We offer free update service for one year!
https://www.certqueen.com

Exam : Consul Associate

Title : HashiCorp Certified: Consul Associate

Version : DEMO

1.Based upon the DNS query output below, select the answers below which are true statements. (select three)

```
$ dig @127.0.0.1 -p 8600 retail.service.consul
;<<>> DiG 9.10.3-P4-Ubuntu <<>> @127.0.0.1 -p 8600 retail.service.consul
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51648
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;retail.service.consul.      IN      A

;; ANSWER SECTION:
retail.service.consul. 0     IN      A       127.0.0.1

;; Query time: 0 msec
;; SERVER: 127.0.0.1#8600(127.0.0.1)
;; WHEN: Tue May 12 14:02:23 UTC 2020
;; MSG SIZE  rcvd: 69
```

A. the retail service is currently unhealthy and no nodes are available
B. the retail service is running on the same host that has been queried
C. the retail service is running and is available
D. there is a single, healthy host running the retail service
E. the retail service is running on port 8600

Answer: B,C,D

Explanation:

The dig command, which is a DNS query tool, was executed on a local Consul server, hence the 127.0.0.1 in the initial command executed. The command was run against port 8600, since that is the default port that Consul listens to for DNS queries.

Based on the answer section, you can see that a single response, which indicates that the retail service is running on 127.0.0.1 - the same host as the dig command was run against. In addition, the fact that an answer was returned indicates that the service is up and running and passing any associated health checks since Consul will not return unhealthy hosts to a DNS query.

https://learn.hashicorp.com/consul/getting-started/services#dns-interface

2.A Consul snapshot saves a point-in-time snapshot of the state of the Consul servers, and includes what type of data? (select five)

A. prepared queries
B. sessions
C. consul-template templates
D. ACLs
E. audit log of API requests
F. KV entries
G. the service catalog

Answer: A,B,D,F,G
Explanation:
Consul provides the snapshot command which can be run using the CLI or the API.
The snapshot command saves a point-in-time snapshot of the state of the Consul servers which includes, but is not limited to:
+ KV entries
+ the service catalog
+ prepared queries
+ sessions
+ ACLs
https://learn.hashicorp.com/consul/datacenter-deploy/backup

3.The organization uses a service named phone-book for hitting a web service to lookup client phone numbers. However, users complain that the service is currently unavailable. You perform a manual DNS query of the service and the DNS response includes no value.
What are some reasons that the service does not return any valid hosts? (select three)
A. the service health checks have failed for each registered instance
B. the service was removed from Consul service registry
C. a prepared query was never configured for the service
D. the node health check has failed for each underlying host
Answer: A,B,D
Explanation:
If Consul does not return a value for a DNS lookup, it means that there are no healthy instances of that service available or the service doesn't exist in Consul. Instances of a service can be removed if a service or host health check fails, although that instance is still registered to Consul but will not be returned. If the service is manually deregistered from Consul, the DNS query will fail as well since it's no longer registered with the Consul registry.
https://learn.hashicorp.com/tutorials/consul/service-registration-health-checks

4.Consul uses a gossip protocol that is powered by Serf.
How is this communication protected between all participating servers and clients?
A. shared secret
B. TLS
C. username and password
D. mutual TLS
Answer: A
Explanation:
Consul's gossip protocol is protected by a symmetric key, or a shared secret, that is configured as part of the configuration file or in a separate file that is read when the Consul service starts. For example, you can add the parameter "encrypt" to the configuration file with 32-byte, Base64 encoded shared secret. All nodes in the Consul cluster, including WAN joined datacenters, must use the same encryption key. An example of this key would be pUqJrVyVRj5jsiYEkM/tFQYfWyJIv4s3XkvDwy7Cu5s= Furthermore, you can generate this 32-byte, Base64 encoded shared secret by using the built-in command consul keygen
$ consul keygen

pUqJrVyVRj5jsiYEkM/tFQYfWyJIv4s3XkvDwy7Cu5s=
More information about the gossip encryption can be found here.
By the way, the HashiCorp Learn platform mentioned that the key is 16-bytes, but that was changed sometime in 2019 in order for Serf to encrypt data using AES256

5.True or False? After executing the command below, the two registered services (front-end & inventory) will be able to communicate, assuming all other configurations are correct? consul intention create front-end inventory
A. True
B. False
Answer: A
Explanation:
When creating an intention, the default action is Allow, therefore the configuration above will permit the front-end service and the inventory service for communication.
To create a Deny intention, use the -deny flag when running the command (i.e, consul intention create front-end inventory -deny)