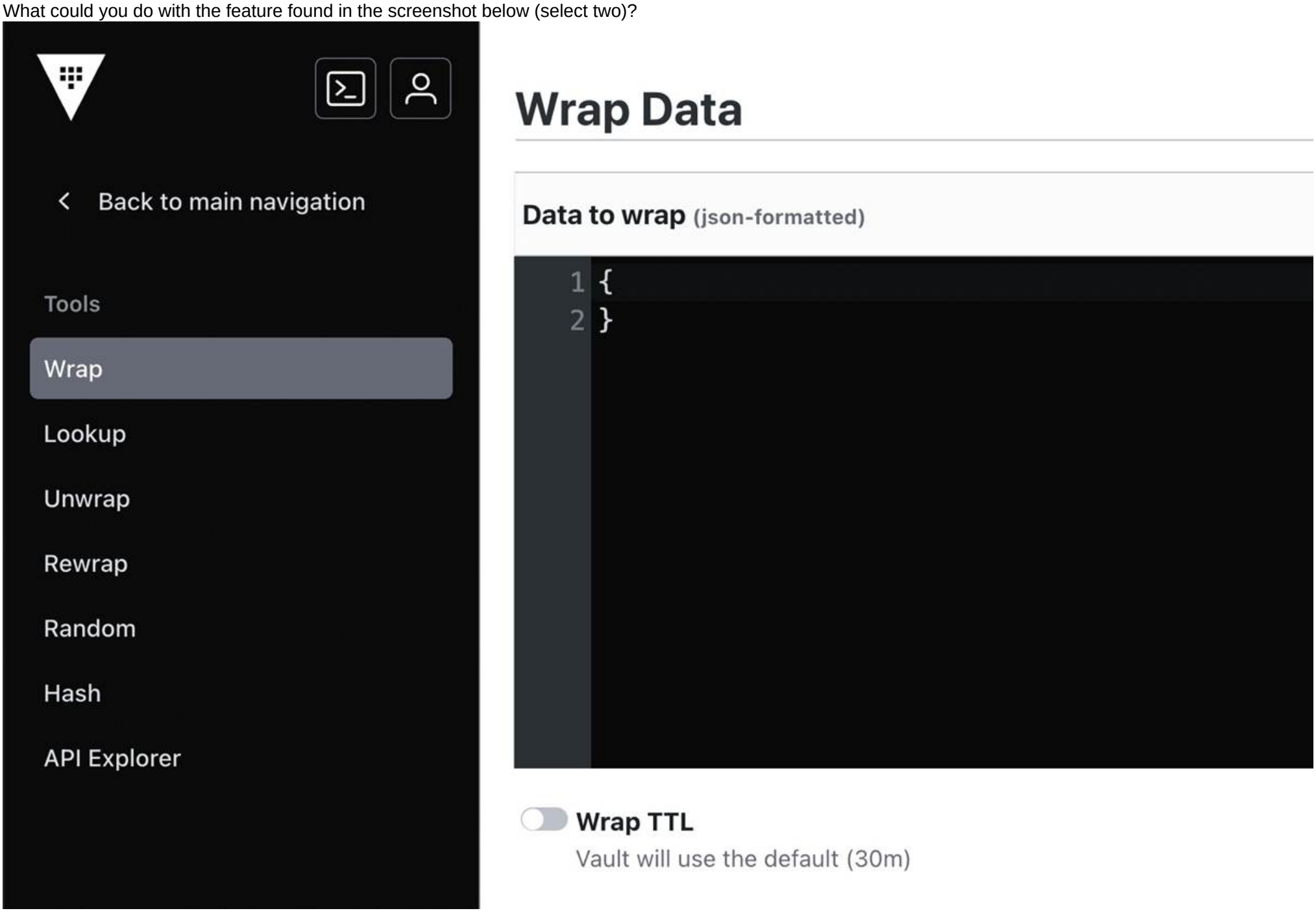
HashiCorp

Exam Questions HCVA0-003

HashiCorp Certified: Vault Associate (003)Exam

NEW QUESTION 1
- (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 2
- (Topic 1)
If Bobby is currently assigned the following policy, what additional policy can be added to ensure Bobby cannot access the data stored at secret/apps/confidential but still read all other secrets?
path "secret/apps/*" { capabilities = ["create", "read", "update", "delete", "list"] }

A. path "secret/apps/confidential" { capabilities = ["deny"] }
B. path "secret/*" { capabilities = ["read", "deny"] }
C. path "secret/apps/*" { capabilities = ["deny"] }
D. path "secret/apps/confidential/*" { capabilities = ["deny"] }

Answer: A

NEW QUESTION 3
- (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

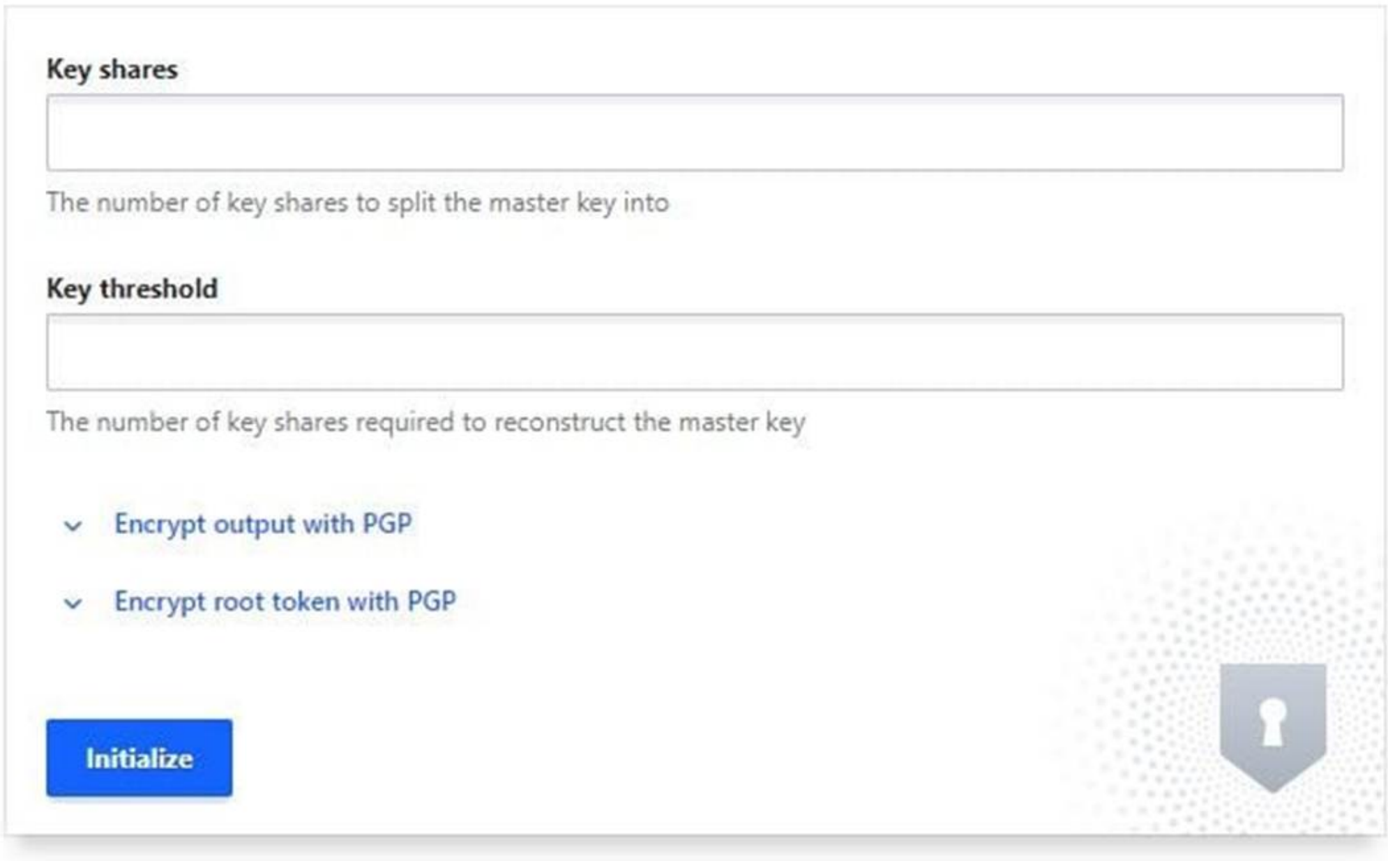
NEW QUESTION 4
- (Topic 1)
In regards to the Transit secrets engine, which of the following is true given the following command and output (select three):

$ 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 5
- (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 6
- (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 7
- (Topic 1)
Which of the following is NOT a valid way in which a lease can be revoked in Vault?

A. Using the user interface (UI)
B. Automatically when the TTL or Max-TTL expires
C. Using the API to call the /v1/sys/leases endpoint
D. Via the CLI using the vault token command

Answer: D

NEW QUESTION 8
- (Topic 1)
? A Jenkins server is using the following token to access Vault. Based on the lookup shown below, what type of token is this?$ vault token lookup hvs.FGP1A77Hxa1Sp6Pkp1yURcZB
?
? Key Value
? --- -----
? accessor RnH8jtgrxBrYanizlyJ7Y8R
? creation_time 1604604512
? creation_ttl 24h
? display_name token
? entity_id n/a
? expire_time 2025-11-06T14:28:32.8891566-05:00
? explicit_max_ttl 0s
? id hvs.FGP1A77Hxa1Sp6KRau5eNB
? issue_time 2025-11-06T14:28:32.8891566-05:00
? meta <nil>
? num_uses 0
? orphan false
? path auth/token/create
? period 24h
? policies [admin default]
? renewable true
? ttl 23h59m50s
? type service

A. Periodic token
B. Batch token
C. Orphaned token
D. Secondary token

Answer: A

NEW QUESTION 9
- (Topic 1)
What is true about the output of the following command (select three)?

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

Answer: ADE

NEW QUESTION 10
- (Topic 1)
You??ve set up multiple Vault clusters, one on-premises intended to be the primary cluster, and the second cluster in AWS, which was deployed for performance replication. After enabling replication, developers complain that all the data they??ve stored in the AWS Vault cluster is missing. What happened?

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

Answer: B

NEW QUESTION 10
- (Topic 1)
Which of the following statements are true regarding Vault seal and unseal (select three)?

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

Answer: ACD

NEW QUESTION 11
- (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 14
- (Topic 1)
What are the primary benefits of running Vault in a production deployment over dev server mode (select two)?

A. Faster deployment
B. Persistent storage
C. Ability to enable auth methods
D. Encryption via TLS

Answer: BD

NEW QUESTION 17
- (Topic 1)
True or False? When using the Transit secrets engine, setting the min_decryption_version will determine the minimum key length of the data key (i.e., 2048, 4096, etc.).

A. True
B. False

Answer: B

NEW QUESTION 18
- (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 22
- (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 25
- (Topic 1)
Which of the following secrets engines does NOT issue a lease upon a read request?

A. KV
B. Consul
C. Database
D. AWS

Answer: A

NEW QUESTION 28
- (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 32
- (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 37
- (Topic 1)
Given the following policy, which command below would not result in a permission denied error (select two)?
path "secret/*" { capabilities = ["create", "update"] allowed_parameters = { "student" = ["steve", "frank", "jamie", "susan", "gerry", "damien"] } }
path "secret/apps/*" { capabilities = ["read"] }
path "secret/apps/results" { capabilities = ["deny"] }

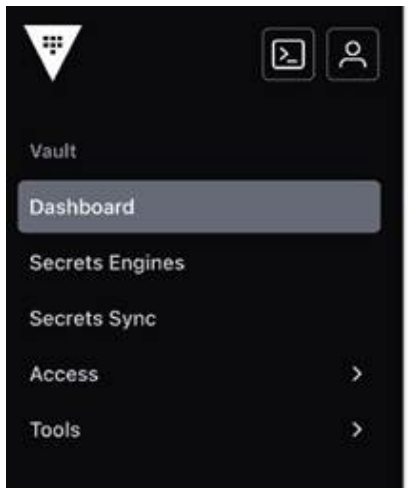
A. vault kv put secret/apps/results student03=practice
B. vault kv put secret/apps/app01 student=bryan
C. vault kv put secret/common/results student=frank
D. vault kv get secret/apps/api_key

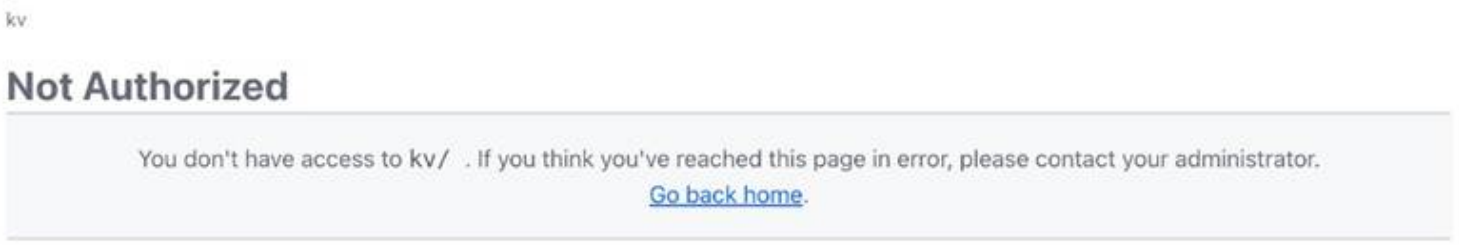
Answer: CD

NEW QUESTION 40
- (Topic 1)
A user is assigned the following policy, and they can successfully retrieve secrets using the CLI. However, the user reports receiving an error message in the UI. Why can??t the user access the secret in the Vault UI?
path "kv/apps/app01" { capabilities = ["read"] }
Successful retrieval using the CLI

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

(Error: Permission denied in UI)





A. The user doesn??t know what they??re doing
B. The user doesn??t have permissions to retrieve the data from the UI, only the CLI
C. The user needs list permissions to browse the UI
D. The user??s token is invalid

Answer: C

NEW QUESTION 41
- (Topic 1)
True or False? All dynamic secrets in Vault are required to have a lease.

A. True
B. False

Answer: A

NEW QUESTION 45
- (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 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)
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 55
- (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 60
- (Topic 2)
Based on the following output, what command can Steve use to determine if the KV store is configured for versioning?
text CollapseWrapCopy
$ vault secrets list
Path Type Accessor Description
---- ---- -------- -----------
automation/ kv kv_56f991b9 Automation team for CI/CD cloud/ kv kv_4426c541 Cloud team for static secrets
cubbyhole/ cubbyhole cubbyhole_9bd538e per-token priv secret storage data_team/ kv kv_96d57692 Data warehouse KV for certs
identity/ identity identity_0042595e identity store network/ kv kv_3e53aaab Network team secret storage secret/ kv kv_d66e2adc key/value secret storage
sys/ system system_d6f218a9 system endpoints

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

Answer: C

NEW QUESTION 62
- (Topic 2)
True or False? The userpass auth method has the ability to access external services in order to provide authentication to Vault.

A. True
B. False

Answer: B

NEW QUESTION 64
- (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 67
- (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 72
- (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 77
- (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 82
- (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 86
- (Topic 2)
True or False? All Vault policies are deny by default.

A. True
B. False

Answer: A

NEW QUESTION 90
- (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 92
- (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 96
- (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 98
- (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 100
- (Topic 2)
Which of the following best describes the function of the Vault Secrets Operator in a Kubernetes environment?

A. It replaces the Kubernetes secrets API entirely and operates purely as a certificate authority for all workloads.
B. It is a standalone Vault server that automatically applies security policies and rotates root tokens.
C. It continuously reconciles and synchronizes secrets from Vault to Kubernetes, ensuring secrets are always updated
D. It provides an interface to dynamically provision Kubernetes clusters through Vault??s infrastructure secrets.

Answer: C

NEW QUESTION 104
- (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 105
- (Topic 2)
When Vault is sealed, which are the only two operations available to a Vault administrator? (Select two)

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

Answer: AE

NEW QUESTION 108
- (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 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 113
- (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 115
- (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 120
- (Topic 2)
You are trying to create a new orphan token but receiving a Permission Denied error. What capabilities are required to create this token without using a root token?

A. write privileges on the path auth/token
B. write privileges on the path sys/mounts
C. sudo privileges on the path auth/token/create
D. sudo privileges on the path sys/mounts/token

Answer: C

NEW QUESTION 125
- (Topic 2)
Holly has discovered that a highly privileged dynamic credential with a very long lease time was created, which could negatively impact the organization??s security. What command can Holly use to invalidate the credential so it can??t be used without affecting other credentials?

A. vault lease revoke aws/creds/admin/27e1b9a1-27b8-83d9-9fe0-d99d786bdc83
B. Holly would need to delete the credential on the cloud platform directly
C. vault lease revoke -all
D. vault lease revoke aws/creds/admin/*

Answer: A

NEW QUESTION 126
- (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 128
- (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 133
- (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 138
- (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 140
- (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 144
- (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 148
- (Topic 3)
Jarrad is an AWS engineer and has provisioned a new EC2 instance running MySQL since his application requires a specific MySQL version. He wants to integrate Vault into his workflow but is new to Vault. What secrets engine should Jarrad use to integrate this new database running in AWS?

A. azure
B. database
C. kv
D. aws

Answer: B

NEW QUESTION 151
- (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 154
- (Topic 3)
Elijah manages a legacy application that requires strict control over when its service account credentials change. Which type of credential should be used for this legacy application?

A. static
B. dynamic

Answer: A

NEW QUESTION 155
- (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 157
- (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 162
- (Topic 3)
Which of the following actions can be performed if you only had access to a token??s accessor? (Select four)

A. Look up a token??s properties

B. Renew the token
C. Retrieve the actual token ID
D. Revoke the token
E. Look up a token??s capabilities on a path

Answer: ABDE

NEW QUESTION 165
- (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 168
- (Topic 3)
When you are unsealing Vault using unseal keys, what are you actually doing?

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

Answer: C

NEW QUESTION 173
- (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 178
- (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 179
- (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 183
- (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 186
- (Topic 3)
What is the default TTL for tokens in Vault if one is not specified?

A. 24 hours (1 day)
B. 15 minutes
C. 768 hours (32 days)
D. 60 minutes (1 hour)

Answer: C

NEW QUESTION 189
- (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 193
- (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 196
- (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 200
- (Topic 3)
Tanner manages a data processing application and needs to be sure the data being processed is encrypted so it is securely stored post-processing. Which secrets engines can encrypt data? (Select three)

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

Answer: ABD

NEW QUESTION 204
- (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 205
- (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 206
- (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 209
- (Topic 3)
Thomas has authenticated to Vault using the API and has received the following response. What data must Thomas parse from the response in order to continue making requests to Vault?
text CollapseWrapCopy
{
"request_id": "65897160-fd8b-1f87-c24e-fdba14c9728e", "lease_id": "",
"renewable": false, "lease_duration": 0, "data": null, "wrap_info": null, "warnings": null, "auth": {
"client_token": "hvss.IzrmRe5Y3LMcDRmOttEjWoagd92fD29fxakwej_38djs", "accessor": "EMX0nv4nr0Y1wXoaN7i0WDW1",
"policies": ["bryan", "default"], "token_policies": ["bryan", "default"], "metadata": {"username": "bryan"}, "lease_duration": 2764800, "renewable": true,
"entity_id": "40e203e8-818e-b6ad-4cb3-0befdbf9b598", "token_type": "service",
"orphan": true
}
}

A. accessor
B. request_id
C. client_token
D. entity_id

Answer: C

NEW QUESTION 211
- (Topic 4)
Over a few years, you have a lot of data that has been encrypted by older versions of a Transit encryption key. Due to compliance regulations, you have to re-encrypt the data using the newest version of the encryption key. What is the easiest way to complete this task without putting the data at risk?

A. Rotate the encryption key used to encrypt the data
B. Decrypt the data manually and encrypt it with the latest version
C. Use the transit rewrap feature
D. Create a new master key used by Vault

Answer: C

NEW QUESTION 212
- (Topic 4)
Why are short-lived, dynamic secrets in Vault more secure than long-lived, static credentials?

A. They provide better performance by caching credentials for longer durations
B. They are created on-demand and expire after a short period, minimizing the risk of credential leakage
C. They eliminate the need for authentication, allowing seamless access to Vault-managed systems
D. They automatically rotate on a set schedule, reducing the need for manual intervention

Answer: B

NEW QUESTION 215
- (Topic 4)
A developer team requests integration of their legacy application with Vault to encrypt and decrypt data for a backend database. They cannot modify the application for Vault authentication. What is the best way to achieve this integration?

A. Enable the Transit secrets engine and configure the secrets engine to send data directly to the legacy app
B. Have the app team call the Vault API to encrypt and decrypt the required data
C. Enable and configure the Kubernetes auth method to allow the application to authenticate to Vault using a JWT
D. Run the Vault Agent on the application server(s) and use the Auto Auth feature to manage the tokens

Answer: D

NEW QUESTION 219
- (Topic 4)
You are the primary Vault operator. During a routine audit, an auditor requested the ability to display all secrets under a specific path in Vault without seeing the actual stored data. Which policy permits the auditor to display the stored secrets without revealing their contents?

A. path "kv/apps/production/" { capabilities = ["list"] }
B. path "kv/apps/+/" { capabilities = ["list"] }
C. path "kv/+/production" { capabilities = ["list"] }
D. path "kv/apps/*" { capabilities = ["list", "read"] }

Answer: C

NEW QUESTION 224
- (Topic 4)
Sara uses the Vault CLI for administrative tasks on the production cluster. However, she encounters permission-denied errors when making changes and needs to check which policies are attached to her token to view and adjust permissions. What command can she run on the Vault node to see the attached policies?

A. vault operator diagnose
B. vault policy list
C. vault token capabilities
D. vault token lookup

Answer: D

NEW QUESTION 228
- (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 229
- (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 230
- (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 233
- (Topic 4)

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

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

Answer: C

NEW QUESTION 235
- (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 237
- (Topic 4)
A security architect is designing a solution to address the "Secret Zero" problem for a Kubernetes-based application that needs to authenticate to HashiCorp Vault. Which approach correctly leverages Vault features to solve this challenge?

A. Store the Vault root token in a ConfigMap and mount it to all containers that require access to sensitive information
B. Generate a long-lived token during deployment and store it as an environment variable within each container that needs to access Vault
C. Configure the Kubernetes auth method in Vault and enable applications to authenticate without pre-shared secrets
D. Implement a custom sidecar container that uses AppRole role-id and secret-id each time the application needs to access Vault

Answer: C

NEW QUESTION 242
- (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 247
- (Topic 4)
You are planning to deploy a new Vault cluster for your organization and notice that Vault supports a wide variety of storage backends. You need high availability since you will have multiple applications relying on the Vault service. When building your cluster, can you choose any of the available storage backends?

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

Answer: B

NEW QUESTION 249
- (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 251
- (Topic 4)
Your organization is integrating its legacy application with Vault to improve its security. However, you have discovered that the application has issues when the token changes for authentication during testing. What type of token could be used to help alleviate this issue without compromising security?

A. Periodic Service Token
B. Root Token
C. Orphan Service Token
D. Batch Token

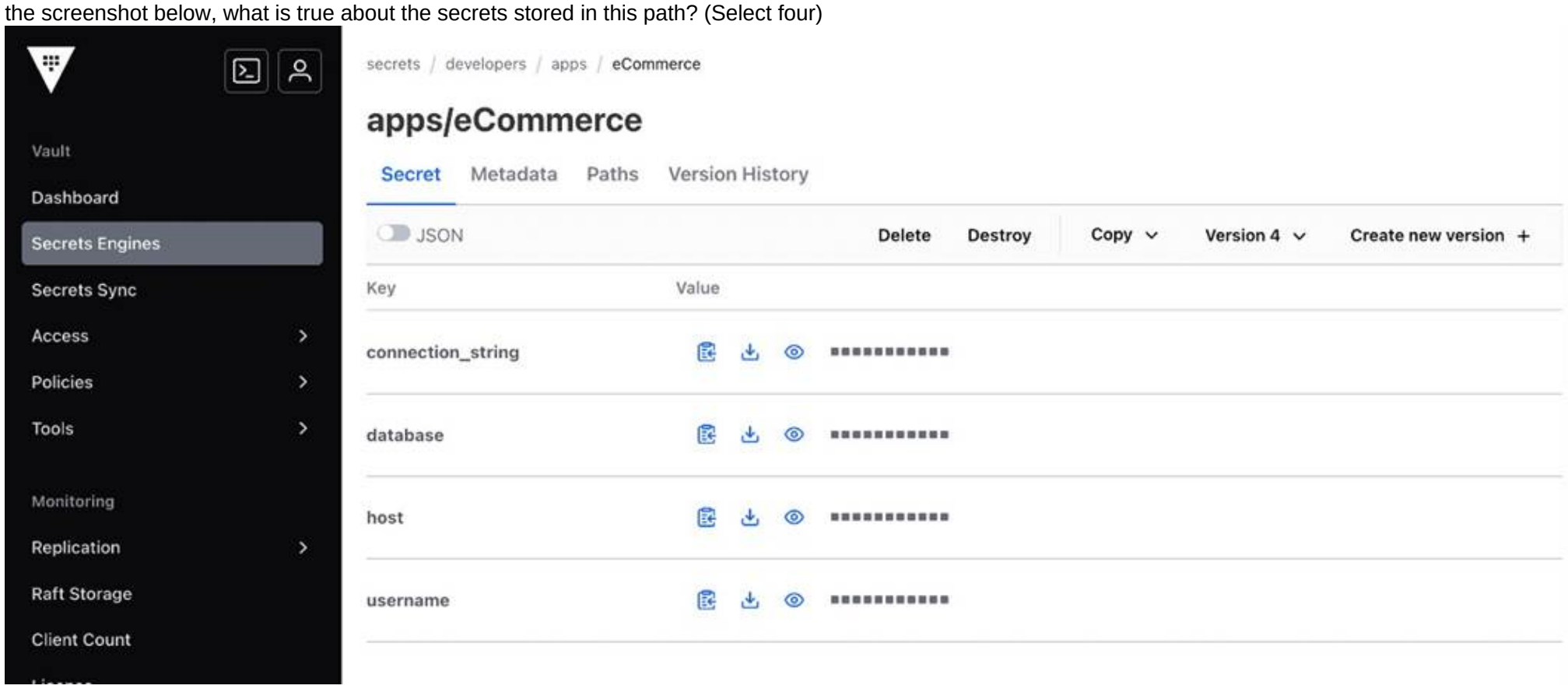
Answer: A

NEW QUESTION 256
- (Topic 4)
You have a CI/CD pipeline using Terraform to provision AWS resources with static privileged credentials. Your security team requests that you use Vault to limit AWS access when needed. How can you enhance this process and increase pipeline security?

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

Answer: D

NEW QUESTION 257
- (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 259
- (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 260
- (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 265
- (Topic 4)

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

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

Answer: D

NEW QUESTION 269
- (Topic 4)
You have enabled the Transit secrets engine on your Vault cluster to provide an "encryption as a service" service as your team develops new applications. What is a prime use case for the Transit secrets engine?

A. Encrypting data before being written to an Amazon S3 bucket
B. Storing the encrypted data in Vault for easy retrieval
C. Generating dynamic SSH credentials for access to local systems
D. Creating X.509 certificates for a new fleet of containers

Answer: A

NEW QUESTION 271
- (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 272
- (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 276
- (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 280
- (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 283
- (Topic 4)
What of the following features are true about batch tokens in Vault? (Select two)

A. Batch tokens are not persisted (written) to storage
B. Batch tokens can be renewed
C. Batch tokens are valid across all clusters when using Vault Enterprise replication
D. Batch tokens can create child tokens

Answer: AC

NEW QUESTION 288
- (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 290
- (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

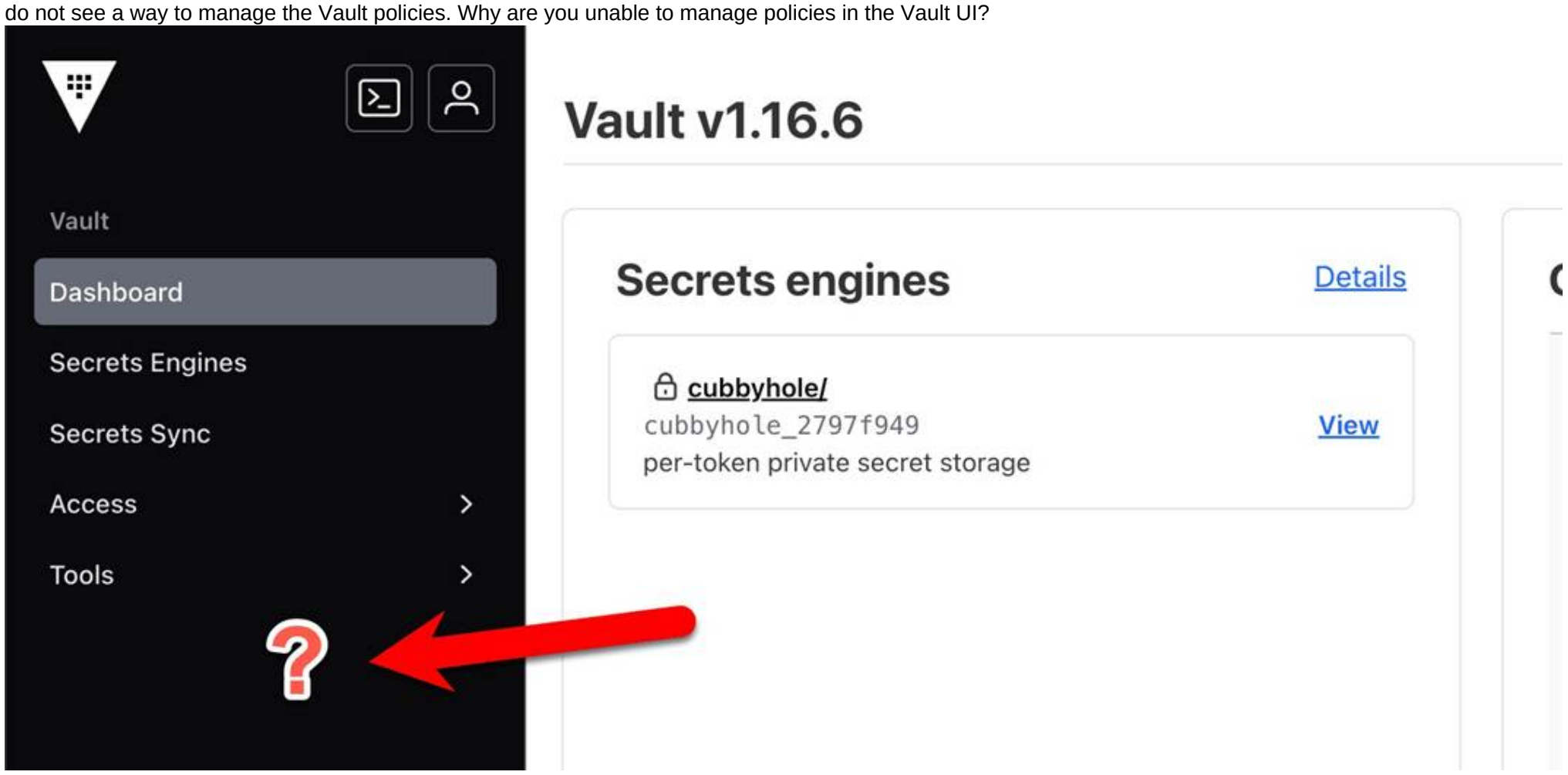
Answer: D

NEW QUESTION 295
- (Topic 4)
Your organization runs workloads on both AWS and Azure for production applications. The security team has requested that a single Vault authentication mechanism be enabled to support applications on both public cloud platforms. Which of the following would be a valid auth method you can use?

A. AWS
B. GitHub
C. AppRole
D. Azure

Answer: C

NEW QUESTION 299
- (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

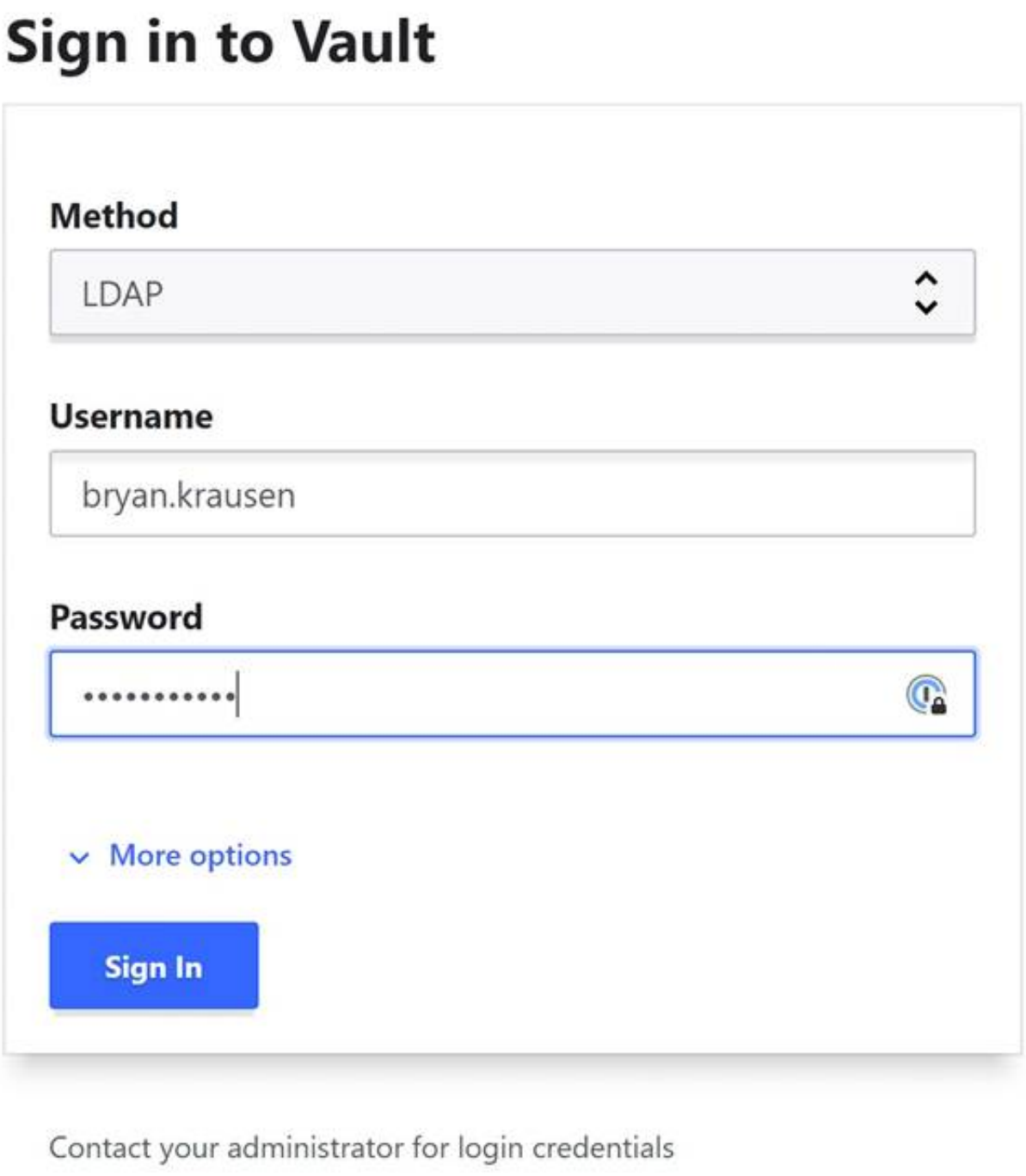
Answer: D

NEW QUESTION 300
- (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 302
- (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 303
- (Topic 4)
You have multiple Vault clusters in your environment, one for test and one for production. You have the CLI installed on your local machine and need to target the production cluster to make configuration changes. What environment variable can you set to target the production cluster?

A. VAULT_REDIRECT_ADDR
B. VAULT_CLUSTER_ADDR
C. VAULT_ADDR
D. VAULT_CAPATH

Answer: C

NEW QUESTION 308
- (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 311
- (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 313
- (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 316
- (Topic 5)
Which Vault secret engine may be used to build your own internal certificate authority?

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

Answer: B

NEW QUESTION 317
- (Topic 5)
Vault supports which type of configuration for source limited token?

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

Answer: C

NEW QUESTION 319
- (Topic 5)
The vault lease renew command increments the lease time from:

A. The current time
B. The end of the lease

Answer: A

NEW QUESTION 320
- (Topic 5)
What are orphan tokens?

A. Orphan tokens are tokens with a use limit so you can set the number of uses when you createthem
B. Orphan tokens are not children of their parent; therefore, orphan tokens do not expire when their parent does
C. Orphan tokens are tokens with no policies attached
D. Orphan tokens do not expire when their own max TTL is reached

Answer:

D

NEW QUESTION 323
- (Topic 5)
How would you describe the value of using the Vault transit secrets engine?

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

Answer: D

NEW QUESTION 328
- (Topic 5)
You are using the Vault userpass auth method mounted at auth/userpass. How do you create a new user named "sally" with password "h0wN0wB4r0wnC0w"? This new user will need the power-users policy.

A.
```
vault put auth/userpass/users/sally \
password=h0wN0wB4r0wnC0w \
policies=power-users
```

B.
```
vault write userpass/sally \
password=h0wN0wB4r0wnC0w \
policies=power-users
```

C.
```
vault kv write userpass/sally \
password=h0wN0wB4r0wnC0w \
policies=power-users
```

D.
```
vault write auth/userpass/users/sally \
password=h0wN0wB4r0wnC0w \
policies=power-users
```

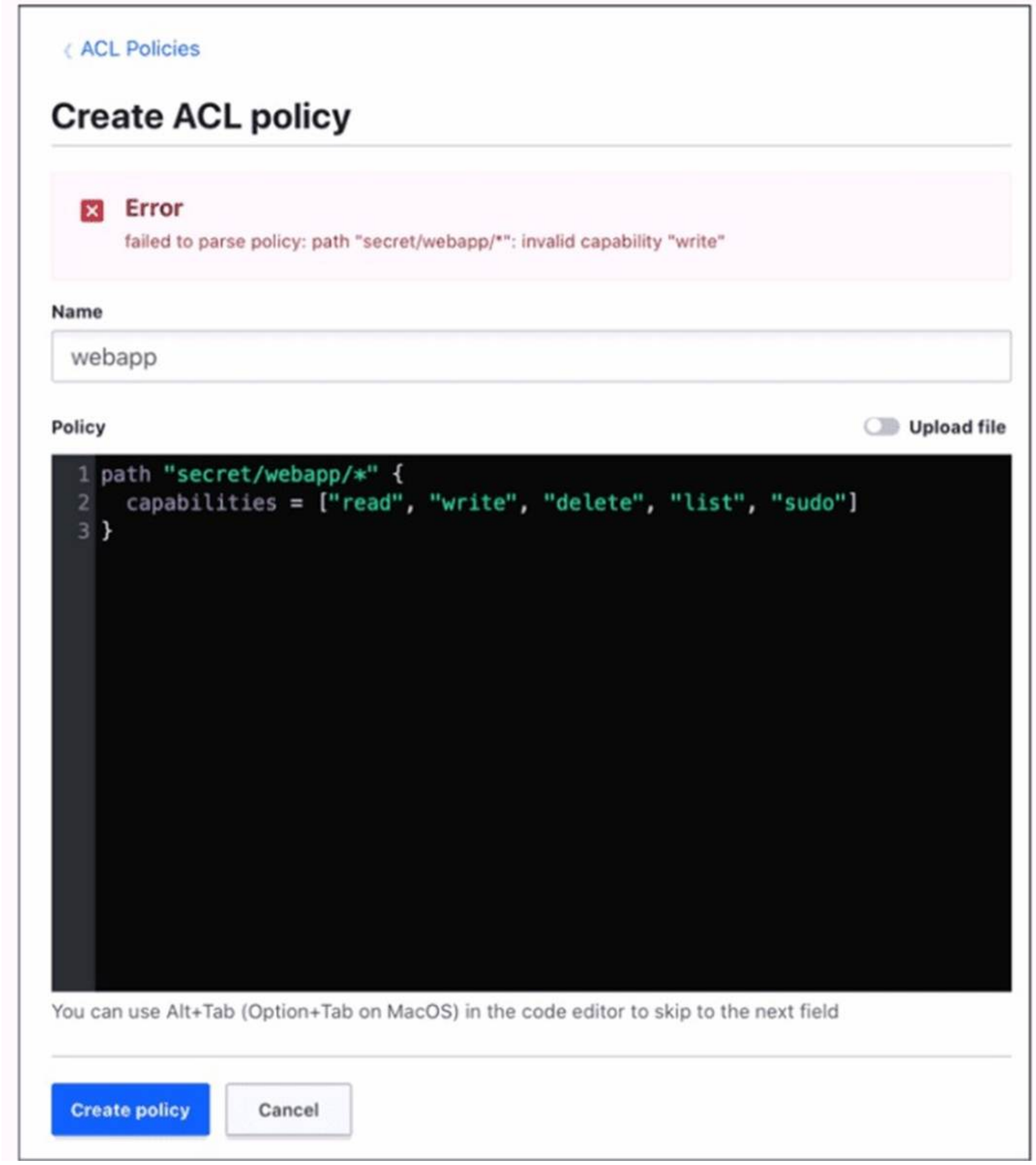
Answer: D

NEW QUESTION 329
- (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 334
- (Topic 5)
When creating a policy, an error was thrown:



Which statement describes the fix for this issue?

A. Replace write with create in the capabilities list
B. You cannot have a wildcard (" • ") in the path
C. sudo is not a capability

Answer: A

NEW QUESTION 336
- (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 339
- (Topic 5)
What command creates a secret with the key "my-password" and the value "53cr3t" at path "my-secrets" within the KV secrets engine mounted at "secret"?

A. vault kv put secret/my-secrets/my-password 53cr3t
B. vault kv write secret/my-secrets/my-password 53cr3t
C. vault kv write 53cr3t my-secrets/my-password
D. vault kv put secret/my-secrets »y-password-53cr3t

Answer: A

NEW QUESTION 341
- (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 342
- (Topic 5)
Examine the command below.Output has been trimmed.

```
  $ vault write auth/approle/login \
    role_id="debb8f13-79ea-3e3d-8100-10711d85c1fb" \
    secret_id="31d52faa-5b0b-711d-2ea2-c197cff6081b"Key Value
---                   -----
token                 b.AAAAAQIlWH-DExezQvz-ZGWMhzsy8uWXEoQYHH6O...trimmed...
token_accessor        n/a
token_duration        1m
token_renewable       false
token_policies        ["shipping"]
identity_policies     []
policies              ["shipping"]
token_meta_role_name  shipping
```

Which of the following statements describe the command and its output?

A. Missing a default token policy
B. Generated token's TTL is 60 hours
C. Generated token is an orphan token which can be renewed indefinitely
D. Configures the AppRole auth method with user specified role ID and secret ID

Answer: BC

NEW QUESTION 345
- (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 349
- (Topic 5)
You have a 2GB Base64 binary large object (blob) that needs to be encrypted. Which of the following best describes the transit secrets engine?

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

Answer: D

NEW QUESTION 354
- (Topic 5)
Which of the following are replication methods available in Vault Enterprise? Choose two correct answers.

A. Cluster sharding
B. Namespaces
C. Performance Replication
D. Disaster Recovery Replication

Answer: CD

NEW QUESTION 358
- (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

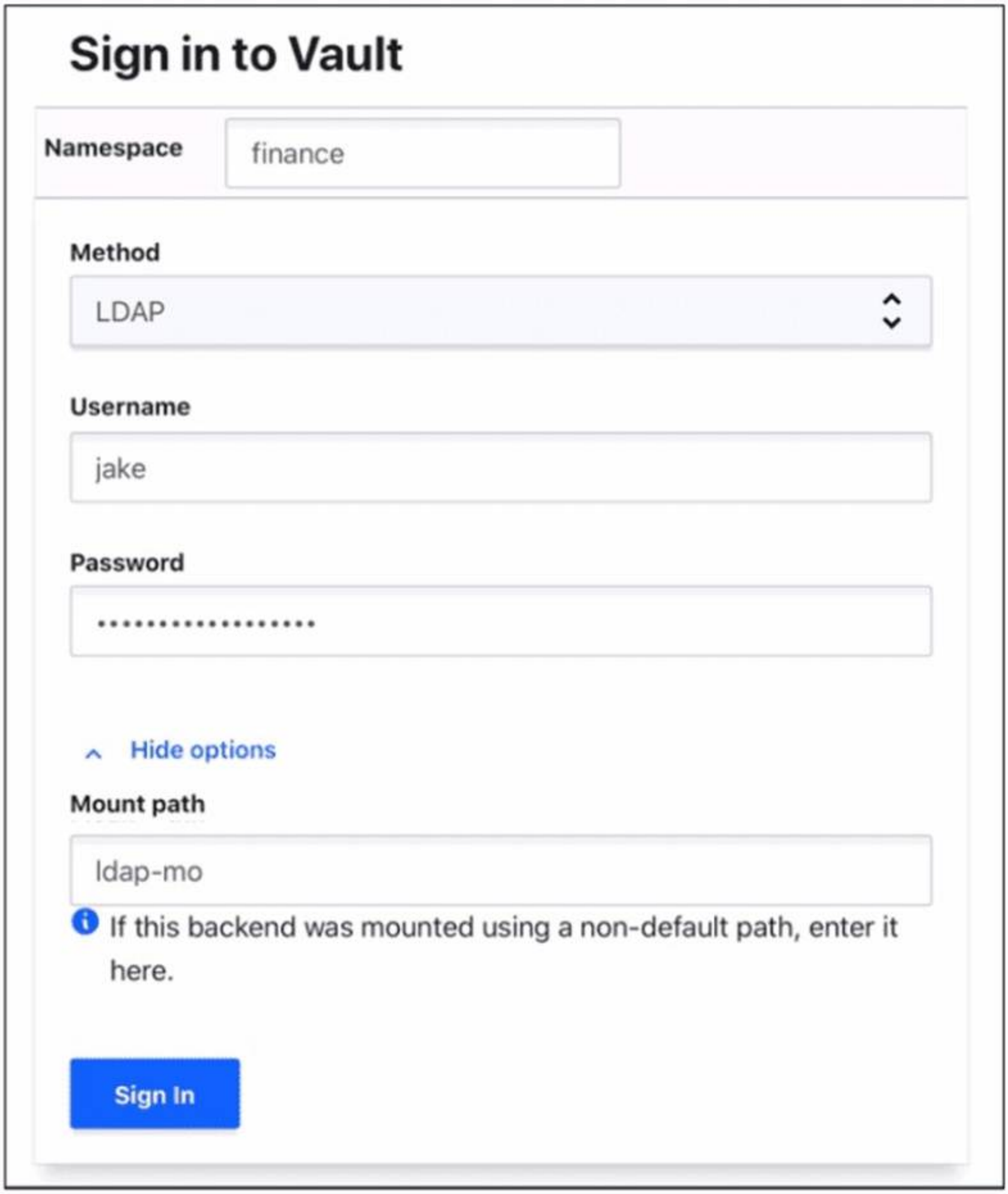
Answer: A

NEW QUESTION 359
- (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

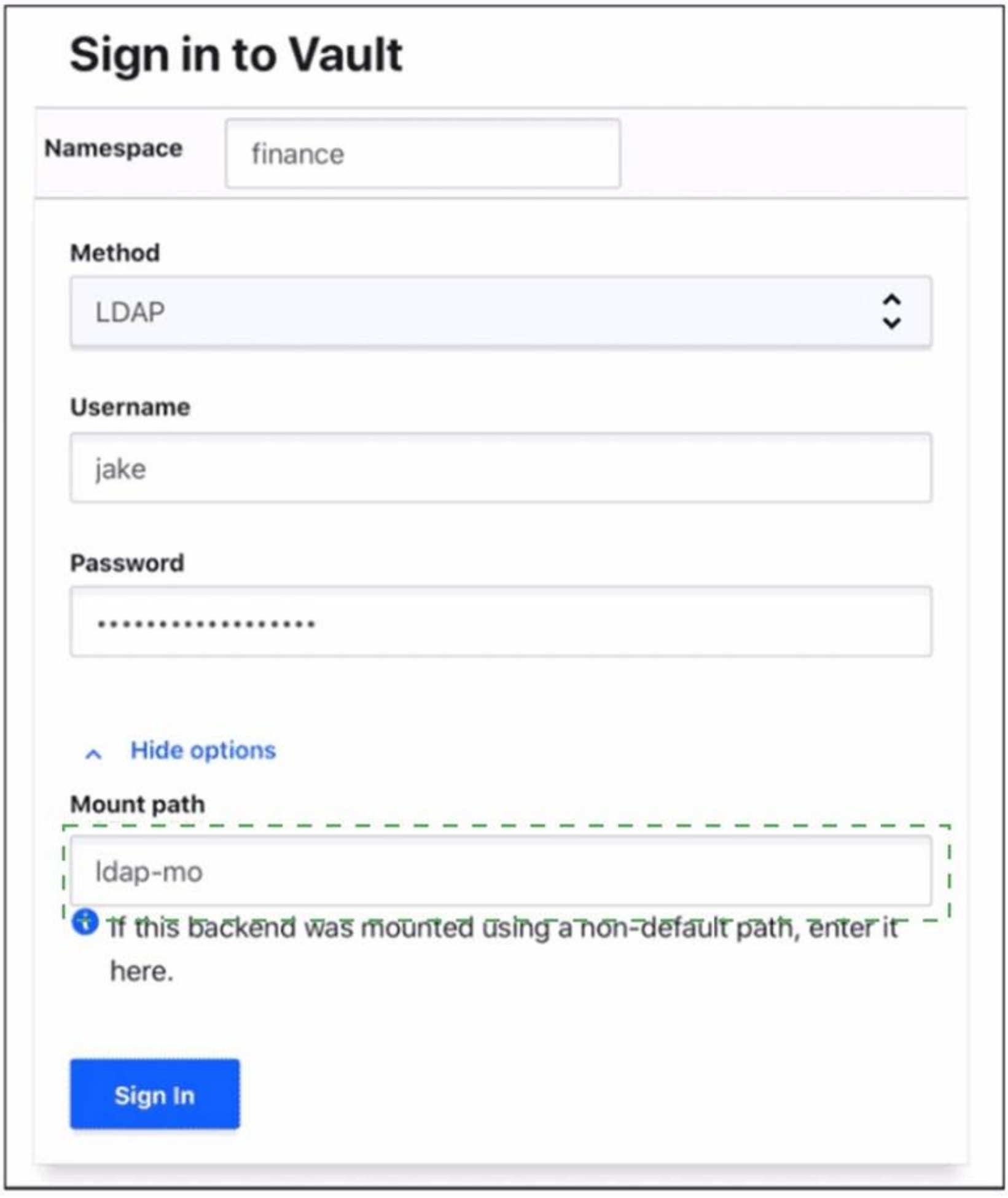
NEW QUESTION 361
HOTSPOT - (Topic 5)
Where do you define the Namespace to log into using the Vault Ul? To answer this question
Use your mouse to click on the screenshot in the location described above. An arrow indicator will mark where you have clicked. Click the "Answer" button once you have positioned 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 366
- (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.

B.

C.

D.

Answer: C

NEW QUESTION 369
- (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 373
- (Topic 5)
A developer mistakenly committed code that contained AWS S3 credentials into a public repository. You have been tasked with revoking the AWS S3 credential that was in the code. This credential was created using Vault's AWS secrets engine and the developer received the following output when requesting a credential from Vault.

```
Key                Value
---                -----
lease_id           aws/creds/s3-access/f3e92392-7d9c-09c8-c921-575d62fe80d8
lease_duration     768h
lease_renewable    true
access_key         AKIAIOWQXTLW36DV7IEA
secret_key         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
```

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

A. vault lease revoke aws/creds/s3-access/f3e92392-7d9c-99c8-c921-57Sd62fe89d8
B. vault lease revoke AKIAI0WQXTLW36DV7IEA
C. vault lease revoke f3e92392-7d9c-O9c8-c921-575d62fe80d8
D. vault lease revoke access_key-AKIAI0WQXTLW36DV7IEA

Answer: A

NEW QUESTION 378
- (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 381
- (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 382
- (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 387
- (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 388
- (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 392
- (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

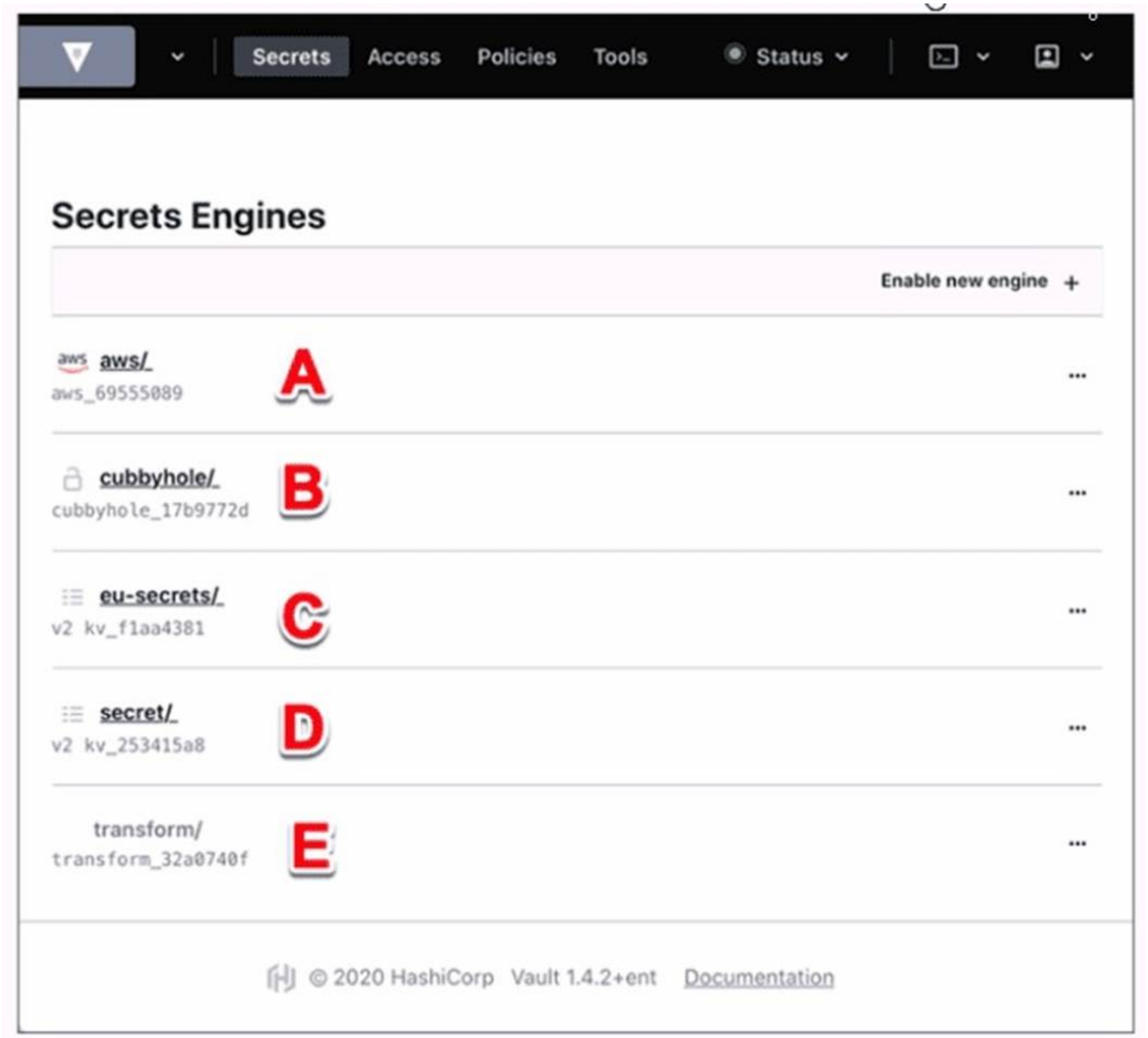
Answer: A

NEW QUESTION 393
- (Topic 5)
How many Shamir's key shares are required to unseal a Vault instance?

A. All key shares
B. A quorum of key shares
C. One or more keys
D. The threshold number of key shares

Answer: D

NEW QUESTION 397
- (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 399
- (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 404
.....

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