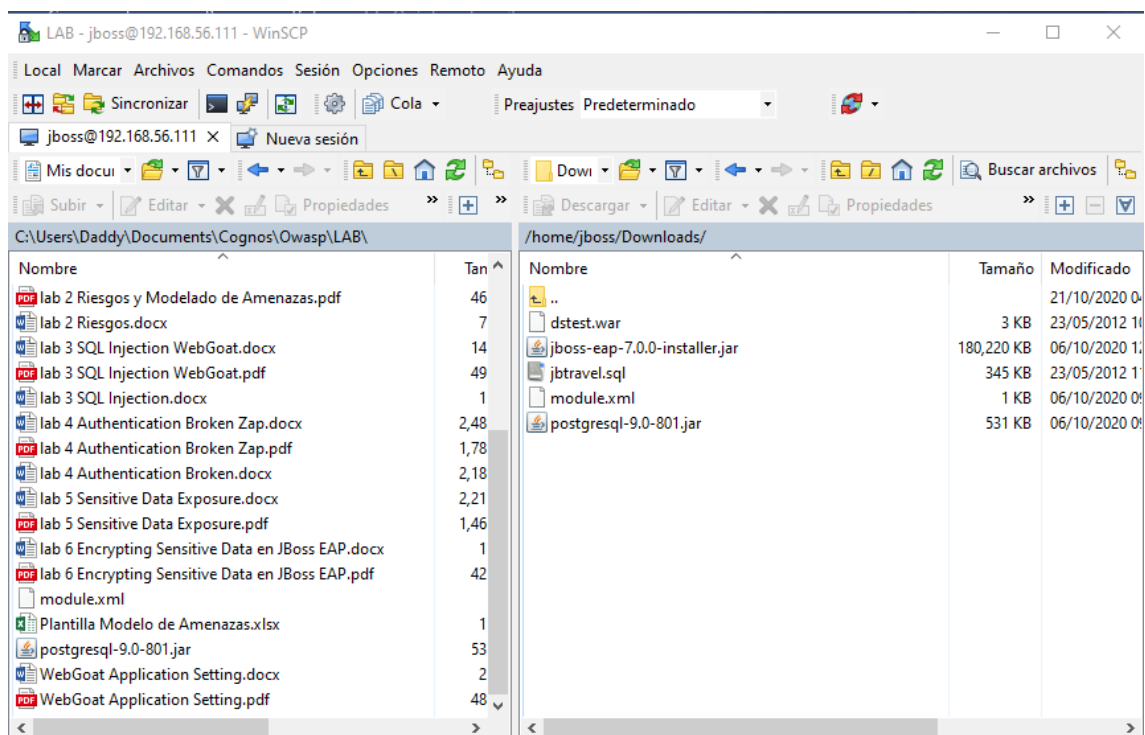
A terminal window titled 'root@buggy:~' with standard window controls. The terminal shows the execution of 'useradd jboss' and 'passwd jboss'. The password prompt is followed by an error message 'BAD PASSWORD: The password is shorter than 8 characters', then 'Retype new password:', and finally 'passwd: all authentication tokens updated successfully.' before returning to the root prompt.

```
root@buggy:~  
File Edit View Search Terminal Help  
[root@buggy ~]# useradd jboss  
[root@buggy ~]# passwd jboss  
Changing password for user jboss.  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@buggy ~]#
```

Ingresa con el usuario jboss, verificar la siguiente estructura.

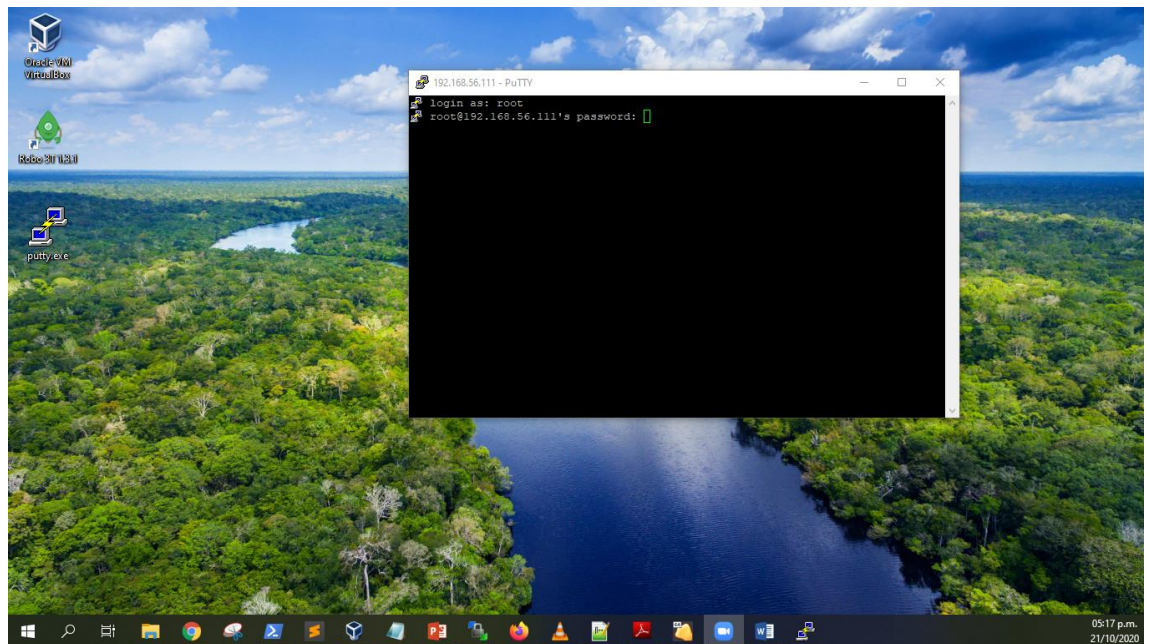
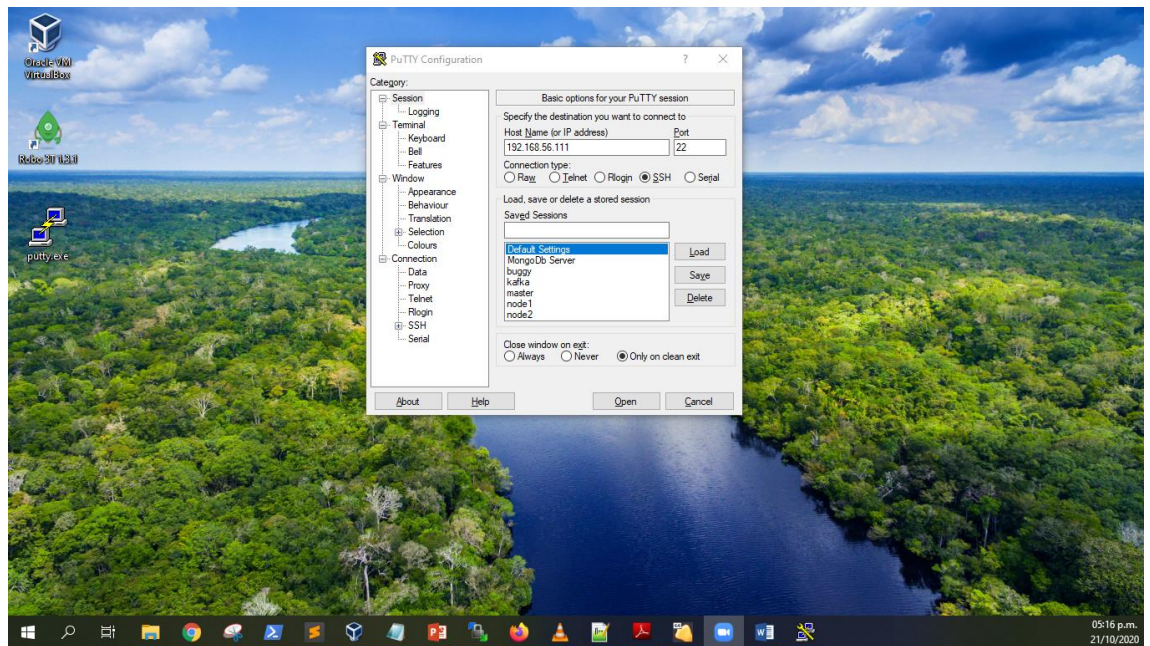
```
jboss@buggy:~  
File Edit View Search Terminal Help  
[jboss@buggy ~]$ ll  
total 0  
drwxr-xr-x 2 jboss jboss 6 Oct 21 16:51 Desktop  
drwxr-xr-x 2 jboss jboss 6 Oct 21 16:51 Documents  
drwxr-xr-x 2 jboss jboss 6 Oct 21 16:51 Downloads  
drwxr-xr-x 2 jboss jboss 6 Oct 21 16:51 Music  
drwxr-xr-x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

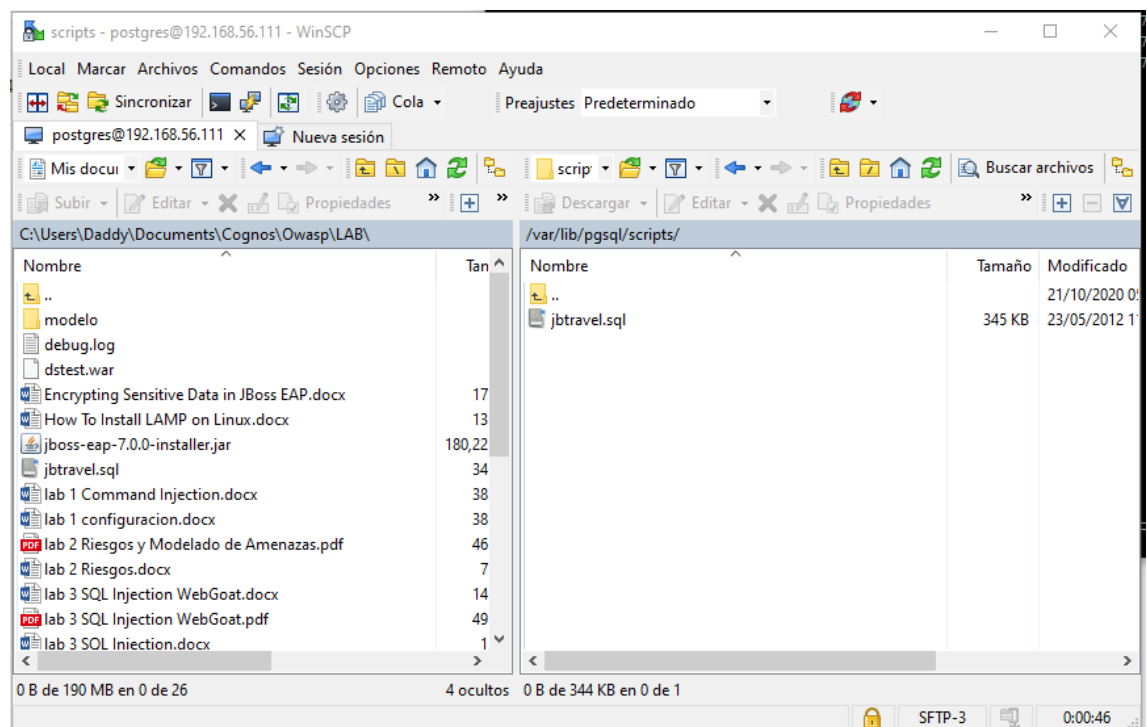
```
# systemctl start postgresql-9.6.service
```

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 ~]#
```

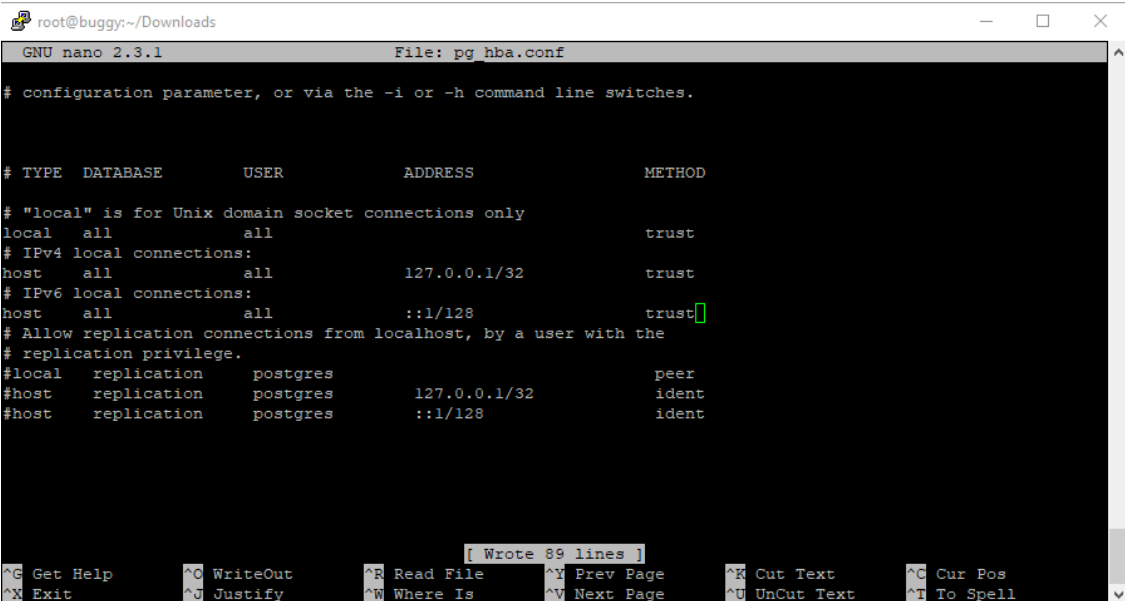
```
[root@buggy ~]# su - postgres
Last login: Wed Oct 21 17:34:31 -05 2020 on pts/1
-bash-4.2$ mkdir scripts
-bash-4.2$ cd scripts
-bash-4.2$ pwd
/var/lib/pgsql/scripts
```

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
```



```
root@buggy:~/Downloads
GNU nano 2.3.1 File: pg_hba.conf
# configuration parameter, or via the -i or -h command line switches.

# TYPE DATABASE USER ADDRESS METHOD
# "local" is for Unix domain socket connections only
local all all trust
# IPv4 local connections:
host all all 127.0.0.1/32 trust
# IPv6 local connections:
host all all ::1/128 trust
# Allow replication connections from localhost, by a user with the
# replication privilege.
#local replication postgres peer
#host replication postgres 127.0.0.1/32 ident
#host replication postgres ::1/128 ident

[ Wrote 89 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^N Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

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;
```

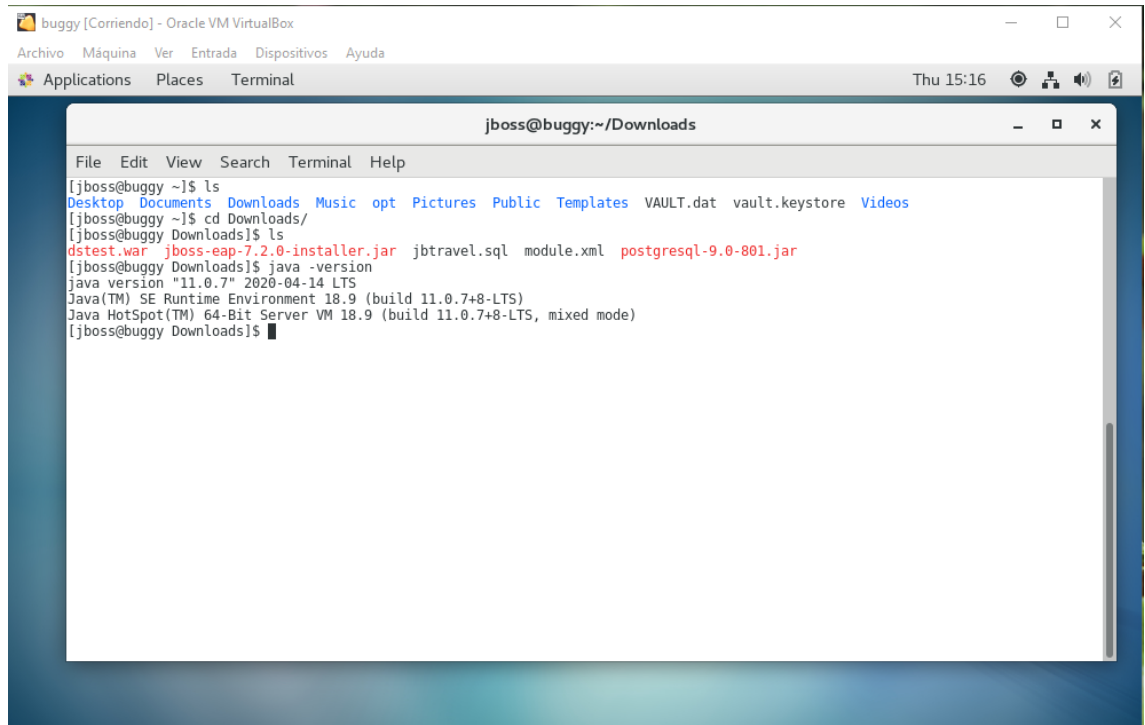
username	password
----------	----------

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

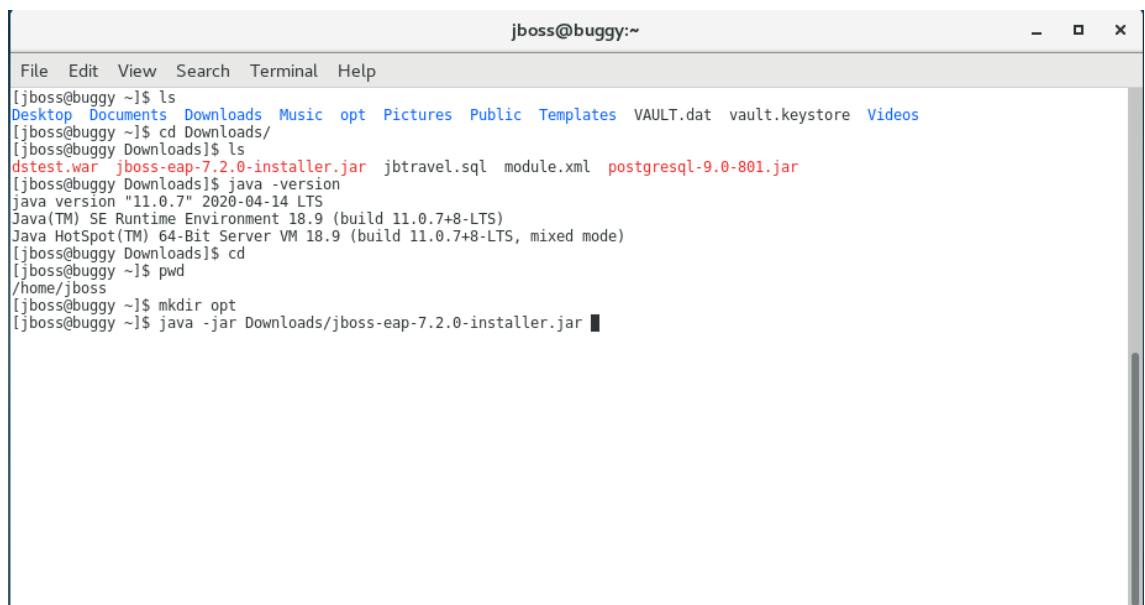
Verificar la versión de Java, debe ser 8 o superior.



```
buggy [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Applications Places Terminal Thu 15:16

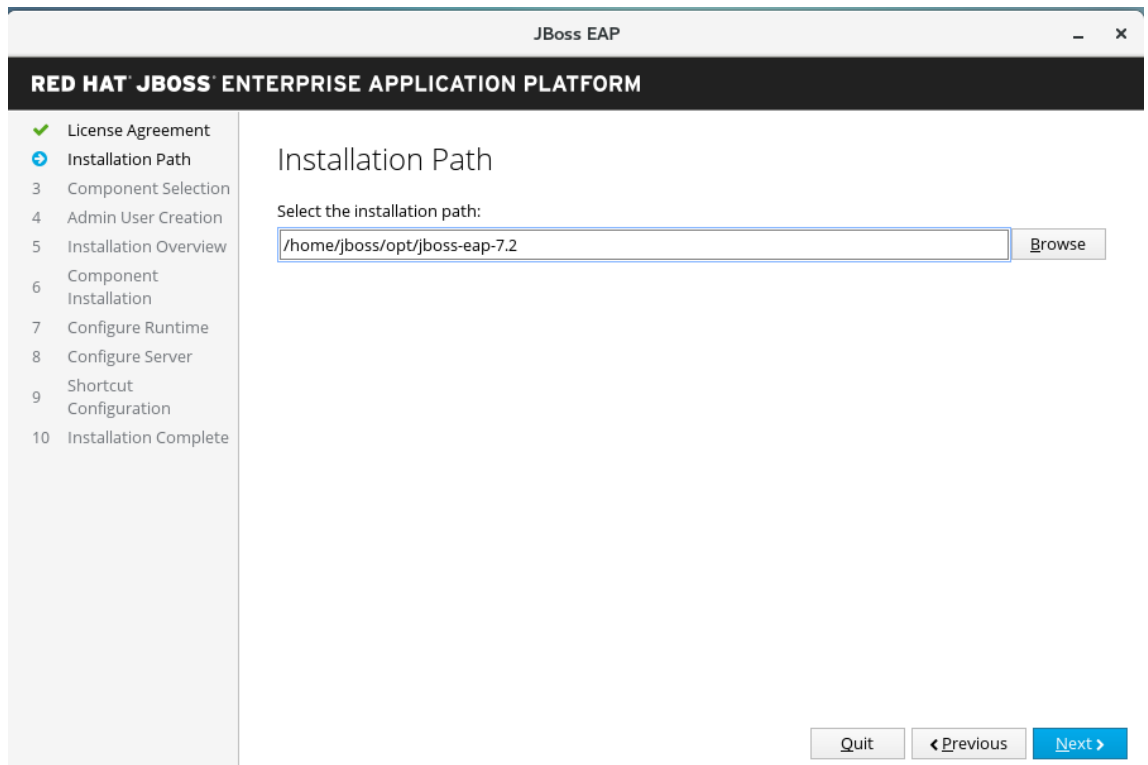
jboss@buggy:~/Downloads
File Edit View Search Terminal Help
[jboss@buggy ~]$ ls
Desktop Documents Downloads Music opt Pictures Public Templates VAULT.dat vault.keystore Videos
[jboss@buggy ~]$ cd Downloads/
[jboss@buggy Downloads]$ ls
dtest.war jboss-eap-7.2.0-installer.jar jbttravel.sql module.xml postgresql-9.0-801.jar
[jboss@buggy Downloads]$ java -version
java version "11.0.7" 2020-04-14 LTS
Java(TM) SE Runtime Environment 18.9 (build 11.0.7+8-LTS)
Java HotSpot(TM) 64-Bit Server VM 18.9 (build 11.0.7+8-LTS, mixed mode)
[jboss@buggy Downloads]$
```

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

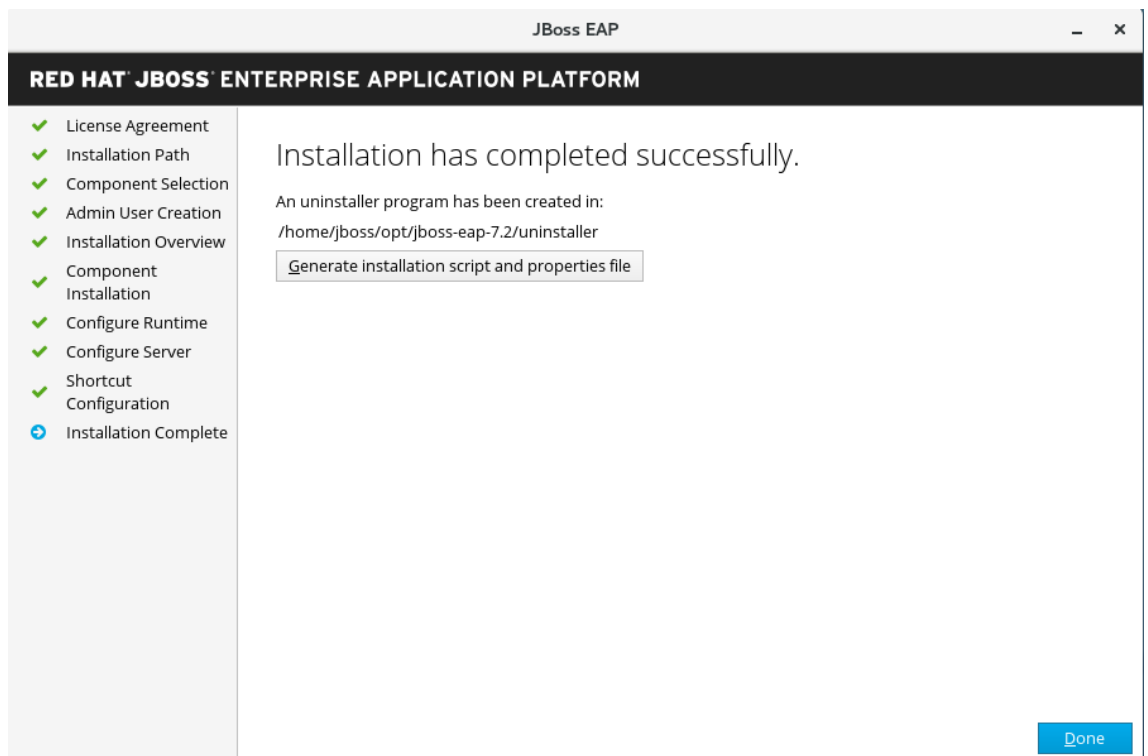


```
jboss@buggy:~
File Edit View Search Terminal Help
[jboss@buggy ~]$ ls
Desktop Documents Downloads Music opt Pictures Public Templates VAULT.dat vault.keystore Videos
[jboss@buggy ~]$ cd Downloads/
[jboss@buggy Downloads]$ ls
dtest.war jboss-eap-7.2.0-installer.jar jbttravel.sql module.xml postgresql-9.0-801.jar
[jboss@buggy Downloads]$ java -version
java version "11.0.7" 2020-04-14 LTS
Java(TM) SE Runtime Environment 18.9 (build 11.0.7+8-LTS)
Java HotSpot(TM) 64-Bit Server VM 18.9 (build 11.0.7+8-LTS, mixed mode)
[jboss@buggy Downloads]$ cd
[jboss@buggy ~]$ pwd
/home/jboss
[jboss@buggy ~]$ mkdir opt
[jboss@buggy ~]$ java -jar Downloads/jboss-eap-7.2.0-installer.jar
```

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

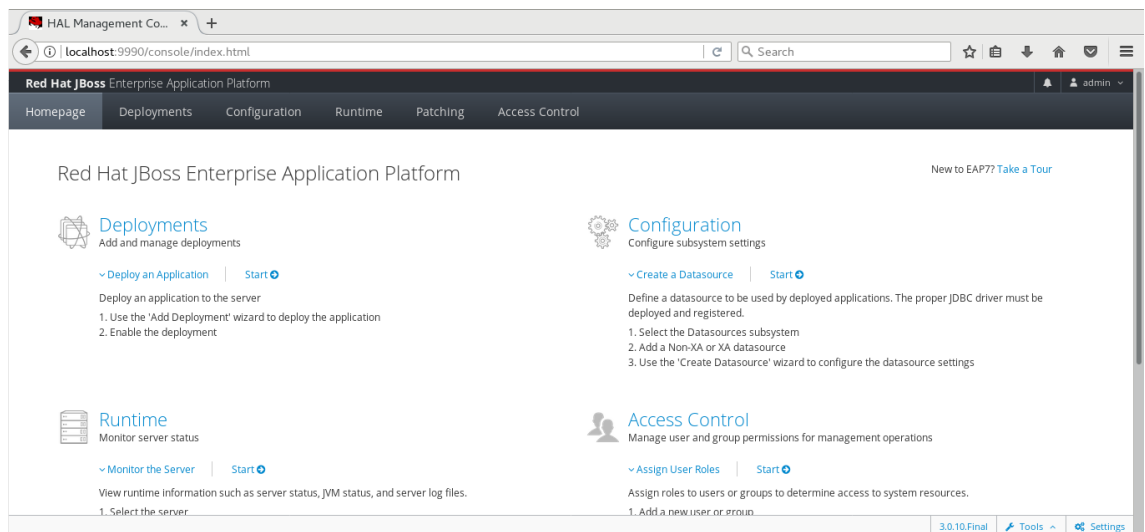
File Edit View Search Terminal Help

[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.xml       service.bat         wsconsume.ps1
appclient.bat        domain.conf.bat    jboss-server-migration.bat standalone.bat       wsconsume.sh
appclient.conf       domain.conf.ps1    jboss-server-migration.sh standalone.conf       wsprovide.bat
appclient.conf.bat   domain.ps1         jconsole.bat        standalone.conf.bat wsprovide.ps1
appclient.conf.ps1   domain.sh          jconsole.ps1        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
=====

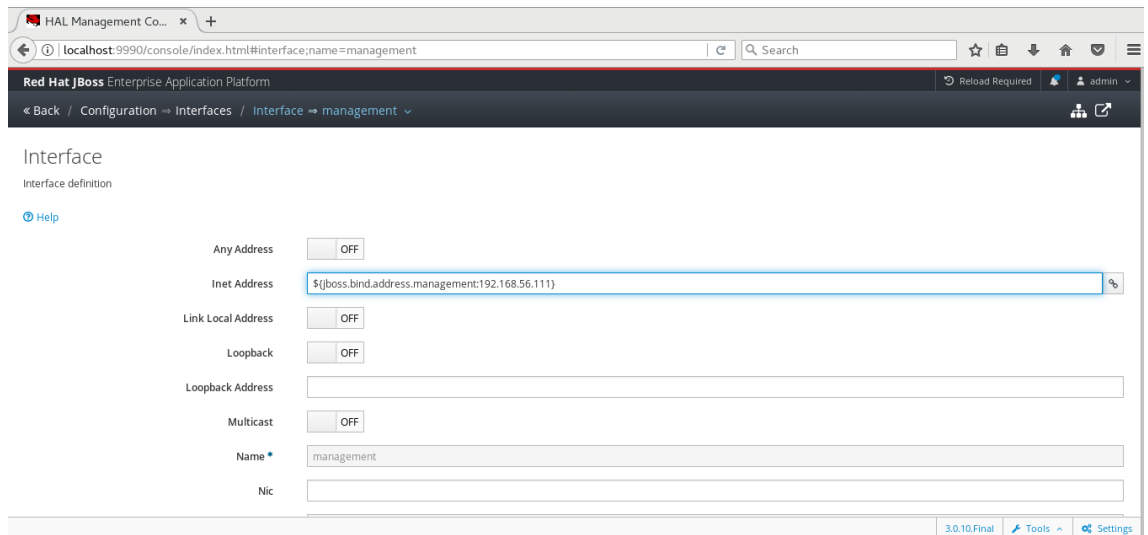
JBoss Bootstrap Environment

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 JTravel

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.PostgreSQLValidConnectionCh
ecker"/>
    <background-validation>true</background-validation>
    <exception-sorter class-
name="org.jboss.jca.adapters.jdbc.extensions.postgres.PostgreSQLExceptionSorter"/>
  </validation>
</datasource>

```

Reinicia el servidor

The screenshot shows a terminal window titled "jboss@buggy:~/opt/jboss-eap-7.2/bin". The terminal output shows the following sequence of commands and responses:

```

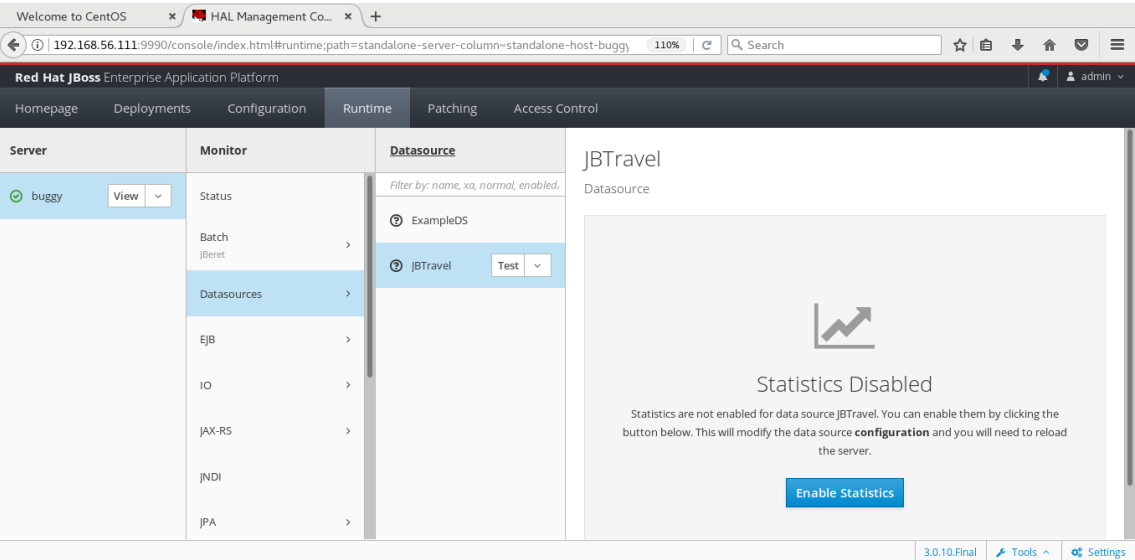
[jboss@buggy ~]$ cd ~/opt/jboss-eap-7.2/bin
[jboss@buggy bin]$ ./jboss-cli.sh -c --controller=192.168.56.111
[standalone@192.168.56.111:9990 /] /subsystem=datasources/jdbc-driver=postgresql:add(driver-name=postgresql, driver-m
driver-major-version driver-minor-version driver-module-name*
[standalone@192.168.56.111:9990 /] /subsystem=datasources/jdbc-driver=postgresql:add(driver-name=postgresql, driver-module-name=org.postgresql)
{"outcome" => "success"}

[standalone@192.168.56.111:9990 /] cd /
[standalone@192.168.56.111:9990 /] :reload
{
  "outcome" => "success",
  "result" => undefined
}

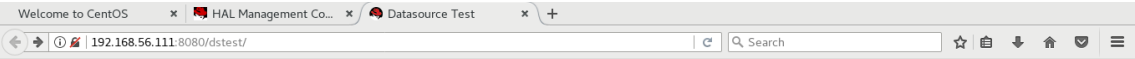
[standalone@192.168.56.111:9990 /]

```

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



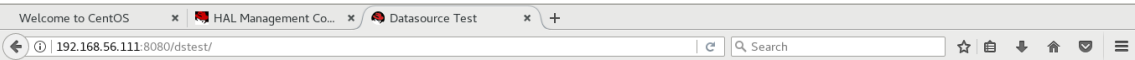
Desplegar la aplicación dctest



Test an EAP Datasource

JNDI Name of Datasource:

Table Name to Query (optional):



Results of Test

Successfully looked up DataSource named java:jboss/JBTravelDatasource

Successfully connected to database.

Attempting query "SELECT * FROM jbstavel.airport"

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	EWK	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

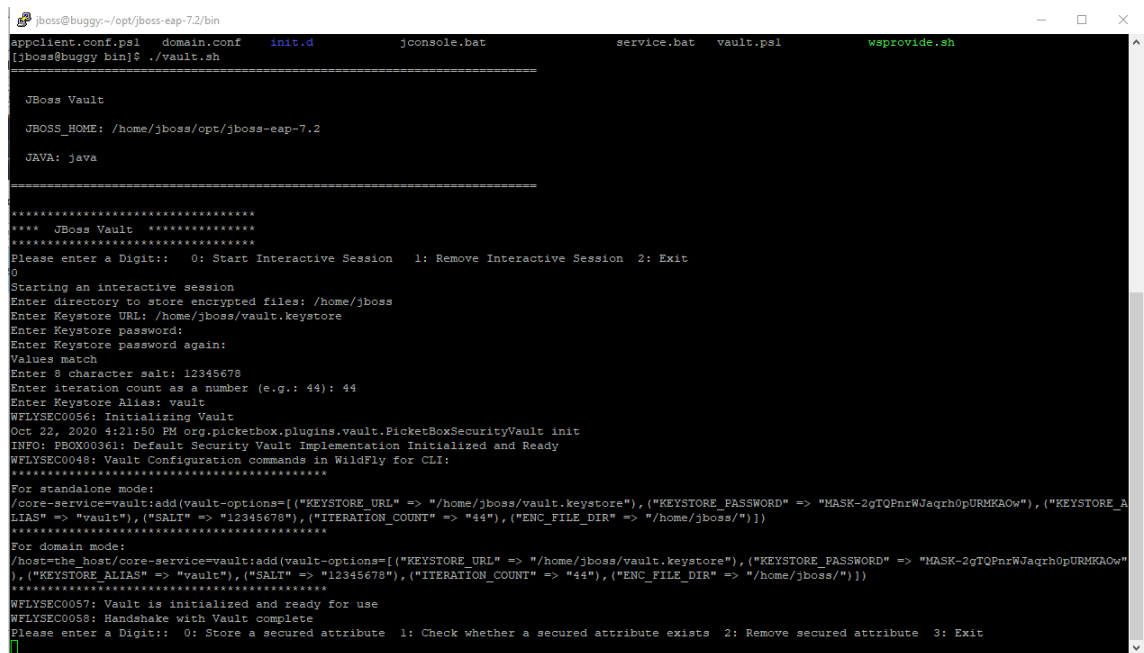
```
[jboss@buggy ~]$ keytool -genseckey -alias vault -keyalg AES -storetype jceks -keysize  
128 -keystore /home/jboss/vault.keystore  
Enter keystore password:  
Re-enter new password:  
Enter key password for <vault>  
(RETURN if same as keystore password):
```

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.



```
jboss@buggy:~/opt/jboss-eap-7.2/bin
appclient.conf.ps1  domain.conf  init.d  jconsole.bat  service.bat  vault.ps1  wsgrovide.sh

[jboss@buggy bin]$ ./vault.sh

JBoss Vault

JBoss HOME: /home/jboss/opt/jboss-eap-7.2

JAVA: java

=====
**** JBoss Vault ****
=====
Please enter a Digit::  0: Start Interactive Session  1: Remove Interactive Session  2: Exit
0
Starting an interactive session
Enter directory to store encrypted files: /home/jboss
Enter Keystore URL: /home/jboss/vault.keystore
Enter Keystore password:
Enter Keystore password again:
Values match
Enter 8 character salt: 12345678
Enter iteration count as a number (e.g.: 44): 44
Enter Keystore Alias: vault
WFLYSEC0056: Initializing Vault
Oct 22, 2020 4:21:50 PM org.picketbox.plugins.vault.PicketBoxSecurityVault init
INFO: FBOX0036: Default Security Vault Implementation Initialized and Ready
WFLYSEC0049: Vault Configuration commands in WildFly for CLI:
=====
For standalone mode:
/core-service=vault:add(vault-options=[("KEYSTORE_URL" => "/home/jboss/vault.keystore"), ("KEYSTORE_PASSWORD" => "MASK-2gTPnrWJaqrhOpURMKaOw"), ("KEYSTORE_ALIAS" => "vault"), ("SALT" => "12345678"), ("ITERATION_COUNT" => "44"), ("ENC_FILE_DIR" => "/home/jboss/")])
=====
For domain mode:
/host=the_host/core-service=vault:add(vault-options=[("KEYSTORE_URL" => "/home/jboss/vault.keystore"), ("KEYSTORE_PASSWORD" => "MASK-2gTPnrWJaqrhOpURMKaOw"), ("KEYSTORE_ALIAS" => "vault"), ("SALT" => "12345678"), ("ITERATION_COUNT" => "44"), ("ENC_FILE_DIR" => "/home/jboss/")])
=====
WFLYSEC0057: Vault is initialized and ready for use
WFLYSEC0058: Handshake with Vault complete
Please enter a Digit::  0: Store a secured attribute  1: Check whether a secured attribute exists  2: Remove secured attribute  3: Exit
1
```

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-
```

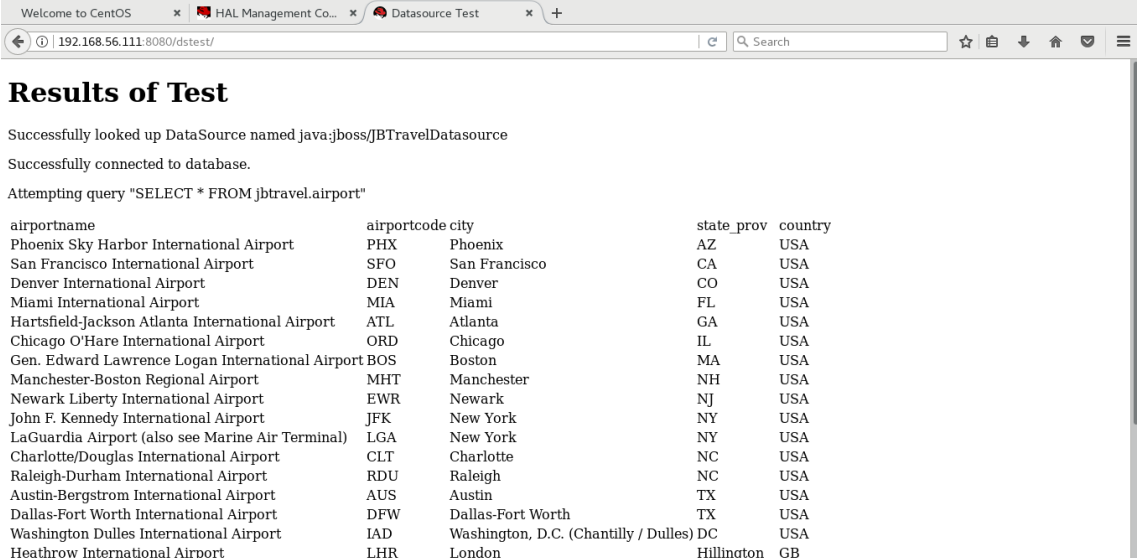
```
2gTQPnrWJaqrh0pURMKAOW"),("KEYSTORE_ALIAS" => "vault"),("SALT" =>
"12345678"),("ITERATION_COUNT" => "44"),("ENC_FILE_DIR" => "/home/jboss/"))
{"outcome" => "success"}
```

```
[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.PostgreSQLValidConnectionCh
ecker"/>
    <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



Welcome to CentOS x HAL Management Co... x Datasource Test x +

192.168.56.111:8080/dstest/ Search

Results of Test

Successfully looked up DataSource named java:jboss/JBTravelDatasource

Successfully connected to database.

Attempting query "SELECT * FROM jbtravel.airport"

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	EWB	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