Section 5, Quiz 1

Question 1: True or False? Vault auth methods are responsible for validating a user's identity and associating policies for authorization?

- True
- False

Answer: A. True. Correct, this is the core function of a Vault auth method.

Question 2: Which of the following are valid auth methods that can be enabled in Vault?

- OIDC
- Azure AD
- SAML 2.0
- MySQL

Answer: Yes, this is a valid auth method - https://www.vaultproject.io/docs/auth/jwt#oidc-authentication

Question 3: When using any auth method beyond the token, what is the result of using an auth method?

- obtaining a Vault token
- validating your credentials
- to get access to a Vault policy
- to generate new dynamic credentials

Answer: A. Yes, this is the goal, or result, of using an auth method. Remember that all subsequent requests to Vault will use the token for authentication

Question 4: Which of the following auth methods are generally associated with machine-to-machine authentication?

- AppRole
- OIDC
- LDAP
- UserPass

Answer: A. Yes, AppRole is frequently the primary auth method used for machine to machine authentication - https://www.vaultproject.io/docs/auth/approle

Question 5: You are using Terraform in your environment to deploy infrastructure to your public cloud platform. Terraform is being executed on a server running in AWS. The Security team has mandated that any credentials for Terraform must be short-lived and rotated often. What auth method should you use to authenticate to Vault and satisfy these requirements?

- AWS auth method
- UserPass
- AppRole
- LDAP

Answer: A. Yes. In this case, the credentials are generated only when Terraform needs them and are automatically revoked after the lease.

Section 6, Quiz 2:

Question 1: Every Vault deployment will have two default policies that are created automatically. What are these two policies?

- The anonymouspolicy and the default policy
- The adminpolicy and the userpolicy
- The primary policy and the secondarypolicy
- The root policy and the default policy

Answer: D. Yes, this is the correct answer.

Question 2: Vault policies contain multiple parts, including the path and capabilities. What are the valid capabilities that can be used in a policy?

- read, write, delete, list, sudo, update
- read, create, delete, list, sudo, update, deny
- get, write, remove, list, sudo, update, deny
- delete, list, update, root, default, deny create, sudo

Answer: B. Yes, these are the only valid capabilities in Vault. Nice job!

Question 3: You've been provided a Vault token that is attached to the following policy. Select the action below that will be permitted.

```
1.  path "kv/data/apps/jenkins" {
2.  capabilities = ["read","update","delete"]
3.  }
4.  path "sys/policies/*" {
5.  capabilities = ["create","update","list","delete"]
6.  }
7.  path "aws/creds/web-app" {
8.  capabilities = ["read"]
9.  }
```

- List secrets stored at kv/data/apps/jenkins
- Modify an existing Vault policy

- Store a new secret stored at kv/data/apps/jenkins
- List the roles for the AWS secrets engine mounted at aws/

Answer: Yes, this is correct because the capability update has been permitted for all policies (sys/policies/*)

Question 4: Given the following policy, select the action that would NOT be permitted.

```
path "kv/apps/webapp/*" {
capabilities = ["read"]
}
path "secret/apps/database/prod-db" {
capabilities = ["read", "create", "update", "delete", "list"]
}
path "kv/data/teams/+/database/db-*" {
capabilities = ["read", "list"]
}
```

- Read a secret at the path kv/data/teams/cloud/database/db2
- Store a new secret at secret/apps/database/prod-db
- Read a secret at kv/apps/webapp/ecommerce/production
- List the secrets stored at kv/data/teams/developers/database/db-001

Answer: This isn't permitted because the wildcard at the end requires that the ending segment be db-. The path selected does not include the dash ("-") character.

Question 5: You have a new team member on the Vault operations team. Their first task is to rotate the encryption key in Vault as part of the organization's security policy. However, when they log in, they get an access denied error when attempting to rotate the key. The policy being used is below. Why can't the user rotate the encryption key?

```
path "auth/*" {
 capabilities = ["create", "read", "update", "delete", "list"]
}
# Rotate encryption key
path "sys/rotate" {
 capabilities = ["read", "update"]
}
```

- The policy requires sudo privileges since it is a root-protected path
- The policy doesn't include create privileges so a new encryption key can't be created.
- The policy should include sys/rotate/<name of key> as part of the path
- The encryption key has a minimum TTL, therefore the key cannot be rotated until that time expires.

Answer: Yes, nice job. Rotating the encryption requires sudo or root access to the path sys/rotate.

Section 7, Quiz 3

Question 1: What is the difference between the TTL and the Max TTL?

- the TTL defines when the token will expire and be revoked
- the max TTL defines the timeframe for which a token cannot be used
- the TTL defines when another token will be generated
- they are essentially the same

Answer: A. Correct answer.

Question 2: True or False? To prepare for day-to-day operations, the root token should be safely saved outside of Vault in order to administer Vault.

- True
- False

Answer: B. False. Correct, for day-to-day operations, the root token should be deleted after configuring other auth methods which will be used by admins and Vault clients.

Question 3: Which of the following best describes a token accessor?

- a value that acts as a reference to a token that can be used to perform limited actions against the token
- a token used for Consul to access Vault auth methods
- describes the value associated with the tokens TTL
- a value that describes which clients have access to the attached token

Answer: A. Correct, nice job

Question 4: What of the following feature is true about batch tokens in Vault?

- batch tokens are not persisted (written) to storage
- batch tokens can create child tokens
- batch tokens are written to storage

Answer: A. Correct, batch tokens are NOT written to storage

Question 5: Sara uses the Vault command-line interface (CLI) to perform various administrative tasks on the production Vault cluster. However, Sara is receiving permission denied errors when

attempting to make changes. She needs to figure out what policies are attached to her token so she can view the policy and determine what permissions need to be added.

What CLI command can Sara run on the Vault node to determine what policies are attached to the current token?

- vault token lookup
- vault operator diagnose
- vault policy list
- vault token capabilities

Answer: A. Correct answer. This was discussed in lecture 80, Introduction to Vault Tokens.