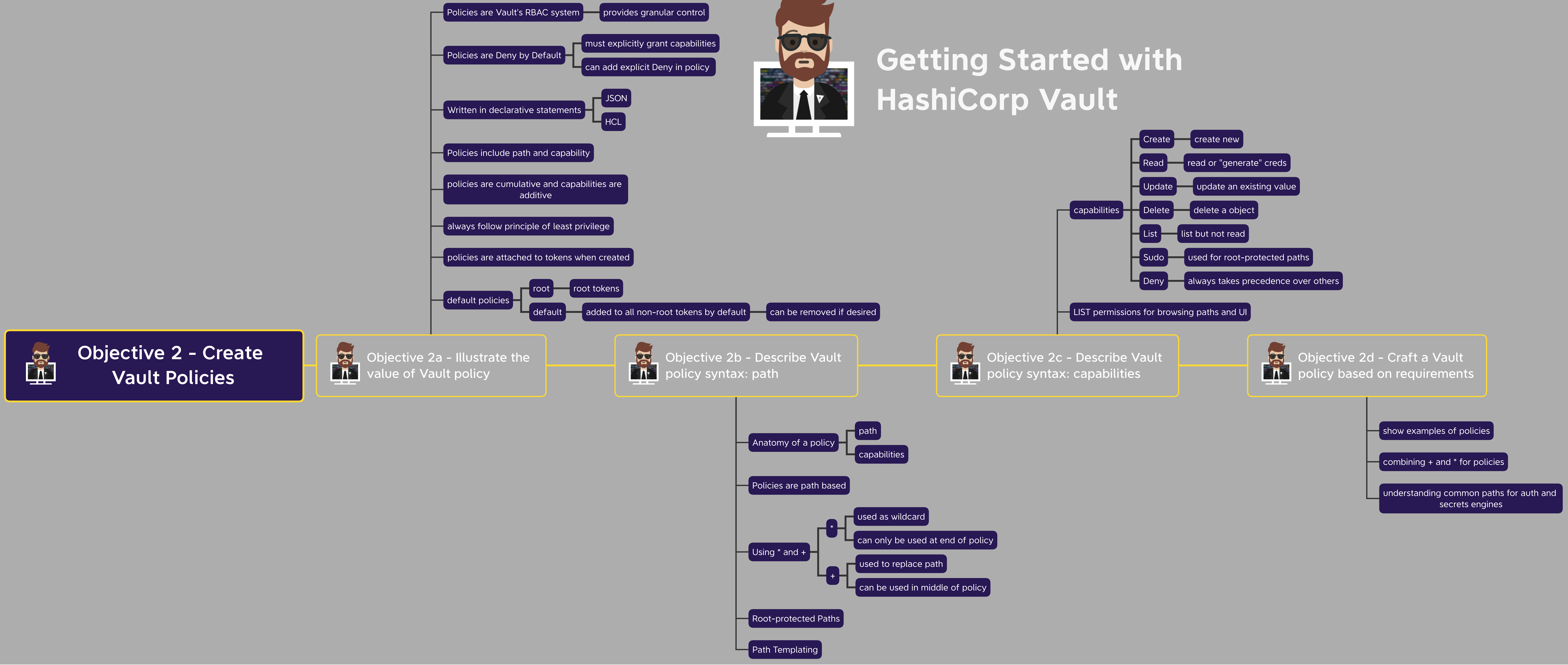
Getting Started with HashiCorp Vault



Objective 2 - Create Vault Policies

- Objective 2a - Illustrate the value of Vault policy
  - Policies are Vault's RBAC system
    - provides granular control
  - Policies are Deny by Default
    - must explicitly grant capabilities
    - can add explicit Deny in policy
  - Written in declarative statements
    - JSON
    - HCL
  - Policies include path and capability
  - policies are cumulative and capabilities are additive
  - always follow principle of least privilege
  - policies are attached to tokens when created
  - default policies
    - root
      - root tokens
    - default
      - added to all non-root tokens by default
        - can be removed if desired
- Objective 2b - Describe Vault policy syntax: path
  - Anatomy of a policy
    - path
    - capabilities
  - Policies are path based
  - Using * and +
    - *
      - used as wildcard
      - can only be used at end of policy
    - +
      - used to replace path
      - can be used in middle of policy
  - Root-protected Paths
  - Path Templating
- Objective 2c - Describe Vault policy syntax: capabilities
  - capabilities
    - Create
      - create new
    - Read
      - read or "generate" creds
    - Update
      - update an existing value
    - Delete
      - delete a object
    - List
      - list but not read
    - Sudo
      - used for root-protected paths
    - Deny
      - always takes precedence over others
  - LIST permissions for browsing paths and UI
- Objective 2d - Craft a Vault policy based on requirements
  - show examples of policies
  - combining + and * for policies
  - understanding common paths for auth and secrets engines