Getting Started with HashiCorp Vault
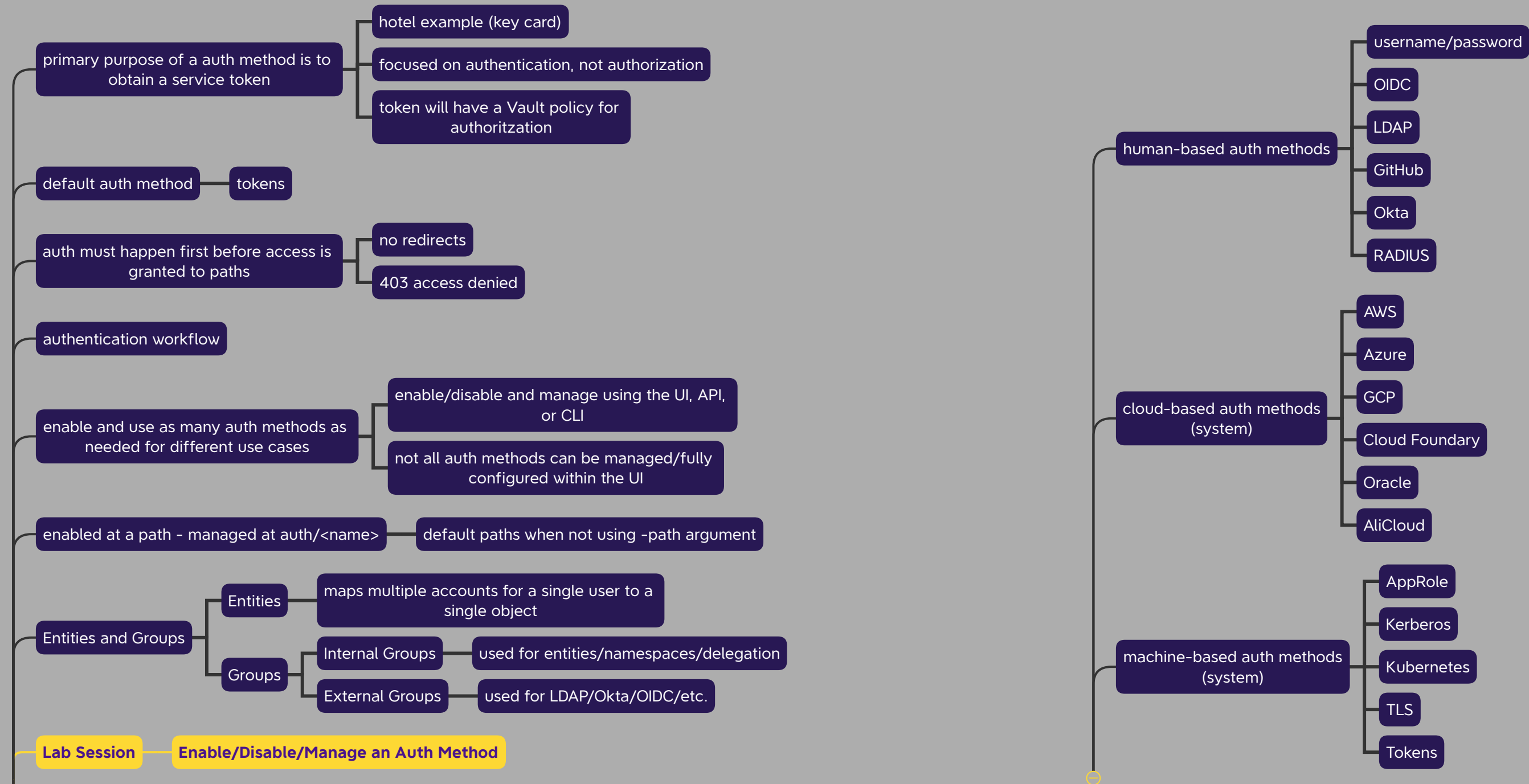
Objective 1 - Compare Authentication Methods

Objective 1a - Describe Authentication Methods

- primary purpose of a auth method is to obtain a service token
  - hotel example (key card)
  - focused on authentication, not authorization
  - token will have a Vault policy for authoritzation
- default auth method — tokens
- auth must happen first before access is granted to paths
  - no redirects
  - 403 access denied
- authentication workflow
- enable and use as many auth methods as needed for different use cases
  - enable/disable and manage using the UI, API, or CLI
  - not all auth methods can be managed/fully configured within the UI
- enabled at a path - managed at auth/<name> — default paths when not using -path argument
- Entities and Groups
  - Entities — maps multiple accounts for a single user to a single object
  - Groups
    - Internal Groups — used for entities/namespaces/delegation
    - External Groups — used for LDAP/Okta/OIDC/etc.
- **Lab Session** — **Enable/Disable/Manage an Auth Method**

Objective 1b - Choose an Authentication Method based on Use Case

- automation
  - AppRole
  - k8s
  - Cloud Foundary
- cloud-based request
  - AWS
  - Azure
  - GCP
- UI/CLI auth
  - GitHub
  - LDAP — Active Directory
  - Okta
  - JWT/OIDC
    - AzureAD
    - Ping Federate

Objective 1c - Differentiate human vs. system auth methods

- human-based auth methods
  - username/password
  - OIDC
  - LDAP
  - GitHub
  - Okta
  - RADIUS
- cloud-based auth methods (system)
  - AWS
  - Azure
  - GCP
  - Cloud Foundary
  - Oracle
  - AliCloud
- machine-based auth methods (system)
  - AppRole
  - Kerberos
  - Kubernetes
  - TLS
  - Tokens

Lab Sessions and Examples

- AppRole
- AWS
- UserPass
- LDAP
- Okta (if I can get test instance)