



HashiCorp

Exam Questions HCVA0-003

HashiCorp Certified: Vault Associate (003)Exam

NEW QUESTION 1

- (Topic 1)

When using the Vault Secrets Operator, where is the secret written to after being retrieved from Vault?

- A. The secret is never written to any service or persistent storage
- B. Directly to the filesystem of the pod
- C. Kubernetes Secrets
- D. To the cloud-provider's native secret manager (Azure Key Vault, AWS Secrets Manager, etc.)

Answer: C

NEW QUESTION 2

- (Topic 1)

What is the difference between the TTL and the Max TTL (select two)?

- A. The TTL defines when the token will expire and be revoked
- B. The TTL defines when another token will be generated
- C. The Max TTL defines the timeframe for which a token cannot be used
- D. The Max TTL defines the maximum timeframe for which a token can be renewed

Answer: AD

NEW QUESTION 3

- (Topic 1)

What is the default maximum time-to-live (TTL) for a token, measured in days?

- A. 32 days (768 hours)
- B. 7 days (168 hours)
- C. 14 days (336 hours)
- D. 31 days (744 hours)

Answer: A

NEW QUESTION 4

- (Topic 1)

You want to encrypt a credit card number using the Transit secrets engine. You enter the following command and receive an error. What can you do to ensure that the credit card number is properly encrypted and the ciphertext is returned?

```
$ vault write -format=json transit/encrypt/creditcards plaintext="1234 5678 9101 1121" Error: * illegal base64 data at input byte 4
```

- A. The plain text data needs to be encoded to base64
- B. The token used to issue the encryption request does not have the appropriate permissions
- C. Credit card numbers are not supported using the Transit secrets engine since it is considered sensitive data
- D. The credit card number should not include spaces

Answer: A

NEW QUESTION 5

- (Topic 1)

When generating dynamic credentials, Vault also creates associated metadata, including information like time duration, renewability, and more, and links it to the credentials. What is this referred to as?

- A. Secret
- B. Token
- C. Lease
- D. Secrets engine

Answer: C

NEW QUESTION 6

- (Topic 1)

Jason has enabled the userpass auth method at the path users/. What path would Jason and other Vault operators use to interact with this new auth method?

- A. users/auth/
- B. authentication/users
- C. auth/users
- D. users/

Answer: C

NEW QUESTION 7

- (Topic 1)

Which of the following is NOT a valid way in which a lease can be revoked in Vault?

- A. Using the user interface (UI)
- B. Automatically when the TTL or Max-TTL expires

- C. Using the API to call the /v1/sys/leases endpoint
- D. Via the CLI using the vault token command

Answer: D

NEW QUESTION 8

- (Topic 1)

What is the proper command to enable the AWS secrets engine at the default path?

- A. vault enable aws secrets engine
- B. vault secrets enable aws
- C. vault secrets aws enable
- D. vault enable secrets aws

Answer: B

NEW QUESTION 9

- (Topic 1)

You logged into the Vault CLI and attempted to enable an auth method, but you received this error message. What can you do to resolve the error and configure Vault?

(Error: dial tcp 127.0.0.1:8200: connect: connection refused)

```
bk~$vault secrets enable transit
Error enabling: Post "https://127.0.0.1:8200/v1/sys/mounts/transit": http: server
gave HTTP response to HTTPS client
bk~$
```

- A. Restart the Vault service on this node
- B. Ask an admin to grant you permission to enable the userpass auth method
- C. Change 'userpass' to 'username and password'
- D. Set the VAULT_ADDR environment variable to HTTP

Answer: D

NEW QUESTION 10

- (Topic 1)

What API endpoint is used to manage secrets engines in Vault?

- A. /secret-engines/
- B. /sys/mounts
- C. /sys/capabilities
- D. /sys/kv

Answer: B

NEW QUESTION 10

- (Topic 1)

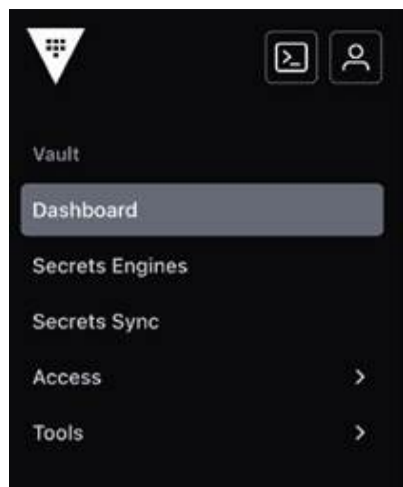
A user is assigned the following policy, and they can successfully retrieve secrets using the CLI. However, the user reports receiving an error message in the UI. Why can't the user access the secret in the Vault UI?

```
path "kv/apps/app01" { capabilities = ["read"] }
```

Successful retrieval using the CLI

```
$ vault kv get kv/apps/app01
===== Data =====
Key                Value
---                -
student01         student01
```

(Error: Permission denied in UI)



kv

Not Authorized

You don't have access to kv/ . If you think you've reached this page in error, please contact your administrator.

[Go back home.](#)

- A. The user doesn't know what they're doing
- B. The user doesn't have permissions to retrieve the data from the UI, only the CLI
- C. The user needs list permissions to browse the UI
- D. The user's token is invalid

Answer: C

NEW QUESTION 11

- (Topic 1)

Which of the following Vault policies will allow a Vault client to read a secret stored at secrets/applications/app01/api_key?

- A. path "secrets/applications/" { capabilities = ["read"] allowed_parameters = { "certificate" = [] } }
- B. path "secrets/*" { capabilities = ["list"] }
- C. path "secrets/applications/+api_*" { capabilities = ["read"] }
- D. path "secrets/applications/app01/api_key/*" { capabilities = ["update", "list", "read"] }

Answer: C

NEW QUESTION 16

- (Topic 1)

True or False? All dynamic secrets in Vault are required to have a lease.

- A. True
- B. False

Answer: A

NEW QUESTION 19

- (Topic 1)

After decrypting data using the Transit secrets engine, the plaintext output does not match the plaintext credit card number that you encrypted. Which of the following answers provides a solution?

\$ vault write transit/decrypt/creditcard ciphertext="vault:v1:cZNVHx+sxdMEr....." Key: plaintext Value: Y3JIZGI0LWNhcmQtbmVtYmVyCg==

- A. Vault is sealed, therefore the data cannot be decrypte
- B. Unseal Vault to properly decrypt the data
- C. The user doesn't have permission to decrypt the data, therefore Vault returns false data
- D. The resulting plaintext data is base64-encode
- E. To reveal the original plaintext, use the base64 --decode command
- F. The data is corrupte
- G. Execute the encryption command again using a different data key

Answer: C

NEW QUESTION 22

- (Topic 1)

True or False? Once you create a KV v1 secrets engine and place data in it, there is no way to modify the mount to include the features of a KV v2 secrets engine.

- A. True
- B. False

Answer: B

NEW QUESTION 23

- (Topic 1)

After issuing the command to delete a secret, you run a vault kv list command, but the path to the secret still seems to exist. What command would permanently delete the path from Vault?

```
$ vault kv delete kv/applications/app01
Success! Data deleted (if it existed) at: kv/applications/app01
$ vault kv list kv/applications
Keys
----
app01
```

- A. vault kv delete -force kv/applications/app01
- B. vault kv destroy -versions=1 kv/applications/app01
- C. vault kv metadata delete kv/applications/app01
- D. vault kv delete -all kv/applications/app01

Answer: C

NEW QUESTION 28

- (Topic 2)

Christy has created a token and needs to use that token to access Vault. What command can she use to authenticate and access secrets stored in Vault?

```
$ vault token create -policy=christy Key Value
```

```
--- -----
```

```
token hvs.hxDIPd8RPVtxu4AzSGS1IArP token_accessor AxwpxDs6LbdFQbWGmBDnwlK3 token_duration 24h
token_renewable true token_policies ["christy" "default"] identity_policies []
policies ["christy" "default"]
```

- A. vault login hvs.hxDIPd8RPVtxu4AzSGS1IArP
- B. vault login -method=password
- C. vault login -method=token christy
- D. vault login -accessor=AxwpxDs6LbdFQbWGmBDnwlK3

Answer: A

NEW QUESTION 30

- (Topic 2)

Which of the following statements best describes the difference between static and dynamic credentials in a secrets management system?

- A. They are functionally identical—the only difference is what secrets engine creates them.
- B. Static credentials only apply to specific use cases, while dynamic credentials can be used everywhere.
- C. Static credentials often remain persistent for long periods of time, while dynamic are short-lived and auto-rotated.
- D. Static credentials are ephemeral and rotated frequently, while dynamic credentials remain unchanged indefinitely.

Answer: C

NEW QUESTION 33

- (Topic 2)

After a client has authenticated to Vault, what security feature is used to make all subsequent calls?

- A. ldap
- B. pgp
- C. path
- D. key shard
- E. listener
- F. token

Answer: F

NEW QUESTION 37

- (Topic 2)

True or False? The command vault lease revoke -prefix aws/ will revoke all leases associated with the secret engine mounted at /aws.

- A. True
- B. False

Answer: A

NEW QUESTION 39

- (Topic 2)

Select the two default policies created in Vault. (Select two)

- A. root
- B. user
- C. admin
- D. default
- E. base

F. vault

Answer: AD

NEW QUESTION 42

- (Topic 2)

True or False? Once the minimum decryption version is set on an encryption key, older versions of the key are removed from Vault and are no longer available for decryption operations.

- A. True
- B. False

Answer: B

NEW QUESTION 47

- (Topic 2)

Mike??s Cereal Shack uses Vault to encrypt customer data to ensure it is always stored securely. They are developing a new application integration to send new customer data to be encrypted using the following API request: text

CollapseWrapCopy

```
$ curl \
```

```
--header "X-Vault-Token: hvs.sf4vj1rFV5PvQSV3M9dcv832brxQFsfbXA" \
```

```
--request POST \
```

```
--data @data.json \ https://vault.mcshack.com:8200/v1/transit/encrypt/customer-data
```

 What would be contained within the data.json file?

- A. Transit secrets engine configuration file
- B. Ciphertext to be decrypted
- C. The encryption key to be used for encrypting the data
- D. Cleartext customer data to be encrypted

Answer: D

NEW QUESTION 49

- (Topic 2)

Which statement best describes the process of sealing a Vault instance?

- A. Disable the TLS certificates on the Vault server by running `vault secrets disable pki`, blocking all requests.
- B. Run `vault operator rotate` to rotate the Vault tokens for all clients, causing them to reauthenticate with the Vault.
- C. Run the `vault operator seal` command, which securely discards the master key from memory and prevents further operations until unsealed.
- D. Revoke all leases so no secrets can be accessed using `vault lease revoke`, but keep the master key in memory for quick recovery.

Answer: C

NEW QUESTION 53

- (Topic 2)

Beyond encryption and decryption of data, which of the following is not a function of the Transit secrets engine?

- A. Generate hashes and HMACs of data
- B. Sign and verify data
- C. Store the encrypted data securely in Vault for retrieval
- D. Act as a source of random bytes

Answer: C

NEW QUESTION 54

- (Topic 2)

When Vault is sealed, which are the only two operations available to a Vault administrator? (Select two)

- A. View the status of Vault
- B. Configure policies
- C. View data stored in the key/value store
- D. Rotate the encryption key
- E. Unseal Vault
- F. Author security policies

Answer: AE

NEW QUESTION 58

- (Topic 2)

You have a legacy application that requires secrets from Vault that must be written to a local configuration file. However, you cannot refactor the application to communicate directly with Vault. What solution should you implement to satisfy the requirements?

- A. Run the Vault Agent and use the templating feature
- B. Use the Vault Proxy with Auto-Auth to authenticate with Vault
- C. Use the Vault Proxy to act as a proxy for the Vault API
- D. Use the Vault Agent and cache the newly created tokens and leases

Answer: A

NEW QUESTION 61

- (Topic 2)

What is the correct order that Vault uses to protect data?

- A. root key --> encryption key --> data
- B. unseal keys --> root key --> data
- C. root key --> data
- D. encryption key --> root key --> data

Answer: A

NEW QUESTION 64

- (Topic 2)

Which statement most accurately describes how the response wrapping feature functions in Vault?

- A. Vault takes the response it would have sent to an HTTP client and instead inserts it into the cubbyhole of a single-use token, returning that single-use token instead.
- B. Vault encrypts the response with a dedicated key and sends it directly to the client, never storing it on the server or using single-use tokens for additional security.
- C. Vault divides the response into separate parts and stores each part in different tokens, requiring all tokens to be combined before disclosing the secret to the requesting client.
- D. Vault duplicates the response within a persistent token and allows multiple unwraps, ensuring that any user with the correct token can retrieve the secret repeatedly without time restrictions.

Answer: A

NEW QUESTION 65

- (Topic 3)

Your organization operates active/active applications across multiple data centers for high availability. Which Vault feature should be used in the secondary data centers to provide local access to secrets?

- A. Performance standby nodes
- B. Customized plugins for the Vault cluster
- C. Disaster recovery cluster
- D. Performance replication cluster

Answer: D

NEW QUESTION 68

- (Topic 3)

Kyle enabled the database secrets engine for dynamic credentials. Amy, the senior DBA, accidentally deleted the database users created by Vault, disrupting client applications.

How can Kyle manually remove the leases in Vault?

- A. No action is required since the leases will eventually expire and be revoked
- B. Obtain the individual lease IDs from the application logs and remove them using the vault lease revoke command
- C. Use the command vault lease revoke -force flag to delete the leases
- D. Revoke all of the leases associated with the entire database secrets engine to be sure they are all removed

Answer: C

NEW QUESTION 70

- (Topic 3)

What header must be included in an API request in order to provide authentication validation?

- A. X-Token-Vault
- B. X-Vault-Token
- C. X-Token-Creds
- D. X-Vault-Creds

Answer: B

NEW QUESTION 74

- (Topic 3)

Based on the output below, how many policies have been added to Vault?

```
$ vault policy list base
default root
web-app-1 automation-team
```

- A. 3
- B. 4
- C. 1
- D. 2

Answer: A

NEW QUESTION 75

- (Topic 3)

True or False? You can create and update Vault policies using the UI.

- A. True
- B. False

Answer: A

NEW QUESTION 77

- (Topic 3)

True or False? To encrypt existing encrypted data with the latest version of the encryption key, you need to first decrypt it and then request Vault to re-encrypt it with the latest version of the encryption key.

- A. True
- B. False

Answer: B

NEW QUESTION 78

- (Topic 3)

You need a simple and self-contained HashiCorp Vault cluster deployment with minimal dependencies. Which storage backend is best suited for this use case, providing all configuration within Vault and avoiding external services?

- A. Local File Storage Backend
- B. Integrated Storage (raft) Backend
- C. Consul Backend
- D. In-Memory Backend

Answer: B

NEW QUESTION 83

- (Topic 3)

True or False? Once the lease for a dynamic secret has expired, Vault revokes the credentials on the backend platform for which they were created (i.e., database, AWS, Kubernetes).

- A. True
- B. False

Answer: A

NEW QUESTION 87

- (Topic 3)

When you are unsealing Vault using unseal keys, what are you actually doing?

- A. Creating the recovery keys
- B. Exporting the encryption key
- C. Reconstructing the root key
- D. Decrypting the Vault data

Answer: C

NEW QUESTION 90

- (Topic 3)

What command would you use to enable the Kubernetes secrets engine at the path of /k8s-cluster?

- A. vault secrets enable -path=k8s-cluster kubernetes
- B. vault kv put k8s-cluster type=kubernetes
- C. vault write sys/mounts/k8s-cluster
- D. vault secrets enable kubernetes -path=k8s-cluster

Answer: A

NEW QUESTION 92

- (Topic 3)

What is the default value of the VAULT_ADDR environment variable?

- A. http://127.0.0.1:8200
- B. https://vault.example.com:8200
- C. https://127.0.0.1:8200
- D. http://vault.example.com:8200

Answer: C

NEW QUESTION 97

- (Topic 3)
What API endpoint is used to enable and configure a secrets engine?

- A. /v1/sys/init
- B. /v1/sys/mounts
- C. /v1/sys/config
- D. /v1/sys/plugins/catalog

Answer: B

NEW QUESTION 99

- (Topic 3)
True or False? Although AppRole is designed for machines, humans can use it to authenticate to Vault if you wish.

- A. True
- B. False

Answer: A

NEW QUESTION 100

- (Topic 3)
You need to decrypt customer data to provide it to an application. When you run the decryption command, you get the output below. Why does the response not directly reveal the cleartext data?

```
$ vault write transit/decrypt/phone_number ciphertext="vault:v1:tgx2vsxtlQRfyLSKvem..." Key Value
```

```
--- -----  
plaintext aGFzaGljb3JwIGNlcnRpZmlZDogdmF1bHQgYXNzb2NpYXRRI
```

- A. The user does not have permission to view the cleartext data
- B. The output is base64 encoded
- C. The output is actually a response wrapped token that needs to be unwrapped
- D. The original data must have been encrypted

Answer: B

NEW QUESTION 104

- (Topic 3)
You are enabling a secrets engine in Vault using the CLI. What subcommands are available when using the vault secrets command? (Select five)

- A. update
- B. migrate
- C. tune
- D. enable
- E. move
- F. disable
- G. list

Answer: CDEFG

NEW QUESTION 107

- (Topic 3)
What features are offered by the Vault Agent? (Select three)

- A. Auditing
- B. Templating
- C. Auto-auth
- D. Secret caching

Answer: BCD

NEW QUESTION 111

- (Topic 3)
True or False? The following policy permits a user to read secrets contained in the path secrets/cloud/apps/jenkins?

```
text CollapseWrapCopy  
path "secrets/cloud/apps/jenkins/*" {  
  capabilities = ["create", "read", "update", "delete", "list"]  
}
```

- A. True
- B. False

Answer: B

NEW QUESTION 115

- (Topic 4)
Before data is written to the storage backend, the data is encrypted by which Vault feature?

- A. TLS certificate

- B. Cryptographic barrier
- C. Unseal keys
- D. Transit secrets engine

Answer: B

NEW QUESTION 118

- (Topic 4)

Frapps, Inc. is a coffee startup specializing in frozen caffeinated beverages. Their new customer loyalty web app uses Vault to store sensitive information, choosing Integrated Storage for its benefits. Select the benefits the organization would see by using Integrated Storage over other storage backends (Select four)

- A. Eliminates network communication between hosts, requiring no open ports between hosts
- B. Uses the SERF gossip protocol to enable communication between cluster nodes
- C. Eliminates the requirement to deploy and manage a separate platform for storing encrypted data
- D. Simplified troubleshooting since Integrated Storage is a built-in solution
- E. Reduces operational overhead since all configuration is within Vault itself
- F. Immediate access to storage since the data is stored locally on disk

Answer: CDEF

NEW QUESTION 119

- (Topic 4)

Which of the following are considered benefits of using policies in Vault? (Select three)

- A. Policies are assigned to a token on a 1:1 basis to eliminate conflicting policies
- B. Provides granular access control to paths within Vault
- C. Policies have an implicit deny, meaning that policies are deny by default
- D. Policies provide Vault operators with role-based access control

Answer: BCD

NEW QUESTION 122

- (Topic 4)

What is the primary role of the Vault Security Operator (VSO) in a Kubernetes environment?

- A. Managing Vault server deployments and auto-scaling Vault instances in Kubernetes
- B. Enforcing Kubernetes network policies for Vault communication
- C. Automating the injection and lifecycle management of Vault secrets for Kubernetes workloads
- D. Replacing Kubernetes Secrets with a built-in alternative that does not require Vault

Answer: C

NEW QUESTION 123

- (Topic 4)

To protect the sensitive data stored in Vault, what key is used to encrypt the data before it is written to the storage backend?

- A. Recovery key
- B. Encryption key
- C. Unseal key
- D. Root key

Answer: B

NEW QUESTION 128

- (Topic 4)

You have a CI/CD pipeline using Terraform to provision AWS resources with static privileged credentials. Your security team requests that you use Vault to limit AWS access when needed. How can you enhance this process and increase pipeline security?

- A. Enable the SSH secrets engine and have Terraform generate dynamic credentials when deploying resources in AWS
- B. Enable the Transit secrets engine to encrypt the AWS credentials and have Terraform retrieve these credentials when needed
- C. Store the AWS credentials in the Vault KV store and use the Vault provider to obtain these credentials on each terraform apply
- D. Enable the aws secrets engine and configure Terraform to dynamically generate a short-lived AWS credential on each terraform apply

Answer: D

NEW QUESTION 133

- (Topic 4)

You are working on a new project and need to retrieve a secret from Vault. You log into the Vault UI and browse to the path where the secret is stored. Based on the screenshot below, what is true about the secrets stored in this path? (Select four)

The screenshot shows the Vault web interface. The breadcrumb path is 'secrets / developers / apps / eCommerce'. The main heading is 'apps/eCommerce'. Below the heading are tabs for 'Secret', 'Metadata', 'Paths', and 'Version History'. A 'JSON' toggle is visible. Action buttons include 'Delete', 'Destroy', 'Copy', 'Version 4', and 'Create new version'. A table lists secrets with columns 'Key' and 'Value':

Key	Value
connection_string
database
host
username

- A. The secrets are stored in a KV v1 secrets engine
- B. The user does not have permission to delete the secret
- C. The secrets are stored in a KV v2 secrets engine
- D. The secrets engine is mounted at the path developers/
- E. There are four previous versions of the secret
- F. The user has additional permissions on the path beyond just list and read

Answer: CDEF

NEW QUESTION 138

- (Topic 4)

You are planning the deployment of your first Vault cluster and have decided to use Integrated Storage as the storage backend. Where do you configure the storage backend to be used by Vault?

- A. In the systemd service file
- B. Inside the Vault service once Vault is up and running
- C. In the Vault configuration file
- D. In the Vault Agent sink file

Answer: C

NEW QUESTION 143

- (Topic 4)

By default, what methods of authentication does Vault support? (Select four)

- A. SSH
- B. Kubernetes
- C. VMware
- D. LDAP
- E. AppRole
- F. JWT

Answer: BDEF

NEW QUESTION 146

- (Topic 4)

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"]
}
path "sys/rotate" {
  capabilities = ["read", "update"]
}
```

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

Answer: A

NEW QUESTION 148

- (Topic 4)

A MySQL server has been deployed on Google Cloud Platform (GCP) to support a legacy application. You want to generate dynamic credentials against this MySQL server rather than use static credentials. What Vault secrets engine would you use to accomplish this?

- A. The GCP secrets engine
- B. The Identity secrets engine
- C. The database secrets engine
- D. The Cubbyhole secrets engine

Answer: C

NEW QUESTION 149

- (Topic 4)

To secure your applications, your organization uses certificates generated by a public CA. However, this strategy has proven expensive and you have to revoke certificates even though they have additional time left. What Vault plugin can be used to quickly generate

- A. X.509 certificates to secure your internal applications?
- B. Identity secrets engine
- C. PKI secrets engine
- D. SSH secrets engine
- E. Transit secrets engine

Answer: B

NEW QUESTION 153

- (Topic 4)

Your Azure Subscription ID is stored in Vault and you need to retrieve it via Vault API for an automated job. The Subscription ID is stored at secret/cloud/azure/subscription. The secret is stored on a KV Version 2 secrets engine. What curl command below would successfully retrieve the latest version of the secret?

- A. curl https://vault.krausen.com:8200/v1/secret/data/cloud/azure/subscription
- B. curl --header "X-Vault-Token: hvs.CbzCNJCVWt63jzyaJakgDwz" https://vault.krausen.com:8200/v1/secret/cloud/azure/subscription
- C. curl --header "X-Vault-Token: hvs.CbzCNJCVWt63jzyaJakgDwz" https://vault.krausen.com:8200/v1/secret/data/cloud/azure/subscription
- D. curl --header "X-Vault-Token: hvs.CbzCNJCVWt63jzyaJakgDwz" https://vault.krausen.com:8200/secret/data/cloud/azure/subscription/latest

Answer: C

NEW QUESTION 155

- (Topic 4)

Which of the following capabilities can be used when writing a Vault policy? (Select four)

- A. list
- B. deny
- C. apply
- D. root
- E. create
- F. write

Answer: ABEF

NEW QUESTION 157

- (Topic 4)

Vault enables the generation of dynamic credentials against many different platforms. When generating these credentials, what Vault feature is used to track the credentials?

- A. namespace
- B. role
- C. token
- D. lease_id

Answer: D

NEW QUESTION 162

- (Topic 4)

True or False? Your organization currently runs all of its workloads on Google Cloud Platform (GCP). Recently, Vault has been deployed, and you need to select an auth method to authenticate your workloads with Vault. Based on this information, GCP is the only auth method that can be used in your environment.

- A. True
- B. False

Answer: B

NEW QUESTION 166

- (Topic 4)

You are using Vault CLI and enable the database secrets engine on the default path of database/. However, the DevOps team wants to enable another database secrets engine for testing but receives an error stating the path is already in use. How can you enable a second database secrets engine using the CLI?

- A. vault secrets enable database database2/
- B. vault secrets enable -force database
- C. vault secrets enable -path=database2 database
- D. vault secrets enable database2/

Answer: C

NEW QUESTION 170

- (Topic 5)

Which of these is not a benefit of dynamic secrets?

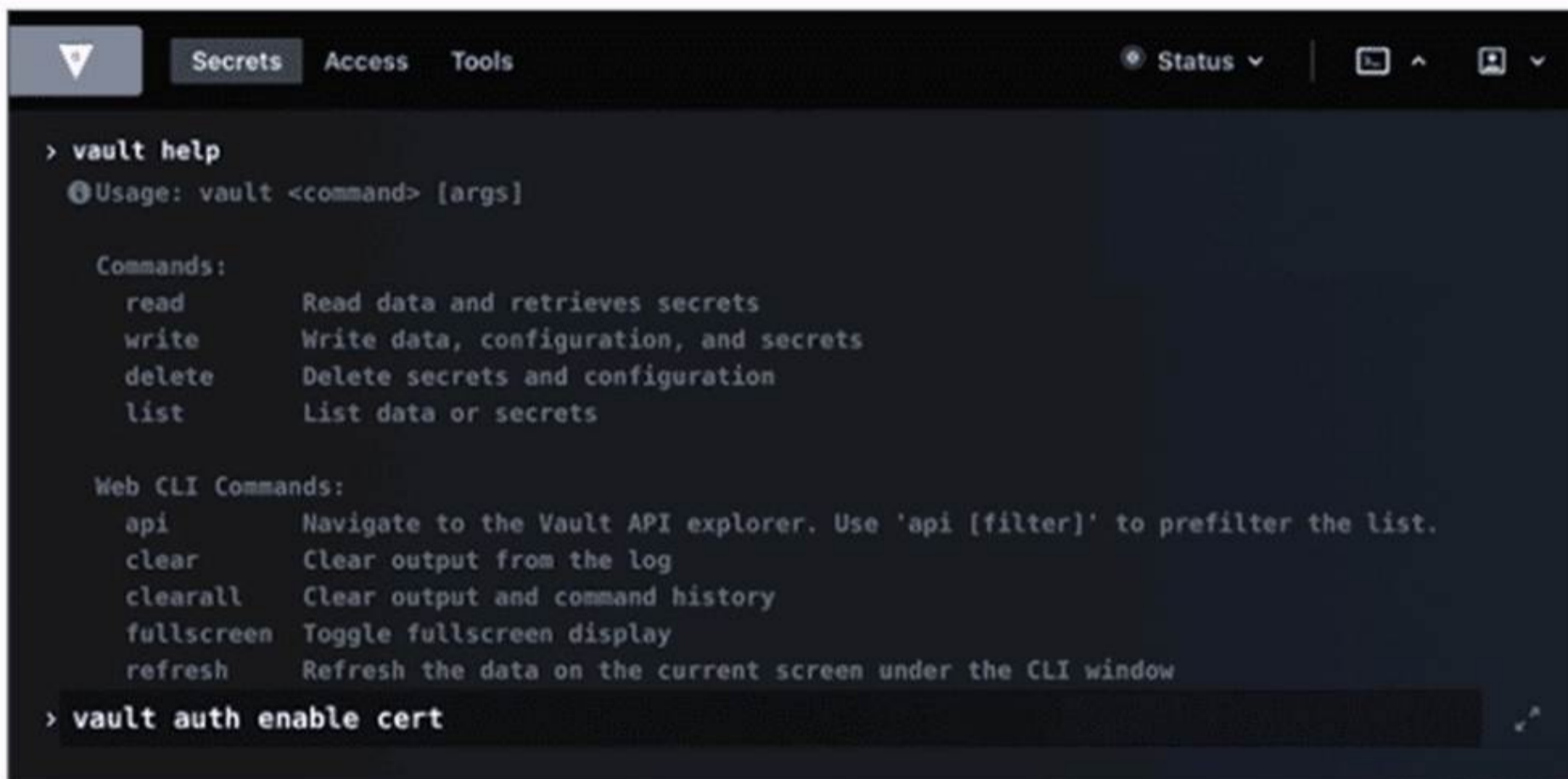
- A. Supports systems which do not natively provide a method of expiring credentials
- B. Minimizes damage of credentials leaking
- C. Ensures that administrators can see every password used
- D. Replaces cumbersome password rotation tools and practices

Answer: C

NEW QUESTION 172

- (Topic 5)

Running the second command in the GUI CLI will succeed.



- A. True
- B. False

Answer: B

NEW QUESTION 173

- (Topic 5)

What does the following policy do?

```

path "secret/data/{{identity.entity.id}}/*" {
  capabilities = ["create", "update", "read", "delete"]
}

path "secret/metadata/{{identity.entity.id}}/*" {
  capabilities = ["list"]
}
  
```

- A. Grants access for each user to a KV folder which shares their id
- B. Grants access to a special system entity folder
- C. Allows a user to read data about the secret endpoint identity
- D. Nothing, this is not a valid policy

Answer: C

NEW QUESTION 174

- (Topic 5)

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

- A. Transit
- B. PKI
- C. PostgreSQL
- D. Generic

Answer: B

NEW QUESTION 176

- (Topic 5)

Vault supports which type of configuration for source limited token?

- A. Cloud-bound tokens
- B. Domain-bound tokens
- C. CIDR-bound tokens
- D. Certificate-bound tokens

Answer: C

NEW QUESTION 177

- (Topic 5)

To give a role the ability to display or output all of the end points under the `/secrets/apps/*` end point it would need to have which capability set?

- A. update
- B. read
- C. sudo
- D. list
- E. None of the above

Answer: C

NEW QUESTION 182

- (Topic 5)

How would you describe the value of using the Vault transit secrets engine?

- A. Vault has an API that can be programmatically consumed by applications
- B. The transit secrets engine ensures encryption in-transit and at-rest is enforced enterprise wide
- C. Encryption for application data is best handled by a storage system or database engine, while storing encryption keys in Vault
- D. The transit secrets engine relieves the burden of proper encryption/decryption from application developers and pushes the burden onto the operators of Vault

Answer: D

NEW QUESTION 183

- (Topic 5)

Where does the Vault Agent store its cache?

- A. In a file encrypted using the Vault transit secret engine
- B. In the Vault key/value store
- C. In an unencrypted file
- D. In memory

Answer: D

NEW QUESTION 184

- (Topic 5)

You are performing a high number of authentications in a short amount of time. You're experiencing slow throughput for token generation. How would you solve this problem?

- A. Increase the time-to-live on service tokens
- B. Implement batch tokens
- C. Establish a rate limit quota
- D. Reduce the number of policies attached to the tokens

Answer: B

NEW QUESTION 186

- (Topic 5)

The Vault encryption key is stored in Vault's backend storage.

- A. True
- B. False

Answer: B

NEW QUESTION 188

- (Topic 5)

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

Answer: D

NEW QUESTION 193

- (Topic 5)

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

Answer: CD

NEW QUESTION 198

- (Topic 5)

Your organization has an initiative to reduce and ultimately remove the use of long lived X.509 certificates. Which secrets engine will best support this use case?

- A. PKI
- B. Key/Value secrets engine version 2, with TTL defined
- C. Cloud KMS
- D. Transit

Answer: A

NEW QUESTION 199

- (Topic 5)

You have been tasked with writing a policy that will allow read permissions for all secrets at path secret/bar. The users that are assigned this policy should also be able to list the secrets.What should this policy look like?

A.

```
path "secret/bar/*" {
  capabilities = ["read","list"]
}
```

B.

```
path "secret/bar/*" {
  capabilities = ["list"]
}

path "secret/bar/" {
  capabilities = ["read"]
}
```

C.

```
path "secret/bar/*" {
  capabilities = ["read"]
}
```

```
path "secret/bar/" {
  capabilities = ["list"]
}
```

D.

```
path "secret/bar/+" {
  capabilities = ["read", "list"]
}
```

Answer: C

NEW QUESTION 201

- (Topic 5)

An organization wants to authenticate an AWS EC2 virtual machine with Vault to access a dynamic database secret. The only authentication method which they can use in this case is AWS.

- A. True
- B. False

Answer: B

NEW QUESTION 204

- (Topic 5)

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

Answer: A

NEW QUESTION 209

- (Topic 5)

Your DevOps team would like to provision VMs in GCP via a CI/CD 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

Answer: A

NEW QUESTION 211

- (Topic 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

Answer: D

NEW QUESTION 215

- (Topic 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

Answer: ACD

NEW QUESTION 219

- (Topic 5)

As a best practice, the root token should be stored in which of the following ways?

- A. Should be revoked and never stored after initial setup
- B. Should be stored in configuration automation tooling
- C. Should be stored in another password safe
- D. Should be stored in Vault

Answer: A

NEW QUESTION 224

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

HCVA0-003 Practice Exam Features:

- * HCVA0-003 Questions and Answers Updated Frequently
- * HCVA0-003 Practice Questions Verified by Expert Senior Certified Staff
- * HCVA0-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * HCVA0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The HCVA0-003 Practice Test Here](#)