

# *HashiCorp*

VA-002-P  
*HashiCorp Certified: Vault Associate*

Product Version

**Questions & Answers PDF**

For More Information – **Visit link below:**

**<https://www.cert4prep.com/>**

---

# Total Questions: 200

## Latest Version

### Question: 1

Select two answers to complete the following sentence:

Before a new provider can be used, it must be \_\_\_\_\_ and \_\_\_\_\_.

- A. approved by HashiCorp
- B. declared in the configuration
- C. initialized
- D. uploaded to source control

**Answer: B, C**

Explanation:

Each time a new provider is added to configuration -- either explicitly via a provider block or by adding a resource from that provider -- Terraform must initialize the provider before it can be used. Initialization downloads and installs the provider's plugin so that it can later be executed.

### Question: 2

Which of the following best describes the default local backend?

- A. The local backend stores state on the local filesystem locks the state using system APIs and performs operations locally.
- B. The local backend is the directory where resources deployed by Terraform have direct access to in order to update their current state
- C. The local backend is how Terraform connects to public cloud services, such as AWS, Azure, or GCP.
- D. The local backend is where Terraform Enterprise stores logs to be processed by a log collector

**Answer: A**

Explanation:

Information on the default local backend can be found at this link.

Example:

```
terraform {  
  backend "local" {  
    path = "relative/path/to/terraform.tfstate"  
  }  
}
```

---

### Question: 3

True or False:

Multiple providers can be declared within a single Terraform configuration file.

- A. False
- B. True

**Answer: B**

Explanation:

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

What Terraform feature is shown in the example below?

```
1. resource "aws_security_group" "example" {  
2.   name = "sg-app-web-01"  
3.   dynamic "ingress" {  
4.     for_each = var.service_ports  
5.     content {  
6.       from_port = ingress.value  
7.       to_port = ingress.value  
8.       protocol = "tcp"  
9.     }  
10.  }  
11. }
```

- A. data source
- B. dynamic block
- C. local values
- D. conditional expression

**Answer: B**

Explanation:

You can dynamically construct repeatable nested blocks like ingress using a special dynamic block type, which is supported inside resource, data, provider, and provisioner blocks

### Question: 5

In regards to Terraform state file, select all the statements below which are correct: (select four)

- A. storing state remotely can provide better security
- B. the Terraform state can contain sensitive data, therefore the state file should be protected from unauthorized access
- C. Terraform Cloud always encrypts state at rest
- D. using the mask feature, you can instruct Terraform to mask sensitive data in the state file
- E. when using local state, the state file is stored in plain-text
- F. the state file is always encrypted at rest

**Answer: A, B, C, E**

Explanation:

Terraform state can contain sensitive data, depending on the resources in use and your definition of "sensitive." The state contains resource IDs and all resource attributes. For resources such as databases, this may contain initial passwords.

When using local state, state is stored in plain-text JSON files.

If you manage any sensitive data with Terraform (like database passwords, user passwords, or private keys), treat the state itself as sensitive data.

Storing Terraform state remotely can provide better security. As of Terraform 0.9, Terraform does not persist state to the local disk when remote state is in use, and some backends can be configured to encrypt the state data at rest.

## Question: 6

What are the benefits of using Infrastructure as Code? (select five)

- A. Infrastructure as Code easily replaces development languages such as Go and .Net for application development
- B. Infrastructure as Code allows a user to turn a manual task into a simple, automated deployment
- C. Infrastructure as Code is relatively simple to learn and write, regardless of a user's prior experience with developing code
- D. Infrastructure as Code is easily repeatable, allowing the user to reuse code to deploy similar, yet different resources
- E. Infrastructure as Code provides configuration consistency and standardization among deployments
- F. Infrastructure as Code gives the user the ability to recreate an application's infrastructure for disaster recovery scenarios

**Answer: B, C, D, E, F**

Explanation:

If you are new to infrastructure as code as a concept, it is the process of managing infrastructure in a file or files rather than manually configuring resources in a user interface. A resource in this instance is any piece of infrastructure in a given environment, such as a virtual machine, security group, network interface, etc.

---

At a high level, Terraform allows operators to use HCL to author files containing definitions of their desired resources on almost any provider (AWS, GCP, GitHub, Docker, etc) and automates the creation of those resources at the time of application.

### Question: 7

What are some of the problems of how infrastructure was traditionally managed before Infrastructure as Code? (select three)

- A. Requests for infrastructure or hardware required a ticket, increasing the time required to deploy applications
- B. Traditional deployment methods are not able to meet the demands of the modern business where resources tend to live days to weeks, rather than months to years
- C. Traditionally managed infrastructure can't keep up with cyclic or elastic applications
- D. Pointing and clicking in a management console is a scalable approach and reduces human error as businesses are moving to a multi-cloud deployment model

**Answer: A, B, C**

Explanation:

Businesses are making a transition where traditionally-managed infrastructure can no longer meet the demands of today's businesses. IT organizations are quickly adopting the public cloud, which is predominantly API-driven.

To meet customer demands and save costs, application teams are architecting their applications to support a much higher level of elasticity, supporting technology like containers and public cloud resources. These resources may only live for a matter of hours; therefore the traditional method of raising a ticket to request resources is no longer a viable option. Pointing and clicking in a management console is NOT scale and increases the chance of human error.

### Question: 8

True or False:

A list(...) may contain a number of values of the same type while an object(...) can contain a number of values of different types.

- A. True
- B. False

**Answer: A**

Explanation:

A collection type allows multiple values of one other type to be grouped together as a single value. This includes a list, map, and set.

A structural type allows multiple values of several distinct types to be grouped together as a single value. This includes object and tuple.

---

### Question: 9

True or False: Provisioners should only be used as a last resort.

- A. true
- B. false

**Answer: A**

Explanation:

Provisioners are used to execute scripts on a local or remote machine as part of resource creation or destruction. Provisioners can be used to bootstrap a resource, cleanup before destroy, run configuration management, etc. Even if the functionality you need is not available in a provider today, HashiCorp suggests that you consider local-exec usage as a temporary workaround and to open an issue in the relevant provider's repo to discuss adding first-class support.

### Question: 10

After running into issues with Terraform, you need to enable verbose logging to assist with troubleshooting the error. Which of the following values provides the MOST verbose logging?

- A. ERROR
- B. INFO
- C. DEBUG
- D. WARN
- E. TRACE

**Answer: E**

Explanation:

Terraform has detailed logs that can be enabled by setting the TF\_LOG environment variable to any value. This will cause detailed logs to appear on stderr.

You can set TF\_LOG to one of the log levels TRACE, DEBUG, INFO, WARN, or ERROR to change the verbosity of the logs. TRACE is the most verbose and it is the default if TF\_LOG is set to something other than a log level name.

### Question: 11

What are some of the features of Terraform state? (select three)

- A. inspection of cloud resources
- B. increased performance
- C. mapping configuration to real-world resources
- D. determining the correct order to destroy resources

---

**Answer: B, C, D**

Explanation:

See this page on the purpose of Terraform state and the benefits it provides.

### Question: 12

In regards to deploying resources in multi-cloud environments, what are some of the benefits of using Terraform rather than a provider's native tooling? (select three)

- A. Terraform simplifies management and orchestration, helping operators build large-scale, multi-cloud infrastructure
- B. Terraform can help businesses deploy applications on multiple clouds and on-premises infrastructure
- C. Terraform can manage cross-cloud dependencies
- D. Terraform is not cloud-agnostic and can be used to deploy resources across a single public cloud

**Answer: A, B, C**

Explanation:

Terraform is a cloud-agnostic tool, and therefore isn't limited to a single cloud provider, such as AWS CloudFormation or Azure Resource Manager. Terraform supports all of the major cloud providers and allows IT organizations to focus on learning a single tool for deploying its infrastructure, regardless of what platform it's being deployed on.

### Question: 13

HashiCorp offers multiple versions of Terraform, including Terraform open-source, Terraform Cloud, and Terraform Enterprise. Which of the following Terraform features are only available in the Enterprise edition? (select four)

- A. Sentinel
- B. SAML/SSO
- C. Audit Logs
- D. Private Network Connectivity
- E. Private Module Registry
- F. Clustering

**Answer: B, C, D, F**

Explanation:

While there are a ton of features that are available to open source users, many features that are part of the Enterprise offering are geared towards larger teams and enterprise functionality.

### Question: 14

True or False:

State is a requirement for Terraform to function.

- A. True
- B. False

**Answer: A**

Explanation:

Terraform requires some sort of database to map Terraform config to the real world. When you have a resource in your configuration, Terraform uses this map to know how that resource is represented. Therefore, to map configuration to resources in the real world, Terraform uses its own state structure.

### Question: 15

In the example below, where is the value of the DNS record's IP address originating from?

1. resource "aws\_route53\_record" "www" {
2. zone\_id = aws\_route53\_zone.primary.zone\_id
3. name = "[www.helloworld.com](http://www.helloworld.com)"
4. type = "A"
5. ttl = "300"
6. records = [module.web\_server.instance\_ip\_addr]
7. }

- A. value of the web\_server parameter from the variables.tf file
- B. the output of a module named web\_server
- C. the regular expression named module.web\_server
- D. by querying the AWS EC2 API to retrieve the IP address

**Answer: B**

Explanation:

In a parent module, outputs of child modules are available in expressions as module.<MODULE NAME>.<OUTPUT NAME>. For example, if a child module named web\_server declared an output named instance\_ip\_addr, you could access that value as module.web\_server.instance\_ip\_addr.

### Question: 16

Using multi-cloud and provider-agnostic tools provides which of the following benefits? (select two)

- A. operations teams only need to learn and manage a single tool to manage infrastructure, regardless of where the infrastructure is deployed
- B. slower provisioning speed allows the operations team to catch mistakes before they are applied
- C. can be used across major cloud providers and VM hypervisors
- D. increased risk due to all infrastructure relying on a single tool for management



---

**Answer: A, C**

Explanation:

Using a tool like Terraform can be advantageous for organizations deploying workloads across multiple public and private cloud environments. Operations teams only need to learn a single tool, single language, and can use the same tooling to enable a DevOps-like experience and workflows.

### Question: 17

True or False:

Workspaces provide identical functionality in the open-source, Terraform Cloud, and Enterprise versions of Terraform.

- A. True
- B. False

**Answer: B**

Explanation:

Workspaces, managed with the terraform workspace command, aren't the same thing as Terraform Cloud workspaces.

Terraform Cloud workspaces act more like completely separate working directories.

CLI workspaces(OSS) are just alternate state files.

### Question: 18

Given the Terraform configuration below, in which order will the resources be created?

1. resource "aws\_instance" "web\_server" {
2. ami = "i-abdce12345"
3. instance\_type = "t2.micro"
4. }
5. resource "aws\_eip" "web\_server\_ip" {
6. vpc = true
7. instance = aws\_instance.web\_server.id
8. }

- A.  
aws\_eip will be created first  
aws\_instance will be created second
- B.  
no resources will be created
- C.  
aws\_instance will be created first  
aws\_eip will be created second
- D.

---

resources will be created simultaneously

**Answer: C**

Explanation:

The `aws_instance` will be created first, and then `aws_eip` will be created second due to the `aws_eip`'s resource dependency of the `aws_instance` id

### Question: 19

Which of the following represents a feature of Terraform Cloud that is NOT free to customers?

- A. private module registry
- B. VCS integration
- C. roles and team management
- D. workspace management

**Answer: C**

### Question: 20

In Terraform Enterprise, a workspace can be mapped to how many VCS repos?

- A. 5
- B. 3
- C. 2
- D. 1

**Answer: D**

Explanation:

A workspace can only be configured to a single VCS repo, however, multiple workspaces can use the same repo, if needed. A good Explanation: of how to configure your code repositories can be found [here](#).

### Question: 21

What Terraform command can be used to inspect the current state file?

```
# aws_instance.example:
resource "aws_instance" "example" {
  ami                = "ami-2757f631"
  arn                = "arn:aws:ec2:us-east-1:130490850807:instance/i-0
  associate_public_ip_address = true
  availability_zone   = "us-east-1c"
  cpu_core_count      = 1
  cpu_threads_per_core = 1
  disable_api_termination = false
  ebs_optimized        = false
  get_password_data    = false
  id                  = "i-0bbf06244e44211d1"
  instance_state       = "running"
  instance_type        = "t2.micro"
```

- A. terraform inspect
- B. terraform show
- C. terraform read
- D. terraform state

**Answer: B**

Explanation:

The terraform show command is used to provide human-readable output from a state or plan file. This can be used to inspect a plan to ensure that the planned operations are expected, or to inspect the current state as Terraform sees it.

Machine-readable output can be generated by adding the -json command-line flag.

Note: When using the -json command-line flag, any sensitive values in Terraform state will be displayed in plain text.

## Question: 22

What is the best and easiest way for Terraform to read and write secrets from HashiCorp Vault?

- A. CLI access from the same machine running Terraform
- B. API access using the AppRole auth method
- C. Vault provider
- D. Integration with a tool like Jenkins

**Answer: C**

Explanation:

The Vault provider allows Terraform to read from, write to, and configure Hashicorp Vault.

## Question: 23

Which of the following connection types are supported by the remote-exec provisioner? (select two)

- A. rdp
- B. smb
- C. ssh
- D. winrm

**Answer: C, D**

Explanation:

The remote-exec provisioner invokes a script on a remote resource after it is created. The remote-exec provisioner supports both ssh and winrm type connections.

### Question: 24

True or False: You can migrate the Terraform backend but only if there are no resources currently being managed.

- A. False
- B. True

**Answer: A**

Explanation:

If you are already using Terraform to manage infrastructure, you probably want to transfer to another backend, such as Terraform Cloud, so you can continue managing it. By migrating your Terraform state, you can hand off infrastructure without de-provisioning anything.

### Question: 25

Which of the following actions are performed during a terraform init? (select three)

- A. provisions the declared resources in your configuration
- B. download the declared providers which are supported by HashiCorp
- C. initializes the backend configuration
- D. initializes downloaded and/or installed providers

**Answer: B, C, D**

Explanation:

The terraform init command is used to initialize a working directory containing Terraform configuration files. This is the first command that should be run after writing a new Terraform configuration or cloning an existing one from version control. It is safe to run this command multiple times.

### Question: 26

---

Which of the following allows Terraform users to apply policy as code to enforce standardized configurations for resources being deployed via infrastructure as code?

- A. functions
- B. workspaces
- C. module registry
- D. sentinel

**Answer: D**

Explanation:

Sentinel is an embedded policy-as-code framework integrated with the HashiCorp Enterprise products. It enables fine-grained, logic-based policy decisions, and can be extended to use information from external sources.

### Question: 27

When multiple engineers start deploying infrastructure using the same state file, what is a feature of remote state storage that is critical to ensure the state does not become corrupt?

- A. state locking
- B. object storage
- C. encryption
- D. workspaces

**Answer: A**

Explanation:

If supported by your backend, Terraform will lock your state for all operations that could write state. This prevents others from acquiring the lock and potentially corrupting your state. State locking happens automatically on all operations that could write state. You won't see any message that it is happening. If state locking fails, Terraform will not continue. You can disable state locking for most commands with the -lock flag but it is not recommended.

### Question: 28

Your organization has moved to AWS and has manually deployed infrastructure using the console. Recently, a decision has been made to standardize on Terraform for all deployments moving forward. What can you do to ensure that all existing is managed by Terraform moving forward without interruption to existing services?

- A. resources that are manually deployed in the AWS console cannot be imported by Terraform
- B. using terraform import, import the existing infrastructure into your Terraform state
- C. delete the existing resources and recreate them using new a Terraform configuration so Terraform can manage them moving forward

---

D. submit a ticket to AWS and ask them to export the state of all existing resources and use terraform import to import them into the state file

**Answer: B**

Explanation:

Terraform is able to import existing infrastructure. This allows you to take resources you've created by some other means and bring it under Terraform management.

This is a great way to slowly transition infrastructure to Terraform or to be sure you're confident that you can use Terraform in the future if it currently doesn't support every AWS service or feature you need

today.

### Question: 29

What happens when a terraform plan is executed?

- A. the backend is initialized and the working directory is prepped
- B. creates an execution plan and determines what changes are required to achieve the desired state in the configuration files.
- C. applies the changes required in the target infrastructure in order to reach the desired configuration
- D. reconciles the state Terraform knows about with the real-world infrastructure

**Answer: B**

Explanation:

The terraform plan command is used to create an execution plan. Terraform performs a refresh, unless explicitly disabled, and then determines what actions are necessary to achieve the desired state specified in the configuration files.

After a plan has been run, it can be executed by running a terraform apply

### Question: 30

Which of the following Terraform files should be ignored by Git when committing code to a repo? (select two)

- A. output.tf
- B. terraform.tfstate
- C. terraform.tfvars
- D. variables.tf

**Answer: B, C**

Explanation:

---

The .gitignore file should be configured to ignore Terraform files that either contain sensitive data or aren't required to save.

The terraform.tfstate file contains the terraform state of a specific environment and doesn't need to be preserved in a repo. The terraform.tfvars file may contain sensitive data, such as passwords or IP addresses of an environment that you may not want to share with others.

### Question: 31

You want to use terraform import to start managing infrastructure that was not originally provisioned through infrastructure as code. Before you can import the resource's current state, what must you do in order to prepare to manage these resources using Terraform?

- A. run terraform refresh to ensure that the state file has the latest information for existing resources.
- B. update the configuration file to include the new resources
- C. modify the Terraform state file to add the new resources
- D. shut down or stop using the resources being imported so no changes are inadvertently missed

**Answer: B**

Explanation:

The current implementation of Terraform import can only import resources into the state. It does not generate a configuration. Because of this, and prior to running terraform import, it is necessary to manually write a resource configuration block for the resource to which the imported object will be mapped.

First, add the resources to the configuration file:

```
resource "aws_instance" "example" {  
  # ...instance configuration...  
}
```

Then run the following command:

```
$ terraform import aws_instance.example i-abcd1234
```

### Question: 32

By default, where does Terraform store its state file?

- A. shared directory
- B. current working directory
- C. Amazon S3 bucket
- D. remotely using Terraform Cloud

**Answer: B**

Explanation:

By default, the state file is stored in a local file named "terraform.tfstate", but it can also be stored remotely, which works better in a team environment.

### Question: 33

Why is it a good idea to declare the required version of a provider in a Terraform configuration file?

1. terraform {
2. required\_providers {
3. aws = "~> 1.0"
4. }
5. }

- A. to remove older versions of the provider
- B. to ensure that the provider version matches the version of Terraform you are using
- C. providers are released on a separate schedule from Terraform itself; therefore a newer version could introduce breaking changes
- D. to match the version number of your application being deployed via Terraform

**Answer: C**

Explanation:

Providers are plugins released on a separate rhythm from Terraform itself, and so they have their own version numbers. For production use, you should constrain the acceptable provider version via configuration. This helps to ensure that new versions with potentially breaking changes will not be automatically installed by terraform init in the future.

### Question: 34

Select the answer below that completes the following statement:

Terraform Cloud can be managed from the CLI but requires \_\_\_\_\_?

- A. a TOTP token
- B. a username and password
- C. authentication using MFA
- D. an API token

**Answer: D**

Explanation:

API and CLI access are managed with API tokens, which can be generated in the Terraform Cloud UI. Each user can generate any number of personal API tokens, which allow access with their own identity and permissions. Organizations and teams can also generate tokens for automating tasks that aren't tied to an individual user.

### Question: 35

Terraform-specific settings and behaviors are declared in which configuration block type?



- A. data
- B. resource
- C. terraform
- D. provider

**Answer: C**

Explanation:

The special terraform configuration block type is used to configure some behaviors of Terraform itself, such as requiring a minimum Terraform version to apply your configuration.

### Question: 36

Which flag would be used within a Terraform configuration block to identify the specific version of a provider required?

- A. required-provider
- B. required\_versions
- C. required\_providers
- D. required-version

**Answer: C**

Explanation:

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"  
  }  
}
```

### Question: 37

What is the purpose of using the local-exec provisioner? (select two)

- A. ensures that the resource is only executed in the local infrastructure where Terraform is deployed
- B. to execute one or more commands on the machine running Terraform
- C. to invoke a local executable
- D. executes a command on the resource to invoke an update to the Terraform state

---

**Answer: B, C**

Explanation:

The local-exec provisioner invokes a local executable after a resource is created. This invokes a process on the machine running Terraform, not on the resource.

Note that even though the resource will be fully created when the provisioner is run, there is no guarantee that it will be in an operable state - for example, system services such as sshd may not be started yet on compute resources.

### Question: 38

What feature of Terraform Cloud and/or Terraform Enterprise can you publish and maintain a set of custom modules which can be used within your organization?

- A. custom VCS integration
- B. remote runs
- C. private module registry
- D. Terraform registry

**Answer: C**

Explanation:

You can use modules from a private registry, like the one provided by Terraform Cloud. Private registry modules have source strings of the form <HOSTNAME>/<NAMESPACE>/<NAME>/<PROVIDER>. This is the same format as the public registry, but with an added hostname prefix.

### Question: 39

Select the operating systems which are supported for a clustered Terraform Enterprise: (select four)

- A. Unix
- B. Amazon Linux
- C. Red Hat
- D. Ubuntu
- E. CentOS

**Answer: B, C, D, E**

Explanation:

Note: (5/27/20) This

**question: has been**

recently updated to reflect documentation updates on the HashiCorp website. It seems they have removed the clustering-specific requirements and are now following the standard Enterprise operating system requirements.

---

Terraform Enterprise currently supports running under the following operating systems for a Clustered deployment:

- Ubuntu 16.04.3 - 16.04.5 / 18.04
- Red Hat Enterprise Linux 7.4 through 7.7
- CentOS 7.4 - 7.7
- Amazon Linux
- Oracle Linux

Clusters currently don't support other Linux variants.

<https://www.terraform.io/docs/enterprise/before-installing/index.html#operating-system-requirements>

Question: 40

Which of the following variable declarations is going to result in an error?

- A.  
variable "example" {  
 type = object({})  
}
- B.  
variable "example" {}
- C.  
variable "example" {  
 description = "This is a test"  
 type = map  
 default = {"one" = 1, "two" = 2, "Three" = "3"}  
}
- D.  
variable "example" {  
 description = "This is a variable description"  
 type = list(string)  
 default = {}  
}

<b>Answer: B</b>
------------------

Explanation:

Lists are defined with [ ], maps are defined with { }.

<https://www.terraform.io/docs/configuration/types.html#structural-types>

## Question: 41

Which of the following is not a valid Terraform string function?

- A. tostring
- B. replace
- C. format
- D. join

---

**Answer: A**

Explanation:

tostring is not a string function, it is a type conversion function. tostring converts its argument to a string value. <https://www.terraform.io/docs/configuration/functions/tostring.html>

### Question: 42

The Terraform language supports a number of different syntaxes for comments. Select all that are supported. (select three)

- A. #
- B. /\* and \*/
- C. <\* and \*>
- D. //

**Answer: A, B, D**

Explanation:

Terraform supports the #, //, and /\*..\*/ for commenting Terraform configuration files. Please use them when writing Terraform so both you and others who are using your code have a full understanding of what the code is intended to do.

<https://www.terraform.io/docs/configuration/syntax.html#comments>

### Question: 43

Which of the following commands will launch the Interactive console for Terraform interpolations?

- A. terraform
- B. terraform console
- C. terraform cmdline
- D. terraform cli

**Answer: B**

Explanation:

The terraform console command provides an interactive console for evaluating expressions.

<https://www.terraform.io/docs/commands/console.html>

### Question: 44

A user runs terraform init on their RHEL based server and per the output, two provider plugins are downloaded:

1. \$ terraform init
- 2.

---

3. Initializing the backend...  
4.  
5. Initializing provider plugins...  
6. - Checking for available provider plugins...  
7. - Downloading plugin for provider "aws" (hashicorp/aws) 2.44.0...  
8. - Downloading plugin for provider "random" (hashicorp/random) 2.2.1...  
9.  
10. Terraform has been successfully initialized!  
Where are these plugins downloaded to?

- A. /etc/terraform/plugins
- B. The .terraform.plugins directory in the directory terraform init was executed in.
- C. The .terraform.d directory in the directory terraform init was executed in.
- D. The .terraform/plugins directory in the directory terraform init was executed in.

<b>Answer: D</b>
------------------

Explanation:

By default, terraform init downloads plugins into a subdirectory of the working directory, .terraform/plugins, so that each working directory is self-contained.

### Question: 45

What is the result of the following terraform function call?

`zipmap(["a", "b"], [1, 2])`

- A.  
{  
  "a",  
  "b",  
  "1",  
  "2",  
}
- B.  
[  
  "a",  
  "b",  
  "1",  
  "2",  
]
- C.  
{  
  "a" = 1  
  "b" = 2  
}
- D.  
[

```
"a" = 1
"b" = 2
]
```

**Answer: C**

Explanation:

zipmap constructs a map from a list of keys and a corresponding list of values. A map is denoted by { } whereas a list is denoted by [ ].

<https://www.terraform.io/docs/configuration/functions/zipmap.html>

### Question: 46

Select the most accurate statement to describe the Terraform language from the following list.

- A. Terraform is an immutable, declarative, Infrastructure as Code provisioning language based on Hashicorp Configuration Language, or optionally JSON.
- B. Terraform is a mutable, declarative, Infrastructure as Code configuration management language based on Hashicorp Configuration Language, or optionally JSON.
- C. Terraform is an immutable, procedural, Infrastructure as Code configuration management language based on Hashicorp Configuration Language, or optionally JSON.
- D. Terraform is a mutable, procedural, Infrastructure as Code provisioning language based on Hashicorp Configuration Language, or optionally YAML.

**Answer: A**

Explanation:

Terraform is not a configuration management tool - <https://www.terraform.io/intro/vs/chef-puppet.html>

Terraform is a declarative language - <https://www.terraform.io/docs/configuration/index.html>

Terraform supports a syntax that is JSON compatible - <https://www.terraform.io/docs/configuration/syntax-json.html>

Terraform is primarily designed on immutable infrastructure principles - <https://www.hashicorp.com/resources/what-is-mutable-vs-immutable-infrastructure>

### Question: 47

Select all Operating Systems that Terraform is available for. (select five)

- A. Linux
- B. Windows
- C. Unix
- D. FreeBSD
- E. Solaris
- F. macOS

---

**Answer: A, B, D, E, F**

Explanation:

Terraform is available for macOS, FreeBSD, OpenBSD, Linux, Solaris, Windows

<https://www.terraform.io/downloads.html>

### Question: 48

In the example below, the `depends_on` argument creates what type of dependency?

```
1. resource "aws_instance" "example" {  
2.   ami           = "ami-2757f631"  
3.   instance_type = "t2.micro"  
4.   depends_on = [aws_s3_bucket.company_data]  
5. }
```

- A. non-dependency resource
- B. implicit dependency
- C. explicit dependency
- D. internal dependency

**Answer: C**

Explanation:

Sometimes there are dependencies between resources that are not visible to Terraform. The `depends_on` argument is accepted by any resource and accepts a list of resources to create explicit dependencies for.

### Question: 49

Why might a user opt to include the following snippet in their configuration file?

```
1. terraform {  
2.   required_version = ">= 0.12"  
3. }
```

- A. this ensures that all Terraform providers are above a certain version to match the application being deployed
- B. the user wants to ensure that the application being deployed is a minimum version of 0.12
- C. versions before Terraform 0.12 were not approved by HashiCorp to be used in production
- D. Terraform 0.12 introduced substantial changes to the syntax used to write Terraform configuration

**Answer: D**

Explanation:

---

You can use `required_version` to ensure that a user deploying infrastructure is using Terraform 0.12 or greater, due to the vast number of changes that were introduced. As a result, many previously written configurations had to be converted or rewritten.

### Question: 50

Terraform has detailed logs which can be enabled by setting the \_\_\_\_\_ environmental variable.

- A. TF\_LOG
- B. TF\_TRACE
- C. TF\_DEBUG
- D. TF\_INFO

**Answer: A**

Explanation:

Terraform has detailed logs that can be enabled by setting the `TF_LOG` environment variable to any value. This will cause detailed logs to appear on `stderr`.

You can set `TF_LOG` to one of the log levels `TRACE`, `DEBUG`, `INFO`, `WARN`, or `ERROR` to change the verbosity of the logs. `TRACE` is the most verbose and it is the default if `TF_LOG` is set to something other than a log level name.

<https://www.terraform.io/docs/internals/debugging.html>

### Question: 51

In the following code snippet, the block type is identified by which string?

```
1. resource "aws_instance" "db" {  
2.   ami = "ami-123456"  
3.   instance_type = "t2.micro"  
4. }
```

- A. "db"
- B. resource
- C. "aws\_instance"
- D. instance\_type

**Answer: B**

Explanation:

The format of resource block configurations is as follows:

`<block type> "<resource type>" "<local name/label>"`

### Question: 52

Choose the correct answer which fixes the syntax of the following Terraform code:



A.  
resource "aws\_security\_group" "vault\_elb" {  
 name = "\${var.name\_prefix}-vault-elb"  
 description = var\_Vault ELB  
 vpc\_id = var.vpc\_id  
}

B.  
resource "aws\_security\_group" "vault\_elb" {  
 name = "\${var.name\_prefix}-vault-elb"  
 description = Vault ELB  
 vpc\_id = var.vpc\_id  
}

C.  
resource "aws\_security\_group" "vault\_elb" {  
 name = "\${var.name\_prefix}-vault-elb"  
 description = "\${Vault ELB}"  
 vpc\_id = var.vpc\_id  
}

D.  
resource "aws\_security\_group" "vault\_elb" {  
 name = "\${var.name\_prefix}-vault-elb"  
 description = [Vault ELB]  
 vpc\_id = var.vpc\_id  
}

E.  
resource "aws\_security\_group" "vault\_elb" {  
 name = "\${var.name\_prefix}-vault-elb"  
 description = "Vault ELB"  
 vpc\_id = var.vpc\_id  
}

**Answer: E**

Explanation:

When assigning a value to an argument, it must be enclosed in quotes ("...") unless it is being generated programmatically.

### Question: 53

A "backend" in Terraform determines how the state is loaded and how an operation such as apply is executed. Which of the following is not a supported backend type?

- A. terraform enterprise
- B. s3
- C. github
- D. consul

E. artifactory

**Answer: C**

Explanation:

github is not a supported backend type.

<https://www.terraform.io/docs/backends/types/index.html>

### Question: 54

When writing the Terraform code, HashiCorp recommends that you use how many spaces between each nesting level?

- A. 2
- B. 5
- C. 4
- D. 1

**Answer: A**

Explanation:

HashiCorp style conventions state that you should use 2 spaces between each nesting level to improve the readability of Terraform configurations.

### Question: 55

Terraform Cloud is more powerful when you integrate it with your version control system (VCS) provider. Select all the supported VCS providers from the answers below. (select four)

- A. CVS Version Control
- B. GitHub Enterprise
- C. Bitbucket Cloud
- D. Azure DevOps Server
- E. GitHub

**Answer: B, C, D, E**

Explanation:

Terraform Cloud supports the following VCS providers:

- GitHub
- GitHub.com (OAuth)
- GitHub Enterprise
- GitLab.com
- GitLab EE and CE
- Bitbucket Cloud

- Bitbucket Server
- Azure DevOps Server
- Azure DevOps Services

<https://www.terraform.io/docs/cloud/vcs/index.html#supported-vcs-providers>

### Question: 56

Complete the following sentence:

For the local state, the workspaces are stored directly in a...

- A. a file called terraform.tfstate
- B. directory called terraform.workspaces.tfstate
- C. directory called terraform.tfstate.d
- D. a file called terraform.tfstate.backup

**Answer: C**

Explanation:

For local state, Terraform stores the workspace states in a directory called terraform.tfstate.d.

<https://www.terraform.io/docs/state/workspaces.html#workspace-internals>

### Question: 57

Which of the following terraform subcommands could be used to remove the lock on the state for the current configuration?

- A. unlock
- B. Removing the lock on a state file is not possible
- C. force-unlock
- D. state-unlock

**Answer: C**

Explanation:

terraform force-unlock removes the lock on the state for the current configuration.

### Question: 58

Provider dependencies are created in several different ways. Select the valid provider dependencies from the following list: (select three)

- A. Use of any resource belonging to a particular provider in a resource or data block in the configuration.
- B. Existence of any provider plugins found locally in the working directory.
- C. Explicit use of a provider block in configuration, optionally including a version constraint.
- D. Existence of any resource instance belonging to a particular provider in the current state.

---

**Answer: A, C, D**

Explanation:

The existence of a provider plugin found locally in the working directory does not itself create a provider dependency. The plugin can exist without any reference to it in the terraform configuration.

<https://www.terraform.io/docs/commands/providers.html>

### Question: 59

Terraform Enterprise (also referred to as pTFE) requires what type of backend database for a clustered deployment?

- A. Cassandra
- B. MSSQL
- C. PostgreSQL
- D. MySQL

**Answer: C**

Explanation:

External Services mode stores the majority of the stateful data used by the instance in an external PostgreSQL database and an external S3-compatible endpoint or Azure blob storage. There are still critical data stored on the instance that must be managed with snapshots. Be sure to check the PostgreSQL Requirements for information that needs to be present for Terraform Enterprise to work. This option is best for users with expertise managing PostgreSQL or users that have access to managed PostgreSQL offerings like AWS RDS.

### Question: 60

A user has created three workspaces using the command line - prod, dev, and test. The user wants to create a fourth workspace named stage. Which command will the user execute to accomplish this?

- A. terraform workspace -new stage
- B. terraform workspace -create stage
- C. terraform workspace create stage
- D. terraform workspace new stage

**Answer: D**

Explanation:

The terraform workspace new command is used to create a new workspace. <https://www.terraform.io/docs/commands/workspace/new.html>

### Question: 61

---

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?

- A. terraform apply
- B. terraform plan
- C. terraform init
- D. terraform delete

**Answer: B**

Explanation:

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.

### Question: 62

What is the result of the following terraform function call?

`index(["a", "b", "c"], "c")`

- A. 1
- B. true
- C. 2
- D. 0

**Answer: C**

Explanation:

index finds the element index for a given value in a list starting with index 0.

<https://www.terraform.io/docs/configuration/functions/index.html>

### Question: 63

The following is a snippet from a Terraform configuration file:

1. provider "aws" {
2. region = "us-east-1"
3. }
4. provider "aws" {
5. region = "us-west-1"
6. }

which, when validated, results in the following error:-

1. Error: Duplicate provider configuration
- 2.
3. on main.tf line 5:
4. 5: provider "aws" {

5.  
6. A default provider configuration for "aws" was already given at  
7. main.tf:1,1-15. If multiple configurations are required, set the " \_\_\_\_\_ "  
8. argument for alternative configurations.  
Fill in the blank in the error message with the correct string from the list below.

- A. label
- B. version
- C. alias
- D. multi

**Answer: C**

Explanation:

An alias meta-argument is used when using the same provider with different configurations for different resources.

<https://www.terraform.io/docs/configuration/providers.html#alias-multiple-provider-instances>

### Question: 64

A user has created a module called "my\_test\_module" and committed it to GitHub. Over time, several commits have been made with updates to the module, each tagged in GitHub with an incremental version number. Which of the following lines would be required in a module configuration block in terraform to select tagged version v1.0.4?

- A. source = "git::https://wpexpertsupport.com/my\_test\_module.git#tag=v1.0.4"
- B. source = "git::https://wpexpertsupport.com/my\_test\_module.git@tag=v1.0.4"
- C. source = "git::https://wpexpertsupport.com/my\_test\_module.git?ref=v1.0.4"
- D. source = "git::https://wpexpertsupport.com/my\_test\_module.git&ref=v1.0.4"

**Answer: C**

Explanation:

By default, Terraform will clone and use the default branch (referenced by HEAD) in the selected repository. You can override this using the ref argument:

```
module "vpc" {source = "git::https://wpexpertsupport.com/vpc.git?ref=v1.2.0"}
```

The value of the ref argument can be any reference that would be accepted by the git checkout command, including branch and tag names.

<https://www.terraform.io/docs/modules/sources.html#selecting-a-revision>

### Question: 65

In terraform, most resource dependencies are handled automatically. Which of the following statements describes best how terraform resource dependencies are handled?

- A. The terraform binary contains a built-in reference map of all defined Terraform resource dependencies. Updates to this dependency map are reflected in terraform versions. To ensure you are working with the latest resource dependency map you must be running the latest version of Terraform.
- B. Terraform analyses any expressions within a resource block to find references to other objects and treats those references as implicit ordering requirements when creating, updating, or destroying resources.
- C. Resource dependencies are identified and maintained in a file called resource. dependencies. Each terraform provider is required to maintain a list of all resource dependencies for the provider and it's included with the plugin during initialization when terraform init is executed. The file is located in the terraform.d folder.
- D. Resource dependencies are handled automatically by the depends\_on meta\_argument, which is set to true by default.

**Answer: B**

Explanation:

Terraform analyses any expressions within a resource block to find references to other objects and treats those references as implicit ordering requirements when creating, updating, or destroying resources.

<https://www.terraform.io/docs/configuration/resources.html>

### Question: 66

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?

- A. terraform workspace select dev
- B. terraform workspace -switch dev
- C. terraform workspace dev
- D. terraform workspace switch dev

**Answer: A**

Explanation:

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>

### Question: 67

Complete the following sentence:

The terraform state command can be used to \_\_\_\_

- A. view the entire state file
- B. modify the current state, such as removing items
- C. refresh the existing state
- D. there is no such command

---

**Answer: B**

Explanation:

The terraform state command is used for advanced state management. Rather than modify the state directly, the terraform state commands can be used in many cases instead.

<https://www.terraform.io/docs/commands/state/index.html>

### Question: 68

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. a private install
- B. disconnected
- C. non-traditional
- D. air-gapped

**Answer: D**

Explanation:

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.

### Question: 69

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.

- A. False
- B. True

**Answer: A**

Explanation:

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.

### Question: 70

During a terraform apply, a resource is successfully created but eventually fails during provisioning. What happens to the resource?



- A. Terraform attempts to provide the resource up to three times before exiting with an error
- B. the terraform plan is rolled back and all provisioned resources are removed
- C. it is automatically deleted
- D. the resource is marked as tainted

**Answer: D**

Explanation:

If a resource successfully creates but fails during provisioning, Terraform will error and mark the resource as "tainted". A resource that is tainted has been physically created, but can't be considered safe to use since provisioning failed.

Terraform also does not automatically roll back and destroy the resource during the apply when the failure happens, because that would go against the execution plan: the execution plan would've said a resource will be created, but does not say it will ever be deleted.

### Question: 71

True or False? By default, Terraform destroy will prompt for confirmation before proceeding.

- A. True
- B. False

**Answer: A**

Explanation:

Terraform destroy will always prompt for confirmation before executing unless passed the -auto-approve flag.

```
$ terraform destroy
```

Do you really want to destroy all resources?

Terraform will destroy all your managed infrastructure, as shown above.

There is no undo. Only 'yes' will be accepted to confirm.

Enter a value:

### Question: 72

When multiple arguments with single-line values appear on consecutive lines at the same nesting level, HashiCorp recommends that you:

- A. place a space in between each line

```
type = "A"
```

```
ttl = "300"
```

```
zone_id = aws_route53_zone.primary.zone_id
```

- B. align their equals signs

```
ami      = "abc123"
```

```
instance_type = "t2.micro"
```

C. place all arguments using a variable at the top

```
ami = var.aws_ami
instance_type = var.instance_size
subnet_id = "subnet-0bb1c79de3EXAMPLE"
tags = {
  Name = "HelloWorld"
}
D. put arguments in alphabetical order
name = "www.pythonfanclub.com"
records = [aws_eip.lb.public_ip]
type = "A"
ttl = "300"
zone_id = aws_route53_zone.primary.zone_id
```

**Answer: B**

Explanation:

HashiCorp style conventions suggest you that align the equals sign for consecutive arguments for easing readability for configurations

```
ami      = "abc123"
instance_type = "t2.micro"
```

### Question: 73

True or False:

The terraform refresh command is used to reconcile the state Terraform knows about (via its state file) with the real-world infrastructure. If the drift is detected between the real-world infrastructure and the last known-state, it will modify the infrastructure to correct the drift.

- A. False
- B. True

**Answer: A**

Explanation:

The terraform refresh command is used to reconcile the state Terraform knows about (via its state file) with the real-world infrastructure. This can be used to detect any drift from the last-known state, and to update the state file.

This does not modify infrastructure but does modify the state file. If the state is changed, this may cause changes to occur during the next plan or apply.

<https://www.terraform.io/docs/commands/refresh.html>

### Question: 74

Which of the following is an invalid variable name?

- A. instance\_name
- B. web
- C. var1
- D. count

**Answer: D**

Explanation:

count is a reserved word. The count parameter on resources can simplify configurations and let you scale resources by simply incrementing a number.

<https://www.terraform.io/intro/examples/count.html>

### Question: 75

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?

- A. terraform format
- B. terraform validate
- C. terraform fmt
- D. terraform show

**Answer: B**

Explanation:

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.

### Question: 76

Select all features which are exclusive to Terraform Enterprise. (select three)

- A. Audit Logs
- B. Cost Estimation
- C. Sentinel
- D. Clustering
- E. SAML/SSO

**Answer: A, D, E**

Explanation:

Sentinel and Cost Estimation are both available in Terraform Cloud, though not at the free tier level.

### Question: 77

In order to reduce the time it takes to provision resources, Terraform uses parallelism. By default, how many resources will Terraform provision concurrently?

- A. 20
- B. 50
- C. 5
- D. 10

**Answer: D**

Explanation:

Terraform can limit the number of concurrent operations as Terraform walks the graph using the `-parallelism=n` argument. The default value for this setting is 10. This setting might be helpful if you're running into API rate limits.

### Question: 78

When using constraint expressions to signify a version of a provider, which of the following are valid provider versions that satisfy the expression found in the following code snippet: (select two)

- ```
1. terraform {  
2.   required_providers {  
3.     aws = "~> 1.2.0"  
4.   }  
5. }
```

- A. 1.2.9
- B. 1.3.1
- C. 1.3.0
- D. 1.2.3

**Answer: A, D**

Explanation:

`~> 1.2.0` will match any non-beta version of the provider between `>= 1.2.0` and `< 1.3.0`. For example, 1.2.X

<https://www.terraform.io/docs/configuration/modules.html#gt-1-2-0-1>

### Question: 79

True or False? Each Terraform workspace uses its own state file to manage the infrastructure associated with that particular workspace.

- A. False
- B. True

**Answer: B**

Explanation:

The persistent data stored in the backend belongs to a workspace. Initially, the backend has only one workspace, called "default", and thus there is only one Terraform state associated with that configuration.

### Question: 80

While Terraform is generally written using the HashiCorp Configuration Language (HCL), what another syntax can Terraform be expressed in?

- A. JSON
- B. XML
- C. TypeScript
- D. YAML

**Answer: A**

Explanation:

The constructs in the Terraform language can also be expressed in JSON syntax, which is harder for humans to read and edit but easier to generate and parse programmatically.

### Question: 81

True or False?

terraform init cannot automatically download Community providers.

- A. False
- B. True

**Answer: B**

Explanation:

Anyone can develop and distribute their own Terraform providers. (See Writing Custom Providers for more about provider development.) These third-party providers must be manually installed, since terraform init cannot automatically download them.

<https://www.terraform.io/docs/configuration/providers.html#third-party-plugins>

### Question: 82

Which of the following statements best describes the Terraform list(...) type?

- A. a collection of unique values that do not have any secondary identifiers or ordering.
- B. a collection of values where each is identified by a string label.
- C. a sequence of values identified by consecutive whole numbers starting with zero.
- D. a collection of named attributes that each have their own type.

**Answer: C**

Explanation:

A terraform list is a sequence of values identified by consecutive whole numbers starting with zero.

<https://www.terraform.io/docs/configuration/types.html#structural-types>

### Question: 83

What is the result of the following terraform function call?

`lookup({a="hello", b="goodbye"}, "c", "what?")`

- A. goodbye
- B. hello
- C. what?
- D. c

**Answer: C**

Explanation:

lookup retrieves the value of a single element from a map, given its key. If the given key does not exist, the given default value is returned instead. In this case, the function call is searching for the key "c". But since there is no key "c", the default value "what?" is returned.

<https://www.terraform.io/docs/configuration/functions/lookup.html>

### Question: 84

Anyone can publish and share modules on the Terraform Public Module Registry, and meeting the requirements for publishing a module is extremely easy. Select from the following list all valid requirements. (select three)

- A. The registry uses tags to identify module versions. Release tag names must be for the format x.y.z, and can optionally be prefixed with a v.
- B. Module repositories must use this three-part name format, terraform-<PROVIDER>-<NAME>.
- C. The module must be PCI/HIPPA compliant.
- D. The module must be on GitHub and must be a public repo

**Answer: A, B, D**

Explanation:

---

The list below contains all the requirements for publishing a module. Meeting the requirements for publishing a module is extremely easy. The list may appear long only to ensure we're detailed, but adhering to the requirements should happen naturally.

GitHub. The module must be on GitHub and must be a public repo. This is only a requirement for the public registry. If you're using a private registry, you may ignore this requirement.

Named terraform-<PROVIDER>-<NAME>. Module repositories must use this three-part name format, where <NAME> reflects the type of infrastructure the module manages, and <PROVIDER> is the main provider where it creates that infrastructure. The <NAME> segment can contain additional hyphens. Examples: terraform-google-vault or terraform-aws-ec2-instance.

Repository description. The GitHub repository description is used to populate the short description of the module. This should be a simple one-sentence description of the module.

Standard module structure. The module must adhere to the standard module structure. This allows the registry to inspect your module and generate documentation, track resource usage, parse submodules and examples, and more.

x.y.z tags for releases. The registry uses tags to identify module versions. Release tag names must be a semantic version, which can optionally be prefixed with a v. For example, v1.0.4 and 0.9.2. To publish a module initially, at least one release tag must be present. Tags that don't look like version numbers are ignored.

<https://www.terraform.io/docs/registry/modules/publish.html#requirements>

## Question: 85

Environment variables can be used to set variables. The environment variables must be in the format "\_\_\_\_"<variablename>. Select the correct prefix string from the following list.

- A. TF\_VAR
- B. TF\_VAR\_NAME
- C. TF\_ENV
- D. TF\_ENV\_VAR

**Answer: A**

Explanation:

Environment variables can be used to set variables. The environment variables must be in the format TF\_VAR\_name and this will be checked last for a value. For example:

```
export TF_VAR_region=us-west-1
```

```
export TF_VAR_ami=ami-049d8641
```

```
export TF_VAR_alist='[1,2,3]'
```

```
export TF_VAR_amap='{ foo = "bar", baz = "qux" }'
```

<https://www.terraform.io/docs/commands/environment-variables.html>

## Question: 86

From the code below, identify the implicit dependency:

1. resource "aws\_eip" "public\_ip" {
2. vpc = true

```
3. instance = aws_instance.web_server.id
4. }
5. resource "aws_instance" "web_server" {
6.   ami      = "ami-2757f631"
7.   instance_type = "t2.micro"
8.   depends_on = [aws_s3_bucket.company_data]
9. }
```

- A. The EC2 instance labeled web\_server
- B. The EIP with an id of ami-2757f631
- C. The AMI used for the EC2 instance
- D. The S3 bucket labeled company\_data

**Answer: A**

Explanation:

The EC2 instance labeled web\_server is the implicit dependency as the aws\_eip cannot be created until the aws\_instance labeled web\_server has been provisioned and the id is available.

Note that aws\_s3\_bucket.example is an explicit dependency.

## Question: 87

Which statements best describes what the local variable assignment is doing in the following code snippet:

```
1. variable "subnet_details" {
2.   type = list(object({
3.     cidr = string
4.     subnet_name = string
5.     route_table_name = string
6.     aznum = number
7.   }))
8. }
9. locals {
10.   route_tables_all = distinct([for s in var.subnet_details : s.route_table_name ])
11. }
```

- A. Create a distinct list of route table name objects
- B. Create a map of route table names to subnet names
- C. Create a map of route table names from a list of subnet names
- D. Create a list of route table names eliminating duplicates

**Answer: D**

Explanation:

route\_tables\_all is assigned a list of unique route table names filtered from a list of objects describing subnet details, one of those object attributes being route\_table\_name.



## Question: 88

Which auth method is ideal for machine to machine authentication?

- A. GitHub
- B. UserPass
- C. AppRole
- D. Okta

**Answer: C**

Explanation:

The ideal method for a machine to machine authentication is AppRole although it's not the only method. The other options are frequently reserved for human access.

Reference link:- <https://www.hashicorp.com/blog/authenticating-applications-with-vault-approle/>

## Question: 89

When Vault is sealed, which are the only two options available to a Vault administrator? (select two)

- A. rotate the encryption key
- B. unseal Vault
- C. view the status of Vault
- D. configure policies
- E. author security policies
- F. view data stored in the key/value store

**Answer: B, C**

Explanation:

When Vault is sealed, the only two options available are, viewing the vault status and unsealing Vault. All the other actions performed after the Vault is unsealed and the user is authenticated.

## Question: 90

After creating a dynamic credential on a database, the DBA accidentally deletes the credentials on the database itself. When attempting to remove the lease, Vault returns an error stating that the credential cannot be found. What command can be run to coerce Vault to remove the secret?

- A. vault lease -renew
- B. vault lease revoke -force -prefix <lease\_path>
- C. vault revoke -apply
- D. vault lease revoke -enforce

---

**Answer: B**

Explanation:

The -force flag is meant for recovery when the secret in the target secrets engine was manually deleted.

### Question: 91

What type of token does not have a TTL (time to live)?

- A. default tokens
- B. parent tokens
- C. user tokens
- D. root tokens
- E. expired tokens
- F. child tokens

**Answer: D**

Explanation:

Non-root tokens are associated with a TTL, which determines how long a token is valid. Root tokens are not associated with a TTL, and therefore, do not expire.

Root tokens are tokens that have the root policy attached to them. They are the only type of token within Vault that are not associated with a TTL, and therefore, do not expire.

### Question: 92

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?

- A. request a new secret and associated lease
- B. try the expired secret in hopes it hasn't been deleted yet
- C. request the TTL be extended for the secret
- D. perform a lease renewal

**Answer: A**

Explanation:

A lease must be renewed before it has expired. Once it has expired, it is permanently revoked and a new secret must be requested.

### Question: 93

Vault has failed to start. You inspect the log and find the error below. What needs to be changed in order to successfully start Vault?

"Error parsing config.hcl: At 1:12: illegal char"

- A. the " character cannot be used in the config file
- B. fix the syntax error in the Vault configuration file
- C. you must use single quotes vs double quotes in the config file
- D. line 1 on the config file is blank

**Answer: B**

Explanation:

It implies that there is a syntax error in the configuration file. The exact location of the error in the file can be identified in the error message

### Question: 94

Which command is used to initialize Vault after first starting the Vault service?

- A. vault create key
- B. vault operator init
- C. vault operator initialize keys
- D. vault start
- E. vault operator unseal

**Answer: B**

Explanation:

The vault operator init command initializes a Vault server. Initialization is the process by which Vault's storage backend is prepared to receive data.

This only happens once when the server is started against a new backend that has never been used with Vault before.

Reference link is below:- <https://www.vaultproject.io/docs/commands/operator/init>

### Question: 95

What is the result of the following Vault command?

vault auth enable userpass

- A. Imports usernames and passwords from LDAP to the local database
- B. allows Vault to access usernames and passwords stored in a second Vault cluster
- C. Enables Vault to use external services to authenticate clients to Vault
- D. mounts the userpass auth method to the default path

**Answer: D**

Explanation:

---

The auth enable command enables an auth method at a given path. If an auth method already exists at the given path, an error is returned.

Command to enable auth method `vault auth <enable/disable>` followed by the name of the auth method.

Additional parameters can be included to specify the name of the mount.

### Question: 96

In order to extend Vault beyond a data center or cloud regional boundary, what feature should be used?

- A. plugins
- B. secrets engine
- C. replication
- D. seal/unseal
- E. snapshots

**Answer: C**

Explanation:

To extend Vault beyond a data center or cloud regional boundary, replication can be used. Vault supports both DR replication and Performance replication to copy data from the primary cluster to a secondary cluster safely.

### Question: 97

When creating a dynamic secret in Vault, Vault returns what value that can be used to renew or revoke the lease?

- A. lease\_id
- B. vault\_accessor
- C. revocation\_access
- D. token\_revocation\_id

**Answer: A**

Explanation:

When reading a dynamic secret, such as via `vault read`, Vault always returns a `lease_id`. This is the ID used with commands such as `vault lease renew` and `vault lease revoke` to manage the lease of the secret.

`vault lease lookup`

Usage: `vault lease <subcommand> [options] [args]`

This command groups subcommands for interacting with leases. Users can revoke or renew leases.

Renew a lease:

`$ vault lease renew database/creds/readonly/2f6a614c...`

Revoke a lease:

`$ vault lease revoke database/creds/readonly/2f6a614c...`

---

Subcommands:

renew   Renews the lease of a secret

revoke   Revokes leases and secrets

Reference link:- <https://www.vaultproject.io/docs/concepts/lease>

### Question: 98

Which is not a capability that can be used when writing a Vault policy?

- A. read
- B. list
- C. delete
- D. create
- E. modify
- F. update

**Answer: E**

Explanation:

When writing a Vault policy, permissions which can be applied to paths include create, read, update, delete, list, deny, and sudo.

<https://www.vaultproject.io/docs/concepts/policies>

Modify is not one of them.

### Question: 99

Which is not a benefit of running HashiCorp Vault in your environment?

- A. Integrate with your code repository to pull secrets when deploying your applications
- B. Consolidate static, long-lived passwords used throughout your organization
- C. Act as root or intermediate certificate authority to automate the generation of PKI certificates
- D. The ability to generate dynamic secrets for applications and resource access

**Answer: A**

Explanation:

Vault does not integrate with any VCS (Version Control System) to checkout or read code. However, It can use GitHub as an auth method.

### Question: 100

Which of the following settings are configured using the configuration file? (select three)

- A. Cluster Name
- B. Replication

- C. Seal Type
- D. Auth Methods
- E. Namespaces
- F. Storage Backend
- G. Audit Devices

**Answer: A, C, F**

Explanation:

Seal types, Storage backends, and cluster names are just a few of the configurations done via the configuration file. The others are configured within Vault itself.

### Question: 101

Vault's User Interface (UI) needs to be enabled in the command line before it can be used.

- A. FALSE
- B. TRUE

**Answer: A**

Explanation:

The UI is enabled in the Vault configuration file, not in the CLI.

### Question: 102

Which of the following unseal options can automatically unseal Vault upon the start of the Vault service? (select four)

- A. Transit
- B. HSM
- C. AWS KMS
- D. Key Shards
- E. Azure KMS

**Answer: A, B, C, E**

Explanation:

When a Vault server is started, it starts in a sealed state and it does not know how to decrypt data. Before any operation can be performed on the Vault, it must be unsealed. Unsealing is the process of constructing the master key necessary to decrypt the data encryption key.

Below are links covering details of each option:- <https://www.vaultproject.io/docs/concepts/seal>

AWS KMS

<https://learn.hashicorp.com/vault/operations/ops-autounseal-aws-kms>

Auto-unseal using Transit Secrets Engine

---

<https://learn.hashicorp.com/vault/operations/autounseal-transit>

Auto-unseal using Azure Key Vault

<https://learn.hashicorp.com/vault/day-one/autounseal-azure-keyvault>

Auto-unseal using HSM

<https://learn.hashicorp.com/vault/operations/ops-seal-wrap>

Key shards don't support auto unseal instead key shards require the user to provide unseal keys to reconstruct the master key

<https://www.vaultproject.io/docs/concepts/seal>

### Question: 103

Which TCP port does Vault use, by default, for its API and UI?

- A. 8600
- B. 8201
- C. 8500
- D. 8301
- E. 8300
- F. 8200

**Answer: F**

Explanation:

By default, Vault uses port 8200 for its API and UI.

8201 is used for the cluster to cluster communication,

8300 is used for Consul Server RPC,

8500 is used for the Consul interface,

8600 is used for Consul DNS,

and 8301 is used for its LAN gossip protocol.

### Question: 104

The userpass auth method has the ability to access external services in order to provide authentication to Vault.

- A. FALSE
- B. TRUE

**Answer: A**

Explanation:

The userpass auth method uses a local database that cannot interact with any services outside of the Vault instance.

### Question: 105

---

What is the default method of authentication after first initializing Vault?

- A. GitHub
- B. AppRole
- C. Admin account
- D. Tokens
- E. Userpass
- F. TLS certificates

**Answer: D**

Explanation:

After initializing, Vault provides the root token to the user, this is the only way to log in to Vault to configure additional auth methods.

### Question: 106

Which of the following best describes the storage backend?

- A. configures client interaction with a cloud storage service, such as Amazon S3
- B. configures the location for storage of Vault data
- C. selects the type of storage the Vault node runs on, such as SSD or traditional spinning hard drive
- D. Encrypts the hard drives of the server which Vault is running on

**Answer: B**

Explanation:

The storage stanza configures the storage backend, which represents the location for the durable storage of Vault's information.

Storage backend configuration is done through the Vault configuration file using the storage stanza.

Reference link:- <https://www.vaultproject.io/docs/configuration/storage>

### Question: 107

Which of the following secrets engine can generate dynamic credentials? (select three)

- A. Azure
- B. database
- C. key/value
- D. Transit
- E. AWS

**Answer: A, B, E**



---

Explanation:

Vault has many secrets engines that can generate dynamic credentials, including AWS, Azure, and database secrets engines. The key/value secret engine is used to store data, and the transit secret engine is used to encrypt data.

### Question: 108

After a client has authenticated, what security feature is used to make subsequent calls?

- A. key shard
- B. ldap
- C. pgp
- D. token
- E. listener
- F. path

**Answer: D**

Explanation:

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.

### Question: 109

Select the two default policies created in Vault. (select two)

- A. default
- B. vault
- C. base
- D. root
- E. admin
- F. user

**Answer: A, D**

Explanation:

Vault creates two default policies; root, and default.

The root policy cannot be deleted or modified.

The default policy is attached to all tokens, by default, however, this action can be modified if needed.

### Question: 110

Which three interfaces can be used to access Vault? (select three)

- A. JSON

- B. CLI
- C. RPC
- D. UI
- E. API
- F. Consul

**Answer: B, D, E**

Explanation:

Vault has three interfaces available.

The API can be used by a user or application, the CLI can be used by a user directly on the Vault server or remotely, and the UI can be used if it's been enabled in the configuration file.

### Question: 111

Vault secrets engines are used to do what with data? (select three)

- A. copy
- B. generate
- C. store
- D. transmit
- E. encrypt

**Answer: B, C, E**

Explanation:

Vault secrets engines are used to store, generate, or encrypt data.

The KV secrets engine can store data, AWS can generate credentials, and the transit secret engine can encrypt data.

### Question: 112

Which commands are available only after Vault has been unsealed? (select two)

- A. vault login -method=ldap -username=vault
- B. vault operator unseal
- C. vault kv get kv/apps/app01
- D. vault status

**Answer: A, C**

Explanation:

Once Vault is unsealed, you can run vault login -method=ldap -username=vault and vault kv get kv/apps/app01. The second command assumes that you have authenticated but it cannot be run unless

---

Vault is unsealed. vault status can be run regardless of Vault is sealed or unsealed, and vault operator unseal can only be run when the vault is sealed.

### Question: 113

Which of the following storage backends are supported by HashiCorp technical support? (select four)

- A. Filesystem
- B. Consul
- C. In-Memory
- D. Raft
- E. DynamoDB
- F. MySQL

**Answer: A, B, C, D**

Explanation:

Just to clarify, "HashiCorp supported" means, it is supported by HashiCorp's technical support, it doesn't mean that Vault supports the platform as a storage backend.

For example, DynamoDB is a valid storage backend, but it is not officially supported by HashiCorp technical support but it has got the community support.

In-Memory - HashiCorp Supported

MySQL - Community Supported

Raft - HashiCorp Supported

Dynamo DB - Community Supported

Consul - HashiCorp Supported

Filesystem - HashiCorp Supported

Check more details on below link:- <https://www.vaultproject.io/docs/configuration/storage/in-memory>

### Question: 114

Which of the following commands will remove all secrets at a specific path?

- A. vault lease revoke -prefix <path>
- B. vault delete lease -all <path>
- C. vault lease revoke -all <path>
- D. vault revoke -all <path>

**Answer: A**

Explanation:

The -prefix flag treats the ID as a prefix instead of an exact lease ID. This can revoke multiple leases simultaneously.

### Question: 115

---

Which of the following best describes a token accessor?

- A. a value that acts as a reference to a token which can be used to perform limited actions against the token
- B. a token used for Consul to access Vault auth methods
- C. describes the value associated with the tokens TTL
- D. a value that describes which clients have access to the attached token

**Answer: A**

Explanation:

When tokens are created, a token accessor is also created and returned. This accessor is a value that acts as a reference to a token and can only be used to perform limited actions:

- Lookup a token's properties (not including the actual token ID)
- Lookup a token's capabilities on a path
- Renew the token
- Revoke the token

Reference link:- <https://www.vaultproject.io/docs/concepts/tokens#token-accessors>

### Question: 116

What command is used to renew a token, if permitted?

- A. vault operator token renew
- B. vault token update
- C. vault new <token-id>
- D. vault update token
- E. vault token renew
- F. vault renew token <token-id>

**Answer: E**

Explanation:

In order to renew a token, a user can issue a vault token renew command to extend the TTL. The token can also be renewed using the API

### Question: 117

Unsealing Vault creates the encryption keys, which is used to unencrypt the data on the storage backend.

- A. FALSE
- B. TRUE

---

**Answer: A**

Explanation:

Unsealing is the process of obtaining the plaintext master key necessary to read the decryption key to decrypt the data, allowing access to the Vault. The master key is used to decrypt the encryption key which can unencrypt the data on the storage backend.

### Question: 118

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

**Answer: A**

Explanation:

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>

### Question: 119

Vault configuration files can be written in what languages? (select two)

- A. XML
- B. JSON
- C. YAML
- D. HCL

**Answer: B, D**

Explanation:

---

The Vault configuration file supports either JSON or HCL, which is HashiCorp Configuration Language

### Question: 120

What happens to child tokens when a parent token is revoked?

- A. the child tokens are renewed
- B. the child tokens are converted to parent tokens
- C. the child tokens create their own child tokens to be used
- D. the child tokens are revoked

**Answer: D**

Explanation:

When a parent token is revoked, all of its child tokens and leases are revoked as well. This ensures that a user cannot skip revocation by simply making a timeless tree of child tokens.

### Question: 121

A Vault client who has read access to the path secrets/apps/app1 is having trouble viewing the secret in the user interface (UI) but can access via the API. What can be done to resolve this issue?

- A. add read permissions to the path secrets/apps
- B. modify the policy to allow the create permission
- C. remove the deny policy blocking access to the secrets/apps/app1 path
- D. add LIST to the policy so the user can browse the paths leading up to the key/value's path

**Answer: D**

Explanation:

To view the paths leading up to the secrets/apps/app1 path in the user interface, the user must have at least LIST permissions to avoid permission denied error in the UI.

### Question: 122

Using the Vault CLI, what command is used to authenticate to Vault?

- A. vault creds
- B. vault user
- C. vault login
- D. vault auth

**Answer: C**

Explanation:

---

vault login command would be issued to log in to Vault via CLI followed by the type of login.  
For example, an LDAP login would use vault login method=ldap username=<user>

### Question: 123

Which two characters can be used when writing a policy to reflect a wildcard or path segment? (select two)

- A. @
- B. \$
- C. &
- D. \*
- E. +

**Answer: D, E**

Explanation:

The splat (\*) can be used as a wildcard but can only be used at the very end of a path.

The plus sign (+) can be used in the middle of a path to denote a path segment.

### Question: 124

Which of the following cloud providers are not supported by Vault secrets engines?

- A. Oracle
- B. Azure
- C. AWS
- D. GCP
- E. AliCloud

**Answer: A**

Explanation:

Vault supports AWS, Azure, Google Cloud, and Alibaba Cloud out of the box for secrets engines

### Question: 125

Vault policies are deny by default

- A. TRUE
- B. FALSE

**Answer: A**

Explanation:

---

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.

### Question: 126

In order to extend a Consul storage backend, Consul nodes should be provisioned across multiple data centers or cloud regions.

- A. True
- B. False

**Answer: B**

Explanation:

Consul nodes in the same cluster should not be provisioned across multiple data centers or cloud regions due to the low-latency requirements.

### Question: 127

Which two interfaces automatically assume the token for subsequent requests after successfully authenticating? (select two)

- A. UI
- B. API
- C. CLI
- D. Consul

**Answer: A, C**

Explanation:

After authenticating, the UI and CLI automatically assume the token for all subsequent requests. The API, however, requires the user to extract the token from the server response after authenticating in order to send with subsequent requests.

### Question: 128

Vault does not trust the storage backend.

- A. False
- B. True

**Answer: B**

Explanation:



---

Storage backends are not trusted by Vault and are only expected to render durability. The storage backend is configured when starting the Vault server.

Reference link:- <https://www.vaultproject.io/docs/internals/architecture>

### Question: 129

As opposed to service tokens, batch tokens are ideal for what type of action?

- A. generating dynamic credentials
- B. configuring Vault features
- C. renewing tokens
- D. issuing snapshots
- E. encrypting data
- F. writing secrets

**Answer: E**

Explanation:

Batch tokens are generally used for encrypting data because they are lightweight and scalable and also include enough information to use with Vault.

### Question: 130

When a primary Vault cluster fails, Vault will automatically promote a secondary cluster to ensure maximum uptime.

- A. False
- B. True

**Answer: A**

Explanation:

Vault secondary clusters must be manually promoted to a primary.

### Question: 131

The Vault Agent provides which of the following benefits? (select three)

- A. client-side caching of responses
- B. automatically creates secrets in the desired storage backend
- C. authentication to Vault
- D. token renewal

**Answer: A, C, D**

---

Explanation:

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

- Auto-Auth
- Caching
- Templating

Reference link:- <https://www.vaultproject.io/docs/agent>

### Question: 132

The command `vault lease revoke -prefix aws/` will revoke all leases associated with the secret engine mounted at `aws/`

- A. False
- B. True

**Answer: B**

Explanation:

The lease command groups subcommands for interacting with leases attached to secrets.

Subcommands:

`renew` Renews the lease of a secret

`revoke` Revokes leases and secrets

Using the `'-prefix'` flag allows you to revoke the entire tree of secrets.

### Question: 133

A user has logged into the Vault user interface but cannot browse to a secret located at `kv/applications/app3`, however, the policy the user is bound by permits read permission to the secret. Because of the read permission, the user should be able to read the secret in the Vault UI.

- A. False
- B. True

**Answer: A**

Explanation:

To browse Vault paths in the UI, the user must have list permissions on the mount and the paths leading up to the secret.

### Question: 134

To prepare for day-to-day operations, the root token should be safely saved outside of Vault in order to administer Vault

- A. False

B. True

**Answer: A**

Explanation:

It is generally considered a best practice to not persist root tokens. Instead, a root token should be generated using Vault's operator generate-root command only when absolutely necessary.

For day-to-day operations, the root token should be deleted after configuring other auth methods which will be used by admins and Vault clients.

### Question: 135

The security barrier protects all of the following Vault components except \_\_\_\_.

- A. secret engine
- B. auth method
- C. storage backend
- D. audit devices
- E. token store

**Answer: C**

Explanation:

storage backend and HTTP API are outside of the security barrier hence can't be protected.

### Question: 136

Which of the following Vault features is available only in the Enterprise version? (select three)

- A. MFA
- B. dynamic credentials
- C. cloud auto unseal
- D. replication
- E. auto unseal with HSM

**Answer: A, D, E**

Explanation:

Most of the important features of Vault are available in the open-source version, however, some of the features which are generally required by large organizations are only available in the Enterprise version such as:-

- MFA - Multi-factor Authentication
  - Replication
  - Auto unseal with HSM and many more.
- Check all the features at the below link.

Reference link:- <https://www.hashicorp.com/products/vault/pricing/>

## Question: 137

Permissions for Vault backend functions are available at which path?

- A. security/
- B. admin/
- C. backend/
- D. system/
- E. vault/
- F. sys/

**Answer: F**

Explanation:

All backend system functions stored in the sys/ backend.

The system backend is a default backend in Vault that is mounted at the /sys endpoint. This endpoint cannot be disabled or moved, and is used to configure Vault and interact with many of Vault's internal features.

## Question: 138

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.<<mount accessor>>.id}}/\*" {  
capabilities = [ "create", "update", "read", "delete", "list" ]  
}
- D.  
path "user-kv/data/{{user}}/\*" {  
capabilities = [ "create", "update", "read", "delete", "list" ]  
}

**Answer: A**

---

Explanation:

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/*`

### Question: 139

While Vault provides businesses tons of functionality out of the box, what feature allows you to extend its functionality with solutions written by third-party providers?

- A. vault agent
- B. namespaces
- C. plugin backend
- D. control groups

**Answer: C**

Explanation:

Plugin backends are the components in Vault that can be implemented separately from Vault's built-in backends. These backends can be either authentication or secrets engines. All Vault auth and secret backends are considered plugins. This simple concept allows both built-in and external plugins to be treated like Legos. Any plugin can exist at multiple different locations. Different versions of a plugin may be at each one, with each version differing from Vault's version.

Reference links:-

<https://www.vaultproject.io/docs/plugin>

<https://www.vaultproject.io/docs/internals/plugins>

### Question: 140

After issuing the command to delete a secret, you run a `vault kv list` command but the secret still exists. What command would permanently delete this secret from Vault?

1. `$ vault kv delete kv/applications/app01`
2. Success! Data deleted (if it existed) at: `kv/applications/app01`
3. `$ vault kv list kv/applications`
4. Keys
5. ----
6. `app01`

- A. `vault kv metadata delete kv/applications/app01`
- B. `vault kv delete -all kv/applications/app01`

- C. vault kv delete -force kv/applications/app01  
D. vault kv destroy -versions=1 kv/applications/app01

**Answer: A**

Explanation:

The kv metadata command has subcommands for interacting with the metadata and versions for the versioned secrets (K/V Version 2 secrets engine) at the specified path.

The kv metadata delete command deletes all versions and metadata for the provided key.

Reference link:- <https://www.vaultproject.io/docs/commands/kv/metadata>

### Question: 141

When architecting a Vault replication configuration, why should you never terminate TLS on a front-end load balancer?

- A. If Vault detects that the traffic has been unencrypted and re-encrypted, due to the load balancer, it will automatically drop the traffic as it is no longer trusted.  
B. Vault generates self-signed mutual TLS for replication. If the LB is performing TLS termination, this will break the mutual TLS between nodes.  
C. Vault requires that only Consul service discovery can be used to direct traffic to an active Vault node.  
D. Vault replication won't work with the type of certificates that a traditional load balancer uses.

**Answer: B**

Explanation:

For replication (port 8201), Vault generates a mutual TLS connection between nodes using self-generated certs/keys (this is different than the TLS you configure in the listener, which is particular to client requests)... server-to-server always uses this mutual TLS, even if you have TLS disabled on the listener.

Reference link:-

<https://www.vaultproject.io/docs/configuration/listener/tcp>

<https://www.vaultproject.io/docs/concepts/ha>

### Question: 142

True or False:

Once you create a KV v1 secrets engine and place data in it, there is no way to modify the mount to include the features of a KV v2 secrets engine.

- A. True  
B. False

**Answer: B**

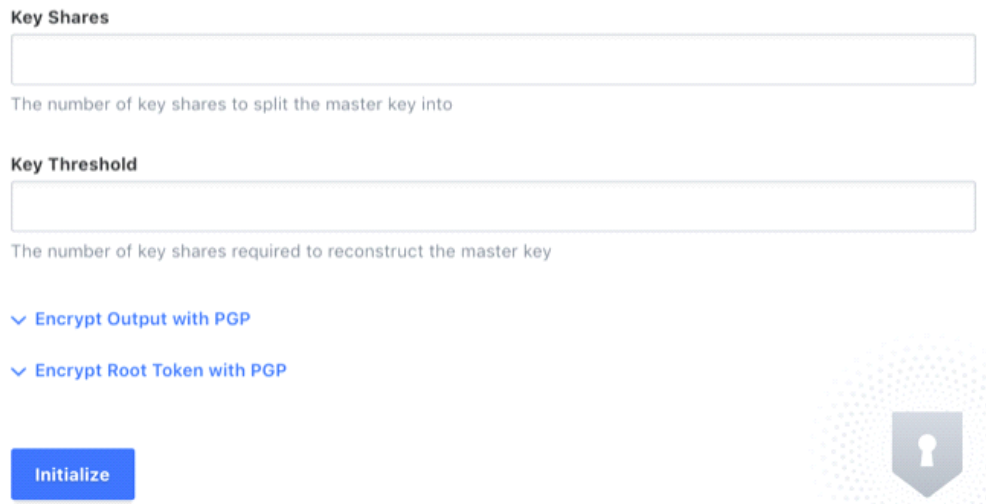
Explanation:

The kv enable-versioning command turns on versioning for an existing non-versioned key/value secrets engine (K/V Version 1) at its path.

Reference link:- <https://www.vaultproject.io/docs/commands/kv/enable-versioning>

## Question: 143

You've hit the URL for the Vault UI, but you're presented with this screen. Why doesn't Vault present you with a way to log in?



- A. a vault policy is preventing you from logging in
- B. the vault configuration file has an incorrect configuration
- C. the consul storage backend was not configured correctly
- D. vault needs to be initialized before it can be used

**Answer: D**

Explanation:

Before Vault can be used, it must be initialized and unsealed. This screen indicates that Vault has not been initialized yet and is offering you a way to do so.

## Question: 144

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

---

**Answer: C**

Explanation:

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: 145

Which of the following policies would permit a user to generate dynamic credentials on a database?

- A.  

```
path "database/creds/read_only_role" {  
  capabilities = ["read"]  
}
```
- B.  

```
path "database/creds/read_only_role" {  
  capabilities = ["generate"]  
}
```
- C.  

```
path "database/creds/read_only_role" {  
  capabilities = ["list"]  
}
```
- D.  

```
path "database/creds/read_only_role" {  
  capabilities = ["sudo"]  
}
```

**Answer: A**

Explanation:

The HTTP request is a GET which corresponds to a read capability. Thus, to grant access to generate database credentials, the policy would grant read access on the appropriate path.

### Question: 146

When registering a plugin with Vault, where would you configure the location where the binaries are located in order for Vault to properly register the plugin?

- A. in the Vault configuration file using `plugin_directory=<path>`
- B. in the UI underneath the plugin tab
- C. in the plugin configuration file using `directory=<path>`
- D. within the CLI command when registering a plug



---

**Answer: A**

Explanation:

The plugin directory is a configuration option of Vault, and can be specified in the configuration file. This setting specifies a directory in which all plugin binaries must live; this value cannot be a symbolic link. A plugin can not be added to Vault unless it exists in the plugin directory. There is no default for this configuration option, and if it is not set plugins can not be added to Vault.

Reference link:- <https://www.vaultproject.io/docs/internals/plugins>

### Question: 147

What is the Consul Agent?

- A. a process that registers services with Consul
- B. an agent that runs in the background to provide additional features for Consul
- C. the core process of Consul which maintains membership information, manages services, runs checks, responds to queries, and more.
- D. a daemon that Vault uses to register auth methods across all of its clusters to ensure consistency among the data written to disk

**Answer: C**

Explanation:

The Consul agent is the core Consul process that runs the Consul service. Everything Consul does is the result of the Consul agent, which can run in either server or client mode.

Reference link:- <https://www.consul.io/docs/agent>

### Question: 148

How can Vault be used to programmatically obtain a generated code for MFA, somewhat similar to Google Authenticator?

- A. cubbyhole
- B. the identity secrets engine
- C. TOTP secrets engine
- D. the random byte generator

**Answer: C**

Explanation:

The TOTP secrets engine generates time-based credentials according to the TOTP standard. The secrets engine can also be used to generate a new key and validate passwords generated by that key.

The TOTP secrets engine can act as both a generator (like Google Authenticator) and a provider (like the Google.com sign-in service).

As a Generator

---

The TOTP secrets engine can act as a TOTP code generator. In this mode, it can replace traditional TOTP generators like Google Authenticator. It provides an added layer of security since the ability to generate codes is guarded by policies and the entire process is audited.

Reference link:- <https://www.vaultproject.io/docs/secrets/totp>

### Question: 149

From the unseal options listed below, select the options you can use if you're deploying Vault on-premises. (select four)

- A. transit
- B. AWS KMS
- C. certificates
- D. key shards
- E. HSM PKCS11

**Answer: A, B, D, E**

Explanation:

Certificates are not a valid unseal option for HashiCorp Vault.

### Question: 150

In regards to the transit secrets engine, which of the following is true given the following command and output: (select three)

1. \$ vault write encryption/encrypt/creditcard plaintext=\$(base64 <<< "1234 5678 9101 1121")
2. Key Value
3. --- -----
4. ciphertext vault:v3:cZNHVx+sxdMErXRSuDa1q/pz49fXTn1PScKfhf+PIZPvy8xKfkytpwKcbC0ff2U=

- A. there are at least three data keys associated with this keyring
- B. the name of the keyring used to encrypt the data is creditcard
- C. the data was written to the encryption path, which is provided by default when enabling the transit secrets engine
- D. the transit secrets engine is mounted at the encryption path

**Answer: A, B, D**

Explanation:

The encryption key used to encrypt the plaintext is regarded as a data key. This data key needs to be protected so that your encrypted data cannot be decrypted comfortably by an unauthorized party. In this case, data has been encrypted by specifying the keyring name creditcard.

### Question: 151

---

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

- A. the original encryption key has been rotated at least once
- B. this is the second version of the encrypted data
- C. similar to the KV secrets engine, the transit secrets engine was enabled using the transit v2 option
- D. the data is stored in Vault using a KV v2 secrets engine

**Answer: A**

Explanation:

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>

### Question: 152

By default, the max TTL for a token is how many days?

- A. 14 days
- B. 32 days
- C. 31 days
- D. 7 days

**Answer: B**

Explanation:

The system max TTL, which is 32 days but can be changed in Vault's configuration file.

The max TTL set on a mount using mount tuning. This value is allowed to override the system max TTL -- it can be longer or shorter, and if set this value will be respected.

A value suggested by the auth method that issued the token. This might be configured on a per-role, per-group, or per-user basis. This value is allowed to be less than the mount max TTL (or, if not set, the system max TTL), but it is not allowed to be longer.

Reference link:- <https://www.vaultproject.io/docs/concepts/tokens>

### Question: 153

What could you do with the feature found in the screenshot below? (select two)

Secrets Access Policies Tools

TOOLS

- Wrap
- Lookup
- Unwrap
- Rewrap
- Random
- Hash

### Wrap data

Data to wrap (json-formatted)

```
1 {  
2 }
```

Wrap TTL

30 seconds

Wrap data

- A. encrypt the Vault master key that is stored in memory
- B. using a short TTL, you could encrypt data in order to place only the encrypted data in Vault
- C. encrypt sensitive data to send to a colleague over email
- D. use response-wrapping to protect data

**Answer: C, D**

Explanation:

Vault includes a feature called response wrapping. When requested, Vault can take the response it would have sent to an HTTP client and instead insert it into the cubbyhole of a single-use token, returning that single-use token instead.

## Question: 154

You've logged into the Vault CLI and attempted to enable an auth method, but received this error message. What can be done to resolve the error and configure Vault?

Error enabling userpass auth: Post https://127.0.0.1:8200/v1/sys/auth/userpass: http: server gave HTTP response to HTTPS client

- A. change 'userpass' to 'username and password'
- B. restart the Vault service on this node
- C. set the VAULT\_ADDR environment variable to HTTP
- D. ask an admin to grant you permission to enable the userpass auth method

**Answer: C**

Explanation:

If you're running Vault in a non-prod environment, you can configure Vault to disable TLS.

In this case, TLS has been disabled but the default value for VAULT\_ADDR is https://127.0.0.1:8200, therefore Vault is sending the request over HTTPS but Vault is responding using HTTP since TLS is disabled.

To handle this error, set the VAULT\_ADDR environment variable to "<http://127.0.0.1:8200>".

### Question: 155

After decrypting data using the transit secrets engine, the plaintext output does not match the plaintext credit card number that you encrypted. Which of the following answers provides a solution?

1. `$ vault write transit/decrypt/creditcard\ ciphertxt="vault:v1:cZNHVx+sxdMErXRSuDa1q/pz49fXTn1PScKfhf+PIZPvy8xKfkytpwKcbC0fF2U=" \`
- 2.
3. Key      Value
4. ---      -----
5. plaintext Y3IJZGI0LWNhcmQtbmVtYmVyCg==

- A. The resulting plaintext data is base64-encoded. To reveal the original plaintext, use the `base64 --decode` command.
- B. The data is corrupted. Execute the encryption command again using a different data key
- C. the user doesn't have permission to decrypt the data, therefore Vault returns false data so as not to reveal if the data was actually encrypted by Vault
- D. Vault is sealed, therefore the data cannot be decrypted. Unseal Vault to properly decrypt the data

**Answer: A**

Explanation:

All plaintext data must be base64-encoded. The reason for this requirement is that Vault does not require that the plaintext is "text". It could be a binary file such as a PDF or image. The easiest safe transport mechanism for this data as part of a JSON payload is to base64-encode it.

Reference link:- <https://learn.hashicorp.com/vault/encryption-as-a-service/eaas-transit>

### Question: 156

After enabling the vault to autocomplete feature, you type `vault` and press the tab button, but nothing happens. Why doesn't vault display the available completions?

1. `$ vault -autocomplete-install`
  2. `$ vault`
- A. your SSH client doesn't support autocompletion
- B. the SSH session needs to be restarted upon installation
- C. you don't have the permissions to use autocomplete
- D. you didn't use `-force` when enabling the feature

**Answer: B**

Explanation:

---

Be sure to restart your shell after installing autocompletion!

### Question: 157

What feature of Vault would allow you to architect a "Vault within a Vault"?

- A. sentinel
- B. secrets engines
- C. control groups
- D. namespaces

**Answer: D**

Explanation:

Namespaces are isolated environments that functionally exist as "Vaults within a Vault." They have separate login paths and support creating and managing data isolated to their namespace. This data includes the following:

- Secret Engines
- Auth Methods
- Policies
- Identities (Entities, Groups)
- Tokens

Reference link:- <https://www.vaultproject.io/docs/enterprise/namespaces>

### Question: 158

What system endpoint can you query to determine which node is the leader of a cluster?

- A. /sys/tools
- B. /sys/leader
- C. /sys/health
- D. /sys/init

**Answer: B**

Explanation:

The /sys/leader endpoint is used to check the current leader of Vault as well as high availability status.

### Question: 159

An application requires a specific key/value to be updated in order to process a batch job. The value should be either "true" or "false". However, when developers have been updating the value, sometimes they mistype the value or capitalize on the value, causing the batch job not to run. What feature of a Vault policy can be used in order to restrict the entry to the required values?

- A. added an allowed\_parameters value to the policy
- B. use a \* wildcard at the end of the policy
- C. change the policy to include the list capability
- D. add a deny statement for all possible misspellings of the value

**Answer: A**

Explanation:

allowed\_parameters - Whitelists a list of keys and values that are permitted on the given path.

Setting a parameter with a value of the empty list allows the parameter to contain any value.

Reference link:- <https://www.vaultproject.io/docs/concepts/policies>

## Question: 160

Your organization is running Vault open source and has decided it wants to use the Identity secrets engine. You log into Vault but are unable to find it in the list to enable. What gives?

### Enable a Secrets Engine

The screenshot shows the 'Enable a Secrets Engine' interface in Vault. It is divided into three sections: Generic, Cloud, and Infra. Each section contains a grid of engine options, each with an icon, a name, and a radio button for selection.

- Generic:** KV, PKI Certificates, SSH, Transit, TOTP.
- Cloud:** Active Directory, AliCloud, AWS, Azure, Google Cloud, Google Cloud KMS.
- Infra:** Consul, Databases, Nomad, RabbitMQ.

A 'Next' button is located at the bottom left of the interface.

- A. because you are running open-source and the identity secrets engine is an Enterprise feature, it is not available to enable.
- B. the identity secrets engine was deprecated in previous versions
- C. this secrets engine will be mounted by default.
- D. the policy attached to your user doesn't allow access to the Identity secrets engine.

---

**Answer: C**

Explanation:

The Identity secrets engine is the identity management solution for Vault. It internally maintains the clients who are recognized by Vault. This secrets engine will be mounted by default. This secrets engine cannot be disabled or moved.

Reference link:- <https://www.vaultproject.io/docs/secrets/identity>

### Question: 161

What are the primary benefits of running Vault in a production deployment over dev server mode? (select two)

- A. ability to enable auth methods
- B. persistent storage
- C. encryption via TLS
- D. faster deployment
- E. access to all of the secret engines

**Answer: B, C**

Explanation:

Dev server mode stores its data in memory, therefore if the Vault service is shut down, any data stored will be lost. Additionally, dev server mode does not use TLS, and all data is sent in cleartext.

### Question: 162

You've deployed Vault in your production environment and are curious to understand metrics on your Vault cluster, such as the number of writes to the backend, the status of WALs, and the seal status. What feature would you configure in order to view these metrics?

- A. audit device
- B. telemetry
- C. nothing to configure, these are available in the Vault log found on the OS
- D. enable logs for each individual secrets engines

**Answer: B**

Explanation:

The Vault server process collects various runtime metrics about the performance of different libraries and subsystems. These metrics are aggregated on a ten-second interval and are retained for one minute. This telemetry information can be used for debugging or otherwise getting a better view of what Vault is doing.

Telemetry information can be streamed directly from Vault to a range of metrics aggregation solutions as described in the telemetry Stanza documentation.



Reference link:- <https://www.vaultproject.io/docs/internals/telemetry>

## Question: 163

You want to encrypt a credit card number using the transit secrets engine. You enter the following command and receive an error. What can you do to ensure that the credit card number is properly encrypted and the ciphertext is returned?

1. `$ vault write -format=json transit/encrypt/creditcards plaintext="1234 5678 9101 1121"`
2. Error writing data to transit/encrypt/orders: Error making API request.
- 3.
4. URL: PUT <http://10.25.16.165:8200/v1/transit/encrypt/creditcards>
5. Code: 400. Errors:
- 6.
7. \* illegal base64 data at input byte 4

- A. credit card numbers are not supported using the transit secrets engine since it is considered sensitive data
- B. the token used to issue the encryption request does not have the appropriate permissions
- C. the plain text data needs to be encoded to base64
- D. the credit card number should not include spaces

**Answer: C**

Explanation:

When you send data to Vault for encryption, it must be in the form of base64-encoded plaintext for safe transport.

## Question: 164

What does the following API request return?

1. `$ curl \`
2. `--header "X-Vault-Token: ..." \`
3. `--request POST \`
4. `--data @payload.json \`
5. <http://127.0.0.1:8200/v1/sys/tools/random/164>

- A. a random string of 164 characters
- B. a random token valid for 164 uses
- C. None
- D. a secured secret based on 164 bytes of data

**Answer: A**

Explanation:

This endpoint returns high-quality random bytes of the specified length.

---

### Question: 165

Which of the following is not an activity associated with the Vault transit secrets engine?

- A. encrypt
- B. decrypt
- C. update
- D. rewrap

**Answer: C**

Explanation:

Since Vault does not store any data, hence Vault transit secrets engine does not support update activity.

### Question: 166

Which TCP port does Vault replication use?

- A. 8200
- B. 8201
- C. 8300
- D. 8301

**Answer: B**

Explanation:

Check below link for details:- <https://learn.hashicorp.com/vault/operations/ops-reference-architecture>

### Question: 167

In a Consul cluster, participating nodes can be only one of two types. Select the valid types. (select two)

- A. follower
- B. secondary
- C. active
- D. primary
- E. leader
- F. passive

**Answer: A, E**

Explanation:

Within each datacenter, we have a mixture of clients and servers. It is expected that there be between three to five servers. This strikes a balance between availability in the case of failure and performance,

---

as consensus gets progressively slower as more machines are added. However, there is no limit to the number of clients, and they can easily scale into the thousands or tens of thousands.

Server or Leader - It indicates whether the agent is running in server or client mode. Server nodes participate in the consensus quorum, storing cluster state, and handling queries. At any given time, the peer set elects a single node to be the leader. The leader is responsible for ingesting new log entries, replicating to followers, and managing when an entry is considered committed.

Client or Follower - Client nodes make up the majority of the cluster, and they are very lightweight as they interface with the server nodes for most operations and maintain a very little state of their own.

Reference link:- <https://www.consul.io/docs/internals/architecture.html>

### Question: 168

After logging into the Vault UI, a user complains that they cannot enable Replication. Why would the replication configuration be missing?

- A. replication wasn't configured in the Vault configuration file
- B. replication hasn't been enabled
- C. Vault is running an open-source version
- D. replication configuration isn't available in the UI

**Answer: C**

Explanation:

Replication is not available in open-source versions of Vault. It is an enterprise feature.

### Question: 169

When configuring Vault replication and monitoring its status, you keep seeing something called 'WALs'. What are WALs?

- A. wake after lan
- B. warning of allocated logs
- C. write-ahead log
- D. write along logging

**Answer: C**

Explanation:

Reference links:-

<https://learn.hashicorp.com/vault/day-one/monitor-replication>

<https://www.vaultproject.io/docs/internals/replication>

### Question: 170

---

You've set up multiple Vault clusters, one on-premises which is intended to be the primary cluster, and the second cluster in AWS, which was deployed to be used for performance replication. After enabling replication, developers complain that all the data they've stored in the AWS Vault cluster is missing. What happened?

- A. the data was moved to a recovery path after replication was enabled. Use the vault secrets move command to move the data back to its intended location
- B. there is a certificate mismatch after replication was enabled since Vault replication generates its own TLS certificates to ensure nodes are trusted entities
- C. the data was automatically copied to the primary cluster after replication was enabled since all writes are always forwarded to the primary cluster
- D. all of the data on the secondary cluster was deleted after replication was enabled

|                  |
|------------------|
| <b>Answer: D</b> |
|------------------|

Explanation:

Replication relies on having a shared keyring between primary and secondaries and a shared understanding of the data store state.

As soon as replication is enabled, all of the secondary's existing data will be destroyed, which is irrevocable.

Generally, activating as a secondary will be the first thing that is done upon setting up a new cluster for replication.

Hence, create a backup first if there is a slight chance that you would need this existing storage in the future.

Reference link:- <https://www.hashicorp.com/resources/setting-up-configuring-performance-replication/>

## Question: 171

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"]
}
```

**Answer: A**

Explanation:

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: 172

True or False:

When using the transit secrets engine, setting the `min_decryption_version` will determine the minimum key length of the data key (i.e., 2048, 4096, etc.)

- A. False
- B. True

**Answer: A**

Explanation:

The Transit engine supports the versioning of keys. Key versions that are earlier than a key's specified `min_decryption_version` gets archived, and the rest of the key versions belong to the working set. This is a performance consideration to keep key loading fast, as well as a security consideration: by disallowing decryption of old versions of keys, found ciphertext corresponding to obsolete (but sensitive) data can not be decrypted by most users, but in an emergency, the `min_decryption_version` can be moved back to allow for legitimate decryption.

Reference link:- <https://www.vaultproject.io/docs/secrets/transit>

### Question: 173

If a client is currently assigned the following policy, what additional policy can be added to ensure they cannot access the data stored at `secret/apps/confidential` but still, read all other secrets?

- A.  

```
path "secret/apps/confidential/*" {
  capabilities = ["deny"]
}
```
- B.  

```
path "secret/apps/*" {
  capabilities = ["deny"]
}
```
- C.  

```
path "secret/apps/confidential" {
```

```
capabilities = ["deny"]
}
D.
path "secret/apps/*" {
capabilities = ["create", "read", "update", "delete", "list"]
}
path "secret/*" {
capabilities = ["read", "deny"]
}
```

**Answer: C**

Explanation:

"Deny" capability generally takes precedence over "allow" capability.

Therefore, if you add the correct deny statement, the user will be able to read all secrets except for the data stored at secret/apps/confidential

### Question: 174

True or False:

Similar to how Vault works with databases and cloud providers, the Active Directory secrets engine dynamically generates the account and password for the requesting Vault client.

A. False

B. True

**Answer: A**

Explanation:

The Active Directory secrets engine rotates Active Directory passwords dynamically. It does not, however, dynamically generate the AD account. The AD account must exist prior to configuring it in Vault. If it does not, the configuration will fail, stating that the account doesn't exist.

Reference link:- <https://www.vaultproject.io/docs/secrets/ad>

### Question: 175

You've decided to use AWS KMS to automatically unseal Vault on private EC2 instances. After deploying your Vault cluster, and running vault operator init, Vault responds with an error and cannot be unsealed. You've determined that the subnet you've deployed Vault into doesn't have internet access. What can you do to enable Vault to communicate with AWS KMS in the most secure way?

A. ask the networking team to provide Vault with inbound access from the internet

B. deploy Vault in a public subnet and provide the Vault nodes with public IP addresses

C. add a VPC endpoint

D. change the permissions on the Internet Gateway to allow the Vault nodes to communicate over the Internet

---

**Answer: C**

Explanation:

In this particular question, a VPC endpoint can provide private connectivity to an AWS service without having to traverse the public internet. This way you hit a private endpoint for the service rather than connecting to the public endpoint.

This is more of an AWS-type question, but the underlying premise still holds regardless of where your Vault cluster is deployed. If you use a public cloud KMS solution, such as AWS KMS, Azure Key Vault, GCP Cloud KMS, or AliCloud KMS, your Vault cluster will need the ability to communicate with that service to unseal itself.

### Question: 176

Given the policy below, what would the user be able to access?

1. path "\*" {
2. capabilities = ["create", "update", "read", "list", "delete", "sudo"]
3. }

- A. anything they want to within Vault
- B. ability to enable a secret engine at the path \*
- C. only make changes to policies
- D. nothing, since the policy doesn't specify any specific paths

**Answer: A**

Explanation:

All interactions with Vault are done through its pathing structure. If you create a policy with a wildcard, you are giving them access to any path within Vault

### Question: 177

Beyond encryption and decryption of data, which of the following is not a function of the Vault transit secrets engine?

- A. generate hashes and HMACs of data
- B. sign and verify data
- C. act as a source of random bytes
- D. store the encrypted data securely in Vault for retrieval

**Answer: D**

Explanation:

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.

### Question: 178

What is the proper command to enable the AWS secrets engine at the default path?

- A. vault enable secrets aws
- B. vault secrets aws enable
- C. vault secrets enable aws
- D. vault enable aws secrets engine

**Answer: C**

Explanation:

The command format for enabling Vault features is vault <feature> <enable/disable> <name>, therefore the correct answer would be vault secrets enable aws

### Question: 179

By default, how long does the transit secrets engine store the resulting ciphertext?

- A. 24 hours
- B. 32 days
- C. transit does not store data
- D. 30 days

**Answer: C**

Explanation:

Vault does NOT store any data encrypted via the transit/encrypt endpoint. The output you received is the ciphertext. You can store this ciphertext at the desired location (e.g. MySQL database) or pass it to another application.

### Question: 180

Select the policies below that permit you to create a new entry of foo=bar at the path /secrets/apps/my\_secret (select three)

- A.  
path "secrets/apps/my\_secret" {  
capabilities = ["create"]  
allowed\_parameters = {  
"foo" = []  
}



```
}  
}  
B.  
path "secrets/+/my_secret" {  
  capabilities = ["create"]  
  allowed_parameters = {  
    "*" = ["bar"]  
  }  
}  
C.  
path "secrets/apps/my_secret" {  
  capabilities = ["update"]  
}  
D.  
path "secrets/apps/*" {  
  capabilities = ["create"]  
  allowed_parameters = {  
    "foo" = ["bar", "zip"]  
  }  
}
```

**Answer: A, B**

Explanation:

Setting a parameter with a value of the empty list allows the parameter to contain any value.

Setting a parameter with a value of a populated list allows the parameter to contain only those values.

If any keys are specified, all non-specified parameters will be denied unless the parameter "\*" is set to an empty array, which will allow all other parameters to be modified. Parameters with specific values will still be restricted to those values.

### Question: 181

From the options below, select the benefits of using the PKI (certificates) secrets engine: (select three)

- A. TTLs on Vault certs are longer to ensure certificates are valid for a longer period of time
- B. Vault can act as an intermediate CA
- C. reducing, or eliminating certificate revocations
- D. reduces time to get a certificate by eliminating the need to generate a private key and CSR

**Answer: B, C, D**

Explanation:

Reference link:- <https://www.vaultproject.io/docs/secrets/pki>

### Question: 182

---

What type of policy is shown below?

```
1. key_prefix "vault/" {  
2. policy = "write"  
3. }  
4. node_prefix "" {  
5. policy = "write"  
6. }  
7. service "vault" {  
8. policy = "write"  
9. }  
10. agent_prefix "" {  
11. policy = "write"  
12. }  
13. session_prefix "" {  
14. policy = "write"  
15. }
```

- A. Vault policy allowing access to certain paths
- B. Consul ACL policy for a Vault node
- C. Consul configuration policy to enable Consul features
- D. Vault token policy is written for a user

**Answer: B**

Explanation:

If using ACLs in Consul, you'll need appropriate permissions. For Consul 0.8, these policies will work for most use-cases, assuming that your service name is vault and the prefix being used is vault/Consul ACLs should always be enabled when using Consul as a storage backend. This policy allows Vault to communicate to the required services hosted on Consul.

Reference link:- <https://www.vaultproject.io/docs/configuration/storage/consul>

### Question: 183

From the options below, select the benefits of using a batch token over a service token. (select three)

- A. no storage cost for token creation
- B. lightweight and scalable
- C. can be a root token
- D. used for ephemeral, high-performance workloads
- E. has accessors

**Answer: A, B, D**

Explanation:

Service Tokens

Service tokens are what users will generally think of as "normal" Vault tokens. They support all features, such as renewal, revocation, creating child tokens, and more. They are correspondingly heavyweight to create and track.

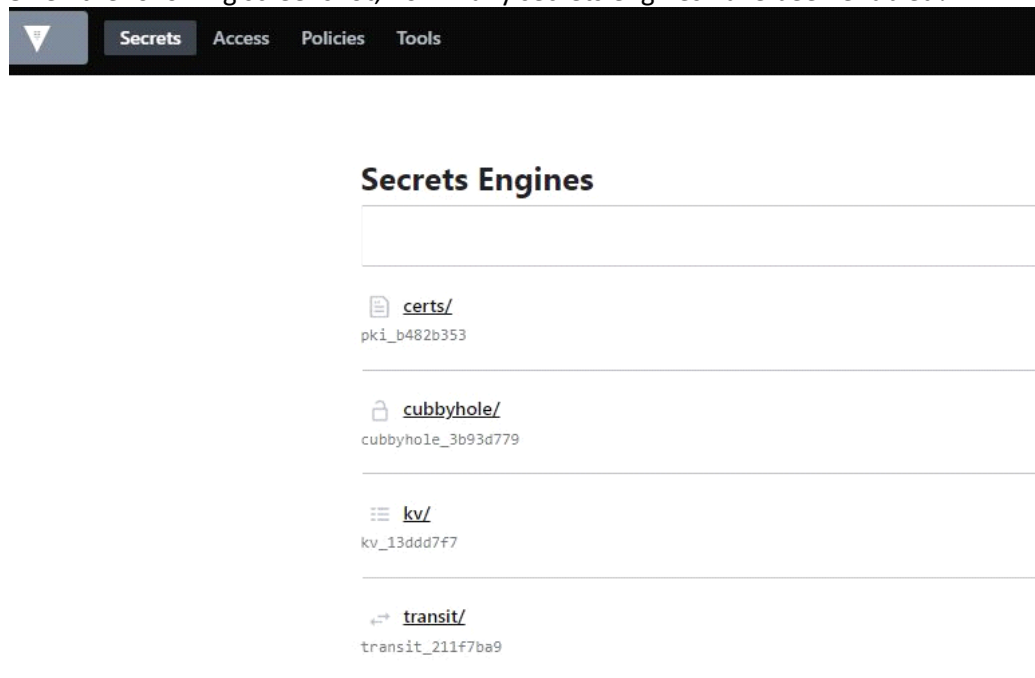
#### Batch Tokens

Batch tokens are encrypted blobs that carry enough information for them to be used for Vault actions, but they require no storage on disk to track them. As a result, they are extremely lightweight and scalable but lack most of the flexibility and features of service tokens.

Reference link:- <https://www.vaultproject.io/docs/concepts/tokens>

## Question: 184

Given the following screenshot, how many secrets engines have been enabled?



- A. 4
- B. 3
- C. 5
- D. 2

**Answer: B**

Explanation:

The Cubbyhole secret engine is a default secrets engine that is enabled by default for each Vault user.

## Question: 185

True or False: When encrypting data with the transit secrets engine, Vault always stores the ciphertext in a dedicated KV store along with the associated encryption key.

- A. False
- B. True

**Answer: A**

Explanation:

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.

Reference link:- <https://www.vaultproject.io/docs/secrets/transit>

## Question: 186

When administering Vault on a day-to-day basis, why is logging in with the root token, as shown below, a bad idea? (select two).

**Sign in to Vault**

token userpass Other

Token

.....

**Sign In**

[Contact your administrator for login credentials](#)

- A. the root token isn't a secure way of logging into Vault
- B. the root token is attached to the root policy, which likely provides too many privileges to a user
- C. the root token should be revoked and not used on a day-to-day basis
- D. It's easier to just use the root token than to configure additional auth methods

**Answer: B, C**

Explanation:

The root token should never be used on a day-to-day basis and should always be revoked once a permanent auth method has been configured.

## Question: 187

---

In regards to using a K/V v2 secrets engine, select the three correct statements below: (select three)

- A. issuing a vault kv destroy statement permanently deletes a single version of a secret
- B. issuing a vault kv destroy statement deletes all versions of a secret
- C. issuing a vault kv delete statement permanently deletes the secret
- D. issuing a vault kv metadata delete statement permanently deletes the secret
- E. issuing a vault kv delete statement performs a soft delete

**Answer: A, D, E**

Explanation:

The kv delete command is like a soft delete which deletes the data for the provided path in the key/value secrets engine. If using K/V Version 2, its versioned data will not be fully removed, but marked as deleted and will no longer be available for normal get requests.

The kv destroy command permanently removes the specified versions' data from the key/value secrets engine. If no key exists at the path, no action is taken. It does not delete all versions of a secret.

The kv metadata delete command deletes all versions and metadata for the provided key.

### Question: 188

After executing a terraform apply, you notice that a resource has a tilde (~) next to it. What does this infer?

- A. the resource will be destroyed and recreated
- B. the resource will be created
- C. Terraform can't determine how to proceed due to a problem with the state file
- D. the resource will be updated in place

**Answer: D**

Explanation:

The prefix -/+ means that Terraform will destroy and recreate the resource, rather than updating it in-place. Some attributes and resources can be updated in-place and are shown with the ~ prefix.

### Question: 189

What does the command terraform fmt do?

- A. formats the state file in order to ensure the latest state of resources can be obtained
- B. updates the font of the configuration file to the official font supported by HashiCorp
- C. rewrite Terraform configuration files to a canonical format and style
- D. deletes the existing configuration file

**Answer: C**

---

Explanation:

The terraform fmt command is used to rewrite Terraform configuration files to a canonical format and style. This command applies a subset of the Terraform language style conventions, along with other minor adjustments for readability.

Other Terraform commands that generate Terraform configuration will produce configuration files that conform to the style imposed by terraform fmt, so using this style in your own files will ensure consistency.

### Question: 190

Select the feature below that best completes the sentence:

The following list represents the different types of \_\_\_\_\_ available in Terraform.

1. max
2. min
3. join
4. replace
5. list
6. length
7. range

- A. named values
- B. backends
- C. functions
- D. data sources

**Answer: C**

Explanation:

The Terraform language includes a number of built-in functions that you can call from within expressions to transform and combine values. The Terraform language does not support user-defined functions, and only the functions built into the language are available for use.

### Question: 191

You have been given requirements to create a security group for a new application. Since your organization standardizes on Terraform, you want to add this new security group with the fewest number \_\_\_\_\_ of \_\_\_\_\_ lines

of code. What feature could you use to iterate over a list of required tcp ports to add to the new security group?

- A. terraform import
- B. splat expression
- C. dynamic block
- D. dynamic backend

---

**Answer: C**

Explanation:

A dynamic block acts much like a for expression but produces nested blocks instead of a complex typed value. It iterates over a given complex value and generates a nested block for each element of that complex value.

### Question: 192

When using parent/child modules to deploy infrastructure, how would you export value from one module to import into another module?

For example, a module dynamically deploys an application instance or virtual machine, and you need the IP address in another module to configure a related DNS record in order to reach the newly deployed application.

- A. configure an output value in the application module in order to use that value for the DNS module
- B. preconfigure the IP address as a parameter in the DNS module
- C. configure the pertinent provider's configuration with a list of possible IP addresses to use
- D. export the value using terraform export and input the value using terraform input

**Answer: A**

Explanation:

Output values are like the return values of a Terraform module and have several uses such as a child module using those outputs to expose a subset of its resource attributes to a parent module.

### Question: 193

From the answers below, select the advantages of using Infrastructure as Code. (select four)

- A. Easily integrate with application workflows (GitLab Actions, Azure DevOps, CI/CD tools)
- B. Safely test modifications using a "dry run" before applying any actual changes
- C. Provide reusable modules for easy sharing and collaboration
- D. Easily change and update existing infrastructure
- E. Provide a codified workflow to develop customer-facing applications

**Answer: A, B, C, D**

Explanation:

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.

---

### Question: 194

Which of the following is considered a Terraform plugin?

- A. Terraform logic
- B. Terraform language
- C. Terraform tooling
- D. Terraform provider

**Answer: D**

Explanation:

Terraform is built on a plugin-based architecture. All providers and provisioners that are used in Terraform configurations are plugins, even the core types such as AWS and Heroku. Users of Terraform are able to write new plugins in order to support new functionality in Terraform.

### Question: 195

What happens when a terraform apply command is executed?

- A. applies the changes required in the target infrastructure in order to reach the desired configuration
- B. creates the execution plan for the deployment of resources
- C. reconciles the state Terraform knows about with the real-world infrastructure
- D. the backend is initialized and the working directory is prepped

**Answer: A**

Explanation:

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.

### Question: 196

Which of the following best describes a Terraform provider?

- A. describes an infrastructure object, such as a virtual network, compute instance, or other components
- B. a container for multiple resources that are used together
- C. serves as a parameter for a Terraform module that allows a module to be customized
- D. a plugin that Terraform uses to translate the API interactions with the service or provider

**Answer: D**

Explanation:



---

A provider is responsible for understanding API interactions and exposing resources. Providers generally are an IaaS (e.g., Alibaba Cloud, AWS, GCP, Microsoft Azure, OpenStack), PaaS (e.g., Heroku), or SaaS services (e.g., Terraform Cloud, DNSimple, CloudFlare).

### Question: 197

What is a downside to using a Terraform provider, such as the Vault provider, to interact with sensitive data, such as reading secrets from Vault?

- A. Terraform and Vault must be running on the same physical host
- B. Terraform and Vault must be running on the same version
- C. Terraform requires a unique auth method to work with Vault
- D. Secrets are persisted to the state file and plans

**Answer: D**

Explanation:

Interacting with Vault from Terraform causes any secrets that you read and write to be persisted in both Terraform's state file and in any generated plan files. For any Terraform module that reads or writes Vault secrets, these files should be treated as sensitive and protected accordingly.

### Question: 198

In order to make a Terraform configuration file dynamic and/or reusable, static values should be converted to use what?

- A. regular expressions
- B. module
- C. input parameters
- D. output value

**Answer: C**

Explanation:

Input variables serve as parameters for a Terraform module, allowing aspects of the module to be customized without altering the module's own source code, and allowing modules to be shared between different configurations.

### Question: 199

Which Terraform command will force a marked resource to be destroyed and recreated on the next apply?

- A. terraform fmt
- B. terraform destroy

- C. terraform taint
- D. terraform refresh

**Answer: C**

Explanation:

The terraform taint command manually marks a Terraform-managed resource as tainted, forcing it to be destroyed and recreated on the next apply. This command will not modify infrastructure but does modify the state file in order to mark a resource as tainted. Once a resource is marked as tainted, the next plan will show that the resource will be destroyed and recreated. The next terraform apply will

implement this change.

### Question: 200

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)

- A. directly querying HashiCorp Vault for the secrets
- B. command-line key/value pairs
- C. use the -backend-config=PATH to specify a separate config file
- D. interactively on the command line

**Answer: B, C, D**

Explanation:

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.

**For More Information – Visit link below:**

**<https://www.cert4prep.com/>**

**Thanks for Using Our Product:**

## **FEATURES:**

- 100% Pass Guarantee
- 30 Days Money Back Guarantee
- 24/7 Live Chat Support(Technical & Sales)
- Instant Download or Email Attachment
- 50,000 +ve Reviews
- 100% Success Rate
- Discounts Available for Bulk Orders