

# HashiCorp

## Exam Questions HCVA0-003

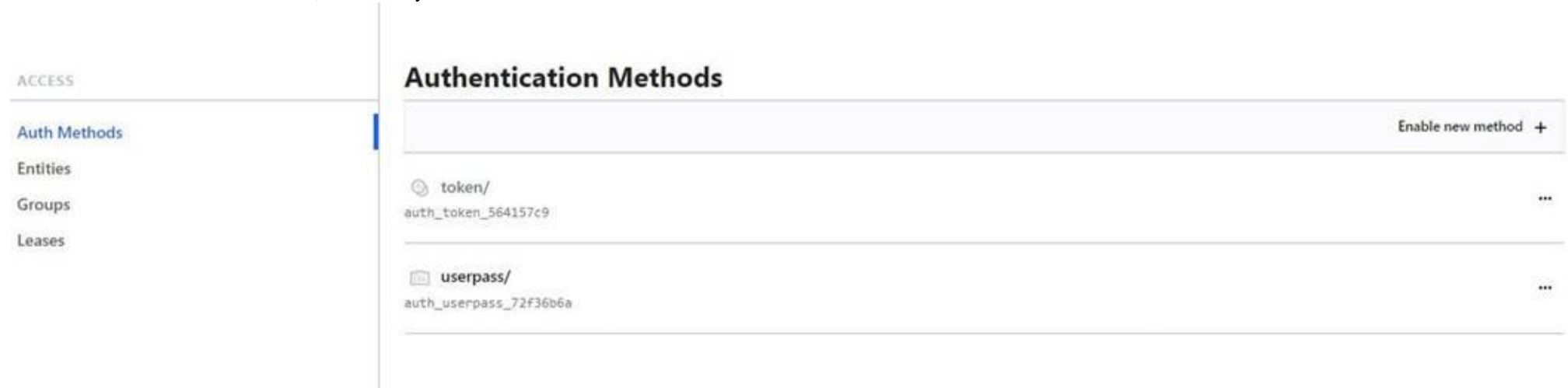
HashiCorp Certified: Vault Associate (003)Exam



**NEW QUESTION 1**

- (Topic 1)

Based on the screenshot below, how many auth methods have been enabled on this Vault instance?



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

**Answer: B**

**NEW QUESTION 2**

- (Topic 1)

During a service outage, you must ensure all current tokens and leases are copied to another Vault cluster for failover so applications don't need to authenticate. How can you accomplish this?

- A. Have Vault write all the tokens and leases to a file so you have a second copy of them
- B. Configure all applications to use the auto-auth feature of the Vault Agent
- C. Configure Disaster Recovery replication and promote the secondary cluster during an outage
- D. Replicate to another cluster using Performance Replication and promote the secondary cluster during an outage

**Answer: C**

**NEW QUESTION 3**

- (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 4**

- (Topic 1)

True or False? The Vault Secrets Operator does NOT encrypt client cache, such as Vault tokens and leases, by default in Kubernetes Secrets.

- A. True
- B. False

**Answer: A**

**NEW QUESTION 5**

- (Topic 1)

You want to integrate a third-party application to retrieve credentials from the HashiCorp Vault API. How can you accomplish this without having direct access to the source code?

- A. You cannot integrate a third-party application with Vault without being able to modify the source code
- B. Put in a request to the third-party application vendor
- C. Instead of the API, have the application use the Vault CLI to retrieve credentials
- D. Use the Vault Agent to obtain secrets and provide them to the application

**Answer: D**

**NEW QUESTION 6**

- (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 7

- (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 8

- (Topic 1)

What is true about the output of the following command (select three)?

- A. The admin never sees all the unseal keys and cannot unseal Vault by themselves
- B. All three users, Jane/John/Student01, will receive all unseal keys and can unseal Vault
- C. The admin will receive the unseal keys and be able to unseal Vault themselves
- D. The keys will be returned encrypted
- E. Each individual can only decrypt their own unseal key using their private PGP key

**Answer: ADE**

#### NEW QUESTION 9

- (Topic 1)

You've set up multiple Vault clusters, one on-premises intended to be the primary cluster, and the second cluster in AWS, which was deployed for performance replication. After enabling replication, developers complain that all the data they've stored in the AWS Vault cluster is missing. What happened?

- A. There is a certificate mismatch after replication was enabled since Vault replication generates its own TLS certificates to ensure nodes are trusted entities
- B. All of the data on the secondary cluster was deleted after replication was enabled
- C. The data was automatically copied to the primary cluster after replication was enabled since all writes are always forwarded to the primary cluster
- D. The data was moved to a recovery path after replication was enable
- E. Use the vault secrets move command to move the data back to its intended location

**Answer: B**

#### NEW QUESTION 10

- (Topic 1)

Which of the following statements are true regarding Vault seal and unseal (select three)?

- A. By default, Vault uses the Shamir Sharing algorithm to create unseal keys during the initialization process
- B. When using Vault Auto Unseal feature, Vault returns unseal keys to the user when it is initialized
- C. Vault can use a third-party KMS solution to automatically unseal during a service restart
- D. Vault supports high availability for the Auto Unseal feature, allowing you to point to multiple keys

**Answer: ACD**

#### NEW QUESTION 10

- (Topic 1)

Which of the following policies would permit a user to generate dynamic credentials on a database?

- A. path "database/creds/read\_only\_role" { capabilities = ["generate"] }
- B. path "database/creds/read\_only\_role" { capabilities = ["update"] }
- C. path "database/creds/read\_only\_role" { capabilities = ["list"] }
- D. path "database/creds/read\_only\_role" { capabilities = ["read"] }

**Answer: D**

#### NEW QUESTION 11

- (Topic 1)

From the options below, select the benefits of using a batch token over a service token (select four).

- A. Often used for ephemeral, high-performance workloads
- B. Can be a root token
- C. Can be used on performance replication clusters (if orphan)
- D. Has accessors
- E. Lightweight and scalable
- F. No storage cost for token creation

**Answer: ACEF**

**NEW QUESTION 15**

- (Topic 1)

True or False? When using the Transit secrets engine, setting the min\_decryption\_version will determine the minimum key length of the data key (i.e., 2048, 4096, etc.).

- A. True
- B. False

**Answer: B**

**NEW QUESTION 20**

- (Topic 1)

What command would have created the token displayed below?

```
$ vault token lookup hvs.nNeZ2l64ALCxuO7dqQEJGPrO
Key: policies Value: [default dev], num_uses: 5, ttl: 767h59m49s
? Key Value
? --- -----
? accessor mfvaVMFgOcXHleqIRasroSON
? creation_time 1604610457
? creation_ttl 768h
? display_name token
? entity_id n/a
? expire_time 2024-12-07T16:07:37.7540672-05:00
? explicit_max_ttl 0s
? id hvs.nNeZ2l64ALCxuO7dqQEJGPrO
? issue_time 2024-11-05T16:07:37.7540672-05:00
? meta <nil>
? num_uses 5
? orphan false
? path auth/token/create
? policies [default dev]
? renewable true
? ttl 767h59m49s
? type service
```

- A. vault token create -policy=dev -use-limit=5
- B. vault token create -policy=dev -ttl=768h
- C. vault token create -policy=dev -policy=default -ttl=768h
- D. vault token create -policy=dev

**Answer: A**

**NEW QUESTION 24**

- (Topic 1)

Which of the following are accurate statements regarding the use of a KV v2 secrets engine (select three)?

- A. Issuing a vault kv destroy command permanently deletes the current version of the secret
- B. Issuing a vault kv destroy command deletes all versions of a secret
- C. Issuing a vault kv delete command performs a soft delete of the current version
- D. Issuing a vault kv metadata delete command permanently deletes the secret

**Answer: ACD**

**NEW QUESTION 25**

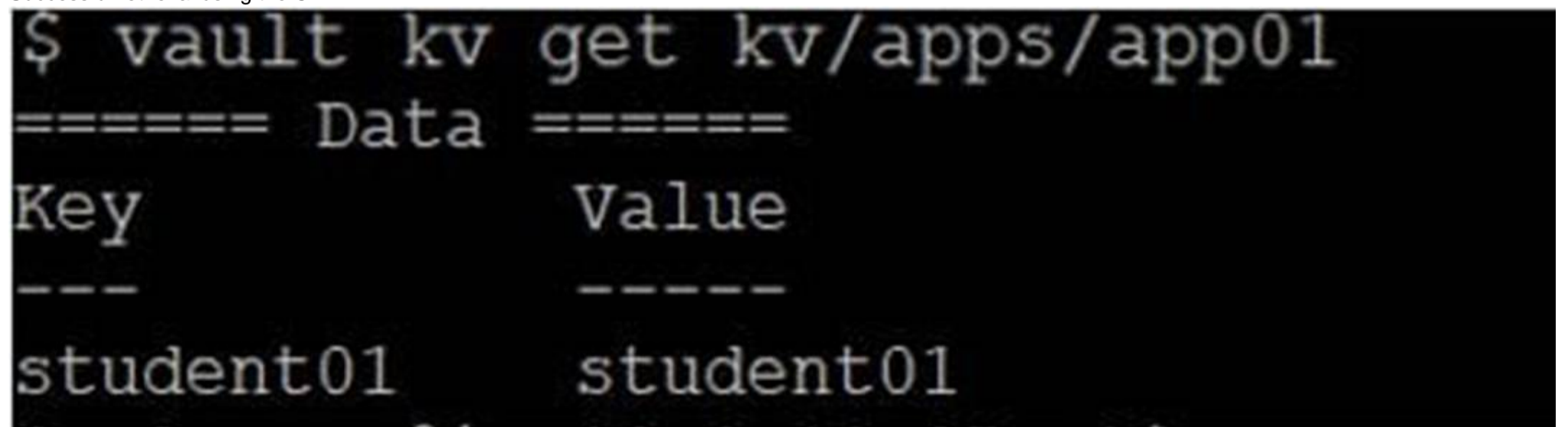
- (Topic 1)

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?

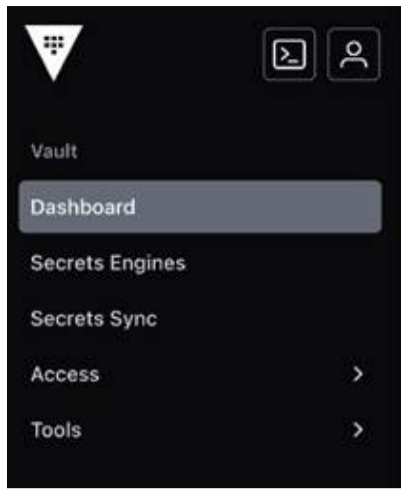
```
path "kv/apps/app01" { capabilities = ["read"] }
```

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.](#)

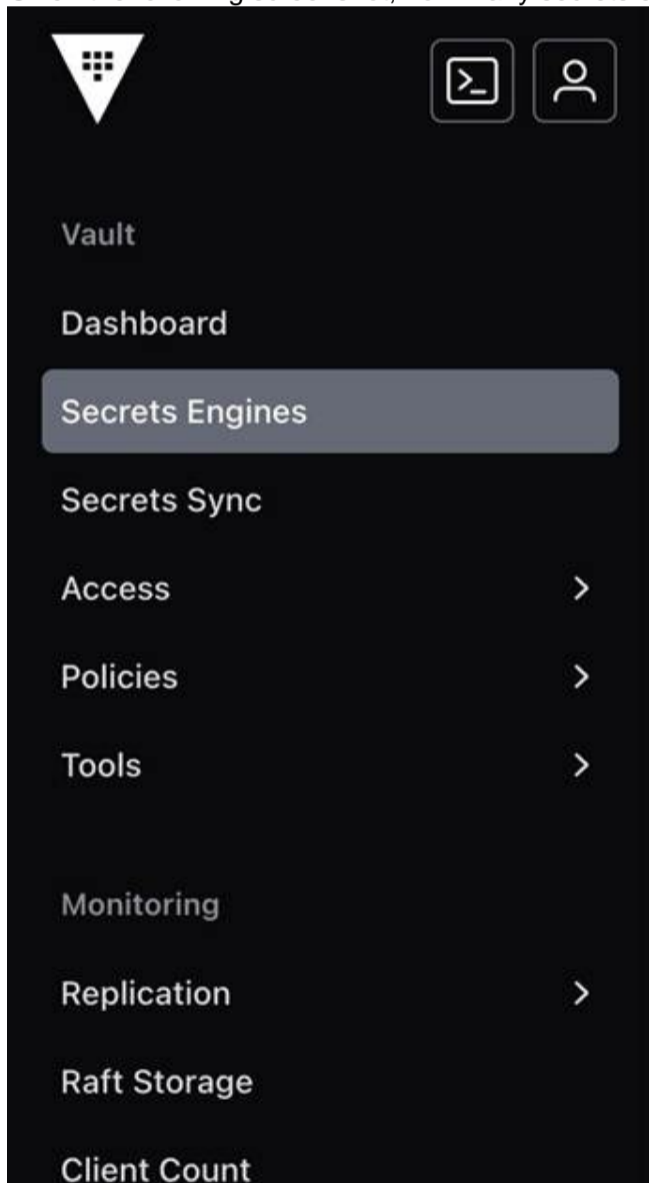
- A. The user doesn't know what they're doing
- B. The user doesn't have permissions to retrieve the data from the UI, only the CLI
- C. The user needs list permissions to browse the UI
- D. The user's token is invalid

Answer: C

### NEW QUESTION 30

- (Topic 1)

Given the following screenshot, how many secrets engines have been enabled by a Vault user?



## Secrets Engines

Filter by engine type

Filter by engine name

**certs/**  
pki\_5f4e8adf

**cubbyhole/**  
cubbyhole\_f333a76e  
per-token private secret storage

**kv/**  
kv\_e8bacb66

**transit/**  
transit\_0e77e4be

- A. 2
- B. 3
- C. 4
- D. 5

Answer: B

### NEW QUESTION 31

- (Topic 1)

Which of the following token attributes can be used to renew a token in Vault (select two)?

- A. TTL
- B. Token ID
- C. Identity policy
- D. Token accessor

Answer: BD

**NEW QUESTION 33**

- (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 37**

- (Topic 1)

Tommy has written an AWS Lambda function that will perform certain tasks for the organization when data has been uploaded to an S3 bucket. Security policies for the organization do not allow Tommy to hardcode any type of credential within the Lambda code or environment variables. However, Tommy needs to retrieve a credential from Vault to write data to an on-premises database. What auth method should Tommy use in Vault to meet the requirements while not violating security policies?

- A. AWS
- B. Userpass
- C. Token
- D. AppRole

**Answer: A**

**NEW QUESTION 42**

- (Topic 1)

Which of the following statements best describes the difference in cluster strategies between self-managed Vault and HashiCorp-managed Vault?

- A. Self-managed clusters require users to handle setup, maintenance, and scaling, whereas HCP Vault Dedicated is fully managed by HashiCorp and offloads most operational tasks
- B. Neither self-managed clusters nor HCP Vault Dedicated include enterprise security features such as replication or disaster recovery
- C. Both self-managed clusters and HCP Vault Dedicated require manual patching and upgrades, but only self-managed clusters are hosted in the user's cloud
- D. In self-managed clusters, HashiCorp is responsible for scaling, upgrades, and patching, while HCP Vault Dedicated requires the user to handle all operational overhead

**Answer: A**

**NEW QUESTION 46**

- (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 49**

- (Topic 2)

Based on the following output, what command can Steve use to determine if the KV store is configured for versioning?

text CollapseWrapCopy

```
$ vault secrets list
```

```
Path Type Accessor Description
-----
```

```
automation/ kv kv_56f991b9 Automation team for CI/CD cloud/ kv kv_4426c541 Cloud team for static secrets
cubbyhole/ cubbyhole cubbyhole_9bd538e per-token priv secret storage data_team/ kv kv_96d57692 Data warehouse KV for certs
identity/ identity identity_0042595e identity store network/ kv kv_3e53aaab Network team secret storage secret/ kv kv_d66e2adc key/value secret storage
sys/ system system_d6f218a9 system endpoints
```

- A. vault secrets list -all
- B. vault kv get automation
- C. vault secrets list -detailed
- D. vault kv list

Answer: C

**NEW QUESTION 51**

- (Topic 2)

An application requires a specific key/value pair to be updated in order to process a batch job. The value should be either "true" or "false." However, when developers have been updating the value, sometimes they mistype the value or capitalize the value, causing the batch job not to run. What feature of a Vault policy can be used to restrict entry to the required values?

- A. Add a deny statement for all possible misspellings of the value
- B. Add an allowed\_parameters value to the policy
- C. Change the policy to include the list capability
- D. Use a \* wildcard at the end of the policy

Answer: B

**NEW QUESTION 56**

- (Topic 2)

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

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

Answer: ABC

**NEW QUESTION 57**

- (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 60**

- (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 62**

- (Topic 2)

Before the following command can be run to encrypt data, what (three) commands must be run to enable and configure the transit secrets engine in Vault? (Select three)

```
text CollapseWrapCopy
```

```
$ vault write transit/encrypt/vendor \ plaintext="aGFzaGljb3JwIGNlcnRpZmlZA=="
```

- A. base64 <<< "hashicorp certified"
- B. vault write transit/encrypt/vendor
- C. vault secrets list
- D. vault secrets enable transit
- E. vault write -f transit/keys/vendor

Answer: ADE

**NEW QUESTION 67**

- (Topic 2)

True or False? All Vault policies are deny by default.

- A. True
- B. False

Answer: A

#### NEW QUESTION 70

- (Topic 2)

What command is used to extend the TTL of a token, if permitted?

- A. vault token revoke <token-id>
- B. vault capabilities <token-id>
- C. vault token lookup <token-id>
- D. vault token renew <token-id>

**Answer:** D

#### NEW QUESTION 71

- (Topic 2)

You are using Azure Key Vault for the auto-unseal configuration on your cluster. After the Vault service restarts, what command must you run to unseal Vault?

- A. You don't need to run a command when using auto-unseal
- B. vault operator members
- C. vault operator unseal
- D. vault operator init

**Answer:** A

#### NEW QUESTION 74

- (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 79

- (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 82

- (Topic 2)

Compared to service tokens, batch tokens are ideal for what type of action?

- A. Generating dynamic credentials
- B. Renewing other tokens
- C. For daily batch jobs requesting secrets from Vault
- D. Short-lived, high-volume, or ephemeral tasks

**Answer:** D

#### NEW QUESTION 84

- (Topic 2)

Which auth method is ideal for machine-to-machine authentication?

- A. Okta
- B. UserPass
- C. GitHub
- D. AppRole

**Answer:** D

#### NEW QUESTION 85

- (Topic 2)

Which of the following auth methods is the best choice for human interaction with Vault (as opposed to machine/system authentication)?

- A. Kubernetes
- B. AppRole
- C. TLS
- D. OIDC

Answer: D

**NEW QUESTION 89**

- (Topic 2)

What is the default method of authentication after first initializing Vault?

- A. TLS certificates
- B. GitHub
- C. Admin account
- D. Tokens
- E. AppRole
- F. Userpass

Answer: D

**NEW QUESTION 93**

- (Topic 2)

True or False? After initializing Vault or restarting the Vault service, each individual node in the cluster needs to be unsealed.

- A. True
- B. False

Answer: A

**NEW QUESTION 97**

- (Topic 2)

What type of Vault token does not have a TTL (Time to Live)?

- A. Child tokens
- B. Parent tokens
- C. Service tokens
- D. Root tokens
- E. Batch tokens

Answer: D

**NEW QUESTION 102**

- (Topic 2)

Which of the following unseal options can automatically unseal Vault upon the start of the Vault service? (Select four)

- A. HSM
- B. Azure KMS
- C. AWS KMS
- D. Transit
- E. Key Shards

Answer: ABCD

**NEW QUESTION 103**

- (Topic 2)

Which of the following statements are true about HCP Vault Dedicated? (Select three)

- A. Provides 100% feature parity compared to Vault self-managed clusters
- B. Helps reduce operational overhead for organizations with push-button deployment and fully managed upgrades
- C. Increases reliability and ease of use so you can onboard applications and teams easily
- D. Increases security across clouds and machines through a single interface

Answer: BCD

**NEW QUESTION 107**

- (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 109**

- (Topic 2)  
 Which of the following are benefits of using the Vault Secrets Operator (VSO)? (Select three)

- A. Support for syncing from multiple secret sources
- B. Bi-directional sync between Vault and Kubernetes Secrets
- C. Automatic secret drift and remediation
- D. Automatic secret rotation for multiple Kubernetes resource types

**Answer:** ACD

**NEW QUESTION 113**

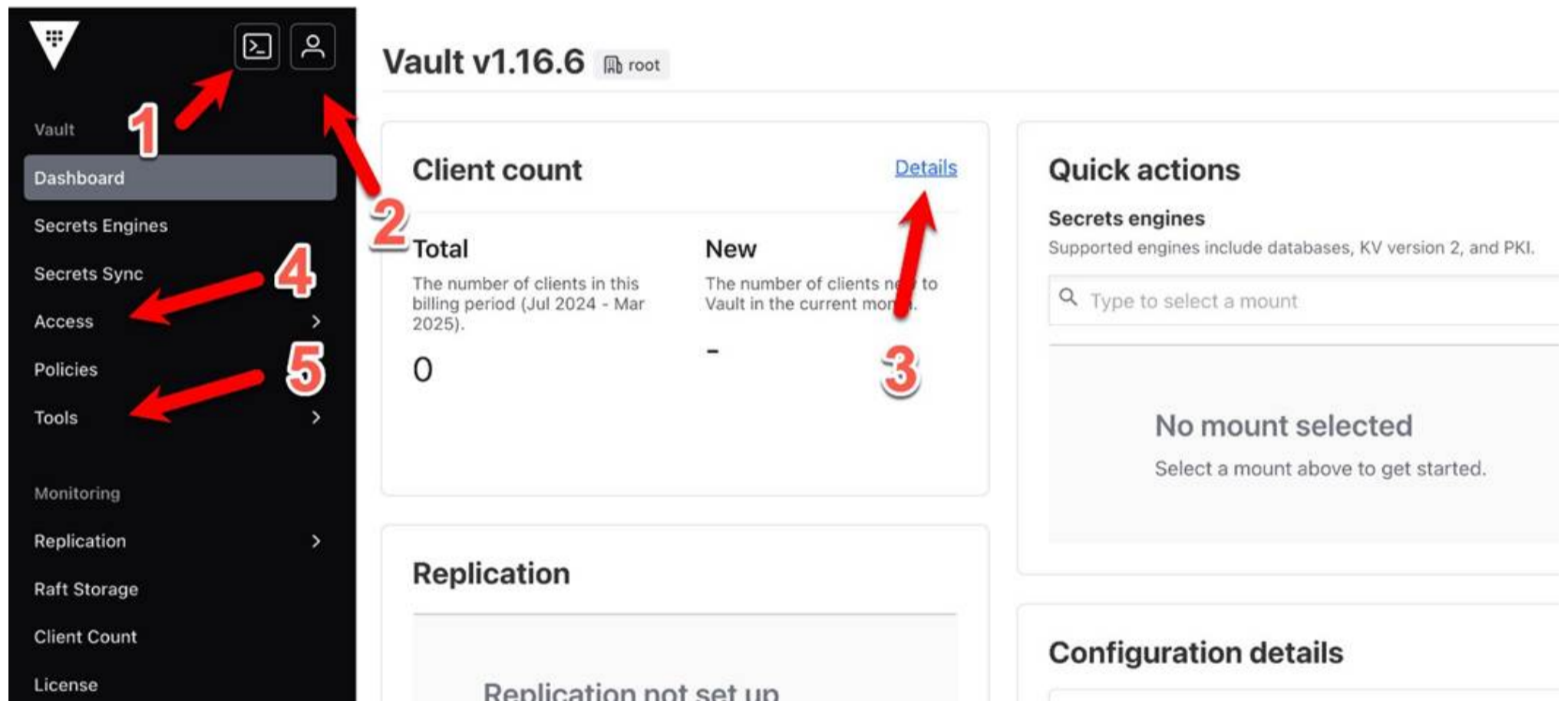
- (Topic 2)  
 You have a long-running app that cannot handle a regeneration of a token or secret. What type of token should be created for this application in order to authenticate and interact with Vault?

- A. Service Token with Use Limit
- B. Periodic Service Token
- C. Batch Token
- D. Orphan Token

**Answer:** B

**NEW QUESTION 117**

- (Topic 2)  
 Without logging into another interface, what feature can Chad use to execute a simple CLI command to enable a new secrets engine?



- A. CLI emulation in the Vault UI (Feature 1)
- B. User information button (Feature 2)
- C. Client count details (Feature 3)
- D. Access management link (Feature 4)

**Answer:** A

**NEW QUESTION 118**

- (Topic 3)  
 Tom needs to set the proper environment variable so he doesn't need to first authenticate to Vault to retrieve dynamically generated credentials for a database server. What environment variable does Tom need to set first before running commands?

- A. VAULT\_NAMESPACE
- B. VAULT\_TOKEN
- C. VAULT\_CAPATH
- D. VAULT\_CLIENT\_KEY

**Answer:** B

**NEW QUESTION 119**

- (Topic 3)  
 You have ciphertext stored in an Amazon S3 bucket encrypted by the key named prod- customer. Will Vault decrypt this data with the command `vault write transit/decrypt/prod- customer ciphertext="vault:v4:xa1f9FIJtn13em/Wb7QCxSUsU/kCOn7..."` given this output?  
 ? \$ vault read transit/keys/prod-customer  
 ? Key Value

```
? --- -----
? ...
? keys map[4:1549347108 5:1549347109 6:1549347110]
? latest_version 6
? min_available_version 0
? min_decryption_version 4
? min_encryption_version 0
Will Vault decrypt this data for you by running the following command?
? $ vault write transit/decrypt/prod-customer ciphertext="vault:v4:xa1f9FIJtn13em/Wb7QCsXsU/kCO7..."
```

- A. Yes, because the minimum decryption key configuration is set to 4
- B. No, since the latest version of the key is 6

**Answer: A**

#### NEW QUESTION 122

- (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 124

- (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 127

- (Topic 3)

What command can be used to update a Vault policy named web-app-1 using the command line?

- A. vault policy create web-app-1 web.hcl
- B. vault policy fmt web.hcl
- C. vault policy update web-app-1 web.hcl
- D. vault policy write web-app-1 web.hcl

**Answer: D**

#### NEW QUESTION 132

- (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 136

- (Topic 3)

What occurs when a Vault cluster cannot maintain a quorum while using the Integrated Storage backend?

- A. Vault continues to operate in read-only mode until quorum is restored
- B. The cluster becomes unavailable and cannot commit new logs
- C. Vault automatically promotes a standby node to a leader to restore quorum
- D. Vault temporarily switches to local storage until quorum is regained

**Answer: B**

#### NEW QUESTION 141

- (Topic 3)

Assuming default configurations, which of the following operations require a threshold of key shares to perform? (Select three)

- A. Rotating the Vault encryption key to adhere to internal security policies

- B. Unsealing Vault after a scheduled maintenance to install patches
- C. Generating a new root token as a break-glass procedure
- D. Creating a new set of recovery keys due to an employee leaving the organization

**Answer:** BCD

#### NEW QUESTION 144

- (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 145

- (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 148

- (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 152

- (Topic 3)

Short-lived, dynamically generated secrets provide organizations with many benefits. Select the benefits from the options below. (Select four)

- A. Each application instance can generate its own credentials, rather than using a shared credential across all application instances
- B. Credentials only exist when needed
- C. Applications only have access to privileged accounts when needed
- D. Credentials accidentally checked into a code repo or discovered in a text file are likely to be invalid
- E. Dynamic credentials do not change, so legacy applications can easily take advantage of them

**Answer:** ABCD

#### NEW QUESTION 157

- (Topic 3)

Which of the following auth methods are intended for machine-to-machine authentication, and not necessarily human (operator) authentication? (Select four)

- A. Okta
- B. Tokens
- C. TLS Certificates
- D. Cloud-based Auth methods (AWS, Azure, GCP)
- E. LDAP
- F. AppRole

**Answer:** BCDF

#### NEW QUESTION 160

- (Topic 3)

Hanna is working with Vault and has been assigned a namespace called integration, where she stores all her secrets. Hanna configured her application to use the following API request, but the request is failing. What changes below will help Hanna correctly retrieve the secret? (Select two)

```
$ curl \
--header "X-Vault-Token:hvs.lzrmRe5Y3LMcDRmOttEjWoag" \
--request GET https://vault.example.com:8200/v1/secret/data/my-secret
```

- A. \$ curl --header "X-Vault-Token:hvs.lzrmRe5Y3LMcDRmOttEjWoag" --request GET integration https://vault.example.com:8200/v1/secret/data/my-secret
- B. \$ curl --header "X-Vault-Token:hvs.lzrmRe5Y3LMcDRmOttEjWoag" --request GET -- namespace "integration" https://vault.example.com:8200/v1/secret/data/my-secret
- C. \$ curl --header "X-Vault-Token:hvs.lzrmRe5Y3LMcDRmOttEjWoag" --request GET https://vault.example.com:8200/v1/integration/secret/data/my-secret
- D. \$ curl --header "X-Vault-Token:hvs.lzrmRe5Y3LMcDRmOttEjWoag" --header "X-Vault- Namespace:integration" --request GET

<https://vault.example.com:8200/v1/secret/data/my-secret>

**Answer:** CD

#### NEW QUESTION 164

- (Topic 3)

Suzy is a Vault user that needs to create and replace values at the path `secrets/automation/apps/chef`. Does the following policy permit her the permissions to do so?

```
text CollapseWrapCopy
```

```
path "secrets/automation/apps/chef" { capabilities = ["create", "read", "list"] }
```

- A. No, the policy would deny Suzy from performing certain actions
- B. Yes, the policy has appropriate permissions

**Answer:** A

#### NEW QUESTION 167

- (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 171

- (Topic 3)

Which of the following best describes response wrapping?

- A. The response is Base64 encoded, and the user must decode the response to retrieve the cleartext data
- B. Rather than provide a direct response, Vault returns a token and an accessor
- C. Vault responds with an encrypted version of the response, decrypted via transit
- D. Vault inserts the response into a single-use token's cubbyhole

**Answer:** D

#### NEW QUESTION 176

- (Topic 3)

Your organization has many applications needing heavy read access to Vault. As these applications integrate with Vault, the primary Vault cluster's performance is negatively impacted. What feature can you use to scale the cluster and improve performance?

- A. Add additional standby nodes
- B. Enable multiple secrets engines for the applications
- C. Enable control groups
- D. Add performance standby nodes

**Answer:** D

#### NEW QUESTION 181

- (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 aGFzaGljb3JwIGNlcnRpZmlZDogdmF1bHQgYXNzb2NpYXRl
```

- 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 183

- (Topic 3)

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)

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

**Answer:** ABD

**NEW QUESTION 184**

- (Topic 3)

Vault operators can create two types of groups in Vault. What are the two types?

- A. External groups
- B. Security groups
- C. Policy groups
- D. Internal groups

**Answer:** AD

**NEW QUESTION 187**

- (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 189**

- (Topic 3)

Which of the following are valid types of tokens available in Vault? (Select five)

- A. Primary token
- B. Batch token
- C. Orphan service token
- D. Service token
- E. Root token
- F. Periodic service token

**Answer:** BCDEF

**NEW QUESTION 193**

- (Topic 4)

Your co-worker has asked you to perform certain operations in Vault and has provided you with a token accessor (not the token itself). What Vault operations would you be allowed to perform using only the provided accessor? (Select three)

- A. Renew the token to extend the TTL
- B. Revoke the token in Vault to make it invalid
- C. Create child tokens associated with the same policies as the related token
- D. Lookup properties of the token, such as the TTL, policies, and metadata

**Answer:** ABD

**NEW QUESTION 198**

- (Topic 4)

You have successfully authenticated using the Kubernetes auth method, and Vault has provided a token. What HTTP header can be used to specify your token when you request dynamic credentials? (Select two)

- A. X-Vault-Token: <token>
- B. Token: <token>
- C. Authentication: <token>
- D. Authorization: Bearer <token>

**Answer:** AD

**NEW QUESTION 203**

- (Topic 4)

Your organization recently suffered a security breach on a specific application, and the security response team believes that MySQL database credentials were likely obtained during the event. The application generated the credentials using the database secrets engine in Vault mounted at the path database/. How can you quickly revoke all of the secrets generated by this secrets engine?

- A. vault token revoke database/\*
- B. vault secrets disable mysql
- C. vault lease renew database/creds/mysql
- D. vault lease revoke -prefix database/

**Answer:** D

**NEW QUESTION 207**

- (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 210**

- (Topic 4)

You are planning to deploy a new Vault cluster for your organization and notice that Vault supports a wide variety of storage backends. You need high availability since you will have multiple applications relying on the Vault service. When building your cluster, can you choose any of the available storage backends?

- A. Yes, because all backends provide similar functionality
- B. No, because not all storage backends provide similar functionality

**Answer: B**

#### **NEW QUESTION 212**

- (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 216**

- (Topic 4)

How does the instance updates feature work when using the Vault Secrets Operator?

- A. By monitoring the Vault audit logs to watch for changes to the target path
- B. By constantly validating the current secret stored in Vault
- C. By continuously launching an init container to check for updates
- D. By subscribing to event notifications from Vault

**Answer: D**

#### **NEW QUESTION 220**

- (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 225**

- (Topic 4)

Your organization has applications in a primary data center and a secondary warm-standby site. You want to configure Vault replication between the primary and secondary clusters. If the primary fails over to the secondary, the applications must interact with Vault without re-authenticating. What type of Vault replication would you use?

- A. Performance Replication
- B. Integrated Storage
- C. Disaster Recovery Replication
- D. Vault Secrets Operator

**Answer: C**

#### **NEW QUESTION 228**

- (Topic 4)

Which of the following is true about the token authentication method in Vault? (Select three)

- A. The token auth method is automatically enabled in Vault and cannot be disabled
- B. External authentication mechanisms, such as GitHub, are used to dynamically create tokens
- C. The token auth method is used as the first method of authentication for Vault for a newly initialized Vault node/cluster
- D. Tokens cannot be used directly; they must be used in conjunction with one of Vault's many auth methods

**Answer: ABC**

#### NEW QUESTION 230

- (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 235

- (Topic 4)

All Vault instances, or clusters, include two built-in policies that are created automatically. Choose the two policies below and the correct information regarding each policy. (Select two)

- A. The root policy is created automaticall
- B. This policy provides superuser privileges and cannot be deleted
- C. The admin policy is created automaticall
- D. It provides administrative permissions but can be deleted if needed
- E. The default policy is created automaticall
- F. This policy can be modified but not deleted
- G. The default policy is created automaticall
- H. This policy cannot be modified but it can be deleted

**Answer:** AC

#### NEW QUESTION 236

- (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 240

- (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 241

- (Topic 4)

Which core component of Vault can store, generate, or encrypt data for organizations?

- A. auth method
- B. storage backend
- C. secrets engine
- D. audit device

**Answer:** C

#### NEW QUESTION 243

- (Topic 4)

You have multiple Vault clusters in your environment, one for test and one for production. You have the CLI installed on your local machine and need to target the production cluster to make configuration changes. What environment variable can you set to target the production cluster?

- A. VAULT\_REDIRECT\_ADDR
- B. VAULT\_CLUSTER\_ADDR
- C. VAULT\_ADDR
- D. VAULT\_CAPATH

**Answer:** C

**NEW QUESTION 246**

- (Topic 5)

Security requirements demand that no secrets appear in the shell history. Which command does not meet this requirement?

- A. generate-password | vault kv put secret/password value
- B. vault kv put secret/password value-itsasecret
- C. vault kv put secret/password value=@data.txt
- D. vault kv put secret/password value-SSECRET\_VALUE

**Answer: B**

**NEW QUESTION 247**

- (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 248**

- (Topic 5)

An organization would like to use a scheduler to track & revoke access granted to a job (by Vault) at completion. What auth-associated Vault object should be tracked to enable this behavior?

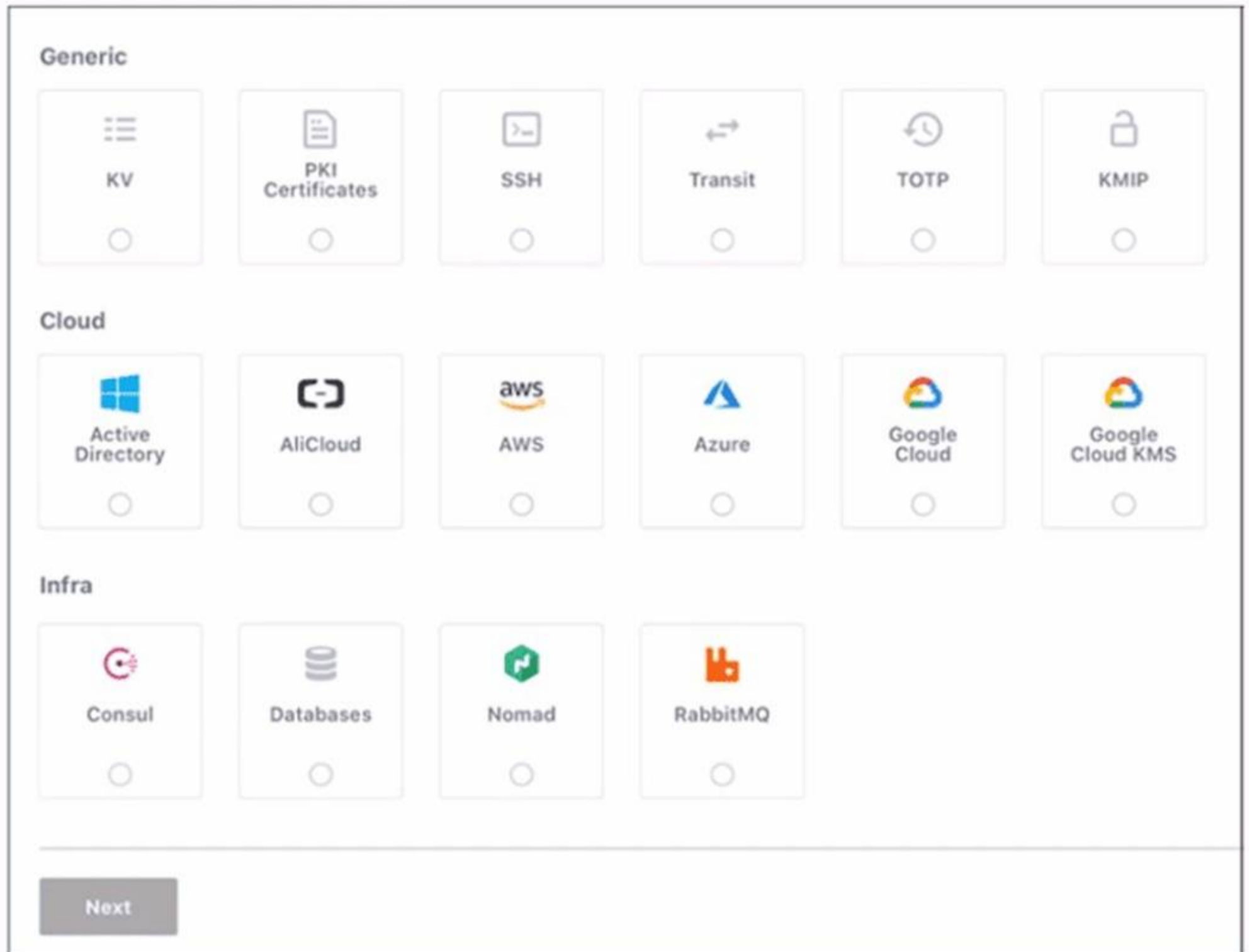
- A. Token accessor
- B. Token ID
- C. Lease ID
- D. Authentication method

**Answer: C**

**NEW QUESTION 249**

- (Topic 5)

Use this screenshot to answer the question below:



When are you shown these options in the GUI?

- A. Enabling policies
- B. Enabling authentication engines
- C. Enabling secret engines
- D. Enabling authentication methods

**Answer: D**

**NEW QUESTION 254**

- (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 256**

- (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 259**

- (Topic 5)

Which of the following describes usage of an identity group?

- A. Limit the policies that would otherwise apply to an entity in the group
- B. When they want to revoke the credentials for a whole set of entities simultaneously
- C. Audit token usage
- D. Consistently apply the same set of policies to a collection of entities

**Answer: D**

**NEW QUESTION 263**

- (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 268**

- (Topic 5)

Where can you set the Vault seal configuration? Choose two correct answers.

- A. Cloud Provider KMS
- B. Vault CLI
- C. Vault configuration file
- D. Environment variables
- E. Vault API

**Answer: CD**

**NEW QUESTION 269**

- (Topic 5)

When unsealing Vault, each Shamir unseal key should be entered:

- A. Sequentially from one system that all of the administrators are in front of
- B. By different administrators each connecting from different computers
- C. While encrypted with each administrators PGP key
- D. At the command line in one single command

**Answer: B**

**NEW QUESTION 270**

- (Topic 5)

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.AAAAAQI1WH-DExezQvz-ZGWMhzy8uWXEoQYHH60...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

**Answer: BC**

**NEW QUESTION 271**

- (Topic 5)

When looking at Vault token details, which key helps you find the paths the token is able to access?

- A. Meta
- B. Path

- C. Policies
- D. Accessor

**Answer: C**

**NEW QUESTION 276**

- (Topic 5)

You have a 2GB Base64 binary large object (blob) that needs to be encrypted. Which of the following best describes the transit secrets engine?

- A. A data key encrypts the blob locally, and the same key decrypts the blob locally.
- B. To process such a large blob
- C. Vault will temporarily store it in the storage backend.
- D. Vault will store the blob permanently
- E. Be sure to run Vault on a compute optimized machine
- F. The transit engine is not a good solution for binaries of this size.

**Answer: D**

**NEW QUESTION 280**

- (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 283**

- (Topic 5)

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

**Answer: D**

**NEW QUESTION 285**

HOTSPOT - (Topic 5)

Where do you define the Namespace to log into using the Vault UI? To answer this question

Use your mouse to click on the screenshot in the location described above. An arrow indicator will mark where you have clicked. Click the "Answer" button once you have positioned the arrow to answer the question. You may need to scroll down to see the entire screenshot.

# Sign in to Vault

Namespace

Method

Username

Password

[^ Hide options](#)

Mount path

**i** If this backend was mounted using a non-default path, enter it here.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

# Sign in to Vault

**Namespace**

**Method**

**Username**

**Password**

[^ Hide options](#)

**Mount path**

**i** If this backend was mounted using a non-default path, enter it here.

**NEW QUESTION 286**

- (Topic 5)

A developer mistakenly committed code that contained AWS S3 credentials into a public repository. You have been tasked with revoking the AWS S3 credential that was in the code. This credential was created using Vault's AWS secrets engine and the developer received the following output when requesting a credential from Vault.

```

Key          Value
---          -
lease_id     aws/creds/s3-access/f3e92392-7d9c-09c8-c921-575d62fe80d8
lease_duration 768h
lease_renewable true
access_key   AKIAI0WQXTLW36DV7IEA
secret_key   iASuXNKcWKFtb08Ef0vOcgtiL6knR20EJkJTH8WI
    
```

Which Vault command will revoke the lease and remove the credential from AWS?

- A. vault lease revoke aws/creds/s3-access/f3e92392-7d9c-99c8-c921-57Sd62fe89d8
- B. vault lease revoke AKIAI0WQXTLW36DV7IEA
- C. vault lease revoke f3e92392-7d9c-09c8-c921-575d62fe80d8

D. vault lease revoke access\_key-AKIAI0WQXTLW36DV7IEA

Answer: A

#### NEW QUESTION 288

- (Topic 5)

The key/value v2 secrets engine is enabled at secret/ See the following policy:

```
path "secret/data/*" {
  capabilities = ["create", "read", "update", "delete", "list"]
}

path "secret/data/super-secret" {
  capabilities = ["deny"]
}
```

Which of the following operations are permitted by this policy? Choose two correct answers.

- A. vault kv get secret/webapp1
- B. vault kv put secret/webapp1 apikey-"ABCDEFGHJI] K123M"
- C. vault kv metadata get secret/webapp1
- D. vault kv delete secret/super-secret
- E. vault kv list secret/super-secret

Answer: AC

#### NEW QUESTION 289

- (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 293

- (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 296

- (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 300

.....

## **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](#)**