**Dynamic Secrets with MYSQL database engine**

**Running a docker image for mysql :**

**Step-1** : docker commands to run mysql container

docker pull mysql

docker run --name db -d -p 3306:3306 -e MYSQL\_ROOT\_PASSWORD=Welcome123 mysql

**Step-2 : get inside the mysql container to check the users present**

docker exec -it c737e4e2914e bin/bash

mysql -uroot –pWelcome123

check the users using following command,

select user from mysql.user;

**output :**

user |

+------------------+

| root |

| mysql.infoschema |

| mysql.session |

| mysql.sys |

| root |

+------------------+

**Configure the mysql database engine for vault on one of the vault vms**

The following command will create new user by replacing the {{name }} & {{password}} with the username and password which is created dynamically during **vault read**

vault write database/roles/my-sql-role \

db\_name=my-mysql-database \

creation\_statements="CREATE USER '{{name}}'@'%' IDENTIFIED BY '{{password}}';GRANT SELECT ON \*.\* TO '{{name}}'@'%';" \

default\_ttl="1h" \

max\_ttl="1h"

The following command will install the required plugin for mysql and then configure the root user credentials using which a dynamic user credentials are generated.

vault write database/config/my-mysql-database \

plugin\_name=mysql-database-plugin \

connection\_url="{{username}}:{{password}}@tcp(54.255.248.129:3306)/" \

allowed\_roles="mysql-role" \

username="root" \

password="Welcome123"

Now, perform vault read operation to generate dynamic mysql credentials

vault read database/creds/my-role

**output:**

Key Value

--- -----

lease\_id database/creds/my-role/aGYp7UIjCqrc3rdRBWbUvwdP

lease\_duration 1h

lease\_renewable true

password A1a-kaJNJ0FiTd2BcahZ

username v-root-my-role-XARNzWzG7o6bfev2t

To check the created temporary users in sql :

docker exec -it c737e4e2914e bin/bash

mysql -uroot –pWelcome123

instead of root you can try using following username and password :

mysql -uv-root-my-role-XARNzWzG7o6bfev2t –pA1a-kaJNJ0FiTd2BcahZ

See all the users using following command ,

select user from mysql.user

**output:**

+----------------------------------+

| user |

+----------------------------------+

| root |

| v-root-my-role-2XZ1FFi4NYTGFdKVe |

| v-root-my-role-XARNzWzG7o6bfev2t |

| mysql.infoschema |

| mysql.session |

| mysql.sys |

| root |

+----------------------------------+

**Curl command to generate mysql secrets :**

curl \

--header "X-Vault-Token:s.IZeqoi10Pez65z1hEqHvbiWb " \

--request GET \

http://52.90.88.15:8200/v1/database/creds/my-role

**output:**

{"request\_id":"bbb61326-8a25-2861-e9c6-9d04c33fa39f","lease\_id":"database/creds/my-role/Vv8gD6ly9IXqYGoOhyNXOIXN","renewable":true,"lease\_duration":3600,"data":{"password":"A1a-O9SYxBREGFTmQvvZ","username":"v-root-my-role-r0By9OWlgdizdFjm7"},"wrap\_info":null,"warnings":null,"auth":null}

**Reference Links :**

<https://www.vaultproject.io/docs/secrets/databases/mysql-maria>

<https://www.vaultproject.io/api/secret/databases/mysql-maria>

**curl --header "X-Vault-Token: s.9NuiX2lkeyVB8YhfC7ct3GDS" http://1c05353a-default-vault-c083-1304294467.ap-southeast-1.elb.amazonaws.com/v1/database/creds/readonly**

root@ip-10-0-101-22:~# vault list database/roles

Keys

----

my-role

readonly

root@ip-10-0-101-22:~# vault write database/roles/my-role \

> db\_name=my-mysql-database \

> creation\_statements="CREATE USER '{{name}}'@'%' IDENTIFIED BY '{{password}}';GRANT SELECT ON \*.\* TO '{{name}}'@'%';" \

> default\_ttl="1h" \

> max\_ttl="1h"

Success! Data written to: database/roles/my-role

root@ip-10-0-101-22:~# vault write database/roles/mysql-role db\_name=my-mysql-database creation\_statements="CREATE US

ER '{{name}}'@'%' IDENTIFIED BY '{{password}}';GRANT SELECT ON \*.\* TO '{{name}}'@'%';" default\_ttl="1h" max\_ttl="1h"

Success! Data written to: database/roles/mysql-role

root@ip-10-0-101-22:~# vault write database/config/my-mysql-database \

> plugin\_name=mysql-database-plugin \

> connection\_url="{{username}}:{{password}}@tcp(54.255.248.129:3306)/" \

> allowed\_roles="mysql-role" \

> username="root" \

> password="Welcome123"

root@ip-10-0-101-22:~#

root@ip-10-0-101-22:~# vault read database/creds/msqly-role

Error reading database/creds/msqly-role: Error making API request.

URL: GET http://127.0.0.1:8200/v1/database/creds/msqly-role

Code: 400. Errors:

\* unknown role: msqly-role

root@ip-10-0-101-22:~# vault read database/creds/mysql-role

Key Value

--- -----

lease\_id database/creds/mysql-role/jyk0YbD44kDqNfMvEUB392tw

lease\_duration 1h

lease\_renewable true

password A1a-dFmr0Ip3vrtsZePA

username v-root-mysql-role-xh1hKcWo9PnziF

root@ip-10-0-101-22:~# vault list database/roles

Keys

----

my-role

mysql-role

readonly