HashiCorp

Exam Questions HCVA0-003

HashiCorp Certified: Vault Associate (003)Exam

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

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

Answer: BCDE

NEW QUESTION 2
- (Topic 1)
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)
True or False? The Vault Secrets Operator does NOT encrypt client cache, such as Vault tokens and leases, by default in Kubernetes Secrets.

A. True
B. False

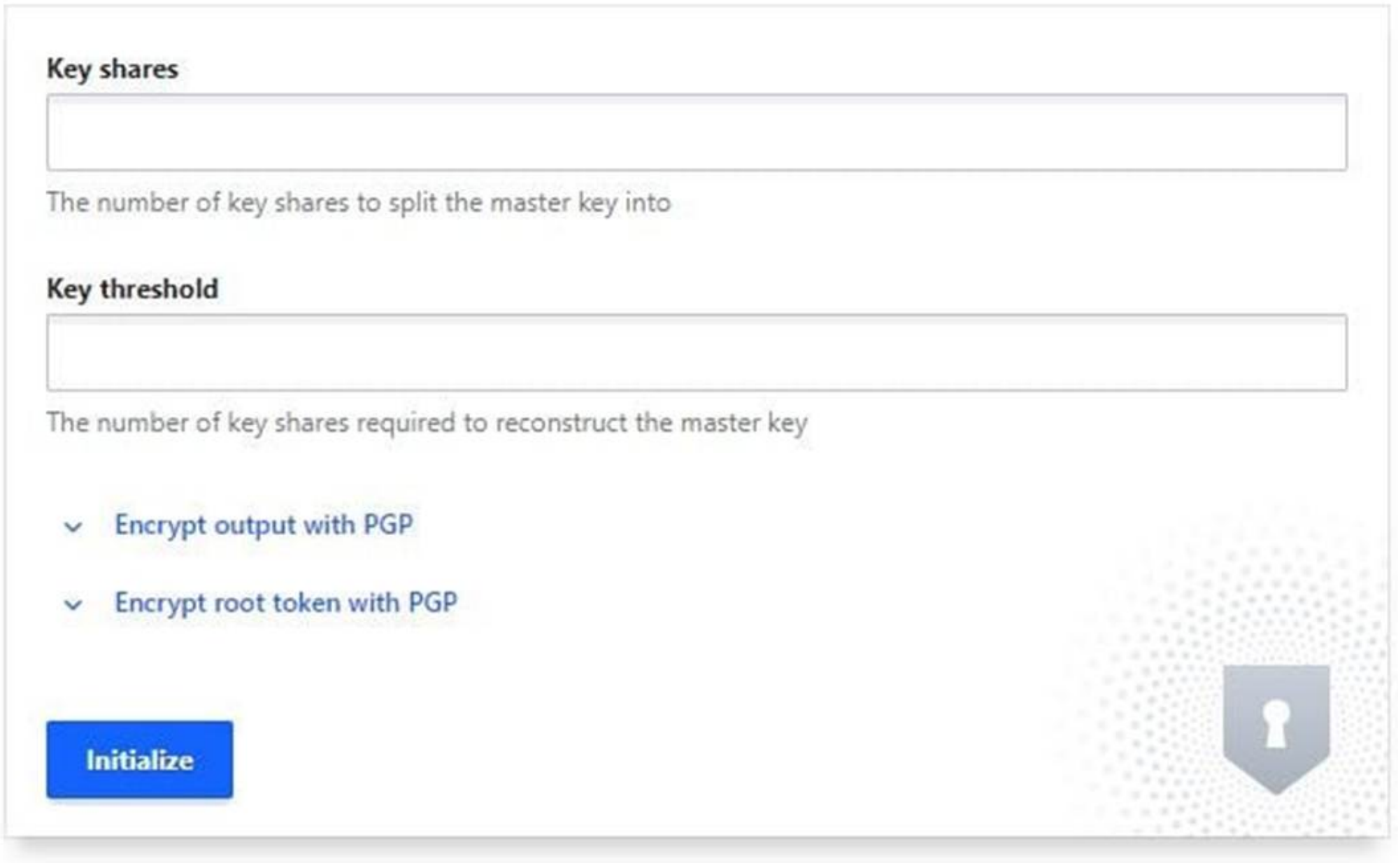
Answer: A

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

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

Answer: ABC

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



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

Answer: B

NEW QUESTION 7
- (Topic 1)
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 8
- (Topic 1)
Which of the following policies would permit a user to generate dynamic credentials on a database?

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

Answer: D

NEW QUESTION 9
- (Topic 1)
How long does the Transit secrets engine store the resulting ciphertext by default?

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

Answer: D

NEW QUESTION 10
- (Topic 1)

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

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

Answer: A

NEW QUESTION 10
- (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 13
- (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 16
- (Topic 2)
After a client has authenticated to Vault, what security feature is used to make all subsequent calls?

A. ldap
B. pgp
C. path
D. key shard
E. listener
F. token

Answer: F

NEW QUESTION 18
- (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 23
- (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 24
- (Topic 2)

Mike??s Cereal Shack uses Vault to encrypt customer data to ensure it is always stored securely. They are developing a new application integration to send new customer data to be encrypted using the following API request: text
CollapseWrapCopy
$ curl \
--header "X-Vault-Token: hvs.sf4vj1rFV5PvQSV3M9dcv832brxQFsfbXA" \
--request POST \
--data @data.json \ https://vault.mcshack.com:8200/v1/transit/encrypt/customer-data What would be contained within the data.json file?

A. Transit secrets engine configuration file
B. Ciphertext to be decrypted
C. The encryption key to be used for encrypting the data
D. Cleartext customer data to be encrypted

Answer: D

NEW QUESTION 27
- (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 29
- (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 30
- (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 31
- (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 34
- (Topic 2)
What type of Vault token does not have a TTL (Time to Live)?

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

Answer: D

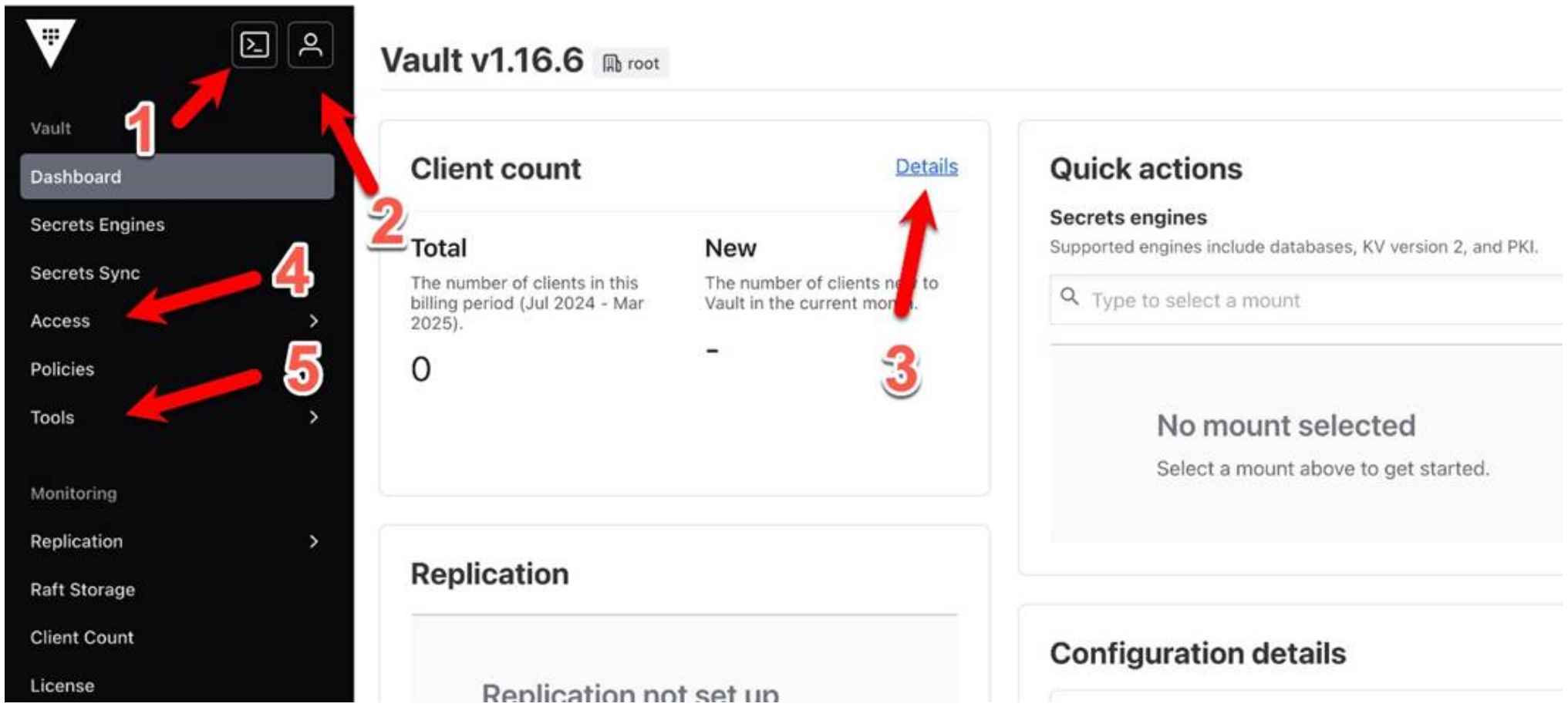
NEW QUESTION 36
- (Topic 2)
Which of the following are benefits of using the Vault Secrets Operator (VSO)? (Select three)

A. Support for syncing from multiple secret sources

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

Answer: ACD

NEW QUESTION 41
- (Topic 2)
Without logging into another interface, what feature can Chad use to execute a simple CLI command to enable a new secrets engine?



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

Answer: A

NEW QUESTION 42
- (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 45
- (Topic 3)
True or False? The root and default policies can be deleted if they are not needed or being used.

A. True
B. False

Answer: B

NEW QUESTION 48
- (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 51
- (Topic 3)
What command can be used to revoke all leases associated with a database role named prod-mysql?

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

Answer: B

NEW QUESTION 52
- (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 55
- (Topic 3)
True or False? You can create and update Vault policies using the UI.

A. True
B. False

Answer: A

NEW QUESTION 59
- (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 60
- (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 65
- (Topic 3)
True or False? Once the lease for a dynamic secret has expired, Vault revokes the credentials on the backend platform for which they were created (i.e., database, AWS, Kubernetes).

A. True
B. False

Answer: A

NEW QUESTION 66
- (Topic 3)
You need to create a limited-privileged token that isn??t impacted by the TTL of its parent. What type of token should you create?

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

Answer: B

NEW QUESTION 70
- (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 75
- (Topic 3)
Which of the following best describes response wrapping?

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

Answer: D

NEW QUESTION 76
- (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 79
- (Topic 3)
True or False? Once you authenticate to Vault using the API, subsequent requests will automatically be permitted without further interaction.

A. True
B. False

Answer: B

NEW QUESTION 81
- (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 84
- (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 87
- (Topic 3)
When a lease is created, what actions can be performed by using only the lease ID? (Choose two)

A. Renew the lease
B. Revoke the lease
C. Extend the max TTL for the lease

D. Authenticate using the lease ID

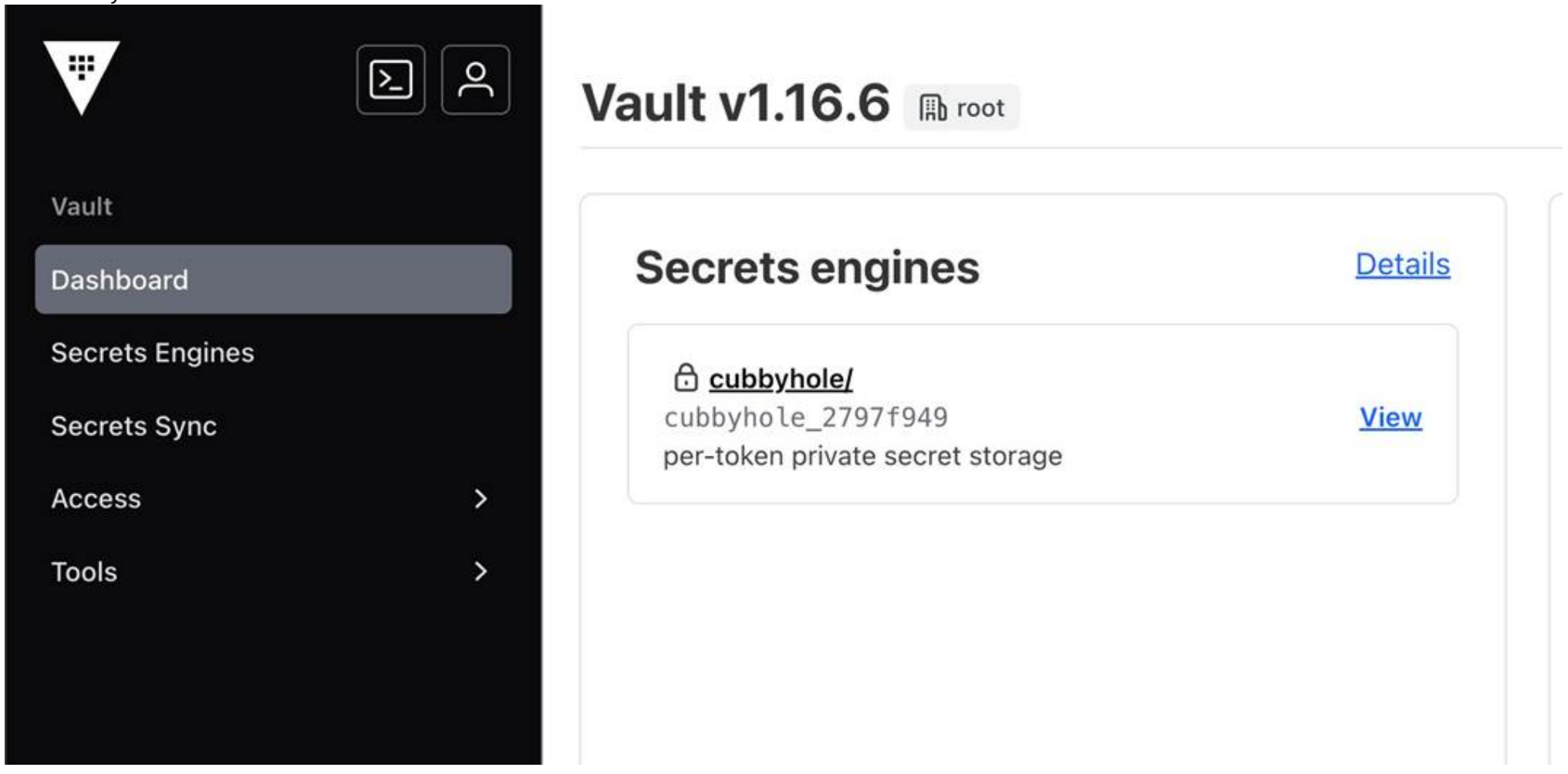
Answer: AB

NEW QUESTION 89
- (Topic 4)
A new application is being provisioned in your environment. The application requires the generation of dynamic credentials against the Oracle database in order to read reporting data. Which is the best auth method to use to permit the application to authenticate to Vault?

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

Answer: D

NEW QUESTION 90
- (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 91
- (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)
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 94
- (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 98
- (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 99
- (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 100
- (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 102
- (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 103
- (Topic 4)
Which core component of Vault can store, generate, or encrypt data for organizations?

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

Answer: C

NEW QUESTION 104
- (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 108
- (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 113
- (Topic 5)
Where does the Vault Agent store its cache?

A. In a file encrypted using the Vault transit secret engine
B. In the Vault key/value store
C. In an unencrypted file
D. In memory

Answer: D

NEW QUESTION 116
- (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 117
- (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 121
- (Topic 5)
Which of the following describes the Vault's auth method component?

A. It verifies a client against an internal or external system, and generates a token with the appropriate policies attached
B. It verifies a client against an internal or external system, and generates a token with root policy
C. It is responsible for durable storage of client tokens
D. It dynamically generates a unique set of secrets with appropriate permissions attached

Answer: A

NEW QUESTION 123
- (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 126
- (Topic 5)
What environment variable overrides the CLI's default Vault server address?

A. VAULT_ADDR
B. VAULT_HTTP_ADORESS
C. VAULT_ADDRESS
D. VAULT _HTTPS_ ADDRESS

Answer: B

NEW QUESTION 128
.....

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