HashiCorp Certified: Consul Associate (002)

Credential validity and objective overview

HashiCorp

HashiCorp Certified: Consul Associate (002)

Credentials (badge and certificate) are valid until their stated expiration date

The HashiCorp Certified: Consul Associate 002 exam version was retired in May 2024. However, the credentials associated with this exam are still a valid indication of one's certification status until their expiration date.

Consul Associate 002 exam objectives

#	Objective description
1	**Explain Consul architecture**
1a	Identify the components of Consul datacenter, including agents and communication protocols
1b	Prepare Consul for high availability and performance
1c	Identify Consul's core functionality
1d	Differentiate agent roles
2	**Deploy a single datacenter**
2a	Start and manage the Consul process
2b	Interpret a Consul agent configuration
2c	Configure Consul network addresses and ports
2d	Describe and configure agent join and leave behaviors
3	**Register services and use service discovery**
3a	Interpret a service registration
3b	Differentiate ways to register a single service

3c	Interpret a service configuration with health check
3d	Check the service catalog status from the output of the DNS/API interface or via the Consul UI
3e	Interpret a prepared query
3f	Use a prepared query
4	**Access the Consul key/value (KV)**
4a	Understand the capabilities and limitations of the KV store
4b	Interact with the KV store using both the Consul CLI and UI
4c	Monitor KV changes using `watch`
4d	Monitor KV changes using `envconsul` and `consul-template`
5	**Back up and restore**
5a	Describe the content of a snapshot
5b	Back up and restore the datacenter
5c	[Enterprise] Describe the benefits of snapshot agent features
6	**Use Consul service mesh**
6a	Understand Consul Connect service mesh high level architecture
6b	Describe configuration for registering a service proxy
6c	Describe intentions for Consul Connect service mesh
6d	Check intentions in both the Consul CLI and UI
7	**Secure agent communication**
7a	Understanding Consul security/threat model
7b	Differentiate certificate types needed for TLS encryption
7c	Understand the different TLS encryption settings for a fully secure datacenter
8	**Secure services with basic access control lists (ACL)**
8a	Set up and configure a basic ACL system
8b	Create policies

8c	Manage token lifecycle: multiple policies, token revoking, ACL roles, service identities
8d	Perform a CLI request using a token
8e	Perform an API request using a token
9	**Use gossip encryption**
9a	Understanding the Consul security/threat model
9b	Configure gossip encryption for the existing data center
9c	Manage the lifecycle of encryption keys

HashiCorp

USA Headquarters

101 Second St., Suite 700, San Francisco, CA, 94105
www.hashicorp.com