Objectives:

- Use a vault to manage secrets
- Access secrets with a Chef cookboook

Use a vault CLI to set a hashed password in the vault

1. Make sure your Vault is running (see the "Setting up a Hashicorp Vault Server" lab if you need help with this)
2. In a second terminal window (so as not to shut down your Vault server) create a hashed password by executing:

   $ openssl passwd -1 -salt $(openssl rand -base64 6) usevaulthashpass

   Note: that is a "-1" flag (using the numeric for 'one')

```
~ $openssl passwd -1 -salt $(openssl rand -base64 6) usevaulthashpass
$1$n1v+Va+1$PLroN1OxORl1mrfWy49tO. <HASH_KEY>
```

3. Use the vault command in the CLI to save a hashed password to the vault:

```
$vault kv put secret/password password='<HASH_KEY>'
```

Expected output:

```
Key              Value
---              -----
created_time     2021-04-22T19:01:39.690771842Z
deletion_time    n/a
destroyed        false
version          1
```

NOTE: if the expected output is displayed, **skip to step 3**, otherwise: if the vault command **fails**, export the vault token created while starting the vault server in dev mode in lab 10:

```
Root Token: s.Oof32bYNKaZC8SUa1UmKlWof
```

Execute: $ export VAULT_TOKEN="<Root Token>"

Verifying the uploaded hashed password using the vault CLI and the Web UI:

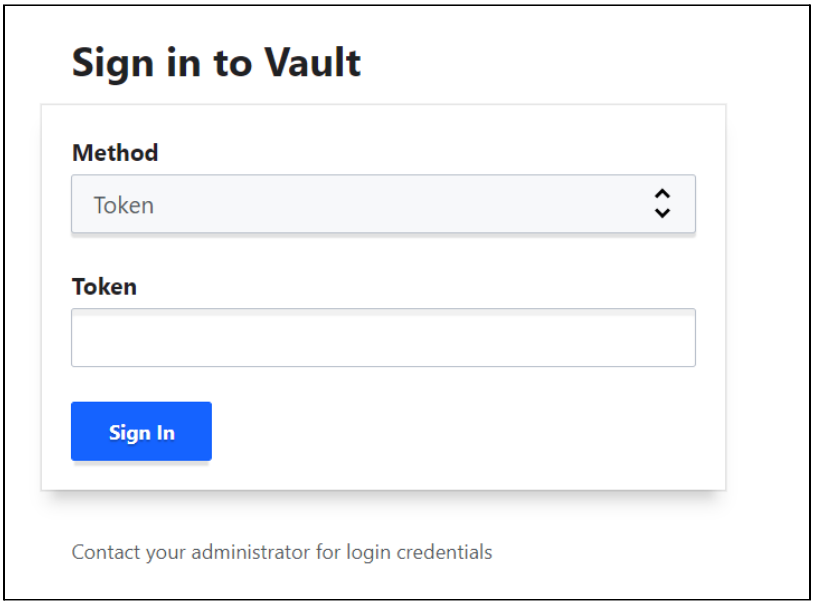
4. Using CLI, execute: `$vault kv get secret/password`

```
~ $vault kv get secret/password
====== Metadata ======
Key              Value
---              -----
created_time     2021-04-22T19:01:39.690771842Z
deletion_time    n/a
destroyed        false
version          1

====== Data ======
Key         Value
---         -----
password    $1$n1v+Va+1$PLroN1OxORl1mrfWy49tO.
```

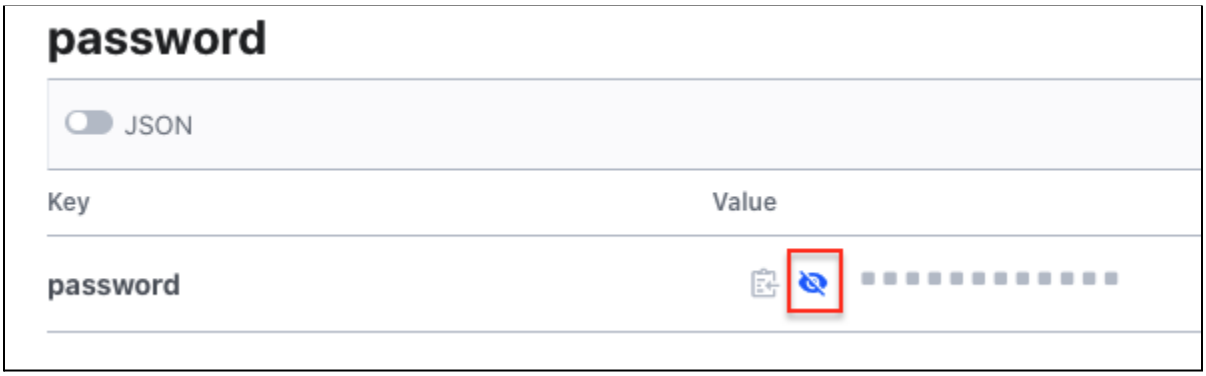
5. Using the web GUI, open a browser window to the IP address:

   http://<VM_PUBLIC_IP>:8200



6. Enter the vault root token to sign in. Click on secret/ :

7. Click on password, then password and finally click on eye button to view the hashed password :



8. Access the hashed password from the recipe by updating **users/recipes/default.rb** file as depicted below:

```
# your_name_password = data_bag_item('passwords', 'your_name')

chef_gem 'vault' do
  compile_time true if respond_to?(:compile_time)
end

require 'vault'

Vault.configure do |config|
  # The address of the Vault server, as read as ENV["VAULT_ADDR"]
  config.address = 'http://<VM_IPADDRESS>:8200'

  # The token to authenticate with Vault, also read as ENV["VAULT_TOKEN"]
  config.token = '<VAULT_ROOT_TOKEN>'
end

creds = Vault.kv('secret').read('password')

user 'your_name' do
  comment 'first and last name'
  uid 2000
  home '/home/your_name'
  shell '/bin/bash'
  manage_home true
#  password your_name_password['password']
  password creds.data[:password]
end
```

This snippet of code contains:

- **Chef_gem:** a Chef resource to download a Ruby gem.
- **Require vault:** this recipe requires vault dependency.
- **Vault.configure:** configures the vault to access secrets.
- **config.token** has the value of the root token of the vault server which should still be running in a separate terminal tab if needed for reference.
- **Vault.kv("secret").read("password")** is used to read credentials.
- **Creds.data[:password]** is used to filter a hashed password in a vault server.

NOTE: It's not good practice to use the vault server root token in a production server.

Verify cookbook execution where values are fetched from the vault using kitchen commands:

9. From the 'users' cookbook, destroy, converge and log into the **Centos-7** kitchen

10. **Execute `# su your_name`, then execute `$ su your_name`**

    Enter '*usevaulthashpass*' when prompted for a password:

```
[root@dokken /]# su your_name
[your_name@dokken /]$ su your_name
Password:
[your_name@dokken /]$
```

Using an incorrect password:

11. Enter an incorrect password when prompted after executing:

```
$ su your_name
```

```
[your_name@dokken /]$ su your_name
Password:
su: Authentication failure
```

12. Exit out of the kitchen, back to the workstation

Notify your instructor that you are done with the lab

END OF LAB