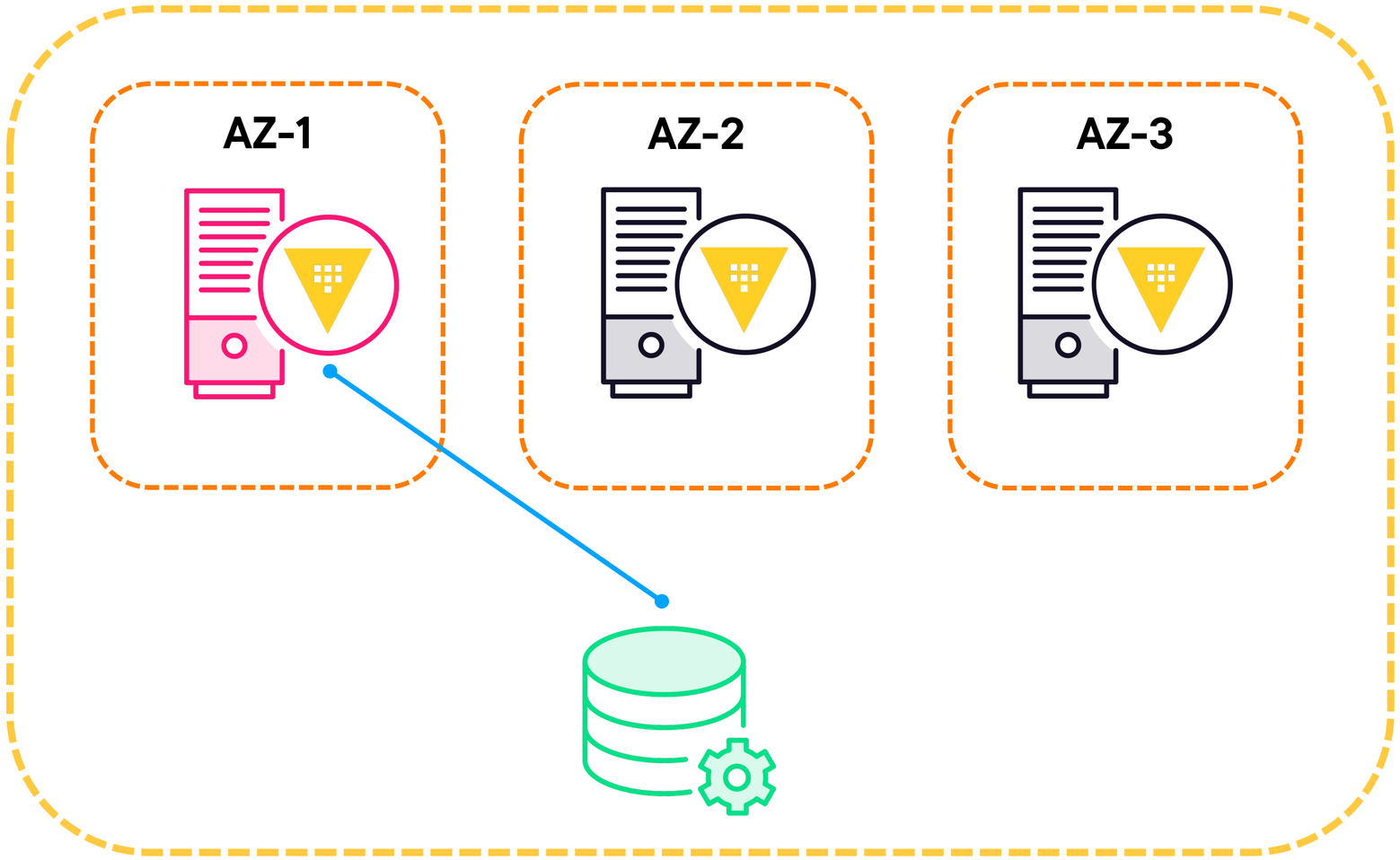
Vault Clustering

Ned Bellavance

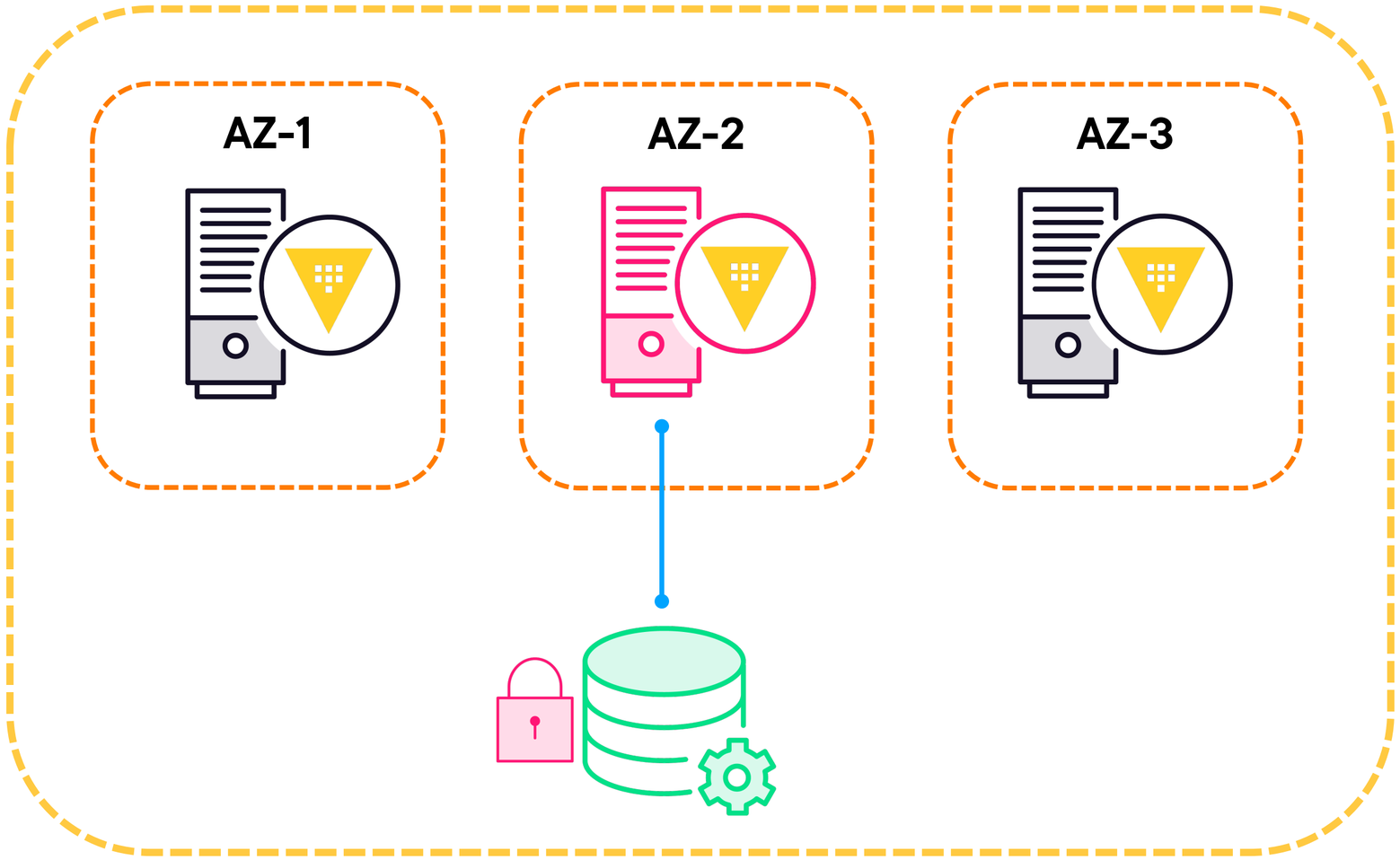
HashiCorp Certified Instructor

@nedinthecloud | nedinthecloud.com

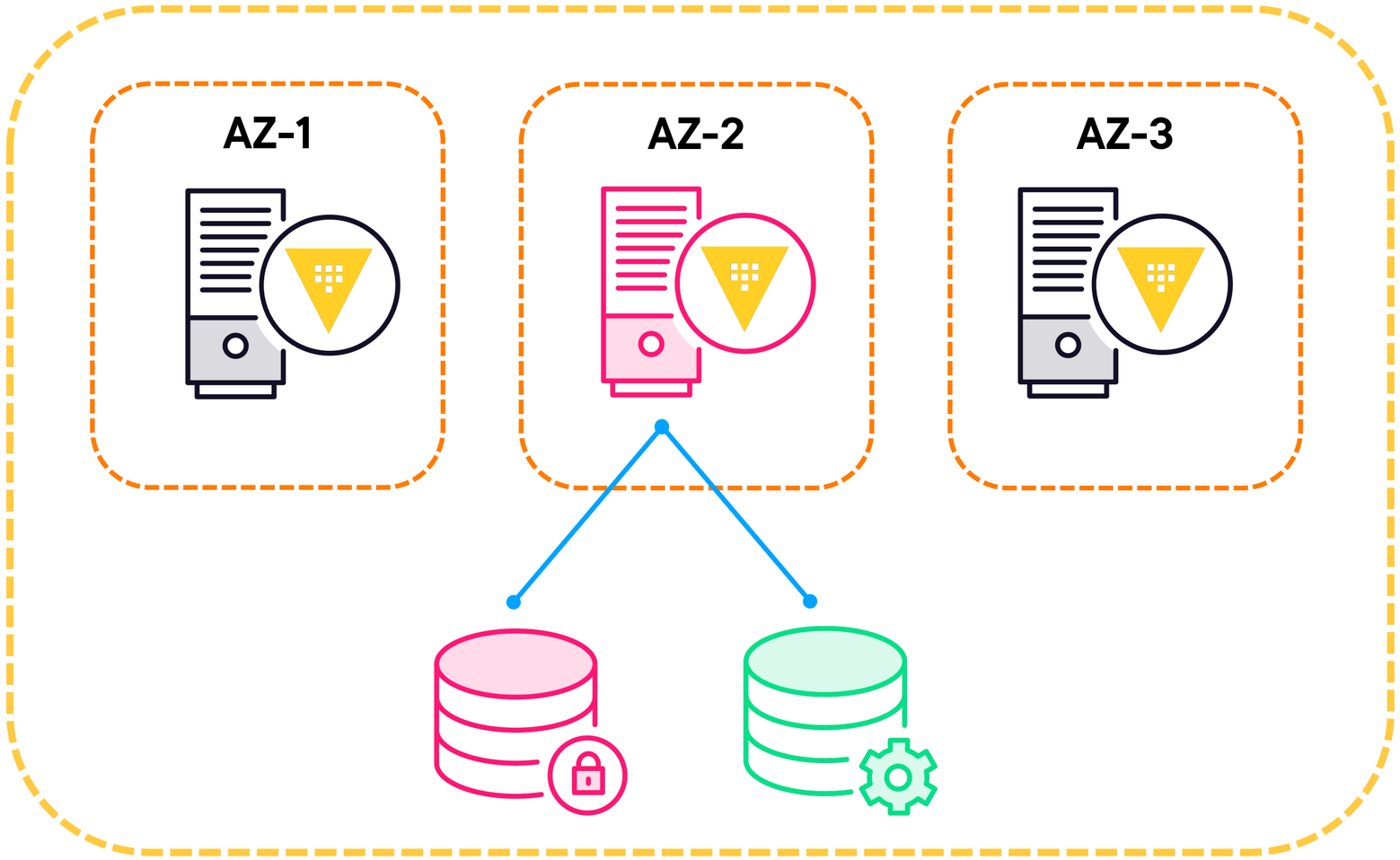
Vault Cluster



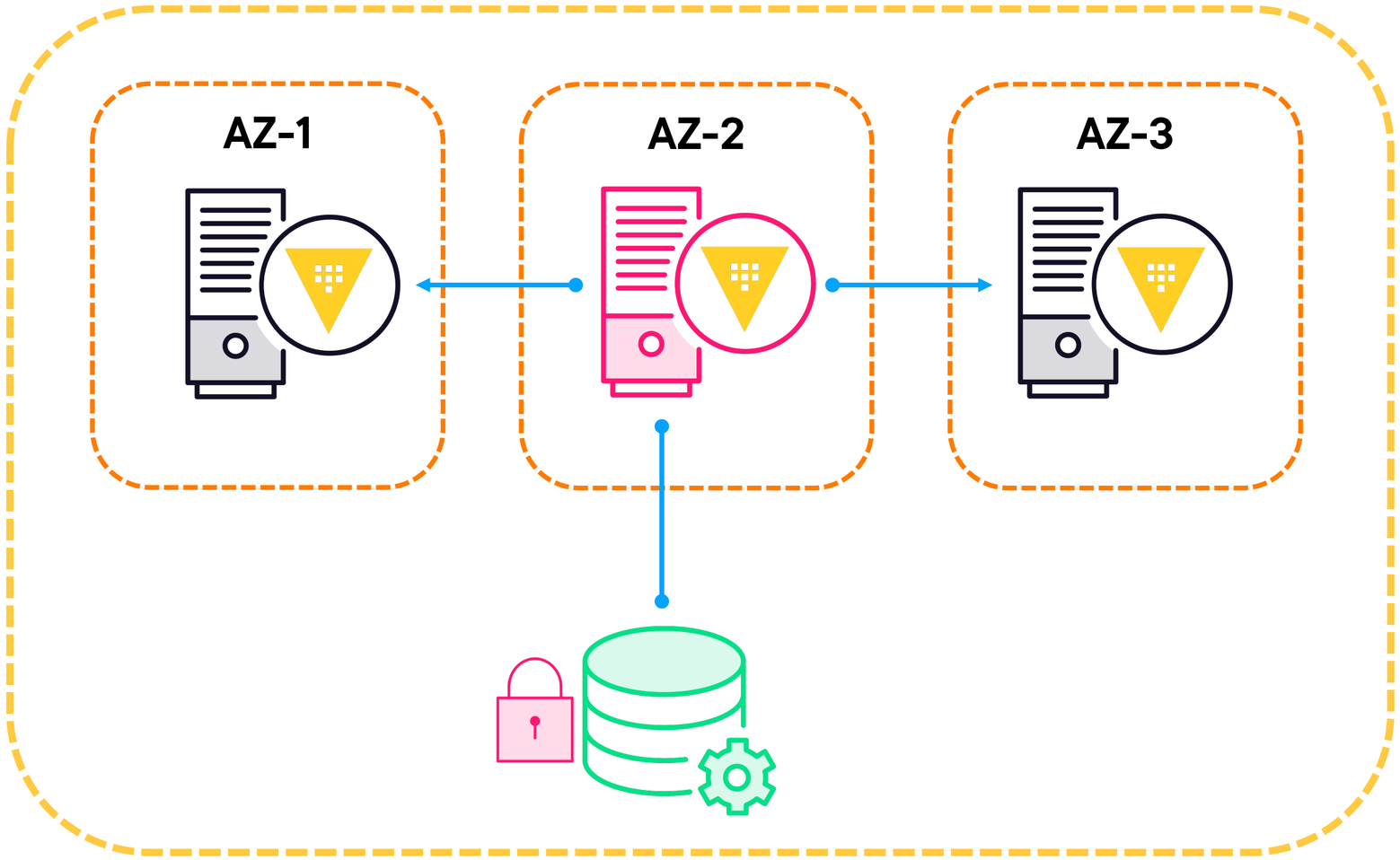
Vault Cluster



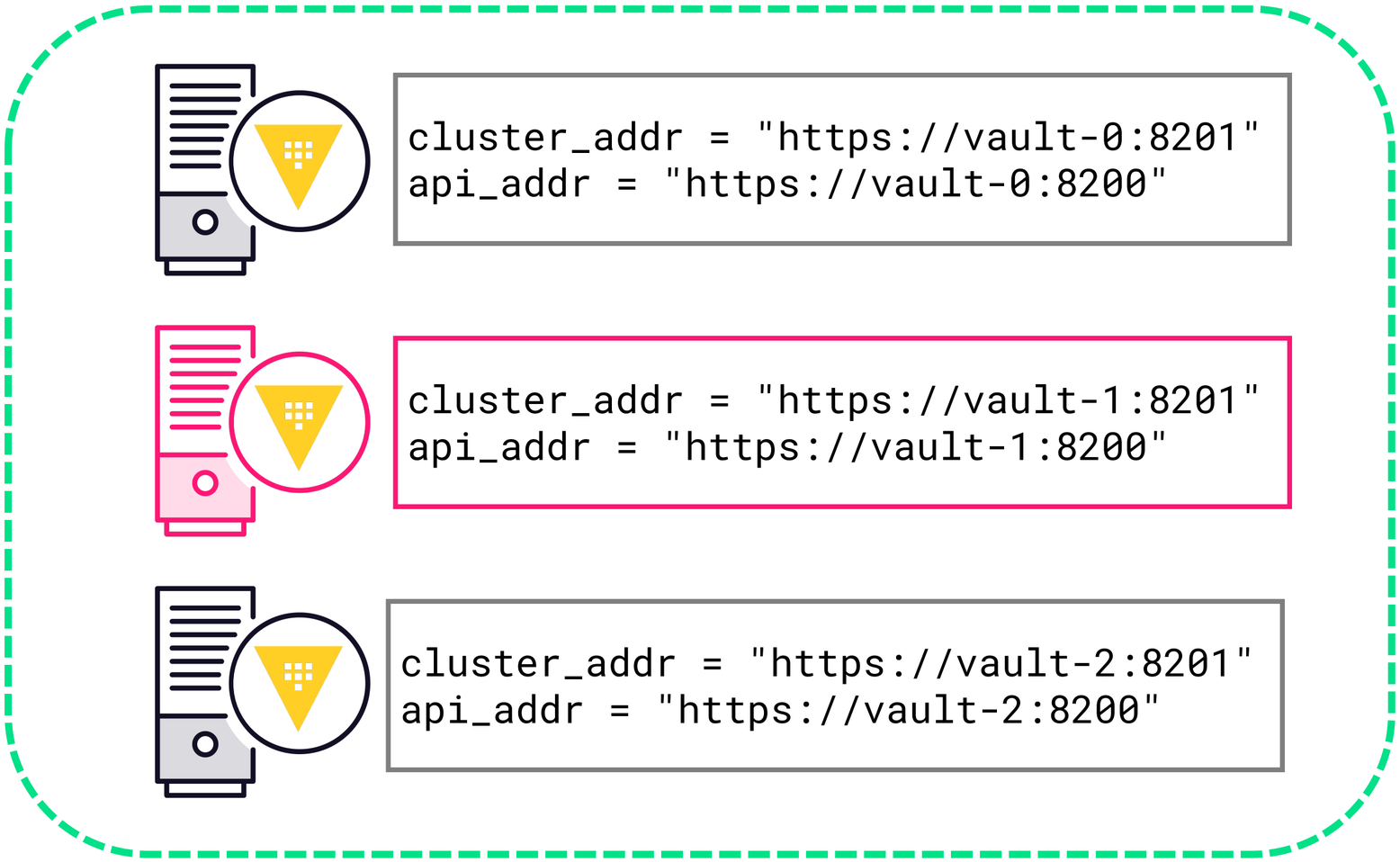
Vault Cluster



Vault Cluster



Vault Cluster Info



```
cluster_addr = "https://vault-0:8201"

api_addr = "https://vault-0:8201"

listener "tcp" {

  address         = "0.0.0.0:8200"

  cluster_address = "10.0.0.1:8201"

  tls_cert_file = "path/to/public/cert.crt"

  tls_key_file  = "path/to/private/cert.key"

}
```

- Server address for other nodes

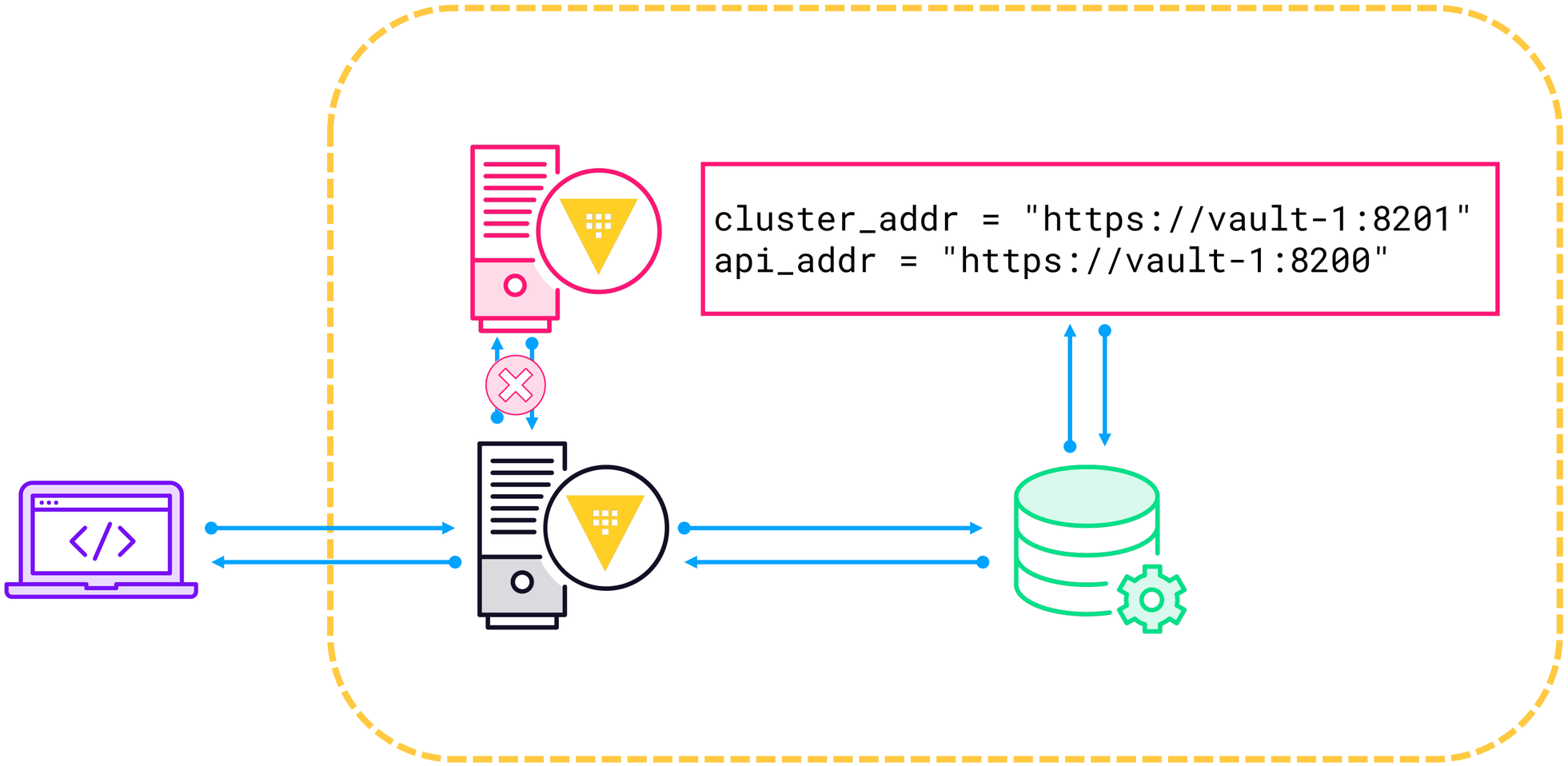
- IP address for client communications

- IP address for cluster communications

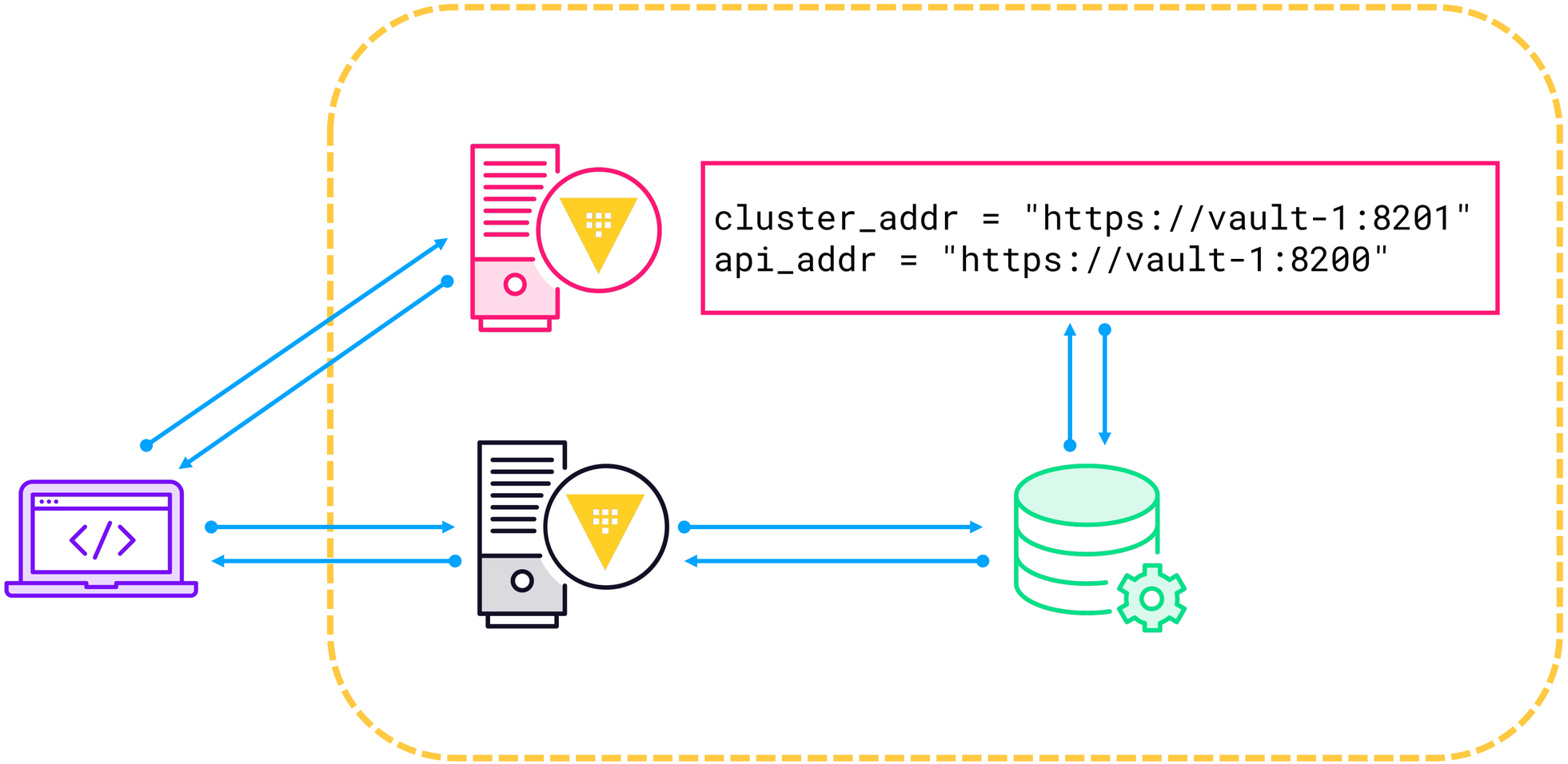
```
cluster_addr = "https://vault-0:8201"

api_addr = "https://vault-0:8201"

listener "tcp" {

  address         = "0.0.0.0:8200"

  cluster_address = "10.0.0.1:8201"

  tls_cert_file = "path/to/public/cert.crt"

  tls_key_file  = "path/to/private/cert.key"

}
```

- Server address for client redirect
- IP address for client communications
- Certificate info for client communications

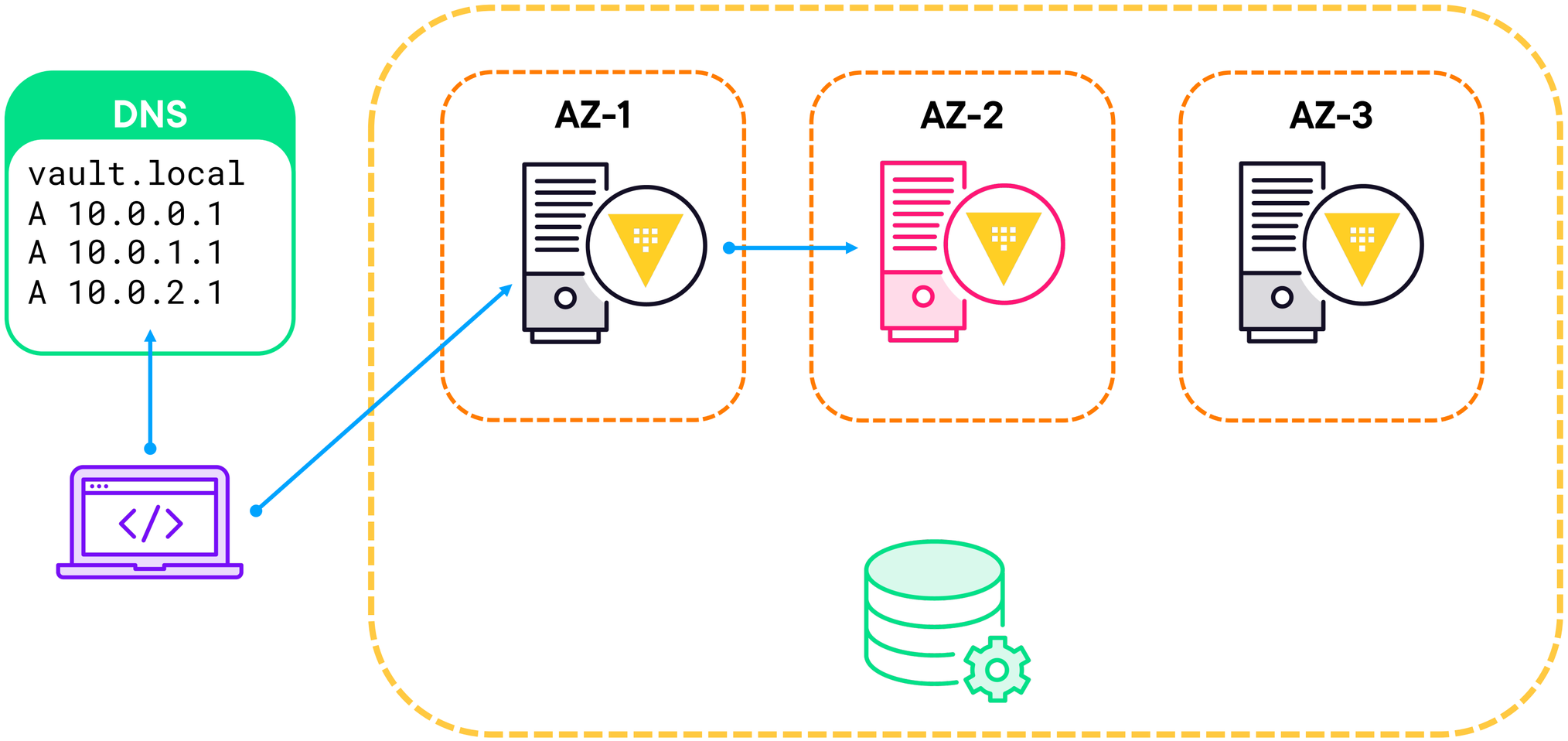
Client Request Forwarding



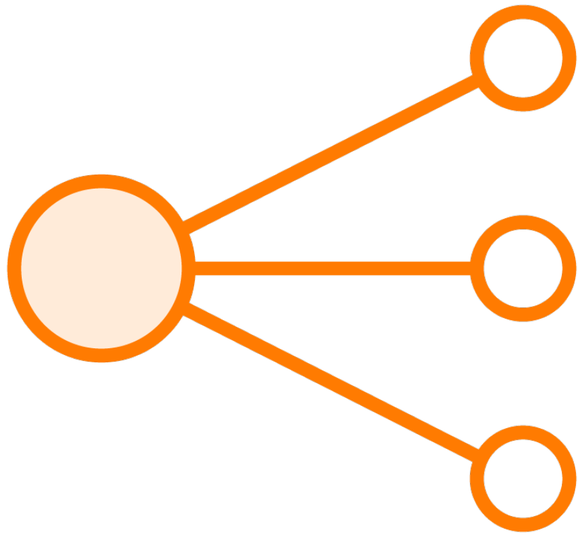
Client Redirection



Vault Cluster



Load Balancers



Layer 4 only

Pass through TLS connections

Port mapping supported

Client traffic only

Probe the endpoint /sys/health

- 200: active node
- 429: standby node
- 473: performance standby node

Performance Standby

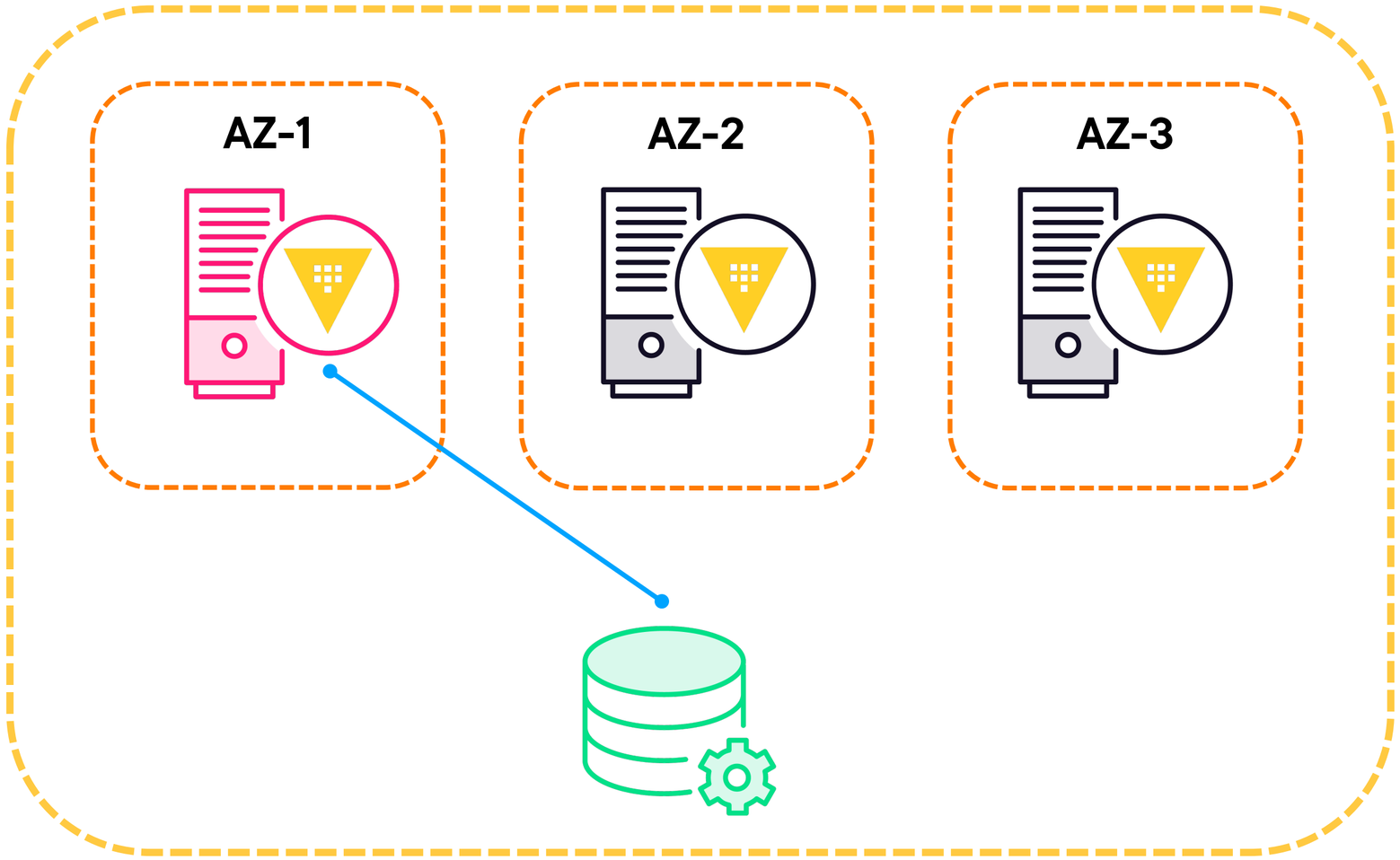
Enterprise feature

Enabled by default

Respond directly to read requests

Forward write requests to active node

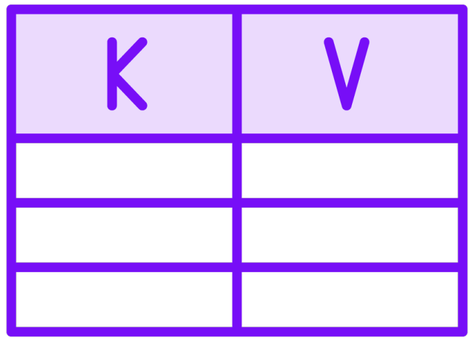
Vault Cluster



Storage Backends

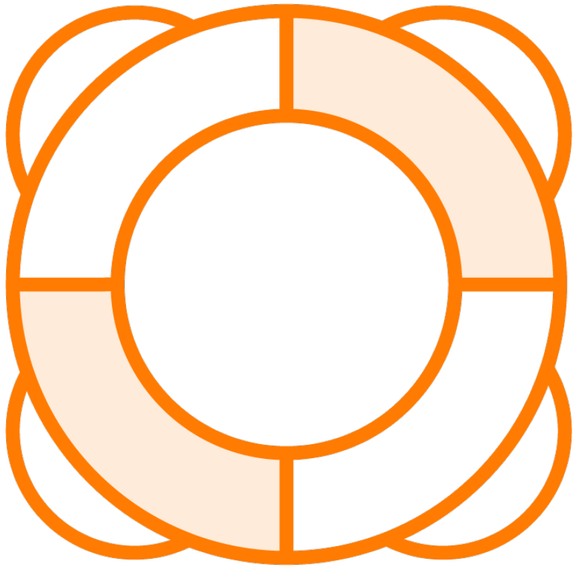
DynamoDB
Azure Storage

Postgres
MySQL



Etcd
Zookeeper

Integrated Storage



Uses local storage

No specialty storage

Supports HA mode

HA Storage Stanza

```
storage "s3" {
  bucket = "vault-bucket"
  path   = "vault-prod/data"
}

ha_storage "dynamodb" {
  ha_enabled = "true"
  region     = "us-west-2"
  table      = "vault-prod-ha"
}
```

Setting up Integrated Storage

Auto join

Cloud-only

Uses cloud metadata

Configuration file

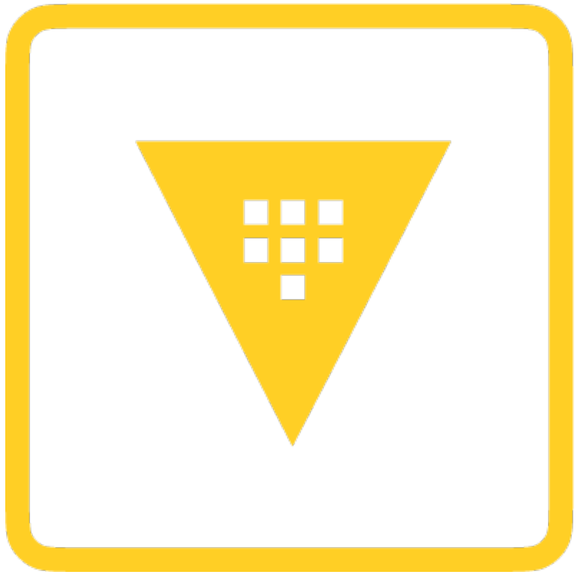
`retry_join` **stanza**

Checks each entry

Creating a Vault Cluster

Update Vault configuration, initialize Vault cluster, and confirm high availability

HCP Vault Dedicated Architecture



Runs the Vault Enterprise binary

Currently runs on AWS or Azure

Deployed to HashiCorp Virtual Network (HVN)

Public endpoint or peered networks

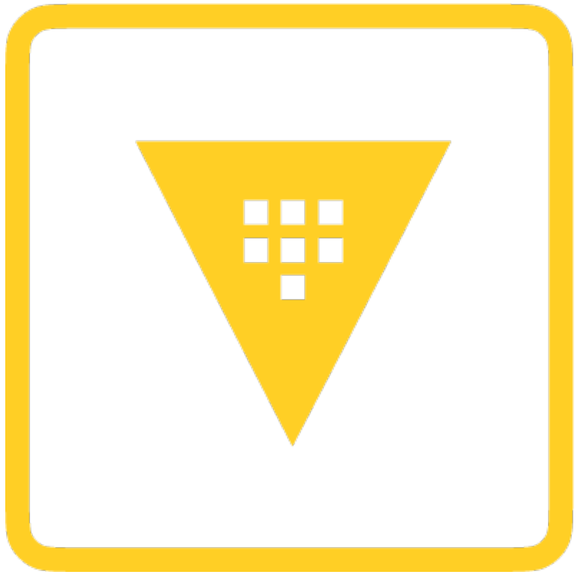
Tiers

- Development, Standard, Plus

Cluster sizes

- Extra small, small, medium, large
- Scalable on demand

HCP Vault Dedicated Constraints



No root namespace access

- Admin parent namespace

No root tokens

- Admin token with hcp-root policy

No community or custom plugins

No direct access to logs