

HashiCorp HCCAO-003

HashiCorp Certified: Consul Associate (003)

**Thank You for Downloading HCCAO-003 Updated Exam
Questions**

<https://certs4sale.com/hashicorp/hccao-003-pdf-exam-dumps>

QUESTION: 1

Given the following ACL policy, what actions below would be permitted by a token assigned to this policy? (select three)

```
1. service "app1" {
2.   policy = "write"
3. }
4.5. service_prefix "" {
6.   policy = "read"
7. }
8.9. node_prefix "" {
10.   policy = "read"
11. }
```

Option A :

query any service registered to Consul to list the active clients for the service

Option B : run the consul members command to view server and client nodes in the cluster

Option C :

create a new Consul service call app1

Option D : register any service on Consul

Correct Answer: A,B,C

Explanation/Reference:

Create a new Consul service called app1 is permitted by the following rule since it's explicitly permitting it by name and the rule is allowing a write.

```
service "app1" {
  policy = "write"
}
```

Run the consul members command to view server and client nodes in the cluster is permitted by the following command since consul members would require you to read information from any node in the cluster

```
node_prefix "" {
  policy = "read"
}
```

Query any service registered to Consul to list the active clients for the service is permitted by the following rule since it permits a read on any service registered to Consul.

If the rule was written as service_prefix = "web", you'd only be able to query a service named web.

```
service_prefix "" {
  policy = "read"
}
```

Incorrect Answer:

Register any service on Consul would not be permitted unless there was a rule that allowed a write on service_prefix. This would likely be a bad idea since you wouldn't

want just anybody to register a service with Consul. Bad actors with this permission could register a node with an existing service as an attempt to direct traffic to a compromised host.

QUESTION: 2

You have deployed a new Consul cluster to be used for service discovery between your microservices for a new application. In the configuration file, as shown below, you have enabled ACLs and bootstrapped the ACL system. However, clients are still being permitted to read and write to the ACL system or register services without a valid token. Based on the policy, what change needs to be made to finish securing Consul?

```
1. {2. "server": true,3. "node_name": "CONSUL-NODE-A",4. "datacenter": "DC-1",5. "data_dir": "/var/consul/data",6. "bind_addr": "0.0.0.0",7. "client_addr": "0.0.0.0",8. "advertise_addr": "10.0.10.208",9. "bootstrap_expect": 5,10. "retry_join": ["provider=aws tag_key=consul tag_value=true"],11. "ui": true,12. "log_level": "INFO",13. "acl": {14. "enabled": true,15. "default_policy": "allow",16. "down_policy": "extend-cache"17. }18. }
```

- Option A : configure the ACL policy for the anonymous token to deny all client requests
- Option B : reload the configuration on all the nodes after the bootstrap token was created
- Option C : update the default_policy across all of the Consul nodes
- Option D : apply the bootstrap token to the other nodes

Correct Answer: C

Explanation/Reference:

Once ACLs have been enabled and the bootstrap token has been created, you will need to modify the configuration file and change the default_policy to deny. This policy change will require all requests to Consul, including those from Consul servers, to have a valid token in order to communicate with the Consul service.

<https://learn.hashicorp.com/consul/security-networking/production-acls>

<https://www.consul.io/docs/acl#acl-documentation>

QUESTION: 3

True or False? When running Consul OSS, you can use the snapshot command/API to natively create and store snapshots to cloud-based storage.

- Option A : True
- Option B : False

Correct Answer: B

Explanation/Reference:

When running open-source, the Consul snapshot command or API only supports saving the Consul snapshot locally. However,

you can automate it with an external tool
and have that tool/script move the snapshot somewhere else.
<https://www.consul.io/commands/snapshot/save>

QUESTION: 4

Scenario: You're deploying Consul in a dedicated environment, and due to the complex network layout, you are forced to funnel traffic through a firewall that will perform a NAT (network address translation) for the Consul node. What configuration parameter can be used to identify what IP address that the other nodes in the cluster should use to communicate with Consul?

Option A :

-client

Option B :

-bind

Option C :

-serf-lan-bind

Option D : -advertise

Correct Answer: D

Explanation/Reference:

The advertise address is used to change the address that Consul advertises to other nodes in the cluster. By default, the -bind address is advertised. However, in some cases, there may be a routable address that cannot be bound. This flag enables gossiping a different address to support this. If this address is not routable, the node will be in a constant flapping state as other nodes will treat the non-routability as a failure.

https://www.consul.io/docs/agent/options#_advertise

QUESTION: 5

You've logged into the Consul UI and want to modify the policy that is used by a token assigned to an application. However, you see this screen when clicking the ACL tab. What must you provide in order to access the ACL configuration page?

[dc-1](#)[Services](#)[Nodes](#)[Key/Value](#)[ACL](#)[Intentions](#)

Access Controls

The Access Control List (ACL) system, which controls permissions for this UI, is enabled for this cluster. ' [REDACTED]

[REDACTED]

Save

Option A : the policy ID that you want to modify

Option B : reconfirm your password used to log into Consul

Option C : the accessor ID of the master token

Option D : provide the master token or another token with sufficient privileges

Correct Answer: D

Explanation/Reference:

When ACLs are enabled, you need sufficient privileges to access the configuration of ACLs. On this screen, you may provide the master token or another token with privileges to manage the ACL system. Once you log in, the UI will change to the following screen, which will allow you to work with policies, roles, and tokens.



Access Controls

Tokens

Roles

Policies

Accessor ID	Scope	Description	Roles & Policies
a5bf5687	global	Bootstrap Token (Global Management)	★ global-management
00000000	global	Anonymous Token	

QUESTION: 6

When running the Consul agent in dev (development) mode, where does Consul write its data?

Option A : in the directory where the Consul agent was started

Option B : the temp directory that the underlying operating system uses

Option C :

the default application data directory, which is different based on the underlying operating system

Option D : stores all data and configuration in non-persistent memory

Correct Answer: D

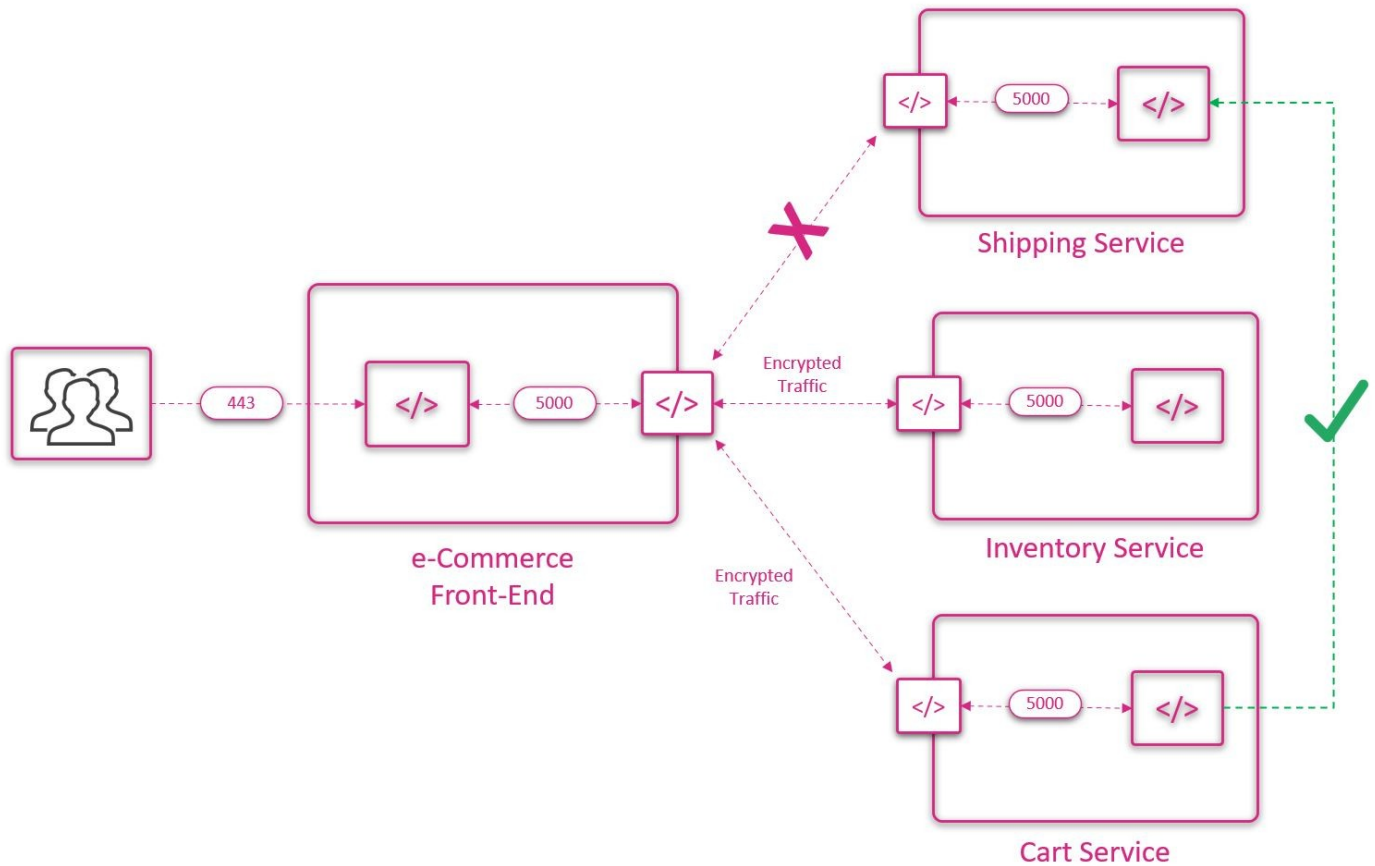
Explanation/Reference:

Starting the Consul agent in dev mode is useful for quickly starting a Consul agent with all persistence options turned off, enabling an in-memory server which can be used for rapid prototyping or developing against the API. In this mode, Connect is enabled and will by default create a new root CA certificate on startup. This mode is not intended for production use as it does not write any data to disk.

https://www.consul.io/docs/agent/options#_dev

QUESTION: 7

Scenario: You have multiple services registered with Consul for your e-commerce site, including the front-end service, the shipping service, the inventory service, and the cart service. To safeguard your customer's shipping addresses, you want to ensure that communication between the front-end and the shipping service is denied and that traffic is only permitted from the cart service. What feature of Consul Connect can you use to permit access to the shipping service from the cart service and deny communication from the front-end service?



Option A : Intentions

Option B : Consul agent

Option C : Consul ACLs

Option D : Consul Namespaces

Correct Answer: A

Explanation/Reference:

Intentions define access control for services via Connect and are used to control which services may establish connections.

Intentions can be managed via the API, CLI, or

UI.

Intentions are enforced by the proxy or natively integrated application on inbound connections. After verifying the TLS client certificate, the authorize API endpoint is

called which verifies the connection is allowed by testing the intentions. If authorize returns false the connection must be

terminated.

<https://www.consul.io/docs/connect/intentions.html>

<https://www.consul.io/docs/connect/intentions>

QUESTION: 8

From the options below, select the features that are available in Consul Enterprise, and not available in the open-source offering.

Option A :

Connect (service to service authorization and encryption)

Option B : Autopilot (automated upgrades)

Option C : Consul snapshot agent (automated backups)

Option D : OIDC auth method (centralized authentication)

Option E : Sentinel (Policy as Code)

Option F :

Namespaces (datacenter isolation)

Correct Answer: A,B,C,D

Explanation/Reference:

While Consul offers a TON of functionality in its open-source, there are several features only available in Enterprise. Back in Consul 1.6, HashiCorp open-sourced lots of the Enterprise features to better compete with Istio. However, newer features are being released to Enterprise-only customers, including several new features in Consul 1.7 and Consul 1.8. <https://www.consul.io/docs/enterprise>

Features include:

- + Automated Backups
- + Automated Upgrades
- + Enhanced Read Scalability
- + Redundancy Zones
- + Advanced Federation for Complex Network Topologies
- + Network Segments
- + Namespaces
- + Sentinel
- + OIDC Auth Method

QUESTION: 9

You are running a Consul Enterprise deployment with immutable nodes and want to establish a backup strategy since Consul is heavily used within your organization. Which method below would provide automated backups and ensure that the snapshots are stored on a secure, durable storage solution?

Option A : logging into the node and executing the consul snapshot save command

Option B : <https://www.mytestengine.com/home/index?code=Consul-Associate>

Option C :

a cron job that executes the command `consul snapshot save backup.snap` every hour

Option D : consul snapshot agent

Correct Answer: D

Explanation/Reference:

The key part of the question is that you are running Consul Enterprise, which permits you to use the Consul Snapshot Agent.

The snapshot agent subcommand starts a

process that takes snapshots of the state of the Consul servers and saves them locally or pushes them to an optional remote storage service.

As of Consul 1.6.1, Consul Snapshot Agent can store snapshots on AWS, Azure, or Google. You can also store them locally if you wish.

QUESTION: 10

You have two Consul datacenters and you want to enable federation so services in dc1 can discover services in dc2. You run the `consul join wan node2.example.com`. However, servers in dc1 can not communicate with servers in dc2 and vice versa. Based on the snippets of the server configuration files can be found below, why would this be assuming network connectivity is working as expected?

dc1 configuration

```
1. "datacenter": "dc1",
2. "server": true,
3. "key_file": "/etc/consul.d/cert.key",
4. "cert_file": "/etc/consul.d/client.pem",
5. "ca_file": "/etc/consul.d/chain.pem",
6. "verify_incoming": true,
7. "verify_outgoing": true,
8. "verify_server_hostname": true,
9. "ui": true,
10. "encrypt": "XIUEktl3YjG9KPJfaBU1xE69IZ0XhsNCSH423FyknJE=",
11. "bootstrap_expect": 5,
12. "enable_syslog": true,
```

dc2 configuration

```
1. "datacenter": "dc2",
2. "server": true,
3. "key_file": "/etc/consul.d/cert.key",
4. "cert_file": "/etc/consul.d/client.pem",
5. "ca_file": "/etc/consul.d/chain.pem",
6. "verify_incoming": true,
7. "verify_outgoing": true,
8. "verify_server_hostname": true,
9. "ui": true,
10. "encrypt": "LSBSOZI5+9EX/kdY8u27mX50rk1ywcprfUCoSZjnpUg=",
11. "bootstrap_expect": 5,
12. "enable_syslog": false,
```

Option A : the gossip keys need to match between federated datacenters

Option B : the `verify_incoming` setting should be set to false before WAN federation can be configured

Option C : the client certificates are issued from different CAs

Option D : the syslog configurations do not match

Correct Answer: A

Explanation/Reference:

If gossip encryption is enabled in one datacenter, it must be enabled in all datacenters because in order to communicate with that one datacenter the encryption key is required.

<https://www.consul.io/docs/security/encryption>

<https://learn.hashicorp.com/tutorials/consul/federation-gossip-wan>

QUESTION: 11

The Consul KV store can be accessed by the following methods: (select three)

Option A : CLI

Option B :
federated cluster

Option C : API

Option D : UI

Correct Answer: A,C,D

Explanation/Reference:

The KV store can be accessed by the consul kv CLI subcommands, HTTP API, and Consul UI.

<https://www.consul.io/docs/agent/kv.html#accessing-the-kv-store>

QUESTION: 12

What ports does Consul use as the default for the incoming DNS listener, where clients can send DNS queries for service discovery? (select two)

Option A : tcp/8600

Option B : tcp/53

Option C : udp/53

Option D : udp/8600

Correct Answer: A,D

Explanation/Reference:

Consul defaults to using TCP & UDP 8600 for DNS requests. This default is overridden by the ports/dns flag in the configuration file. DNS should be run as a higher port

since ports below 1024 cannot be run using a standard service account, and must have root privileges. Therefore, it's best to run Vault on a higher port, so you don't need

to run the Consul service as a privileged user.

If you do need to resolve queries on Consul using the standard DNS port of 53, check out this article, which shows how to use something like BIND to automatically

forward queries received on port 53 to the Consul default of 8600. This capability is super helpful when Consul is running in environments that can't forward DNS queries

to Consul using another port besides 53 (like Microsoft DNS server)

https://www.consul.io/docs/agent/options.html#dns_port

QUESTION: 13

Which of the following security methods does Consul use to secure gossip communication throughout the cluster?

- Option A : ACLs
- Option B : pre-shared symmetric key
- Option C : TLS certificates
- Option D : mutual TLS certificates

Correct Answer: B

Explanation/Reference:

Gossip protocol can encrypt communications throughout the cluster using a symmetric key. This is essentially a 'shared secret' method for both servers and clients in a cluster.

<https://www.consul.io/docs/security/encryption#gossip-encryption>

QUESTION: 14

You need to determine the leader node for the Consul cluster. What command allows you to quickly identify the nodes and their current roles within the cluster? Example of the command's output:

```
1. Node ID Address State Voter RaftProtocol
2. CONSUL-NODE-A 121abb4c-16fb-c8ec-2e2b-9595925de4dc 10.0.10.238:8300 follower true
33. CONSUL-NODE-C 4bead426-4471-0924-598f-cd6ce0015ebc 10.0.10.48:8300 follower true
34. CONSUL-NODE-E c44e8ab1-1132-1b22-9501-479c690c9e1b 10.0.10.105:8300 leader true
35. CONSUL-
```

NODE-D ba86541f-cd93-6ada-b763-709b0fc6c09f 10.0.11.163:8300 follower true 36. CONSUL-NODE-B 2528cba1-06ea-4837-fc7b-13e44af19b0d 10.0.11.141:8300 follower true 3

Option A : consul nodes -leader
Option B : consul members
Option C :
consul raft- list

Option D :
consul operator raft list-peers

Correct Answer: D

Explanation/Reference:

The Raft operator command is used to interact with Consul's Raft subsystem. Specifically, the list-peers command will display the current Raft peer configuration, which

shows the state of each node, being either a leader or a follower.

<https://www.consul.io/docs/commands/operator/raft.html#list-peers>

QUESTION: 15

Which of the following are benefits of using Consul for service discovery? (select 3)

Option A :
simplified communication between microservices

Option B : reduction or elimination of load balancers for east/west traffic

Option C : single point of contact for a service where the underlying containers may be dynamic or frequently change

Option D : scheduling of services and containers for application redundancy

Correct Answer: A,B,C

Explanation/Reference:

Service discovery provides a service registry for services that have registered and are reporting as healthy. This allows microservices to easily communicate by using

Consul rather than having to deploy load balancers in front of each individual service. This simplifies communication between these dynamic services while getting rid of

the load balancers needed for this east/west traffic. Health checks also allow containers or VMs to be easily scaled up and down, or completely replaced, and Consul will

direct traffic to only health nodes.

More information can be found on Consul's discovery page found [here](#).

QUESTION: 16

During leadership election, which members in the local datacenter get a vote to elect a new leader?

Option A : Consul server nodes

Option B :

Consul servers and clients

Option C : Consul servers, read-only server nodes, and clients

Option D : Consul clients

Correct Answer: A

Explanation/Reference:

Consul's consensus protocol (Serf) is responsible for electing a leader during a new cluster creation or if an existing leader fails.

The consensus protocol is only used on

Consul server nodes, therefore clients do not participate in voting for a new cluster leader. Furthermore, read-only nodes are also known as non-voting nodes and do not

participate in voting for a new leader (hence the name).

<https://www.consul.io/docs/architecture/gossip>

QUESTION: 17

Complete the sentence using the correct answer below: When authentication is enabled, a Consul token should be provided to make API requests using the _____ or _____ header

Option A : X-Consul-Token

Option B :

ACL-Token

Option C : Consul-Token

Option D :

Token

Option E : Authorization: Bearer

Correct Answer: A

Explanation/Reference:

When authentication is enabled, a Consul token should be provided to API requests using the X-Consul-Token or the Authorization: Bearer header. As an example, an API call should include the token as shown below:

```
$ curl \
--header "X-Consul-Token: 988b8fb4-357a-376d-057e-9d9fd5a170a2" \
http://consul.example.com:8500/v1/agent/members
...or...
$ curl \
--header "Authorization: Bearer 988b8fb4-357a-376d-057e-9d9fd5a170a2" \
http://127.0.0.1:8500/v1/agent/members
https://www.consul.io/api-docs/acl
```


THANK YOU FOR DOWNLOADING HCCAO-003 UPDATED EXAM QUESTIONS

Note: Thanks For Trying The Demo Of Our HCCAO-003 Exam Product

Visit Our Site to Purchase the Full Set of Actual HCCAO-003 Exam Questions With Answers.

Money Back Guarantee



Click The Link Below

<https://certs4sale.com/hashicorp/hccao-003-pdf-exam-dumps>