Free Questions for Vault-Associate by vceexamstest

Shared by Douglas on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Vault supports which type of configuration for source limited token?

Options:

A- Cloud-bound tokens

B- Domain-bound tokens

C- CIDR-bound tokens

D- Certificate-bound tokens

Answer:

C

Explanation:

Vault supports CIDR-bound tokens, which are tokens that can only be used from a specific set of IP addresses or network ranges. This is a way to limit the scope and exposure of a token in case it is compromised or leaked. CIDR-bound tokens can be created by specifying the bound_cidr_list parameter when creating or updating a token role, or by using the -bound-cidr option when creating a token using the vault token create command. CIDR-bound tokens can also be created by some auth methods, such as AWS or Kubernetes, that can automatically bind the tokens to the source IP or network of the client.Reference:Token - Auth Methods | Vault | HashiCorp Developer,vault token create - Command | Vault | HashiCorp Developer

Question 2

Question Type: MultipleChoice

Which of the following describes usage of an identity group?

Options:

A- Limit the policies that would otherwise apply to an entity in the group

B- When they want to revoke the credentials for a whole set of entities simultaneously

C- Audit token usage

D- Consistently apply the same set of policies to a collection of entities

Answer:

D

Explanation:

An identity group is a collection of entities that share some common attributes. An identity group can have one or more policies attached to it, which are inherited by all the members of the group. An identity group can also have subgroups, which can further refine the policies and attributes for a subset of entities.

One of the use cases of an identity group is to consistently apply the same set of policies to a collection of entities. For example, an organization may have different teams or departments, such as engineering, sales, or marketing. Each team may have its own identity group, with policies that grant access to the secrets and resources that are relevant to their work. By creating an identity group for each team, the organization can ensure that the entities belonging to each team have the same level of access and permissions, regardless of which authentication method they use to log in to Vault.Reference:Identity: entities and groups | Vault | HashiCorp Developer,vault_identity_group | Resources | hashicorp/vault | Terraform | Terraform Registry

Question 3

Question Type: MultipleChoice

Which of these are a benefit of using the Vault Agent?

Options:

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

Explanation:

Vault Agent is a client daemon that provides the following features:

Auto-Auth - Automatically authenticate to Vault and manage the token renewal process for locally-retrieved dynamic secrets.

API Proxy - Allows Vault Agent to act as a proxy for Vault's API, optionally using (or forcing the use of) the Auto-Auth token.

Caching - Allows client-side caching of responses containing newly created tokens and responses containing leased secrets generated off of these newly created tokens. The agent also manages the renewals of the cached tokens and leases.

Templating - Allows rendering of user-supplied templates by Vault Agent, using the token generated by the Auto-Auth step.

Process Supervisor Mode - Runs a child process with Vault secrets injected as environment variables.

One of the benefits of using the Vault Agent is that it will manage the lifecycle of cached tokens and leases automatically. This means that the agent will handle the token renewal and revocation logic, as well as the lease renewal and revocation logic for the secrets that are cached by the agent. This reduces the burden on the application developers and operators, and ensures that the tokens and secrets are always valid and up-to-date.Reference:Vault Agent | Vault | HashiCorp Developer,Caching - Vault Agent | Vault | HashiCorp Developer

Question 4

Question Type: **MultipleChoice**

How many Shamir's key shares are required to unseal a Vault instance?

Options:

A- All key shares

B- A quorum of key shares

C- One or more keys

D- The threshold number of key shares

Answer:

D

Explanation:

Shamir's Secret Sharing is a cryptographic algorithm that allows a secret to be split into multiple parts, called key shares, such that a certain number of key shares are required to reconstruct the secret. The number of key shares and the threshold number are configurable parameters that depend on the desired level of security and availability. Vault uses Shamir's Secret Sharing to protect its master key, which is used to encrypt and decrypt the data encryption key that secures the Vault data. When Vault is initialized, it generates a master key and splits it into a configured number of key shares, which are then distributed to trusted operators. To unseal Vault, the threshold number of key shares must be provided to reconstruct the master key and decrypt the data encryption key.This process ensures that no single operator can access the Vault data without the cooperation of other key holders.Reference: https://developer.hashicorp.com/vault/docs/concepts/seal4, https://developer.hashicorp.com/vault/docs/commands/operator/init5, https://developer.hashicorp.com/vault/docs/commands/operator/unseal6

Question 5

Question Type: MultipleChoice

When using Integrated Storage, which of the following should you do to recover from possible data loss?

Options:

A- Failover to a standby node

B- Use snapshot

C- Use audit logs

D- Use server logs

Answer:

B

Explanation:

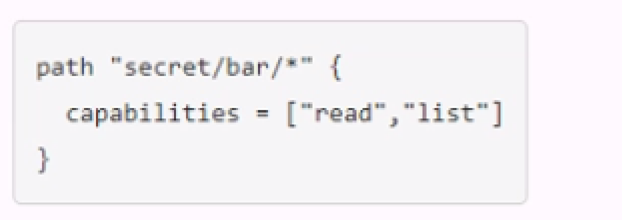
Integrated Storage is a Raft-based storage backend that allows Vault to store its data internally without relying on an external storage system. It also enables Vault to run in high availability mode with automatic leader election and failover. However, Integrated Storage is not immune to data loss or corruption due to hardware failures, network partitions, or human errors. Therefore, it is recommended to use the snapshot feature to backup and restore the Vault data periodically or on demand. A snapshot is a point-in-time capture of the entire Vault data, including the encrypted secrets, the configuration, and the metadata. Snapshots can be taken and restored using the vault operator raft snapshot command or the sys/storage/raft/snapshot API endpoint. Snapshots are encrypted and can only be restored with a quorum of unseal keys or recovery keys.Snapshots are also portable and can be used to migrate data between different Vault clusters or storage backends.Reference: https://developer.hashicorp.com/vault/docs/concepts/integrated-storage1, https://developer.hashicorp.com/vault/docs/commands/operator/raft/snapshot2, https://developer.hashicorp.com/vault/api-docs/system/storage/raft/snapshot3

Question 6

Question Type: MultipleChoice

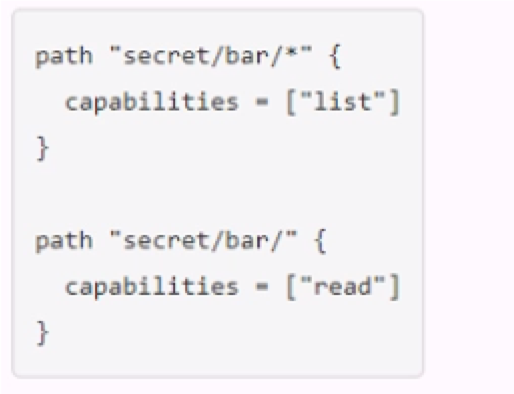
You have been tasked with writing a policy that will allow read permissions for all secrets at path secret/bar. The users that are assigned this policy should also be able to list the secrets. What should this policy look like?

A.



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

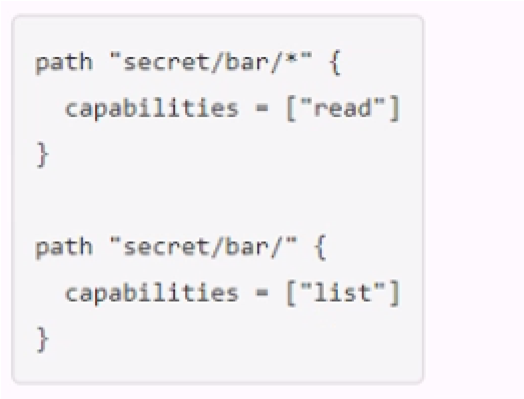
B.



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

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

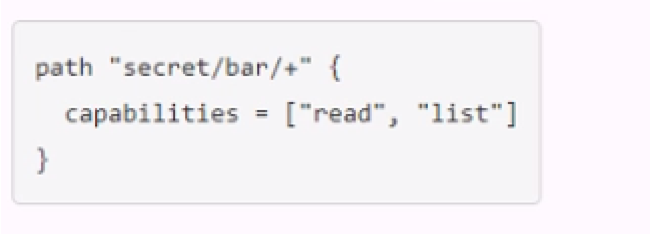
C.



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

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

D.



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

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

C

Explanation:

This policy would allow read permissions for all secrets at path secret/bar, as well as list permissions for the secret/bar/ path.The list permission is required to be able to see the names of the secrets under a given path1. The wildcard () character matches any number of characters within a single path segment, while the slash (/) character matches the end of the path2. Therefore, the policy would grant read access to any secret that starts with secret/bar/, such as secret/bar/foo or secret/bar/baz, but not to secret/bar itself. To grant list access to secret/bar, the policy needs to specify the exact path with a slash at the end.This policy follows the principle of least privilege, which means that it only grants the minimum permissions necessary for the users to perform their tasks3.

The other options are not correct because they either grant too much or too little permissions. Option A would grant both read and list permissions to all secrets under secret/bar, which is more than what is required. Option B would grant list permissions to all secrets under secret/bar, but only read permissions to secret/bar itself, which is not what is required. Option D would use an invalid character (+) in the policy, which would cause an error.

Policy Syntax | Vault | HashiCorp Developer

Policy Syntax | Vault | HashiCorp Developer

Policies | Vault | HashiCorp Developer