VAULT-ASSOCIATE Q&As

HashiCorp Certified: Vault Associate (002)

Pass HashiCorp VAULT-ASSOCIATE Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/vault-associate.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HashiCorp Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following statements describe the secrets engine in Vault? Choose three correct answers.

A. Some secrets engines simply store and read data

B. Once enabled, you cannot disable the secrets engine

C. You can build your own custom secrets engine

D. Each secrets engine is isolated to its path

E. A secrets engine cannot be enabled at multiple paths

Correct Answer: ACD

Secrets engines are components that store, generate, or encrypt data in Vault. They are enabled at a specific path in Vault and have their own API and configuration. Some of the statements that describe the secrets engines in Vault are:

Some secrets engines simply store and read data, such as the key/value secrets engine, which acts like an encrypted Redis or Memcached. Other secrets engines perform more complex operations, such as generating dynamic credentials,

encrypting data, issuing certificates, etc1.

You can build your own custom secrets engine by using the plugin system, which allows you to write and run your own secrets engine as a separate process that communicates with Vault over gRPC. You can also use the SDK to create your

own secrets engine in Go and compile it into Vault2. Each secrets engine is isolated to its path, which means that the secrets engine cannot access or interact with other secrets engines or data outside its path. The path where the secrets

engine is enabled can be customized and can have multiple segments. For example, you can enable the AWS secrets engine at aws/ or aws/prod/ or aws/dev/3.

The statements that are not true about the secrets engines in Vault are:

You can disable an existing secrets engine by using the vault secrets disable command or the sys/mounts API endpoint. When a secrets engine is disabled, all of its secrets are revoked and all of its data is deleted from the storage backend4.

A secrets engine can be enabled at multiple paths, with a few exceptions, such as the system and identity secrets engines. Each secrets engine enabled at a different path is independent and isolated from others. For example, you can

enable the KV secrets engine at kv/ and secret/ and they will not share any data3.

References

: 1(https://developer.hashicorp.com/vault/docs/secrets), 2(https://developer.hashicorp.com/ vault/docs/secrets), 3(https://developer.hashicorp.com/vault/docs/secrets), 4(https://develo per.hashicorp.com/vault/docs/secrets)

QUESTION 2

Your organization has an initiative to reduce and ultimately remove the use of long lived

A. 509 certificates. Which secrets engine will best support this use case?

B. PKI

C. Key/Value secrets engine version 2, with TTL defined

D. Cloud KMS

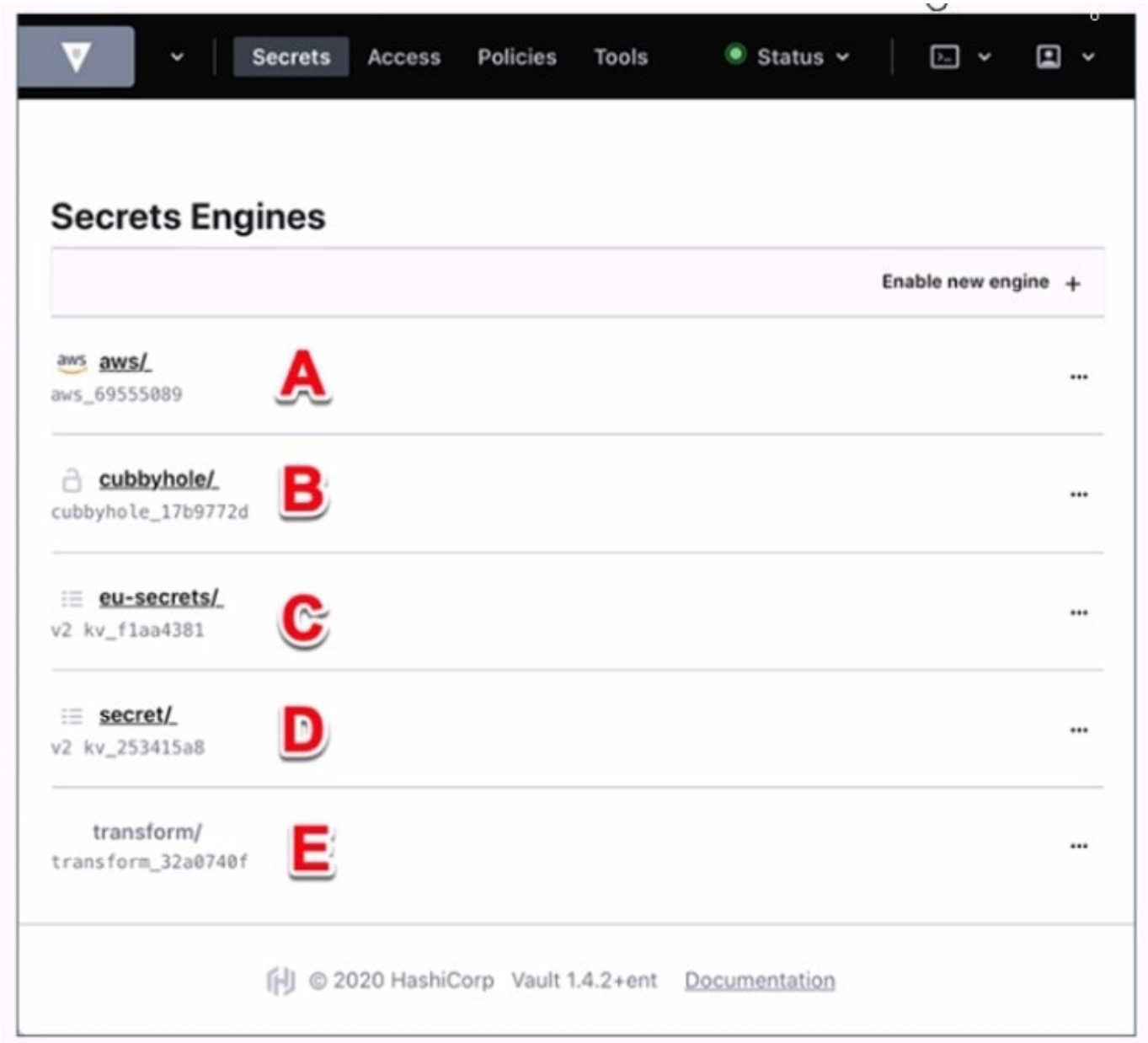
E. Transit

Correct Answer: A

The PKI secrets engine is designed to support the use case of reducing and ultimately removing the use of long lived X.509 certificates. The PKI secrets engine can generate dynamic X.509 certificates on demand, with short time-to-live (TTL) and automatic revocation. This eliminates the need for manual processes of generating, signing, and rotating certificates, and reduces the risk of certificate compromise or misuse. The PKI secrets engine can also act as a certificate authority (CA) or an intermediate CA, and can integrate with external CAs or CRLs. The PKI secrets engine can issue certificates for various purposes, such as TLS, SSH, code signing, email encryption, etc. References: https://developer.hashicorp.com/vault/docs/secrets/pki1, https://developer.hashicorp.com/vault/tutorials/getting-started/getting-started-dynamic- secrets

QUESTION 3

Use this screenshot to answer the question below: Where on this page would you click to view a secret located at secret/my-secret?



A. A

B. B

C. C

D. D

E. E

Correct Answer: C

In the HashiCorp Vault UI, secrets are organized in a tree-like structure. To view a secret located at secret/my-secret, you would click on the "secret/" folder in the tree, then clickon the "my-secret" file. In this screenshot, the "secret/" folder is

located at option C. This folder contains the secrets that are stored in the key/value secrets engine, which is the default

secrets engine in Vault. The key/value secrets engine allows you to store arbitrary secrets as key/value pairs. The key is

the path of the secret, and the value is the data of the secret. For example, the secret located at secret/my-secret has a key of "my- secret" and a value of whatever data you stored there.

References:

[KV - Secrets Engines | Vault | HashiCorp Developer]

QUESTION 4

The vault lease renew command increments the lease time from:

A. The current time

B. The end of the lease

Correct Answer: A

The vault lease renew command increments the lease time from the current time, not the end of the lease. This means that the user can request a specific amount of time they want remaining on the lease, termed the increment. This is not an increment at the end of the current TTL; it is an increment from the current time. For example, vault lease renew -increment=3600 my-lease-id would request that the TTL of the lease be adjusted to 1 hour (3600 seconds) from now. Having the increment be rooted at the current time instead of the end of the lease makes it easy for users to reduce the length of leases if they don\\'t actually need credentials for the full possible lease period, allowing those credentials to expire sooner and resources to be cleaned up earlier. The requested increment is completely advisory. The backend in charge of the secret can choose to completely ignore it1. References: Lease, Renew, and Revoke | Vault | HashiCorp Developer

QUESTION 5

Which Vault secret engine may be used to build your own internal certificate authority?

A. Transit

B. PKI

C. PostgreSQL D. Generic

Correct Answer: B

The Vault secret engine that can be used to build your own internal certificate authority is the PKI secret engine. The PKI secret engine generates dynamic X.509 certificates on-demand, without requiring manual processes of generating private keys and CSRs, submitting to a CA, and waiting for verification and signing. The PKI secret engine can act as a root CA or an intermediate CA, and can issue certificates for various purposes, such as TLS, code signing, email encryption, etc. The PKI secret engine can also manage the certificate lifecycle, such as rotation, revocation, renewal, and CRL generation. The PKI secret engine can also integrate with external CAs, such as Venafi or Entrust, to delegate the certificate issuance and management. References: PKI - Secrets Engines | Vault | HashiCorp Developer, Build Your Own Certificate Authority (CA) | Vault - HashiCorp Learn