## Section 2, Quiz 1 - Create a Working Vault Server Config

**Question 1: Vault supports both “rekey” and “rotate” operations in Vault. While the commands sound similar, it is important to understand the key differences between these unique operations.**

**What statement most accurately describes the difference between “rekey” and “rotate” operations?**

- Rekey is used to generate new unseal/recovery keys, and rotate is used to generate a new root key.
- Rekey is used to generate a new root key and unseal/recovery keys, and rotate is used to change the encryption key used to encrypt data written to the storage backend.
- Rekey is used to generate a new root key, and rotate is used to generate new unseal/recovery keys.
- Rekey is used to change the encryption key used to encrypt data written to the storage backend, and rotate is used to generate a new root key and unseal/recovery keys.

Answer: B. Yes, you got it! Rekeying is the process of generating a new root key and the unseal/recovery key shares used to reconstruct the root key. Rotating is used to change the underlying key used to encrypt/decrypt Vault data. New keys are added to the keyring and old values can still be decrypted with the old key.

**Question 2: Due to an internal compliance audit at your client, Binford Tools, they have contacted you about performing a rotate and rekey in their Vault environment. They are unsure if and when they will need their current unseal keys during these processes.**

**Select the statement that is true regarding the rotate and rekey process.**

- Both the rekey and rotate processes will require a threshold of key holders.
- Neither process requires a threshold of key holders if you are logged in as a root token.
- The rekey operation requires a threshold of key holders. The rotate operation does NOT require a threshold of key holders.
- The rekey operations require sudo privileges on the root-protected path. However, the rotate operation requires a threshold of key holders.

Answer: C. Yes, this is the correct answer.

**Question 3: Your management team has approached you regarding the Vault environment at your organization. They recently heard something about an “auto unseal” feature, and what options are available to enable it.**

**Which of the following options is NOT a supported method for auto unseal?**

- Shamir

- Cloud Key Management services like AWS KMS or Azure Key Vault
- Vault's Transit Secret Engine
- Hardware Security Module (HSM)

Answer: A. Correct. Shamir is the default seal mechanism for Vault but does not support auto unseal. When using Shamir a threshold of key shares must be supplied to unseal Vault. All other options support auto unseal.

**Question 4: You are currently working with Vance Refrigeration on deploying a highly scalable Vault environment with Integrated Storage (Raft) as the storage backend. Performance is a key factor for the team, as they want to ensure that Vault is available when clients need to request secrets from Vault.**

**When deploying a Vault cluster with Raft, which hardware resource is TYPICALLY the key bottleneck for performance?**

- CPU
- Network Throughput
- Disk IOPS
- Memory

Answer: C. Yes, that's correct. As Integrated Storage stores all data on a local disk, Vault servers should have a relatively high-performance hard disk optimized for high IOPS.

**Question 5: 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?**

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

Answer: C. Correct choice. Raft stores data on local disk, NOT in-memory (Consul does). All other options are valid benefits for using Raft as the storage backend.

**Question 6: Your organization is currently using Vault's KV store to consolidate secrets and sensitive data accessed by applications and users across the organization. Right now, the KV**

**version 1 secrets engine is being used, but multiple Vault consumers are requesting you to add versioning capabilities to the KV secrets engine.**

**How can you add versioning to the KV store while minimizing the impacts to existing clients?**

- Enable a new KV version 2 secrets engine on a new path. Use the **vault move** command to migrate all of the data from the old path to the new path.
- Upgrade the KV store to KV version 2 using the command **kv enable-versioning/path**.
- KV does not support versioning and is not a capability that can be added.
- Enable a KV version 2 secrets engine at the same path as the existing KV version 1 store. This will allow clients to start taking advantage of versioning capabilities.

Answer: B. Yes, this is correct. Nice job. Keep in mind that this might require clients to add the /data prefix that we discussed during the lecture.

## Section 3, Quiz 2 - Monitor a Vault Environment

**Question 1: You have been tasked with increasing the visibility the organization has about the Vault environment. As part of this task, you need to configure Vault telemetry settings. Where would you find telemetry settings to forward telemetry data to a collector agent?**

- In the Vault UI under the “Status” menu
- sys/telemetry
- The Vault configuration file
- sys/tools/telemetry

Answer: C. Yes! Telemetry is configured in the Vault configuration file using the telemetry stanza.

**Question 2: Your security and compliance team has approached you with questions regarding logs that are currently being collected from Vault. They are interested in understanding what sort of information the different Vault logs contain. Which statement best describes the difference between audit and telemetry logs?**

- Audit logs are a detailed log of all authenticated requests and responses to Vault, and telemetry simply tracks Raft leadership elections and changes.
- Audit logs are a collection of various runtime metrics about the performance of different components of the Vault environment, and telemetry logs are a detailed log of all authenticated requests and responses to Vault.
- Audit logs only contain information about initial client authentication requests; all other authenticated requests and responses are in telemetry logs.
- Audit logs are a detailed log of all authenticated requests and responses to Vault, and telemetry logs are a collection of various runtime metrics about the performance of different components of the Vault environment.

Answer: D. Audit logs contain detailed information about ALL authenticated requests and responses to Vault, essentially the who, what, when, and where. Telemetry logs contain various runtime metrics like how much memory the Vault process is using, as well as endpoint usage and performance.

**Question 3: Your security and compliance team has concerns regarding Vault audit logs and the potential of storing sensitive information in plaintext. In what case will Vault audit logs store sensitive information such as secrets and tokens in plaintext?**

- Sensitive information is hashed and never stored in plaintext
- Only when using the “File” audit method
- Only when using the “Syslog” audit method
- Only when using the “Socket” audit method

Answer: A. Yes! Sensitive information is hashed with a salt using HMAC-SHA256 to ensure secrets and tokens are never in plaintext.

**NOTE**: There is a parameter available for audit logs that does allow Vault to send sensitive data to the audit device, but this is disabled by default.

**Question 4: 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 likeliest cause?**

- The new audit device detected malicious activity and automatically sealed your Vault environment.
- After enabling the audit device, the servers hosting Vault could not handle the additional resource-intensive load are unresponsive.
- 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.
- It is likely just some sort of network issue that will resolve itself.

Answer: C. The key piece here is that you just turned on a single audit device a few days ago. If there are any audit devices enabled, Vault requires that it can write to the log before completing any client requests.

## Section 4, Quiz 3 - Employ the Vault Security Model

**Question 1: You have been hired by the Real Good Foods Company to assist with improving their current usage of Vault. A number of applications are already integrated with Vault, but they want to ensure that the interactions and workflows they use are secure.**

**Which of the following choices is NOT a good goal for secure introduction of Vault clients?**

- Using short TTLs on Tokens and leases wherever possible
- Using hardcoded credentials in code to ensure uptime
- Using a trusted platform to verify the identity of applications/clients
- Using a trusted orchestrator to inject secrets into applications

Answer: B. Yes. You should try to avoid the use of hardcoded credentials whenever possible. All other choices are great goals for the secure introduction of Vault clients.

**Question 2: The Real Good Foods Company has also approached you regarding the patterns of authentication applications use to integrate with Vault. Currently, a vast majority of their applications run in either AWS or GCP. They are considering the use of the platform integration model, but have heard that cloud-based auth providers such as AWS, GCP, and Azure are not recommended and that AppRole auth is more secure.**

**True or False? AppRole auth is recommended for use over third-party/cloud auth methods.**

- True
- False

Answer: B. Yes, you got it! If another platform method of authentication is available through a trusted third-party authenticator, it is best practice to use that instead of AppRole. In some situations, it may not be possible to use a trusted third-party auth provider, and AppRole exists for these cases.

**Question 3: You are currently working to onboard applications to leverage Vault for secure secret storage. You have been instructed to use a "trusted orchestrator" to handle the way these applications get their secrets.**

**Which of the following is an example of the "trusted orchestrator" model for secure introduction of Vault clients?**

- The Vault Agent using auto-auth
- Using a cloud provider such as AWS to gather metadata for an EC2 instance to verify application identities during authentication
- Terraform using an existing token with capabilities to generate AppRole credentials, and injecting the secrets into an application build

- The GitHub authentication method

Answer: C. Yes! The Terraform example best represents the use of a “trusted orchestrator”. Option A, the Vault agent, is another method of securely introducing Vault clients, and option B describes the “platform integration” model. The last option is just the GitHub auth method and does not describe the trusted orchestrator model.

**Question 4: Many organizations are moving to host applications in Kubernetes clusters. When it comes to Vault, it is important to understand additional considerations when hosting services in a container-based environment.**

**Which of the following items is NOT a recommended step to mitigate potential security vulnerabilities when running Vault on Kubernetes?**

- Ensure **mlock** is enabled
- Ensure end-to-end encryption using TLS certificates
- Ensure the Vault process is not running as the root user
- Offload TLS by ensuring that traffic is terminated at load balancers

Answer: D. Correct. It is always recommended to NOT terminate TLS at load balancers to ensure that the Vault traffic is always encrypted in transit.

## Section 5, Quiz 4 - Build Fault-Tolerant Vault Environments

**Question 1: Your operations team has been experiencing outages lately on numerous applications. Your manager has approached you regarding the Vault environment to ensure it is highly available and fault-tolerant. Currently, the primary Vault cluster is using Integrated Storage (Raft) in a three-node cluster.**

**In the current configuration, how many Vault nodes could you lose and still have an available Vault service?**

- 1
- 2
- 3
- In a three-node cluster, you cannot lose ANY nodes

Answer: A. Yes, you got it! In order to maintain a quorum and have Vault service requests you can lose one node and the remaining two nodes will handle requests. A quorum is a majority of members from a peer set: for a set of size n, quorum requires at least (n+1)/2 members. So a three-node cluster requires two nodes *(3+1)/2 = 2*.

**Question 2: 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 following configuration information, what would be the easiest change to ensure that Vault is highly available and ready for production?**

```
1. - Running in a five (5) node cluster
2. - Using Integrated Storage (Raft) as the storage backend
3. - Using Shamir as the seal type
4. - Virtual machines hosting the Vault service are running in an on-prem datacenter
```

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

Answer: B. Raft as a storage backend has become the standard approach and will be more than adequate for nearly any production deployment, so Consul is not necessary. A five-node Vault cluster should meet the needs for the vast majority of deployments, and adding additional nodes would be a very rare circumstance. There is no real benefit between using private versus public cloud. Moving from Shamir to an auto-unseal is the clear answer, as it is a relatively simple change and would ensure that Vault is unsealed automatically following any service restarts.

**Question 3: Your team has recently upgraded to Vault Enterprise, in part to take advantage of Disaster Recovery (DR) replication. During a discovery meeting, one of the on-call managers asked**

**a question regarding DR clusters and if applications would need to re-authenticate in the event of promoting the DR to act as a primary.**

**True or False? DR clusters mirror the tokens and leases for applications and users interacting with the primary cluster.**

- True: DR clusters mirror tokens and leases, so applications would NOT need to re-authenticate
- False: DR clusters keep track of their own tokens and leases, and applications WOULD need to re-authenticate

Answer: A. DR clusters act as a warm standby and duplicate all the data of the primary, including tokens and leases.

**Question 4: You have been approached by a member of your team that wants to implement an "active-active" architecture of your Vault clusters to maintain high availability. Vault currently supports active-active implementations where multiple clusters can act as the primary.**

**Is this True or False?**

- True
- False

Answer: B. The replication model is not designed for active-active and enabling two primaries should never be done. It is known as a "split-brain" scenario and could result in data loss.

## Section 6, Quiz 5 - Understand the Hardware Security Module (HSM) Integration

**Question 1: Due to a new compliance initiative, the ACME company would like to increase security and compliance for their Vault environment. They have sought out your guidance regarding the use of a Hardware Security Module (HSM). They want clarification regarding the availability of their HSM once it is integrated with their Vault cluster as the seal mechanism. ACME currently believes that there is no need for the HSM to be online and available to Vault once the Vault cluster has been unsealed.**

**True or False? Is this a valid statement?**

- True
- False

Answer: B. You got it! The HSM is used for the auto-unseal process, but is also used for other potential operations during normal activity, such as generating various CSPs or for entropy augmentation, any write operations on mount points with seal wrapping enabled, and Vault token generations with entropy augmentation enabled.

**Question 2: 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?**

- True
- False

Answer: A. Yes! You've got it! Vault supports the use of an HSM, as well as various cloud KMS services for auto-unseal.

**Question 3: Your organization has already configured the current Vault environment to use an HSM as the seal mechanism for your Vault cluster. Your manager now wants to explore the use of seal wrapping.**

**What statement most accurately describes the benefits of using seal wrapping with an HSM?**

- Seal wrapping adds an extra layer of security by adding an extra layer an unseal keys. Essentially requiring two different sets of unseal keys to be supplied to unseal the Vault cluster.
- Seal wrapping is the default encryption used to encrypt Vault data and does not require a Vault Enterprise license.

- Seal wrapping adds an extra layer of protection by wrapping values with an extra layer of encryption, and when used with an HSM, conforms with FIPS 140-2 directives on Key Storage and Key Transport.

- Seal wrapping adds an extra layer of protection by wrapping values with an extra layer of encryption but does not provide an accredited or certified benefits.

Answer: C. Yes! Seal wrapping is a mechanism to wrap values with an extra layer of encryption. Vault's Seal Wrap feature has been evaluated by Leidos for compliance with FIPS 140-2 requirements. When used with a FIPS 140-2-compliant HSM, Vault will store Critical Security Parameters (CSPs) in a manner that is compliant with KeyStorage and KeyTransit requirements. By the way, starting with newer versions of Vault, HashiCorp now provides binaries that can provide FIPS 140-2 compliance WITHOUT an HSM.

## Section 7, Quiz 6 - Scale Vault for Performance

**Question 1: Your organization has recently integrated Vault with a large-scale container-based application. The application frequently spins up a large number of containers and each container will request a token from Vault. Your team has noticed that this activity has a noticeable impact on performance and the storage backend of the Vault cluster. To reduce that impact, you are exploring the use of batch tokens.**

**Which statement is true regarding the benefits of batch tokens?**

- Batch tokens can be set as "periodic", essentially making tokens never expire as long as they are renewed within the TTL.

- Batch tokens are actually more "heavyweight" than service tokens and require multiple writes to create tokens.

- You can create batch tokens to act as root tokens.

- Batch token creations can scale with the number of performance standby nodes.

Answer: D. Boom! Nice job! Typical service tokens require a write/create operation, which would need to be forwarded to the leader node. Batch tokens are encrypted blobs that carry enough information for them to be used for Vault actions and can scale with the number of performance standby nodes in the cluster.

**Question 2: You are currently working with the executive team to grow the usage of Vault Enterprise to multiple cloud regions and data centers across your infrastructure. The goal is to have applications in multiple clouds, in multiple regions, all interact with Vault to retrieve secrets. In addition, you want to ensure that applications can communicate with Vault in the local region to reduce latency for network requests.**

**What would be the best solution to meet these requirements?**

- Increase the number of nodes in the Vault cluster and use performance standbys to increase performance for the new load from applications.

- Create new Vault clusters in each region where applications reside. Then enable Disaster Recovery Replication on the new clusters, allowing client requests to be handled locally.
- Create new Vault clusters in each region where applications reside. Then enable Performance Replication on the new clusters, allowing client requests to be handled locally.
- Create multiple secret engine mount points on a per-region basis. Each region will have dedicated secret engine mount points, splitting the load of requests from new applications.

Answer: C. Yes! PR clusters replicate Vault data to new regions, as well as enabling the handling of client requests locally.

**Question 3: 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?**

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

Answer: A. Yes, perfect! Remember that Performance standby nodes only handle read requests locally.

**Question 4: Your organization has already implemented Vault Enterprise and plans to use Performance Replication between the North American and European regions. Due to GDPR compliance, you need to ensure that certain secret data is not replicated from the European region to North America once replication is enabled.**

**Which Vault feature would allow you to enable replication, while also ensuring that specific data in Europe is NOT replicated to North America?**

- Endpoint Governing Policies (EGPs)
- Paths filters
- Namespaces
- Vault tokens configured with “token bound CIDRs”

Answer: B. You got it! The paths filter feature enables users to allow or deny which secrets engines are replicated between clusters, and is the best choice.

## Section 8, Quiz 7 - Configure Access Control

**Question 1: 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 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"]
  }

Answer: B. Correct answer.

**Question 2: Your organization has begun using Vault Namespaces to more securely segment data with multi-tenancy. A Vault namespace was created named NA at the root level. A secret lives at the secret/database/postgres path in the NA namespace. Assuming that a Vault policy was granting the read permission, which of the following configurations would NOT properly grant access to that secret?**

- A Vault policy created at the root level with permissions on the **secret/database/postgres** path
- A Vault policy created at the root level with permissions on the **NA/secret/database/postgres** path
- A Vault policy created in the **NA** Namespace with permissions on the **secret/database/postgres** path

- A Vault policy created at the root level with permissions on the **+/secret/database/postgres** path

Answer: A. Correct, this configuration would NOT grant access to the path in the NA namespace.

**Question 3: As part of an internal initiative, your organization has decided to implement the Vault Enterprise feature of Control Groups. The goal is to add a layer of protection for certain activities in Vault. Which of the following statements most accurately describes the function of a Control Group?**

- Control Groups are a different way of managing access to items in vault
- Control Groups enable fine-grained control through "policy as code"
- Control Groups help organize Vault identities into logical groups to more easily manage access
- Control Groups add additional authorization factors to be required before satisfying a request

Answer: D. Yes, you got it. Control Groups provide and additional method to permit/deny access to resources/paths in Vault.

**Question 4: An internal compliance initiative has been adopted at your organization, and the head of the compliance team is interested in how Sentinel can integrate with Vault. Sentinel can provide a rich set of access control functionality that goes beyond the standard Vault ACL policies. What are the two additional policy types that can be used with Sentinel?**

- Secret Governing Policies (SGPs) and Authentication Governing Policies (AGPs)
- Role Governing Policies (RGPs) and Endpoint Governing Policies (EGPs)
- Extended Governance Policies (EGPs) and Token Governing Policies (TGPs)
- Functional Governance Policies (FGPs) and Path-Based Governing Policies (PGPs)

Answer: B. Correct Answer.

**Question 5: Your organization's Vault environment has multiple auth methods enabled in multiple Namespaces. In the current setup, users may have more than one login method to use when authenticating to Vault, and each method would provide different sets of access. This has led to confusion with end-users not knowing which auth method or Namespace to use, or experiencing permission issues if they log into the auth method with different permissions.**

**To simplify authentication, you would like to have only one auth method enabled at the root level and use existing Vault policies in each Namespace to grant access. How could you accomplish this goal using identity groups and group aliases?**

- Create internal groups in each namespace with the required policies attached to the group. Then use group aliases to attach those groups to the auth method at the root level.

- Simply use group aliases at the root level and add the required policies from other Namespaces to be assigned.
- Create internal groups in each Namespace with the required policies attached to the group. Then add the desired group ID(s) or entity ID(s) that exist at the root level as member group IDs and/or member entity IDs.
- It is not possible to have a user authenticate at the root level and inherit policies from child Namespaces.

Answer: C. Correct Answer.

## Section 9, Quiz 8 - Configure Vault Agent

**Question 1: Your organization has begun using the Vault Agent to more easily integrate applications with Vault for secure secrets. In addition to managing the token lifecycle for these applications, Vault Agent templating will be used to automatically format a secret retrieved from Vault. As part of the implementation, you will need to configure the Vault agent to run as a daemon on the application servers.**

**Based on the following configuration, which statement is correct?**

```
listener "tcp" {
  address = "127.0.0.1:8200"
}

vault {
  address = "https://vault-demo.com:8200"
}

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.txt"
    mode = "0640"
  }
}

template {
  source = "./test.tmpl"
  destination = "./test.txt"
}
```

- The Vault Agent will store the Vault token retrieved during authentication and make it readable to ALL users on the system.
- The Vault Agent will attempt to use templating configurations found in the **./test.tmpl** file.
- The Vault Agent is using response wrapping to more securely authenticate to Vault with a role ID and secret ID.
- They Vault Agent will attempt to use templating instructions found in the **'./test.txt'** file.

Answer: B. Yes, this is correct. You can tell by the template stanza, in which the source is ./test.tmpl.

**Question 2: Based on the following configuration, the Vault Agent will authenticate to Vault, retrieve a Vault token, and then exit/shutdown the Vault Agent process.**

```
listener "tcp" {
  address = "127.0.0.1:8200"
}

vault {
  address = "https://vault-demo.com:8200"
}

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"
}
```

- True
- False

Answer: B. Yes, correct. The configuration of exit_after_auth = false tells the Vault Agent not to exit. This is also the default setting for this feature.

**Question 3: Based on the following configuration, the Vault Agent will attempt to connect to the Vault cluster at which address?**

Top of Form

```
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”
}
```

Bottom of Form

- https://127.0.0.1:8200
- It is using a Unix socket listener on localhost
- The configuration file does not contain that information and needs to be configured in the unit file or startup command
- https://vault-demo.com:8200

Answer: D. Correct, nice job.

**Question 4: 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?**

- AWS
- Kubernetes
- LDAP
- Azure
- AppRole

Answer: C. Correct, this is not a valid auth method because LDAP is an interactive auth method and the Vault Agent can’t use that type of auth method to communicate to Vault.

**Question 5: Vault Agent's Template functionality allows Vault secrets to be rendered to files using Consul Template markup. Your team has a use case to retrieve and format a secret from Vault before an application consumes it for usage. Here is an example template configuration; which of the following is NOT a valid statement?**

```
1. {{ with secret "secret/data/app1" }}
2. ID: {{ .Data.data.username }}
3. Color: {{ .Data.data.color }}
4. {{ end }}
```

Top of Form

```
1. {{ end }}
```

- The path of the secret in Vault is **secret/data/app1**
- The secret in Vault contains a key with the name **ID**
- The secret in Vault contains a key with the name **username**
- The secret in Vault contains a key with the name **color**

Answer: B. Correct, there is no reference to getting a secret with a key of ID.