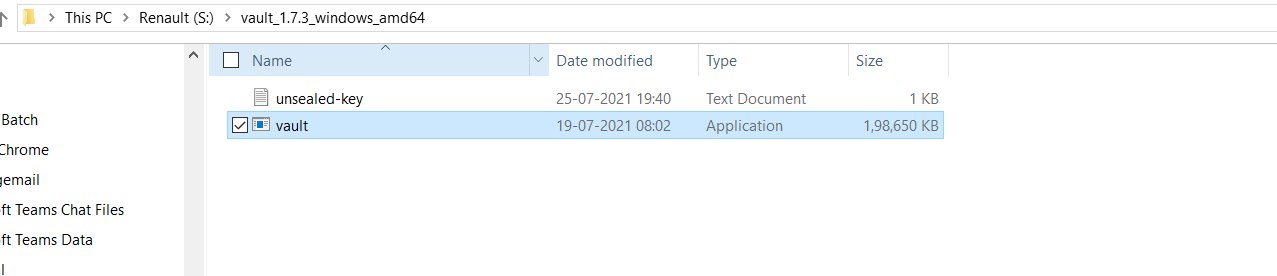
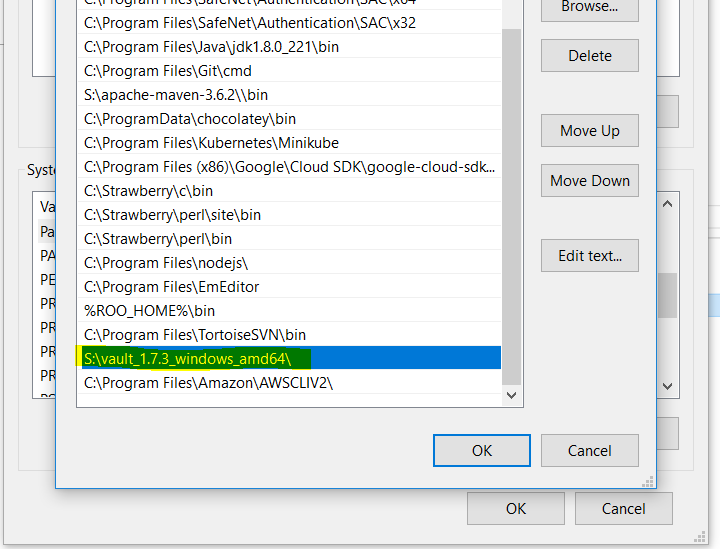
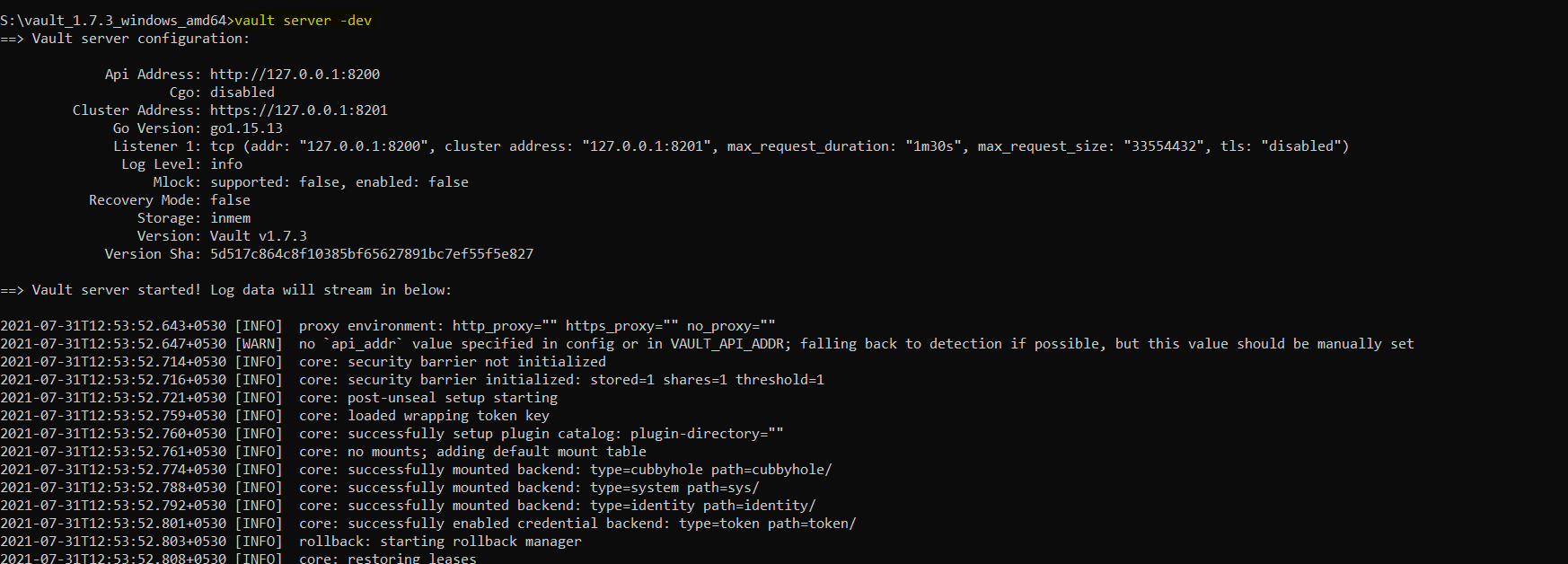
Vault installation

Download vault.exe for windows, set it to environment path



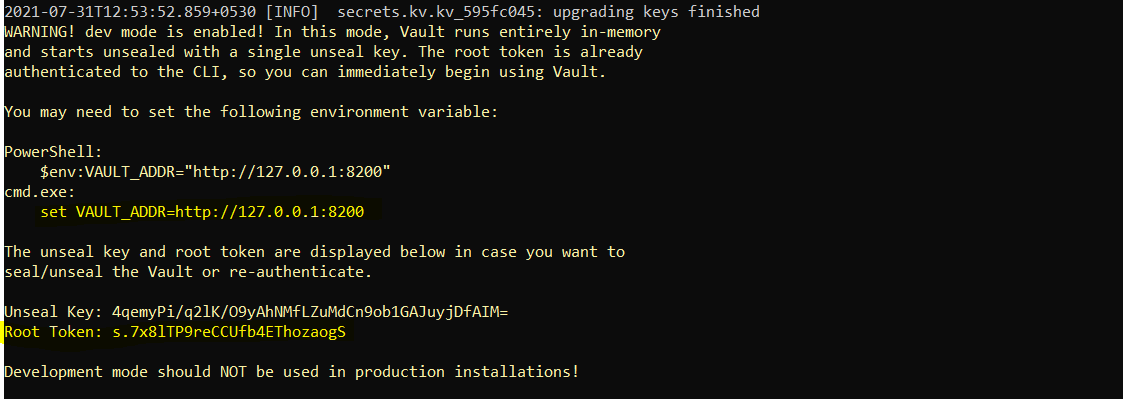


How to start vault in dev mode



Open new command window-

Set the VAULT\_ADDR and VAULT\_TOKEN variables in cmd line so that , vault commands will be using that for authentication



|  |
| --- |
| set VAULT\_ADDR=http://127.0.0.1:8200  set VAULT\_TOKEN=token-------------- |

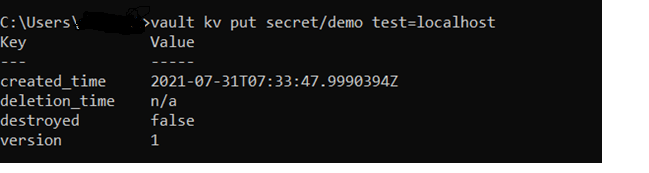
Various secret engines plugins are available like kv , aws , gcp .

Kv is default enable in dev mode with the name secret.

Kv helps us to store the key value pairs in vault.

In order to create entries we can use put cmd..

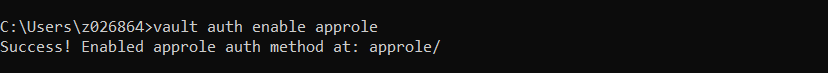
|  |
| --- |
| vault kv put secret/demo test=localhost |



In Org. we are using APPRole Auth method to authenticate config clients (may be pull method)

Enabling APPROLE auth method

|  |
| --- |
| vault auth enable approle |

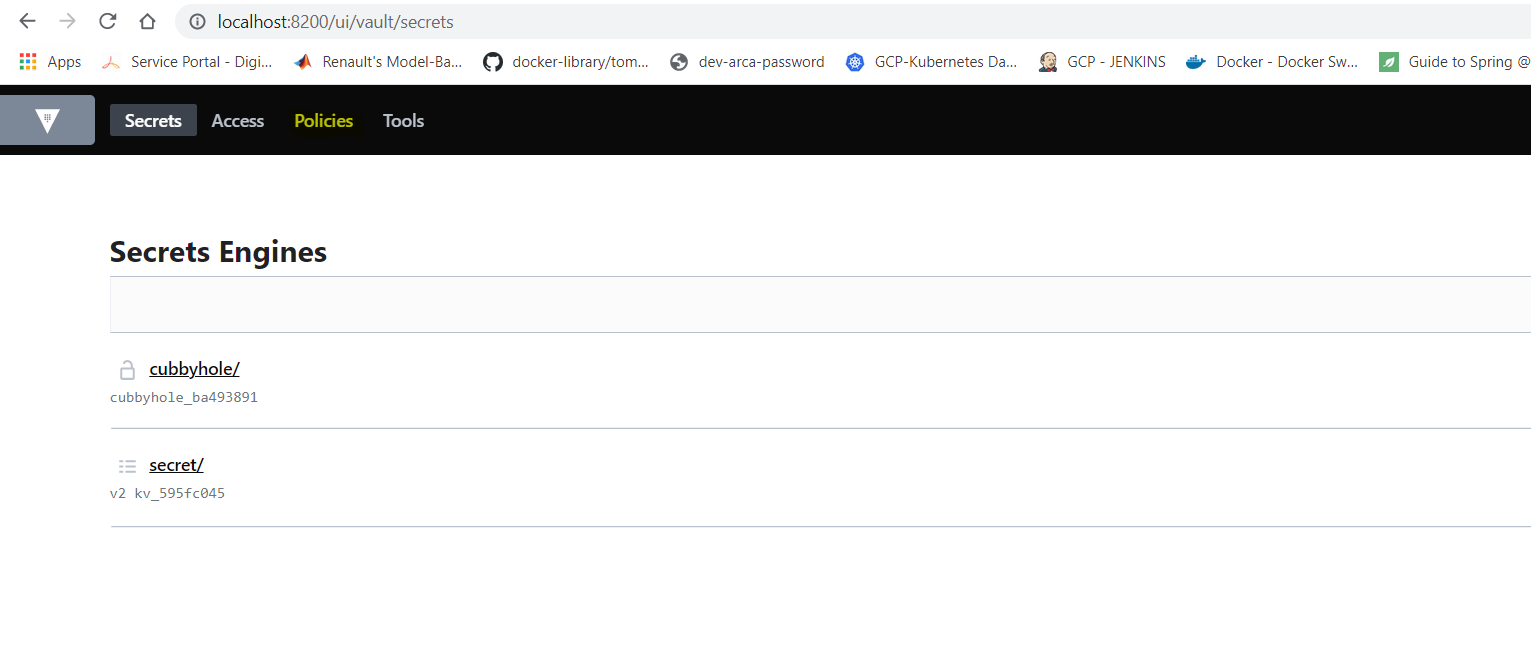




Follow the instruction given in this UI to create policy to attach to the role,

Login to UI using root token, Navigate to policy

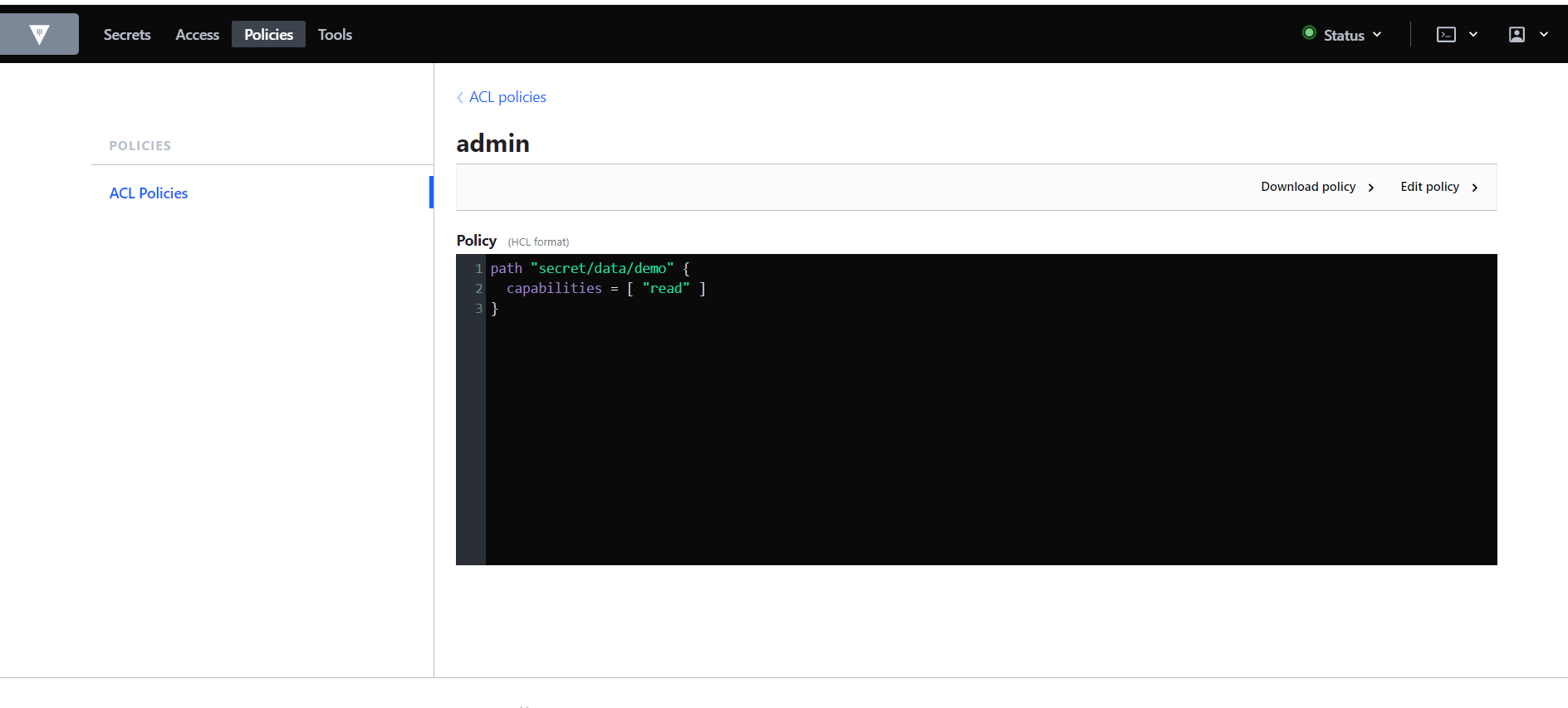
<https://learn.hashicorp.com/tutorials/vault/approle>





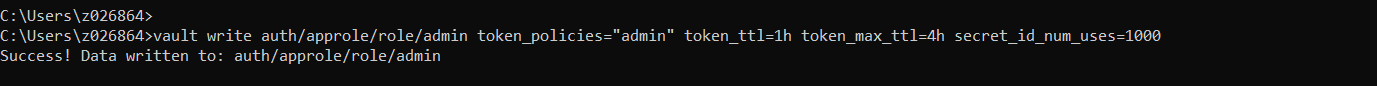
Read only access

**Note-** path will be default prefixed by **data**



Create admin role

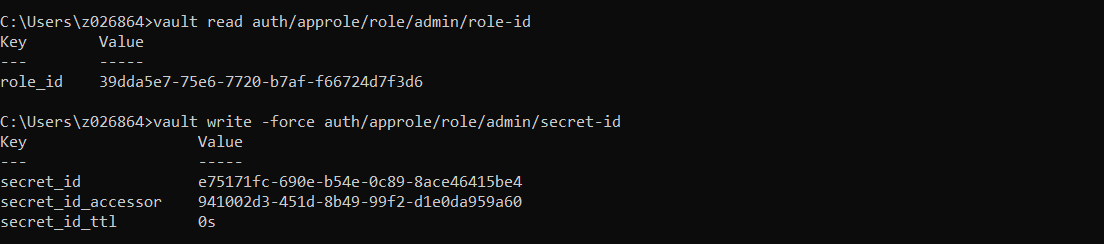
|  |
| --- |
| vault write auth/approle/role/admin token\_policies="admin" token\_ttl=1h token\_max\_ttl=4h secret\_id\_num\_uses=1000 |





To read role -id and secret-id

|  |
| --- |
| vault read auth/approle/role/admin/role-id  vault write -force auth/approle/role/admin/secret-id |

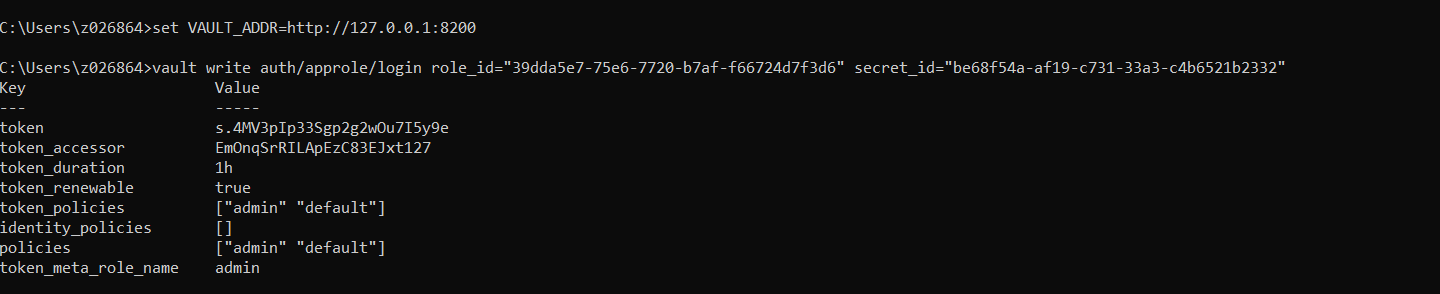




Open a new cmd prompt to check APPRole Auth method

Set the VAULT\_ADDR again for new command session

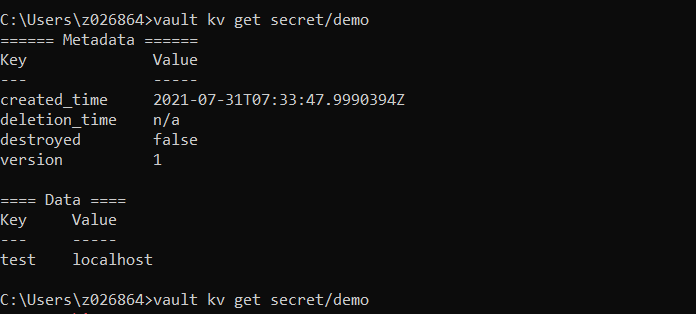
|  |
| --- |
| vault write auth/approle/login role\_id="39dda5e7-75e6-7720-b7af-f66724d7f3d6" secret\_id="be68f54a-af19-c731-33a3-c4b6521b2332" |





Now set the token for this cmd session from previous step token

Set VAULT\_TOKEN={token}





For Spring boot –

Reference-

<https://stackoverflow.com/questions/64994034/bootstrap-yml-configuration-not-processed-anymore-with-spring-cloud-2020-0/65009480#65009480>

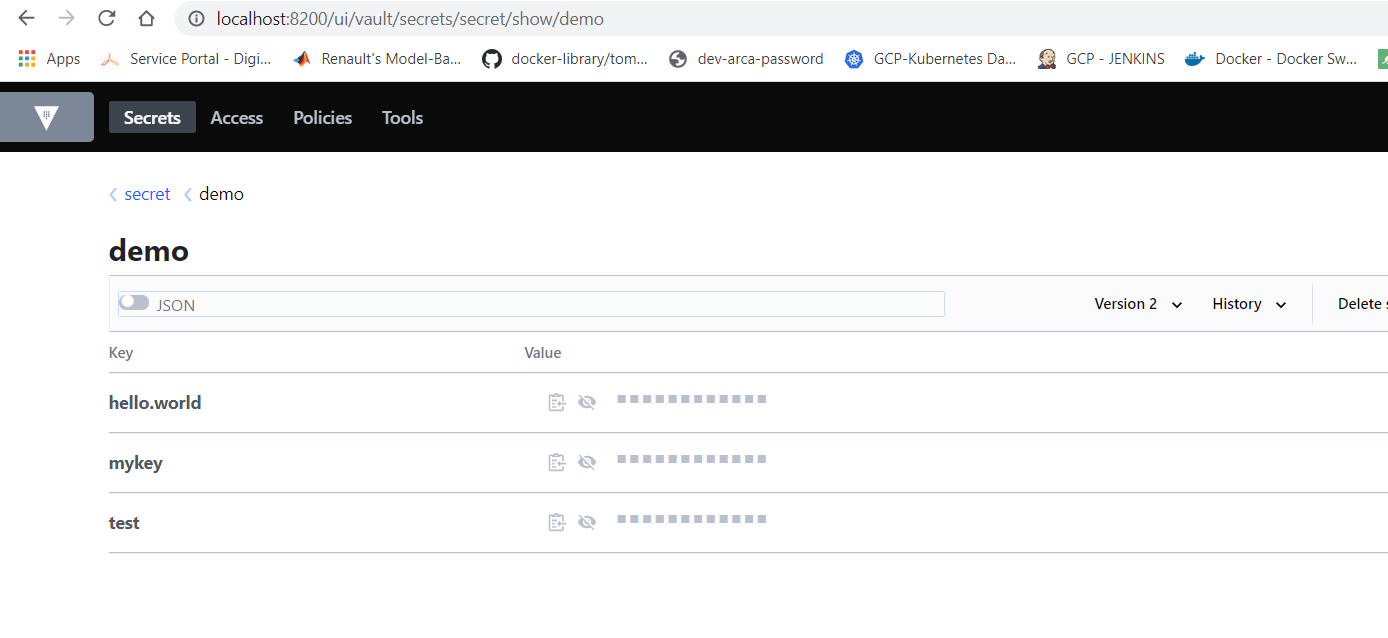
Two approaches –in that followed first which doesn’t use bootstrap.yml.

Properties file usage –

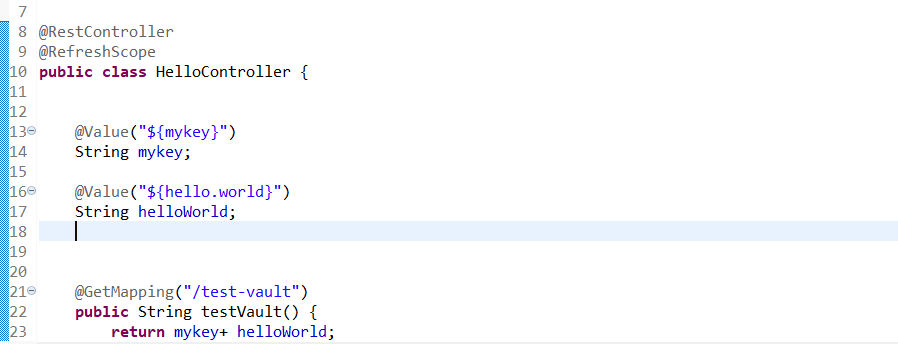
|  |
| --- |
| **spring:**  **cloud:**  **vault:**  **authentication:** APPROLE  **app-role:**  **role-id:** 39dda5e7-75e6-7720-b7af-f66724d7f3d6  **secret-id:** be68f54a-af19-c731-33a3-c4b6521b2332  **role:** admin  **app-role-path:** approle  **uri:** http://localhost:8200  **connection-timeout:** 5000  **read-timeout:** 15000  **config:**  **import:** vault://secret/demo  **mykey:** ${mykey}  **hello.world:** ${hello.world} |
|  |

Pom

|  |
| --- |
| <dependency>  <groupId>org.springframework.cloud</groupId>  <artifactId>spring-cloud-starter-vault-config</artifactId>  </dependency>  <dependency>  <groupId>org.springframework.boot</groupId>  <artifactId>spring-boot-devtools</artifactId>  <scope>runtime</scope>  <optional>true</optional>  </dependency> |







Actuator to restart –

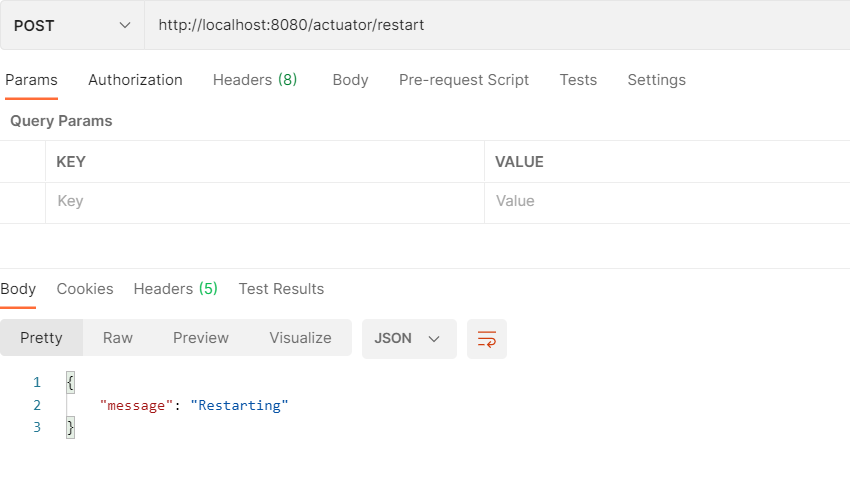
Dependency

|  |
| --- |
| <dependency>  <groupId>org.springframework.boot</groupId>  <artifactId>spring-boot-starter-actuator</artifactId>  </dependency> |

Properties

|  |
| --- |
| **management.endpoint.restart.enabled:** true  **management.endpoints.web.exposure.include:** restart,health |

Post request to server actuator endpoint will restart the server



If APPRole – pull method, we need to update the role to mention Don’t bind the secret-id with role-id by following command, but it also requires ip list to access the roles.

Reference - https://groups.google.com/g/vault-tool/c/D0yyMGPNkzM?pli=1

vault write auth/approle/role/admin token\_policies="admin" bind\_secret\_id=false secret\_id\_bound\_cidrs=127.0.0.1/24 token\_ttl=1h token\_max\_ttl=4h

