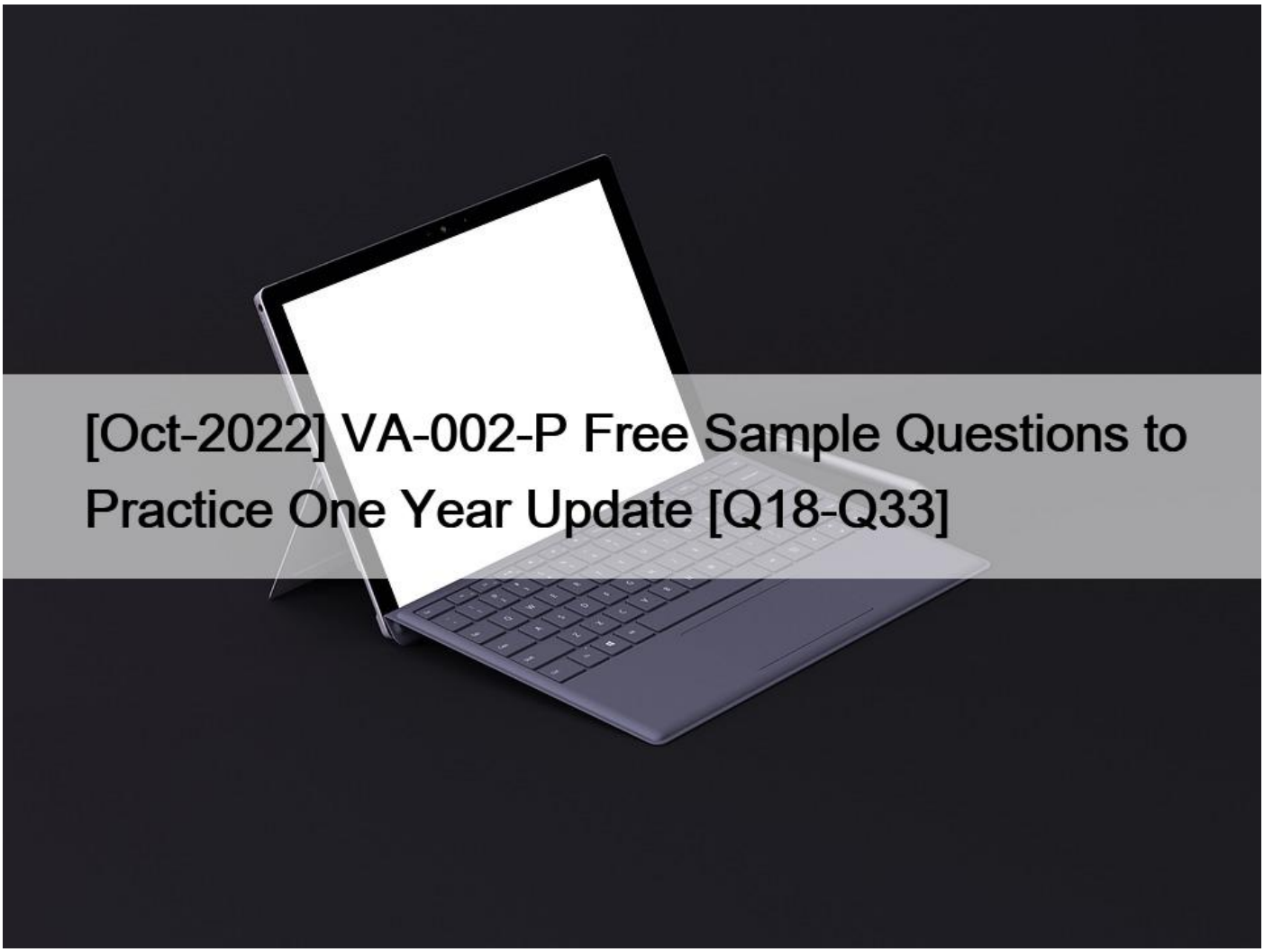
[Oct-2022 VA-002-P Free Sample Questions to Practice One Year Update [Q18-Q33



[Oct-2022] VA-002-P Free Sample Questions to Practice One Year Update
Download VA-002-P exam with HashiCorp VA-002-P Real Exam Questions

NEW QUESTION 18

Which flag would be used within a Terraform configuration block to identify the specific version of a provider required?
* required-provider
* required_versions
* required_providers
* required-version
For production use, you should constrain the acceptable provider versions via configuration file to ensure that new versions with breaking changes will not be automatically installed by terraform init in the future. When terraform init is run without provider version constraints, it prints a suggested version constraint string for each provider For example:

terraform {

required_providers {

aws = “>= 2.7.0”

}

}

NEW QUESTION 19

A user creates three workspaces from the command line – prod, dev, and test. Which of the following commands will the user run to switch to the dev workspace?
* terraform workspace select dev
* terraform workspace -switch dev
* terraform workspace dev
* terraform workspace switch dev
The terraform workspace select command is used to choose a different workspace to use for further operations.
https://www.terraform.io/docs/commands/workspace/select.html

NEW QUESTION 20

Which type of Vault replication copies all data from Vault, including K/V data, policies, and client tokens?
* DR replication
* performance replication
* failover replication
* online replication
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/ops-disaster-recovery

NEW QUESTION 21

True or False? When using the Terraform provider for Vault, the tight integration between these HashiCorp tools provides the ability to mask secrets in the terraform plan and state files.
* False
* True
Currently, Terraform has no mechanism to redact or protect secrets that are returned via data sources, so secrets read via this provider will be persisted into the Terraform state, into any plan files, and in some cases in the console output produced while planning and applying. These artifacts must, therefore, all be protected accordingly.

NEW QUESTION 22

When configuring a remote backend in Terraform, it might be a good idea to purposely omit some of the required arguments to ensure secrets and other relevant data are not inadvertently shared with others. What are the ways the remaining configuration can be added to Terraform so it can initialize and communicate with the backend? (select three)
* directly querying HashiCorp Vault for the secrets
* command-line key/value pairs
* use the -backend-config=PATH to specify a separate config file
* interactively on the command line
You do not need to specify every required argument in the backend configuration. Omitting certain arguments may be desirable to avoid storing secrets, such as access keys, within the main configuration. When some or all of the arguments are omitted, we call this a partial configuration.

With a partial configuration, the remaining configuration arguments must be provided as part of the initialization process. There are several ways to supply the remaining arguments:

Interactively: Terraform will interactively ask you for the required values unless interactive input is disabled. Terraform will not prompt for optional values.

File: A configuration file may be specified via the init command line. To specify a file, use the -backend-config=PATH option when running terraform init. If the file contains secrets it may be kept in a secure data store, such as Vault, in which case it must be downloaded to the local disk before running Terraform.

Command-line key/value pairs: Key/value pairs can be specified via the init command line. Note that many shells retain command-line flags in a history file, so this isn’t recommended for secrets. To specify a single key/value pair, use the -backend-config=”KEY=VALUE” option when running terraform init.

NEW QUESTION 23

Beyond encryption and decryption of data, which of the following is not a function of the Vault transit secrets engine?
* generate hashes and HMACs of data
* sign and verify data
* act as a source of random bytes
* store the encrypted data securely in Vault for retrieval
Vault doesn’t store the data sent to the secrets engine.

The transit secrets engine handles cryptographic functions on data-in-transit. It can also be viewed as “cryptography as a service” or “encryption as a service”. The transit secrets engine can also sign and verify data; generate hashes and HMACs of data; and act as a source of random bytes.

NEW QUESTION 24

When using providers that require the retrieval of data, such as the HashiCorp Vault provider, in what phase does Terraform actually retrieve the data required?
* terraform apply
* terraform plan
* terraform init
* terraform delete

It is important to consider that Terraform reads from data sources during the plan phase and writes the result into the plan. For something like a Vault token which has an explicit TTL, the apply must be run before the data, or token, in this case, expires, otherwise, Terraform will fail during the apply phase.

NEW QUESTION 25

From the answers below, select the advantages of using Infrastructure as Code. (select four)
* Easily integrate with application workflows (GitLab Actions, Azure DevOps, CI/CD tools)
* Safely test modifications using a “dry run” before applying any actual changes
* Provide reusable modules for easy sharing and collaboration
* Easily change and update existing infrastructure
* Provide a codified workflow to develop customer-facing applications

Infrastructure as Code is not used to develop applications, but it can be used to help deploy or provision those applications to a public cloud provider or on-premises infrastructure.

All of the others are benefits to using Infrastructure as Code over the traditional way of managing infrastructure, regardless if it’s public cloud or on-premises.

NEW QUESTION 26

When Terraform needs to be installed in a location where it does not have internet access to download the installer and upgrades, the installation is generally known as to be _____.
* a private install
* disconnected
* non-traditional
* air-gapped

A Terraform Enterprise install that is provisioned on a network that does not have Internet access is generally known as an air-gapped install. These types of installs require you to pull updates, providers, etc. from external sources vs. being able to download them directly.

NEW QUESTION 27

After a client has authenticated, what security feature is used to make subsequent calls?
* key shard
* ldap
* pgp
* token
* listener
* path

After authenticating, a client is issued a security token which is associated with a policy. That token is used to make a subsequent request to Vault, such as read, write, etc.

NEW QUESTION 28

Which Terraform command will check and report errors within modules, attribute names, and value types to make sure they are syntactically valid and internally consistent?
* terraform format
* terraform validate
* terraform fmt
* terraform show
The terraform validate command validates the configuration files in a directory, referring only to the configuration and not accessing any remote services such as remote state, provider APIs, etc.

Validate runs checks that verify whether a configuration is syntactically valid and internally consistent, regardless of any provided variables or existing state. It is thus primarily useful for general verification of reusable modules, including the correctness of attribute names and value types.

NEW QUESTION 29

What happens when a terraform apply command is executed?
* applies the changes required in the target infrastructure in order to reach the desired configuration
* creates the execution plan for the deployment of resources
* reconciles the state Terraform knows about with the real-world infrastructure
* the backend is initialized and the working directory is prepped
The terraform apply command is used to apply the changes required to reach the desired state of the configuration, or the pre-determined set of actions generated by a terraform plan execution plan.

NEW QUESTION 30

An application is trying to use a secret in which the lease has expired. What can be done in order for the application to successfully request data from Vault?
* request a new secret and associated lease
* try the expired secret in hopes it hasn’t been deleted yet
* request the TTL be extended for the secret
* perform a lease renewal
A lease must be renewed before it has expired. Once it has expired, it is permanently revoked and a new secret must be requested.

NEW QUESTION 31

The userpass auth method has the ability to access external services in order to provide authentication to Vault.
* FALSE
* TRUE
The userpass auth method uses a local database that cannot interact with any services outside of the Vault instance.

NEW QUESTION 32

Vault policies are deny by default
* TRUE
* FALSE
Everything in Vault is path-based including policies. Policies provide a declarative way to grant or forbid access to certain paths and operations in Vault.

Policies are deny by default, so an empty policy grants no permission in the system.

NEW QUESTION 33

After encrypting data using the transit secrets engine, you’ve received the following output. Which of the following is true based upon the output?

1. Key Value

2. — —–

3. ciphertext vault:v2:45f9zW6cglbrzCjI0yCyC6DBYtSBSxnMgUn9B5aHcGEit71xefPEmmjMbrk3
* the original encryption key has been rotated at least once
* this is the second version of the encrypted data
* similar to the KV secrets engine, the transit secrets engine was enabled using the transit v2 option
* the data is stored in Vault using a KV v2 secrets engine

When data is encrypted using Vault, the resulting ciphertext is prepended by the version of the key used to encrypt it. In this case, the version is v2, which means that the encryption key was rotated at least one time. Any data that was encrypted with the original key would have been prepended with vault:v1 To rotate a key, use the command vault write -f transit/keys/<key name>/rotate
Reference link:- https://learn.hashicorp.com/vault/encryption-as-a-service/eaas-transit

HashiCorp VA-002-P Exam Syllabus Topics:

TopicDetailsTopic 1- Describe Shamir secret sharing and unsealing- Craft a Vault policy based on requirements- Describe Vault policy syntax: capabilitiesTopic 2- Configure transit secret engine- Compare authentication methods- Illustrate the value of Vault policyTopic 3- Describe secrets caching- Configure Vault policies- Explain orphaned tokens- Configure Vault policiesTopic 4- Access Vault secrets via Curl- Manage Vault leases- Define token accessors- Create Vault policiesTopic 5 - Differentiate between service and batch tokens. Choose one based on use-case- Describe authentication methodsTopic 6- Explain encryption as a service- Explain response wrapping- Explain Vault architecture- Authenticate to VaultTopic 7- Explain the value of short-lived, dynamically generated secrets- Choose an authentication method based on use case