Interpret Vault Identity Entities and Groups

Vault Entities

- Vault creates an entity and attaches an alias to it if a corresponding entity doesn't already exist.
  - This is done using the Identity secrets engine, which manages internal identities that are recognized by Vault

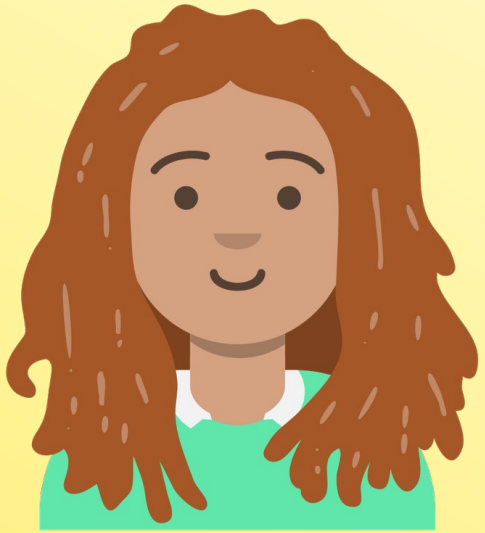
- An entity is a representation of a single person or system used to log into Vault. Each has a unique value. Each entity is made up of zero or more aliases

- Alias is a combination of the auth method plus some identification. It is a mapping between an entity and auth method(s)

Vault Entities

Vault
CERTIFIED OPERATIONS PROFESSIONAL

Julie Smith
Finance Specialist



UserPass

alias

entity_id

UserPass: jsmith

Entity_ID: b81de864-75fa-5619-1fca-ddd72bbe5b29

department: finance
office: San Francisco
team: accounts-payable

accounting

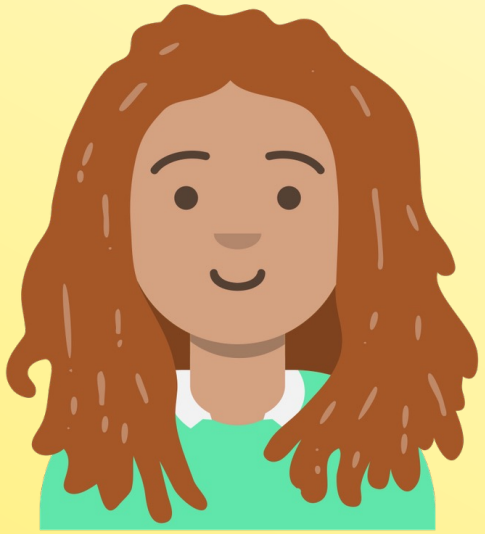
metadata

policy

Vault Entities

Julie Smith

Finance Specialist



Auth Options:

UserPass
LDAP
GitHub

UserPass: jsmith
Entity_ID: b81de864-75fa-5619-1fca-ddd72bbe5b29

department: accounting
sub-team: accounts-payable

accounting

LDAP: jsmith@example.com
Entity_ID: e93d24b2a-b894-0998-43ce-4294cb9ea9b

department: finance
team: management

finance

GitHub: jsmith22
Entity_ID: 4c9ed3482-4894-ced9-a1b2-90344be93aa

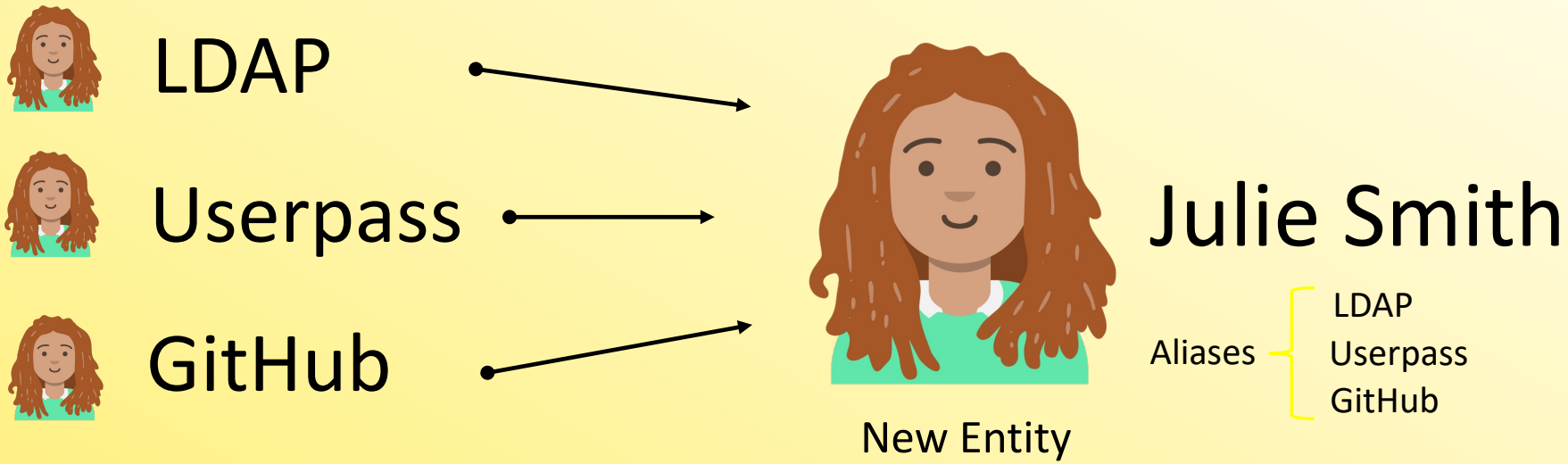
location: us
sales-region: west

accounts payable

Vault Entities

- An entity can be manually created to map multiple entities for a single user to provide more efficient authorization management

- Any tokens that are created for the entity inherit the capabilities that are granted by alias(es).



Vault Entities

Entity

Name: Julie Smith
Entity_ID: e48de234-58fa-0093-5fde-e5b99abe8b33
Policy: *management*

Aliases:

GitHub: jsmith22
Entity_ID: 4c9ed3482-4894-ced9-a1b2-90344be93aa
Policy: *finance*

LDAP: jsmith@example.com
Entity_ID: e93d24b2a-b894-0998-43ce-4294cb9ea9b
Policy: *accounting*

UserPass: jsmith
Entity_ID: b81de864-75fa-5619-1fca-ddd72bbe5b29

Aliases

Vault Entities

Name: Julie Smith
Entity_ID: e48de234-58fa-0093-5fde-e5b99abe8b33
Policy: *management*

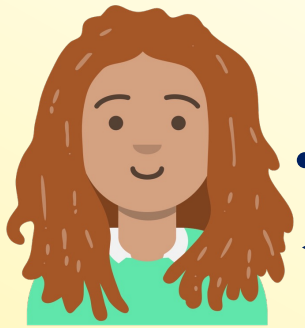
Aliases:

GitHub: jsmith22
Entity_ID: 4c9ed3482-4894-ced9-a1b2-90344be93aa
Policy: *finance*

LDAP: jsmith@example.com
Entity_ID: e93d24b2a-b894-0998-43ce-4294cb9ea9b
Policy: *accounting*

LDAP

2. Validate with LDAP



jsmith@example.com

1. Authenticate with LDAP credentials

3. Return a Vault token

Policies
accounting
management

Token inherits **capabilities** granted by both policies

Create an Entity

TERMINAL

```
$ vault write identity/entity name="Julie Smith" \
     policies="it-management" \
     metadata="organization"="HCVOP, Inc" \
     metadata="team"="management"
```

Add an Alias to an Entity

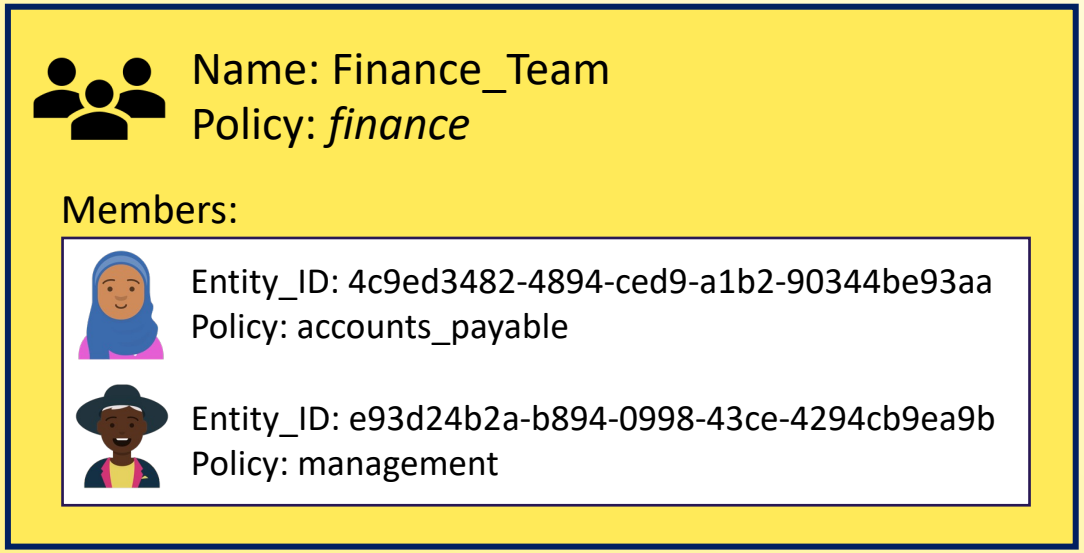
TERMINAL

```
# Add GitHub auth as an alias
$ vault write identity/entity-alias name="jsmith22" \
     canonical_id=<entity_id> \
     mount_accessor=<github_auth_accessor>


# Add LDAP auth as an alias
$ vault write identity/entity-alias \
     name="jsmith@hcvop.com" \
     canonical_id=<entity_id> \
     mount_accessor=<ldap_auth_accessor>
```

Vault Groups

- A group can contain multiple entities as its members.
- A group can also have subgroups.
- Policies can be set on the group and the permissions will be granted to all members of the group.



Vault Groups

Name: Finance_Team
Policy: *finance*

Members:

Name: Maria Shi
Entity_ID: 4c9ed3482-4894-ced9-a1b2-90344be93aa
Policy: *accounts_payable*

Entity Aliases:

Username: maria.shi
Policy: *base-user*

Name: John Lee
Entity_ID: e93d24b2a-b894-0998-43ce-4294cb9ea9b
Policy: *management*

Entity Aliases:

Username: john.lee
Policy: *super-user*

TOKEN

Token inherits **capabilities** granted by alias, entity, and the group

Policies

super-user
management
finance

Vault Groups

Internal Group

Groups created in Vault to group entities to propagate identical permissions

Created Manually

External Group

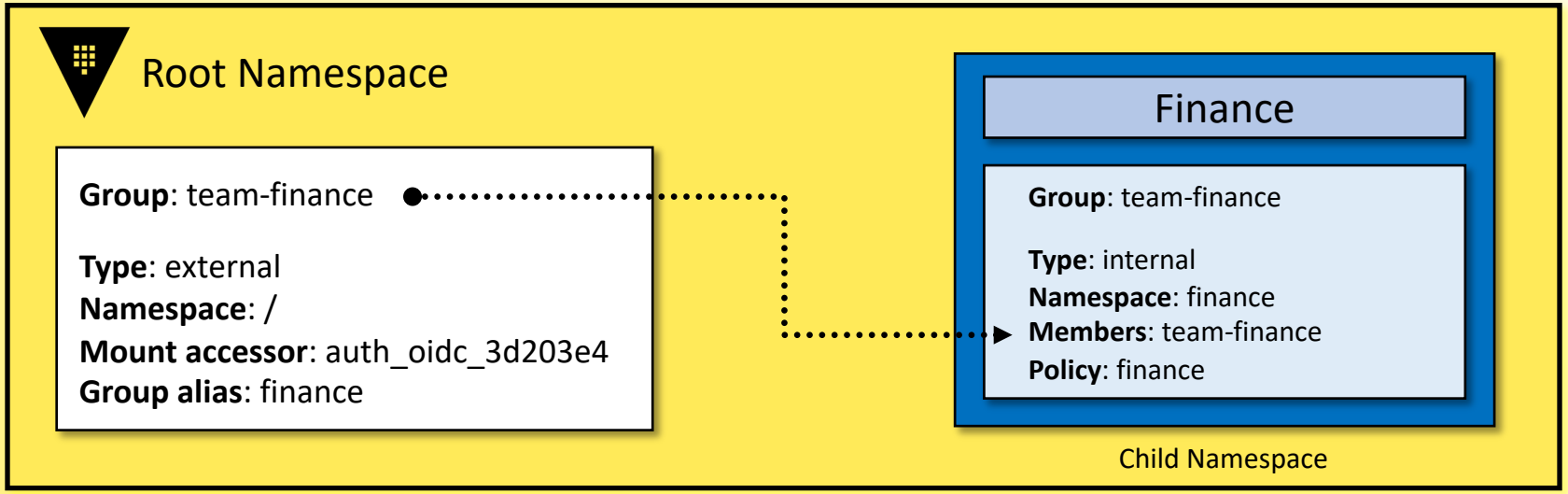
Groups which Vault infers and creates based on group associations coming from auth methods

Created Manually or Automatically

Vault Groups

Internal Groups

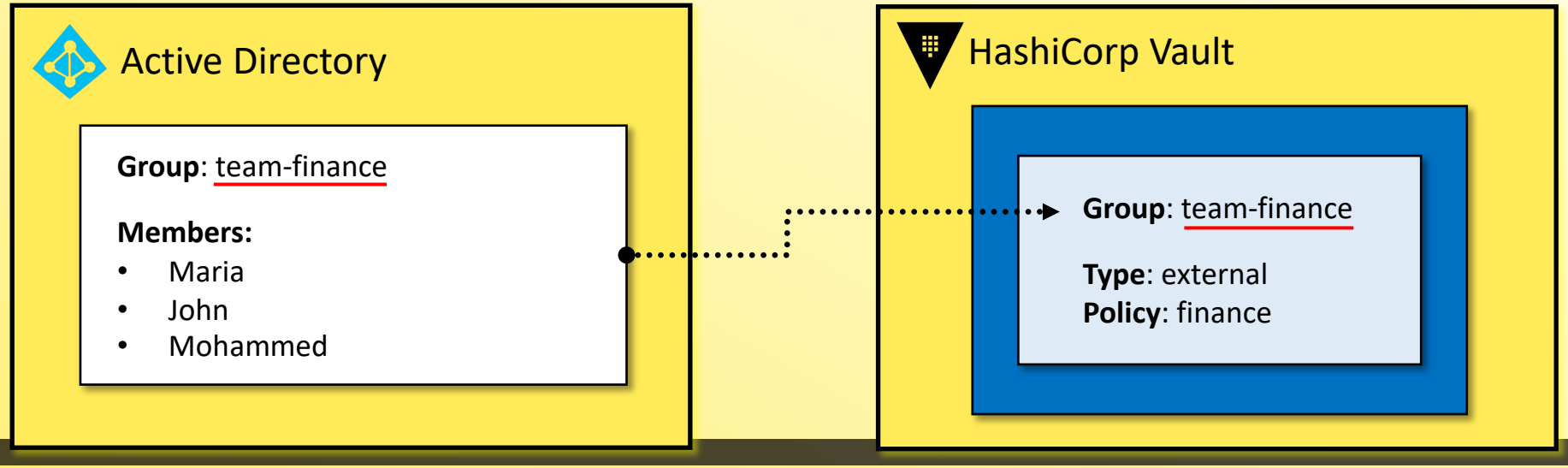
- Internal groups can be used to easily manage permissions for entities
- Frequently used when using Vault Namespaces to propagate permissions down to child namespaces
  - Helpful when you don't want to configure an identical auth method on every single namespace



Vault Groups

External Groups

- External groups are used to set permissions based on group membership from an external identity provider, such as LDAP, Okta, or OIDC provider.
- Allows you to set up once in Vault and continue manage permissions in the identity provider.
  - Note that the group name must match the group name in your identity provider



END OF SECTION

Vault

CERTIFIED OPERATIONS PROFESSIONAL