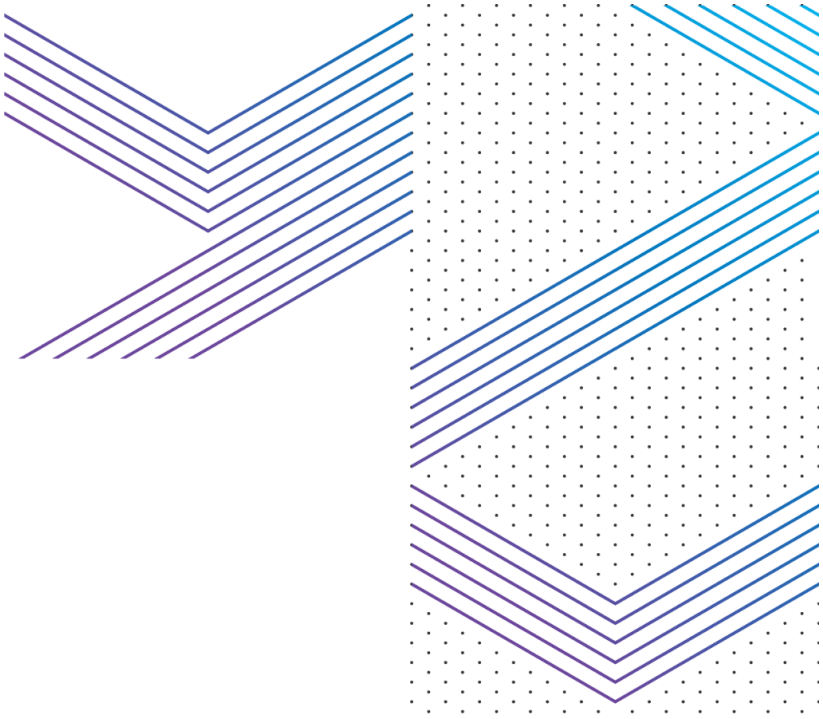


HashiCorp Certified: Consul Associate (003)

Credential validity and objective overview

HashiCorp

HashiCorp Certified: Consul Associate (003)

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

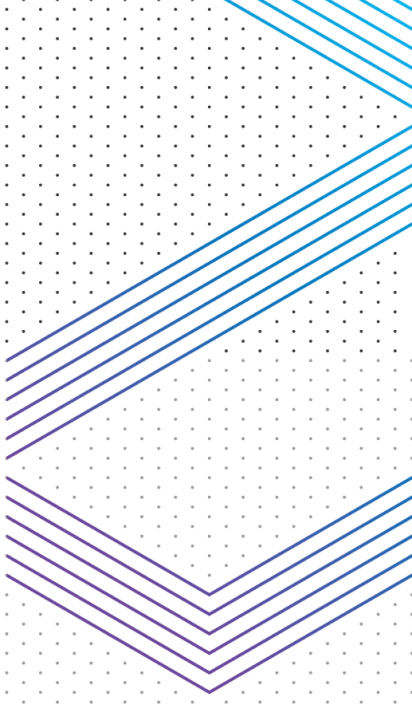
The HashiCorp Certified: Consul Associate (003) exam version was retired in July 2026. However, the credentials associated with this exam are still a valid indication of one's certification status until their expiration date.

Consul Associate 003 exam objectives

#	Objective description
1	**Understand the pillars of service networking**
1a	Understand how Consul discovers, tracks, and monitors the health of services
1b	Explain how Consul secures service to service communication
1c	Summarize how Consul controls access to services at point of entry
1d	Discus how Consul automates networking tasks
2	**Describe Consul architecture**
2a	Identify Consul datacenter components including agents and communication protocols options

2b	Review Consul server high availability & scalability options
2c	Differentiate between server agents and data plane components (client agents and Consul Dataplane)
2d	Understand that Consul can run on multiple platforms
3	**Deploy a single datacenter**
3a	Configure, bootstrap, and start Consul server agents
3b	Configure and start Consul client agents
3c	Configure and start Consul on Kubernetes
3d	Explain Consul agent join methods and behavior
4	**Register services and use service discovery**
4a	Interpret a service registration
4b	Differentiate between service registration methods
4c	Understand service health check configuration options and behaviors
4d	Query Consul's service catalog via CLI, API, UI, and/or DNS, and interpret the results
4e	Interpret & use prepared queries
5	**Use Consul service mesh**
5a	Consider high level architecture & key benefits of Consul service mesh
5b	Understand Consul service mesh intentions & when to use them
5c	Apply proxy configurations options within Consul service mesh

6	**Secure agent communication**
6a	Understand Consul security/threat model
6b	Differentiate certificate types needed for TLS encryption
6c	Interpret TLS encryption settings & intended use
6d	Configure gossip encryption
7	**Secure services with basic access control lists (ACLs)**
7a	Understand Consul ACL system components and usage
7b	Create and configure ACL policies and tokens
7c	Use ACL tokens to communicate securely with Consul services and agents
8	**Secure and connect service mesh applications**
8a	Use Consul gateways to securely connect and access services into, out of, and within the service mesh
8b	Understand how to enable communication between multiple Consul datacenters
9	**Monitor Consul**
9a	Describe Consul service mesh observability
9b	Review Consul datacenter observability
10	**Operate and maintain Consul**
10a	Manage Consul servers
10b	Maintain Consul communications security
10c	Backup and restore Consul cluster state
10d	Understand Consul datacenter troubleshooting options



USA Headquarters

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