Vault Tokens for Vault Associate (003)

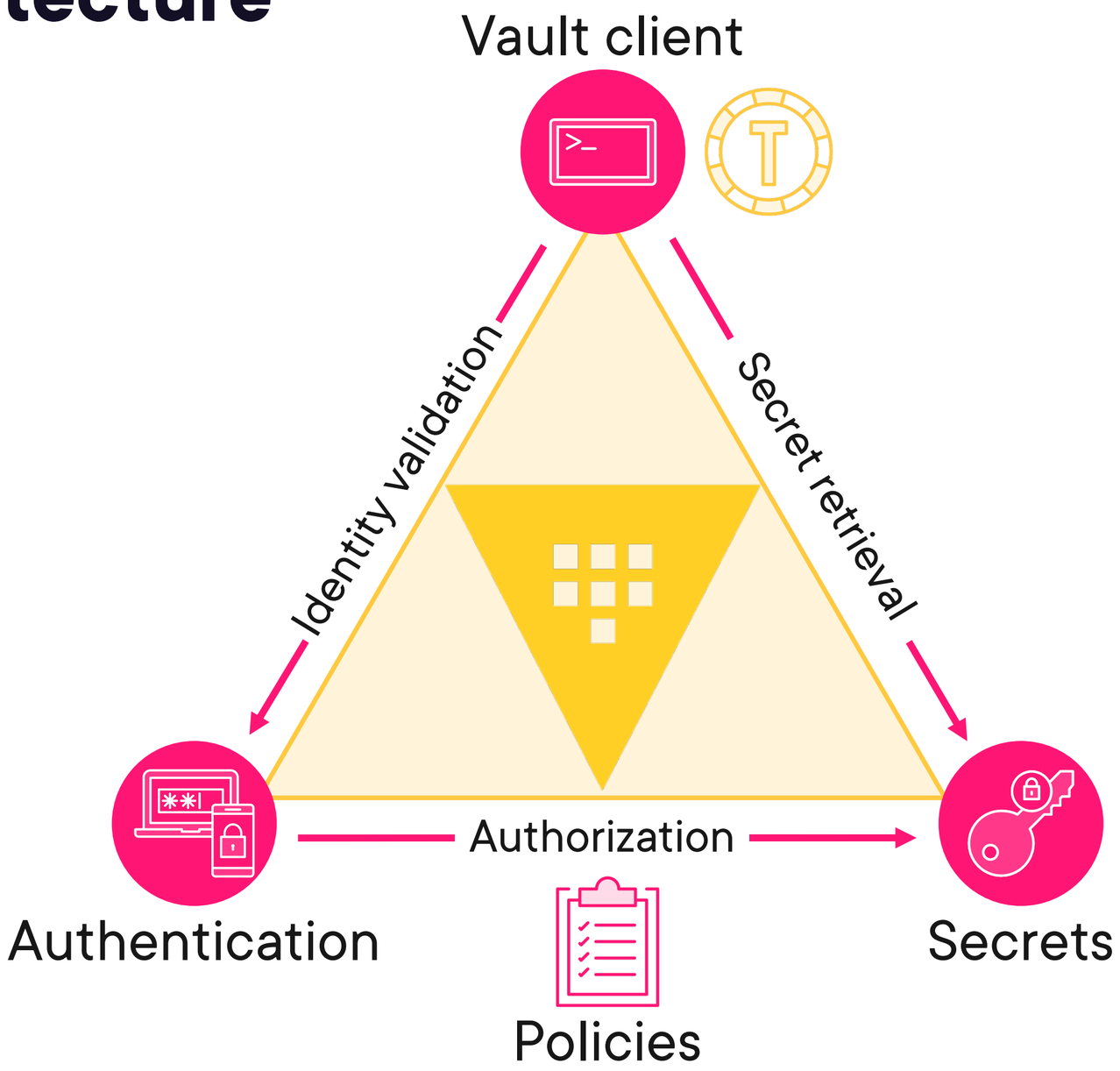
Vault Tokens Overview

Ned Bellavance

HashiCorp Certified Instructor

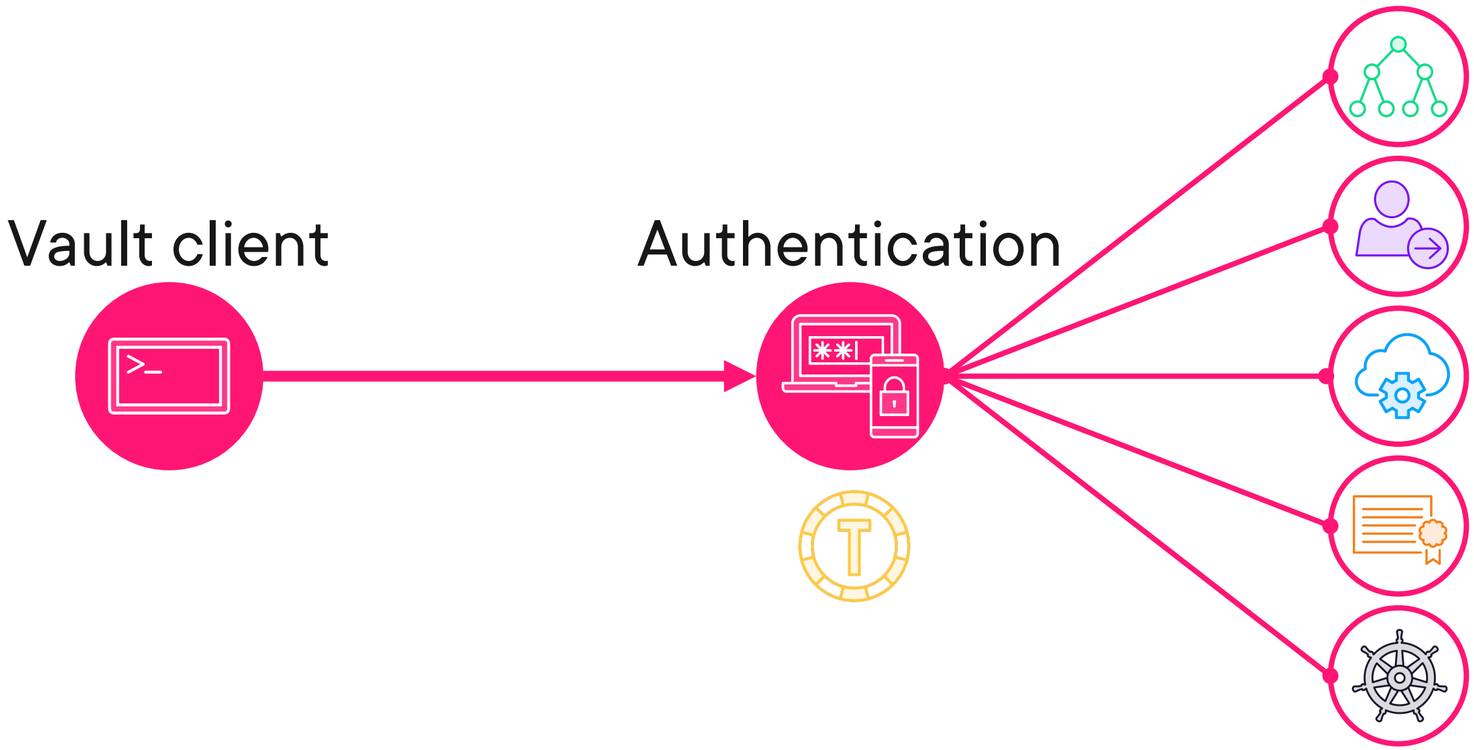
@nedinthecloud | nedinthecloud.com

Vault Architecture

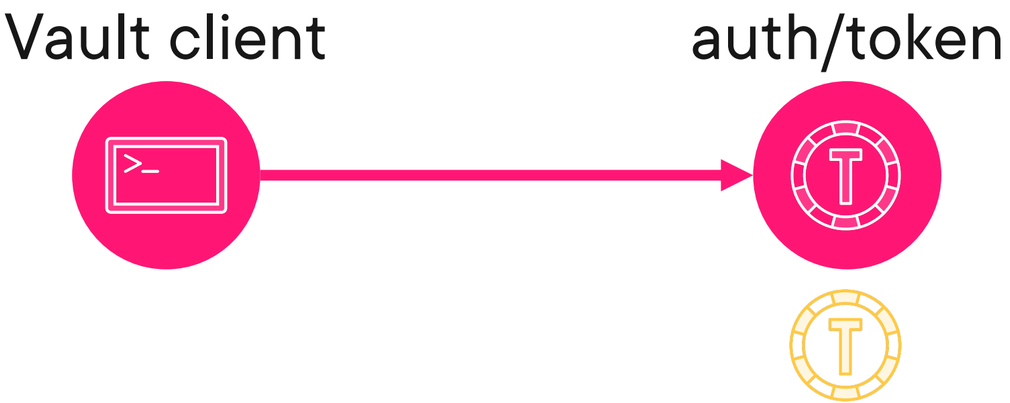


Token Fundamentals

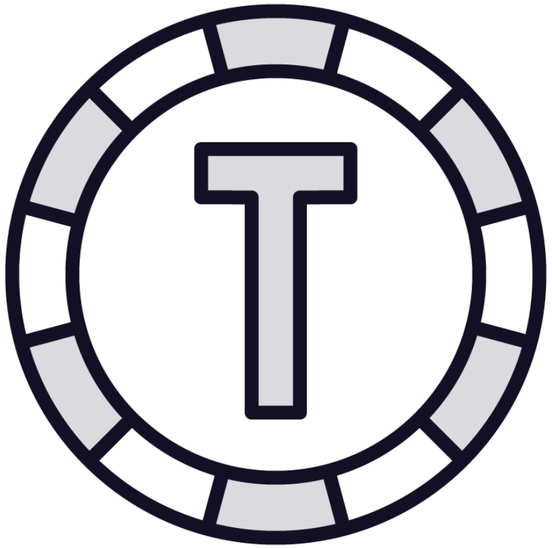
Authentication Methods



Direct Creation



Root Token



Created during Vault initialization

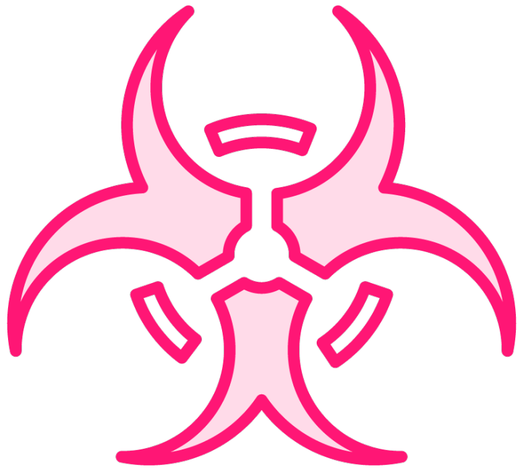
Root policy attached

- Can do ANYTHING

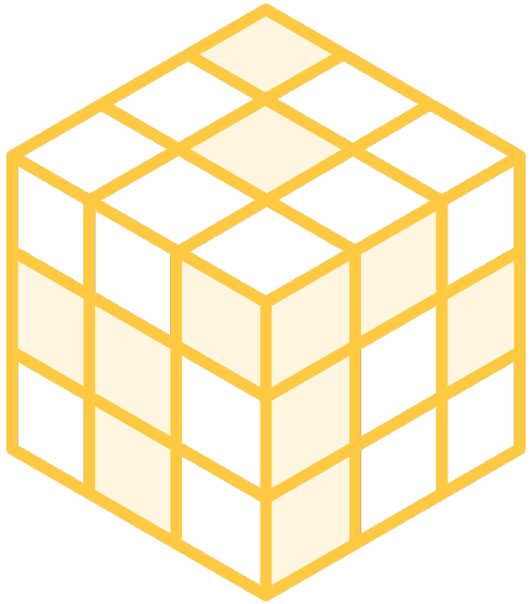
Revoke after setup

Create through special process

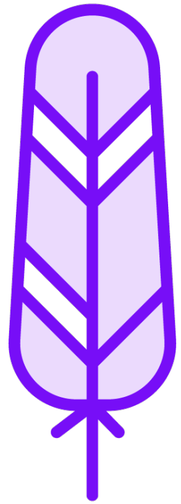
Token Categories



Recovery

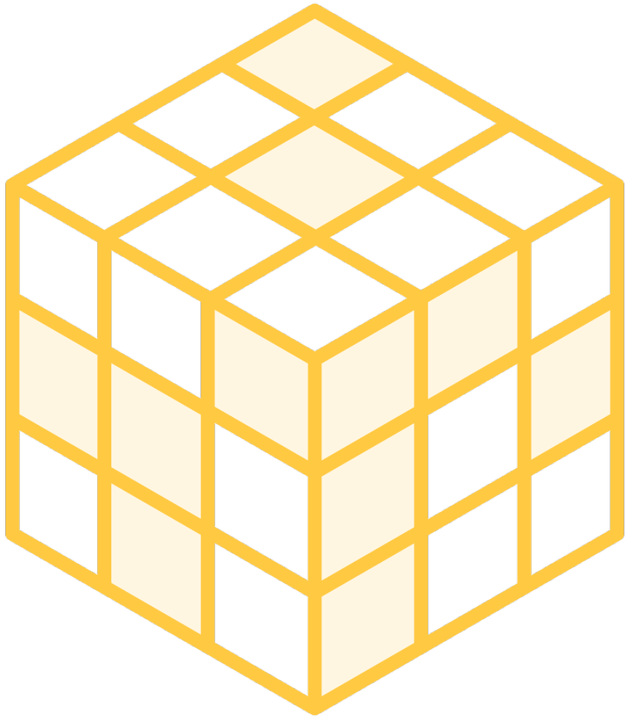


Service



Batch

Service Tokens



Stored in the token auth method

Written to backend storage

Default token type

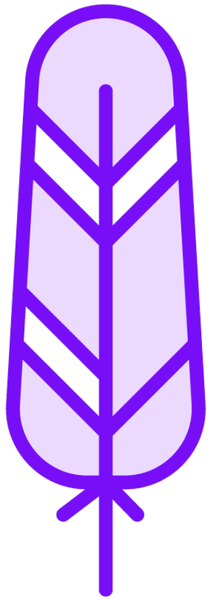
Token prefix

- hvs

Service Token Properties

```
Key                  Value
---                  -----
accessor             Qaxbxud7QaIYWr7IdU1JmsL0
creation_time        1740166449
creation_ttl         768h
display_name         token
entity_id            n/a
expire_time          2025-03-25T15:34:09.1520294-04:00
explicit_max_ttl     0s
id                   hvs.CAESIKoGLaI63IT1S77cfMZ1tWA0eq-
Dr8qWPm1uHUdWWMxlGh4KHGh2cy43YXVDczRIR1VSblQzRHA1cmlYanhPZFk
issue_time           2025-02-21T14:34:09.1520294-05:00
meta                 <nil>
num_uses             0
orphan               false
path                 auth/token/create
policies             [default vault-admins]
renewable            true
ttl                  767h59m30s
type                 service
```

Batch Tokens



Encrypted self-contained blobs

Not stored in the backend

Limited functionality

Used for high-volume creation

Token prefix

- hvb

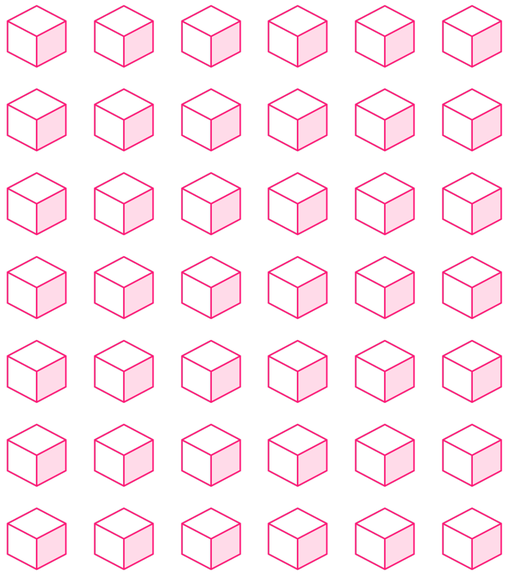
Service Token Properties

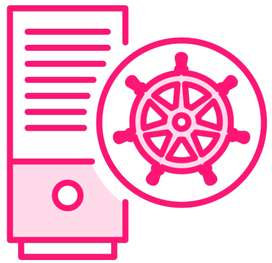
```
Key                  Value
---                  -----
accessor             n/a
creation_time        1740167097
creation_ttl         768h
display_name         token
entity_id            n/a
expire_time          2025-03-25T15:44:57-04:00
explicit_max_ttl     0s
id                   hvb.AAAAAQI35_mFZQ1MFh_iAkO2qcK-
k1uaXlOq7913s_l7CjJgGCMeBSfAdzfFhZ_xqpin_ZJT2cPpqjhB2mFvW0DBbTwf7bEFUSMduvy2TdZ4lnSEID2c34weybsr4wn7A5i88V
rn2Kr0cSkgmHlKlQDkXRwapzo-20IcqKJ7ZxfTF-kjSsk7cnA
issue_time           2025-02-21T14:44:57-05:00
meta                 <nil>
num_uses             0
orphan               false
path                 auth/token/create
policies             [default vault-admins]
renewable            false
ttl                  767h59m49s
type                 batch
```

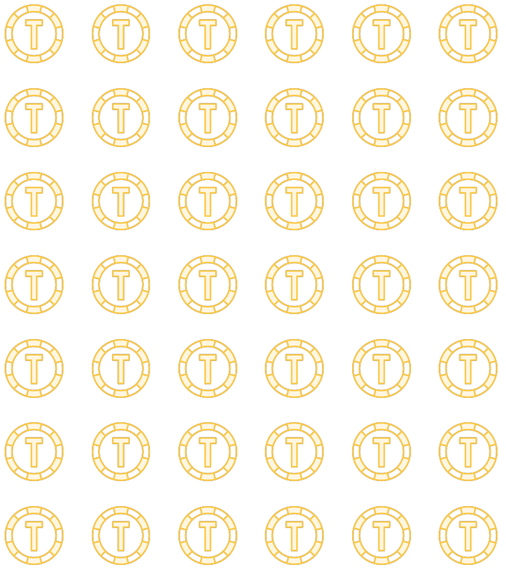
Service and Batch Token Comparison

Feature	Service	Batch
Can be root token	Yes	No
Can create child token	Yes	No
Can be renewable	Yes	No
Manually revocable	Yes	No
Can be periodic	Yes	No
Can have explicit max TTL	Yes	No
Has accessor	Yes	No
Has cubbyhole	Yes	No
Revoked with parent (not orphan)	Yes	Stops working
Dynamic secrets lease assignment	Self	Parent
Creation scales with Performance Standby	No	Yes
Can be used across Performance clusters	No	Yes
Cost	Heavyweight	Lightweight

Batch Token Use Case







Batch Token Use Case