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.pass4itsure.com/vault-associate.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A web application uses Vault\\'s transit secrets engine to encrypt data in-transit. If an attacker intercepts the data in transit which of the following statements are true? Choose two correct answers.

A. You can rotate the encryption key so that the attacker won\\'t be able to decrypt the data

B. The keys can be rotated and min_decryption_version moved forward to ensure this data cannot be decrypted

C. The Vault administrator would need to seal the Vault server immediately

D. Even if the attacker was able to access the raw data, they would only have encrypted bits (TLS in transit)

Correct Answer: BD

A web application that uses Vault\\'s transit secrets engine to encrypt data in- transit can benefit from the following security features: Even if the attacker was able to access the raw data, they would only have encrypted bits (TLS in transit). This means that the attacker would need to obtain the encryption key from Vault in order to decrypt the data, which is protected by Vault\\'s authentication and authorization mechanisms. The transit secrets engine does not store the data sent to it, so the attacker cannot access the data from Vault either. The keys can be rotated and min_decryption_version moved forward to ensure this data cannot be decrypted. This means that the web application can periodically change the encryption key used to encrypt the data, and set a minimum decryption version for the key, which prevents older versions of the key from being used to decrypt the data. This way, even if the attacker somehow obtained an old version of the key, they would not be able to decrypt the data that was encrypted with a newer version of the key. The other statements are not true, because: You cannot rotate the encryption key so that the attacker won\\'t be able to decrypt the data. Rotating the key alone does not prevent the attacker from decrypting the data, as they may still have access to the old version of the key that was used to encrypt the data. You need to also move the min_decryption_version forward to invalidate the old version of the key. The Vault administrator would not need to seal the Vault server immediately. Sealing the Vault server would make it inaccessible to both the attacker and the legitimate users, and would require unsealing it with the unseal keys or the recovery keys. Sealing the Vault server is a last resort option in case of a severe compromise or emergency, and is not necessary in this scenario, as the attacker does not have access to the encryption key or the data in Vault. References: Transit Secrets Engines | Vault | HashiCorp Developer, Encryption as a service: transit secrets engine | Vault | HashiCorp Developer

QUESTION 2

When using Integrated Storage, which of the following should you do to recover from possible data loss?

A. Failover to a standby node

B. Use snapshot

C. Use audit logs

D. Use server logs

Correct Answer: B

Integrated Storage is a Raft-based storage backend that allows Vault to store its data internally without relying on an external storage system. It also enables Vault to run in high availability mode with automatic leader election and failover. However, Integrated Storage is not immune to data loss or corruption due to hardware failures, network partitions, or human errors. Therefore, it is recommended to use the snapshot feature to backup and restore the Vault data periodically or on demand. A snapshot is a point-in-time capture of the entire Vault data, including the encrypted

secrets, the configuration, and the metadata. Snapshots can be taken and restored using the vault operator raft snapshot command or the sys/ storage/raft/snapshot API endpoint. Snapshots are encrypted and can only be restored with a quorum of unseal keys or recovery keys. Snapshots are also portable and can be used to migrate data between different Vault clusters or storage backends. References:
https://developer.hashicorp.com/vault/docs/concepts/integrated- storage1,
https://developer.hashicorp.com/vault/docs/commands/operator/raft/snapshot2,
https://developer.hashicorp.com/vault/api-docs/system/ storage/raft/snapshot3

QUESTION 3

Examine the command below. Output has been trimmed.

```
$ vault write auth/approle/login \
  role_id="debb8f13-79ea-3e3d-8100-10711d85c1fb" \
  secret_id="31d52faa-5b0b-711d-2ea2-c197cff6081b"Key Value
---                  -----
token                b.AAAAAQIlWH-DExezQvz-ZGWMhzsy8uWXEoQYHH6O...trimmed...
token_accessor       n/a
token_duration       1m
token_renewable      false
token_policies       ["shipping"]
identity_policies    []
policies             ["shipping"]
token_meta_role_name shipping
```

Which of the following statements describe the command and its output?

A. Missing a default token policy

B. Generated token\\'s TTL is 60 hours

C. Generated token is an orphan token which can be renewed indefinitely

D. Configures the AppRole auth method with user specified role ID and secret ID

Correct Answer: BC

The command shown in the image is:

vault token create -policy=approle -orphan -period=60h This command creates a new token with the following characteristics:

It has the policy "approle" attached to it, which grants or denies access to certain paths and operations in Vault according to the policy rules. The policy can be defined by using the vault policy write command or the sys/policy API endpoint12.

It is an orphan token, which means it has no parent token and it will not be revoked when its parent token is revoked. Orphan tokens can be useful for creating long- lived tokens that are not affected by the token hierarchy3. It has a period of

60 hours, which means it has a renewable TTL of 60 hours. This means that the token can be renewed indefinitely as long as it does not go past the 60-hour mark from the last renewal time. The token\\'s TTL will be reset to 60 hours upon

each renewal. Periodic tokens are useful for creating tokens that have a fixed lifetime and can be easily revoked4.

References: [1]1,

[2]2, 3(https://developer.hashicorp.com/vault/docs/secrets/kv), 4(https://developer.hashicorp.com/vault/docs/secrets/kv)

QUESTION 4

The following three policies exist in Vault. What do these policies allow an organization to do?

app.hcl

```
path "transit/encrypt/my_app_key" {
  capabilities = ["update"]
}
```

callcenter.hcl

```
path "transit/decrypt/my_app_key" {
  capabilities = ["update"]
}
```

rewrap.hcl

```
path "transit/keys/my_app_key" {
  capabilities = ["read"]
}

path "transit/rewrap/my_app_key" {
  capabilities = ["update"]
}
```

A. Separates permissions allowed on actions associated with the transit secret engine

B. Nothing, as the minimum permissions to perform useful tasks are not present

C. Encrypt, decrypt, and rewrap data using the transit engine all in one policy

D. Create a transit encryption key for encrypting, decrypting, and rewrapping encrypted data

Correct Answer: C

The three policies that exist in Vault are: admins: This policy grants full access to all secrets and operations in Vault. It can be used by administrators or operators who need to manage all aspects of Vault. default: This policy grants access to all secrets and operations in Vault except for those that require specific policies. It can be used as a fallback policy when no other policy matches. transit: This policy grants access only to the transit secrets engine, which handles cryptographic functions on data in-transit. It can be used by applications or services that need to encrypt or decrypt data using Vault. These policies allow an organization to perform useful tasks such as: Encrypting, decrypting, and rewrapping data using the transit engine all in one policy: This policy grants access to both the transit secrets engine

and the default policy, which allows performing any operation on any secret in Vault. Creating a transit encryption key for encrypting, decrypting, and rewrapping encrypted data: This policy grants access only to the transit secrets engine and its associated keys, which are used for encrypting and decrypting data in transit using AES-GCM with a 256-bit AES key or other supported key types. Separating permissions allowed on actions associated with the transit secret engine: This policy grants access only to specific actions related to the transit secrets engine, such as creating keys or wrapping requests. It does not grant access to other operations or secrets in Vault.

QUESTION 5

How many Shamir\\'s key shares are required to unseal a Vault instance?

A. All key shares

B. A quorum of key shares

C. One or more keys

D. The threshold number of key shares

Correct Answer: D

Shamir\\'s Secret Sharing is a cryptographic algorithm that allows a secret to be split into multiple parts, called key shares, such that a certain number of key shares are required to reconstruct the secret. The number of key shares and the threshold number are configurable parameters that depend on the desired level of security and availability. Vault uses Shamir\\'s Secret Sharing to protect its master key, which is used to encrypt and decrypt the data encryption key that secures the Vault data. When Vault is initialized, it generates a master key and splits it into a configured number of key shares, which are then distributed to trusted operators. To unseal Vault, the threshold number of key shares must be provided to reconstruct the master key and decrypt the data encryption key. This process ensures that no single operator can access the Vault data without the cooperation of other key holders. References:
https://developer.hashicorp.com/vault/docs/concepts/seal4,
https://developer.hashicorp.com/vault/docs/commands/operator/init5,
https://developer.hashicorp.com/vault/docs/commands/operator/unseal6

QUESTION 6

Which of the following vault lease operations uses a lease_id as an argument? Choose two correct answers.

A. renew

B. revoke -prefix

C. create

D. describe

E. revoke

Correct Answer: AE

The vault lease operations that use a lease_id as an argument are renew and revoke. The renew operation allows a client to extend the validity of a lease associated with a secret or a token. The revoke operation allows a client to terminate a lease immediately and invalidate the secret or the token. Both operations require a lease_id as an argument to identify the lease to be renewed or revoked. The lease_id can be obtained from the response of reading a secret or

creating a token, or from the vault lease list command. The other operations, revoke-prefix, create, and describe, do not use a lease_id as an argument. The revoke-prefix operation allows a client to revoke all secrets or tokens generated under a given prefix. The create operation allows a client to create a new lease for a secret. The describe operation allows a client to view information about a lease, such as its TTL, policies, and metadata. References: Lease, Renew, and Revoke | Vault | HashiCorp Developer, vault lease - Command | Vault | HashiCorp Developer

QUESTION 7

Which of these are a benefit of using the Vault Agent?

A. Vault Agent allows for centralized configuration of application secrets engines

B. Vault Agent will auto-discover which authentication mechanism to use

C. Vault Agent will enforce minimum levels of encryption an application can use

D. Vault Agent will manage the lifecycle of cached tokens and leases automatically

Correct Answer: D

Vault Agent is a client daemon that provides the following features:

Auto-Auth - Automatically authenticate to Vault and manage the token renewal process for locally-retrieved dynamic secrets.

API Proxy - Allows Vault Agent to act as a proxy for Vault\\'s API, optionally using (or forcing the use of) the Auto-Auth token.

Caching - Allows client-side caching of responses containing newly created tokens and responses containing leased secrets generated off of these newly created tokens. The agent also manages the renewals of the cached tokens and

leases. Templating - Allows rendering of user-supplied templates by Vault Agent, using the token generated by the Auto-Auth step.

Process Supervisor Mode - Runs a child process with Vault secrets injected as environment variables.

One of the benefits of using the Vault Agent is that it will manage the lifecycle of cached tokens and leases automatically. This means that the agent will handle the token renewal and revocation logic, as well as the lease renewal and

revocation logic for the secrets that are cached by the agent. This reduces the burden on the application developers and operators, and ensures that the tokens and secrets are always valid and up-to-date. References: Vault Agent | Vault |

HashiCorp Developer, Caching - Vault Agent | Vault | HashiCorp Developer

QUESTION 8

What is a benefit of response wrapping?

A. Log every use of a secret

B. Load balanc secret generation across a Vault cluster

C. Provide error recovery to a secret so it is not corrupted in transit

D. Ensure that only a single party can ever unwrap the token and see what\\'s inside

Correct Answer: D

Response wrapping is a feature that allows Vault to take the response it would have sent to a client and instead insert it into the cubbyhole of a single-use token, returning that token instead. The client can then unwrap the token and retrieve the original response. Response wrapping has several benefits, such as providing cover, malfeasance detection, and lifetime limitation for the secret data. One of the benefits is to ensure that only a single party can ever unwrap the token and see what\\'s inside, as the token can be used only once and cannot be unwrapped by anyone else, even the root user or the creator of the token. This provides a way to securely distribute secrets to the intended recipients and detect any tampering or interception along the way5. The other options are not benefits of response wrapping: Log every use of a secret: Response wrapping does not log every use of a secret, as the secret is not directly exposed to the client or the network. However, Vault does log the creation and deletion of the response-wrapping token, and the client can use the audit device to log the unwrapping operation6. Load balance secret generation across a Vault cluster: Response wrapping does not load balance secret generation across a Vault cluster, as the secret is generated by the Vault server that receives the request and the response- wrapping token is bound to that server. However, Vault does support high availability and replication modes that can distribute the load and improve the performance of the cluster7. Provide error recovery to a secret so it is not corrupted in transit: Response wrapping does not provide error recovery to a secret so it is not corrupted in transit, as the secret is encrypted and stored in the cubbyhole of the token and cannot be modified or corrupted by anyone. However, if the token is lost or expired, the secret cannot be recovered either, so the client should have a backup or retry mechanism to handle such cases. References: 5(https://developer.hashicorp.com/vault/docs/concepts/response- wrapping), 6(https://developer.hashicorp.com/vault/docs/secrets), 7(https://developer.hashi corp.com/vault/docs/secrets), (https://developer.hashicorp.com/vault/ tutorials/secrets- management/cubbyhole-response-wrapping)

QUESTION 9

Which statement describes the results of this command: $ vault secrets enable transit

A. Enables the transit secrets engine at transit path

B. Requires a root token to execute the command successfully

C. Enables the transit secrets engine at secret path

D. Fails due to missing -path parameter

E. Fails because the transit secrets engine is enabled by default

Correct Answer: A

The command vault secrets enable transit enables the transit secrets engine at the transit path. The transit secrets engine is a secrets engine that handles cryptographic functions on data in-transit, such as encryption, decryption, signing, verification, hashing, and random bytes generation. The transit secrets engine does not store the data sent to it, but only performs the requested operations and returns the results. The transit secrets engine can also be viewed as "cryptography as a service" or "encryption as a service". The command vault secrets enable transit uses the default path of transit for the secrets engine, but this can be changed by using the -path option. For example, vault secrets enable path=my-transit transit would enable thetransit secrets engine at the my-transit path. References: Transit - Secrets Engines | Vault | HashiCorp Developer, vault secrets enable - Command | Vault | HashiCorp Developer

QUESTION 10

Which of the following are replication methods available in Vault Enterprise? Choose two correct answers.

A. Cluster sharding

B. Namespaces

C. Performance Replication

D. Disaster Recovery Replication

Correct Answer: CD

The replication methods available in Vault Enterprise are performance replication and disaster recovery replication. These methods allow critical data to be replicated across clusters to support horizontally scaling and disaster recovery workloads. Performance replication enables a primary cluster to replicate data to one or more secondary clusters, which can handle client requests and improve performance and availability. Performance replication replicates most Vault data, such as secrets, policies, auth methods, and leases, but not tokens. Performance secondaries generate their own tokens and leases, which are not replicated back to the primary. Performance replication also supports filtering, which allows selective replication of data based on namespaces or paths. Disaster recovery replication enables a primary cluster to replicate data to one or more secondary clusters, which act as standby clusters in case of a failure or outage of the primary. Disaster recovery replication replicates all Vault data, including tokens and leases, and maintains the same configuration and state as the primary. Disaster recovery secondaries do not handle client requests, but they can be promoted to a primary in a disaster recovery scenario. References: Replication - Vault Enterprise | Vault | HashiCorp Developer, Performance Replication - Vault Enterprise | Vault | HashiCorp Developer, Disaster Recovery Replication - Vault Enterprise | Vault | HashiCorp Developer