



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**

Which of the following settings are configured using the configuration file? (select three)

- A. Cluster Name
- B. Replication
- C. Seal Type
- D. Auth Methods
- E. Namespaces
- F. Storage Backend
- G. Audit Devices

Correct Answer: ACF

Seal types, Storage backends, and cluster names are just a few of the configurations done via the configuration file. The others are configured within Vault itself.

QUESTION 2

The following is a snippet from a Terraform configuration file:

1.

```
provider "aws" {
```
2.

```
  region = "us-east-1"
```
3.

```
}
```
4.

```
provider "aws" {
```
5.

```
  region = "us-west-1"
```
6.

```
}
```

which, when validated, results in the following error:



1.

Error: Duplicate provider configuration

2.

3.

on main.tf line 5:

4.

```
5: provider "aws" {
```

5.

6.

A default provider configuration for "aws" was already given at

7.

main.tf:1,1-15. If multiple configurations are required, set the "_____"

8.

argument for alternative configurations.

Fill in the blank in the error message with the correct string from the list below.

A. label

B. version

C. alias

D. multi

Correct Answer: C

An alias meta-argument is used when using the same provider with different configurations for different resources.

<https://www.terraform.io/docs/configuration/providers.html#alias-multiple-provider-instances>

QUESTION 3

The security barrier protects all of the following Vault components except ____.

A. secret engine

B. auth method

C. storage backend

D. audit devices



E. token store

Correct Answer: C

storage backend and HTTP API are outside of the security barrier hence can't be protected.

QUESTION 4

You've logged into the Vault CLI and attempted to enable an auth method, but received this error message. What can be done to resolve the error and configure Vault? Error enabling userpass auth: Post https://127.0.0.1:8200/v1/sys/auth/userpass: http: server gave HTTP response to HTTPS client

- A. change 'userpass' to 'username and password'
- B. restart the Vault service on this node
- C. set the VAULT_ADDR environment variable to HTTP
- D. ask an admin to grant you permission to enable the userpass auth method

Correct Answer: C

If you're running Vault in a non-prod environment, you can configure Vault to disable TLS. In this case, TLS has been disabled but the default value for VAULT_ADDR is https://127.0.0.1:8200, therefore Vault is sending the request over HTTPS but Vault is responding using HTTP since TLS is disabled.

To handle this error, set the VAULT_ADDR environment variable to "http://127.0.0.1:8200".

QUESTION 5

Which of the following allows Terraform users to apply policy as code to enforce standardized configurations for resources being deployed via infrastructure as code?

- A. functions
- B. workspaces
- C. module registry
- D. sentinel

Correct Answer: D

Sentinel is an embedded policy-as-code framework integrated with the HashiCorp Enterprise products. It enables fine-grained, logic-based policy decisions, and can be extended to use information from external sources.