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

To make an authenticated request via the Vault HTTP API, which header would you use?

A. The X-Vault-Token HTTP Header

B. The x-Vault-Request HTTP Header

C. The Content-Type HTTP Header

D. The X-Vault-Namespace HTTP Header

Correct Answer: A

To make an authenticated request via the Vault HTTP API, you need to use the X-Vault-Token HTTP Header or the Authorization HTTP Header using the Bearer scheme. The token is a string that represents your identity and permissions in Vault. You can obtain a token by using an authentication method, such as userpass, approle, aws, etc. The token can also be a root token, which has unlimited access to Vault, or a wrapped token, which is a response

wrapping token that can be used to unwrap the actual token. The token must be sent with every request to Vault that requires authentication, except for the unauthenticated endpoints, such as sys/init, sys/seal-status, sys/unseal, etc. The

token is used by Vault to verify your identity and enforce the policies that grant or deny access to various paths and operations. References:

https://developer.hashicorp.com/vault/api-docs3,

https://developer.hashicorp.com/vault/docs/concepts/tokens4,
https://developer.hashicorp.com/vault/docs/concepts/auth5

QUESTION 2

When an auth method is disabled all users authenticated via that method lose access.

A. True

B. False

Correct Answer: A

The statement is true. When an auth method is disabled, all users authenticated via that method lose access. This is because the tokens issued by the auth method are automatically revoked when the auth method is disabled. This prevents the users from performing any operation in Vault using the revoked tokens. To regain access, the users have to authenticate again using a different auth method that is enabled and has the appropriate policies attached. References: Auth Methods | Vault | HashiCorp Developer, auth disable - Command | Vault | HashiCorp Developer

QUESTION 3

Which of the following is a machine-oriented Vault authentication backend?

A. Okta

B. AppRole

C. Transit

D. GitHub

Correct Answer: B

AppRole is a machine-oriented authentication method that allows machines or applications to authenticate with Vault using a role ID and a secret ID. The role ID is aunique identifier for the application, and the secret ID is a single-use credential that can be delivered to the application securely. AppRole is designed to provide secure introduction of machines and applications to Vault, and to support the principle of least privilege by allowing fine-grained access control policies to be attached to each role1. Okta, GitHub, and Transit are not machine-oriented authentication methods. Okta and GitHub are user-oriented authentication methods that allow users to authenticate with Vault using their Okta or GitHub credentials23. Transit is not an authentication method at all, but a secrets engine that provides encryption as a service4. References: AppRole Auth Method | Vault | HashiCorp Developer Okta Auth Method | Vault | HashiCorp Developer GitHub Auth Method | Vault | HashiCorp Developer Transit Secrets Engine | Vault | HashiCorp Developer

QUESTION 4

Your DevOps team would like to provision VMs in GCP via a CICD pipeline. They would like to integrate Vault to protect the credentials used by the tool. Which secrets engine would you recommend?

A. Google Cloud Secrets Engine

B. Identity secrets engine

C. Key/Value secrets engine version 2

D. SSH secrets engine

Correct Answer: A

The Google Cloud Secrets Engine is the best option for the DevOps team to provision VMs in GCP via a CICD pipeline and integrate Vault to protect the credentials used by the tool. The Google Cloud Secrets Engine can dynamically generate GCP service account keys or OAuth tokens based on IAM policies, which can be used to authenticate and authorize the CICD tool to access GCP resources. The credentials are automatically revoked when they are no longer used or when the lease expires, ensuring that the credentials are short-lived and secure. The DevOps team can configure rolesets or static accounts in Vault to define the scope and permissions of the credentials, and use the Vault API or CLI to request credentials on demand. The Google Cloud Secrets Engine also supports generating access tokens for impersonated service accounts,which can be useful for delegating access to other service accounts without storing or managing their keys1. The Identity Secrets Engine is not a good option for this use case, because it does not generate GCP credentials, but rather generates identity tokens that can be used to access other Vault secrets engines or namespaces2. The Key/Value Secrets Engine version 2 is also not a good option, because it does not generate dynamic credentials, but rather stores and manages static secrets that the user provides3. The SSH Secrets Engine is not a good option either, because it does not generate GCP credentials, but rather generates SSH keys or OTPs that can be used to access remote hosts via SSH4. References: Google Cloud - Secrets Engines | Vault | HashiCorp Developer Identity - Secrets Engines | Vault | HashiCorp Developer KV - Secrets Engines | Vault | HashiCorp Developer SSH - Secrets Engines | Vault | HashiCorp Developer

QUESTION 5

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)