HashiCorp

Exam Questions HCVA0-003

HashiCorp Certified: Vault Associate (003)Exam

NEW QUESTION 1
- (Topic 1)
During a service outage, you must ensure all current tokens and leases are copied to another Vault cluster for failover so applications don??t need to authenticate. How can you accomplish this?

A. Have Vault write all the tokens and leases to a file so you have a second copy of them
B. Configure all applications to use the auto-auth feature of the Vault Agent
C. Configure Disaster Recovery replication and promote the secondary cluster during an outage
D. Replicate to another cluster using Performance Replication and promote the secondary cluster during an outage

Answer: C

NEW QUESTION 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"] }

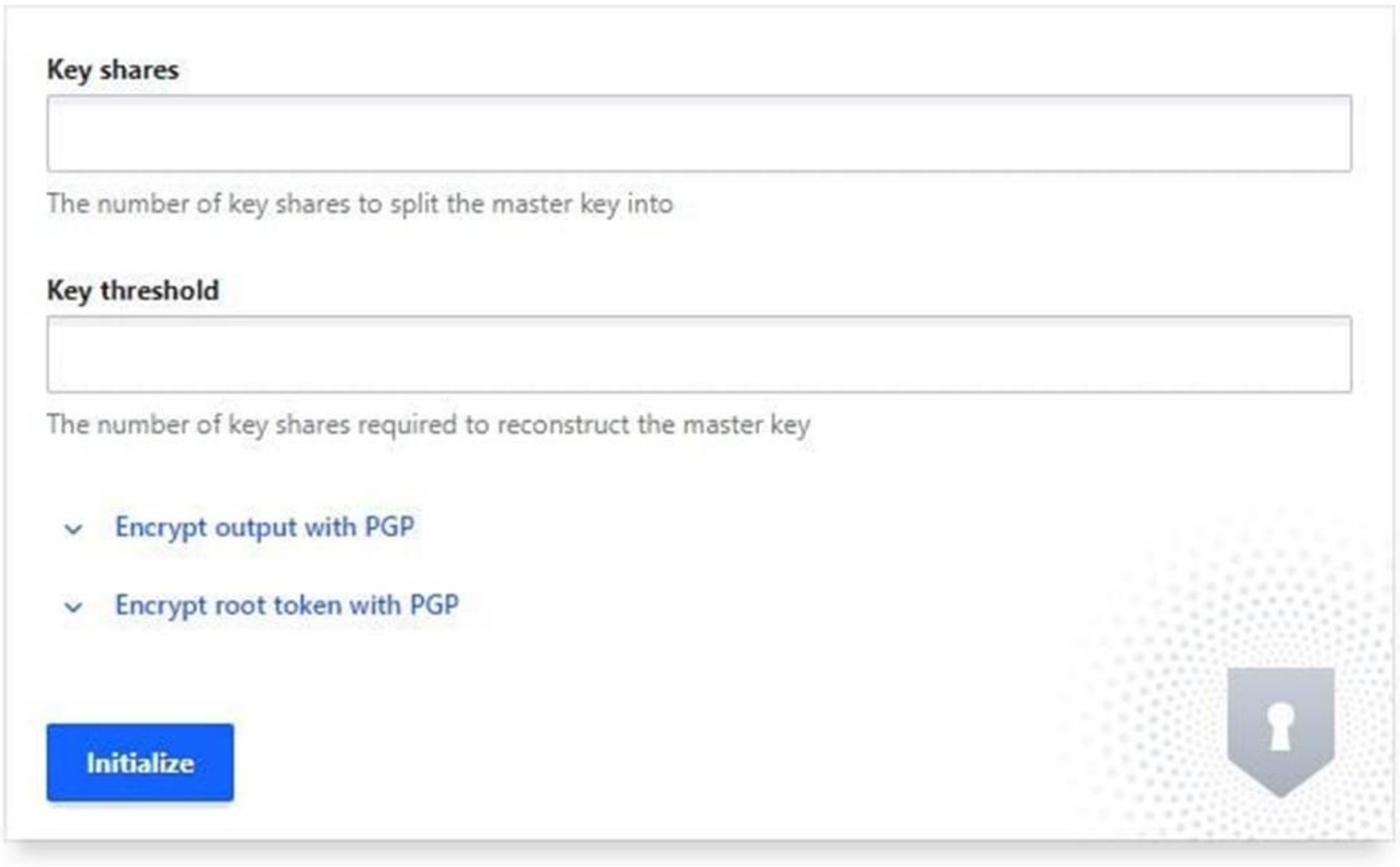
Answer: A

NEW QUESTION 3
- (Topic 1)
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 4
- (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 5
- (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 6
- (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 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)
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 9
- (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 10
- (Topic 1)
What API endpoint is used to manage secrets engines in Vault?

A. /secret-engines/
B. /sys/mounts
C. /sys/capabilities
D. /sys/kv

Answer: B

NEW QUESTION 10
- (Topic 1)
Which of the following Vault policies will allow a Vault client to read a secret stored at secrets/applications/app01/api_key?

A. path "secrets/applications/" { capabilities = ["read"] allowed_parameters = { "certificate" = [] } }
B. path "secrets/*" { capabilities = ["list"] }
C. path "secrets/applications/+/api_*" { capabilities = ["read"] }
D. path "secrets/applications/app01/api_key/*" { capabilities = ["update", "list", "read"] }

Answer: C

NEW QUESTION 11
- (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 16
- (Topic 1)
Which of the following statements best describes the difference in cluster strategies between self-managed Vault and HashiCorp-managed Vault?

A. Self-managed clusters require users to handle setup, maintenance, and scaling, whereas HCP Vault Dedicated is fully managed by HashiCorp and offloads most operational tasks
B. Neither self-managed clusters nor HCP Vault Dedicated include enterprise security features such as replication or disaster recovery
C. Both self-managed clusters and HCP Vault Dedicated require manual patching and upgrades, but only self-managed clusters are hosted in the user??s cloud
D. In self-managed clusters, HashiCorp is responsible for scaling, upgrades, and patching, while HCP Vault Dedicated requires the user to handle all operational overhead

Answer: A

NEW QUESTION 18
- (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 19
- (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 20
- (Topic 1)
True or False? Once you create a KV v1 secrets engine and place data in it, there is no way to modify the mount to include the features of a KV v2 secrets engine.

A. True
B. False

Answer: B

NEW QUESTION 24
- (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 29
- (Topic 2)
Christy has created a token and needs to use that token to access Vault. What command can she use to authenticate and access secrets stored in Vault?
$ vault token create -policy=christy Key Value
--- -----
token hvs.hxDIPd8RPVtxu4AzSGS1lArP token_accessor AxwxpDs6LbdFQbWGmBDnwIK3 token_duration 24h
token_renewable true token_policies ["christy" "default"] identity_policies []
policies ["christy" "default"]

A. vault login hvs.hxDIPd8RPVtxu4AzSGS1lArP
B. vault login -method=password
C. vault login -method=token christy
D. vault login -accessor=AxwxpDs6LbdFQbWGmBDnwIK3

Answer: A

NEW QUESTION 33
- (Topic 2)
After creating a dynamic credential on a database, the DBA accidentally deletes the credentials on the database itself. When attempting to remove the lease, Vault returns an error stating that the credential cannot be found. What command can be run to make Vault remove the secret?

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

Answer: A

NEW QUESTION 35
- (Topic 2)
Before the following command can be run to encrypt data, what (three) commands must be run to enable and configure the transit secrets engine in Vault? (Select three)
text CollapseWrapCopy
$ vault write transit/encrypt/vendor \ plaintext="aGFzaGljb3JwIGNlcnRpZmllZA=="

A. base64 <<< "hashicorp certified"
B. vault write transit/encrypt/vendor
C. vault secrets list
D. vault secrets enable transit
E. vault write -f transit/keys/vendor

Answer: ADE

NEW QUESTION 40
- (Topic 2)
What is the result of the following Vault command?
$ vault auth enable kubernetes

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

Answer: B

NEW QUESTION 41
- (Topic 2)
True or False? All Vault policies are deny by default.

A. True
B. False

Answer: A

NEW QUESTION 42
- (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 43
- (Topic 2)
True or False? Once the minimum decryption version is set on an encryption key, older versions of the key are removed from Vault and are no longer available for decryption operations.

A. True
B. False

Answer: B

NEW QUESTION 47
- (Topic 2)
You are using Azure Key Vault for the auto-unseal configuration on your cluster. After the Vault service restarts, what command must you run to unseal Vault?

A. You don??t need to run a command when using auto-unseal
B. vault operator members
C. vault operator unseal
D. vault operator init

Answer: A

NEW QUESTION 51
- (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 54
- (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 55
- (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 58
- (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 60

- (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 61
- (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 62
- (Topic 2)
You need to write a Vault operator policy and give the users access to perform administrative actions in Vault. What path is used for Vault backend functions?

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

Answer: E

NEW QUESTION 64
- (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 65
- (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 68
- (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 69
- (Topic 3)
Tom needs to set the proper environment variable so he doesn??t need to first authenticate to Vault toretrieve dynamically generated credentials for a database server. What environment variable does Tom need to set first before running commands?

A. VAULT_NAMESPACE

B. VAULT_TOKEN
C. VAULT_CAPATH
D. VAULT_CLIENT_KEY

Answer: B

NEW QUESTION 70
- (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 74
- (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 75
- (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 78
- (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 80
- (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 83

- (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 87
- (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 91
- (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 96
- (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 99
- (Topic 3)
Suzy is a Vault user that needs to create and replace values at the path secrets/automation/apps/chef. Does the following policy permit her the permissions to do so?
text CollapseWrapCopy
path "secrets/automation/apps/chef" { capabilities = ["create", "read", "list"]
}

A. No, the policy would deny Suzy from performing certain actions
B. Yes, the policy has appropriate permissions

Answer: A

NEW QUESTION 103
- (Topic 3)
What API endpoint is used to enable and configure a secrets engine?

A. /v1/sys/init
B. /v1/sys/mounts
C. /v1/sys/config
D. /v1/sys/plugins/catalog

Answer: B

NEW QUESTION 107
- (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 111
- (Topic 3)
You are enabling a secrets engine in Vault using the CLI. What subcommands are available when using the vault secrets command? (Select five)

A. update
B. migrate
C. tune
D. enable
E. move
F. disable
G. list

Answer: CDEFG

NEW QUESTION 115
- (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 118
- (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 119
- (Topic 4)
Frapps, Inc. is a coffee startup specializing in frozen caffeinated beverages. Their new customer loyalty web app uses Vault to store sensitive information, choosing Integrated Storage for its benefits. Select the benefits the organization would see by using Integrated Storage over other storage backends (Select four)

A. Eliminates network communication between hosts, requiring no open ports between hosts
B. Uses the SERF gossip protocol to enable communication between cluster nodes
C. Eliminates the requirement to deploy and manage a separate platform for storing encrypted data
D. Simplified troubleshooting since Integrated Storage is a built-in solution
E. Reduces operational overhead since all configuration is within Vault itself
F. Immediate access to storage since the data is stored locally on disk

Answer: CDEF

NEW QUESTION 124
- (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 129
- (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 131
- (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 132
- (Topic 4)
Your organization recently suffered a security breach on a specific application, and the security response team believes that MySQL database credentials were likely obtained during the event. The application generated the credentials using the database secrets engine in Vault mounted at the path database/. How can you quickly revoke all of the secrets generated by this secrets engine?

A. vault token revoke database/*
B. vault secrets disable mysql
C. vault lease renew database/creds/mysql
D. vault lease revoke -prefix database/

Answer: D

NEW QUESTION 135
- (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 140
- (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 141
- (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 144
- (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 146
- (Topic 4)
Your organization audited an essential application and found it isn??t securely storing data. For added security, auditors recommended encrypting all data before storing it in a backend database, and the application server should not store encryption keys locally. Which secrets engine meets these requirements?

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

Answer: C

NEW QUESTION 147
- (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 152
- (Topic 4)
All Vault instances, or clusters, include two built-in policies that are created automatically. Choose the two policies below and the correct information regarding each policy. (Select two)

A. The root policy is created automaticall
B. This policy provides superuser privileges and cannot be deleted
C. The admin policy is created automaticall
D. It provides administrative permissions but can be deleted if needed
E. The default policy is created automaticall
F. This policy can be modified but not deleted
G. The default policy is created automaticall
H. This policy cannot be modified but it can be deleted

Answer: AC

NEW QUESTION 156
- (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

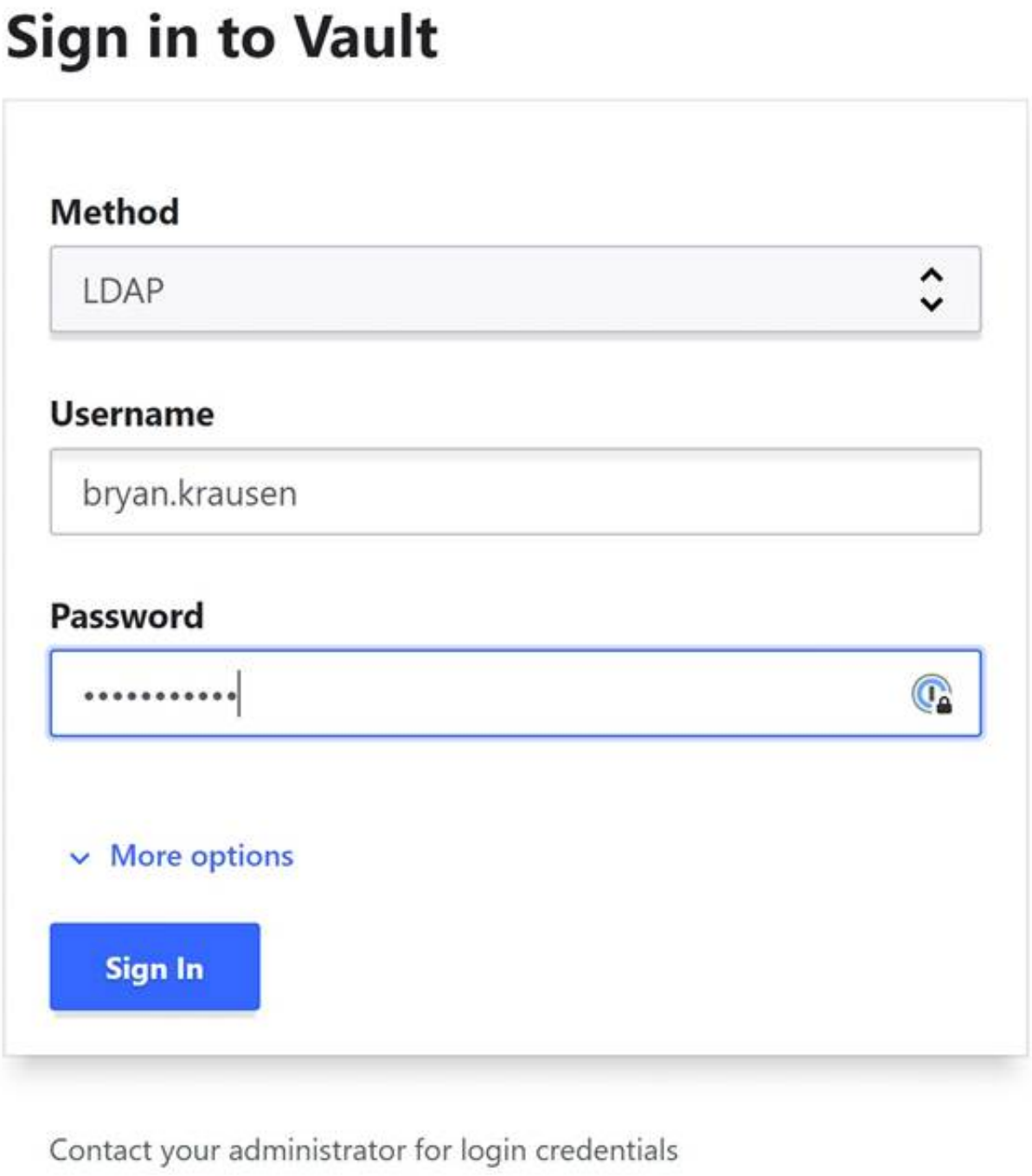
Answer: B

NEW QUESTION 159
- (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 161
- (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 163
- (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 166
- (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 171
- (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 172
- (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 175
- (Topic 5)
To give a role the ability to display or output all of the end points under the /secrets/apps/* end point it would need to have which capability set?

A. update
B. read
C. sudo
D. list
E. None of the above

Answer: C

NEW QUESTION 178
- (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 180
- (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.

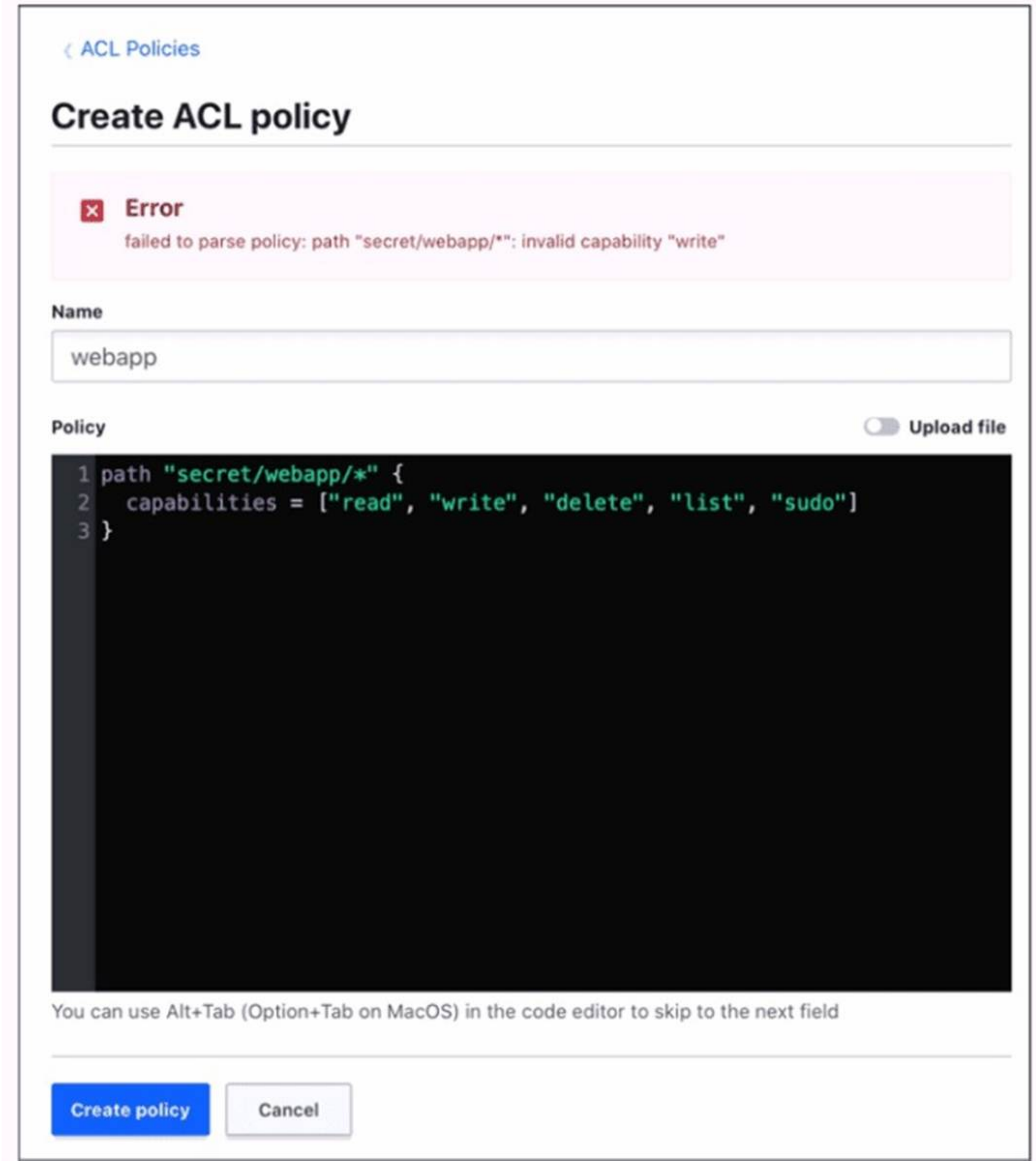
```
vault kv write userpass/sally \
password=h0wN0wB4r0wnC0w \
policies=power-users
```

D.

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

Answer: D

NEW QUESTION 185
- (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 186
- (Topic 5)
The Vault encryption key is stored in Vault's backend storage.

A. True
B. False

Answer: B

NEW QUESTION 187
- (Topic 5)
Which of the following is a machine-oriented Vault authentication backend?

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

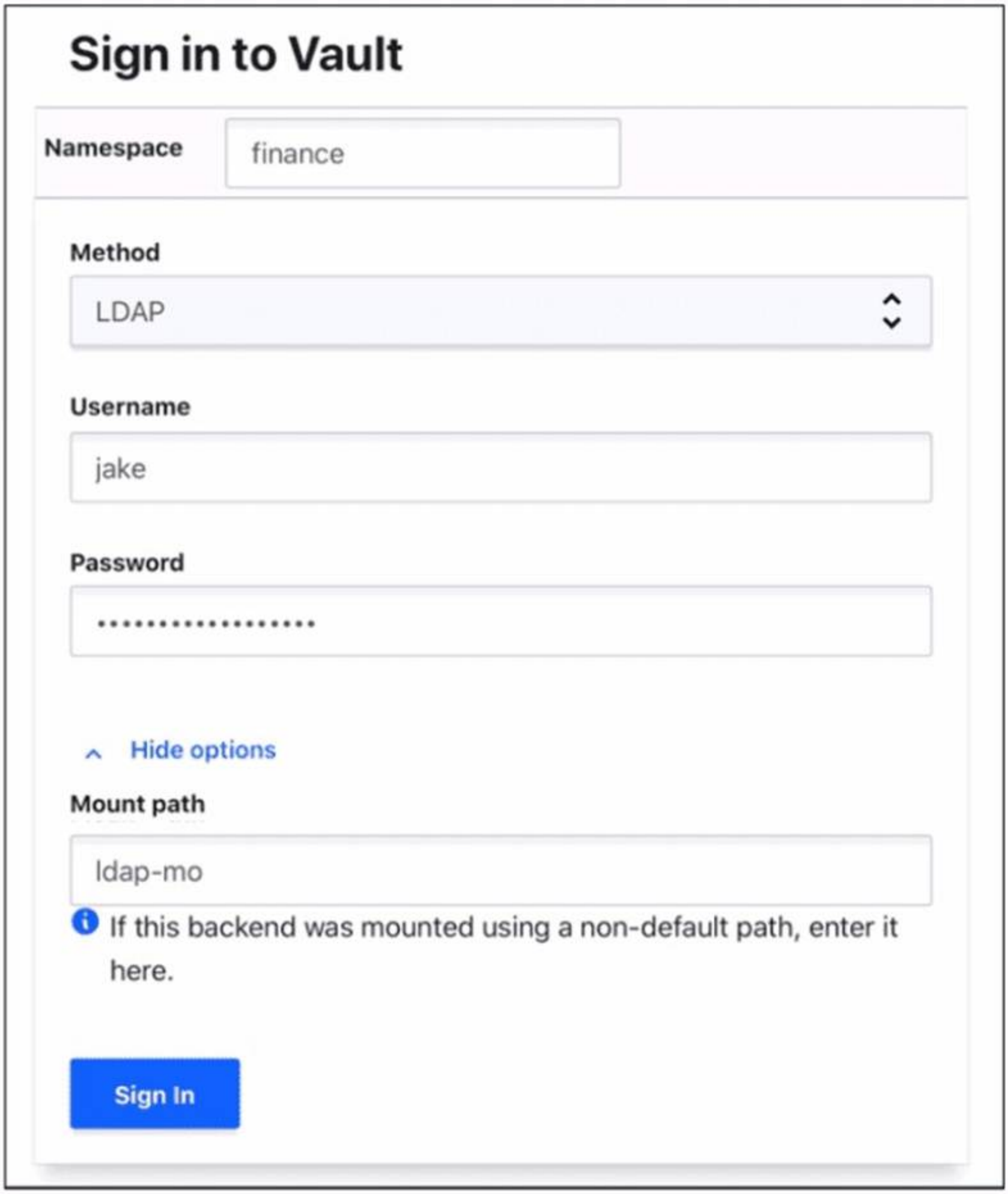
Answer: B

NEW QUESTION 192
- (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

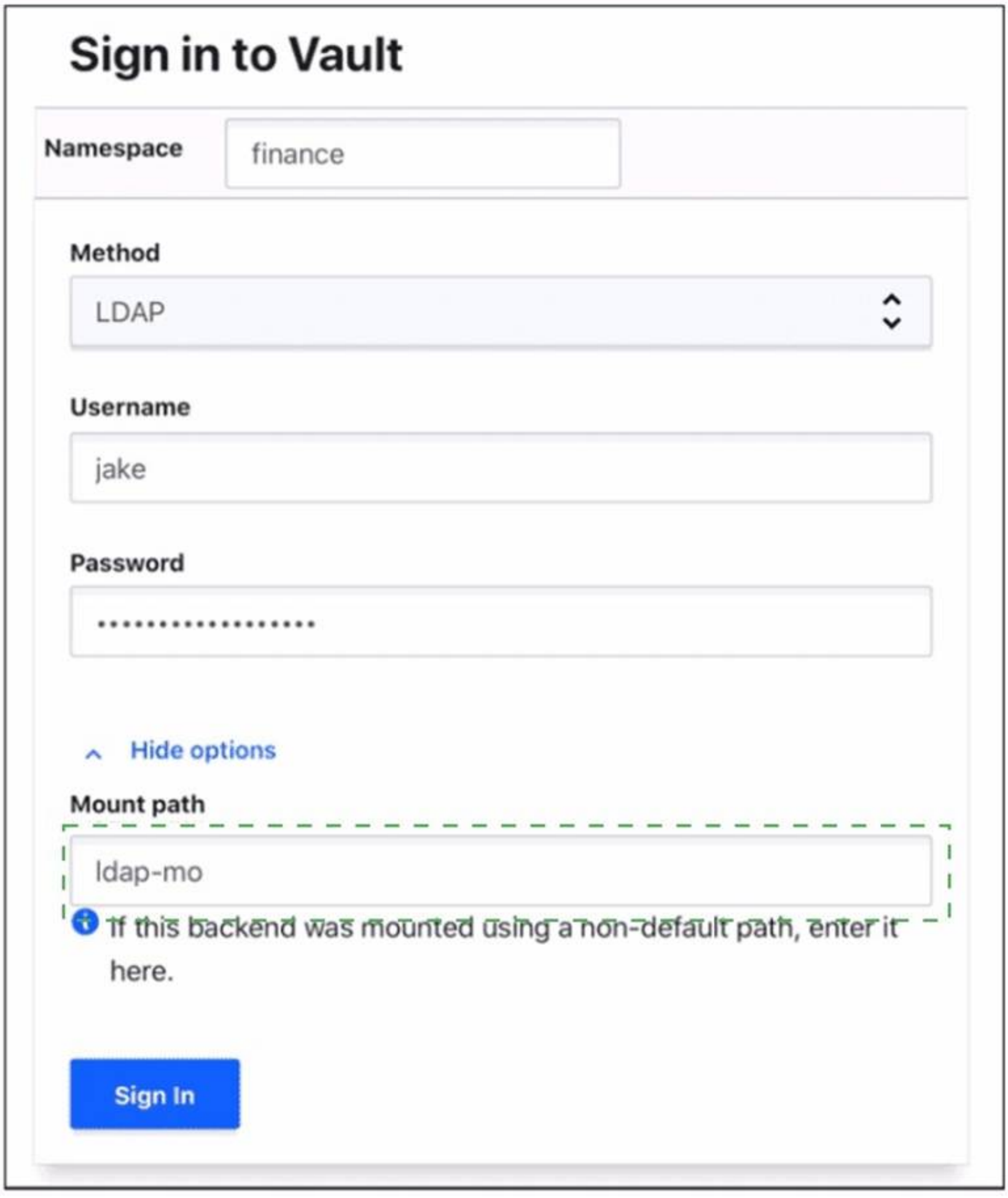
NEW QUESTION 193
HOTSPOT - (Topic 5)
Where do you define the Namespace to log into using the Vault Ul? To answer this question
Use your mouse to click on the screenshot in the location described above. An arrow indicator will mark where you have clicked. Click the "Answer" button once you have positioned 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 197
- (Topic 5)
You have been tasked with writing a policy that will allow read permissions for all secrets at path secret/bar. The users that are assigned this policy should also be able to list the secrets.What should this policy look like?

A.

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

B.

C.

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

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

D.

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

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

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

Answer: C

NEW QUESTION 198
- (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 200
- (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 202
- (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 204
- (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 209
- (Topic 5)
Which of the following cannot define the maximum time-to-live (TTL) for a token?

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

Answer: B

NEW QUESTION 213
- (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 217
- (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 218

.....

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