VA-002-P$^{Q\&As}$

HashiCorp Certified: Vault Associate

Pass HashiCorp VA-002-P Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/va-002-p.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HashiCorp
Official Exam Center

● **Instant Download** After Purchase

● **100% Money Back** Guarantee

● **365 Days** Free Update

● **800,000+** Satisfied Customers

QUESTION 1

True or False:

Multiple providers can be declared within a single Terraform configuration file.

A. False

B. True

Correct Answer: B

Multiple provider blocks can exist if a Terraform configuration is composed of multiple providers, which is a common situation. To add multiple providers in your configuration, declare the providers, and create resources associated with those providers.

QUESTION 2

Select the two default policies created in Vault. (select two)

A. default

B. vault

C. base

D. root

E. admin

F. user

Correct Answer: AD

Vault creates two default policies; root, and default.

The root policy cannot be deleted or modified.

The default policy is attached to all tokens, by default, however, this action can be modified if needed.

QUESTION 3

When configuring Vault replication and monitoring its status, you keep seeing something called \\'WALs\\'. What are WALs?

A. wake after lan

B. warning of allocated logs

C. write-ahead log

D. write along logging

Correct Answer: C

Reference links:https://learn.hashicorp.com/vault/day-one/monitor-replication https://www.vaultproject.io/docs/internals/replication

---

QUESTION 4

A "backend" in Terraform determines how the state is loaded and how an operation such as apply is executed. Which of the following is not a supported backend type?

A. terraform enterprise

B. s3

C. github

D. consul

E. artifactory

Correct Answer: C

github is not a supported backend type. https://www.terraform.io/docs/backends/types/index.html

---

QUESTION 5

A Vault client who has read access to the path secrets/apps/app1 is having trouble viewing the secret in the user interface (UI) but can access via the API. What can be done to resolve this issue?

A. add read permissions to the path secrets/apps

B. modify the policy to allow the create permission

C. remove the deny policy blocking access to the secrets/apps/app1 path

D. add LIST to the policy so the user can browse the paths leading up to the key/value\\'s path

Correct Answer: D

To view the paths leading up to the secrets/apps/app1 path in the user interface, the user must have at least LIST permissions to avoid permission denied error in the UI.