

The Container Security in Healthcare Data Exchange System

Bachelor's degree graduation project

Chih-Hsuan Yang

National Sun Yat-sen University

Advisor: Chun-I Fan

September 3, 2021

Outline

1 TL;DR

2 Screenshots

Flow chart



TL;DR

Current state

- Got a hazard these weeks. I will hurry up.
- Can get system call manually.
- Can enforce the system call limitation.
- Need a registry server to register those certs.
- Generate the "sanitizing image" automatically.

Next state

- Generate the FHIR RESTful api fuzz script.
 - Deploy the registry server.
 - Performance benchmark.
-
- 1 Combine the "sanitizing image" and fuzz script.
 - 2 Combine registry server and policy rule.

Screenshots

```
postgres_1 | done
postgres_1 | server started
```

```
Removing intermediate container bc446052dc43
```

```
----> bf89205a32f6
```

```
Step 23/27 : COPY --chown=1001:0 --from=base /opt/ibm-fhir-server /opt/ibm-fhir-server
```

```
----> 5421540c0251
```

```
Step 24/27 : RUN mkdir -p /config/configDropins/overrides &&      chmod -R 775 /config/configDropins/overrides &&      chmod -R 775 /opt/ol/wlp/usr/servers/defaultServer/configDropins/defaultServer
```

```
----> Running in ed1af89f496f
```

```
Removing intermediate container ed1af89f496f
```

```
----> dd4d5cef2ea7
```

```
Step 25/27 : WORKDIR ${FHIR_CONFIG_HOME}
```

```
----> Running in 1924bd160fa9
```

```
Removing intermediate container 1924bd160fa9
```

```
----> ae82f2a7c8d7
```

```
Step 26/27 : ENTRYPOINT ["/opt/ibm-fhir-server/bootstrap.sh"]
```

```
----> Running in cc18cc907a49
```

```
Removing intermediate container cc18cc907a49
```

```
----> 88a27bf03125
```

```
Step 27/27 : CMD ["/opt/ol/wlp/bin/server", "run", "defaultServer"]
```

```
----> Running in b20f72939d05
```

```
Removing intermediate container b20f72939d05
```

```
----> a24cd4da2175
```

```
Successfully built a24cd4da2175
```

```
Successfully tagged fhir-server-base:03
```

```
→ auto_catch
```

```
0
```

```
↑ 3h 42m
```

```
1 python
```



```

demo git:(a9d0305c7e) eg 'fhiradmin'
./postgres/resources/db.sql
#-- only for the fhiradmin user
#1:GRANT ALL ON schema fhirdata TO fhiradmin WITH GRANT OPTION;
#2:GRANT ALL ON schema fhir_admin TO fhiradmin WITH GRANT OPTION;
#3:GRANT ALL ON schema fhir_oauth TO fhiradmin WITH GRANT OPTION;
#4:GRANT ALL ON schema fhir_jbatch TO fhiradmin WITH GRANT OPTION;
#5:GRANT USAGE ON SCHEMA fhirdata TO fhiradmin;
#6:GRANT USAGE ON SCHEMA fhir_oauth TO fhiradmin;
#7:GRANT USAGE ON SCHEMA fhir_jbatch TO fhiradmin;

./postgres/resources/docker-motrgpsql.sh
#1: su - postgres -c "/usr/local/bin/psql -c \"CREATE USER fhiradmin WITH LOGIN encrypted password 'hey_yoh_what';\""
#4: su - postgres -c "/usr/local/bin/psql -c \"CREATE DATABASE fhirdb OWNER 'fhiradmin';\""

./postgres/DockerFile
#7:# Add the fhiradmin user
#8:RUN addgroup -S fhir && adduser -S fhiradmin -G fhir
#9:RUN echo "fhiradmin:hey_yoh_what" | chpasswd

./fhir/config/default/fhir-server-config.json
#12: "user": "fhiradmin",

./fhir/config/properties/overrides/datasources.xml
#7: user="fhiradmin"

./docker-compose.yml
#4: test: ["CMD-SHELL", "pg_isready -d fhirdb -U fhiradmin"]
#5: --db-type postgresql --prop db.host:postgres --prop db.port:5432 --prop db.database:fhirdb --prop user=fhiradmin --prop password:hey_yoh_what
demo git:(a9d0305c7e)

```

30.5°C | 15:01 | 03 Sep acc acc-lab

```

postgres_1 2021-09-03 06:49:50.749 UTC [9] LOG: listening on IPv4 address "0.0.0.0", port 5432
postgres_1 2021-09-03 06:49:50.749 UTC [9] LOG: listening on IPv6 address "::", port 5432
postgres_1 2021-09-03 06:49:50.754 UTC [9] LOG: listening on Unix socket "/var/run/postgresql/.s.PGSQL.5432"
postgres_1 2021-09-03 06:49:50.807 UTC [10] LOG: database system was interrupted; last known up at 2021-09-03 06:46:57 UTC
postgres_1 2021-09-03 06:49:50.885 UTC [10] LOG: database system was not properly shut down; automatic recovery in progress
postgres_1 2021-09-03 06:49:50.888 UTC [10] LOG: redo starts at 0/2A86C30
postgres_1 2021-09-03 06:49:50.888 UTC [10] LOG: invalid record length at 0/2A86C68: wanted 24, got 0
postgres_1 2021-09-03 06:49:50.888 UTC [10] LOG: redo done at 0/2A86C30
postgres_1 2021-09-03 06:49:50.917 UTC [9] LOG: database system is ready to accept connections
postgres_1 done
postgres_1 server started
fhir-server_1 bootstrap.sh - [INFO]: 2021-09-03_06:50:06 - Current directory: /opt/ibm-fhir-server
fhir-server_1 bootstrap.sh - [INFO]: 2021-09-03_06:50:06 - Skipping Derby database bootstrapping
fhir-server_1 2021-09-03 06:50:07.464 00000001 INFO com.ibm.fhir.database.utils.api.DataAccessException: org.postgresql.util.PSQLException: FATAL: password authentication failed for user "fhiradmin"
fhir-server_1 2021-09-03 06:50:07.464 00000001 INFO com.common.JdbcConnectionProvider Opening connection to database: jdbc:postgresql://postgres:5432/fhirdb?resourceTypes=AllergyIntolerance,Case,CodeSystem,Condition,Consent,Coverage,Device,DiagnosticReport,DocumentReference,Encounter,ExplanationOfBenefit,Goal,Group,Immunization,List,Location,Medication,MedicationAdministration,MedicationDispense,MedicationRequest,MedicationStatement,Observation,Organization,Practitioner,PractitionerRole,Procedure,Provenance,StructureDefinition,ValueSet
postgres_1 2021-09-03 06:50:07.508 UTC [24] FATAL: password authentication failed for user "fhiradmin"
postgres_1 2021-09-03 06:50:07.508 UTC [24] DETAIL: Password does not match for user "fhiradmin".
postgres_1 Connection matched pg_hba.conf line 99: "host all all 0.0.0.0/0 md5"
fhir-server_1 2021-09-03 06:50:07.511 00000001 SEVERE com.ibm.fhir.schema.app.Main schema tool failed
fhir-server_1 org.postgresql.util.PSQLException: FATAL: password authentication failed for user "fhiradmin"
fhir-server_1 com.ibm.fhir.database.utils.api.DataAccessException: org.postgresql.util.PSQLException: FATAL: password authentication failed for user "fhiradmin"
fhir-server_1 at com.ibm.fhir.database.utils.common.PostgresTranslator.translate(PostgresTranslator.java:104)
fhir-server_1 at com.ibm.fhir.database.utils.common.JdbcConnectionProvider.getConnection(JdbcConnectionProvider.java:54)
fhir-server_1 at com.ibm.fhir.database.utils.pool.PoolConnectionProvider.getConnection(PoolConnectionProvider.java:134)
fhir-server_1 at com.ibm.fhir.database.utils.common.CommonDatabaseAdapter.runStatement(CommonDatabaseAdapter.java:486)
fhir-server_1 at com.ibm.fhir.database.utils.postgres.PostgresAdapter.doesTableExist(PostgresAdapter.java:192)
fhir-server_1 at com.ibm.fhir.database.utils.model.Table.exists(Table.java:830)
fhir-server_1 at com.ibm.fhir.database.utils.version.CreateVersionHistory.createTableIfNeeded(CreateVersionHistory.java:48)
fhir-server_1 at com.ibm.fhir.schema.app.Main.updateSchema(Main.java:392)
fhir-server_1 at com.ibm.fhir.schema.app.Main.process(Main.java:209)
fhir-server_1 at com.ibm.fhir.schema.app.Main.main(Main.java:2195)
fhir-server_1 Caused by: org.postgresql.util.PSQLException: FATAL: password authentication failed for user "fhiradmin"
fhir-server_1 at org.postgresql.core.v3.ConnectionFactoryImpl.doAuthentication(ConnectionFactoryImpl.java:613)
fhir-server_1 at org.postgresql.core.v3.ConnectionFactoryImpl.tryConnect(ConnectionFactoryImpl.java:161)
fhir-server_1 at org.postgresql.core.v3.ConnectionFactoryImpl.openConnectionImpl(ConnectionFactoryImpl.java:213)
fhir-server_1 at org.postgresql.core.ConnectionFactory.openConnection(ConnectionFactory.java:51)
fhir-server_1 at org.postgresql.jdbc.PgConnection.<init>(PgConnection.java:225)
fhir-server_1 at org.postgresql.Driver.makeConnection(Driver.java:465)
fhir-server_1 at org.postgresql.Driver.connect(Driver.java:264)
fhir-server_1 at java.sql/java.sql.DriverManager.getConnection(DriverManager.java:677)
fhir-server_1 at java.sql/java.sql.DriverManager.getConnection(DriverManager.java:189)
fhir-server_1 at com.ibm.fhir.database.utils.common.JdbcConnectionProvider.getConnection(JdbcConnectionProvider.java:42)
fhir-server_1 ... 8 more
fhir-server_1 2021-09-03 06:50:07.513 00000001 SEVERE com.ibm.fhir.schema.app.Main SCHEMA CHANGE: RUNTIME ERROR
fhir-server_1 demo.fhir-server_1 exited with code 1
fhir-server_1 Gracefully stopping... (press Ctrl+C again to force)
stopping demo-postgres_1 ... done
demo f811a9d0305c70

```

40, 8333°C | 14:53 | 03 Sep scc scc-lab