HashiCorp

Exam Questions HCVA0-003

HashiCorp Certified: Vault Associate (003)Exam

NEW QUESTION 1
- (Topic 1)
Based on the screenshot below, how many auth methods have been enabled on this Vault instance?

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

Answer: B

NEW QUESTION 2
- (Topic 1)
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)
You want to encrypt a credit card number using the Transit secrets engine. You enter the following command and receive an error. What can you do to ensure that the credit card number is properly encrypted and the ciphertext is returned?
$ vault write -format=json transit/encrypt/creditcards plaintext="1234 5678 9101 1121" Error: * illegal base64 data at input byte 4

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

Answer: A

NEW QUESTION 4
- (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 5
- (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 6
- (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 7
- (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.).
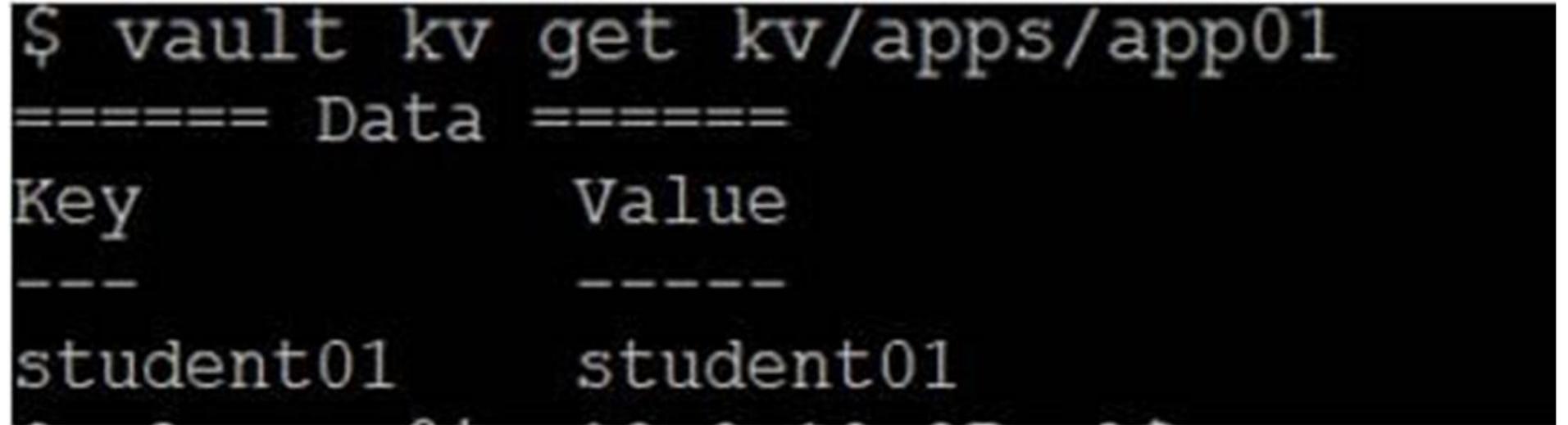
A. True
B. False

Answer: B

NEW QUESTION 8
- (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?
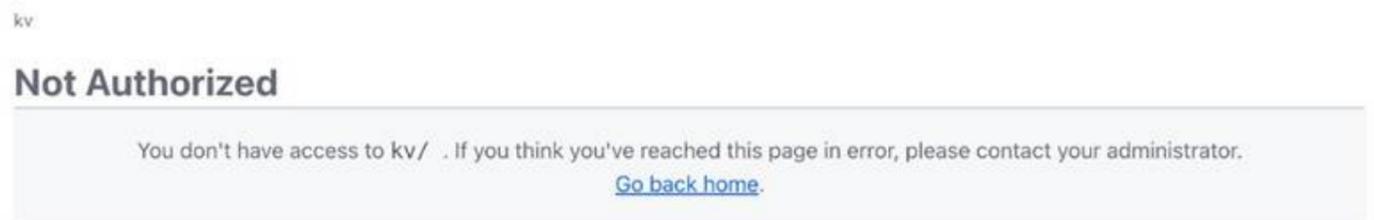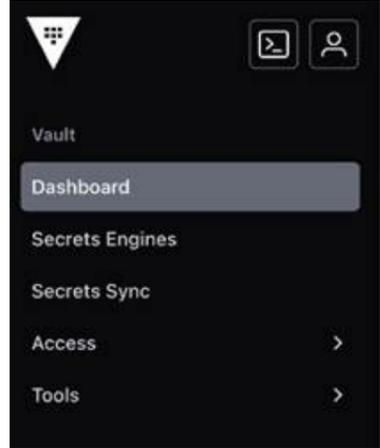path "kv/apps/app01" { capabilities = ["read"] }
Successful retrieval using the CLI

(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 9
- (Topic 1)
Which of the following token attributes can be used to renew a token in Vault (select two)?

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

Answer: BD

NEW QUESTION 10
- (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 10
- (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 14
- (Topic 2)
An application requires a specific key/value pair to be updated in order to process a batch job. Thevalue should be either "true" or "false." However, when developers have been updating the value, sometimes they mistype the value or capitalize the value, causing the batch job not to run. What feature of a Vault policy can be used to restrict entry to the required values?

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

Answer: B

NEW QUESTION 15
- (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 17
- (Topic 2)
Which of the following best describes a token accessor?

A. A value that describes which clients have access to the attached token
B. Describes the value associated with the token??s TTL
C. A token used for clients to access Vault secrets engines
D. A value that acts as a reference to a token which can be used to perform limited actions against the token

Answer: D

NEW QUESTION 21
- (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 23
- (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 27
- (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 31
- (Topic 2)
Which two interfaces automatically assume the token for subsequent requests after successfully authenticating? (Select two)

A. CLI
B. API
C. UI

Answer: AC

NEW QUESTION 36
- (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 38
- (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 39
- (Topic 2)
Which of the following auth methods is the best choice for human interaction with Vault (as opposed to machine/system authentication)?

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

Answer: D

NEW QUESTION 43
- (Topic 2)
Which isnota capability that can be used when writing a Vault policy?

A. delete
B. modify
C. create
D. list

E. read
F. update

Answer: B

NEW QUESTION 44
- (Topic 2)
What is the default method of authentication after first initializing Vault?

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

Answer: D

NEW QUESTION 49
- (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 51
- (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 55
- (Topic 2)
You have a long-running app that cannot handle a regeneration of a token or secret. What type of token should be created for this application in order to authenticate and interact with Vault?

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

Answer: B

NEW QUESTION 58
- (Topic 2)
An application has authenticated to Vault and has obtained dynamic database credentials with a lease of 4 hours. Four hours later, the credentials expire, and the application can no longer communicate with the backend database, so the application goes down. What should the developers instruct the application to do to prevent this from happening again while maintaining the same level of security?

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

Answer: B

NEW QUESTION 61
- (Topic 3)
Select the two paths below that would be permitted for read access based on the following Vault policy:
path "secret/+/training/*" { capabilities = ["create", "read"]
}

A. secret/business/training
B. secret/cloud/training/test/exam
C. secret/departments/certification/api
D. secret/departments/training/vault

Answer: BD

NEW QUESTION 63
- (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 67
- (Topic 3)
Your organization operates active/active applications across multiple data centers for high availability. Which Vault feature should be used in the secondary data centers to provide local access to secrets?

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

Answer: D

NEW QUESTION 68
- (Topic 3)
In Vault, there are two main types of tokens, batch and service. Which of the following is true about the renewable capabilities of each?

A. Batch tokens cannot be renewed, but service can be renewed up to the max TTL
B. Tokens cannot be renewed without reauthenticating to Vault
C. Service tokens cannot be renewed, but batch can be renewed up to the max TTL
D. Both batch and service tokens can be renewed up to the max TTL

Answer: A

NEW QUESTION 69
- (Topic 3)
You are considering using HCP Vault Dedicated but are concerned about differences between a hosted version and a self-hosted deployment. Which of the following statements is true about HCP Vault Dedicated?

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

Answer: A

NEW QUESTION 71
- (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 75
- (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 77
- (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 78
- (Topic 3)
You need to decrypt customer data to provide it to an application. When you run the decryption command, you get the output below. Why does the response not directly reveal the cleartext data?
$ vault write transit/decrypt/phone_number ciphertext="vault:v1:tgx2vsxtlQRfyLSKvem..." Key Value
--- -----
plaintext aGFzaGljb3JwIGNlcnRpZmllZDogdmF1bHQgYXNzb2NpYXRl

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

Answer: B

NEW QUESTION 83
- (Topic 4)
A developer has requested access to manage secrets at the path kv/apps/webapp01. You create the policy below which gives them the proper access:
path "kv/apps/webapp01" {
capabilities = ["read", "create", "update", "list"]
}
However, when the developer logs in to the Vault UI, they see the following screenshot and cannot access the desired secret. Why can??t the developer see the secrets they need?
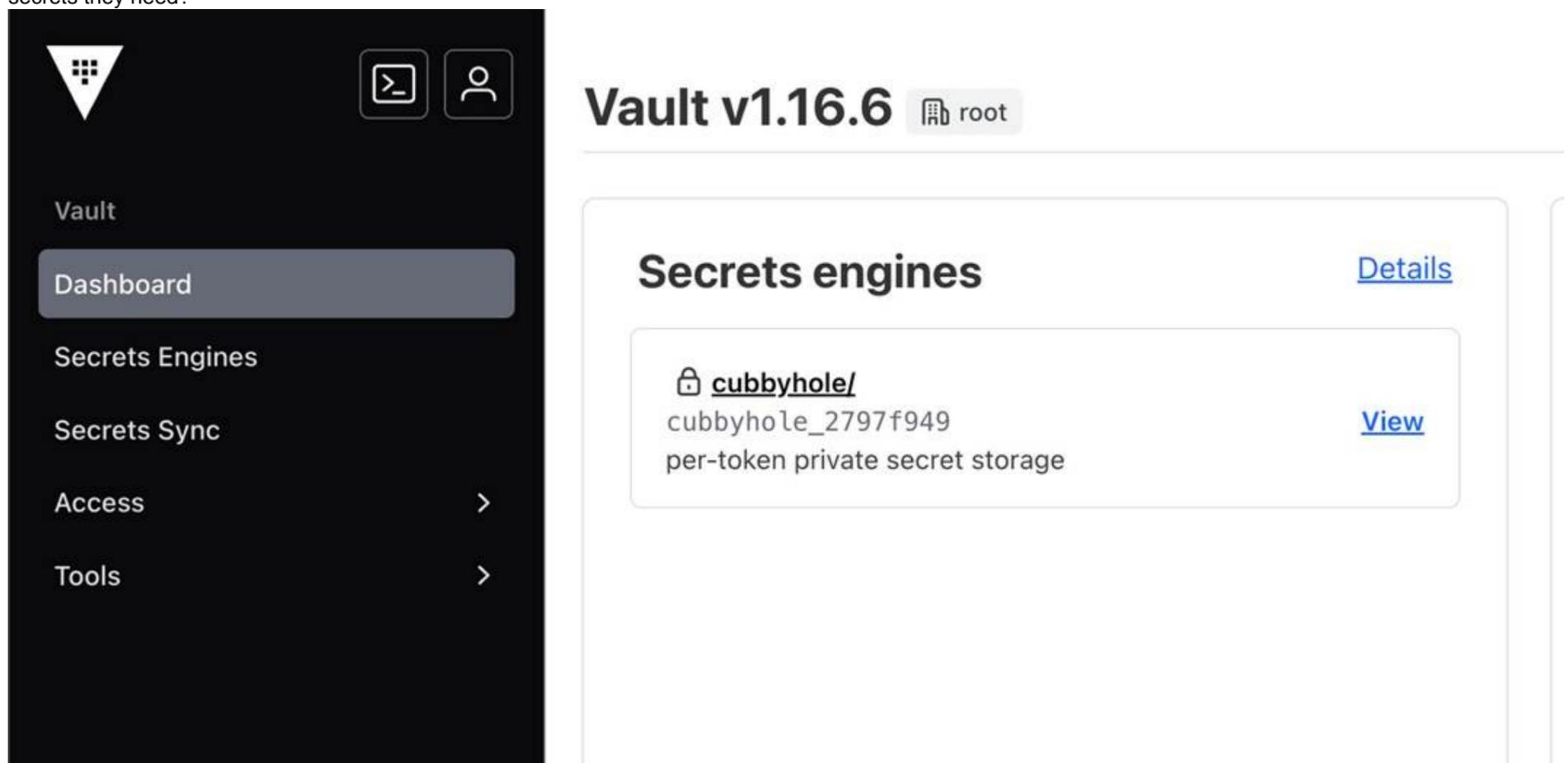
A. The Vault UI isn??t enabled for the developer, therefore they will only see the default options
B. The key/value secrets engine isn??t available in the Vault UI, therefore the developer should use a different Vault interface instead
C. The policy doesn??t permit list access to the paths prior to the secret so the Vault UI doesn??t display the mount path
D. The secrets are stored under the cubbyhole secrets engine, so the developer should browse to that secrets engine

Answer: C

NEW QUESTION 86
- (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 87
- (Topic 4)
Your co-worker has asked you to perform certain operations in Vault and has provided you with a token accessor (not the token itself). What Vault operations would you be allowed to perform using only the provided accessor? (Select three)

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

Answer: ABD

NEW QUESTION 88
- (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 92
- (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 93
- (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 97
- (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 102
- (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 105
- (Topic 4)
You need to write a new policy for Vault for a group of users on the automation team. The requirements stipulate that each user (and all future users) get access to their own private section of a KV secrets engine at the path kv/team/ and be able to manage their own secrets. Which policy below meets these requirements while minimizing the administrative effort and following the principle of least privilege?

A. path "secret/data/groups/{{identity.groups.ids.2f62-9503-42aa7A869741.name}}/" { capabilities = ["list"] }

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

Answer: D

NEW QUESTION 107
- (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 110
- (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 112
- (Topic 4)
You are planning the deployment of your first Vault cluster and have decided to use Integrated Storage as the storage backend. Where do you configure the storage backend to be used by Vault?

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

Answer: C

NEW QUESTION 115
- (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 119
- (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 123
- (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?
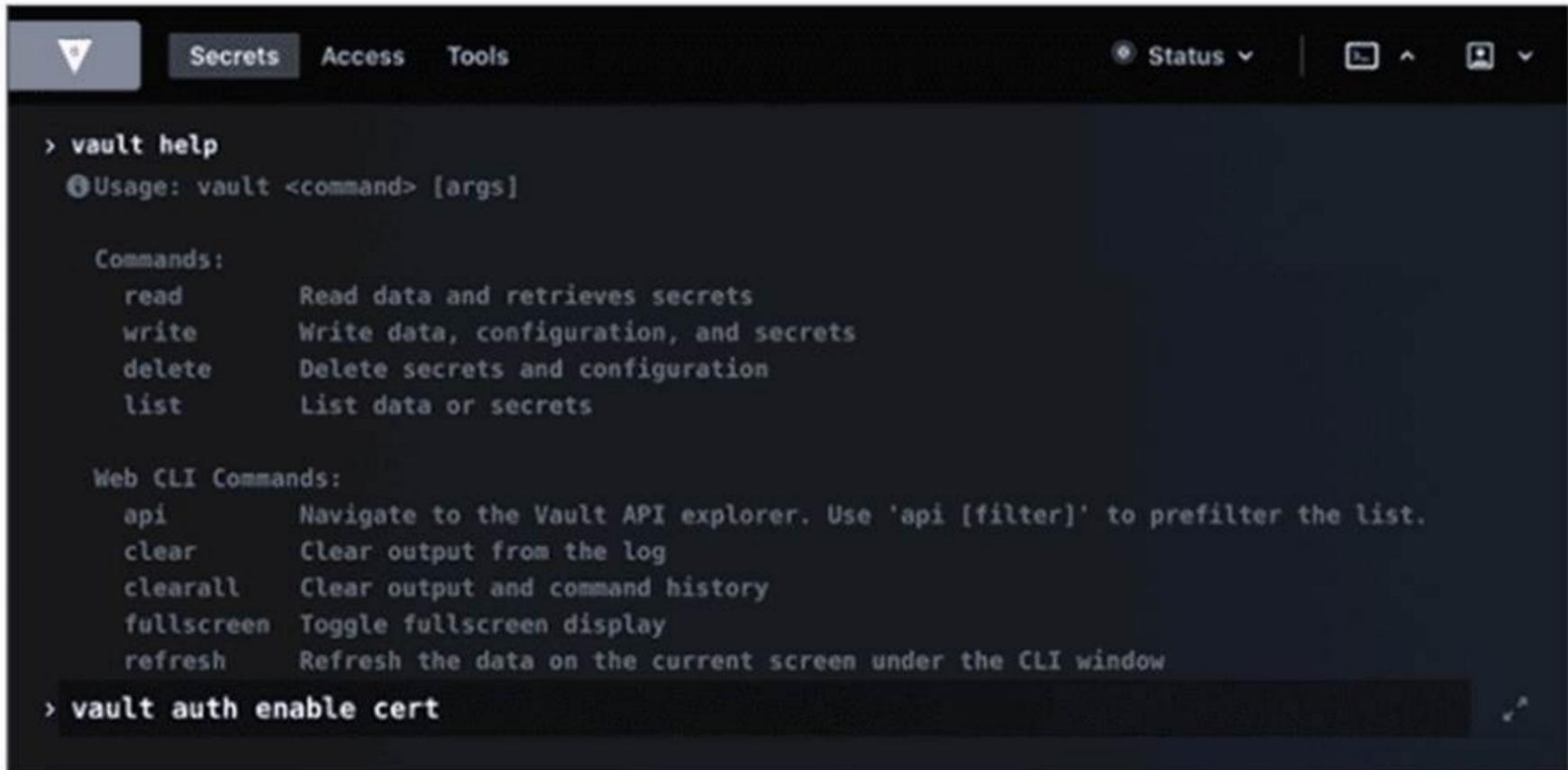B. Identity secrets engine
C. PKI secrets engine
D. SSH secrets engine

E. Transit secrets engine

Answer: B

NEW QUESTION 128
- (Topic 5)
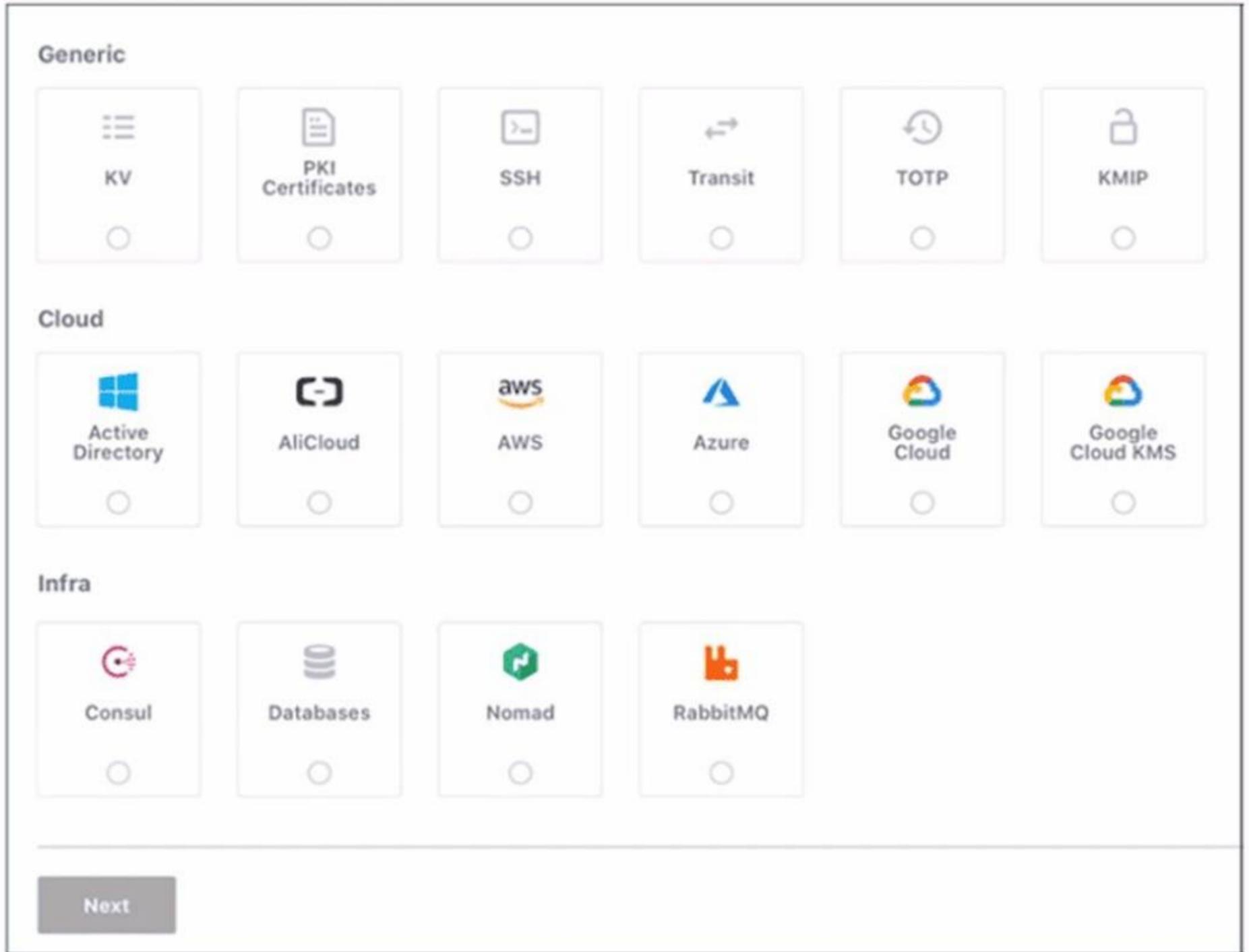Running the second command in the GUI CLI will succeed.

A. True
B. False

Answer: B

NEW QUESTION 131
- (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 133
- (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 136
- (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 138
- (Topic 5)
What is the Vault CLI command to query information about the token the client is currently using?

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

Answer: B

NEW QUESTION 141
- (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 143
- (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 145
- (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 150
- (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 155
- (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 156
- (Topic 5)
Which of the following statements describe the secrets engine in Vault? Choose three correct answers.

A. Some secrets engines simply store and read data
B. Once enabled, you cannot disable the secrets engine
C. You can build your own custom secrets engine
D. Each secrets engine is isolated to its path
E. A secrets engine cannot be enabled at multiple paths

Answer: ACD

NEW QUESTION 158
......