HashiCorp

Exam Questions HCVA0-003

HashiCorp Certified: Vault Associate (003)Exam

NEW QUESTION 1
- (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

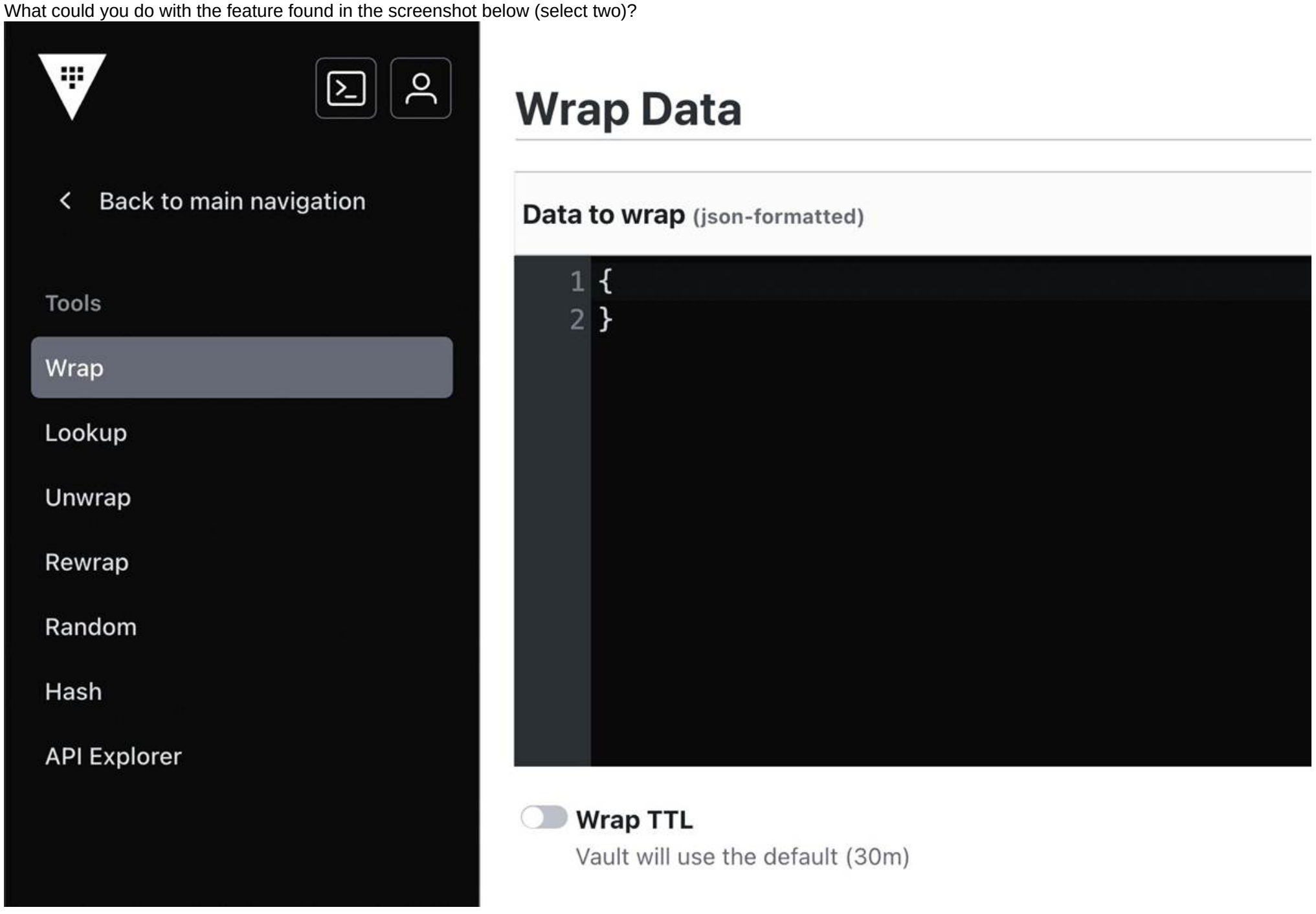
Answer: BCDE

NEW QUESTION 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 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)
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 5
- (Topic 1)
What is the default maximum time-to-live (TTL) for a token, measured in days?

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

Answer: A

NEW QUESTION 6
- (Topic 1)
How does the Vault Secrets Operator (VSO) assist in integrating Kubernetes-based workloads with Vault?

A. By enabling a local API endpoint to allow the workload to make requests directly from the VSO
B. By using client-side caching for KVv1 and KVv2 secrets engines
C. By injecting a Vault Agent directly into the pod requesting secrets from Vault
D. By watching for changes to its supported set of Custom Resource Definitions (CRD)

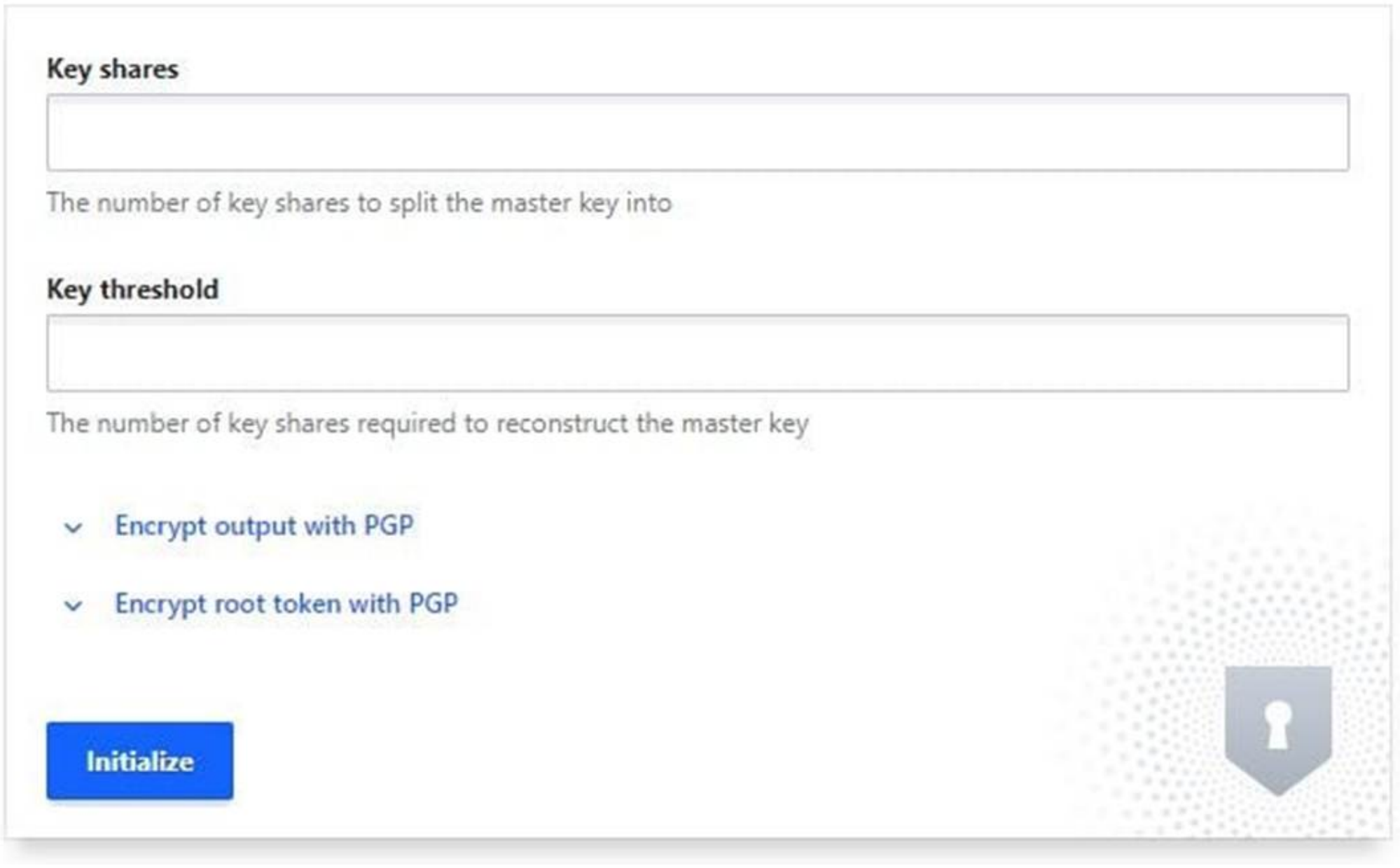
Answer: D

NEW QUESTION 7
- (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 8
- (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 9
- (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 10
- (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 10
- (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 12
- (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 16
- (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 17
- (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 18
- (Topic 1)
You logged into the Vault CLI and attempted to enable an auth method, but you received this error message. What can you do to resolve the error and configure Vault?
(Error: dial tcp 127.0.0.1:8200: connect: connection refused)

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

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

Answer: D

NEW QUESTION 22
- (Topic 1)
How long does the Transit secrets engine store the resulting ciphertext by default?

A. 24 hours
B. 30 days
C. 32 days
D. Transit does not store data

Answer: D

NEW QUESTION 25
- (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 30
- (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 31
- (Topic 1)
From the options below, select the auth methods that are better suited for machine-to- machine authentication (select five):

A. Kubernetes
B. GitHub
C. TLS
D. Token
E. AppRole
F. AWS
G. LDAP
H. OIDC

Answer: ACDEF

NEW QUESTION 33
- (Topic 1)
True or False? All dynamic secrets in Vault are required to have a lease.

A. True
B. False

Answer: A

NEW QUESTION 37
- (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 42
- (Topic 1)
Your company's security policies require that all encryption keys must be rotated at least once per year. After using the Transit secrets engine for a year, the Vault admin issues the proper command to rotate the key named ecommerce that was used to encrypt your data. What command can be used to easily re-encrypt the original data with the new version of the key?

A. vault write -f transit/keys/ecommerce/rotate <old data>
B. vault write -f transit/keys/ecommerce/update <old data>
C. vault write transit/encrypt/ecommerce v1:v2 <old data>
D. vault write transit/rewrap/ecommerce ciphertext=<old data>

Answer: D

NEW QUESTION 47
- (Topic 1)
Below is a list of parent and child tokens and their associated TTL. Which token(s) will be revoked first?

A. hvs.y4fUERqCtUV0xsQjWLJar5qX - TTL: 4 hours
B. hvs.FNiIFU14RUxxUYAl4ErLfPVR - TTL: 6 hours
C. hvs.Jw9LMpu7oCQgxiKbjfyzyg75 - TTL: 4 hours (child of B)
D. hvs.3IrlhEvcerEGbae11YQf9FvI - TTL: 3 hours
E. hvs.hOpweMVFvqfvoVnNgvZq8jLS - TTL: 5 hours (child of D)

Answer: D

NEW QUESTION 51
- (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 56
- (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 60
- (Topic 2)
Which of the following statements best describes the difference between static and dynamic credentials in a secrets management system?

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

Answer: C

NEW QUESTION 65
- (Topic 2)
Which statement best explains how Vault handles data encryption?

A. Vault uses encryption to secure data at rest and in transit, using an encryption key protected by the root key.
B. Vault encrypts data using a root key stored in plain text on the server??s filesystem.
C. Vault stores data in plaintext on disk but encrypts it only when transmitting it over the network.
D. Vault offloads all encryption to third-party services, so no secret data is ever processed by Vault.

Answer: A

NEW QUESTION 70
- (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 73
- (Topic 2)
True or False? The command vault lease revoke -prefix aws/ will revoke all leases associated with the secret engine mounted at /aws.

A. True
B. False

Answer: A

NEW QUESTION 76
- (Topic 2)
After creating a dynamic credential on a database, the DBA accidentally deletes the credentials on the database itself. When attempting to remove the lease, Vault returns an error stating that the credential cannot be found. What command can be run to make Vault remove the secret?

A. vault lease revoke -force -prefix <lease_path>
B. vault lease -renew
C. vault lease revoke -enforce
D. vault revoke -apply

Answer: A

NEW QUESTION 81

- (Topic 2)
Which of the following features are not available in the Vault Community version?

A. Cloud KMS auto-unseal
B. Single sign-on support
C. Event notifications and filtering
D. Multi-factor authentication (auth)
E. Dynamic secrets engines
F. HSM auto-unseal

Answer: F

NEW QUESTION 82
- (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 85
- (Topic 2)
True or False? All Vault policies are deny by default.

A. True
B. False

Answer: A

NEW QUESTION 86
- (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 87
- (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)
Which statement best describes the process of sealing a Vault instance?

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

Answer: C

NEW QUESTION 93
- (Topic 2)
By default, what happens to child tokens when a parent token is revoked?

A. The child tokens are revoked
B. The child tokens are renewed
C. The child tokens are converted to parent tokens
D. The child tokens create their own child tokens to be used

Answer: A

NEW QUESTION 98

- (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)
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 103
- (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 106
- (Topic 2)
What is the correct order that Vault uses to protect data?

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

Answer: A

NEW QUESTION 107
- (Topic 2)
You have deployed an application that needs to encrypt data before writing to a database. What secrets engine should you use?

A. Transit
B. SSH
C. PKI
D. TOTP

Answer: A

NEW QUESTION 112
- (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 117
- (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 122
- (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 123
- (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 127
- (Topic 3)
Kyle enabled the database secrets engine for dynamic credentials. Amy, the senior DBA, accidentally deleted the database users created by Vault, disrupting client applications.
How can Kyle manually remove the leases in Vault?

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

Answer: C

NEW QUESTION 130
- (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/Wb7QCsXsU/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/kCOn7..."

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 134
- (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 135
- (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 137
- (Topic 3)
True or False? You can create and update Vault policies using the UI.

A. True
B. False

Answer: A

NEW QUESTION 139
- (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 142
- (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 143
- (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 144
- (Topic 3)
Which of the following storage backends support high availability? (Select four)

A. Consul
B. etcd
C. DynamoDB
D. Integrated Storage (raft)
E. Amazon S3
F. In-Memory

Answer: ABCD

NEW QUESTION 149
- (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 152

- (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 156
- (Topic 3)
Which of the following secrets engines can store static secrets in Vault for future retrieval?

A. KV
B. PKI (certificates)
C. Database
D. Transit

Answer: A

NEW QUESTION 161
- (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 166
- (Topic 3)
Although batch and service tokens share many characteristics, which of the following are true only about batch tokens? (Select three)

A. Can create child tokens
B. Are renewable up until the max TTL
C. Maintain a single fixed TTL
D. They are valid for either the primary or any secondary clusters
E. They are not persisted to disk

Answer: CDE

NEW QUESTION 167
- (Topic 3)
You have TBs of data encrypted by Vault stored in a database and are worried about Vault becoming unavailable and not being able to decrypt the data. Is it possible to export the encryption key to store it somewhere else in the event Vault becomes unavailable?

A. Yes, as long as the key was configured to be exportable when it was created
B. No, you cannot export the encryption key from Vault

Answer: A

NEW QUESTION 169
- (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 173
- (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 176
- (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 179
- (Topic 3)
True or False? The following policy permits a user to read secrets contained in the path secrets/cloud/apps/jenkins?
text CollapseWrapCopy
path "secrets/cloud/apps/jenkins/*" {
capabilities = ["create", "read", "update", "delete", "list"]
}

A. True
B. False

Answer: B

NEW QUESTION 184
- (Topic 3)
When a lease is created, what actions can be performed by using only the lease ID? (Choose two)

A. Renew the lease
B. Revoke the lease
C. Extend the max TTL for the lease
D. Authenticate using the lease ID

Answer: AB

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)
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

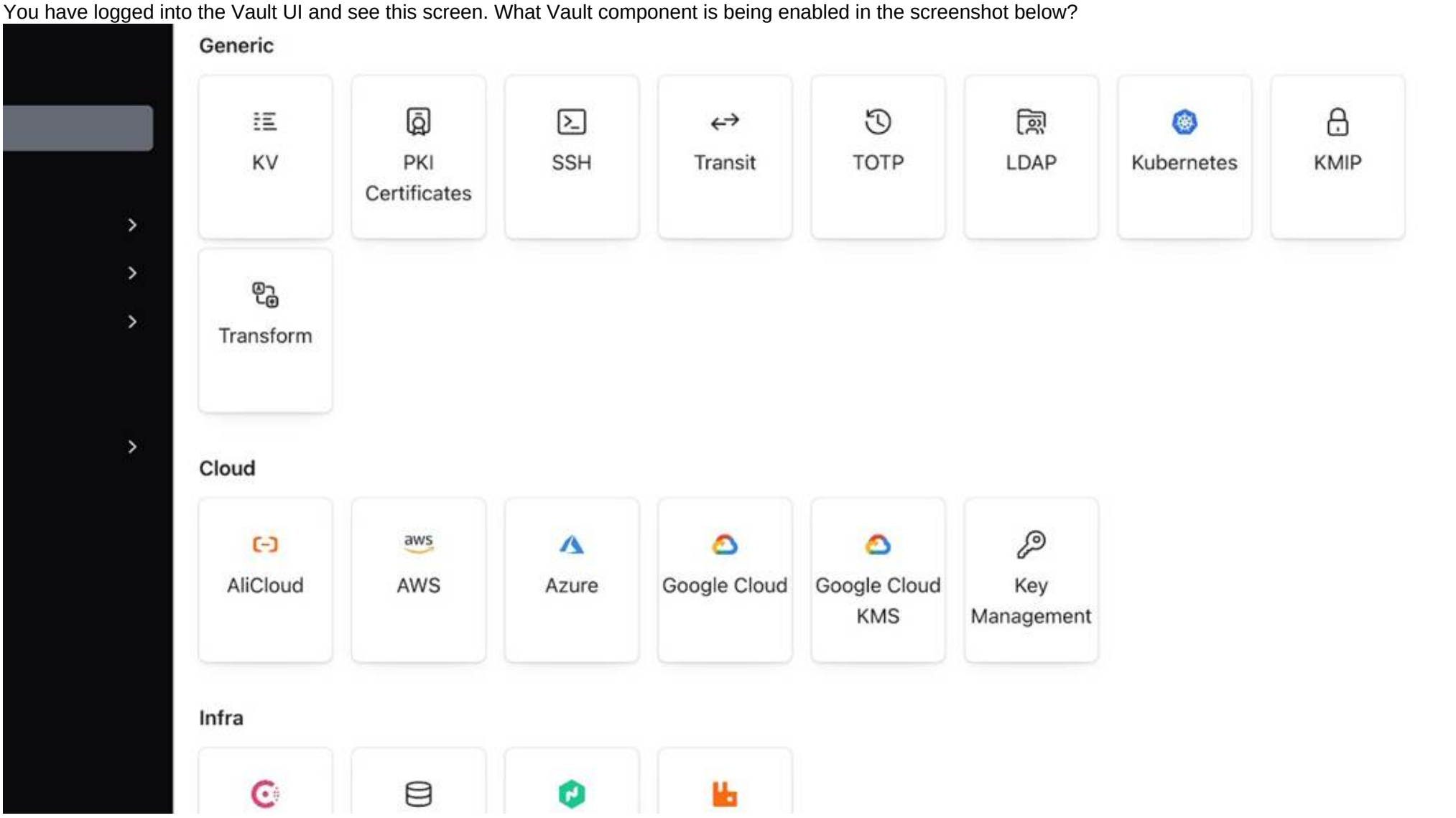
NEW QUESTION 198
- (Topic 4)
Before data is written to the storage backend, the data is encrypted by which Vault feature?

A. TLS certificate
B. Cryptographic barrier
C. Unseal keys
D. Transit secrets engine

Answer: B

NEW QUESTION 200

- (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 201
- (Topic 4)
Your organization uses a CI/CD pipeline to deploy its applications on Azure. During testing, you generate new credentials to validate Vault can create new credentials. The result of this command is below:
text CollapseWrapCopy
$ vault read azure/creds/bryan-krausen Key Value
--- -----
lease_id azure/creds/bryan-krausen/9eed0373-ca92-99b6-b914-779b7bb0e1d9 lease_duration 60m
lease_renewable true
client_id 532bf678-ee4e-6be1-116b-4e4221e445dd client_secret be60395b-4e6b-2b7e-a4b3-c449a5c00973
What commands can be used to revoke this secret after you have finished testing? (Select three)

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

Answer: BCE

NEW QUESTION 204
- (Topic 4)
You are using the Vault API to test authentication before modifying your CI/CD pipeline to properly authenticate to Vault. You manually authenticate to Vault and receive the response below. Based on the provided options, which of the following are true? (Select four)
? $ curl \
? --request POST \
? --data @payload.json \
? https://vault.krausen.com:8200/v1/auth/userpass/login/bryan.krausen | jq
?
? **
? ******* RESPONSE BELOW ***
? **
?
? {
? "request_id": "f758e8da-11b6-8341-d404-56f0c370a7fa",
? "lease_id": "",
? "renewable": false,
? "lease_duration": 0,

? "data": null,
? "wrap_info": null,
? "warnings": null,
? "auth": {
? "client_token": "hvs.CbzCNJCVWt63jyzyaJakgDwz",
? "accessor": "rffwXzKFcxvaQi6Vgo8tY4Lt",
? "policies": [
? "training",
? "default"
?],
? "token_policies": [
? "training",
? "default"
?],
? "metadata": {
? "username": "bryan.krausen"
? },
? "lease_duration": 84600,
? "renewable": true,
? "entity_id": "f1795f6a-c576-d619-b2d5-74c0aee08edb",
? "token_type": "service",
? "orphan": true
? }
? }

A. The token required to retrieve a secret is hvs.CbzCNJCVWt63jyzyaJakgDwz
B. The returned token is a batch token
C. The user needs to retrieve .auth.client_token in order to perform other actions
D. The accessor will be used to authenticate to Vault to retrieve secrets
E. The user is using the userpass auth method
F. The user??s password is stored in a file named payload.json

Answer: ACEF

NEW QUESTION 208
- (Topic 4)
A large organization uses Vault for various use cases with multiple auth methods enabled. A user can authenticate via LDAP, OIDC, or a local userpass account, but they receive different policies for each method and often need to log out and back in for different actions. What can be configured in Vault to ensure users have consistent policies regardless of their authentication method?

A. Enable the SSH secrets engine and instruct the user to obtain credentials using the new secrets engine
B. Create a new entity and map the aliases from each of the available auth methods
C. Assign the default policy to the user's policy used by each auth method
D. Provide the user with an AppRole role-id and secret-id for authentication

Answer: B

NEW QUESTION 213
- (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 218
- (Topic 4)
There are a few ways in Vault that can be used to obtain a root token. Select the valid methods from the answers below. (Select three)

A. Generating a root token using a quorum of recovery keys when using Vault auto unseal
B. Initializing Vault when first creating the cluster by using vault operator init
C. Using a batch DR operation token to create a new root token in the event of an emergency
D. Running the command vault token create when using a valid root token

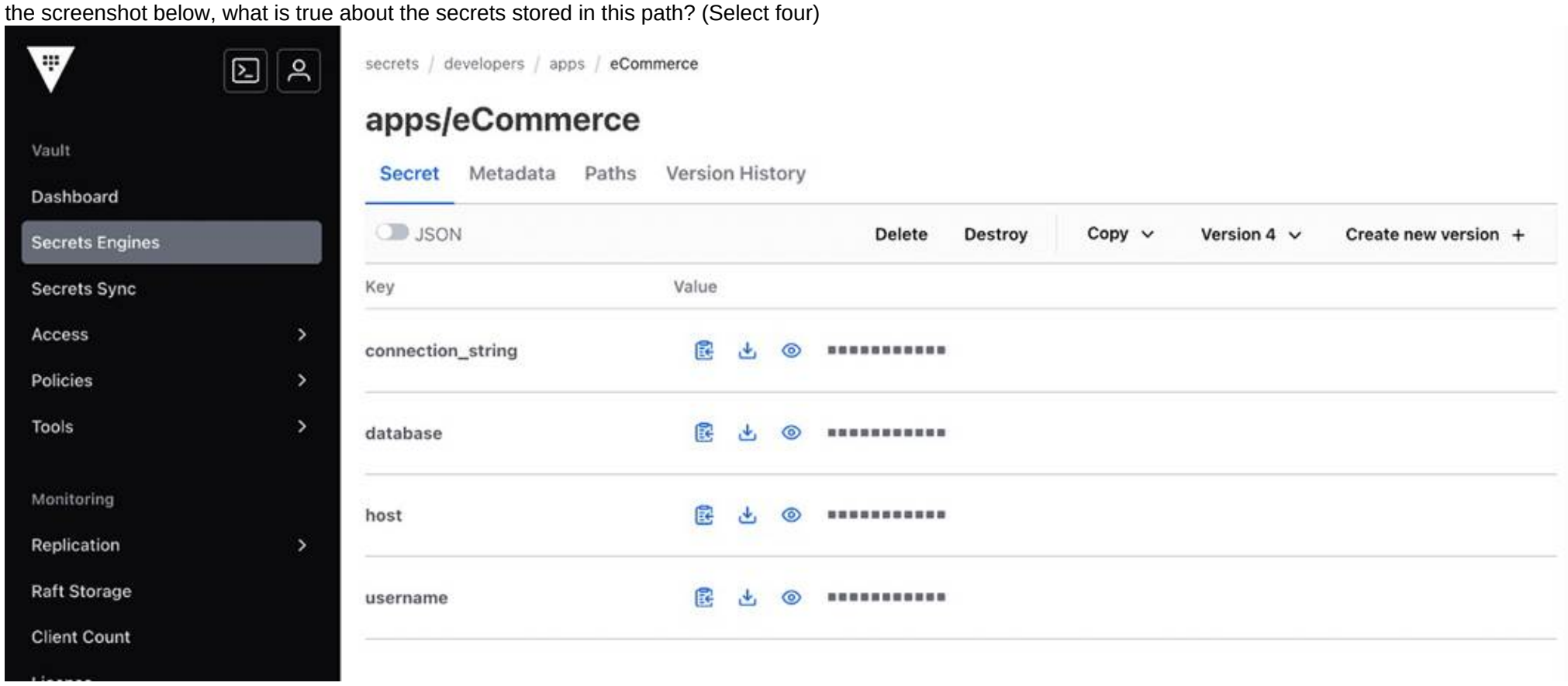
Answer: ABD

NEW QUESTION 220
- (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 221
- (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 226
- (Topic 4)
You have enabled the Transit secrets engine and want to start encrypting data to store in Azure Blob storage. What is the next step that needs to be completed before you can encrypt data? (Select two)

A. Export the encryption key and upload it to the application server
B. Enable the Transit secrets engine API
C. Create an encryption key for the application to use
D. Write a policy that permits the application to use the encryption key

Answer: CD

NEW QUESTION 227
- (Topic 4)
True or False? After rotating a transit encryption key, all data encrypted with the previous version must be rewrapped or re-encrypted with the new key.

A. True
B. False

Answer: B

NEW QUESTION 230
- (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 234
- (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 235
- (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 239
- (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 241
- (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 245
- (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 248
- (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

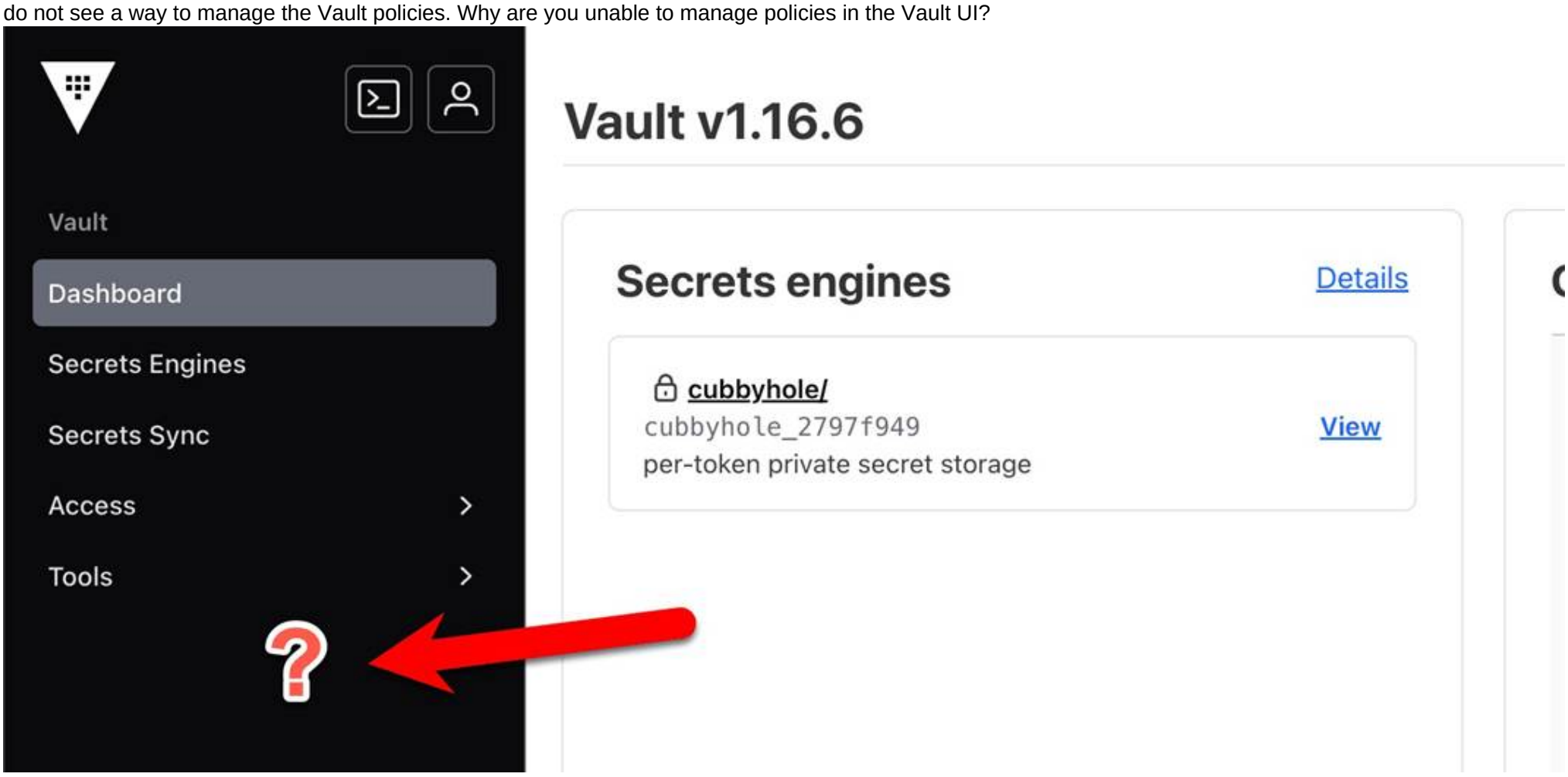
NEW QUESTION 250

- (Topic 4)
An Active Directory admin created a service account for an internal application. You want to store these credentials in Vault, allowing a CI/CD pipeline to read and configure the application with them during provisioning. Vault should maintain the last 3 versions of this secret. Which Vault secrets engine should you use?

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

Answer: D

NEW QUESTION 254
- (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

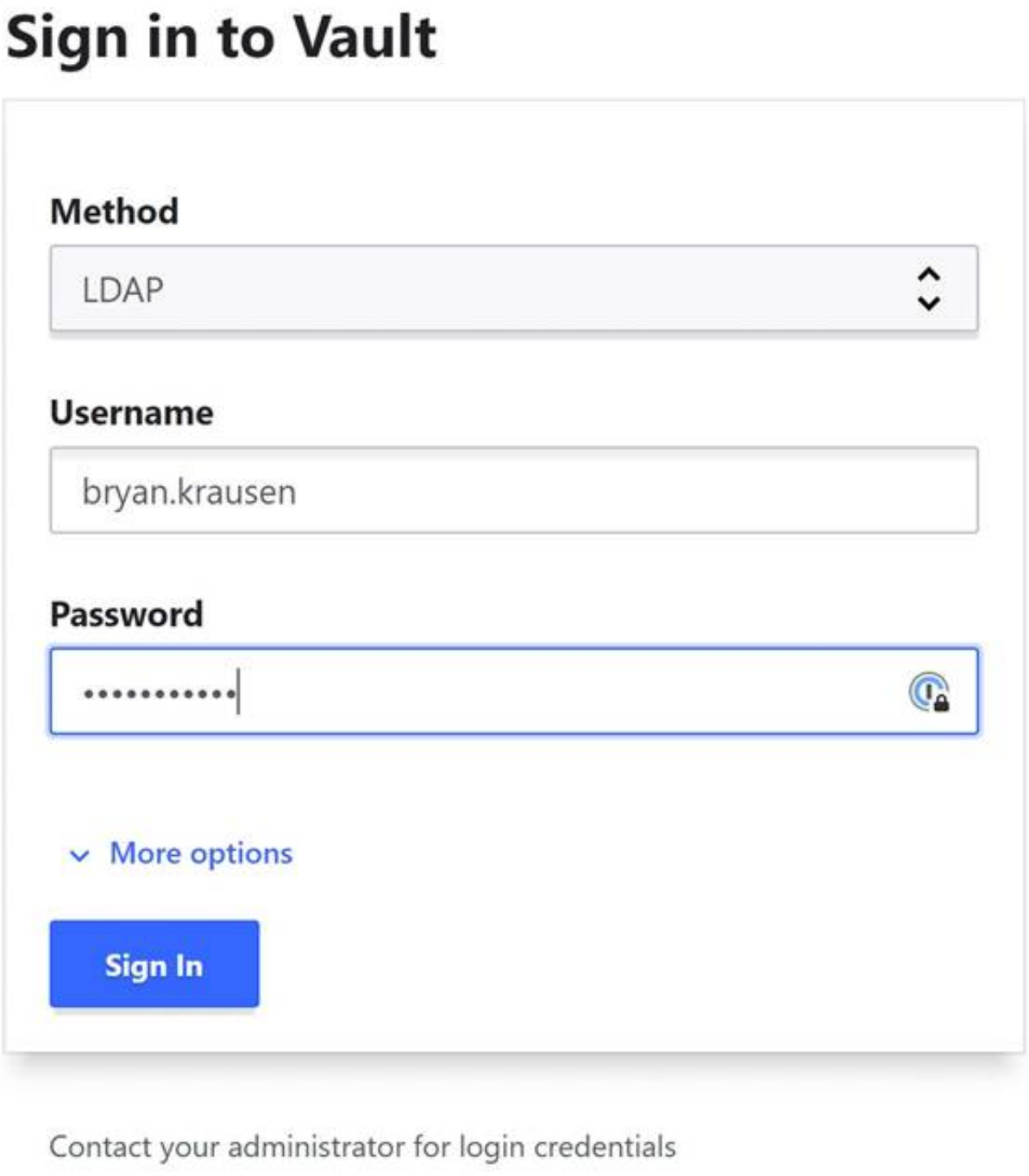
Answer: D

NEW QUESTION 257
- (Topic 4)
You are using Vault CLI and enable the database secrets engine on the default path of database/. However, the DevOps team wants to enable another database secrets engine for testing but receives an error stating the path is already in use. How can you enable a second database secrets engine using the CLI?

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

Answer: C

NEW QUESTION 258
- (Topic 4)
Your organization has enabled the LDAP auth method on the path of corp-auth/. When you access the Vault UI, you cannot log in despite providing the correct credentials. Based on the screenshot below, what action should you take to log in?



A. Select corp-auth from the dropdown list
B. Enter the username as corp-auth/bryan.krausen
C. Select More Options and enter the Mount path that LDAP was enabled on (corp-auth/)
D. Change to the Namespace of corp-auth before trying to authenticate

Answer: C

NEW QUESTION 260
- (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 264
- (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 269
- (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

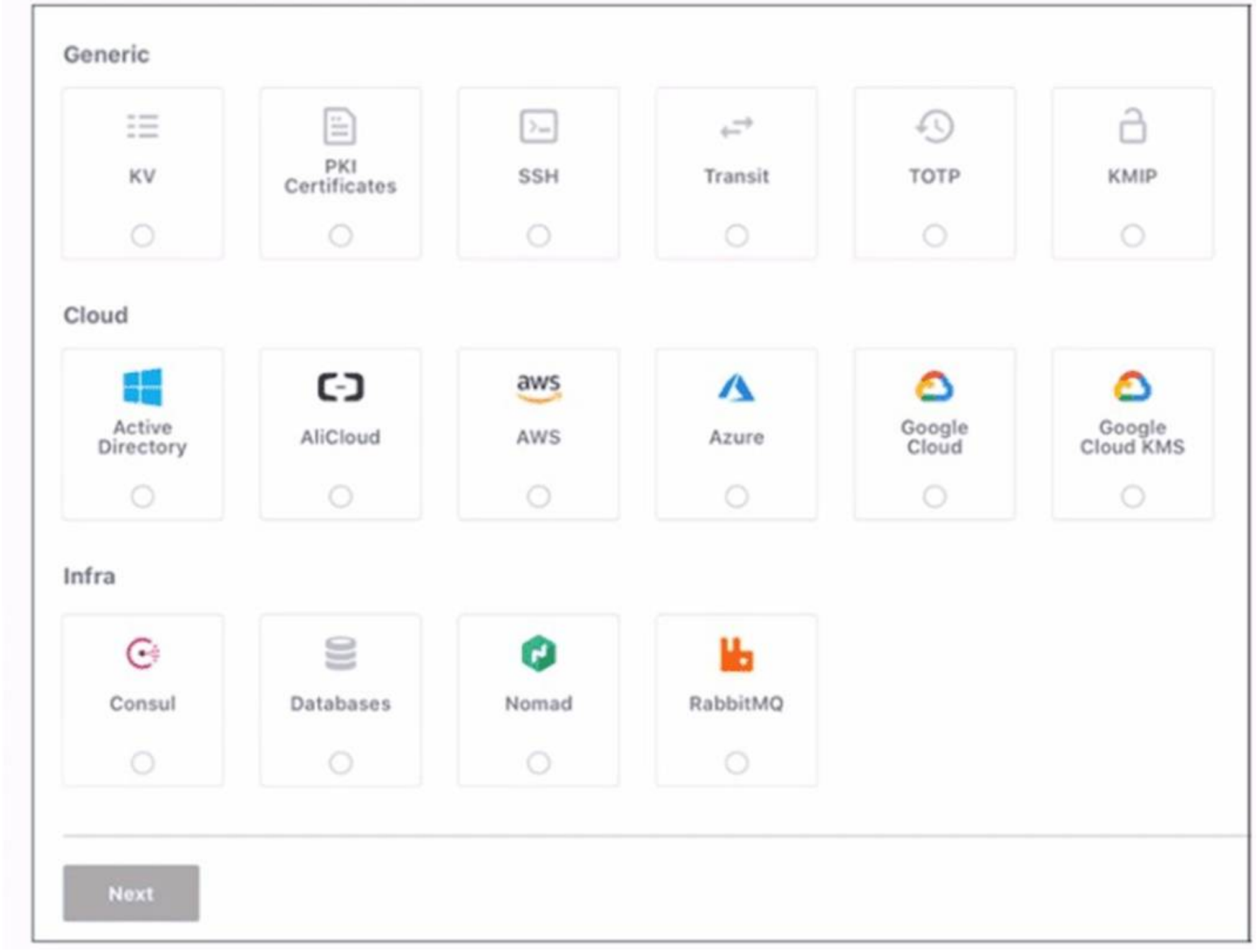
Answer: C

NEW QUESTION 270
- (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 274
- (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 275
- (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 279
- (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 283
- (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 286
- (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 288
- (Topic 5)
What is a benefit of response wrapping?

A. Log every use of a secret
B. Load balanc secret generation across a Vault cluster
C. Provide error recovery to a secret so it is not corrupted in transit
D. Ensure that only a single party can ever unwrap the token and see what's inside

Answer: D

NEW QUESTION 292
- (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 296
- (Topic 5)
Which of the following is a machine-oriented Vault authentication backend?

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

Answer: B

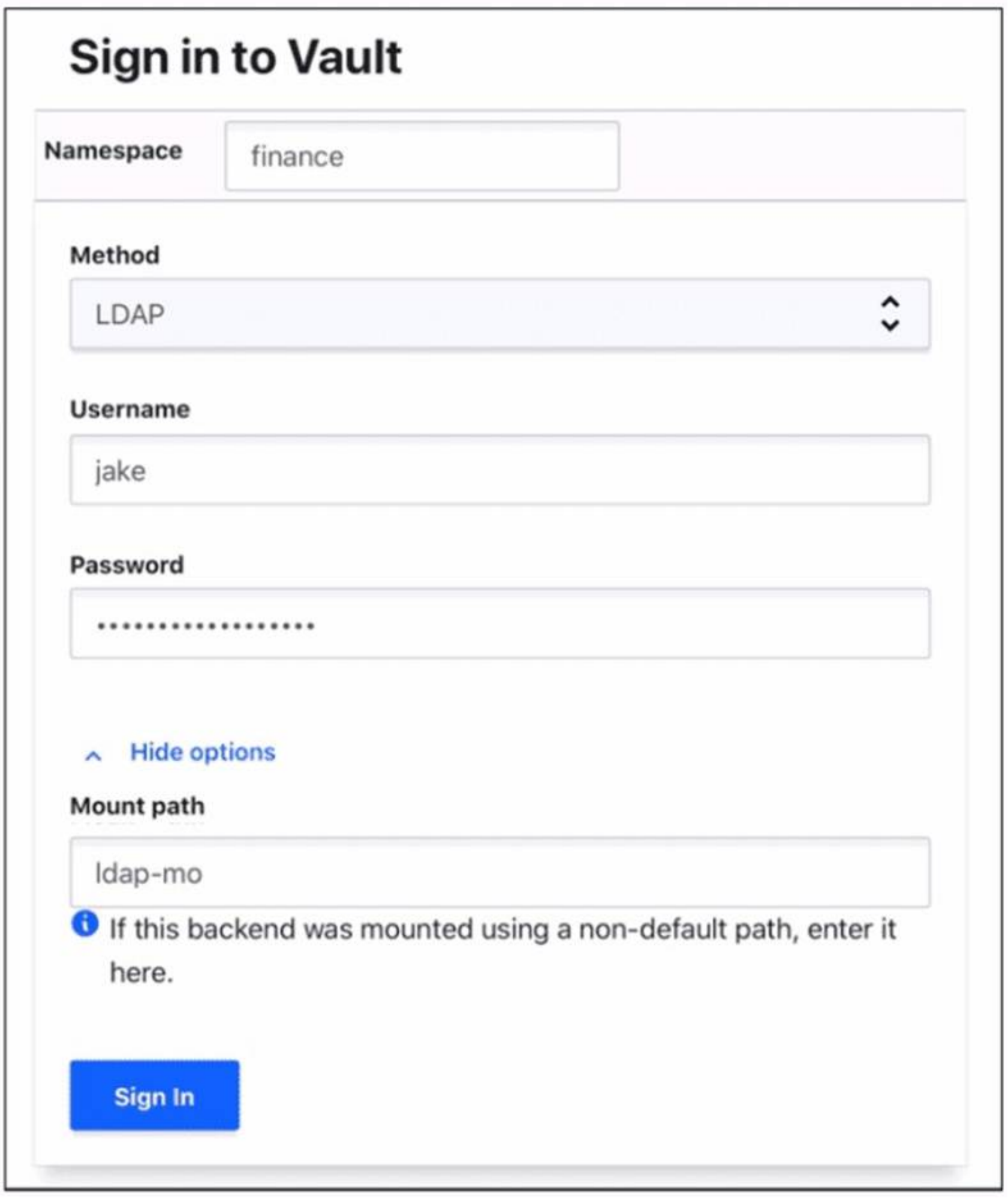
NEW QUESTION 298

- (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

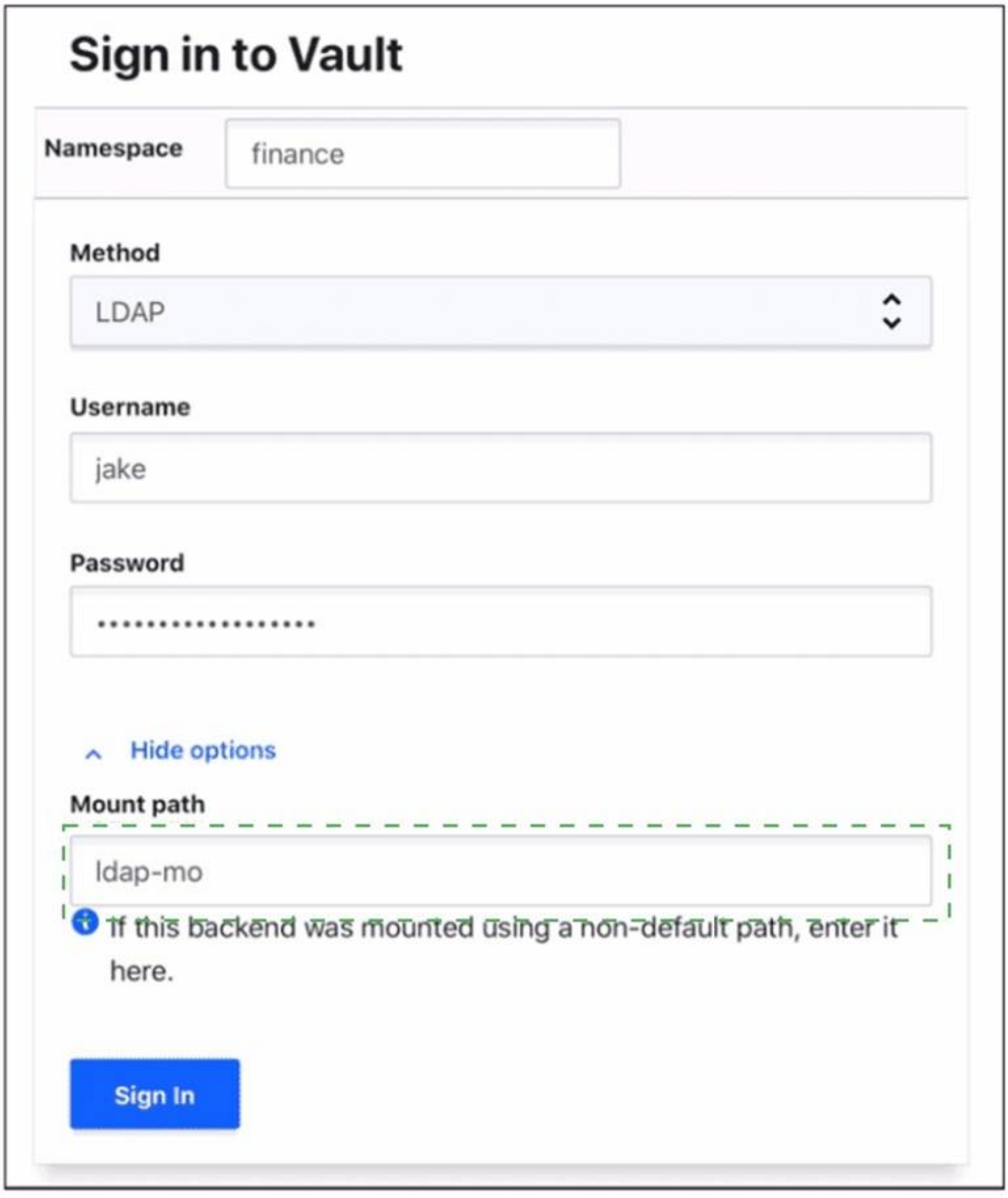
NEW QUESTION 299
HOTSPOT - (Topic 5)
Where do you define the Namespace to log into using the Vault UI? To answer this question
Use your mouse to click on the screenshot in the location described above. An arrow indicator will mark where you have clicked. Click the "Answer" button once you have positioned the arrow to answer the question. You may need to scroll down to see the entire screenshot.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 302
- (Topic 5)
You have been tasked with writing a policy that will allow read permissions for all secrets at path secret/bar. The users that are assigned this policy should also be able to list the secrets.What should this policy look like?

A.

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

B.

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

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

C.

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

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

D.

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

Answer: C

NEW QUESTION 306
- (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 311
- (Topic 5)
When using Integrated Storage, which of the following should you do to recover from possible data loss?

A. Failover to a standby node
B. Use snapshot
C. Use audit logs
D. Use server logs

Answer: B

NEW QUESTION 312
- (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 317
- (Topic 5)
An authentication method should be selected for a use case based on:

A. The auth method that best establishes the identity of the client
B. The cloud provider for which the client is located on
C. The strongest available cryptographic hash for the use case
D. Compatibility with the secret engine which is to be used

Answer: A

NEW QUESTION 320
- (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 322
- (Topic 5)
The following three policies exist in Vault. What do these policies allow an organization to do?

app.hcl

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

callcenter.hcl

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

rewrap.hcl

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

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

A. Separates permissions allowed on actions associated with the transit secret engine
B. Nothing, as the minimum permissions to perform useful tasks are not present
C. Encrypt, decrypt, and rewrap data using the transit engine all in one policy
D. Create a transit encryption key for encrypting, decrypting, and rewrapping encrypted data

Answer: C

NEW QUESTION 325
- (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 326
- (Topic 5)
Which of the following cannot define the maximum time-to-live (TTL) for a token?

A. By the authentication method t natively provide a method of expiring credentials
B. By the client system f credentials leaking
C. By the mount endpoint configuration very password used
D. A parent token TTL e password rotation tools and practices
E. System max TTL

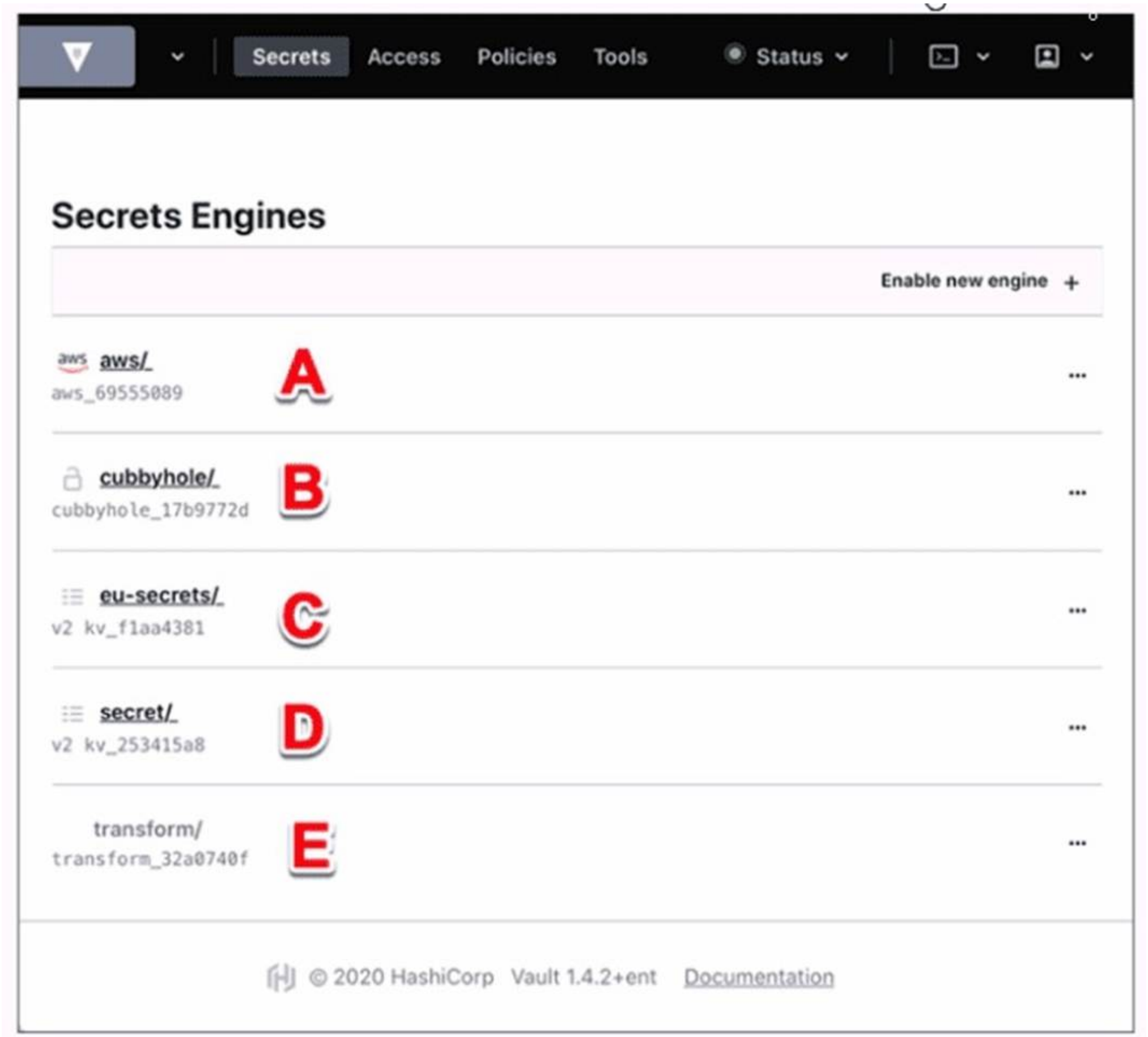
Answer: B

NEW QUESTION 330
- (Topic 5)
You can build a high availability Vault cluster with any storage backend.

A. True
B. False

Answer: B

NEW QUESTION 332
- (Topic 5)
Use this screenshot to answer the question below:



Where on this page would you click to view a secret located at secret/my-secret?

A. A
B. B
C. C
D. D
E. E

Answer: C

NEW QUESTION 335
.....

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