Vault Leases for Vault Associate (003)

Vault Leases Overview
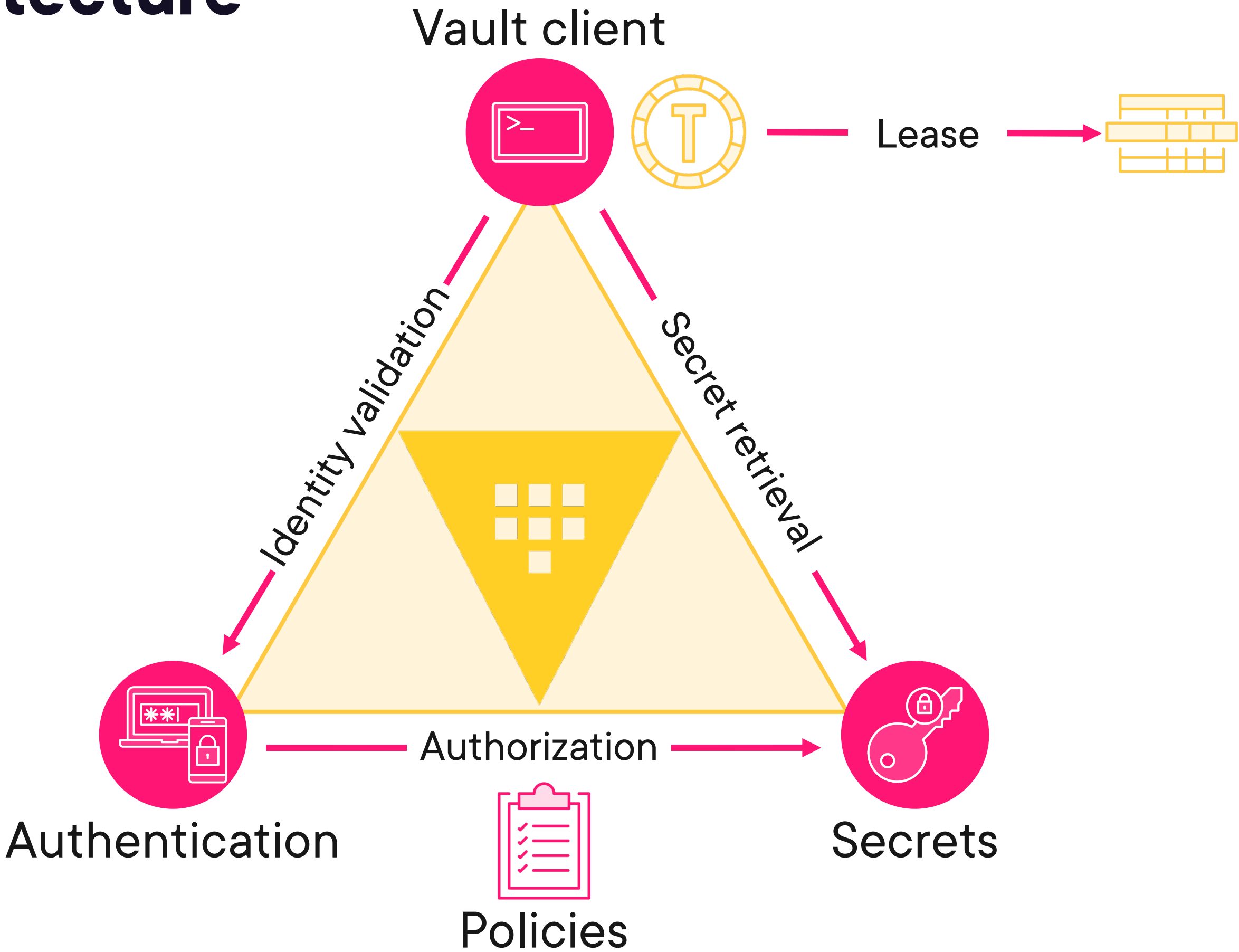
Ned Bellavance

HashiCorp Certified Instructor
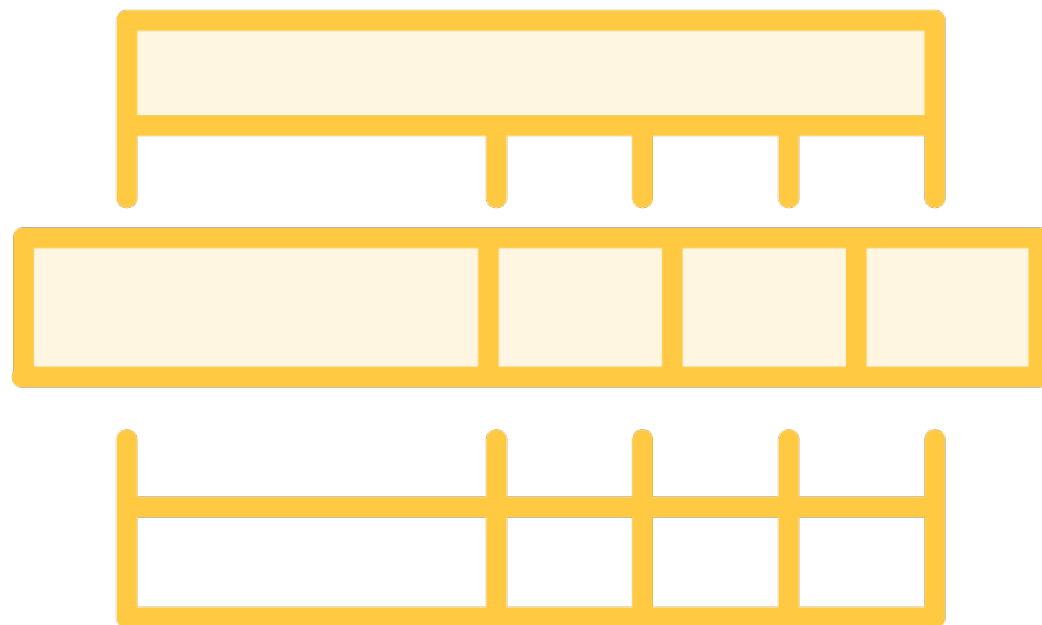
@nedinthecloud | nedinthecloud.com

Vault Architecture

Vault client

Lease

Identity validation

Secret retrieval

Authentication

Authorization

Secrets

Policies

Vault Leases

Created with dynamic secrets or non-root tokens

Guarantee of validity from Vault

Tokens managed through auth method

Focus on dynamic secrets

Lease ID
- Similar to token accessor
- Used to interact with lease

Lease Properties

```
Key                Value
---                -----
expire_time        2025-02-24T15:01:22.9931487-05:00
id                 database/creds/readonly/y0pnZCQjG3yQlbmBqgkYm5iM
issue_time         2025-02-24T14:01:22.9931487-05:00
last_renewal       <nil>
renewable          true
ttl                59m48s
```
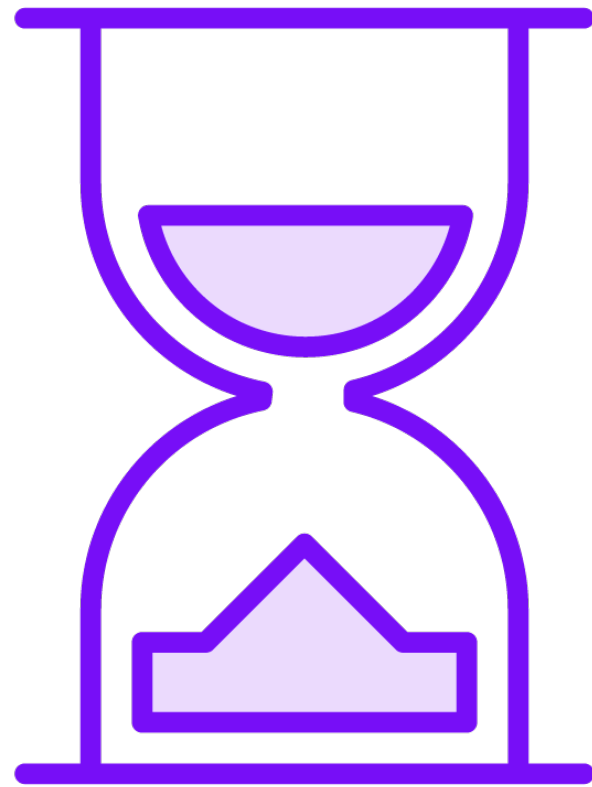
Lease Time-to-live

All leases have a TTL

TTL is an absolute value

Lease expires when TTL runs out

Max TTL

Maximum lifetime based on creation time

Max TTL sources
- System max TTL
- Secrets engine max TTL
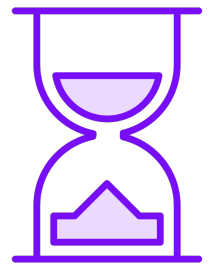- Object max TTL

Most stringent wins
- Object cannot be longer than secrets engine
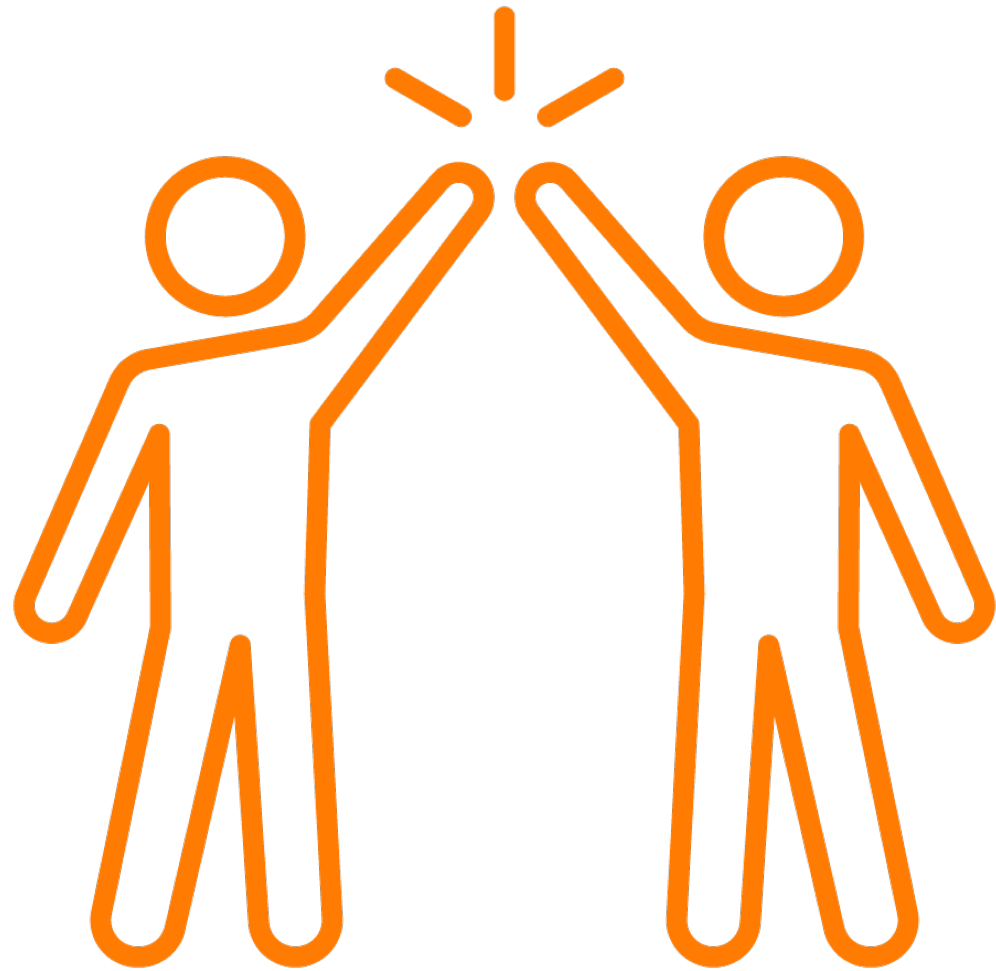
Lease Renewal

Renewal extends TTL

Cannot exceed max TTL

Evaluated during renewal

Tokens and Leases

Leases guarantee validity

Secret or token purges at expiry

Token expiry managed by auth method

Secret expiry
- Secrets engine settings
- Requestor token lifetime

Tokens and leases work together