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.pass2lead.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 type of Vault replication copies all data from Vault, including K/V data, policies, and client tokens?

A. DR replication

B. performance replication

C. failover replication

D. online replication

Correct Answer: A

Vault Enterprise supports multi-datacenter deployment where you can replicate data across data centers for performance as well as disaster recovery. In DR replication, secondary clusters do not forward service read or write requests until they are elevated and become a new primary. DR replicated cluster will replicate all data from the primary cluster, including tokens. A performance replicated cluster, however, will not replicate the tokens from the primary, as the performance replicated cluster will generate its own client tokens for requests made directly to it. In performance replication, secondaries keep track of their own tokens and leases but share the underlying configuration, policies, and supporting secrets (K/V values, encryption keys for transit, etc). Note: Failover and Online replication, there is no such replication exist in hashicorp vault. Check below links for more details:https://www.vaultproject.io/docs/enterprise/replication https://learn.hashicorp.com/vault/operations/opsdisaster-recovery

QUESTION 2

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/+/api_*" { capabilities = ["read"] }

B. path "secrets/applications/" { capabilities = ["read"] allowed_parameters = { "certificate" = [] } }

C. path "secrets/*" { capabilities = ["list"] }

D. path "secrets/applications/app01/api_key" { capabilities = ["update", "list"] }

Correct Answer: A

Wildcards and path segments can be used to allow access to a broader set of secrets rather than having to call out each individual secret itself. None of the other policies will allow a client to actually read the data stored at the path secrets/applications/app01/api_key

QUESTION 3

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 4

You are deploying Vault in a local data center, but want to be sure you have a secondary cluster in the event the primary cluster goes offline. In the secondary data center, you have applications that are running, as they are architected to run active/active. Which type of replication would be best in this scenario?

A. disaster recovery replication

B. single-node replication

C. performance replication

D. end-to-end replication

Correct Answer: C

In this scenario, the key to answering is that there are applications actively running the secondary data center. Because of this, you can deploy Performance Replication and the applications can now use the Vault cluster in their respective data center. This reduces network latency for your applications and provides you with a secondary cluster for redundancy.

QUESTION 5

An administrator wants to create a new KV mount for individual users to maintain their own secrets but needs a way to simplify the policy so they don\\'t need to write a new one for each new user? With the requirements listed below, what would such a policy look like? Requirement: Each user can perform all operations on their allocated key/value secret path

A. path "user-kv/data/{{identity.entity.name}}/*" { capabilities = ["create", "update", "read", "delete", "list"] }

B. path "user-kv/data/{{identity.entity.id.name}}/*" { capabilities = ["create", "update", "read", "delete", "list"] }

C. path "user-kv/data/{{identity.entity.aliases..id}}/*" { capabilities = ["create", "update", "read", "delete", "list"] }

D. path "user-kv/data/{{user}}/*" { capabilities = ["create", "update", "read", "delete", "list"] }

Correct Answer: A

Everything in the Vault is path-based, and policies are no exception. Policies provide a declarative way to grant or forbid access to certain paths and operations in Vault. The policy template makes it very flexible to customize the environment. By using parameters within your template, you can have Vault "insert" a value into the path based upon things like identity values, group membership, and metadata associated with either the user\\'s identity or group they are a member of. Using the parameter, the path user-kv/data/{{identity.entity.name}}/* converts to user- kv/data/student01/*

VA-002-P VCE Dumps VA-002-P Practice Test VA-002-P Exam Questions