





HashiCorp
Consul


Objective 8 - Secure Services with ACLs




Objective 8a: Set up and configure a basic ACL system




Objective 8b: Create policies



Objective 8c: Manage token lifecycle: multiple policies, token revoking, ACL roles, service identities



Objective 8d: Perform a CLI request using a token



Objective 8e: Perform an API request using a token



Getting Started with HashiCorp Consul

Created by Bryan Krausen

- optional ACL system
 - control access to data and API
 - uses tokens associated with policies
 - must be enabled in the Agent config file
 - configuration includes default policy and other parameters
 - includes config on both servers and clients

- policies
 - grouping of rules that can be used and associated with tokens
 - multiple policies can be created as needed

- tokens
 - aka bearer token
 - includes an Accessor (name/id)
 - includes a Secret ID (actual token)

- roles
 - grouping of a set of policies and service identities
 - can be applied to many tokens

- service identities
 - used for Service Mesh
 - policy template to link a policy
 - used at authorized to allow a service and sidecar to access services and features in Consul

- bootstrapping the ACL system
 - creates the bootstrap and anonymous token
 - required before ACL system can be used
 - only done one time
 - there is a "reset" feature if bootstrap token is lost
 - default policy should be set to allow during bootstrapping process
 - all actions require a token after the default policy is set to deny
 - eventually you need to set default policy as deny after updating agent configurations with the proper token

- default policies
 - global management
 - namespace-management
- define different resources available to create rules
 - differentiate between <resource> and <resource>_prefix
 - node identities in a policy
- policies are attached to a token
 - multiple policies can be attached to a single token (combination of permissions)
- consul acl policy create
- creating a policy for the anonymous token

- consul acl token create
 - create token attached to policy
 - create a token with multiple policies
 - add a description
 - clone
 - delete
 - list
 - read
 - update
- default tokens
 - bootstrap (aka master)
 - always ID 00000000-0000-0000-0000-000000000001
 - anonymous
 - always ID 00000000-0000-0000-0000-000000000002

- set the CONSUL_HTTP_TOKEN environment variable
- set the CONSUL_HTTP_TOKEN_FILE environment variable
- reference token value stored in a file using the -token-file flag
- using the -token flag when issuing a command

- set the token using the X-Consul-Token header in the API request
- set the token using the Authorization: Bearer header in the API request