Download HashiCorp HCVA0-003 Exam Dumps Free

Shared by Talley on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Using the Vault CLI, there are several ways to create a new policy. Select the valid commands (Select three)

Options:

A- vault policy write my-policy - << EOF
path 'secret/data/*' {
capabilities = ['create', 'update']
}
EOF
B- vault policy create my-policy /tmp/policy.hcl
C- vault policy write my-policy /tmp/policy.hcl
D- $ cat user.hcl | vault policy write my-policy -

Answer:

A, C, D

Explanation:

Comprehensive and Detailed in Depth

Vault provides multiple valid ways to create a policy via the CLI using the vault policy write command. The HashiCorp Vault documentation states: 'To write a policy, use the vault policy write command.' The valid methods are:

A: 'vault policy write my-policy - << EOF ... EOF uses heredoc syntax to inline policy content, which Vault accepts directly.'

C: 'vault policy write my-policy /tmp/policy.hcl writes a policy from a file, a standard method per the docs: 'The policy can be read from a file or piped from stdin.''

D: 'cat user.hcl | vault policy write my-policy - pipes policy content from a file via stdin, another documented approach: 'You can pipe the policy content to the command using -.''

Option B, vault policy create, is invalid as no such command exists---only vault policy write is used. Thus, A, C, and D are correct.

HashiCorp Vault Documentation - Policies: Write a Policy

Question 2

Question Type: MultipleChoice

An Active Directory admin created a service account for an internal application. You want to store these credentials in Vault, allowing a CI/CD pipeline to read and configure the application with them during provisioning. Vault should maintain the last 3 versions of this secret. Which Vault secrets engine should you use?

Options:

A- The KV secrets engine
B- The LDAP secrets engine
C- The Identity secrets engine
D- The KV v2 secrets engine

Answer:

D

Explanation:

Comprehensive and Detailed In-Depth

The requirement is to store static credentials (from Active Directory) in Vault with versioning (last 3 versions) for a CI/CD pipeline. The KV v2 secrets engine is designed for this: it stores arbitrary key-value pairs and supports versioning, allowing configuration of a maximum version count (e.g., vault kv metadata put -max-versions=3 kv/path). KV v1 (option A) lacks versioning. The LDAP engine (B) is for dynamic LDAP credentials, not static storage. The Identity engine (C) manages identities, not secrets. KV v2's versioning capability meets all needs, per its documentation.

KV v2 Docs

KV Versions Comparison

Question 3

Question Type: MultipleChoice

Which option best actions can be performed if you only had access to a token's accessor? (Select

four)

Options:

A- Look up a token's properties
B- Renew the token
C- Retrieve the actual token ID
D- Revoke the token
E- Look up a token's capabilities on a path

Answer:

A, B, D, E

Explanation:

Comprehensive and Detailed In-Depth

A token accessor allows:

A, B, D, E: 'This accessor can only be used to perform limited actions: Look up a token's properties, Look up a token's capabilities on a path, Renew the token, Revoke the token.' The calling token needs permissions.

Incorrect Option:

C: 'Not including the actual token ID.'

Question 4

Question Type: MultipleChoice

Vault is configured with the oidc auth method and you need to log in using the CLI. What command would you use to authenticate so you can make configuration changes to Vault?

Options:

A- vault login -method=oidc username=bryan
B- vault auth oidc
C- vault login auth/oidc/users/bryan
D- vault login username=bryan

Answer:

A

Explanation:

Comprehensive and Detailed In-Depth

To authenticate via the OIDC auth method using the CLI, the vault login command with the -method flag is used. The Vault documentation states:

'To authenticate using the CLI, you could use the command vault login and specify the auth method you wish to use by using the -method flag. For example, if you wanted to authenticate using OIDC, you could use vault login -method=oidc [options].'

--- Vault Commands: login

A: vault login -method=oidc username=bryan is correct, specifying the OIDC method and username:

'The correct command to authenticate using the oidc auth method in Vault is vault login -method=oidc username=bryan.'

--- Vault Auth: OIDC

B: vault auth oidc is invalid; auth is not a login command.

C: vault login auth/oidc/users/bryan is incorrect syntax; it mimics an API path, not a CLI command.

D: vault login username=bryan lacks the method specification, defaulting to token auth.

Vault Commands: login

Vault Auth: OIDC

Question 5

Question Type: MultipleChoice

True or False? After rotating a transit encryption key, all data encrypted with the previous version must be rewrapped or re-encrypted with the new key.

Options:

A- True
B- False

Answer:

B

Explanation:

Comprehensive and Detailed In-Depth

False. When a transit encryption key is rotated in Vault (e.g., via vault write -f transit/keys/<key_name>/rotate), the new key version becomes the default for future encryptions, but data encrypted with previous versions remains decryptable without rewrapping or re-encryption. Vault maintains a keyring with all versions, and the ciphertext prefix (e.g., vault:v1:) indicates which version was used, allowing automatic decryption with the corresponding key. This seamless handling simplifies key management and avoids mandatory data re-encryption post-rotation. Only if you set a min_decryption_version to archive older keys would rewrapping be needed, but that's optional, not default behavior.

Option A is incorrect per Vault's Transit documentation, which notes that old data can still be decrypted without immediate action after rotation.

Transit Secrets Engine Usage

Key Version Management

Question 6

Question Type: MultipleChoice

When generating a dynamic secret, what value is returned that a user can use to renew or revoke the lease?

Options:

A- renewable
B- token_ttl
C- lease_max
D- lease_id

Answer:

D

Explanation:

Comprehensive and Detailed in Depth

When Vault generates a dynamic secret, it returns a lease_id, which is the value a user can use to renew or revoke the lease. The HashiCorp Vault documentation states: 'When creating a dynamic secret, Vault always returns a lease_id. This lease_id can be used to do a vault lease renew or a vault lease revoke command to manage the lease of a secret.' The lease_id uniquely identifies the lease associated with the dynamic secret, enabling precise management of its lifecycle.

The documentation under the 'Lease Renew and Revoke' section explains: 'Every secret in Vault is associated with a lease. When that lease expires, Vault revokes the secret and removes access to it. Associated with every lease is a unique lease_id. This identifier can be used to renew the lease before it expires or revoke it manually.' In contrast, renewable is a boolean indicating if the lease can be renewed, not a value for management. token_ttl relates to token duration, not lease management. lease_max is not a standard term in Vault's lease system. Thus, D (lease_id) is the correct answer.

HashiCorp Vault Documentation - Leases: Lease Renew and Revoke

Question 7

Question Type: MultipleChoice

Tanner manages a data processing application and needs to be sure the data being processed is encrypted so it is securely stored post-processing. Which secrets engines can encrypt data? (Select three)

Options:

A- transit
B- KMIP
C- SSH
D- transform

Answer:

A, B, D

Explanation:

Comprehensive and Detailed In-Depth

Vault offers secrets engines for encryption:

A . transit: 'Designed specifically for encryption and decryption operations,' ideal for securing data at rest.

B . KMIP: 'Integrates with external Key Management Systems that support the KMIP protocol,' enabling encryption via external keys.

D . transform: 'Used for data transformation operations, including encryption and decryption,' with custom pipelines.

Incorrect Option:

C . SSH: 'Used for dynamic SSH key generation and management,' not general data encryption.

'Only the Transit and Transform secrets engines can encrypt/decrypt data,' with KMIP adding external key support.

Question 8

Question Type: MultipleChoice

Your organization uses a CI/CD pipeline to deploy its applications on Azure. During testing, you generate new credentials to validate Vault can create new credentials. The result of this command is below:

text

CollapseWrapCopy

$ vault read azure/creds/bryan-krausen

Key Value

--- -----

lease_id azure/creds/bryan-krausen/9eed0373-ca92-99b6-b914-779b7bb0e1d9

lease_duration 60m

lease_renewable true

client_id 532bf678-ee4e-6be1-116b-4e4221e445dd

client_secret be60395b-4e6b-2b7e-a4b3-c449a5c00973

What commands can be used to revoke this secret after you have finished testing? (Select three)

Options:

A- vault lease revoke azure/
B- vault lease revoke -prefix azure/
C- vault lease revoke azure/creds/bryan-krausen/9eed0373-ca92-99b6-b914-779b7bb0e1d9
D- vault lease revoke azure/creds/bryan-krausen
E- vault lease revoke -prefix azure/creds/bryan-krausen

Answer:

B, C, E

Explanation:

Comprehensive and Detailed In-Depth

Dynamic credentials are tracked by leases, revocable via vault lease revoke. The Vault documentation states:

'The vault lease revoke command is used to revoke a lease/secret created by a Vault secrets engine. Each lease that is created is tracked using a unique lease ID, which can be used to renew or revoke a lease.

You can revoke an individual lease using the command vault lease revoke <lease_id>

You can also revoke ALL leases from a secrets engine using the -prefix flag, such as vault lease revoke -prefix azure/

You can also revoke leases created from a specific role by using the -prefix flag but specifying the path all the way to the role like this: vault lease revoke -prefix azure/creds/<role_name>'

--- Vault Commands: lease revoke

B: Correct. vault lease revoke -prefix azure/ revokes all leases under azure/.

C: Correct. vault lease revoke azure/creds/bryan-krausen/9eed0373-ca92-99b6-b914-779b7bb0e1d9 targets the specific lease ID.

E: Correct. vault lease revoke -prefix azure/creds/bryan-krausen revokes all leases for that role.

A: Incorrect; lacks the -prefix flag, making it invalid syntax.

D: Incorrect; lacks the -prefix flag and isn't a full lease ID.

Vault Commands: lease revoke

Question 9

Question Type: MultipleChoice

The Vault Agent provides which of the following benefits? (Choose three)

Options:

A- Token renewal
B- Authentication to Vault
C- Client-side caching of responses
D- Automatically creates secrets in the desired storage backend

Answer:

A, B, C

Explanation:

Comprehensive and Detailed in Depth

The Vault Agent is a client daemon designed to simplify integration with Vault by providing several key benefits. According to the HashiCorp Vault documentation, these include:

Token Renewal: 'Vault Agent automatically renews tokens issued by Vault,' ensuring continuous access without manual intervention.

Authentication to Vault: 'Vault Agent provides authentication to Vault,' allowing applications to authenticate using their identity without managing tokens directly.

Client-side caching of responses: 'Vault Agent offers client-side caching of responses,' improving performance by reducing server requests.

However, automatically creating secrets in the desired storage backend is not a function of Vault Agent. Secret creation is handled by Vault's secrets engines, not the agent, which focuses on authentication, token management, and caching. Thus, A, B, and C are the correct benefits.

HashiCorp Vault Documentation - Vault Agent