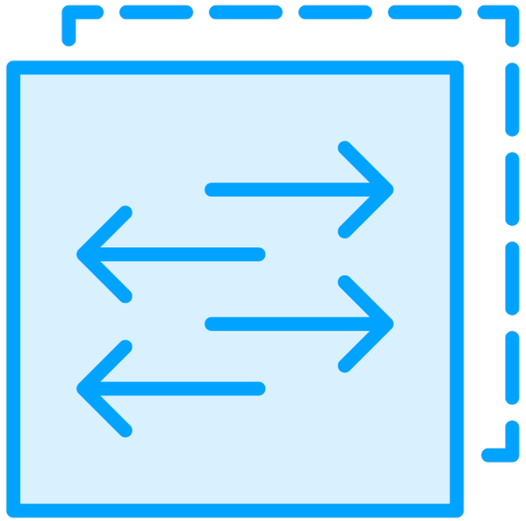
Vault Replication

Ned Bellavance

HashiCorp Certified Instructor

@nedinthecloud | nedinthecloud.com

Vault Replication Support

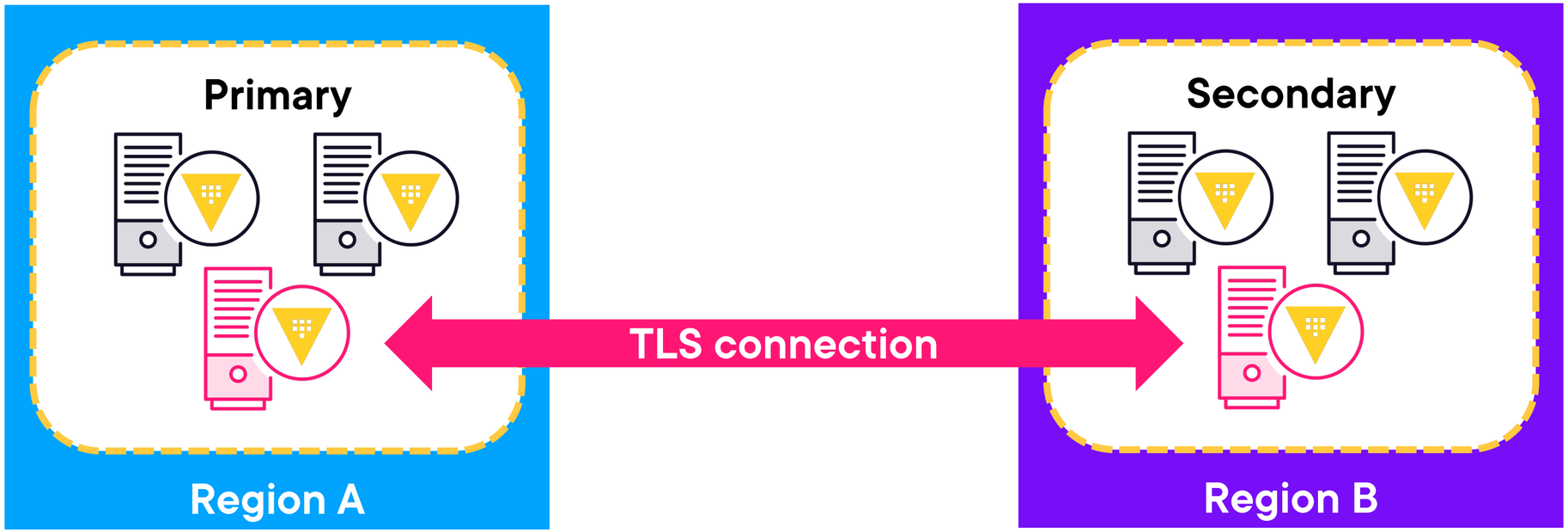


Enterprise feature

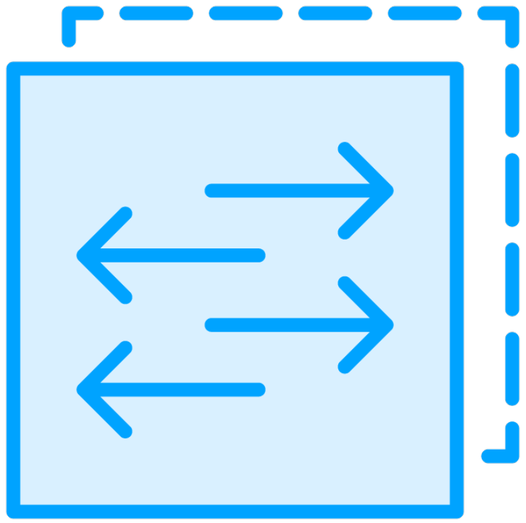
HCP Vault Dedicated

- Standard supports DR replication
- Plus supports performance replication
- Different setup and failover

Vault Replication



Replication Details



Clusters need network connectivity

Do not need the same seal type or storage

Primary version same or older than secondary

Replication mechanism

- Write ahead log shipping (WALS)
- Merkle tree index comparison

Replication Setup

Primary cluster

Enable replication

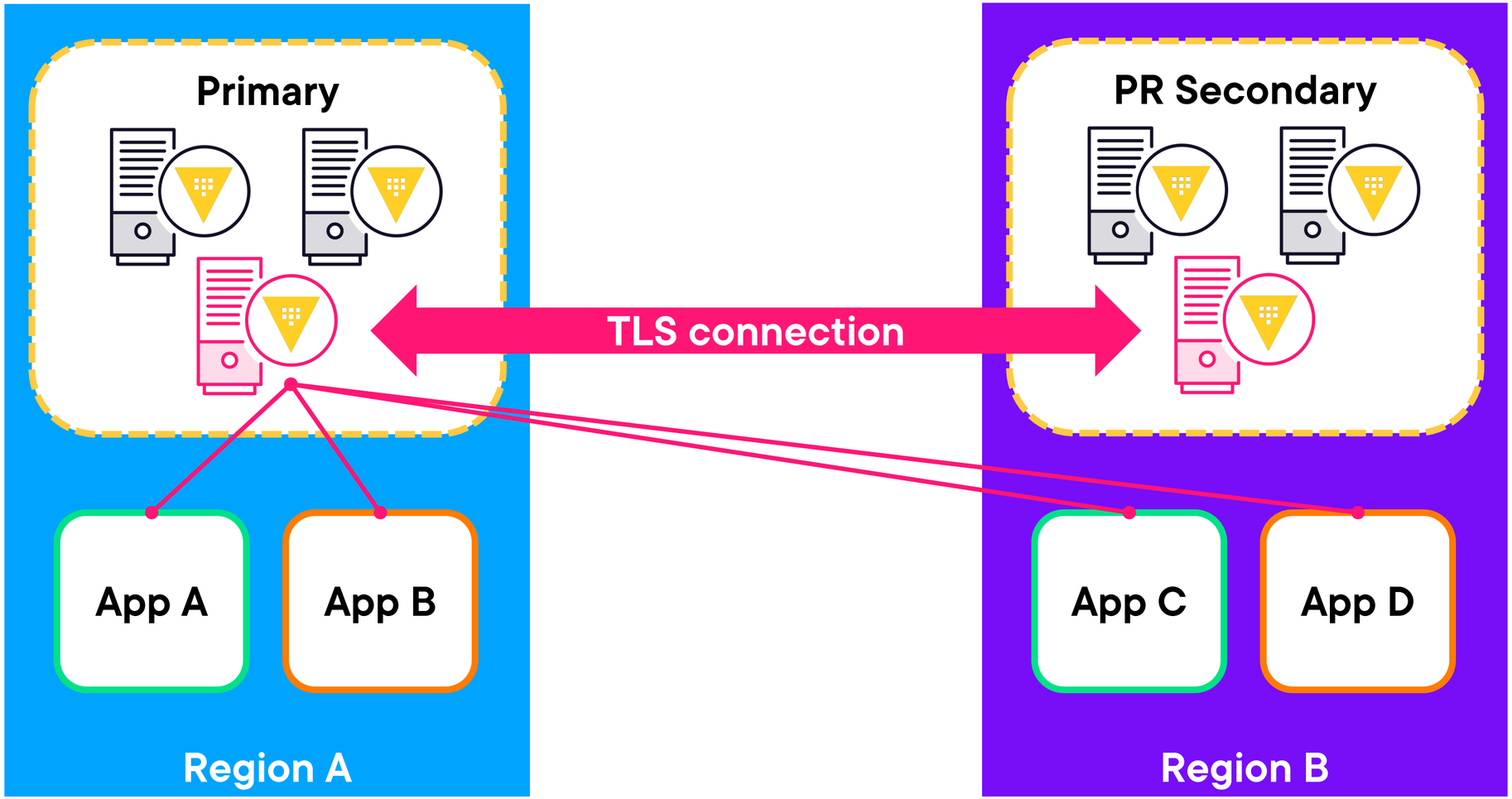
Generate secondary activation token

Secondary cluster

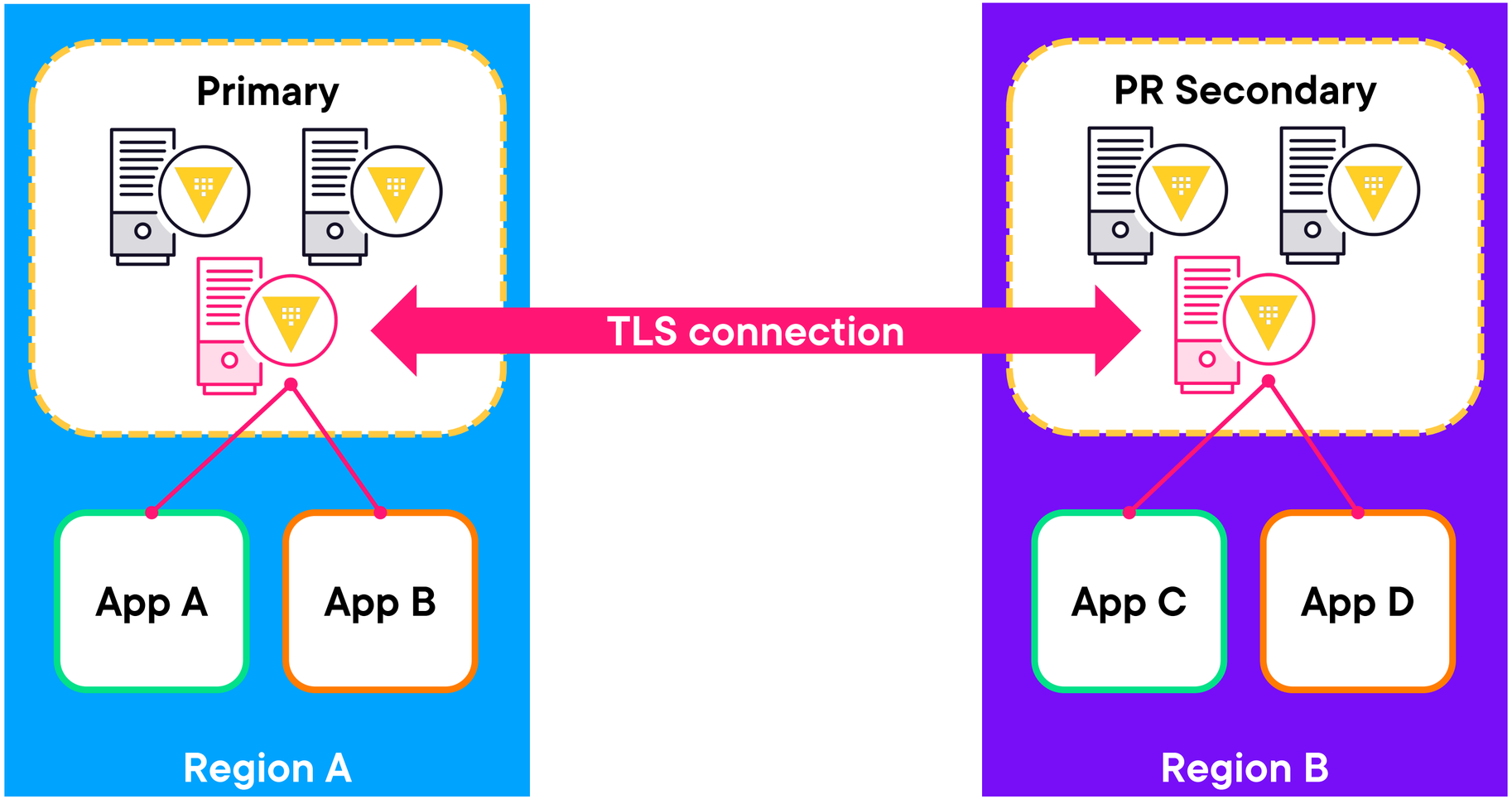
Use secondary token to enable replication

All data is wiped!

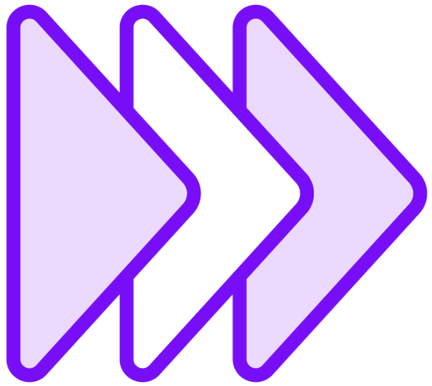
Performance Clusters



Performance Clusters



Performance Clusters



Handle authentication and tokens locally

Supports one-to-many replication

Replicated data

- Configuration, ACL policies, audit devices
- Authentication methods and secrets engines

Tokens and leases not replicated

Data Filtering

Local only

Not replicated

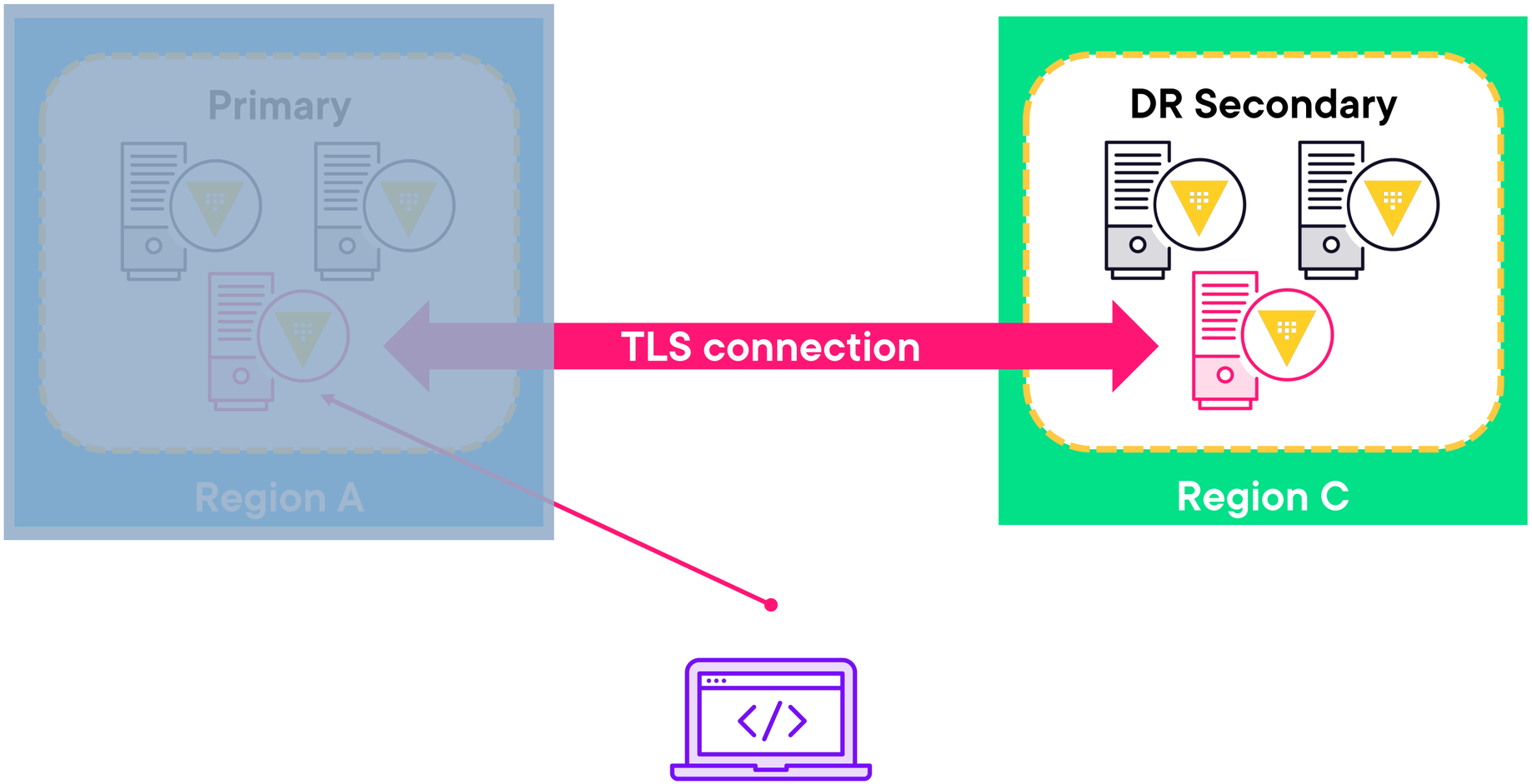
Supported on secondary

Path filtering

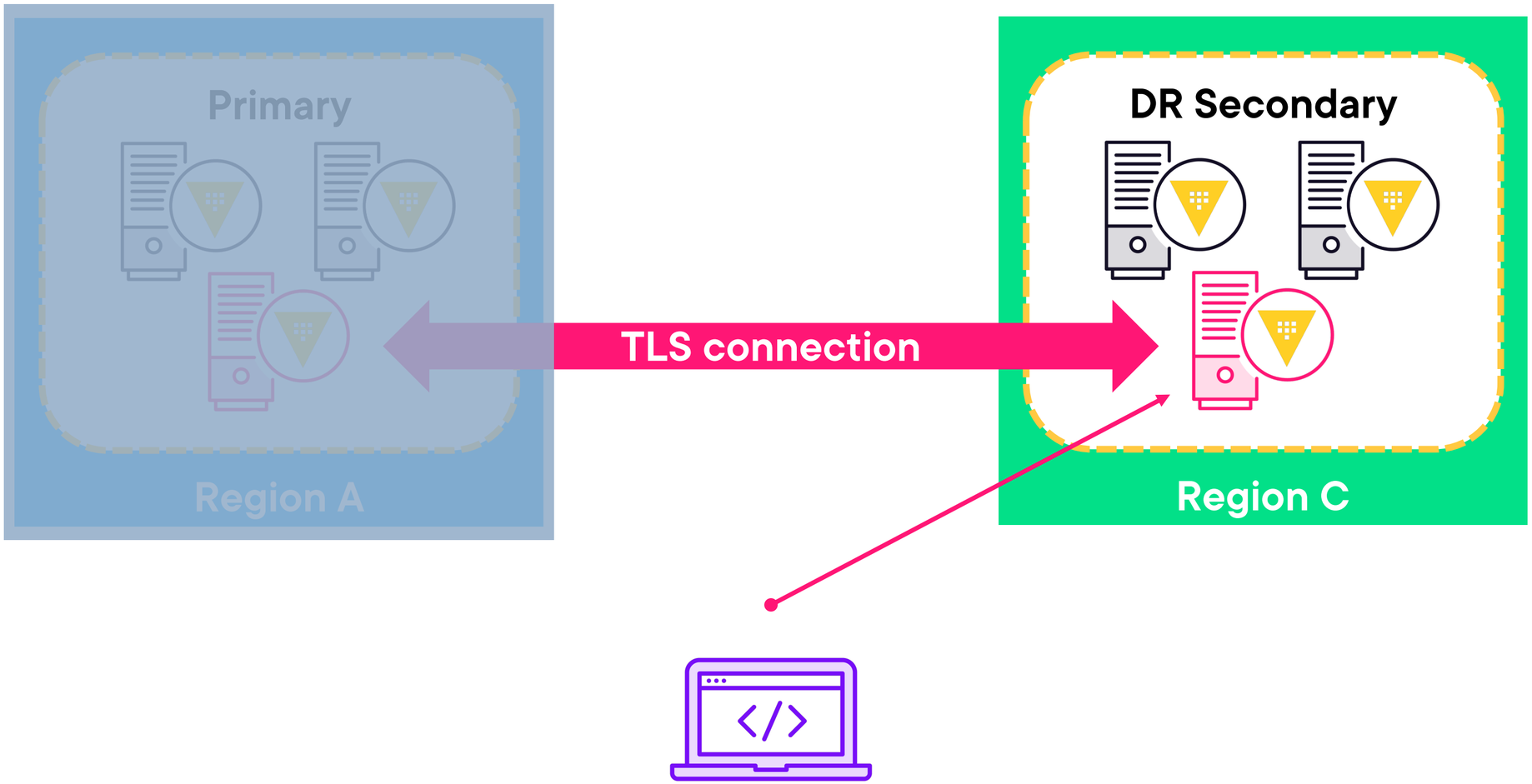
Per cluster basis

Include or exclude mode

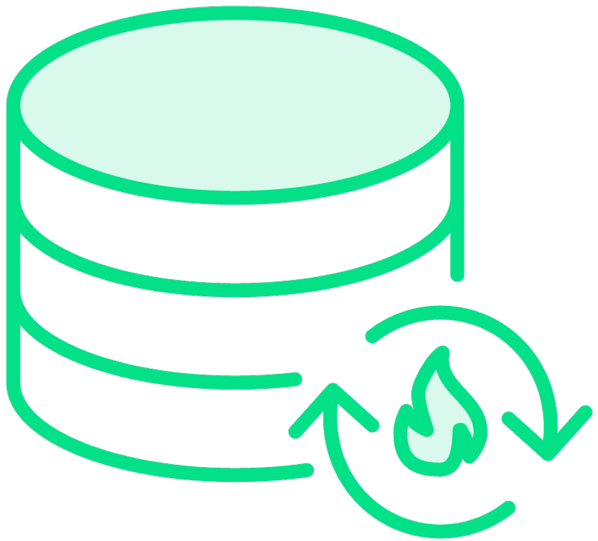
Vault Replication



Vault Replication



Disaster Recovery Clusters



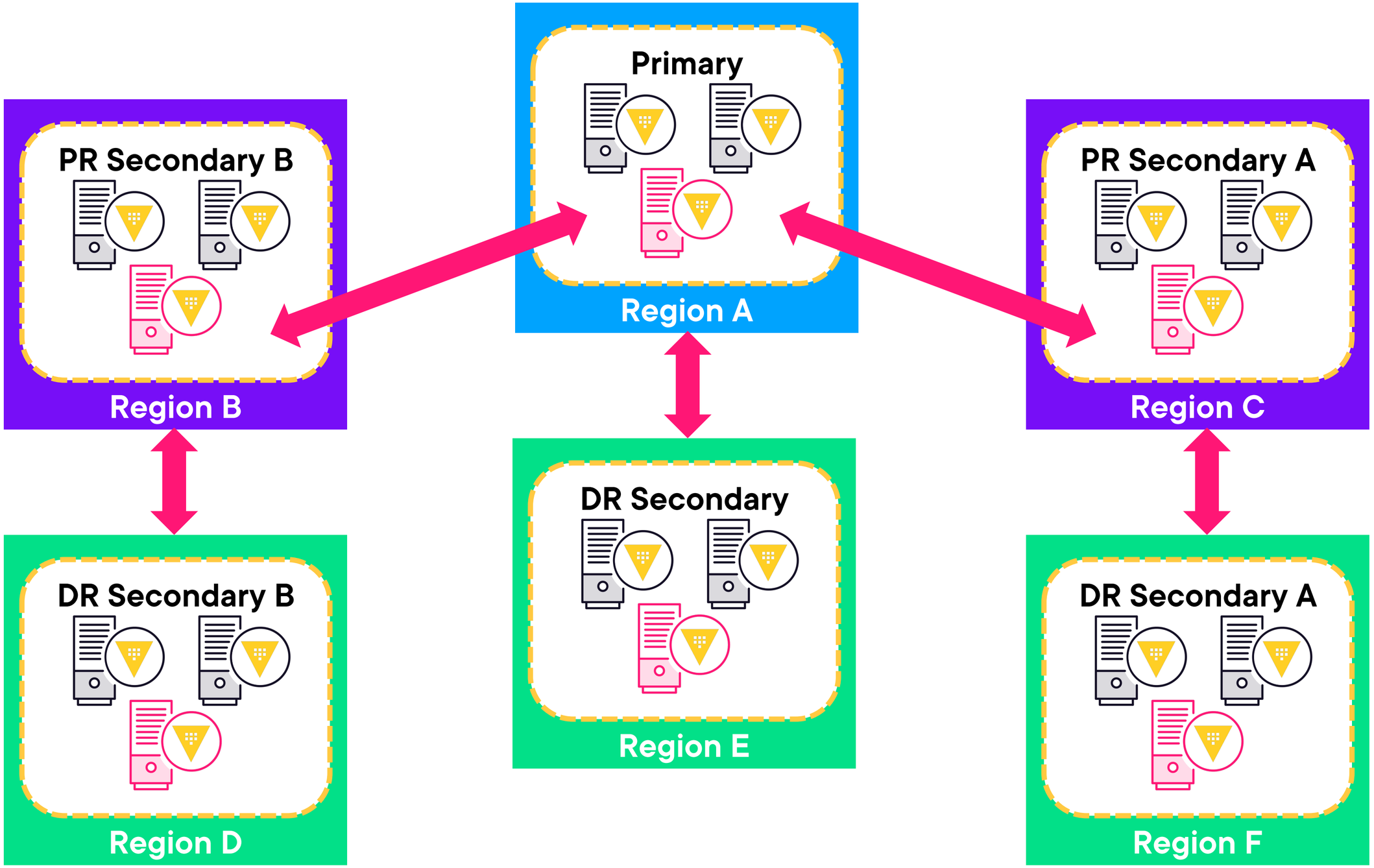
Supports one-to-one replication

Supports performance secondaries

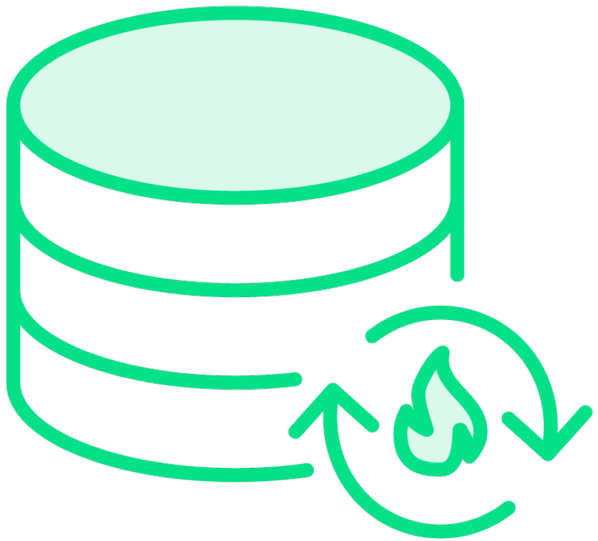
Replicated data

- Configuration, ACL policies, audit devices
- Authentication methods and secrets engines
- Includes local mounts
- No path filtering

Tokens and leases replicated


Primary
Region A
PR Secondary B
Region B
PR Secondary A
Region C
DR Secondary
Region E
DR Secondary B
Region D
DR Secondary A
Region F

Disaster Recovery Clusters



Supports one-to-one replication

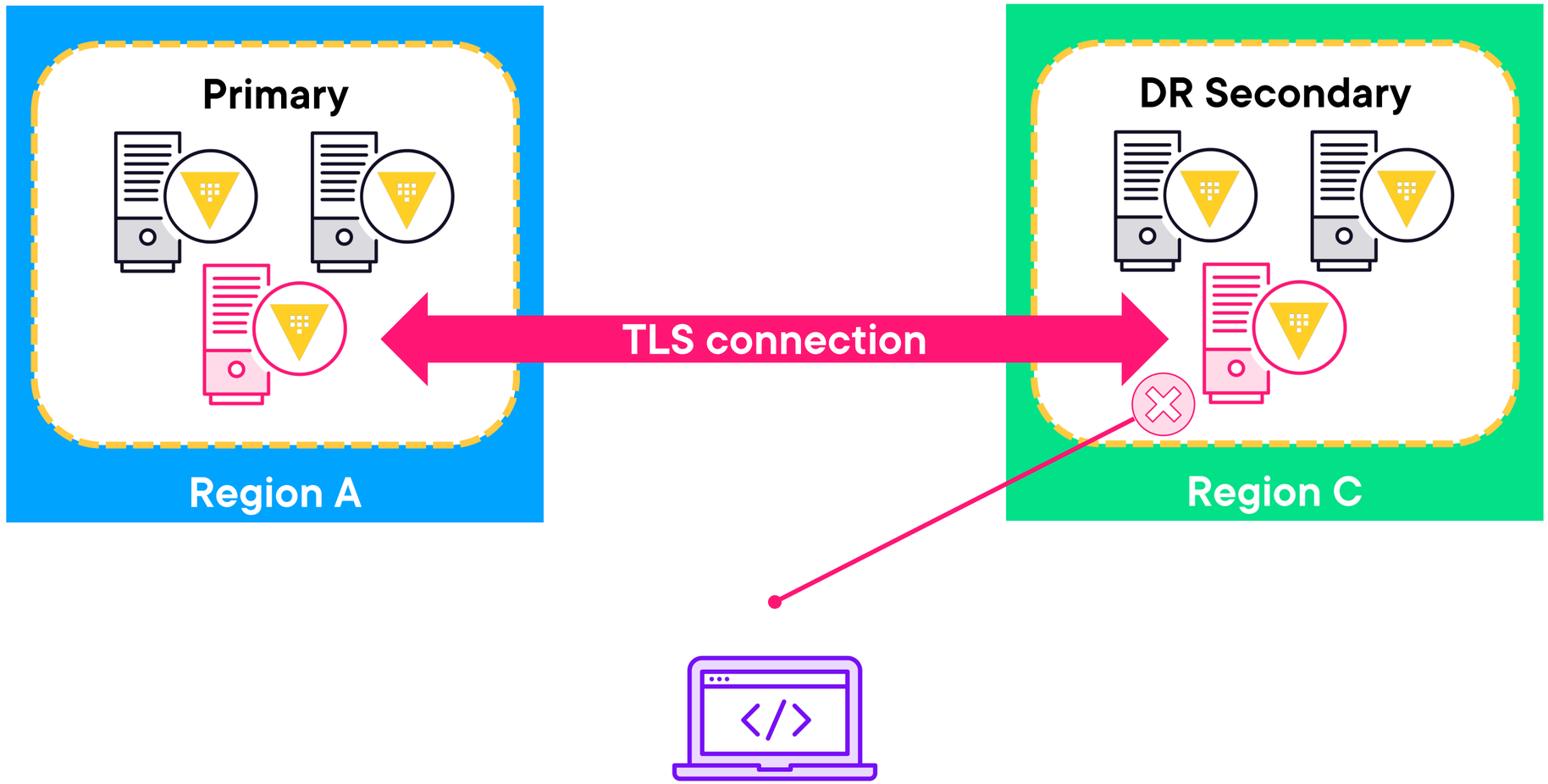
Supports performance secondaries

Replicated data

- Configuration, ACL policies, audit devices
- Authentication methods and secrets engines
- Includes local mounts
- No path filtering

Tokens and leases replicated

Vault DR Cluster



Failover Process

Generate a DR operations token

Demote primary (if possible)

Promote secondary

Not automatic!

Failback Process

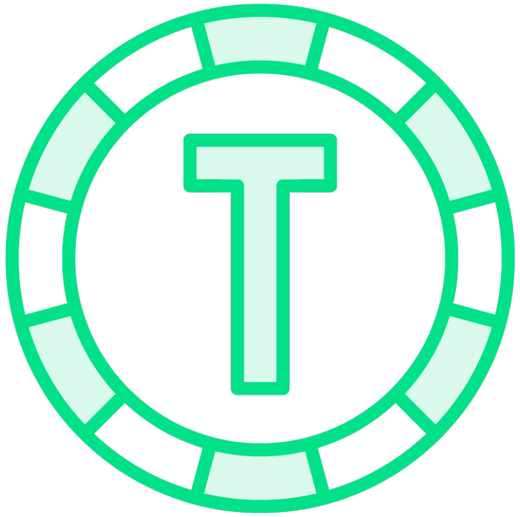
Demote primary (while isolated)

Former primary becomes DR secondary

Replicate changes

Failback to original primary

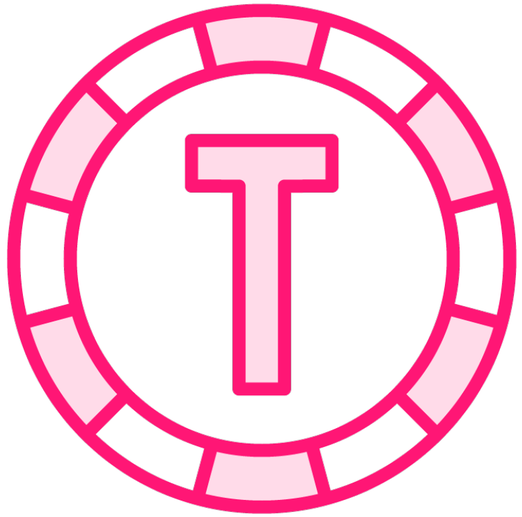
DR Operations Token



Service token

Unseal or recovery keys

Does not require primary



Batch token

Does not require keys

Requires primary cluster