

John Oliver Dela Cruz
N01609389
Cloud Security
Vault

1. Update the package manager and install GPG and wget.

```
sudo apt update && sudo apt install gpg wget
```

2. Download the keyring.

```
wget -O- https://apt.releases.hashicorp.com/gpg | sudo gpg --dearmor -o  
/usr/share/keyrings/hashicorp-archive-keyring.gpg
```

```
john@j0:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$ wget -O- https://apt.releases.hashicorp.com/gpg | sudo gpg --dearmor -o /usr/share/keyrings/hashicorp-archive-keyring.gpg
--2024-04-08 21:34:54-- https://apt.releases.hashicorp.com/gpg
Resolving apt.releases.hashicorp.com (apt.releases.hashicorp.com)... 18.67.17.94, 18.67.17.183, 18.67.17.8, ...
Connecting to apt.releases.hashicorp.com (apt.releases.hashicorp.com)|18.67.17.94|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3986 (3.9K) [binary/octet-stream]
Saving to: 'STDOUT'

-
100%[=====>] 3.89K --.-KB/s in 0s

2024-04-08 21:34:54 (118 MB/s) - written to stdout [3986/3986]

john@j0:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$ ls
```

3. Verify the keyring.

```
gpg --no-default-keyring --keyring /usr/share/keyrings/hashicorp-archive-keyring.gpg --  
fingerprint
```

```
john@j0:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$ gpg --no-default-keyring --keyring /usr/share/keyrings/hashicorp-archive-keyring.gpg --fingerprint
gpg: directory '/home/john/.gnupg' created
gpg: '/home/john/.gnupg/trustdb.gpg': trustdb created
/usr/share/keyrings/hashicorp-archive-keyring.gpg
-----
pub  rsa4096 2023-01-10 [SC] [expires: 2028-01-09]
     798A EC65 4E5C 1542 8C8E 42EE AA16 FC8C A621 E781
uid  [ unknown] HashiCorp Security (HashiCorp Package Signing) <security+packaging@hashicorp.com>
sub  rsa4096 2023-01-10 [S] [expires: 2028-01-09]

john@j0:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$
```

4. Add the HashiCorp repository.

```
echo "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/hashicorp-  
archive-keyring.gpg] https://apt.releases.hashicorp.com $(lsb_release -cs) main" | sudo tee  
/etc/apt/sources.list.d/hashicorp.list
```

```
john@j0:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$ echo "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/hashicorp-archive-keyring.gpg] https://apt.releases.hashicorp.com $(lsb_release -cs) main" | sudo tee /etc/apt/sources.list.d/hashicorp.list
deb [arch=amd64 signed-by=/usr/share/keyrings/hashicorp-archive-keyring.gpg] https://apt.releases.hashicorp.com jammy main
john@j0:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$
```

5. Install Vault.

```
sudo apt update && sudo apt install vault
```

6. Verifying the Installation

```
vault
```

John Oliver Dela Cruz

N01609389

Cloud Security

Vault

```
john@Jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$ vault
Usage: vault <command> [args]

Common commands:
  read      Read data and retrieves secrets
  write     Write data, configuration, and secrets
  delete    Delete secrets and configuration
  list      List data or secrets
  login     Authenticate locally
  agent     Start a Vault agent
  server    Start a Vault server
  status    Print seal and HA status
  unwrap    Unwrap a wrapped secret

Other commands:
  audit      Interact with audit devices
  auth       Interact with auth methods
  debug      Runs the debug command
  events
  hcp
  kv          Interact with Vault's Key-Value storage
  lease       Interact with leases
  monitor    Stream log messages from a Vault server
  namespace  Interact with namespaces
  operator    Perform operator-specific tasks
  patch      Patch data, configuration, and secrets
  path-help  Retrieve API help for paths
  pki        Interact with Vault's PKI Secrets Engine
  plugin     Interact with Vault plugins and catalog
  policy     Interact with policies
  print      Prints runtime configurations
  proxy      Start a Vault Proxy
  secrets    Interact with secrets engines
  ssh        Initiate an SSH session
  token      Interact with tokens
  transform  Interact with Vault's Transform Secrets Engine
  transit    Interact with Vault's Transit Secrets Engine
  version-history Prints the version history of the target Vault server
john@Jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$
```

7. Start Vault: This is used to start the Vault server.

```
vault server -dev -dev-listen-address="0.0.0.0:8200"
```

John Oliver Dela Cruz
N01609389
Cloud Security
Vault

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS SEARCH ERROR CODE REFERENCE LOG
2024-04-08T21:57:14.239-0400 [INFO] core: successfully setup plugin runtime catalog
2024-04-08T21:57:14.239-0400 [INFO] core: successfully setup plugin catalog: plugin-directory=""
2024-04-08T21:57:14.239-0400 [INFO] core: no mounts; adding default mount table
2024-04-08T21:57:14.240-0400 [INFO] core: successfully mounted: type=cubbyhole version="v1.16.1+builtin.vault" path=cubbyhole/ namespace="ID: root. Path: "
2024-04-08T21:57:14.241-0400 [INFO] core: successfully mounted: type=system version="v1.16.1+builtin.vault" path=sys/ namespace="ID: root. Path: "
2024-04-08T21:57:14.241-0400 [INFO] core: successfully mounted: type=identity version="v1.16.1+builtin.vault" path=identity/ namespace="ID: root. Path: "
2024-04-08T21:57:14.243-0400 [INFO] core: successfully mounted: type=token version="v1.16.1+builtin.vault" path=token/ namespace="ID: root. Path: "
2024-04-08T21:57:14.243-0400 [INFO] rollback: Starting the rollback manager with 256 workers
2024-04-08T21:57:14.243-0400 [INFO] rollback: starting rollback manager
2024-04-08T21:57:14.243-0400 [INFO] core: restoring leases
2024-04-08T21:57:14.244-0400 [INFO] expiration: lease restore complete
2024-04-08T21:57:14.245-0400 [INFO] identity: entities restored
2024-04-08T21:57:14.245-0400 [INFO] identity: groups restored
2024-04-08T21:57:14.245-0400 [INFO] core: Recorded vault version: vault version=1.16.1 upgrade time="2024-04-09 01:57:14.2453299 +0000 UTC" build date=2024-04-03T12:35:53Z
2024-04-08T21:57:14.245-0400 [INFO] core: post-unseal setup complete
2024-04-08T21:57:14.246-0400 [INFO] core: root token generated
2024-04-08T21:57:14.246-0400 [INFO] core: pre-seal teardown starting
2024-04-08T21:57:14.246-0400 [INFO] rollback: stopping rollback manager
2024-04-08T21:57:14.246-0400 [INFO] core: pre-seal teardown complete
2024-04-08T21:57:14.246-0400 [INFO] core: cluster-listener.tcp: starting listener: listener_address=0.0.0.0:8201
2024-04-08T21:57:14.246-0400 [INFO] core: cluster-listener: serving cluster requests: cluster_listen_address=[::]:8201
2024-04-08T21:57:14.246-0400 [INFO] core: post-unseal setup starting
2024-04-08T21:57:14.246-0400 [INFO] core: loaded wrapping token key
2024-04-08T21:57:14.247-0400 [INFO] core: successfully setup plugin runtime catalog
2024-04-08T21:57:14.247-0400 [INFO] core: successfully setup plugin catalog: plugin-directory=""
2024-04-08T21:57:14.247-0400 [INFO] core: successfully mounted: type=system version="v1.16.1+builtin.vault" path=sys/ namespace="ID: root. Path: "
2024-04-08T21:57:14.247-0400 [INFO] core: successfully mounted: type=identity version="v1.16.1+builtin.vault" path=identity/ namespace="ID: root. Path: "
2024-04-08T21:57:14.247-0400 [INFO] core: successfully mounted: type=cubbyhole version="v1.16.1+builtin.vault" path=cubbyhole/ namespace="ID: root. Path: "
2024-04-08T21:57:14.248-0400 [INFO] core: successfully mounted: type=token version="v1.16.1+builtin.vault" path=token/ namespace="ID: root. Path: "
2024-04-08T21:57:14.248-0400 [INFO] rollback: Starting the rollback manager with 256 workers
2024-04-08T21:57:14.248-0400 [INFO] rollback: starting rollback manager
2024-04-08T21:57:14.248-0400 [INFO] core: restoring leases
2024-04-08T21:57:14.249-0400 [INFO] identity: entities restored
2024-04-08T21:57:14.249-0400 [INFO] identity: groups restored
2024-04-08T21:57:14.250-0400 [INFO] expiration: lease restore complete
2024-04-08T21:57:14.250-0400 [INFO] core: post-unseal setup complete
2024-04-08T21:57:14.250-0400 [INFO] core: vault is unsealed
2024-04-08T21:57:14.254-0400 [INFO] core: successful mount: namespace="" path=secret/ type=kv version="v0.17.0+builtin"
WARNING! dev mode is enabled! In this mode, Vault runs entirely in-memory
and starts unsealed with a single unseal key. The root token is already
authenticated to the CLI, so you can immediately begin using Vault.

You may need to set the following environment variables:

$ export VAULT_ADDR='http://0.0.0.0:8200'

The unseal key and root token are displayed below in case you want to
seal/unseal the Vault or re-authenticate.

Unseal Key: F
Root Token: h

Development mode should NOT be used in production installations!
```

8. Enable kv Secret Engine and Create Vault

vault secrets enable -path=secret kv

```
john@jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$ vault secrets list
Path      Type      Accessor      Description
----      -
cubbyhole/ cubbyhole  cubbyhole_dd9bb1aa  per-token private secret storage
identity/  identity  identity_79bba58d    identity store
secret/    kv         kv_2e970f62         key/value secret storage
sys/       system    system_2be68075      system endpoints used for control, policy and debugging
john@jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$ vault kv put secret/test-secret Username=credentials
===== Secret Path =====
secret/data/test-secret

===== Metadata =====
Key      Value
---      -
created_time  2024-04-09T02:03:15.488444476Z
custom_metadata  <nil>
deletion_time  n/a
destroyed      false
version        1
john@jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$
```

John Oliver Dela Cruz
N01609389
Cloud Security
Vault
9. Enable AppRole Authentication

```
vault auth enable approle
```

```
john@Jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$ vault auth enable approle
Success! Enabled approle auth method at: approle/
john@Jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$
```

10. Create a Policy

```
vault policy write terraform - <<EOF

path "secret/data/*" {

  capabilities = ["create", "read", "update", "delete", "list"]

}

EOF
```

```
john@Jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$ vault policy write terraform - <<EOF
path "secret/data/*" {
  capabilities = ["create", "read", "update", "delete", "list"]
}
EOF
Success! Uploaded policy: terraform
john@Jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$
```

11. Create an AppRole

```
vault write auth/approle/role/terraform \

secret_id_ttl=10m \

token_num_uses=10 \

token_ttl=20m \

token_max_ttl=30m \

secret_id_num_uses=40 \

token_policies=terraform
```

```
john@Jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$ vault write auth/approle/role/terraform \
secret_id_ttl=10m \
token_num_uses=10 \
token_ttl=20m \
token_max_ttl=30m \
secret_id_num_uses=40 \
token_policies=terraform
Success! Data written to: auth/approle/role/terraform
john@Jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$
```

John Oliver Dela Cruz
N01609389
Cloud Security
Vault
12. Generate Role ID

`vault read auth/approle/role/terraform/role-id`

```
john@Jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$ vault read auth/approle/role/terraform/role-id
Key      Value
---      -
role_id  9[REDACTED]
```

13. Generate Secret ID

`vault write -f auth/approle/role/terraform/secret-id`

```
john@Jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$ vault write -f auth/approle/role/terraform/secret-id
Key      Value
---      -
secret_id      c[REDACTED]
secret_id_accessor  c[REDACTED]
secret_id_num_uses  40
secret_id_ttl       10m
```

John Oliver Dela Cruz

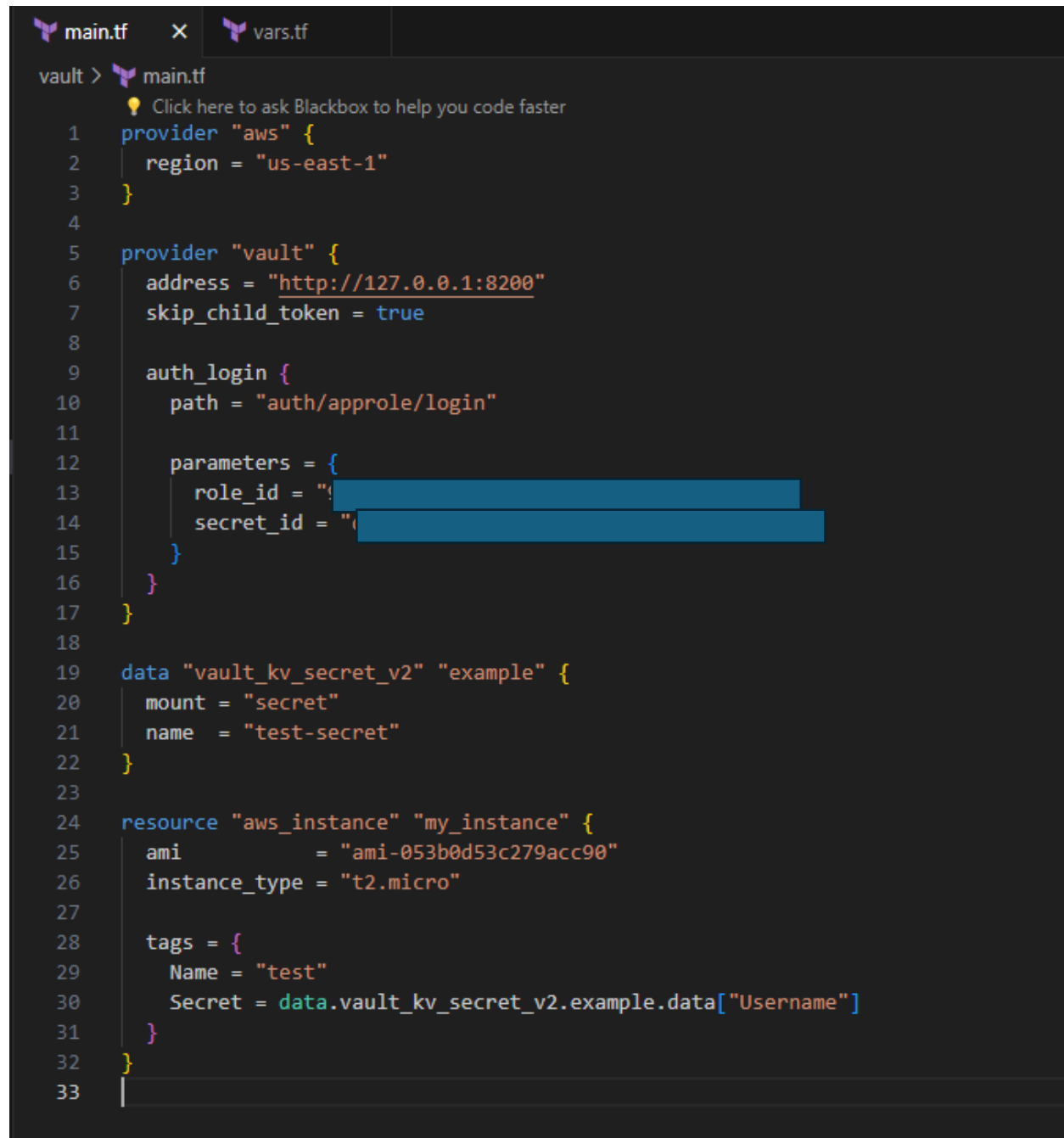
N01609389

Cloud Security

Vault

14. Terraform Configuration files:

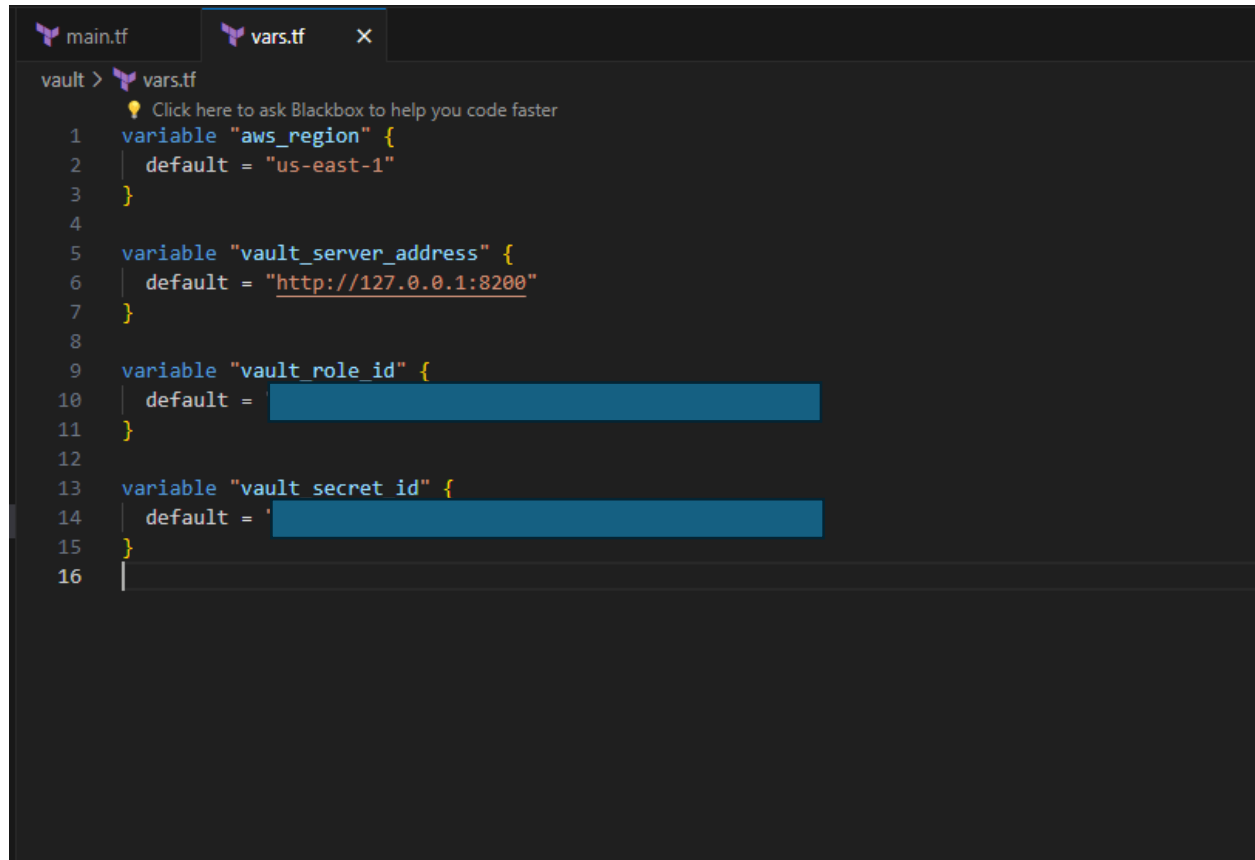
main.tf



```
main.tf X vars.tf
vault > main.tf
  Click here to ask Blackbox to help you code faster
1 provider "aws" {
2   region = "us-east-1"
3 }
4
5 provider "vault" {
6   address = "http://127.0.0.1:8200"
7   skip_child_token = true
8
9   auth_login {
10    path = "auth/approle/login"
11
12    parameters = {
13     role_id = "XXXXXXXXXXXXXXXXXXXX"
14     secret_id = "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
15    }
16  }
17 }
18
19 data "vault_kv_secret_v2" "example" {
20   mount = "secret"
21   name = "test-secret"
22 }
23
24 resource "aws_instance" "my_instance" {
25   ami = "ami-053b0d53c279acc90"
26   instance_type = "t2.micro"
27
28   tags = {
29     Name = "test"
30     Secret = data.vault_kv_secret_v2.example.data["Username"]
31   }
32 }
33
```

John Oliver Dela Cruz
N01609389
Cloud Security
Vault

Vars.tf



```
main.tf  vars.tf  X
vault > vars.tf
  Click here to ask Blackbox to help you code faster
1  variable "aws_region" {
2    | default = "us-east-1"
3  }
4
5  variable "vault_server_address" {
6    | default = "http://127.0.0.1:8200"
7  }
8
9  variable "vault_role_id" {
10   | default = 
11 }
12
13 variable "vault_secret_id" {
14   | default = '
15 }
16 |
```

John Oliver Dela Cruz
N01609389
Cloud Security
Vault

15. terraform init

```
john@Jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$ terraform init
```

Initializing the backend...

Initializing provider plugins...

- Finding latest version of hashicorp/vault...
- Finding latest version of hashicorp/aws...
- Installing hashicorp/vault v4.2.0...
- Installed hashicorp/vault v4.2.0 (signed by HashiCorp)
- Installing hashicorp/aws v5.44.0...
- Installed hashicorp/aws v5.44.0 (signed by HashiCorp)

Terraform has created a lock file `.terraform.lock.hcl` to record the provider selections it made above. Include this file in your version control repository so that Terraform can guarantee to make the same selections by default when you run "terraform init" in the future.

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see any changes that are required for your infrastructure. All Terraform commands should now work.

If you ever set or change modules or backend configuration for Terraform, rerun this command to reinitialize your working directory. If you forget, other commands will detect it and remind you to do so if necessary.

```
john@Jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$
```


16. terraform apply

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS  SEARCH ERROR  CODE REFERENCE LOG

+ id = (known after apply)
+ instance_initiated_shutdown_behavior = (known after apply)
+ instance_lifecycle = (known after apply)
+ instance_state = (known after apply)
+ instance_type = "t2.micro"
+ ipv6_address_count = (known after apply)
+ ipv6_addresses = (known after apply)
+ key_name = (known after apply)
+ monitoring = (known after apply)
+ outpost_arn = (known after apply)
+ password_data = (known after apply)
+ placement_group = (known after apply)
+ placement_partition_number = (known after apply)
+ primary_network_interface_id = (known after apply)
+ private_dns = (known after apply)
+ private_ip = (known after apply)
+ public_dns = (known after apply)
+ public_ip = (known after apply)
+ secondary_private_ips = (known after apply)
+ security_groups = (known after apply)
+ source_dest_check = true
+ spot_instance_request_id = (known after apply)
+ subnet_id = (known after apply)
+ tags = {
  + "Name" = "test"
  + "Secret" = (sensitive value)
}
+ tags_all = {
  + "Name" = "test"
  + "Secret" = "credentials"
}
+ tenancy = (known after apply)
+ user_data = (known after apply)
+ user_data_base64 = (known after apply)
+ user_data_replace_on_change = false
+ vpc_security_group_ids = (known after apply)
}

Plan: 1 to add, 0 to change, 0 to destroy.

Do you want to perform these actions?
Terraform will perform the actions described above.
Only 'yes' will be accepted to approve.

Enter a value: yes

aws_instance.my_instance: Creating...
aws_instance.my_instance: Still creating... [10s elapsed]
aws_instance.my_instance: Still creating... [20s elapsed]
aws_instance.my_instance: Still creating... [30s elapsed]
aws_instance.my_instance: Creation complete after 33s [id=i-075459dd6a62f4c0c]

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.
john@Jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$
```

John Oliver Dela Cruz
N01609389
Cloud Security
Vault

17. terraform state list | nl

```
john@Jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$ terraform state list | nl
1 data.vault_kv_secret_v2.example
2 aws_instance.my_instance
john@Jo:/mnt/c/Users/jodel/OneDrive/Documents/Acads/Acads/Winter-2024/Cloud Security/Lab/vault$
```

AWS Console Management:

