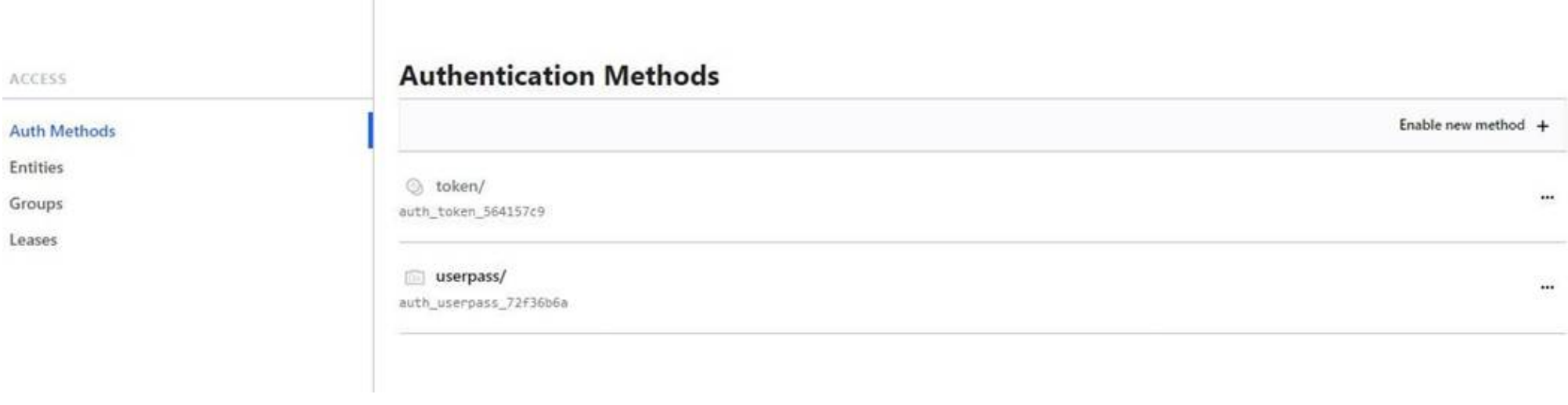
HashiCorp

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

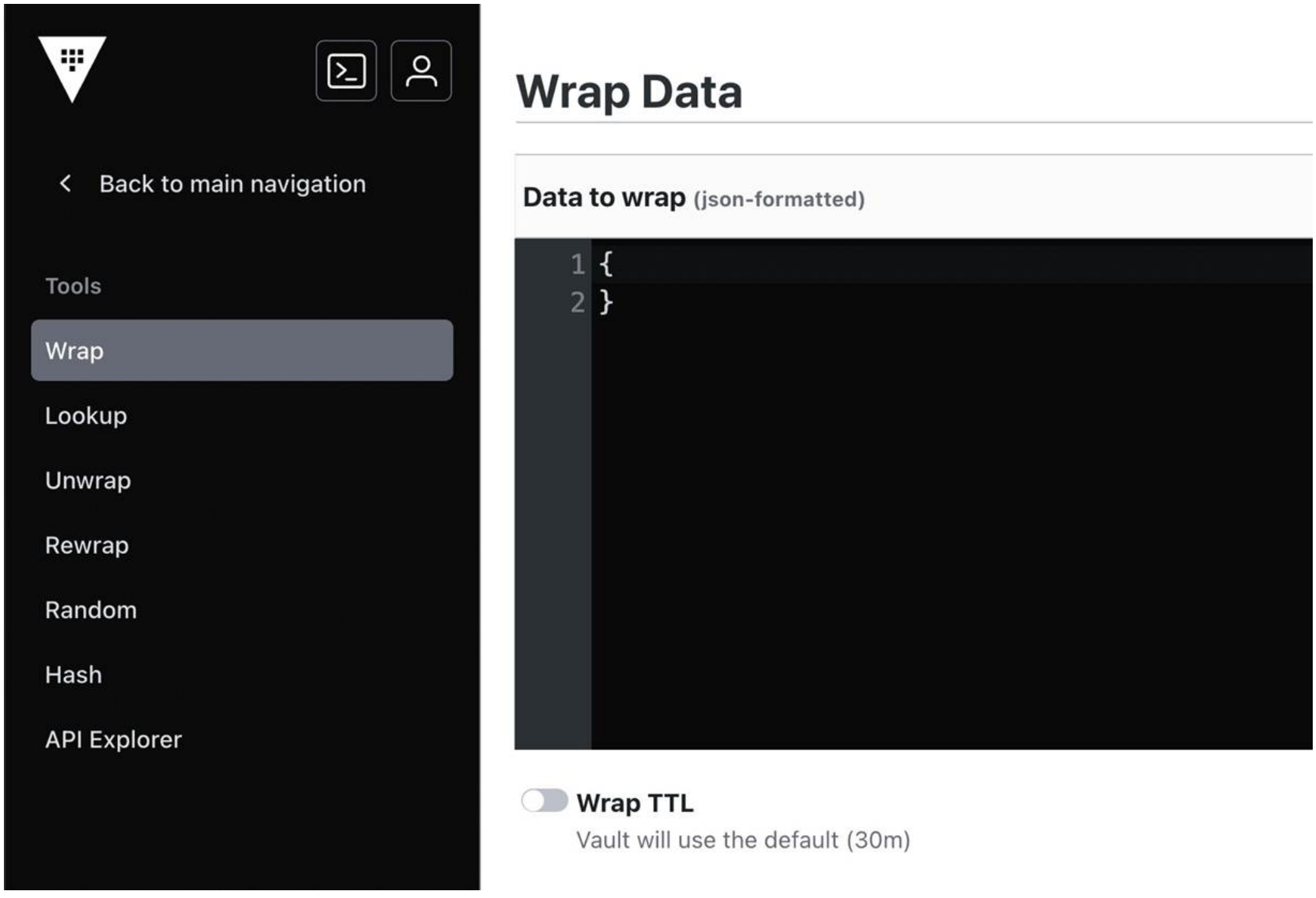
Answer: B

NEW QUESTION 2
- (Topic 1)
From the unseal options listed below, select the options you can use if you're deploying Vault on-premises (select four).

A. Certificates
B. Transit
C. AWS KMS
D. HSM PKCS11
E. Key shards

Answer: BCDE

NEW QUESTION 3
- (Topic 1)
What could you do with the feature found in the screenshot below (select two)?



A. Using a short TTL, you could encrypt data in order to place only the encrypted data in Vault
B. Encrypt the Vault master key that is stored in memory
C. Encrypt sensitive data to send to a colleague over email
D. Use response-wrapping to protect data

Answer: CD

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

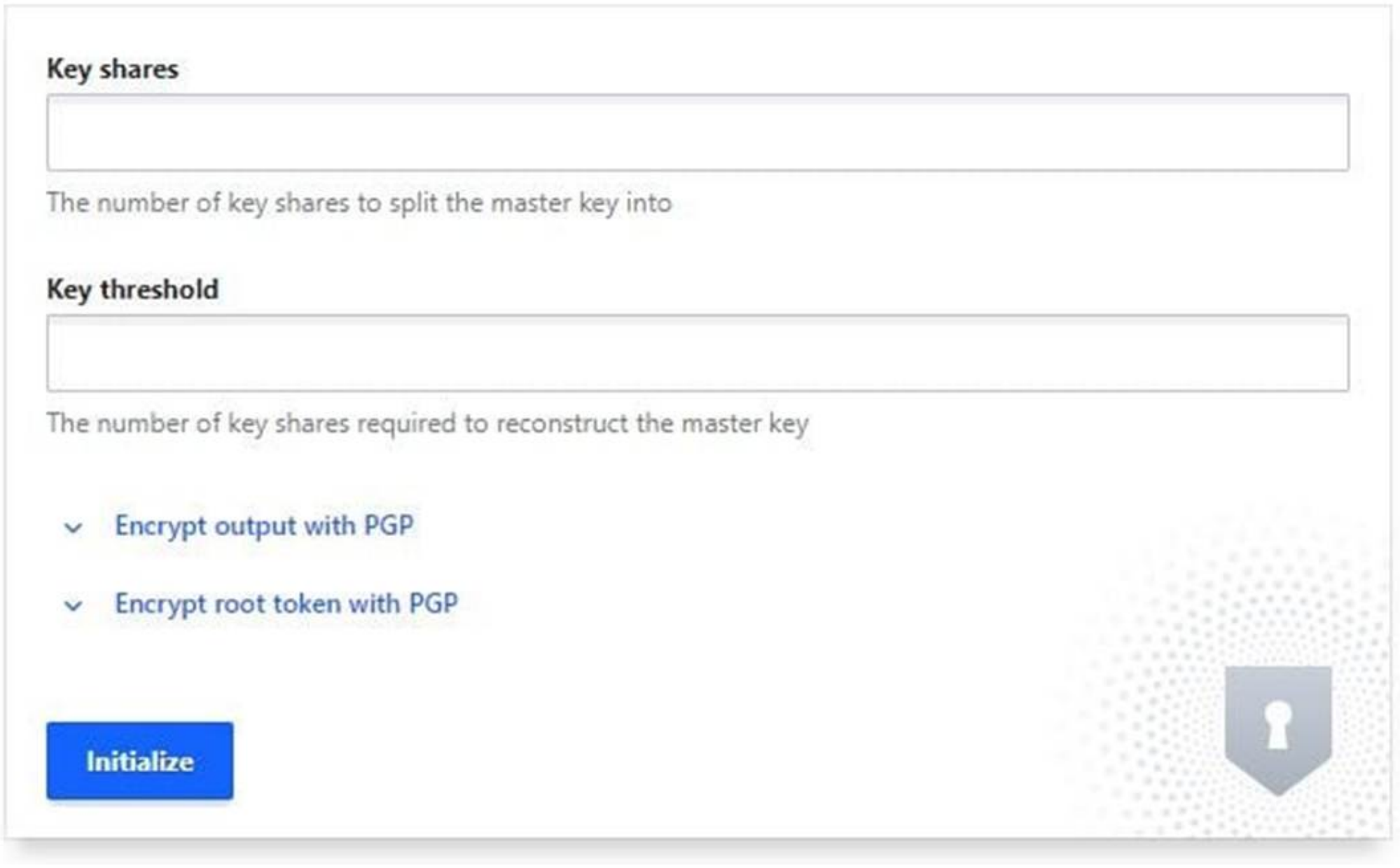
Answer: A

NEW QUESTION 5
- (Topic 1)
In regards to the Transit secrets engine, which of the following is true given the following command and output (select three):
$ vault write encryption/encrypt/creditcard plaintext=$(base64 <<< "1234 5678 9101 1121") Key: ciphertext Value:
vault:v3:cZNHVx+sxdMErXRSuDa1q/pz49fXTn1PScKfhf+PIZPvy8xKfkytpwKcbC0fF2U=

A. The Transit secrets engine is mounted at the encryption path
B. The name of the keyring used to encrypt the data is creditcard
C. There are at least three data keys associated with this keyring
D. The data was written to the encryption path, which is provided by default when enabling the Transit secrets engine

Answer: ABC

NEW QUESTION 6
- (Topic 1)
You??ve hit the URL for the Vault UI, but you??re presented with this screen. Why doesn??t Vault present you with a way to log in?



A. The Consul storage backend was not configured correctly
B. Vault needs to be initialized before it can be used
C. A Vault policy is preventing you from logging in
D. The Vault configuration file has an incorrect configuration

Answer: B

NEW QUESTION 7
- (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 8
- (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 9
- (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)
True or False? When encrypting data with the Transit secrets engine, Vault always stores the ciphertext in a dedicated KV store along with the associated encryption key.

A. True
B. False

Answer: B

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 15
- (Topic 1)
When configuring Vault replication and monitoring its status, you keep seeing something called 'WALs'. What are WALs?

A. Warning of allocated logs
B. Write along logging
C. Write-ahead logs
D. Wake after LAN

Answer: C

NEW QUESTION 19
- (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 22
- (Topic 1)
What command would have created the token displayed below?
$ vault token lookup hvs.nNeZ2I64ALCxuO7dqQEJGPrO
Key: policies Value: [default dev], num_uses: 5, ttl: 767h59m49s
? Key Value
? --- -----
? accessor mfvaVMFgOcXHIeqlRasroSOn
? 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.nNeZ2I64ALCxuO7dqQEJGPrO
? 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 25
- (Topic 1)
You are deploying Vault in a local data center, but want to be sure you have a secondary Vault cluster in the event the primary cluster goes offline. In the

secondary data center, you have applications that are running, as they are architected to run active/active. Which type of replication would be best in this scenario?

A. Disaster Recovery replication
B. Performance replication

Answer: B

NEW QUESTION 30
- (Topic 1)
After encrypting data using the Transit secrets engine, you??ve received the following output. Which of the following is true based on the output displayed below?
Key: ciphertext Value: vault:v2:45f9zW6cglbrzCjI0yCyC6DBYtSBSxnMgUn9B5aHcGEit71xefPEmmjMbrk3

A. The original encryption key has been rotated at least once
B. The data is stored in Vault using a KV v2 secrets engine
C. This is the second version of the encrypted data
D. Similar to the KV secrets engine, the Transit secrets engine was enabled using the transit v2 option

Answer: A

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 38
- (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 scenario most strongly indicates a need to run a self-hosted Vault cluster instead of using HCP Vault Dedicated?

A. Your organization doesn??t require any custom security policies or intricate network topologies
B. You want to offload all operational tasks and rely on HashiCorp to manage patching, upgrades, and infrastructure
C. You prefer a fully managed environment that is readily scalable with minimal configuration overhead
D. You must maintain specific compliance or custom integration requirements that demand full control over the Vault environment, including infrastructure provisioning and plugin development

Answer: D

NEW QUESTION 44
- (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:cZNHVx+sxdMEr....." Key: plaintext Value: Y3JlZGl0LWNhcmQtbnVtYmVyCg==

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 49
- (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 53
- (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 55
- (Topic 2)
When generating a dynamic secret, what value is returned that a user can use to renew or revoke the lease?

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

Answer: D

NEW QUESTION 56
- (Topic 2)
Using the Vault CLI, there are several ways to create a new policy. Select the valid commands (Select three)

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: ACD

NEW QUESTION 58
- (Topic 2)
Your application cannot manage authentication with Vault, but it can communicate with a local service to retrieve secrets. What solution can enable your app to generate dynamic credentials from Vault?

A. Vault Proxy with caching feature enabled
B. Vault Agent with environment variable secret injection
C. Vault Proxy with Auto-Auth feature enabled
D. Vault Agent with the templating feature configured

Answer: C

NEW QUESTION 61
- (Topic 2)
An application requires a specific key/value pair to be updated in order to process a batch job. Thevalue 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 63
- (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 67

- (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 69
- (Topic 2)
Which statement best explains the role and usage of storage backends in HashiCorp Vault?

A. They store Vault??s persistent data, affecting the scalability and performance of managing Vault.
B. They handle the encryption of all secrets so that Vault remains completely stateless.
C. They store only ephemeral tokens, ensuring no persistent data is ever saved.
D. They store only unseal keys, while all secret data remains in Vault??s memory.

Answer: A

NEW QUESTION 71
- (Topic 2)
What is the result of the following Vault command?
$ vault auth enable kubernetes

A. Allows Vault to access usernames and passwords stored in a Kubernetes cluster
B. Mounts the Kubernetes auth method to the default path of kubernetes/
C. Imports Kubernetes secrets to the local KV database
D. Enables Vault to host an IdP for Kubernetes workloads

Answer: B

NEW QUESTION 74
- (Topic 2)
True or False? To prepare for day-to-day operations, the root token should be safely saved outside of Vault in order to administer Vault.

A. True
B. False

Answer: B

NEW QUESTION 76
- (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 81
- (Topic 2)
You need to connect to and manage a new HCP Vault cluster using the Vault CLI on your laptop. What environment variables should you set to establish connectivity?

A. VAULT_CLIENT_KEY=<path-to-key-file>, VAULT_TOKEN=<token-here>
B. VAULT_NAMESPACE=root, VAULT_REDIRECT_ADDR=<cluster-address>
C. VAULT_ADDR=https://<cluster-address>:8200, VAULT_NAMESPACE=admin
D. VAULT_TOKEN=<token-here>, VAULT_CLUSTER_ADDR=https://<cluster- address>:8200

Answer: C

NEW QUESTION 86
- (Topic 2)
Which of the following is not an action associated with the Transit secrets engine when interacting with data?

A. encrypt
B. decrypt
C. rewrap
D. update

Answer: D

NEW QUESTION 88
- (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 92
- (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 95
- (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 99
- (Topic 2)
Which two characters can be used when writing a policy to reflect a wildcard or path segment? (Select two)

A. The ampersand &
B. The at symbol @
C. The splat character *
D. A dollar sign $
E. The pound symbol #
F. The plus symbol +

Answer: CF

NEW QUESTION 102
- (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 107
- (Topic 2)
Which auth method is ideal for machine-to-machine authentication?

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

Answer: D

NEW QUESTION 112
- (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 115
- (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 116
- (Topic 2)
An application is trying to use a dynamic secret in which the lease has expired. What can be done in order for the application to successfully request data from Vault?

A. Try the expired secret in hopes it hasn??t been deleted yet
B. Perform a lease renewal
C. Request a new secret and associated lease
D. Request the TTL be extended for the secret lease

Answer: C

NEW QUESTION 118
- (Topic 2)
Which isnota capability that can be used when writing a Vault policy?

A. delete
B. modify
C. create
D. list
E. read
F. update

Answer: B

NEW QUESTION 122
- (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 127
- (Topic 2)
Your organization wants to set up human-based authentication for AzureAD. What authentication method should you enable and configure for Vault?

A. OIDC/JWT
B. Okta
C. Active Directory
D. UserPass

Answer: A

NEW QUESTION 128
- (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 133
- (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

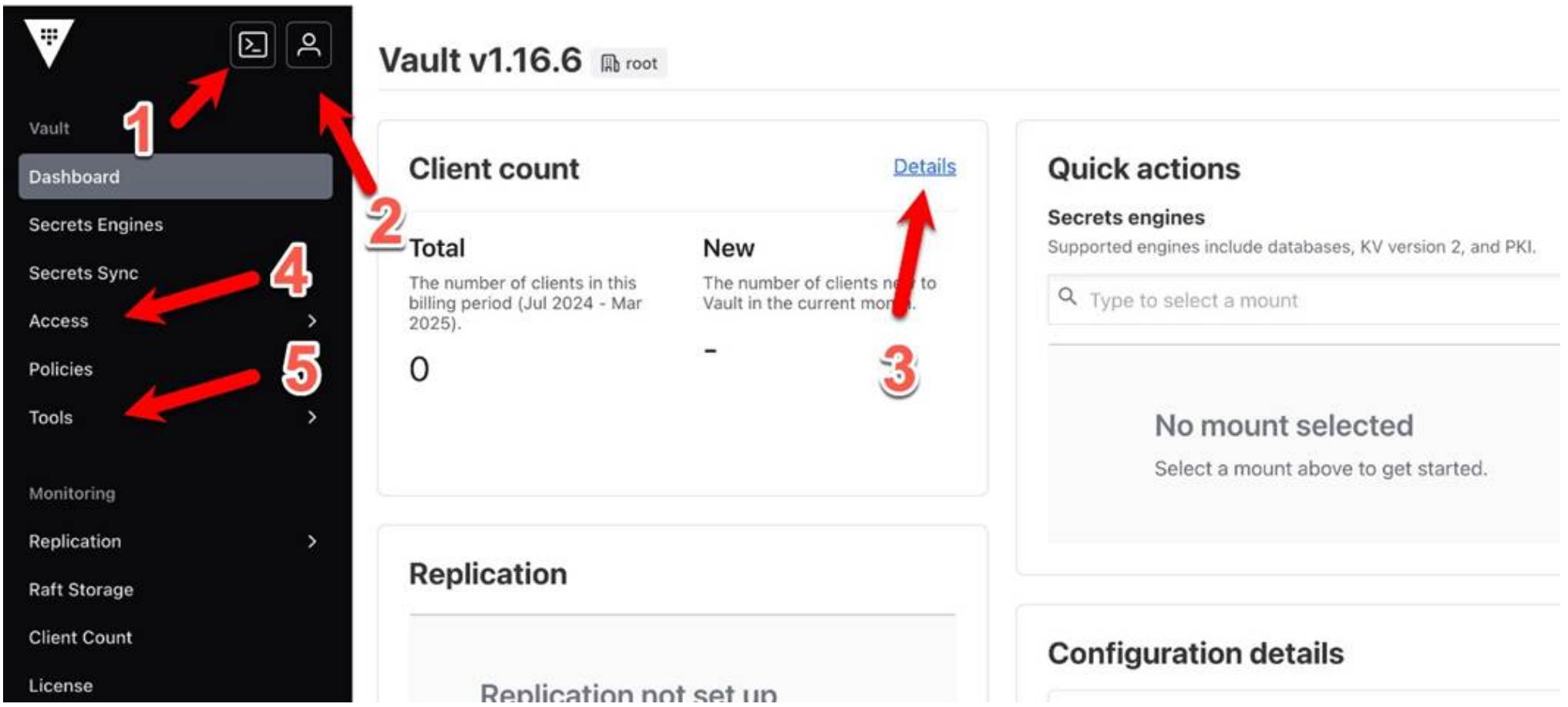
Answer: BCD

NEW QUESTION 135
- (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 137
- (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 141
- (Topic 2)
You need to write a Vault operator policy and give the users access to perform administrative actions in Vault. What path is used for Vault backend functions?

A. /security
B. /admin
C. /vault
D. /system
E. /sys
F. /backend

Answer: E

NEW QUESTION 143

- (Topic 2)
An application has authenticated to Vault and has obtained dynamic database credentials with a lease of 4 hours. Four hours later, the credentials expire, and the application can no longer communicate with the backend database, so the application goes down. What should the developers instruct the application to do to prevent this from happening again while maintaining the same level of security?

A. Go back to using static credentials
B. Renew the lease before expiration
C. Revoke the lease before expiration
D. Use a different auth method

Answer: B

NEW QUESTION 145
- (Topic 3)
True or False? The root and default policies can be deleted if they are not needed or being used.

A. True
B. False

Answer: B

NEW QUESTION 146
- (Topic 3)
What command can be used to revoke all leases associated with a database role named prod-mysql?

A. vault lease revoke database/role/prod-mysql
B. vault lease revoke -prefix database/creds/prod-mysql
C. vault revoke database/role/prod-mysql
D. vault lease revoke database/creds/prod-mysql

Answer: B

NEW QUESTION 149
- (Topic 3)
Tom needs to set the proper environment variable so he doesn??t need to first authenticate to Vault toretrieve 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 154
- (Topic 3)
Julie is a developer who needs to ensure an application can properly renew its lease for AWS credentials it uses to access data in an S3 bucket. Although the application would generally use the API, what is the equivalent CLI command to perform this action?

A. vault renew aws/roles/s3-read-only/39e6b9a2-296-83d9-2fe0-c11e846bdc99
B. vault lease renew aws/creds/s3-read-only/39e6b9a2-296-83d9-2fe0-c11e846bdc99
C. vault lease renew aws/roles/s3-read-only/39e6b9a2-296-83d9-2fe0-c11e846bdc99
D. vault lease renew aws/creds/s3-read-only

Answer: B

NEW QUESTION 158
- (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 160
- (Topic 3)
True or False? A token can be renewed up until the max TTL, even if the TTL has been reached.

A. True
B. False

Answer: B

NEW QUESTION 162
- (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 166
- (Topic 3)
After setting up a new HashiCorp Vault server with the default configurations, which method can be used to unseal Vault?

A. Log on to each Vault node and provide the root token
B. Running vault operator init to regenerate unseal keys and automatically unseal the Vault
C. Submit a threshold of unseal keys to reconstruct the root key
D. Restart the Vault service, which will automatically unseal it

Answer: C

NEW QUESTION 170
- (Topic 3)
True or False? You can create and update Vault policies using the UI.

A. True
B. False

Answer: A

NEW QUESTION 175
- (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 179
- (Topic 3)
Tom is authenticating to Vault using the CLI. Which of the following commands allows Tom to authenticate using the userpass method WITHOUT logging his password to the shell history?

A. vault login tom
B. vault login -method=userpass username=tom
C. vault login userpass username=tom password=jerry
D. vault login -method=userpass username=tom password=jerry

Answer: B

NEW QUESTION 181
- (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 186
- (Topic 3)
You are considering using HCP Vault Dedicated but are concerned about differences between a hosted version and a self-hosted deployment. Which of the following statements is true about HCP Vault Dedicated?

A. HCP Vault Dedicated provides a similar experience to self-hosted Vault Enterprise because it uses the same Vault binary
B. HCP Vault Dedicated can be deployed on any cloud provider, including AWS, Azure, and Google Cloud, with full multi-cloud support
C. HCP Vault Dedicated requires different CLI commands and APIs compared to self- hosted Vault Enterprise
D. HCP Vault Dedicated is currently limited to a single region and cannot be deployed across multiple regions

Answer: A

NEW QUESTION 191
- (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 194
- (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 196
- (Topic 3)
You need to create a limited-privileged token that isn??t impacted by the TTL of its parent. What type of token should you create?

A. Service token with a use limit
B. Orphan token
C. Periodic token
D. Root token

Answer: B

NEW QUESTION 199
- (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 202
- (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 203
- (Topic 3)
Which of the following features in Vault will replicate service tokens between clusters?

A. Disaster Recovery Replication
B. Performance Replication
C. Vault Agent
D. Integrated Storage

Answer: A

NEW QUESTION 206
- (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 208
- (Topic 3)
Which of the following are supported auth methods for Vault? (Select six)

A. AWS
B. Kubernetes
C. Token
D. OIDC/JWT
E. Userpass
F. Cubbyhole
G. AppRole

Answer: ABCDEG

NEW QUESTION 213
- (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 214
- (Topic 3)
A DevOps engineer has set up LDAP and GitHub auth methods. The engineer must ensure user Sarah, who authenticates via either method, has consistent access permissions. Which approach correctly describes how to achieve this in Vault?

A. Create an entity for Sarah and map both her LDAP and GitHub identities as entity aliases to this single entity
B. Create an external group and add the LDAP and GitHub providers as members of the group
C. Create separate policies for each auth method and manually ensure they remain synchronized
D. Configure a trust relationship between the LDAP and GitHub providers to ensure Sarah??s account is synced

Answer: A

NEW QUESTION 216
- (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 219
- (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 221
- (Topic 3)
You have multiple Kubernetes pods that need frequent access to Vault to retrieve credentials for establishing connectivity to a backend database. You enable the Kubernetes auth method in Vault. What resource do you need to create within Kubernetes to complete this configuration?

A. Username and password for kubectl
B. k8s service account token
C. A Vault token for authentication
D. An AppRole role_id and secret_id

Answer: B

NEW QUESTION 222
- (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 aGFzaGljb3JwIGNlcnRpZmllZDogdmF1bHQgYXNzb2NpYXRl

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 223
- (Topic 3)
True or False? Once you authenticate to Vault using the API, subsequent requests will automatically be permitted without further interaction.

A. True
B. False

Answer: B

NEW QUESTION 228
- (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

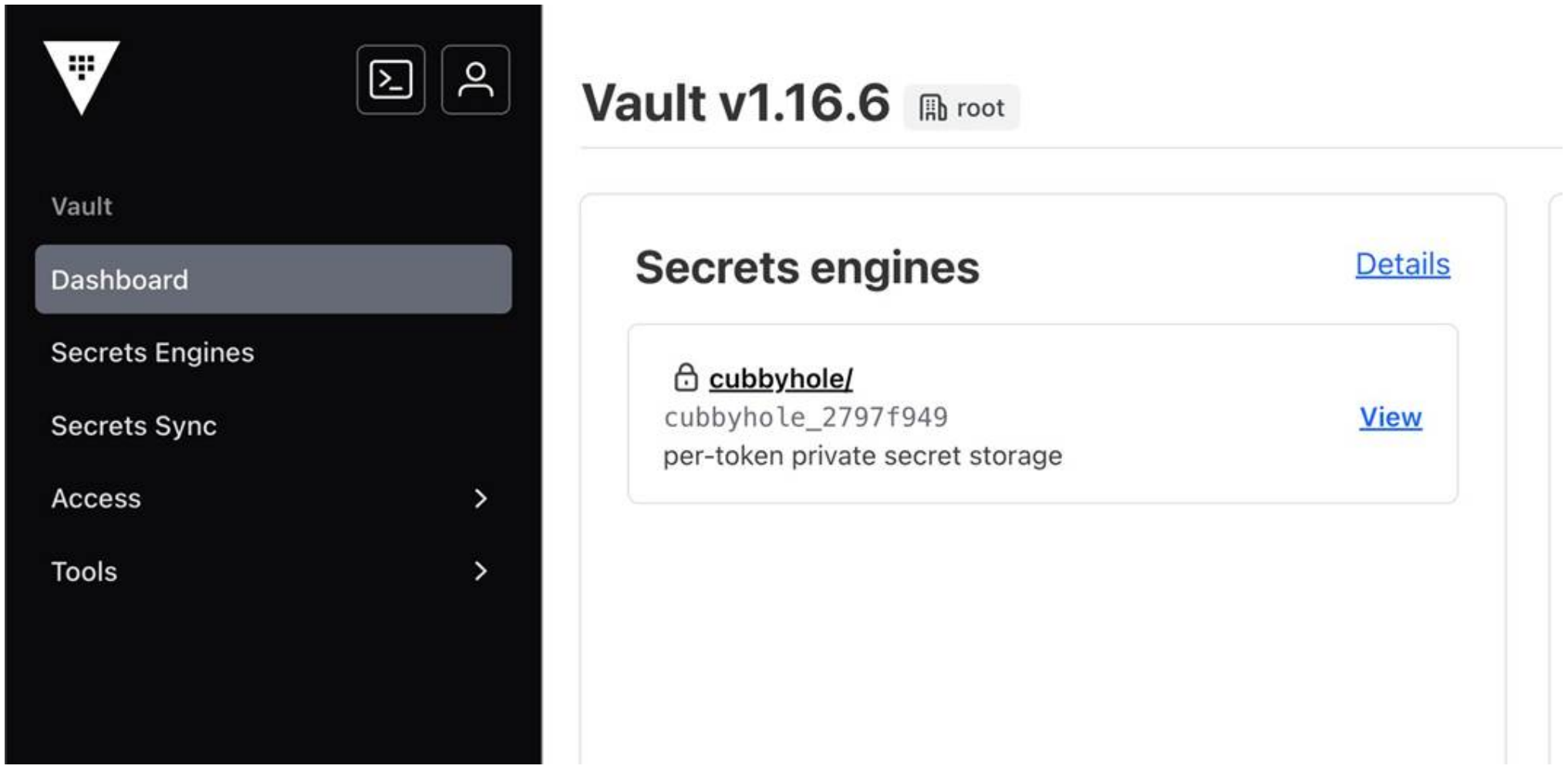
Answer: AD

NEW QUESTION 230
- (Topic 4)
A new application is being provisioned in your environment. The application requires the generation of dynamic credentials against the Oracle database in order to read reporting data. Which is the best auth method to use to permit the application to authenticate to Vault?

A. OIDC
B. GitHub
C. Userpass
D. AppRole

Answer: D

NEW QUESTION 235
- (Topic 4)
A developer has requested access to manage secrets at the path kv/apps/webapp01. You create the policy below which gives them the proper access:
path "kv/apps/webapp01" {
capabilities = ["read", "create", "update", "list"]
}
However, when the developer logs in to the Vault UI, they see the following screenshot and cannot access the desired secret. Why can??t the developer see the secrets they need?



A. The Vault UI isn??t enabled for the developer, therefore they will only see the default options
B. The key/value secrets engine isn??t available in the Vault UI, therefore the developer should use a different Vault interface instead
C. The policy doesn??t permit list access to the paths prior to the secret so the Vault UI doesn??t display the mount path
D. The secrets are stored under the cubbyhole secrets engine, so the developer should browse to that secrets engine

Answer: C

NEW QUESTION 239
- (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

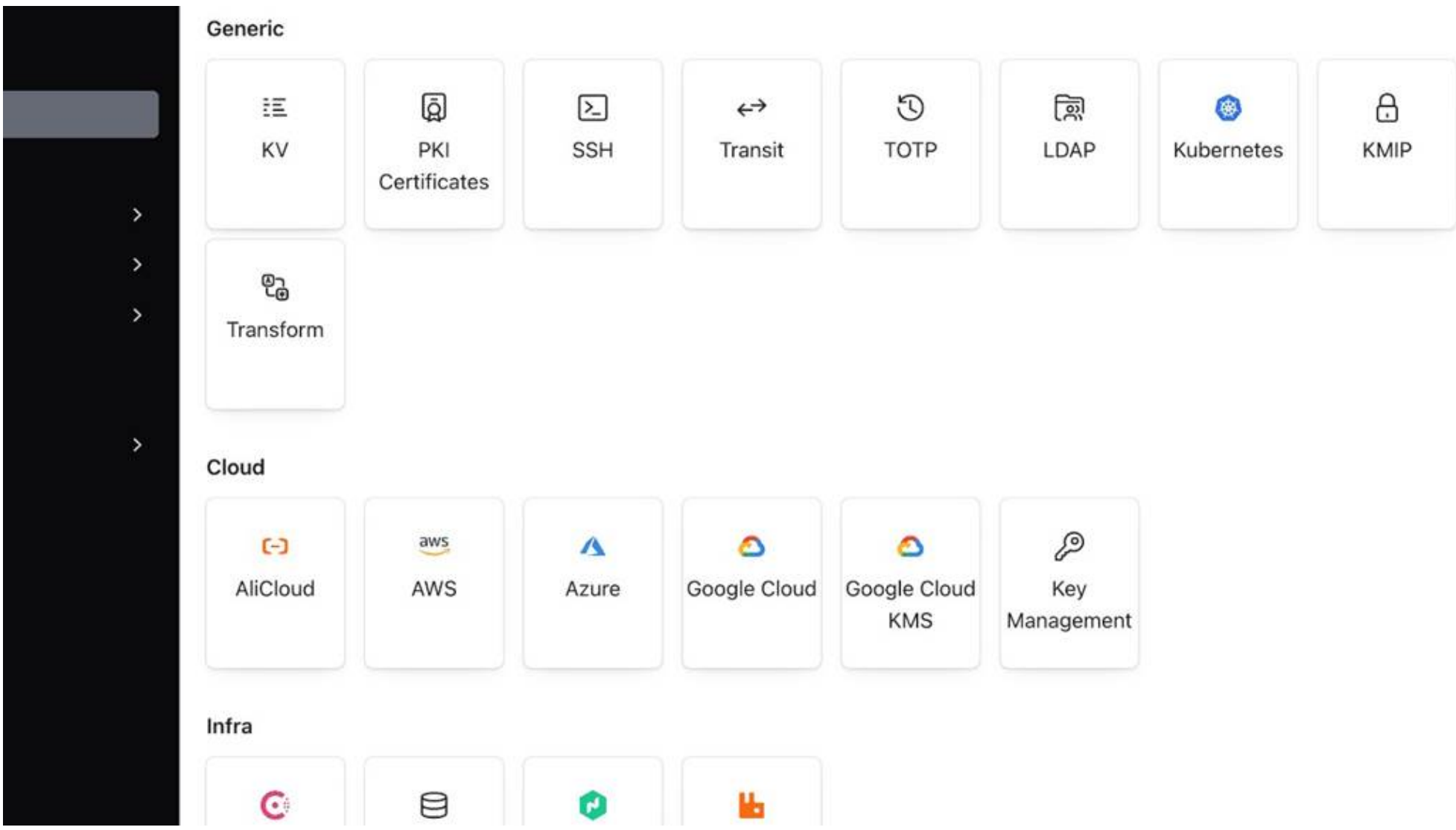
Answer: CDEF

NEW QUESTION 240
- (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 244
- (Topic 4)
You have logged into the Vault UI and see this screen. What Vault component is being enabled in the screenshot below?



A. Storage Backends
B. Secrets Engine
C. Auth Methods
D. Audit Devices

Answer: B

NEW QUESTION 249
- (Topic 4)
You are configuring your application to retrieve a new PKI certificate upon provisioning. The Vault admins have given you an AppRole role-id and secret-id to inject into the CI/CD pipeline job that provisions your app. The application uses the credentials to successfully authenticate to Vault using the API. Which of the following is true about the step next required after authenticating to Vault?

A. The client token needs to be retrieved from the API response before requesting the new PKI certificate
B. The initial API response should include the new PKI certificate and no further action is required
C. The app still needs to use the role-id and secret-id to request the new PKI certificate via API
D. Now that the app is authenticated, it can simply make another API request for the PKI certificate

Answer: A

NEW QUESTION 251
- (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 254
- (Topic 4)
Your team uses the Transit secrets engine to encrypt all data before writing it to a MySQL database server. During testing, you manually retrieve ciphertext from the database and decrypt it to ensure the data can be read. After decrypting the data, you are worried something is wrong because the plaintext data isn??t legible. Why can you not read the original plaintext data after decrypting the ciphertext?
? $ vault write transit/decrypt/krausen-key ciphertext=vault:v1:8SDd3WHDOjf7mq69C.....
? Key Value
? --- -----
? plaintext Zml2ZSBzdGFyIHByYWN0aWNlIGV4YW1zIGJ5IGJyeWFuIGtyYXVzZW4=

A. The incorrect key was selected when decrypting the ciphertex
B. Use the correct key to successfully read the data
C. The incorrect key version was used to decrypt the dat
D. Update the ciphertext and change the v1 to v3 to use the latest key version
E. The plaintext is Base64 encode

F. Decode the plaintext to see the original data
G. The data was also encrypted on the databas
H. Therefore Vault cannot decrypt the original data

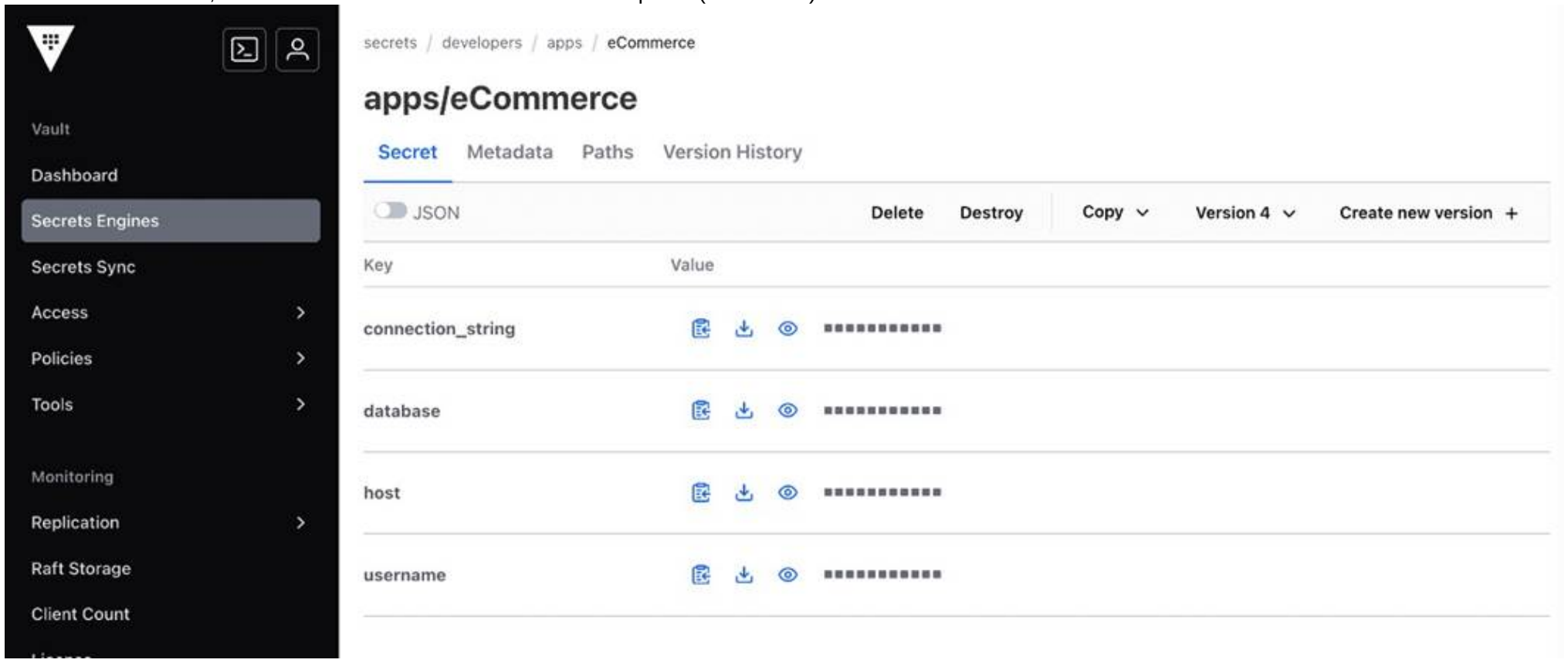
Answer: C

NEW QUESTION 259
- (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 260
- (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)



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 261
- (Topic 4)
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?

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

NEW QUESTION 266
- (Topic 4)
You need to write a new policy for Vault for a group of users on the automation team. The requirements stipulate that each user (and all future users) get access to their own private section of a KV secrets engine at the path kv/team/ and be able to manage their own secrets. Which policy below meets these requirements while minimizing the administrative effort and following the principle of least privilege?

A. path "secret/data/groups/{{identity.groups.ids.2f62-9503-42aa7A869741.name}}/" { capabilities = ["list"] }
B. path "kv/team/frank/" { capabilities = ["create", "update", "read", "delete"] } path "kv/team/steve/" { capabilities = ["create", "update", "read", "delete"] } path "kv/team/bryan/ " { capabilities = ["create", "update", "read", "delete"] }
C. path "kv/team/" { capabilities = ["create", "update", "read", "delete"] }

D. path "kv/team/{{identity.entity.id}}/" { capabilities = ["create", "update", "read", "delete"] } path "kv/team/{{identity.entity.id}}" { capabilities = ["create", "update", "read", "delete"] }

Answer: D

NEW QUESTION 269
- (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 274
- (Topic 4)
Your organization audited an essential application and found it isn??t securely storing data. For added security, auditors recommended encrypting all data before storing it in a backend database, and the application server should not store encryption keys locally. Which secrets engine meets these requirements?

A. PKI secrets engine
B. SSH secrets engine
C. Transit secrets engine
D. Cubbyhole secrets engine

Answer: C

NEW QUESTION 279
- (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 284
- (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 285
- (Topic 4)
You are using Vault to generate dynamic credentials for a Microsoft SQL server to perform queries for a month-end report. The report seems to be taking much longer than expected due to degradation on the underlying server, and you are afraid that Vault might automatically revoke the credentials. How can you extend the time the credentials are valid to ensure your month-end query is successful?

A. Renew the lease
B. Generate a new lease
C. Create a new role within the secrets engine for the database
D. Revoke the lease

Answer: A

NEW QUESTION 290
- (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 291
- (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 294
- (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.CbzCNJCVWt63jyzyaJakgDwz" https://vault.krausen.com:8200/v1/secret/cloud/azure/subscription
C. curl --header "X-Vault-Token: hvs.CbzCNJCVWt63jyzyaJakgDwz"https://vault.krausen.com:8200/v1/secret/data/cloud/az ure/subscription
D. curl --header "X-Vault-Token: hvs.CbzCNJCVWt63jyzyaJakgDwz" https://vault.krausen.com:8200/secret/data/cloud/azure/subscription/latest

Answer: C

NEW QUESTION 297
- (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 302
- (Topic 4)
True or False? Performing a rekey operation using the vault operator rekey command creates new unseal/recovery keys as well as a new root key?

A. True
B. False

Answer: B

NEW QUESTION 304
- (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

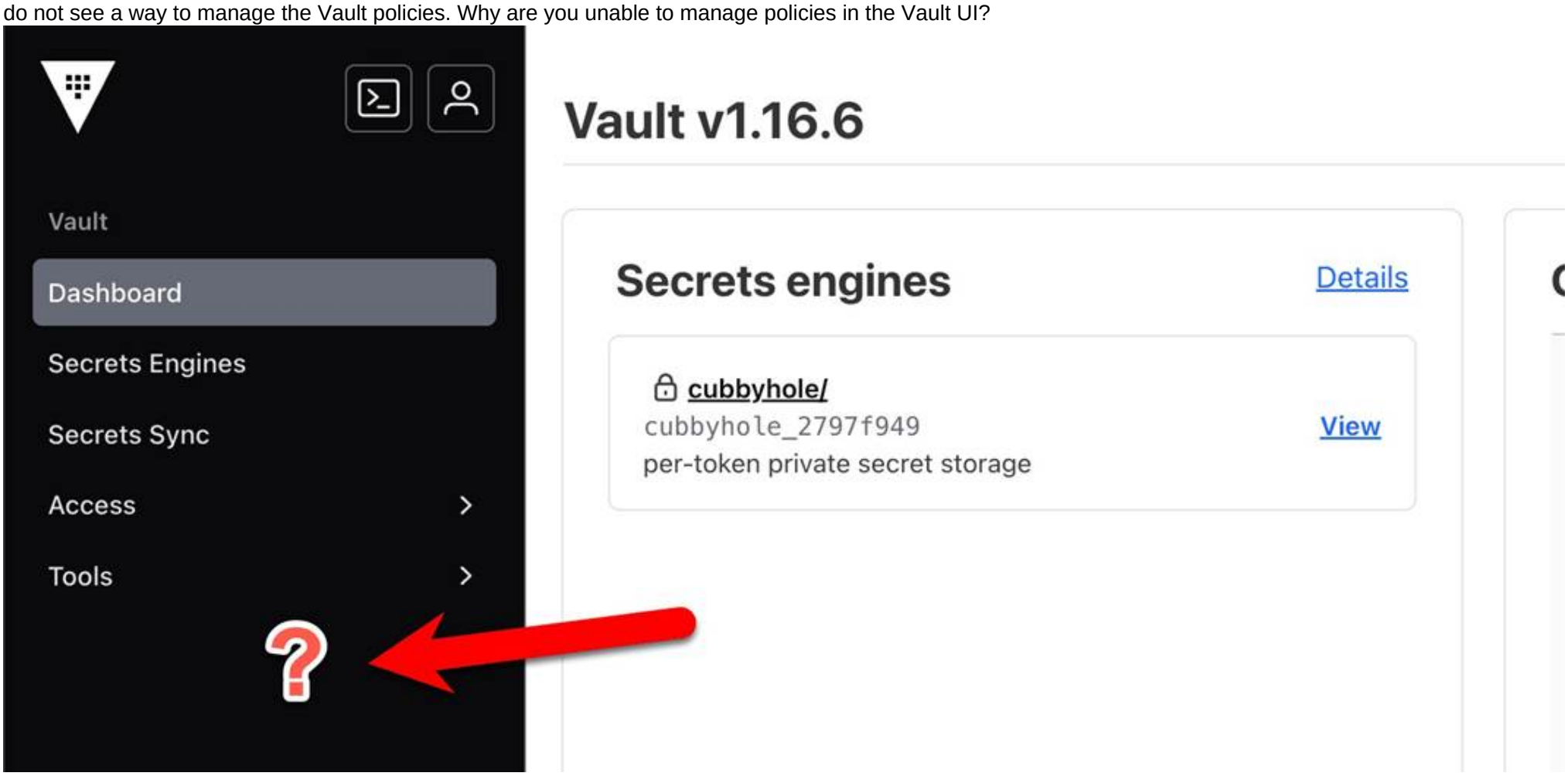
Answer: C

NEW QUESTION 309
- (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 310
- (Topic 4)
Your supervisor has requested that you log into Vault and update a policy for one of the development teams. You successfully authenticated to Vault via OIDC but do not see a way to manage the Vault policies. Why are you unable to manage policies in the Vault UI?



A. Policies are only available on Vault Enterprise
B. The Vault node is sealed, and therefore you cannot manage policies
C. Policies cannot be managed in the UI, only the CLI and API
D. The policy associated with your login does not permit access to manage policies

Answer: D

NEW QUESTION 312
- (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 317
- (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

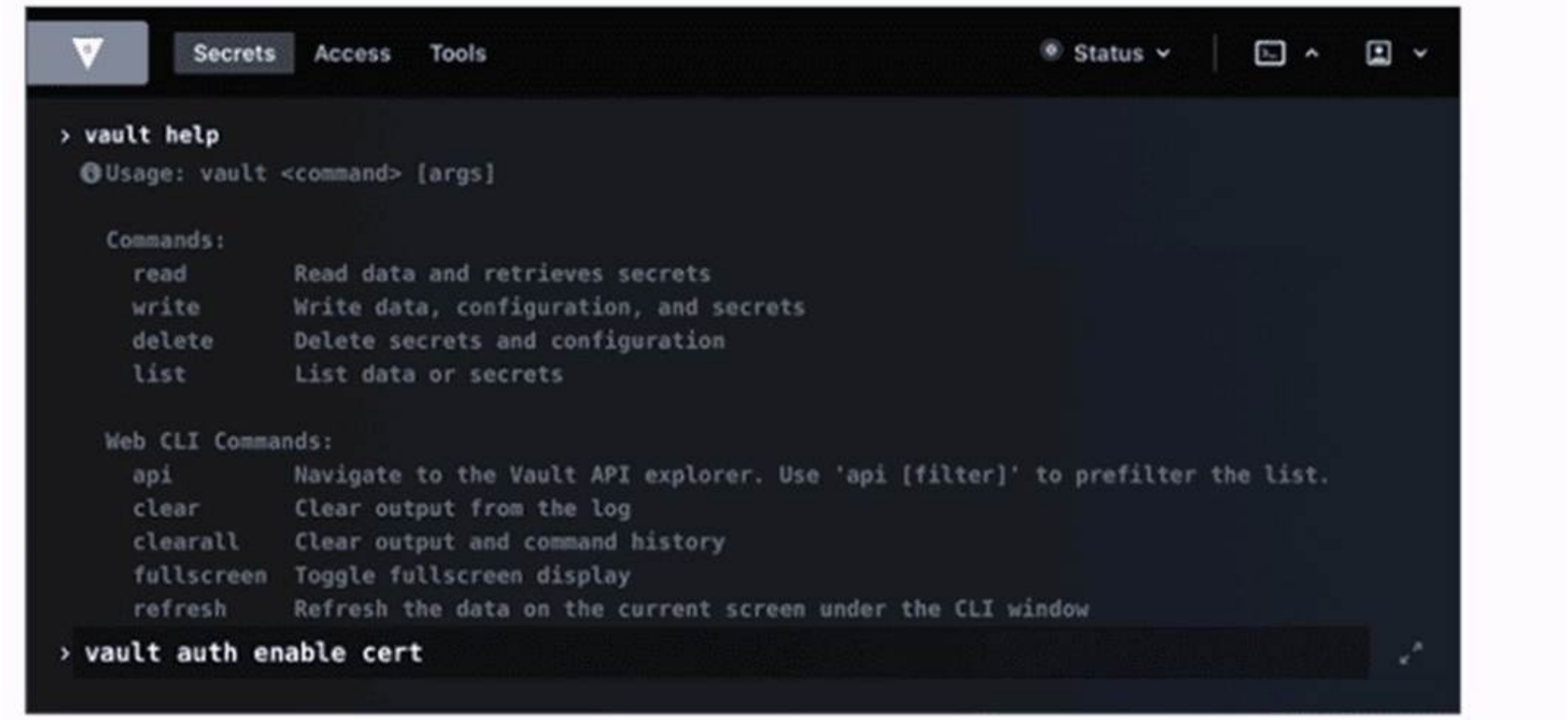
NEW QUESTION 318
- (Topic 5)
Which of the following statements are true about Vault policies? Choose two correct answers.

A. The default policy can not be modified
B. You must use YAML to define policies
C. Policies provide a declarative way to grant or forbid access to certain paths and operations in Vault
D. Vault must be restarted in order for a policy change to take an effect
E. Policies deny by default (empty policy grants no permission)

Answer: CE

NEW QUESTION 320
- (Topic 5)

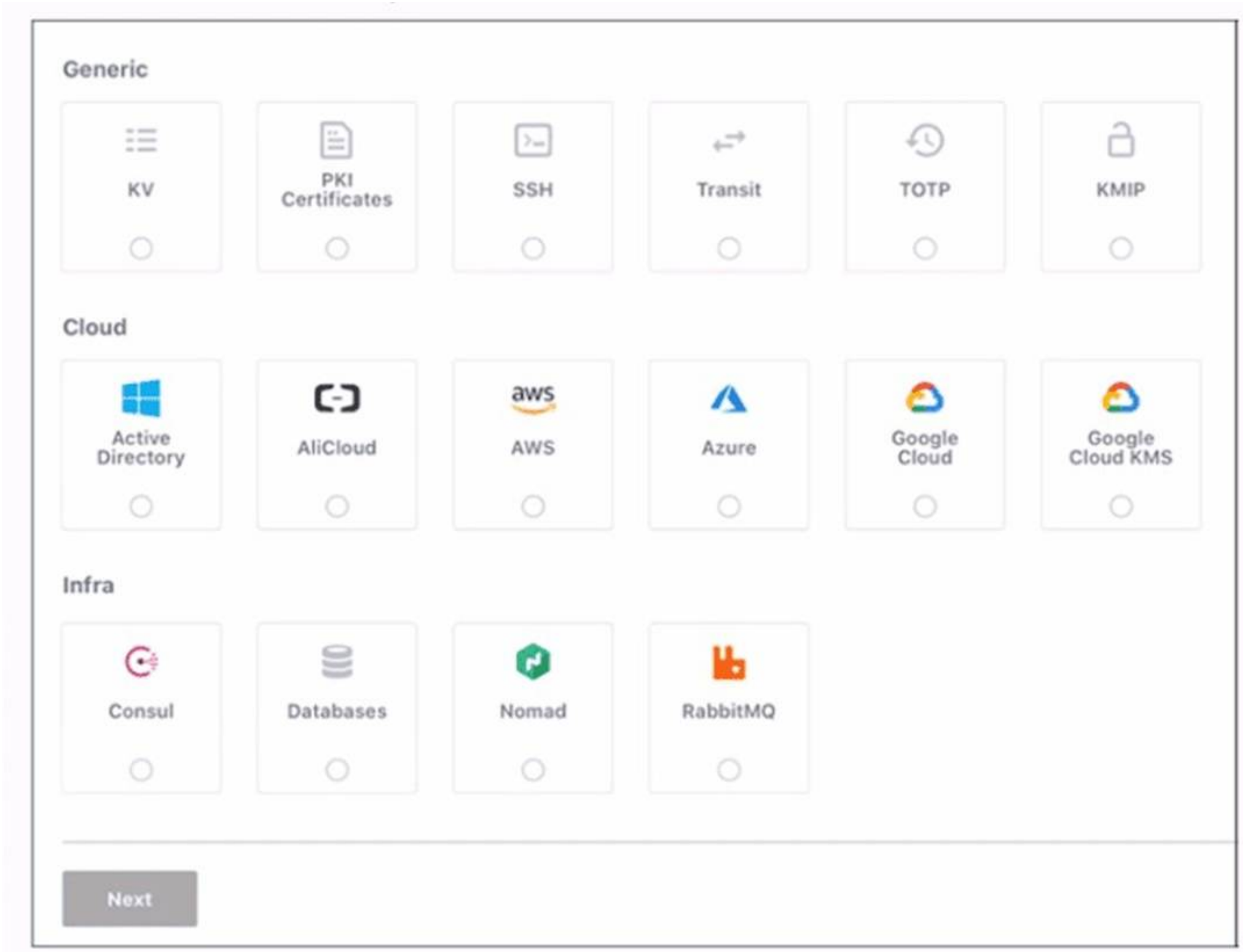
Running the second command in the GUI CLI will succeed.



A. True
B. False

Answer: B

NEW QUESTION 321
- (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 324
- (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 327
- (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 331
- (Topic 5)
Which of the following vault lease operations uses a lease _ id as an argument? Choose two correct answers.

A. renew
B. revoke -prefix
C. create
D. describe
E. revoke

Answer: AE

NEW QUESTION 335
- (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 340
- (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 344
- (Topic 5)
Which of the following statements describe the CLI command below? S vault login -method-1dap username-mitche11h

A. Generates a token which is response wrapped
B. You will be prompted to enter the password
C. By default the generated token is valid for 24 hours
D. Fails because the password is not provided

Answer: A

NEW QUESTION 349
- (Topic 5)
What is the Vault CLI command to query information about the token the client is currently using?

A. vault lookup token
B. vault token lookup
C. vault lookup self
D. vault self-lookup

Answer: B

NEW QUESTION 353
- (Topic 5)
You are using Vault's Transit secrets engine to encrypt your data. You want to reduce the amount of content encrypted with a single key in case the key gets compromised. How would you do this?

A. Use 4096-bit RSA key to encrypt the data
B. Upgrade to Vault Enterprise and integrate with HSM
C. Periodically re-key the Vault's unseal keys
D. Periodically rotate the encryption key

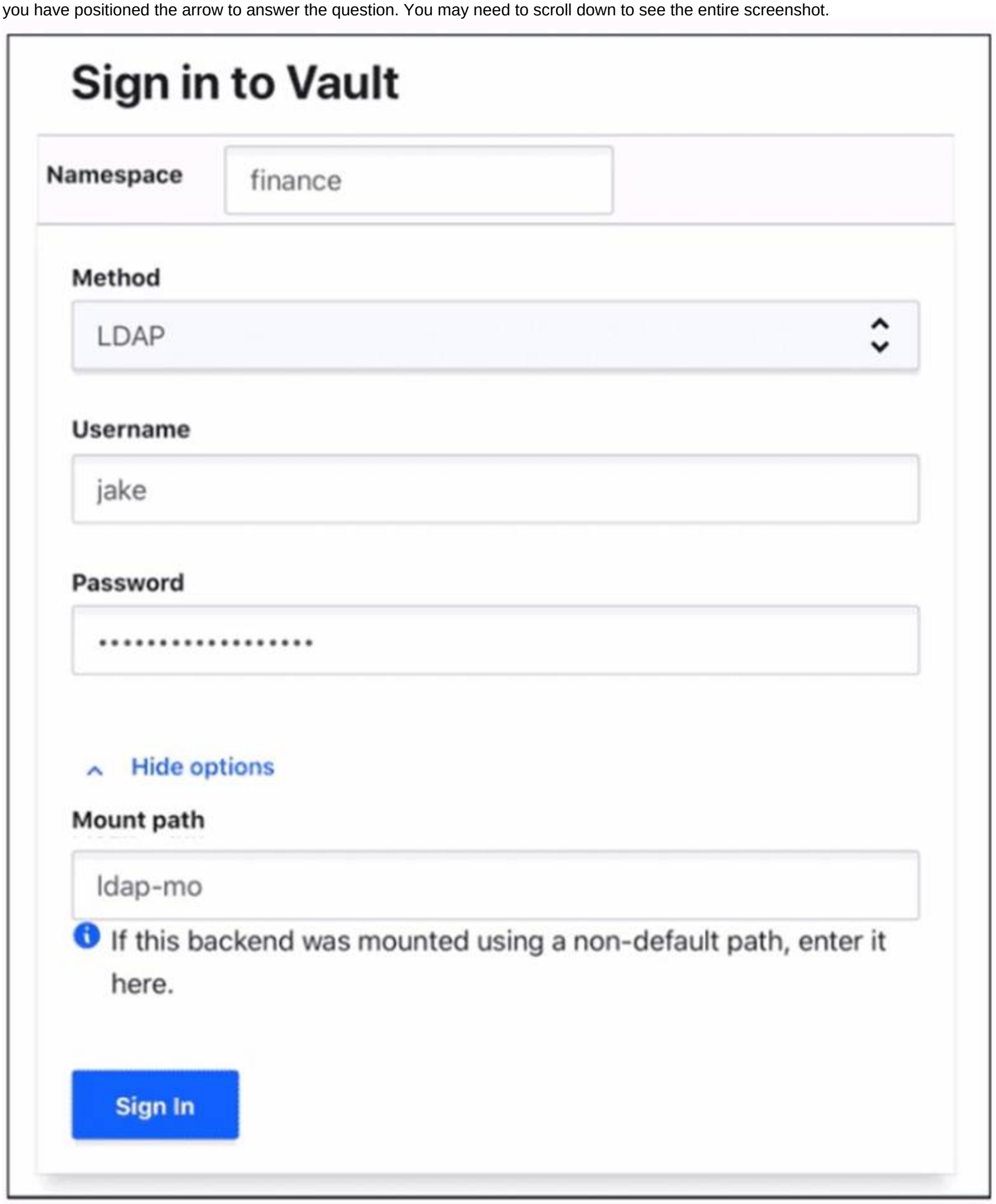
Answer: D

NEW QUESTION 355
- (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

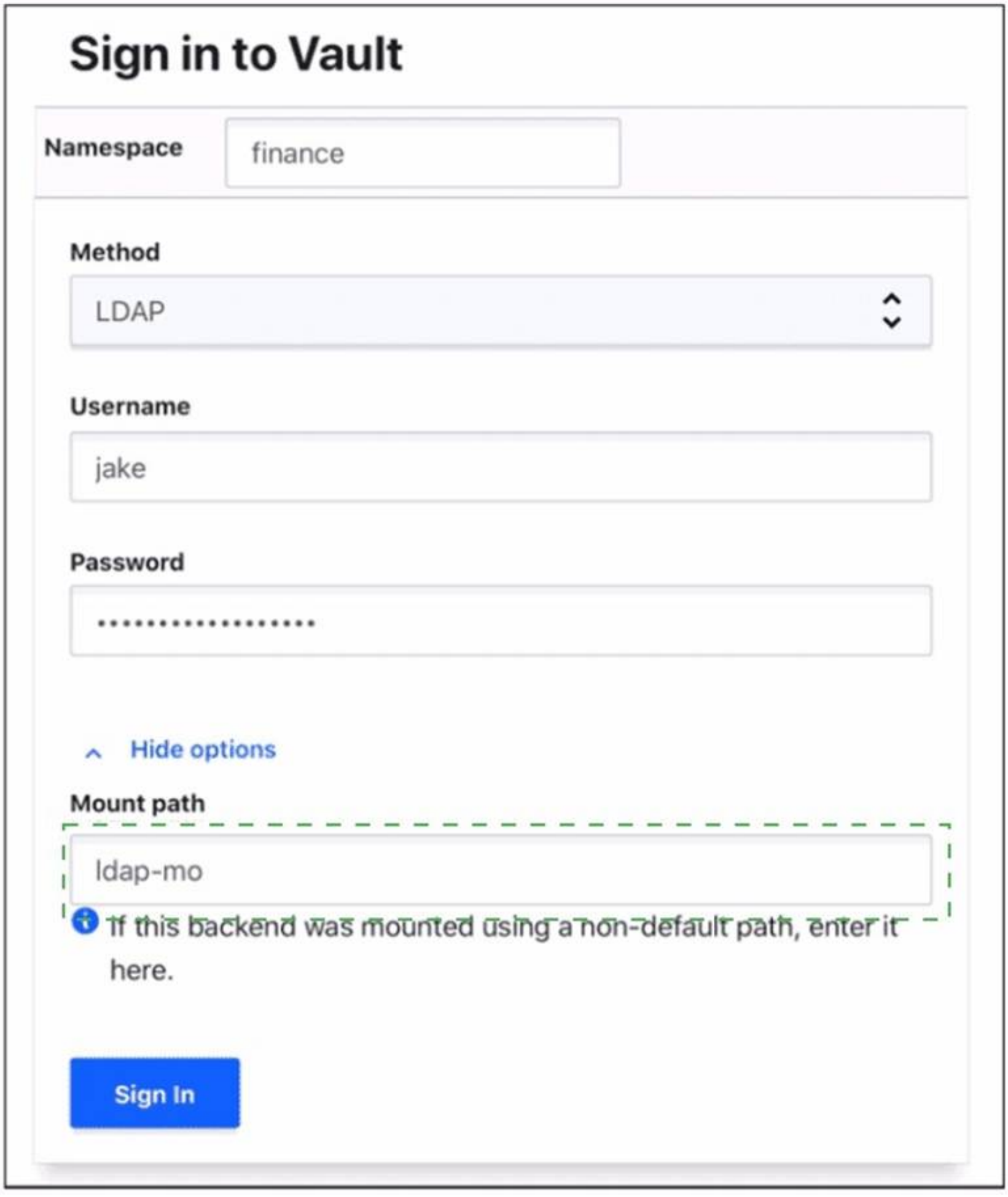
NEW QUESTION 358
HOTSPOT - (Topic 5)
Where do you define the Namespace to log into using the Vault Ul? To answer this question
Use your mouse to click on the screenshot in the location described above. An arrow indicator will mark where you have clicked. Click the "Answer" button once you have positioned the arrow to answer the question. You may need to scroll down to see the entire screenshot.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 362
- (Topic 5)
A user issues the following cURL command to encrypt data using the transit engine and the Vault AP:

```
curl \
--header "X-Vault-Token: c4f280f6-fdb2-18eb-89d3-589e2e834cdb" \
--request POST \<
--data @payload.json \
http://127.0.0.1:8200/v1/transit/encrypt/my-key
```

Which payload.json file has the correct contents?

A.

```
{
  "plaintext": "dGhlIHF1aWNrIGJyb3duIGZveA=="
}
```

B.

```
{
  "ciphertext": "vault:v1:abcdefgh"
}
```

C.

```
{
  "data": {
    "plaintext": "dGhlIHF1aWNrIGJyb3duIGZveA=="
  }
}
```

D.

```
{
  "data": {
    "ciphertext": "vault:v1:abcdefgh"
  }
}
```

Answer: C

NEW QUESTION 365
- (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-"ABCDEFGHI] 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 369

- (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 371
- (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 373
- (Topic 5)
Your DevOps team would like to provision VMs in GCP via a CICD pipeline. They would like to integrate Vault to protect the credentials used by the tool. Which secrets engine would you recommend?

A. Google Cloud Secrets Engine
B. Identity secrets engine
C. Key/Value secrets engine version 2
D. SSH secrets engine

Answer: A

NEW QUESTION 374
- (Topic 5)
When an auth method is disabled all users authenticated via that method lose access.

A. True
B. False

Answer: A

NEW QUESTION 379
- (Topic 5)
A web application uses Vault's transit secrets engine to encrypt data in-transit. If an attacker intercepts the data in transit which of the following statements are true? Choose two correct answers.

A. You can rotate the encryption key so that the attacker won??t be able to decrypt the data
B. The keys can be rotated and min_decryption_version moved forward to ensure this data cannot be decrypted
C. The Vault administrator would need to seal the Vault server immediately
D. Even if the attacker was able to access the raw data, they would only have encrypted bits (TLS in transit)

Answer: BD

NEW QUESTION 380
- (Topic 5)
You can build a high availability Vault cluster with any storage backend.

A. True
B. False

Answer: B

NEW QUESTION 382
- (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 384

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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