**GETTING SECRETS USING CURL COMMAND**

**REFERENCE LINK :**

[**https://www.vaultproject.io/api-docs/secret/aws**](https://www.vaultproject.io/api-docs/secret/aws)

**Tasks :**

* **Create 2 roles one with s3 access and the other with ec2 access in vault**
* **Connect using the curl command and generate secrets.**

**Step-1 : Enabling AWS secrets engine from UI**

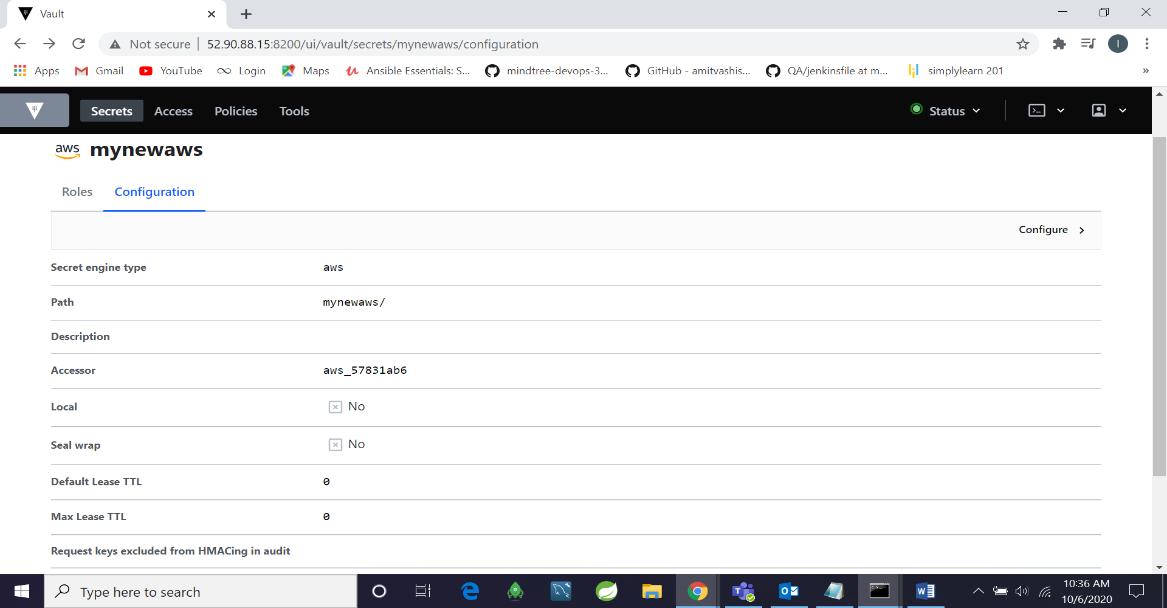
Goto the vault ui 🡺 click on **secrets 🡺** click on **enable new engine .**

Select **AWS** from the list 🡺 click on next.

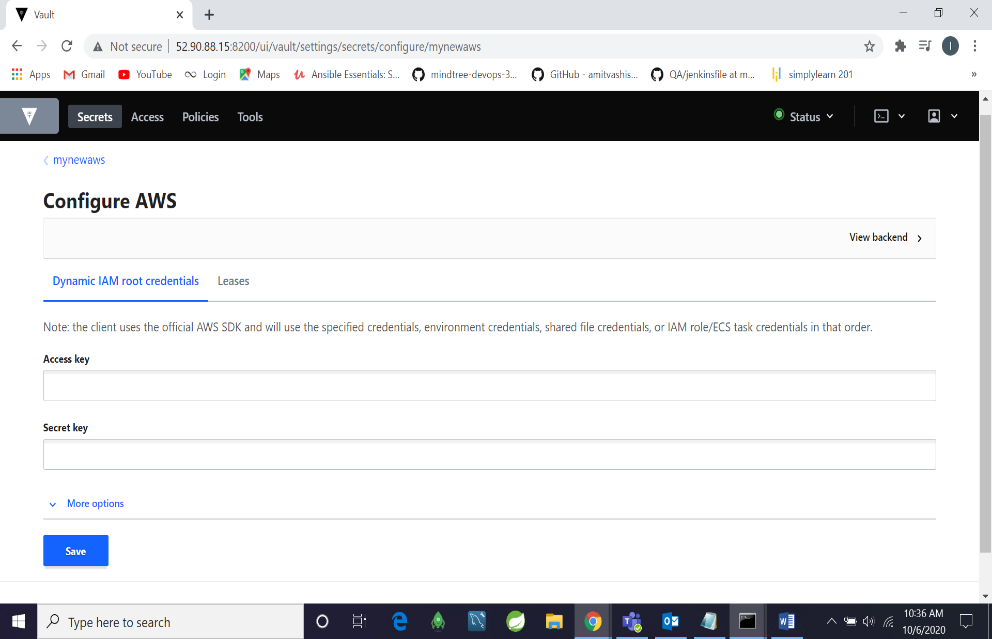
Give a **path**, this will be your path for the roles that you create.

Then click on **Enable engine**

You need to configure the lease time by clicking on configuration.



Click on configure and configure root credentials and also set expiry of your leases.



**Create role for ec2 & s3:**

Click on roles 🡺 click on create role 🡺 Give a role name, role arn or policy document.

ROLE NAME : ec2-role

Credential type : iam user

Policy document :

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": "ec2:\*",

"Resource": "\*"

}

]

}

Similarly, **create role for s3**:

ROLE NAME : s3user

Credential type : iam user

Policy document :

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": "s3:\*",

"Resource": "\*"

}

]

}

**CURL COMMANDS TO GENERATE AWS CREDENTIALS FOR THE ABOVE ROLES :**

Using the following command you can see the roles that are present in your path:

curl

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

--request LIST \

http://52.90.88.15:8200/v1/aws/roles

give your root token to connect to your vault then mention the path from which you want to list roles.

Using the following command we will be able to generate a user with the role that you mention in the url.

curl \

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

--request GET \

http://52.90.88.15:8200/v1/aws/creds/s3user

curl \

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

--request GET \

http://52.90.88.15:8200/v1/aws/creds/ec2-role

vault write database/config/postgresql \

plugin\_name=postgresql-database-plugin \

connection\_url="postgresql://root:rootpassword@localhost:5432/postgres?sslmode=disable" \

allowed\_roles=readonly \

username="root" \

password="rootpassword"