Ventanilla Única Nacional
Componentes de Interoperabilidad
Instalación Autoridad Certificadora (CA)
VUN.X-ROAD v6.16
Versión 1.0.0

gob.mx

ÍNDICE

Colaboradores

Ítem	Nombres y Apellido	Oficina
1.	Jorge Sepúlveda	GOBMX
2.	Viviana Cano	GOBMX
3.	Ricardo Lona	GOBMX
4.	Arturo Silva	GOBMX
5.	Vanessa Vega	GOBMX

1. Objetivo del documento

El presente manual se realizó con base en la información obtenida de la página https://www.ejbca.org/docs/installation.html. El objetivo de este manual es apoyar en la instalación de una Autoridad Certificadora (CA) piloto como parte de los esfuerzo para poder interoperar por medio del uso de la herramienta X-Road en diferentes organismos de la Ventanilla Única Nacional.

2. Aspectos requeridos de Sistema Operativo

SO Ubuntu 14.04.5 LTS

3. Puertos Requeridos

3.1 Consideraciones adicionales de puertos después de instalación

Ejemplo de validación de puertos: **netstat** -a | grep 8443

Puertos Requeridos para IP-publica

In / Out: 8442
Protocol TCP
Source 0.0.0.0/0 ::/0

4. Software requerido

Para la instalación del CA es necesario descargar los archivos:

- Ejbca 6.5.0 (https://sourceforge.net/projects/ejbca/files/ejbca6/ejbca_6_5_0/ejbca_ce_6_5.0.5.zip/download)

- Wilfly 10.0.0 (download.jboss.org/wildfly/10.0.0.Final/wildfly-10.0.0.Final.tar.gz)

- Java 8 (Se instala con: sudo apt-get install openjdk-8-jdk)

- JDBC mariadb-java-client-1.2.0.jar (https://downloads.mariadb.com/Connectors/java/connector-java-1.2.0/mariadb-java-client-1.2.0.jar)

- MariaDB (MariaDB mysql Ver 15.1 Distrib 10.0.31-MariaDB, for debian-linux-gnu (x86_64))

5. Instalación y configuración de Base de Datos

- Descargar BD

```
sudo apt-get install software-properties-common
sudo apt-key adv --recv-keys --keyserver hkp://keyserver.ubuntu.com:80 0xcbcb082a1bb943db
sudo add-apt-repository 'deb http://ftp.osuosl.org/pub/mariadb/repo/10.0/ubuntu trusty main'
```

- Instalar MariaDB con apt-get

```
sudo apt-get update
sudo apt-get install mariadb-server
    - pass default root (**********)
```

- Copiar JDBC en WILDFLY10

El JDBC maria-java-client-1.2.0.jar previamente descargado se debe copiar en la carpeta del WILDFLY10 renombrando el archivo: cp mariadb-java-client-1.2.0.jar wildfly_home/standalone/deployments/mariadb-java-client.jar

- Configuración de la BD para el EJBCA

```
mysql -u root -p

mysql> CREATE DATABASE ejbca CHARACTER SET utf8 COLLATE utf8_general_ci;

mysql> GRANT ALL PRIVILEGES ON ejbca.* TO 'ejbca'@'%' IDENTIFIED BY '**********';
mysql> exit;
```

- Configurar visibilidad de mysql

En el archivo /etc/mysql/my.cnf en la sección "Basic settings" debe de estar bind-address = ip_servidor y en la sección "InnoDB" se debe agregar la linea binlog_format=mixed

Se reinicia Mysql: sudo service mysql restart

6. Configuración de EJBCA

Se descomprimen los archivos ejbca.tar.gz y wilfly10.tar.gz en el directorio raíz del usuario

- En el archivo de EJBCA/config/ejbca.properties se configura:

```
appserver.home=appserver.home=/home/ubuntu/wildfly-10.0.0.Final        /*  Ruta del deploy */
ejbca.cli.defaultusername=ejbca
ejbca.cli.defaultpassword=pass_EJBCA
```

- En el archivo de EJBCA/config/database.properties se configura:

```
datasource.jndi-name=EjbcaDS
database.name=mysql
database.url=jdbc:mysql://ip_servidor:3306/ejbca
database.driver=org.mariadb.jdbc.Driver
database.username=ejbca
database.password=**********
```

- En el archivo EJBCA/src/appserver/sun/ejbca_ds.xml se configura la información del resource jndi-name="jdbc/EjbcaDS" para conectar a la BD:

```
<resources>
<jdbc-connection-pool allow-non-component-callers="true"
 name="mysql-pool"
 datasource-classname="com.mysql.jdbc.jdbc2.optional.MysqlConnectionPoolDataSource"
 non-transactional-connections="false"
 res-type="javax.sql.DataSource">
 <property name="datasourceName" value="EjbcaDS"/>
 <property name="user" value="ejbca"/>
 <property name="password" value="**********"/>
 <property name="port" value="3306"/>
 <property name="databaseName" value="ejbca"/>
 <property name="serverName" value="ip_servidor"/>
</jdbc-connection-pool>
<jdbc-resource enabled="true" pool-name="mysql-pool" jndi-name="jdbc/EjbcaDS"/>
</resources>
```

- En el archivo EJBCA/src/appserver/jboss/jboss7/jboss-ejb-client.properties se configura:

```
remote.connectionprovider.create.options.org.xnio.Options.SSL_ENABLED=false
remote.connections=default
remote.connection.default.host=ip_servidor
remote.connection.default.port = 4447
remote.connection.default.connect.options.org.xnio.Options.SASL_POLICY_NOANONYMOUS=false
```

- En el archivo EjBCA/doc/howto/mysql-priviledes.sh se configura la ip del host y se debe de ejecutar como el archivo especifica.

7. Configuración de WILDFLY10

- En el archivo WILDFLY10/domain/configuration/host.xml y WILDFLY10/domain/configuration/domain.xml se debe cambiar la ip 127.0.0.1 por la del server (ej.188.20.30.4)

- En el archivo WILDFLY10/standalone/configuration/standalone.xml se debe cambiar la ip 127.0.0.1 por la del server (ej.188.20.30.4)

- En el archivo WILDFLY10/appclient/config/standalone.conf se debe configurar JAVA_OPTS y cambiar los valores de -Xms, -Xmx, -XX:MetaspaceSize, -XX:MaxMetaspaceSize :

Ej. de configuración:

```
if [ "x$JAVA_OPTS" = "x" ]; then
  JAVA_OPTS="-Xms2048m -Xmx2048m -XX:MetaspaceSize=96M -XX:MaxMetaspaceSize=256m
-Djava.net.preferIPv4Stack=true”
  JAVA_OPTS="$JAVA_OPTS -Djboss.modules.system.pkgs=$JBOSS_MODULES_SYSTEM_PKGS
-Djava.awt.headless=true"
else
  echo "JAVA_OPTS already set in environment; overriding default settings with values: $JAVA_OPTS"
fi
```

8. Configuración de jboss-cli

Para hacer uso de la consola JBoss-cli mientras el server esté corriendo.

- En el archivo WILDFLY10/bin/jboss-cli.xml se debe cambiar la ip 127.0.0.1 por la del server (ej.188.20.30.4)
- En el archivo WILDFLY10/appclient/config/appclient.xml se debe cambiar la ip 127.0.0.1 por la del server (ej.188.20.30.4)

9. Instalación del EJBCA en WILDFLY10

- Se debe iniciar el server con WILDFLY10/bin/standalone.sh y mantener en ejecución durante todo el proceso

- Se inicia el jboss-cli con WILDFLY10/bin/jboss-cli.sh -c

  En la consola del Jboss-cli:

```
/* ===== Eliminar el DS de ejemplo porque causa errores ====== */

/subsystem=datasources/data-source=ExampleDS:remove()
/subsystem=ee/service=default-bindings:write-attribute(name=data-source,value=undefined)
:reload
```

Nota: Buscar “ExampleDS” en archivo WILDFLY10/conf/standalone.xml y cambiar por EjdbcDS al cerrar el jboss-cli y antes del deploy del EJBCA

```
/* ===== Agregar el DS de EjbcaDS con la siguiente configuración ==== */
```

```
data-source add --name=ejbcads --driver-name="mariadb-java-client.jar" --connection-url="jdbc:mysql://ip_servidor:3306/ejbca" --jndi-name="java:/EjbcaDS" --use-ccm=true --driver-class="org.mariadb.jdbc.Driver" --user-name="ejbca" --password="**********" --validate-on-match=true --background-validation=false --prepared-statements-cache-size=50 --share-prepared-statements=true --min-pool-size=5 --max-pool-size=150 --pool-prefill=true --transaction-isolation=TRANSACTION_READ_COMMITTED --check-valid-connection-sql="select 1;"
:reload

/* ==== Eliminar viejas configuraciones, si es que existen ===== */

/subsystem=remoting/http-connector=http-remoting-connector:remove
/subsystem=remoting/http-connector=http-remoting-connector:add(connector-ref="remoting",security-realm="ApplicationRealm")
/socket-binding-group=standard-sockets/socket-binding=remoting:add(port="4447")
/subsystem=undertow/server=default-server/http-listener=remoting:add(socket-binding=remoting)
:reload

/* ===== Configurar Logging ===== */

/subsystem=logging/logger=org.ejbca:add
/subsystem=logging/logger=org.ejbca:write-attribute(name=level, value=DEBUG)
/subsystem=logging/logger=org.cesecore:add
/subsystem=logging/logger=org.cesecore:write-attribute(name=level, value=DEBUG)



/* ===== Eliminar configuración TLS y HTTP,  si es que existe ===== */

/subsystem=undertow/server=default-server/http-listener=default:remove
/subsystem=undertow/server=default-server/https-listener=https:remove
/socket-binding-group=standard-sockets/socket-binding=http:remove
/socket-binding-group=standard-sockets/socket-binding=https:remove
:reload
exit
```

- Se configura el archivo EJBCA/conf/web.properties

```
java.trustpassword=**********
superadmin.cn=SuperAdmin
superadmin.password=pass_EJBCA
superadmin.batch=true
httpsserver.password=**********
httpsserver.hostname=ip_servidor
httpsserver.dn=CN=${httpsserver.hostname},O=EJBCA Sample,C=SE
```

- Se realiza el deploy EJBCA en el servidor indicado previamente (Archivo EJBCA/config/ejbca.properties)
  En la ruta del EJBCA se ejecuta:

ant clean deployear /* Realiza el deploy en WILDFLY10/standalone/deploy */

ant runinstall /* Crea la CA inicial, sólo se ingresó el nombre de la CA como: NombreCA y el password: pass_EJBCA todo lo demás fueron las características por default" */

/* ================ ejemplo de resultado con la configuración por default ======== */

```
jbca:init:
    [echo]
    [echo] ------------------- CA Properties ----------------
    [echo] ca.name               : NombreCA
    [echo] ca.dn                 : CN=ManagementCA,O=EJBCA Sample,C=SE
    [echo] ca.tokentype          : soft
    [echo] ca.keytype            : RSA
    [echo] ca.keyspec            : 2048
    [echo] ca.signaturealgorithm  : SHA256WithRSA
    [echo] ca.validity           : 3650
    [echo] ca.policy             : null
    [echo] ca.tokenproperties     : ${ca.tokenproperties}
    [echo] httpsserver.hostname   : ip_servidor
    [echo] httpsserver.dn         : CN=ip_servidor,O=EJBCA Sample,C=SE
    [echo] superadmin.cn          : SuperAdmin
    [echo] superadmin.dn          : CN=SuperAdmin
    [echo] superadmin.batch       : true
    [echo] appserver.home         : /home/ubuntu/wildfly-10.0.0.Final
    [echo]
```

/* == */

ant deploy-keystore /* Realiza una copia de los archivos generados en EJBCA/p12 despues del ant runinstall al directorio WILDFLY10/standalone/configuration/keystore */

- Se debe de copiar el archivo EJBCA/p12/superadmin.p12 a la máquina local del administrador para agregarla en los certificados del navegador y poder entrar a la parte del admin posteriormente.
  ej. scp ubuntu@ip_servidor:ejbca_ce_6_5.0.5/p12/superadmin.p12 .

- Se inicia el jboss-cli con WILDFLY10/bin/jboss-cli.sh -c

En la consola del Jboss-cli:

```
/* ====== Configuración del TLS ======= */
/interface=http:add(inet-address="0.0.0.0")
/interface=httpspub:add(inet-address="0.0.0.0")
/interface=httpspriv:add(inet-address="0.0.0.0")
/socket-binding-group=standard-sockets/socket-binding=http:add(port="8080",interface="http")
/subsystem=undertow/server=default-server/http-listener=http:add(socket-binding=http)
```

```
/subsystem=undertow/server=default-server/http-listener=http:write-attribute(name=redirect-socket,
value="httpspriv")
:reload
:read-attribute(name=server-state)

/* ===== Configuración de identities y sockets-bindings, estos valores se configuran igual que los
configurados en el archivo EJBCA/conf/web.properties ===== */
/core-service=management/security-realm=SSLRealm:add()
/core-service=management/security-realm=SSLRealm/server-identity=ssl:add(keystore-path="$
{jboss.server.config.dir}/keystore/keystore.jks", keystore-password="**********", alias="ip_servidor")
/core-service=management/security-realm=SSLRealm/authentication=truststore:add(keystore-path="$
{jboss.server.config.dir}/keystore/truststore.jks", keystore-password="**********")
/socket-binding-group=standard-sockets/socket-binding=httpspriv:add(port="8443",interface="httpspriv")
/socket-binding-group=standard-sockets/socket-binding=httpspub:add(port="8442", interface="httpspub")
:reload

/system-property=org.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH:add(value=true)
/system-property=org.apache.catalina.connector.CoyoteAdapter.ALLOW_BACKSLASH:add(value=true)
/system-property=org.apache.catalina.connector.URI_ENCODING:add(value="UTF-8")
/system-
property=org.apache.catalina.connector.USE_BODY_ENCODING_FOR_QUERY_STRING:add(value=true)
/subsystem=webservices:write-attribute(name=wsdl-host, value=jbossws.undefined.host)
/subsystem=webservices:write-attribute(name=modify-wsdl-address, value=true)
:reload
exit
```

- Se puede ver el EJBCA corriendo en https://ip_servidor:8443/ejbca/adminweb (al ingresar solicitara el .p12 previamente guardado en la máquina, favor de agregarlo al navegador en Preferencias->Avanzado->Certificados->Ver Certificados -> Import) Password: pass_EJBCA