

Dynamic Secrets with Cassandra



Download JDK 11 – it has the least issues (still a lot, but workable) <http://jdk.java.net/11>

Install on a Mac:

```
tar xf openjdk-11.0.2_osx-x64_bin.tar.gz
sudo mv jdk-11.0.2.jdk /Library/Java/JavaVirtualMachines
java -version
openjdk version "11.0.2" 2018-10-16
OpenJDK Runtime Environment 18.9 (build 11.0.2+7)
OpenJDK 64-Bit Server VM 18.9 (build 11.0.2+7, mixed mode)
```

Install on Windows – LOL ☹

Download Datastax Community Edition

curl -OL <http://downloads.datastax.com/community/dsc.tar.gz>

tar xzf dsc.tar.gz

It expands to: dsc-cassandra-3.0.9

The directories of interest are: dsc-cassandra-3.0.9/bin and dsc-cassandra-3.0.9/conf

In the dsc-cassandra-3.0.9/conf, copy my versions of the:

cassandra.yaml

jvm.options

Two changes for Cassandra to work with vault. First, Basic Authentication needs to be enabled.

```
# - AllowAllAuthenticator performs no checks - set it to disable authentication.
# - PasswordAuthenticator relies on username/password pairs to authenticate
# users. It keeps usernames and hashed passwords in system_auth.credentials table.
# Please increase system_auth keyspace replication factor if you use this authenticator.
# If using PasswordAuthenticator, CassandraRoleManager must also be used (see below)
## authenticator: AllowAllAuthenticator
authenticator: PasswordAuthenticator
```

Next, due to the changes to RBAC in Cassandra, I found an obscure article on how to handle this, as Vault complained with just Basic Authentication (PasswordAuthenticator)

```
# - AllowAllAuthorizer allows any action to any user - set it to disable authorization.
# - CassandraAuthorizer stores permissions in system_auth.permissions table. Please
```

```
# increase system_auth keyspace replication factor if you use this authorizer.  
## authorizer: AllowAllAuthorizer  
authorizer: org.apache.cassandra.auth.CassandraAuthorizer
```

In the jvm option file, I pretty much commented out all options for the GC. I also had to create a logs directory at the dsc-cassandra-3.0.9 level. I cd into the logs directory and did a touch on gc.log.

From that point cd to dsc-cassandra-3.0.9/bin and ./cassandra. You should have a healthy Cassandra – for working with to experiment with vault.

Demo – Cassandra Dynamic Passwords

Start Vault

```
$ vault server -dev
```

```
$ vault secrets enable -path=devel-mobile-cassandra database
```

```
$ vault write devel-mobile-cassandra/config/my-cassandra-database \
  plugin_name="cassandra-database-plugin" \
  hosts=127.0.0.1 protocol_version=4 \
  username=cassandra \
  password=cassandra \
  allowed_roles=my-role
```

```
$ vault write devel-mobile-cassandra/roles/my-role \
  db_name=my-cassandra-database \
  creation_statements="CREATE USER '{{username}}' WITH PASSWORD '{{password}}'
NOSUPERUSER; \
  GRANT SELECT ON ALL KEYSPACES TO {{username}};" \
  default_ttl="1h" \
  max_ttl="24h"
```

```
$ vault read devel-mobile-cassandra/creds/my-role
```

Key	Value
lease_id	database/creds/my-role/4OW0hhUySpE4mUVitP3727Md
lease_duration	1h
lease_renewable	true
password	A1a-10u4AttatKi9zSI8
username	v_root_my_role_2glj44wnzycntgscqkuq_1547610359

From the dsc-cassandra-3.0.9/bin run:

```
$ ./cqqlsh localhost -u v_root_my_role_2glj44wnzycntgscqkuq_1547610359 -p
A1a-10u4AttatKi9zSI8
```

Connected to Test Cluster at localhost:9042.

[cqqlsh 5.0.1 | Cassandra 3.0.9 | CQL spec 3.4.0 | Native protocol v4]

Use HELP for help.

```
v_root_my_role_2glj44wnzycntgscqkuq_1547610359@cqqlsh> list users;
```

name		super
v_root_my_role_2glj44wnzycntgscqkuq_1547610359		False