CertKillers

Guaranteed Success with Accurate & Updated Questions.

# HashiCorp

*Vault-Operations-Professional*
*HashiCorp Certified Vault Operations Professional*

## Questions & Answers PDF

For More Information - Visit:
https://www.certkillers.net/

# Latest Version: 7.0

## Question: 1

Your team has recently upgraded from open source Vault to Vault Enterprise so you can use performance standby nodes. Which of the following is true regarding performance standby nodes?
Response:

A. Performance standby nodes will attempt to locally process client read requests and automatically forward write requests to the leader/active node.
B. Performance standby nodes are only available when using the Consul storage backend.
C. Performance standby nodes scale the overall performance of the Vault cluster by handling both read and write requests locally.
D. Performance standby nodes can only be used when Performance replication is also enabled.

**Answer: A**

## Question: 2

What are the use cases of performance standby nodes in Vault Enterprise?
Response:

A. To improve the performance and availability of Vault in case of failures or outages
B. To manage encryption keys and certificates for Vault
C. To monitor and analyze access logs and telemetry data
D. To improve Vault performance and scalability for large-scale deployments

**Answer: A**

## Question: 3

The Vault Agent allows for the use of "auto-auth", which allows the agent to authenticate, retrieve a Vault token, and manage the token lifecycle with the configured method. Which of the following auto-auth methods is ***NOT*** a valid option for the Vault Agent to use during authentication to Vault?
Response:

A. AWS
B. Kubernetes
C. LDAP
D. Azure
E. AppRole

**Answer: C**

## Question: 4

Many organizations seek to reduce the operational complexity of running Vault by using auto-unseal to automatically unseal the Vault cluster without needing to supply unseal keys.
Your leadership team wants to use an HSM in the current Vault environment and believes that Vault supports the use of an HSM for auto-unseal. Is this true or false?
Response:

A. True
B. False

**Answer: A**

## Question: 5

Based on the above configuration the Vault Agent will attempt to connect to the Vault cluster at which address?

```
listener "tcp" {
  address = "127.0.0.1:8200"
}
vault {
  address = "https://vault-demo.com:8200"
}
### Depending on how difficult we want to make the question this can be removed. Default
value/behavior is false.
exit_after_auth = false
auto_auth {
  method "approle" {
    config = {
      role_id_file_path = "./roleid"
      secret_id_file_path = "./secretid"
      remove_secret_id_file_after_reading  = false
    }
  }
}
sink {
  type = "file"
  config = {
    path = "/opt/sink_file_1.txt"
    mode = "0640"
  }
}
template {
  source = "./test.tmpl"
  destination = "./test.txt"
}
```

Response:

A. https://127.0.0.1:8200

B. It is using a Unix socket listener on localhost

C. The configuration file does not contain that information and needs to be configured in the unit file or startup command

D. https://vault-demo.com:8200

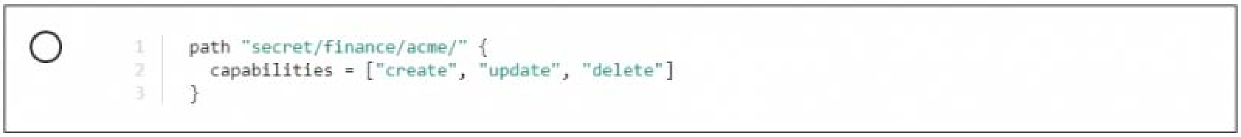
**Answer: D**

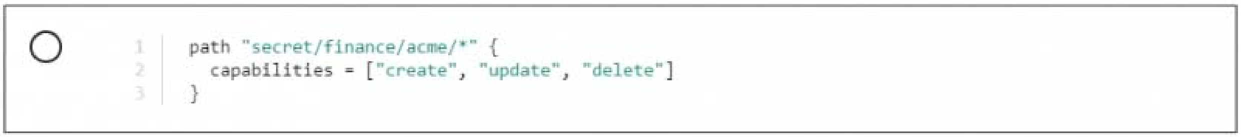
## Question: 6

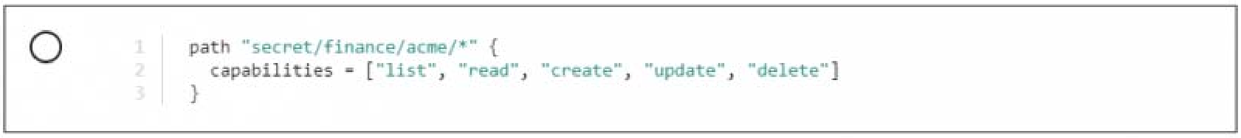
You are currently working on constructing Vault policies to allow other teams to manage secrets for their specific applications. The acme-secret-manager policy should grant sufficient permissions to create new secrets, revise existing secrets, and delete secrets under the secret/finance/acme/ path, as well as ALL child paths.

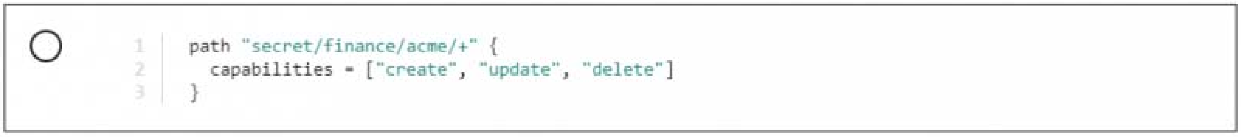
Which Vault policy stanza below would grant the required permissions while ALSO following the concept of "least privilege"?

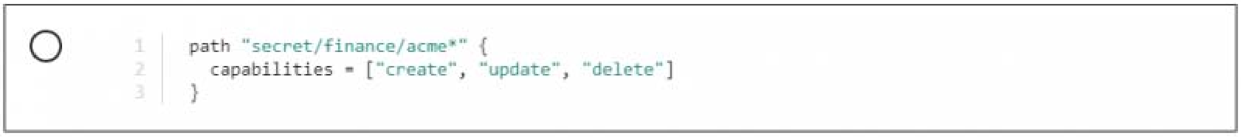
(select one)


○
```
path "secret/finance/acme/" {
  capabilities = ["create", "update", "delete"]
}
```


○
```
path "secret/finance/acme/*" {
  capabilities = ["create", "update", "delete"]
}
```


○
```
path "secret/finance/acme/*" {
  capabilities = ["list", "read", "create", "update", "delete"]
}
```


○
```
path "secret/finance/acme/+" {
  capabilities = ["create", "update", "delete"]
}
```


○
```
path "secret/finance/acme*" {
  capabilities = ["create", "update", "delete"]
}
```

Response:

A. Option A
B. Option B
C. Option C
D. Option D
E. Option E

**Answer: B**

## Question: 7

As part of a new compliance standard, you have recently turned on one audit device using the file audit method. After a few days, you start getting messages from your team that they cannot interact with Vault and it appears that the service is down to all Vault clients.
After some initial investigation, you discover that the Vault service is running, but you get errors when you run any Vault command. What is the most likely cause?
Response:

A. The new audit device detected malicious activity and automatically sealed your Vault environment
B. After enabling the audit device, the servers hosting Vault could not handle the additional resource-intensive load and are unresponsive
C. Drive space on the server has filled up and the file audit method cannot write to the log file, causing to Vault stop handling requests
D. It is likely just some sort of network issue that will resolve itself

**Answer: C**

## Question: 8

What is the purpose of identity entities and groups in Vault access control?
Response:

A. To define the roles and permissions of users and applications
B. To manage authentication methods and credentials
C. To monitor and audit access to Vault resources
D. To encrypt and decrypt data in transit and at rest

**Answer: A**

## Question: 9

Your team has been running Vault for a few months and has created demos for onboarding a few application teams. You have now been tasked with making sure that Vault is ready for full production deployment.
Given the below configuration information, what would be the easiest change to ensure Vault is highly available and ready for production?
- Running in a five (5) node cluster
- Using Integrated Storage (Raft) as the storage backend
- Using Shamir as the seal type
- Virtual machines hosting the Vault service are running in an on-prem datacenter
Response:

A. Switch to using Consul as a storage backend
B. Increase the number of Vault nodes in the cluster from 5 to 7
C. Migrate the Vault deployment to a public cloud with a shared responsibility model
D. Switch the seal mechanism from Shamir to one supporting auto-unseal

**Answer: D**

## Question: 10

Vance Refrigeration has an Enterprise Architect that had previously deployed Vault a few years ago using Consul as the storage backend. She is not familiar with Integrated Storage (Raft) and wants to know why they should use it.
Which of the following is NOT a benefit of deploying Vault with Raft as the storage backend, compared to Consul?
Response:

A. Using Raft reduces the number of network ports used for communication
B. Raft can reduce operational costs by lowering the total number of nodes/VMs required for an HA cluster
C. Raft stores all data in memory
D. Raft stores data locally and reduces extra network hops when data needs to be retrieved from the storage backend.

**Answer: C**