HashiCorp.VA-002-P.v2022-11-18.q73

Exam Code:	VA-002-P
Exam Name:	HashiCorp Certified: Vault Associate Exam
Certification Provider:	HashiCorp
Free Question Number:	73
Version:	v2022-11-18
# of views:	1308
# of Questions views:	730
https://www.freeqas.com/qa/HashiCorp/VA-002-P/HashiCorp.VA-002-P.v2022-11-18.q73.html	

NEW QUESTION: 1
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 (LEAVE A REPLY)
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.

NEW QUESTION: 2
What is the purpose of using the local-exec provisioner? (select two)
A. to invoke a local executable
B. executes a command on the resource to invoke an update to the Terraform state
C. to execute one or more commands on the machine running Terraform
D. ensures that the resource is only executed in the local infrastructure where Terraform is deployed
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 3
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 (LEAVE A REPLY)
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

NEW QUESTION: 4
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 (LEAVE A REPLY)
zipmap constructs a map from a list of keys and a corresponding list of values. A map is denoted by { } whereas a list is donated by [ ].
https://www.terraform.io/docs/configuration/functions/zipmap.html

NEW QUESTION: 5
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 (LEAVE A REPLY)
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>

NEW QUESTION: 6
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 (LEAVE A REPLY)
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 change of human error.

NEW QUESTION: 7
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 (LEAVE A REPLY)

The terraform workspace select command is used to choose a different workspace to use for further operations. https://www.terraform.io/docs/commands/workspace/select.html

NEW QUESTION: 8

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 (LEAVE A REPLY)

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

NEW QUESTION: 9

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: (SHOW ANSWER)

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

NEW QUESTION: 10
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 (LEAVE A REPLY)
HashiCorp style conventions suggest you that align the equals sign for consecutive arguments for easing readability for configurations ami = "abc123" instance_type = "t2.micro"

NEW QUESTION: 11
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 (LEAVE A REPLY)
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.

NEW QUESTION: 12

Vault does not trust the storage backend.
A. False
B. True
Answer: B (LEAVE A REPLY)
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

NEW QUESTION: 13
When a primary Vault cluster fails, Vault will automatically promote a secondary cluster to ensure maximum uptime.
A. False
B. True
Answer: (SHOW ANSWER)
Vault secondary clusters must be manually promoted to a primary.

NEW QUESTION: 14
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 (LEAVE A REPLY)
It is important to consider that Terraform reads from data sources during the plan phase and writes the result into the plan. For something like a Vault token which has an explicit TTL, the apply must be run before the data, or token, in this case, expires, otherwise, Terraform will fail during the apply phase.

NEW QUESTION: 15
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: (SHOW ANSWER)
To browse Vault paths in the UI, the user must have list permissions on the mount and the paths leading up to the secret.

NEW QUESTION: 16

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: (SHOW ANSWER)

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

NEW QUESTION: 17

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: (SHOW ANSWER)

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

NEW QUESTION: 18
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 (LEAVE A REPLY)
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.

NEW QUESTION: 19
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 (LEAVE A REPLY)
~> 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

NEW QUESTION: 20

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 (LEAVE A REPLY)
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.

NEW QUESTION: 21
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 (LEAVE A REPLY)
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.

NEW QUESTION: 22
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: (SHOW ANSWER)

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

NEW QUESTION: 23
What could you do with the feature found in the screenshot below? (select two)

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: (SHOW ANSWER)
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.

NEW QUESTION: 24
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 (LEAVE A REPLY)
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.

NEW QUESTION: 25
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 (LEAVE A REPLY)
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

NEW QUESTION: 26
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: (SHOW ANSWER)
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

NEW QUESTION: 27
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 (LEAVE A REPLY)
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

NEW QUESTION: 28
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: (SHOW ANSWER)
When you send data to Vault for encryption, it must be in the form of base64-encoded plaintext for safe transport.

NEW QUESTION: 29
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\ ciphertext="vault:v1:cZNHVx
+sxdMErXRSuDa1q/pz49fXTn1PScKfhf+PIZPvy8xKfkytpwKcbC0fF2U=" \
2.
3. Key Value
4. --- -----
5. plaintext Y3JlZGl0LWNhcmQtbnVtYmVyCg==

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 (LEAVE A REPLY)

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

NEW QUESTION: 30

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: (SHOW ANSWER)

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

- Auto-Auth
- Caching
- Templating

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

NEW QUESTION: 31

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 (LEAVE A REPLY)

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

NEW QUESTION: 32
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 (LEAVE A REPLY)
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.

NEW QUESTION: 33
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 (LEAVE A REPLY)
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.

NEW QUESTION: 34
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 much 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: (SHOW ANSWER)
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

NEW QUESTION: 35
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 (LEAVE A REPLY)
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.

NEW QUESTION: 36
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 (LEAVE A REPLY)

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

NEW QUESTION: 37

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 (LEAVE A REPLY)

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.

NEW QUESTION: 38

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"
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: (SHOW ANSWER)

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.

NEW QUESTION: 39
Which of the following secrets engine can generate dynamic credentials? (select three)
A. Azure
B. database
C. key/value
D. Transit
E. AWS
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 40
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 (LEAVE A REPLY)
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.

NEW QUESTION: 41
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 (LEAVE A REPLY)
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.

NEW QUESTION: 42
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 (LEAVE A REPLY)
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

NEW QUESTION: 43
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 (LEAVE A REPLY)
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.

NEW QUESTION: 44
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 (LEAVE A REPLY)
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).

NEW QUESTION: 45
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 (LEAVE A REPLY)
Currently, Terraform has no mechanism to redact or protect secrets that are returned via data sources, so secrets read via this provider will be persisted into the Terraform state, into any plan files, and in some cases in the console output produced while planning and applying. These artifacts must, therefore, all be protected accordingly.

NEW QUESTION: 46
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: (SHOW ANSWER)
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.

NEW QUESTION: 47
Vault's User Interface (UI) needs to be enabled in the command line before it can be used.
A. FALSE
B. TRUE
Answer: A (LEAVE A REPLY)
The UI is enabled in the Vault configuration file, not in the CLI.

NEW QUESTION: 48
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 (LEAVE A REPLY)
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

NEW QUESTION: 49
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: (SHOW ANSWER)
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.

NEW QUESTION: 50
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 (LEAVE A REPLY)

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.

NEW QUESTION: 51
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 (LEAVE A REPLY)
Reference link:- https://www.vaultproject.io/docs/secrets/pki

NEW QUESTION: 52
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 (LEAVE A REPLY)
Since Vault does not store any data, hence Vault transit secrets engine does not support update activity.

NEW QUESTION: 53
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 (LEAVE A REPLY)

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.

NEW QUESTION: 54

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: (SHOW ANSWER)

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

NEW QUESTION: 55

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: (SHOW ANSWER)

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

NEW QUESTION: 56

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 (LEAVE A REPLY)

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

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

NEW QUESTION: 57

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 (LEAVE A REPLY)

For production use, you should constrain the acceptable provider versions via configuration file to ensure that new versions with breaking changes will not be automatically installed by terraform init in the future. When terraform init is run without provider version constraints, it prints a suggested version constraint string for each provider For example:

terraform {

required_providers {

aws = ">= 2.7.0"

}

}

NEW QUESTION: 58

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 (LEAVE A REPLY)

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.

NEW QUESTION: 59

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 (LEAVE A REPLY)
Replication is not available in open-source versions of Vault. It is an enterprise feature.

NEW QUESTION: 60
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 (LEAVE A REPLY)
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

NEW QUESTION: 61
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: (SHOW ANSWER)
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 deletes all versions of a secret.
The kv metadata delete command deletes all versions and metadata for the provided key.

NEW QUESTION: 62
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 (LEAVE A REPLY)
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.

NEW QUESTION: 63
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 (LEAVE A REPLY)
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

NEW QUESTION: 64
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 (LEAVE A REPLY)
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.

NEW QUESTION: 65
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: (SHOW ANSWER)
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.

NEW QUESTION: 66

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

Answer: D (LEAVE A REPLY)

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/

NEW QUESTION: 67

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: (SHOW ANSWER)

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.

NEW QUESTION: 68
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 (LEAVE A REPLY)
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.

NEW QUESTION: 69
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 (LEAVE A REPLY)
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

NEW QUESTION: 70
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 (LEAVE A REPLY)

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

NEW QUESTION: 71
In Terraform Enterprise, a workspace can be mapped to how many VCS repos?
A. 5
B. 3
C. 2
D. 1
Answer: D (LEAVE A REPLY)
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.

NEW QUESTION: 72
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: (SHOW ANSWER)
A lease must be renewed before it has expired. Once it has expired, it is permanently revoked and a new secret must be requested.

NEW QUESTION: 73
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 (LEAVE A REPLY)
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.