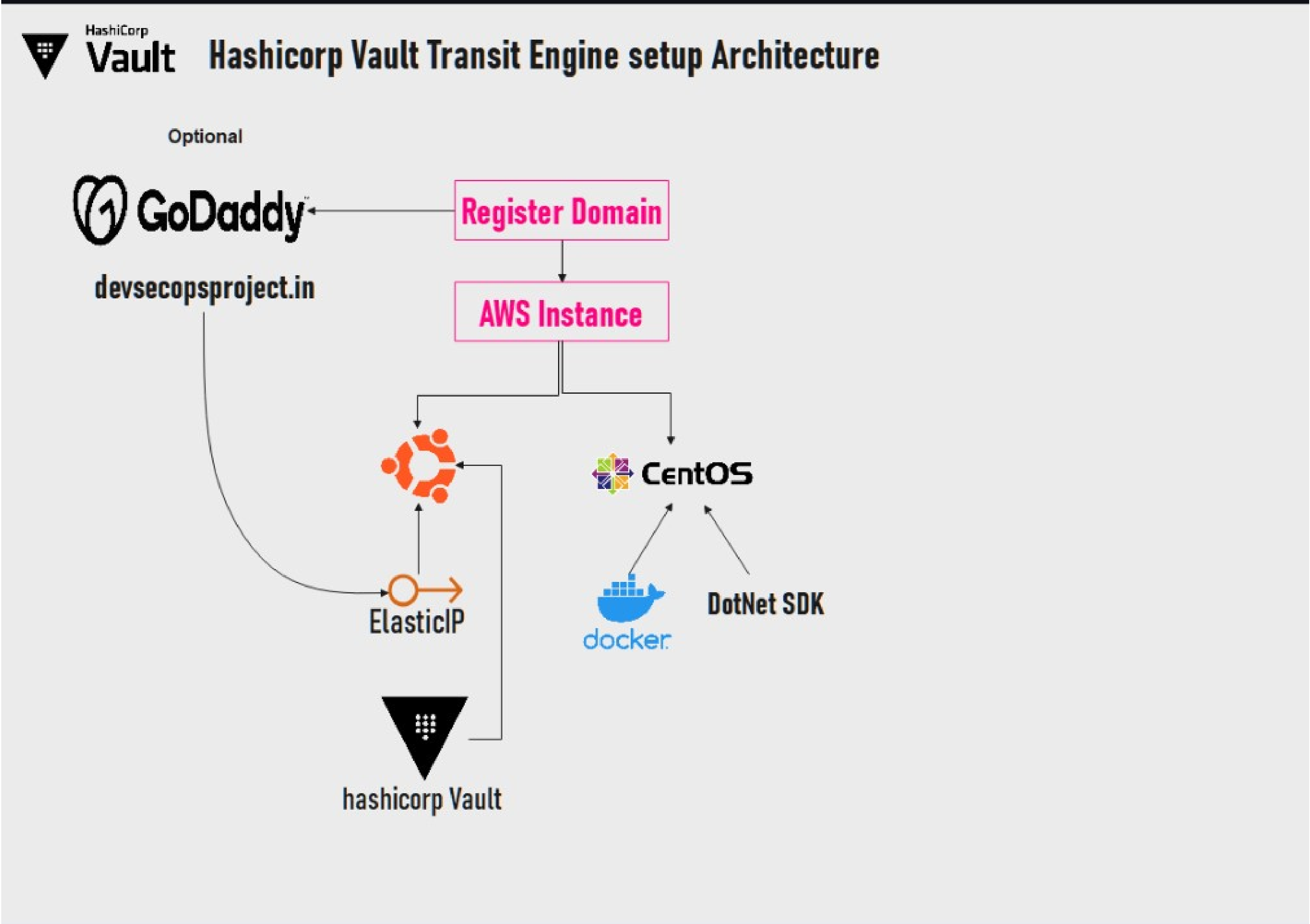
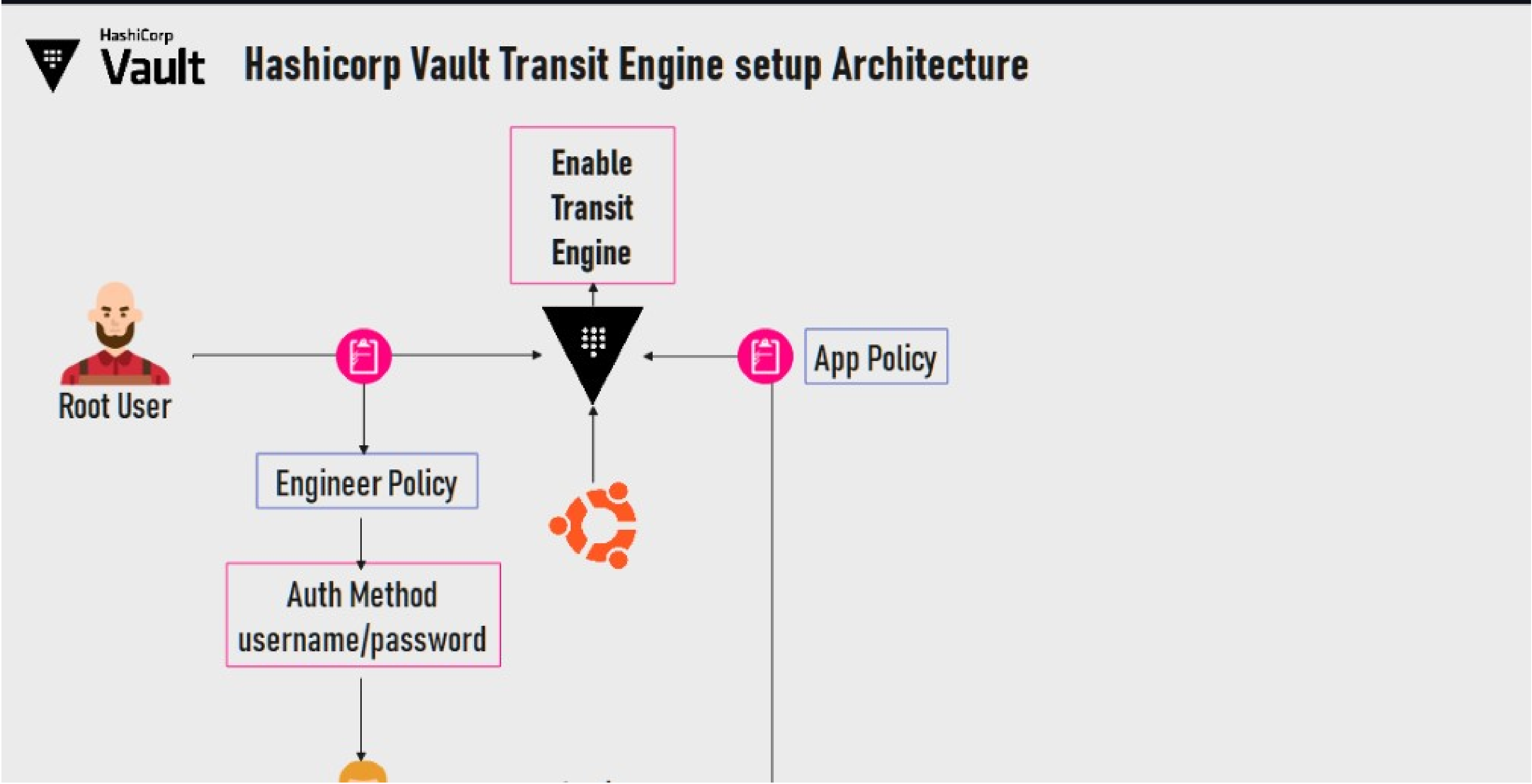
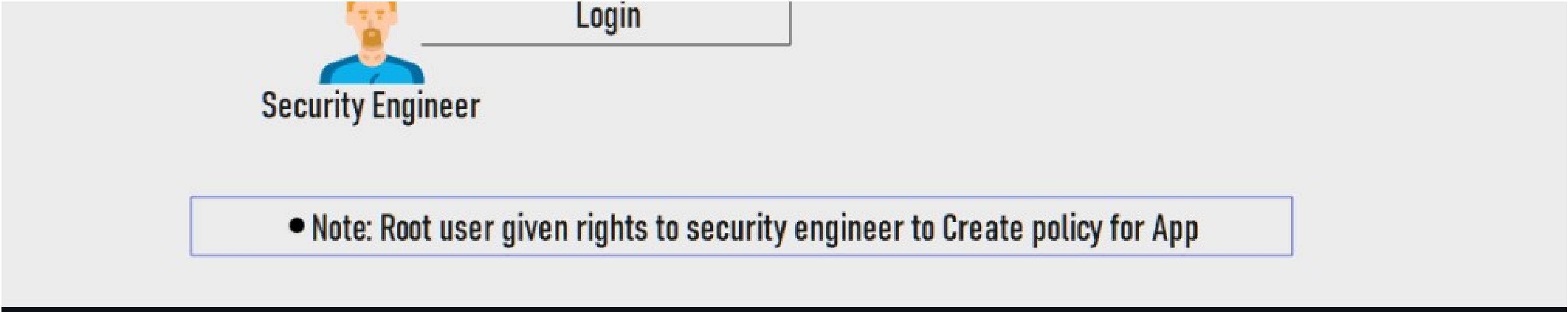
Transist secret engine

Transit Secret engine Architecuture

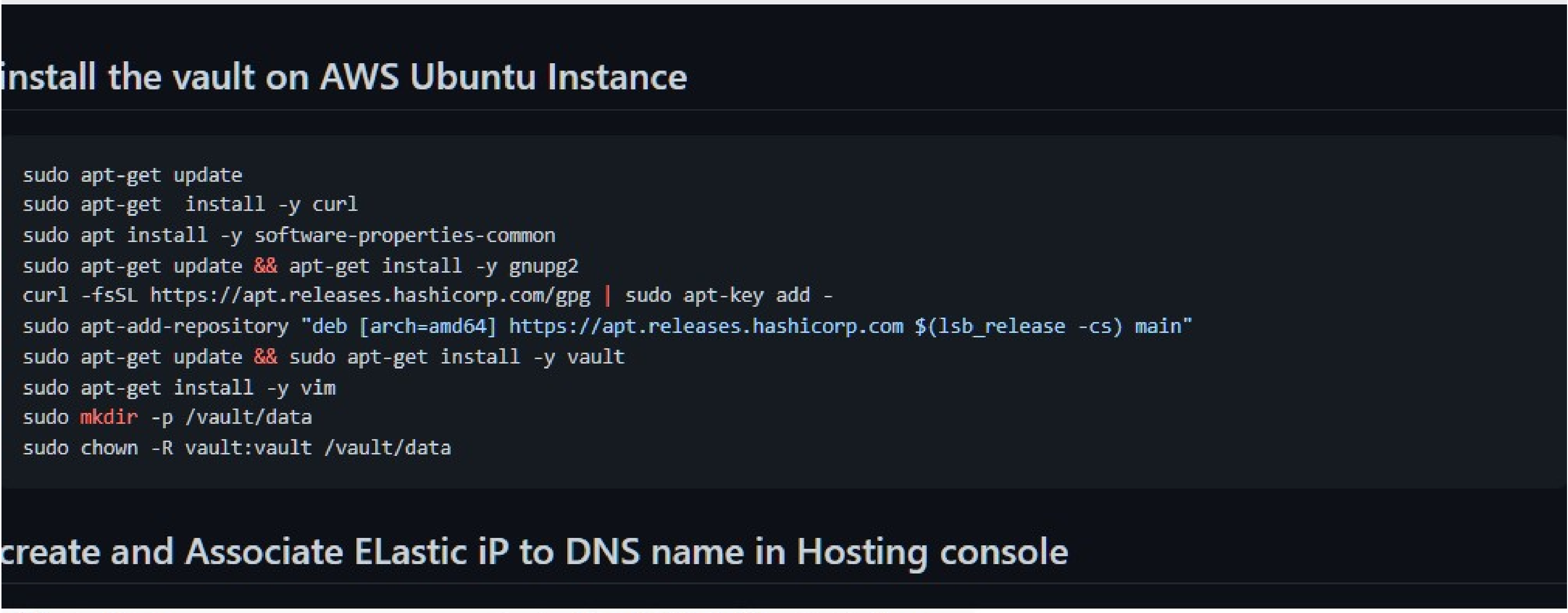


Transit engine configuration flow


HashiCorp
Vault
Hashicorp Vault Transit Engine setup Architecture
Enable Transit Engine
Root User
App Policy
Engineer Policy
Auth Method username/password



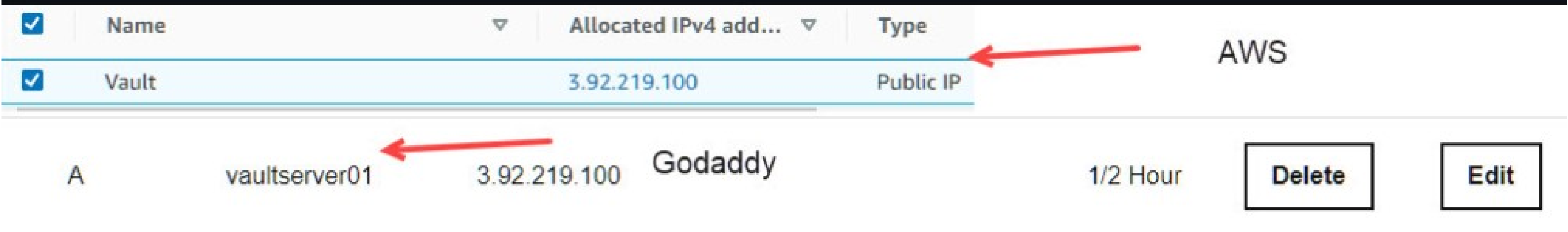
- Note: Root user given rights to security engineer to Create policy for App



install the vault on AWS Ubuntu Instance

```
sudo apt-get update
sudo apt-get  install -y curl
sudo apt install -y software-properties-common
sudo apt-get update && apt-get install -y gnupg2
curl -fsSL https://apt.releases.hashicorp.com/gpg | sudo apt-key add -
sudo apt-add-repository "deb [arch=amd64] https://apt.releases.hashicorp.com $(lsb_release -cs) main"
sudo apt-get update && sudo apt-get install -y vault
sudo apt-get install -y vim
sudo mkdir -p /vault/data
sudo chown -R vault:vault /vault/data
```

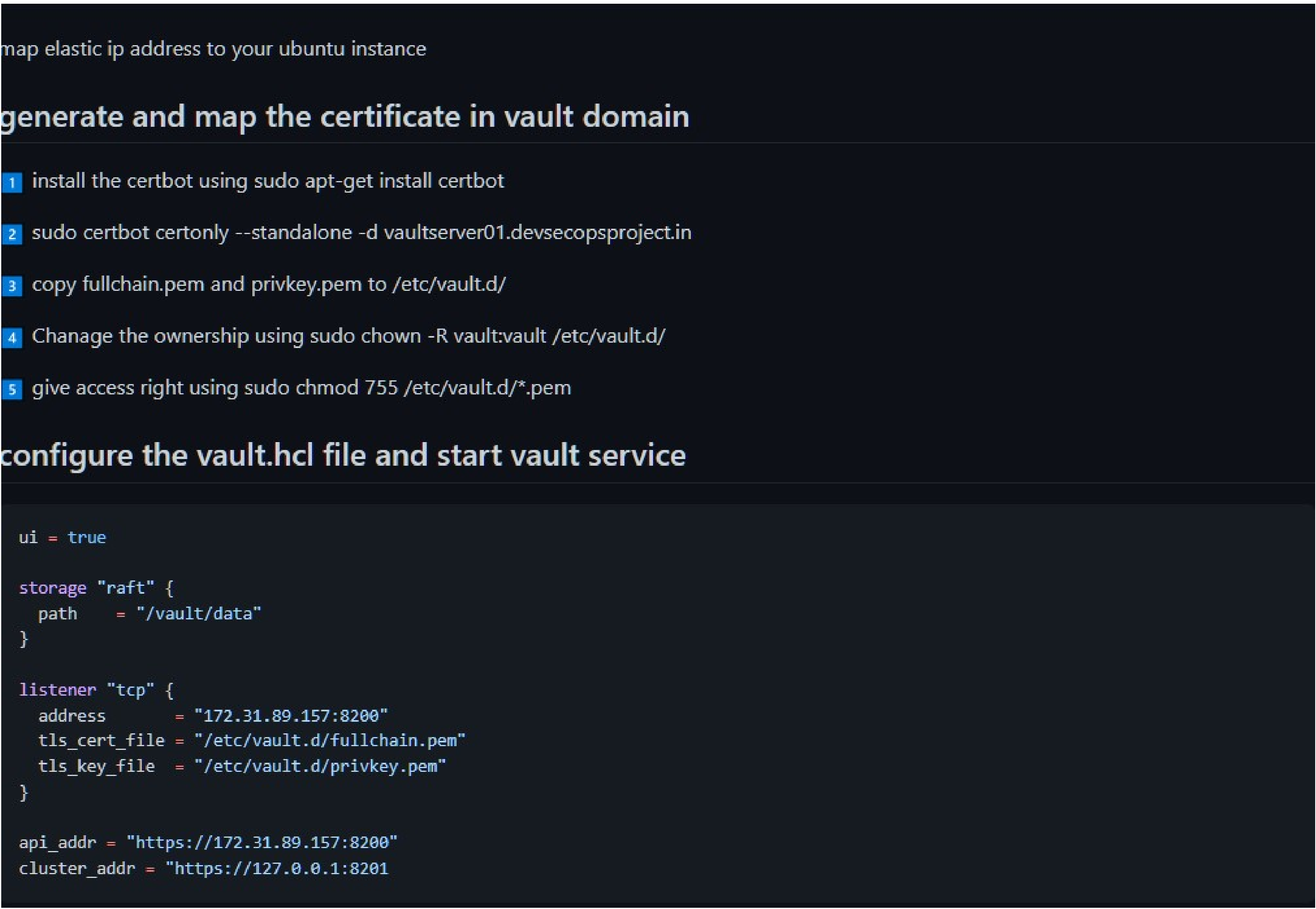
create and Associate ELastic iP to DNS name in Hosting console



☑	Name	Allocated IPv4 add...	Type
☑	Vault	3.92.219.100	Public IP

AWS

A	vaultserver01	3.92.219.100	Godaddy	1/2 Hour	Delete	Edit



map elastic ip address to your ubuntu instance

generate and map the certificate in vault domain

1. install the certbot using sudo apt-get install certbot
2. sudo certbot certonly --standalone -d vaultserver01.devsecopsproject.in
3. copy fullchain.pem and privkey.pem to /etc/vault.d/
4. Chanage the ownership using sudo chown -R vault:vault /etc/vault.d/
5. give access right using sudo chmod 755 /etc/vault.d/*.pem

configure the vault.hcl file and start vault service

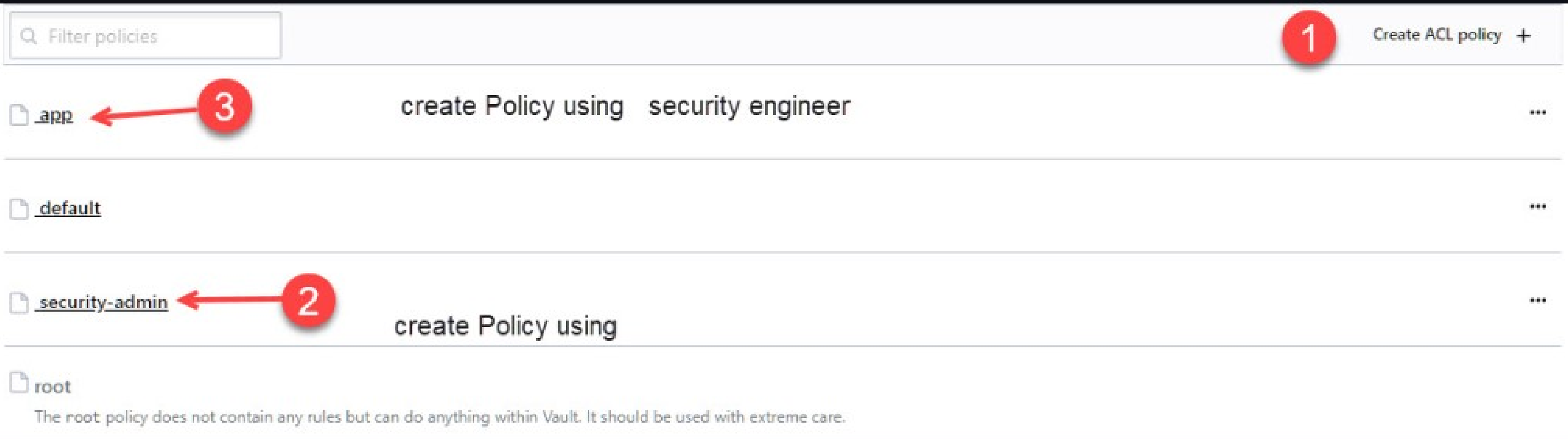
```
ui = true

storage "raft" {
  path    = "/vault/data"
}

listener "tcp" {
  address       = "172.31.89.157:8200"
  tls_cert_file = "/etc/vault.d/fullchain.pem"
  tls_key_file  = "/etc/vault.d/privkey.pem"
}

api_addr = "https://172.31.89.157:8200"
cluster_addr = "https://127.0.0.1:8201
```

then run sudo systemctl enable --now vault.service

Access the vault ui using https://vaultserver01.devsecopsproject.in:8200

generate shamir secret and root key and unseal the vault

create security engineer policy



create Policy using security engineer

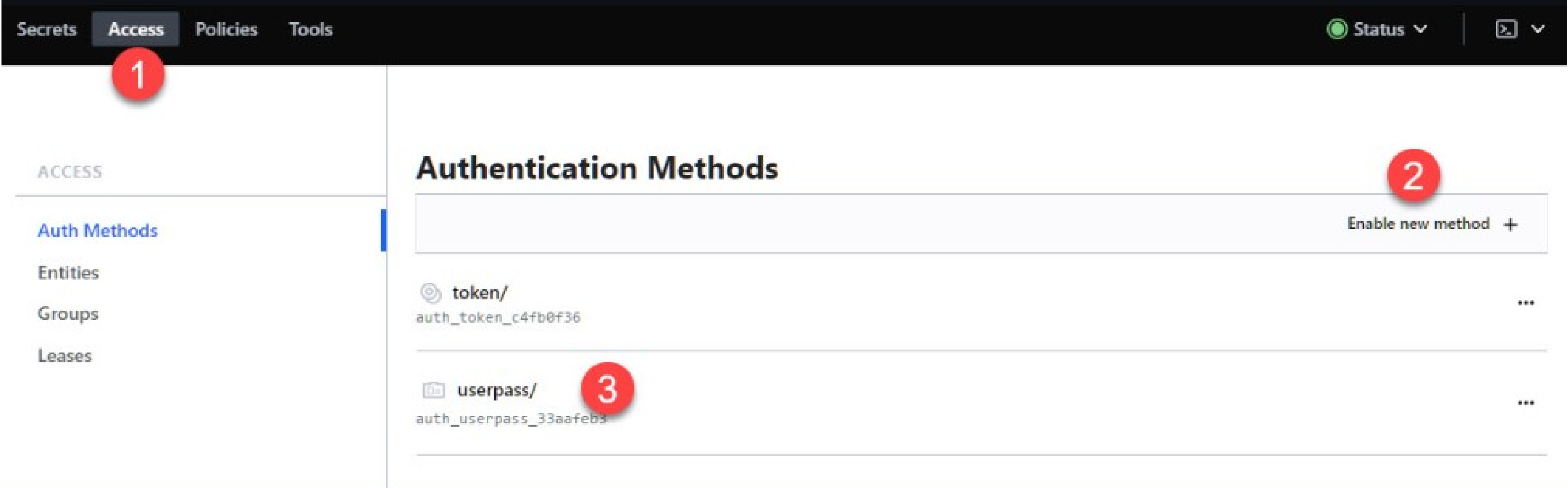
create Policy using

The root policy does not contain any rules but can do anything within Vault. It should be used with extreme care.

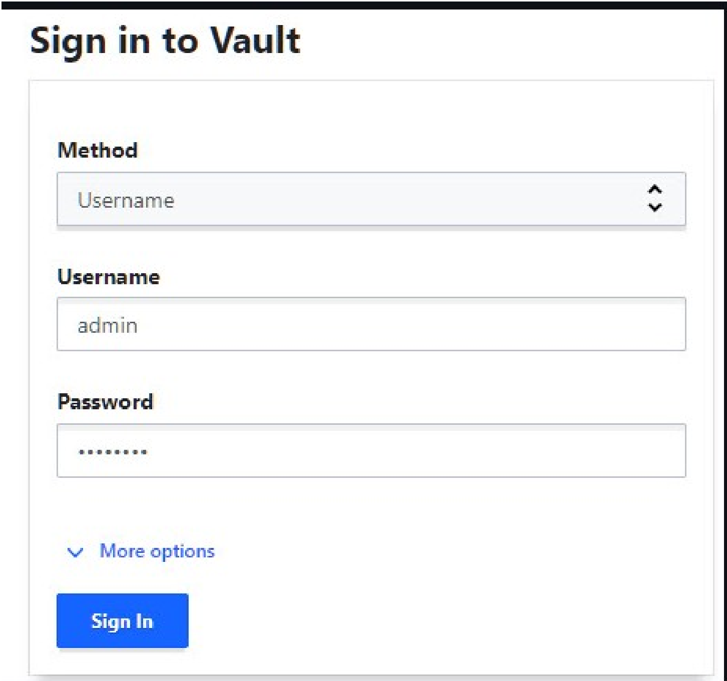
enable transit secret engine name mu_app_key and create Policy for security Engineer

```
# Manage the transit secrets engine
path "transit/keys/*" {
  capabilities = [ "create", "read", "update", "delete", "list", "sudo" ]
}

# Enable the transit secrets engine
path "sys/mounts/transit" {
  capabilities = [ "create", "update" ]
}

# Write ACL policies
path "sys/policies/acl/*" {
  capabilities = [ "create", "read", "update", "delete", "list" ]
}

# Create tokens for verification & test
path "auth/token/create" {
  capabilities = [ "create", "update", "sudo" ]
}
```

attach policy to username/password auth



login with username and password and copy security engineer token



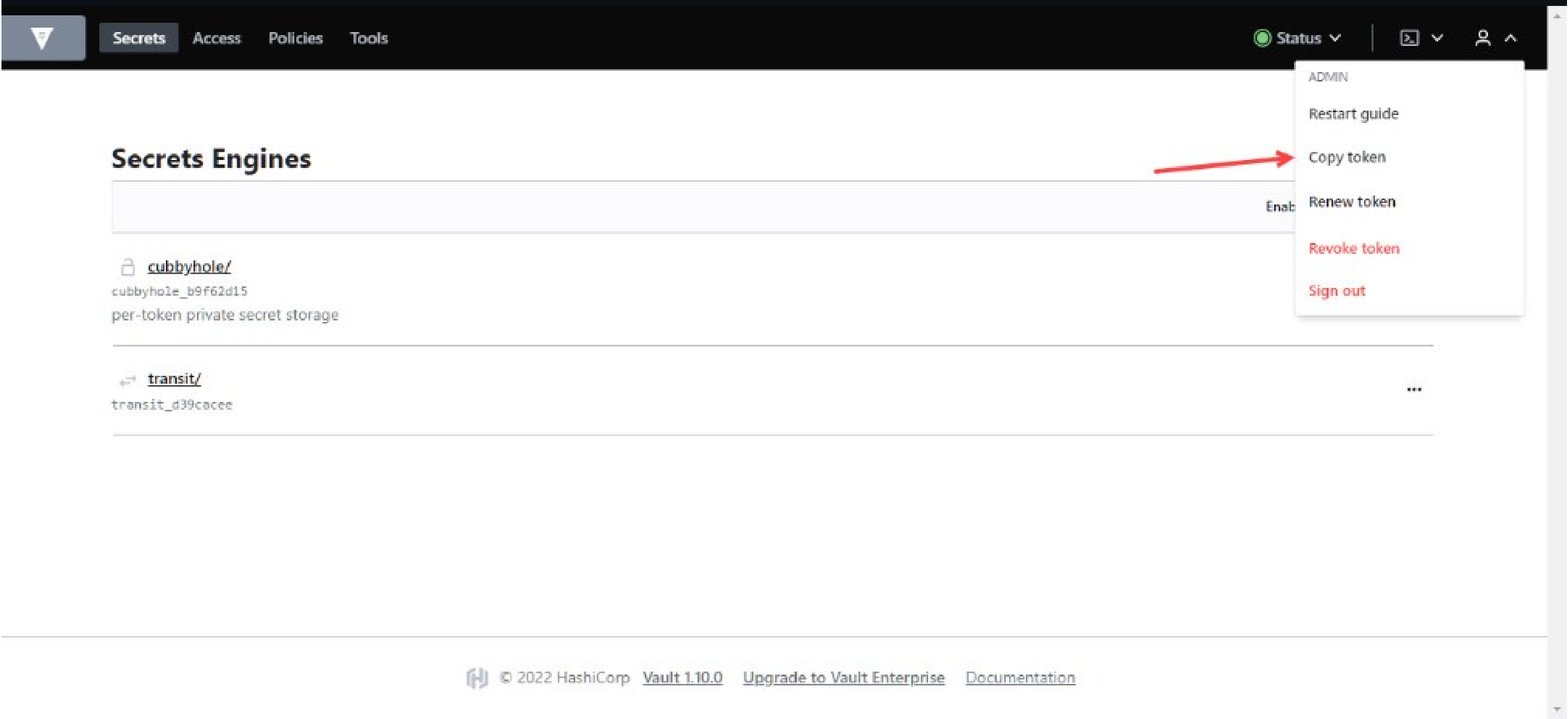
Sign in to Vault

Method: Username

Username: admin

Password: ••••••••

copy token for security engineer



Secrets Engines

cubbyhole/
cubbyhole_b9f62d15
per-token private secret storage

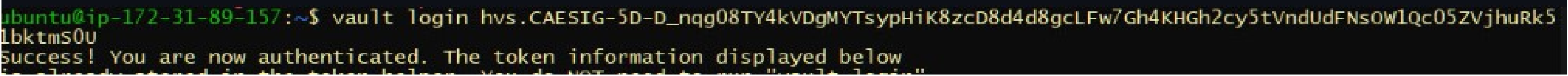
transit/
transit_d39cacee

© 2022 HashiCorp Vault 1.10.0 Upgrade to Vault Enterprise Documentation

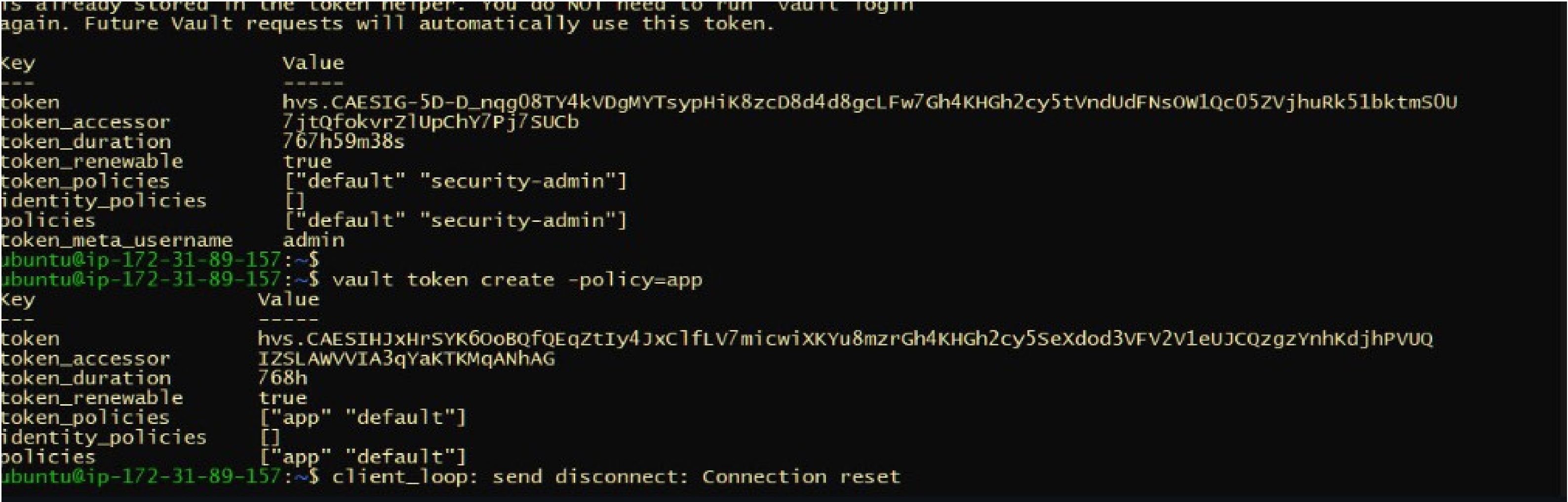
login with security engineer from ui and create app policy

```
path "transit/keys/my_app_key" {
  capabilities = ["read"]
}

path "transit/rewrap/my_app_key" {
  capabilities = ["update"]
}

path "transit/encrypt/my_app_key" {
  capabilities = ["update"]
}
```

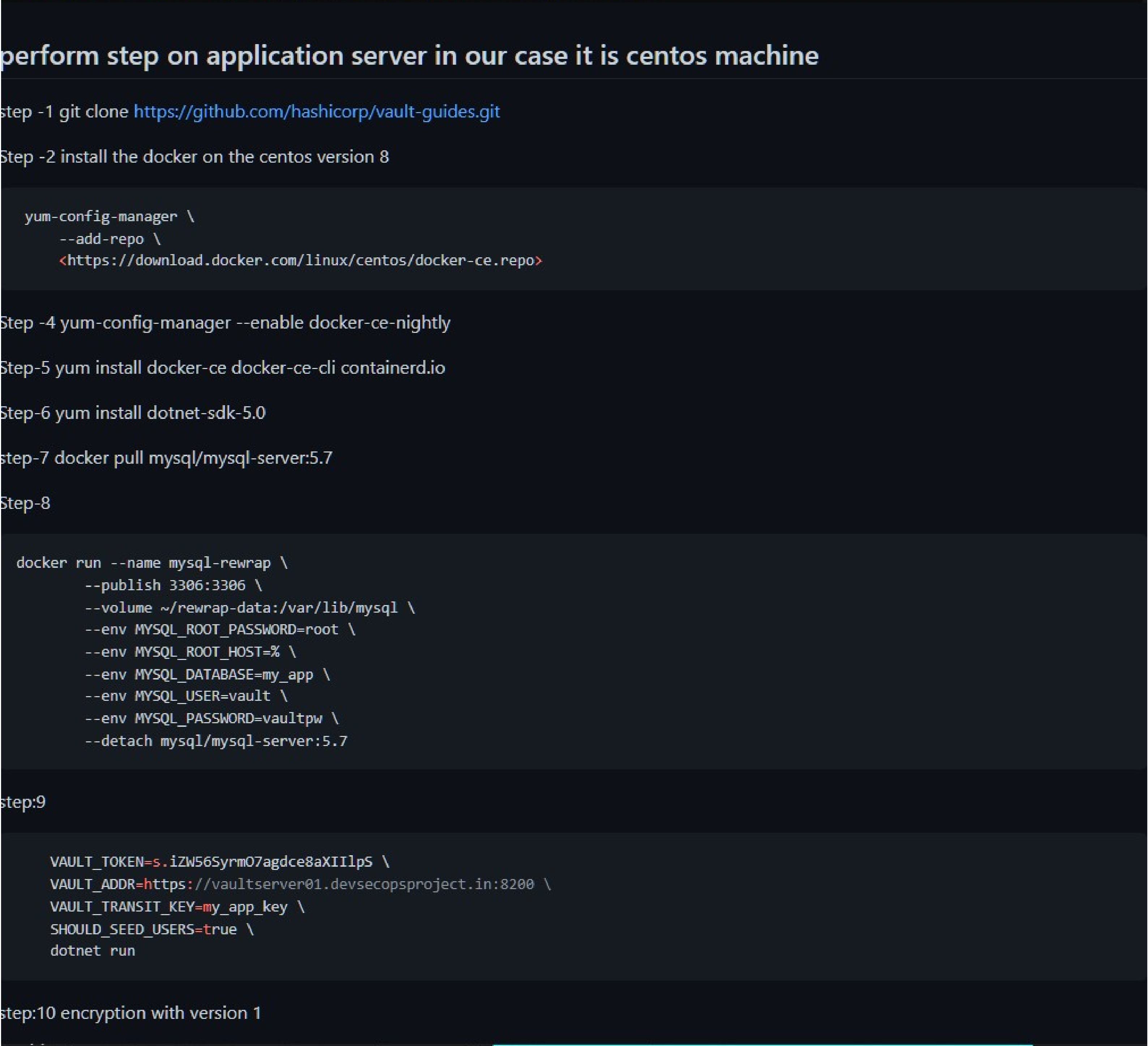
login security engineer token using cli and create app policy token



```
ubuntu@ip-172-31-89-157:~$ vault login hvs.CAESIG-5D-D_nqg08TY4kVDgMYTsypHiK8zcD8d4d8gcLFw7Gh4KHGh2cy5tVndUdFNsOW1Qc05ZVjhuRk5
1bktmS0U
Success! You are now authenticated. The token information displayed below
is already stored in the token helper. You do NOT need to run "vault login"
```



```
is already stored in the token helper. You do NOT need to run "vault login"
again. Future Vault requests will automatically use this token.

Key                      Value
---                      -----
token                    hvs.CAESIG-5D-D_nqg08TY4kVDgMYTsypHiK8zcD8d4d8gcLFw7Gh4KHGh2cy5tVndUdFNsOW1Qc05ZVjhuRk51bktmS0U
token_accessor           7jtQfokvrZlUpChY7Pj7SUCb
token_duration           767h59m38s
token_renewable          true
token_policies           ["default" "security-admin"]
identity_policies        []
policies                 ["default" "security-admin"]
token_meta_username      admin
ubuntu@ip-172-31-89-157:~$
ubuntu@ip-172-31-89-157:~$ vault token create -policy=app
Key                    Value
---                    -----
token                  hvs.CAESIHJxHrSYK6OoBQfQEqZtIy4JxClfLV7micwiXKYu8mzrGh4KHGh2cy5SeXdod3VFV2V1eUJCQzgzYnhKdjhPVUQ
token_accessor         IZSLAWVVIA3qYaKTKMqANhAG
token_duration         768h
token_renewable        true
token_policies         ["app" "default"]
identity_policies      []
policies               ["app" "default"]
ubuntu@ip-172-31-89-157:~$ client_loop: send disconnect: Connection reset
```



perform step on application server in our case it is centos machine

step -1 git clone https://github.com/hashicorp/vault-guides.git

Step -2 install the docker on the centos version 8

```
yum-config-manager \
    --add-repo \
    <https://download.docker.com/linux/centos/docker-ce.repo>
```

Step -4 yum-config-manager --enable docker-ce-nightly

Step-5 yum install docker-ce docker-ce-cli containerd.io

Step-6 yum install dotnet-sdk-5.0

step-7 docker pull mysql/mysql-server:5.7

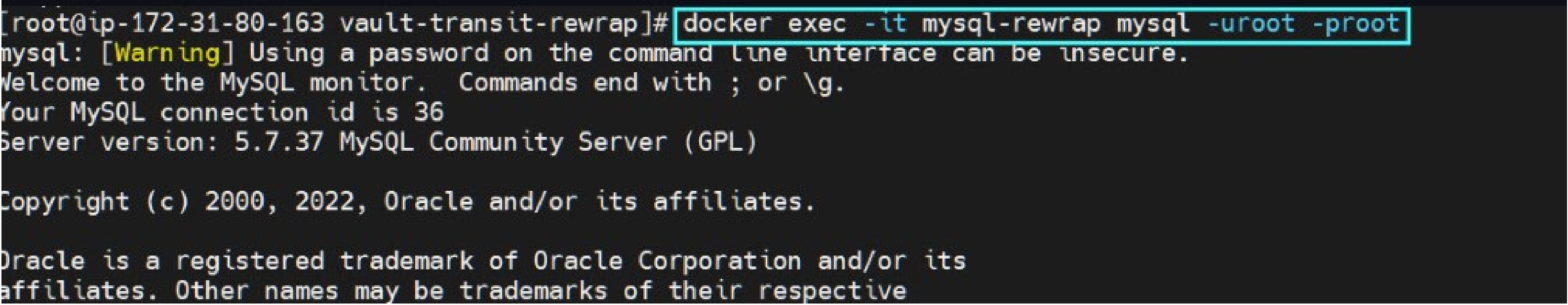
Step-8

```
docker run --name mysql-rewrap \
        --publish 3306:3306 \
        --volume ~/rewrap-data:/var/lib/mysql \
        --env MYSQL_ROOT_PASSWORD=root \
        --env MYSQL_ROOT_HOST=% \
        --env MYSQL_DATABASE=my_app \
        --env MYSQL_USER=vault \
        --env MYSQL_PASSWORD=vaultpw \
        --detach mysql/mysql-server:5.7
```

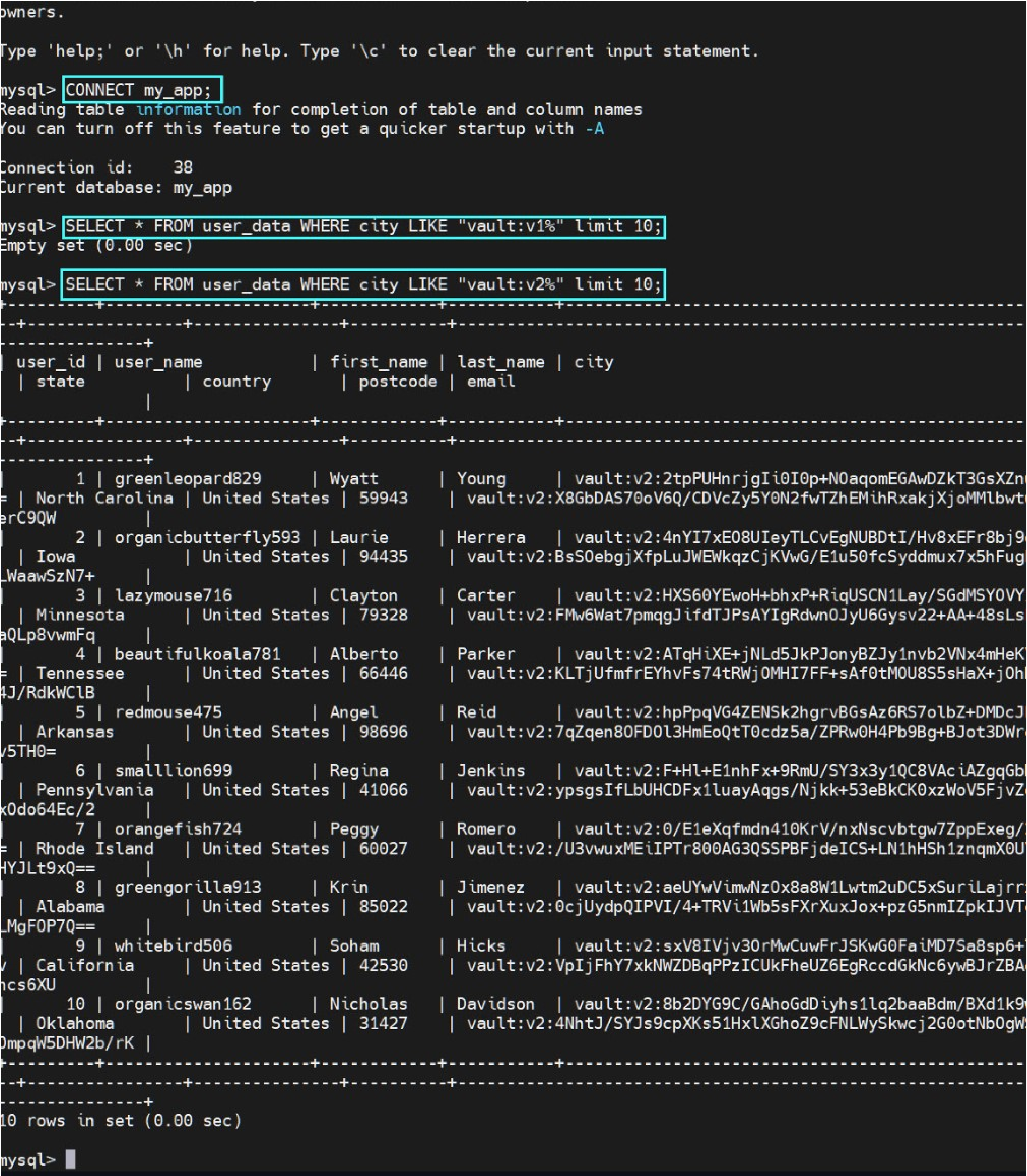
step:9

```
VAULT_TOKEN=s.iZW56SyrmO7agdce8aXIIlpS \
VAULT_ADDR=https://vaultserver01.devsecopsproject.in:8200 \
VAULT_TRANSIT_KEY=my_app_key \
SHOULD_SEED_USERS=true \
dotnet run
```

step:10 encryption with version 1

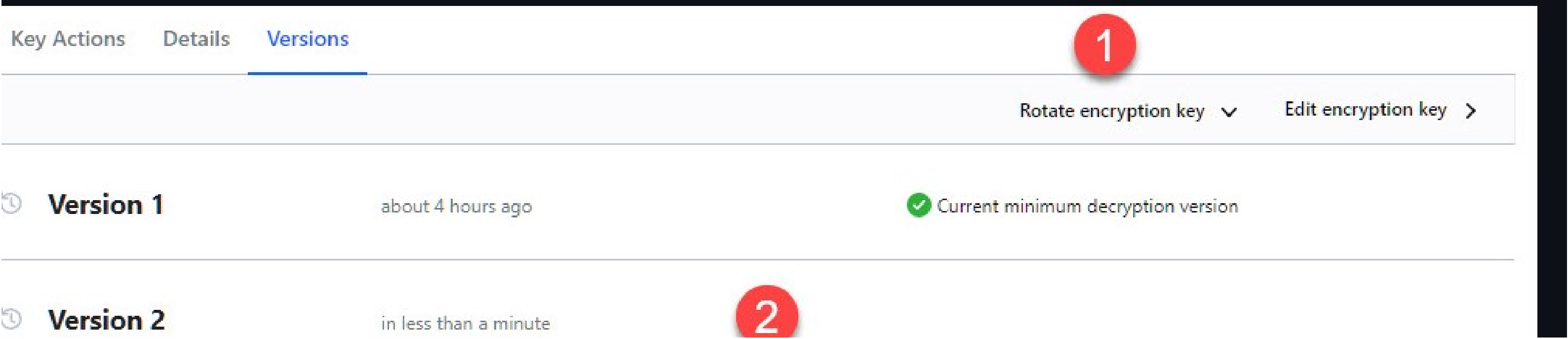


```
[root@ip-172-31-80-163 vault-transit-rewrap]# docker exec -it mysql-rewrap mysql -uroot -proot
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 36
Server version: 5.7.37 MySQL Community Server (GPL)

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
```



```
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CONNECT my_app;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Connection id:    38
Current database: my_app

mysql> SELECT * FROM user_data WHERE city LIKE "vault:v1%" limit 10;
Empty set (0.00 sec)

mysql> SELECT * FROM user_data WHERE city LIKE "vault:v2%" limit 10;
+---------+--------------------+------------+-----------+------------------------------------------------------
--+---------------+---------------+----------+----------------------------------------------------------------
--------------+
| user_id | user_name          | first_name | last_name | city
  | state         | country       | postcode | email
              |
+---------+--------------------+------------+-----------+------------------------------------------------------
--+---------------+---------------+----------+----------------------------------------------------------------
--------------+
|       1 | greenleopard829    | Wyatt      | Young     | vault:v2:2tpPUHnrjgIi0I0p+NOaqomEGAwDZkT3GsXZn
= | North Carolina | United States | 59943    | vault:v2:X8GbDAS70oV6Q/CDVcZy5Y0N2fwTZhEMihRxakjXjoMMlbwt
erC9QW        |
|       2 | organicbutterfly593 | Laurie     | Herrera   | vault:v2:4nYI7xE08UIeyTLCvEgNUBDtI/Hv8xEFr8bj9
  | Iowa          | United States | 94435    | vault:v2:BsSOebgjXfpLuJWEWkqzCjKVwG/E1u50fcSyddmux7x5hFug
LWaawSzN7+    |
|       3 | lazymouse716       | Clayton    | Carter    | vault:v2:HXS60YEwoH+bhxP+RiqUSCN1Lay/SGdMSYOVY
  | Minnesota     | United States | 79328    | vault:v2:FMw6Wat7pmqgJifdTJPsAYIgRdwnOJyU6Gysv22+AA+48sLs
aQLp8vwmFq    |
|       4 | beautifulkoala781  | Alberto    | Parker    | vault:v2:ATqHiXE+jNLd5JkPJonyBZJy1nvb2VNx4mHeK
= | Tennessee     | United States | 66446    | vault:v2:KLTjUfmfrEYhvFs74tRWjOMHI7FF+sAf0tMOU8S5sHaX+jOh
4J/RdkWClB    |
|       5 | redmouse475        | Angel      | Reid      | vault:v2:hpPpqVG4ZENSk2hgrvBGsAz6RS7olbZ+DMDcJ
  | Arkansas      | United States | 98696    | vault:v2:7qZqen80FDOl3HmEoQtT0cdz5a/ZPRw0H4Pb9Bg+BJot3DWr
v5TH0=        |
|       6 | smalllion699       | Regina     | Jenkins   | vault:v2:F+Hl+E1nhFx+9RmU/SY3x3y1QC8VAciAZgqGb
  | Pennsylvania  | United States | 41066    | vault:v2:ypsgsIfLbUHCDFx1luayAqgs/Njkk+53eBkCK0xzWoV5FjvZ
xOdo64Ec/2    |
|       7 | orangefish724      | Peggy      | Romero    | vault:v2:0/E1eXqfmdn410KrV/nxNscvbtgw7ZppExeg/
= | Rhode Island  | United States | 60027    | vault:v2:/U3vwuxMEiIPTr800AG3QSSPBFjdeICS+LN1hHSh1znqmX0U
HYJLt9xQ==    |
|       8 | greengorilla913    | Krin       | Jimenez   | vault:v2:aeUYwVimwNzOx8a8W1Lwtm2uDC5xSuriLajrr
  | Alabama       | United States | 85022    | vault:v2:0cjUydpQIPVI/4+TRVi1Wb5sFXrXuxJox+pzG5nmIZpkIJVT
LMgFOP7Q==    |
|       9 | whitebird506       | Soham      | Hicks     | vault:v2:sxV8IVjv3OrMwCuwFrJSKwG0FaiMD7Sa8sp6+
v | California    | United States | 42530    | vault:v2:VpIjFhY7xkNWZDBqPPzICUkFheUZ6EgRccdGkNc6ywBJrZBA
ncs6XU        |
|      10 | organicswan162     | Nicholas   | Davidson  | vault:v2:8b2DYG9C/GAhoGdDiyhs1lq2baaBdm/BXd1k9
  | Oklahoma      | United States | 31427    | vault:v2:4NhtJ/SYJs9cpXKs51HxlXGhoZ9cFNLWySkwcj2G0otNbOgW
OmpqW5DHW2b/rK |
+---------+--------------------+------------+-----------+------------------------------------------------------
--+---------------+---------------+----------+----------------------------------------------------------------
--------------+
10 rows in set (0.00 sec)

mysql> █
```

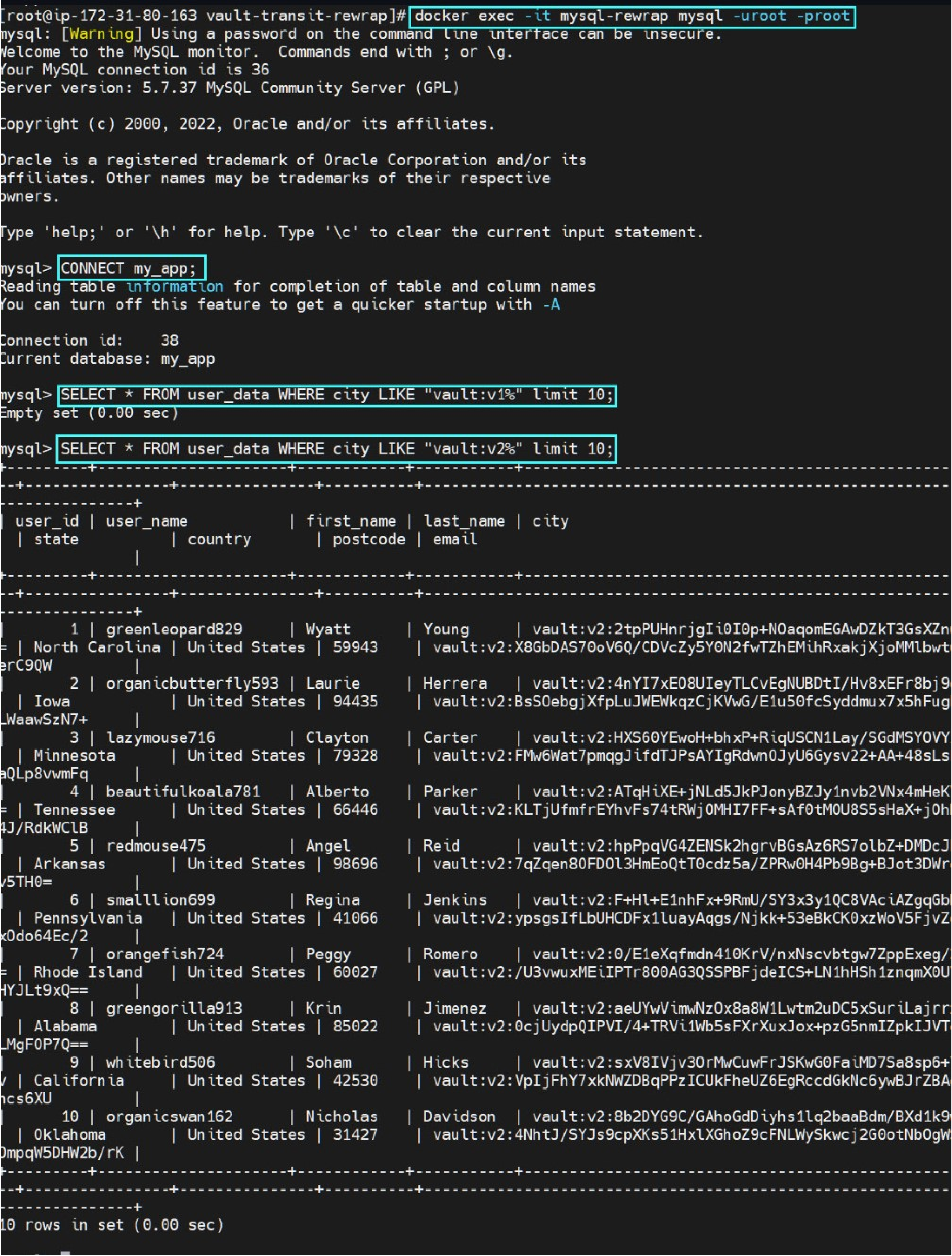
step:11 now rotate the key version using vault ui



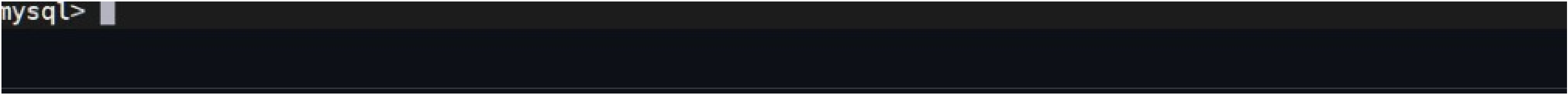
Version 1 about 4 hours ago ✓ Current minimum decryption version

Version 2 in less than a minute

step:12 Verify the effects



```
[root@ip-172-31-80-163 vault-transit-rewrap]# docker exec -it mysql-rewrap mysql -uroot -proot
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 36
Server version: 5.7.37 MySQL Community Server (GPL)

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CONNECT my_app;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Connection id:    38
Current database: my_app

mysql> SELECT * FROM user_data WHERE city LIKE "vault:v1%" limit 10;
Empty set (0.00 sec)

mysql> SELECT * FROM user_data WHERE city LIKE "vault:v2%" limit 10;
+---------+---------------------+------------+-----------+-----------------------------------------------------
--+-----------------+---------------+----------+----------------------------------------------------------------
--------------+
| user_id | user_name           | first_name | last_name | city
  | state           | country       | postcode | email
              |
+---------+---------------------+------------+-----------+-----------------------------------------------------
--+-----------------+---------------+----------+----------------------------------------------------------------
--------------+
|       1 | greenleopard829     | Wyatt      | Young     | vault:v2:2tpPUHnrjgIi0I0p+NOaqomEGAwDZkT3GsXZn
= | North Carolina | United States | 59943    | vault:v2:X8GbDAS70oV6Q/CDVcZy5Y0N2fwTZhEMihRxakjXjoMMlbwt
erC9QW        |
|       2 | organicbutterfly593 | Laurie     | Herrera   | vault:v2:4nYI7xEO8UIeyTLCvEgNUBDtI/Hv8xEFr8bj9
  | Iowa           | United States | 94435    | vault:v2:BsSOebgjXfpLuJWEWkqzCjKVwG/E1u50fcSyddmux7x5hFug
LWaawSzN7+    |
|       3 | lazymouse716        | Clayton    | Carter    | vault:v2:HXS60YEwoH+bhxP+RiqUSCN1Lay/SGdMSYOVY
  | Minnesota      | United States | 79328    | vault:v2:FMw6Wat7pmqgJifdTJPsAYIgRdwnOJyU6Gysv22+AA+48sLs
aQLp8vwmFq    |
|       4 | beautifulkoala781   | Alberto    | Parker    | vault:v2:ATqHiXE+jNLd5JkPJonyBZJy1nvb2VNx4mHeK
= | Tennessee      | United States | 66446    | vault:v2:KLTjUfmfrEYhvFs74tRWjOMHI7FF+sAf0tMOU8S5sHaX+jOh
4J/RdkWClB    |
|       5 | redmouse475         | Angel      | Reid      | vault:v2:hpPpqVG4ZENSk2hgrvBGsAz6RS7olbZ+DMDcJ
  | Arkansas       | United States | 98696    | vault:v2:7qZqen8OFDOl3HmEoQtT0cdz5a/ZPRw0H4Pb9Bg+BJot3DWr
v5TH0=        |
|       6 | smalllion699        | Regina     | Jenkins   | vault:v2:F+Hl+E1nhFx+9RmU/SY3x3y1QC8VAciAZgqGb
  | Pennsylvania   | United States | 41066    | vault:v2:ypsgsIfLbUHCDFx1luayAqgs/Njkk+53eBkCK0xzWoV5FjvZ
xOdo64Ec/2    |
|       7 | orangefish724       | Peggy      | Romero    | vault:v2:0/E1eXqfmdn410KrV/nxNscvbtgw7ZppExeg/
= | Rhode Island   | United States | 60027    | vault:v2:/U3vwuxMEiIPTr800AG3QSSPBFjdeICS+LN1hHSh1znqmX0U
HYJLt9xQ==    |
|       8 | greengorilla913     | Krin       | Jimenez   | vault:v2:aeUYwVimwNzOx8a8W1Lwtm2uDC5xSuriLajrr
  | Alabama        | United States | 85022    | vault:v2:0cjUydpQIPVI/4+TRVi1Wb5sFXrXuxJox+pzG5nmIZpkIJVT
LMgFOP7Q==    |
|       9 | whitebird506        | Soham      | Hicks     | vault:v2:sxV8IVjv3OrMwCuwFrJSKwG0FaiMD7Sa8sp6+
v | California     | United States | 42530    | vault:v2:VpIjFhY7xkNWZDBqPPzICUkFheUZ6EgRccdGkNc6ywBJrZBA
ncs6XU        |
|      10 | organicswan162      | Nicholas   | Davidson  | vault:v2:8b2DYG9C/GAhoGdDiyhs1lq2baaBdm/BXd1k9
  | Oklahoma       | United States | 31427    | vault:v2:4NhtJ/SYJs9cpXKs51HxlXGhoZ9cFNLWySkwcj2G0otNbOgW
OmpqW5DHW2b/rK |
+---------+---------------------+------------+-----------+-----------------------------------------------------
--+-----------------+---------------+----------+----------------------------------------------------------------
--------------+
10 rows in set (0.00 sec)
```



```
mysql>
```