6. Log in to the HashiCorp Vault server and verify its status.

   Prepare the environment variables required for logging in as root:

   ```
   vault login s.vTvXeo3tPEYehfcd9WH7oUKz
   ```

   For the token value in that command, substitute the content of the root token obtained previously during Vault initialization.

   Verify the Vault server status:

   ```
   vault status
   ```

   The output should contain these lines (among others):

   ```
   ...
   Initialized     true
   Sealed          false
   ...
   ```

7. Set up HashiCorp Vault authentication and storage.

   > **Note**
   >
   > The operations described in this step are needed only the first time the Vault instance is run. They need not be repeated afterward.

   Enable the AppRole authentication method and verify that it is in the authentication method list:

   ```
   vault auth enable approle
   vault auth list
   ```

   Enable the Vault KeyValue storage engine:

   ```
   vault secrets enable -version=1 kv
   ```

   Create and set up a role for use with the `keyring_hashicorp` plugin (enter the command on a single line):

   ```
   vault write auth/approle/role/mysql token_num_uses=0
     token_ttl=20m token_max_ttl=30m secret_id_num_uses=0
   ```

8. Add an AppRole security policy.

   > **Note**
   >
   > The operations described in this step are needed only the first time the Vault instance is run. They need not be repeated afterward.

   Prepare a policy that to permit the previously created role to access appropriate secrets. Create a new file named `mysql.hcl` with the following content:

   ```
   path "kv/mysql/*" {
     capabilities = ["create", "read", "update", "delete", "list"]
   ```