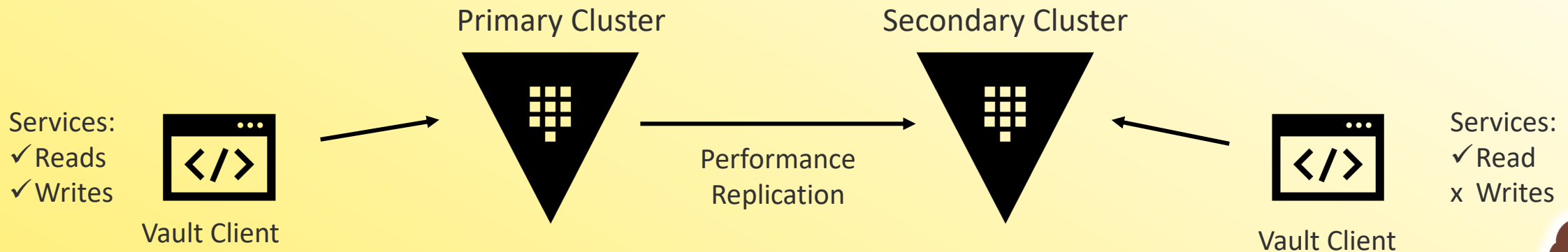# Enable and Configure Performance Replication
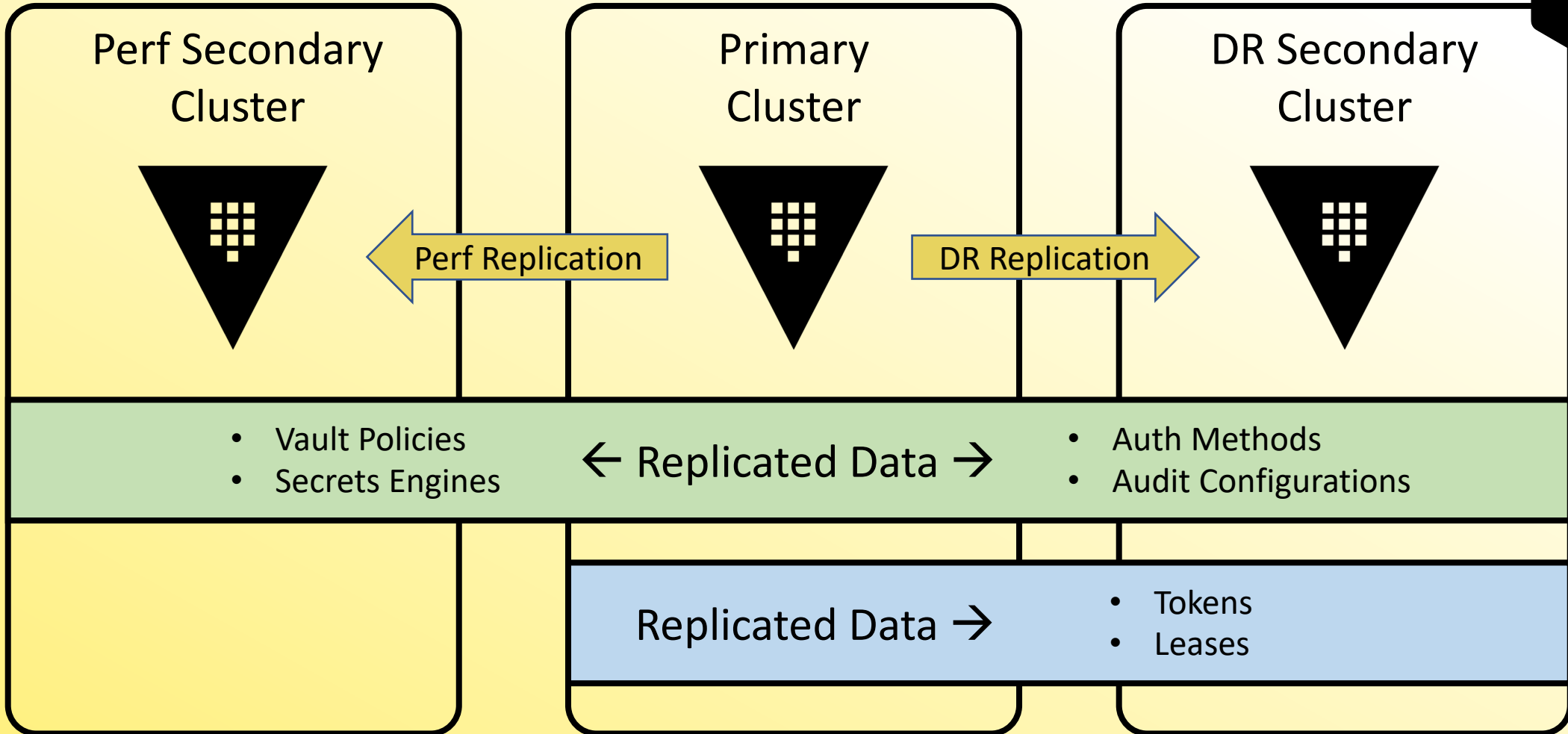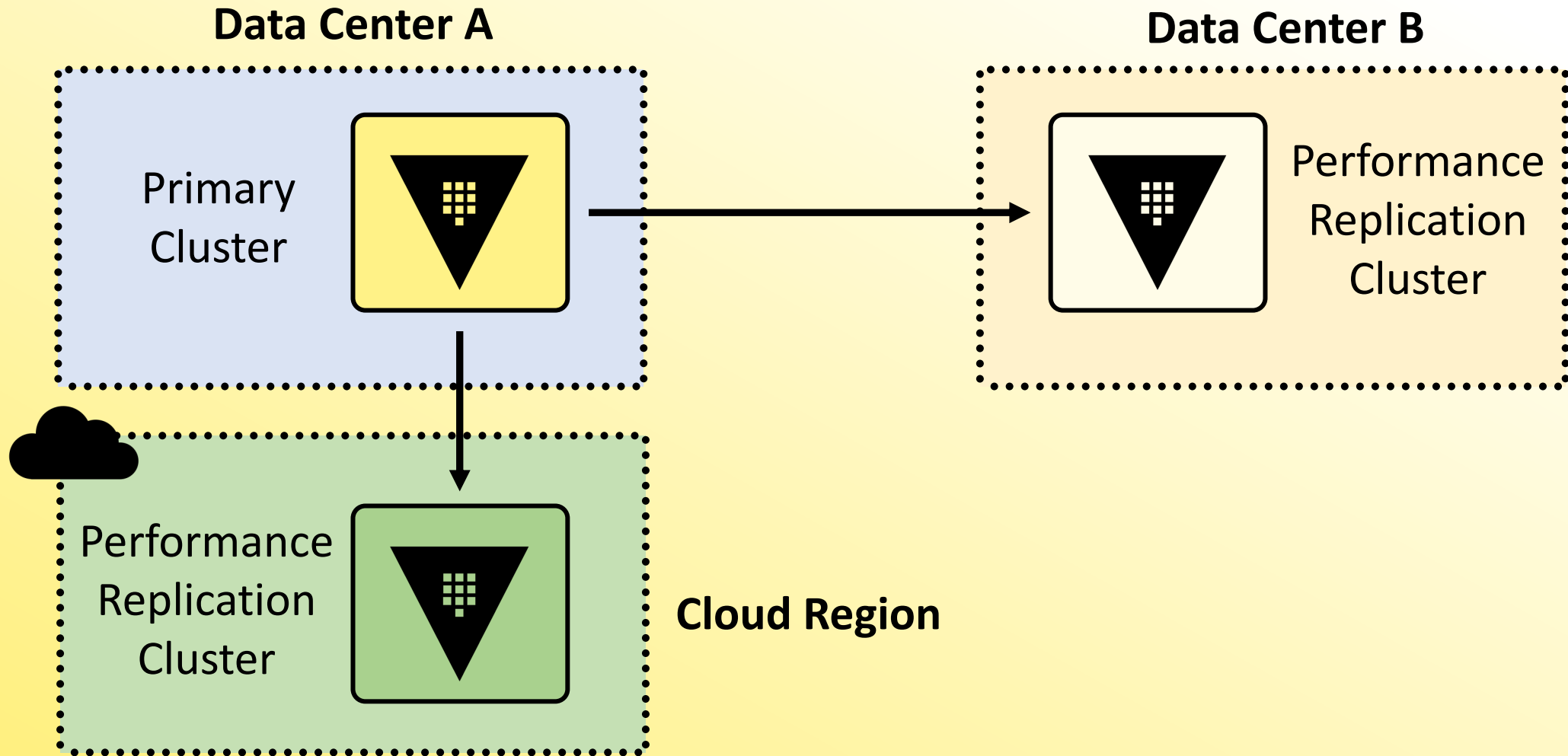
Intro to Performance Replicaiton

- Replicates the underlying configuration, policies, and other data

- Ability to service reads from client requests

- Clients will authenticate to the performance replicated cluster separately

- Does not replicate tokens or leases to performance secondaries

Primary Cluster   Secondary Cluster

Services:
✓ Reads
✓ Writes

Vault Client

Performance
Replication

Services:
✓ Read
x Writes

Vault Client

Compare Performance & DR Replication

Perf Secondary Cluster

Primary Cluster

DR Secondary Cluster

← Perf Replication

DR Replication →

← Replicated Data →

- Vault Policies
- Secrets Engines

- Auth Methods
- Audit Configurations

Replicated Data →

- Tokens
- Leases

Replication Architecture

Data Center A

Data Center B

Primary Cluster

Performance Replication Cluster

Performance Replication Cluster

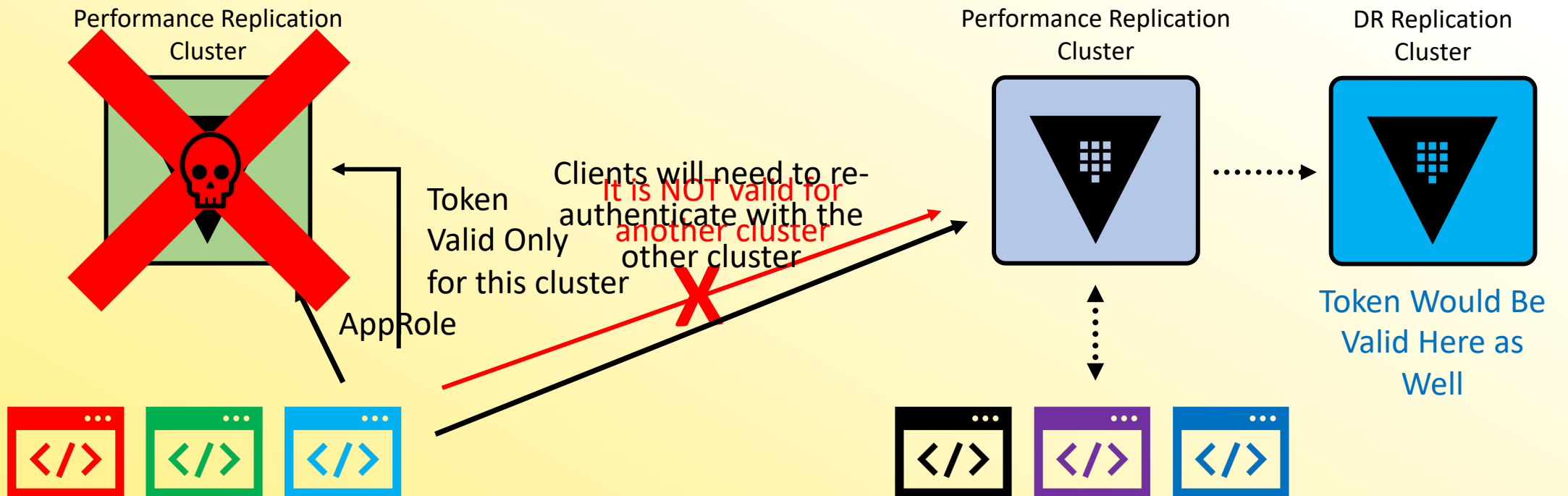**Cloud Region**

Application Communication
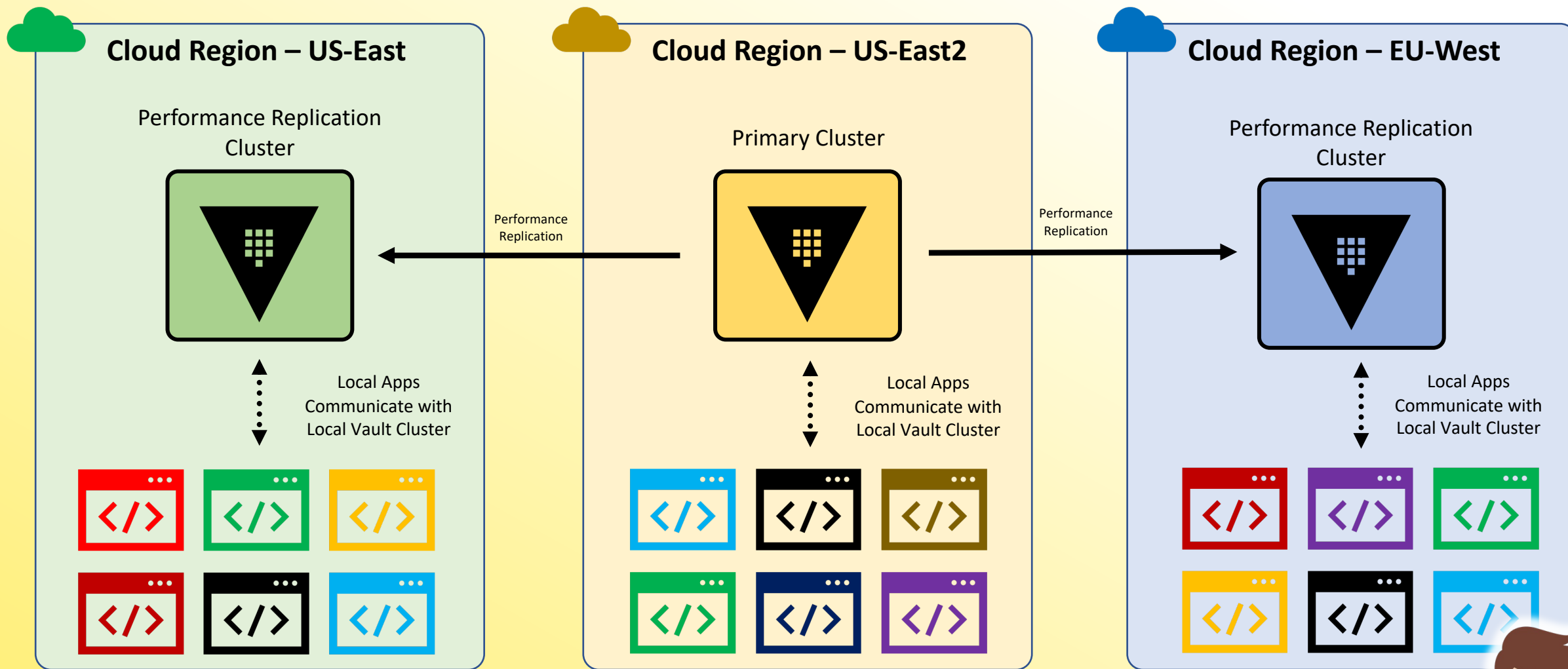
Performance Replication

- Provides active/active solution for applications running in multiple data centers

- Applications authenticate with the LOCAL Vault cluster. Tokens are created and maintained on each cluster and are not replicated via Perf Replication

- If a cluster becomes unavailable and you failover, applications will need to reauthenticate with the new Vault cluster

  - Exception here is if you failover to a DR cluster

Performance Replication

Performance Replication Cluster

Token Valid Only for this cluster

AppRole

Clients will need to re-authenticate with the other cluster

It is NOT valid for another cluster

Performance Replication Cluster

DR Replication Cluster

Token Would Be Valid Here as Well
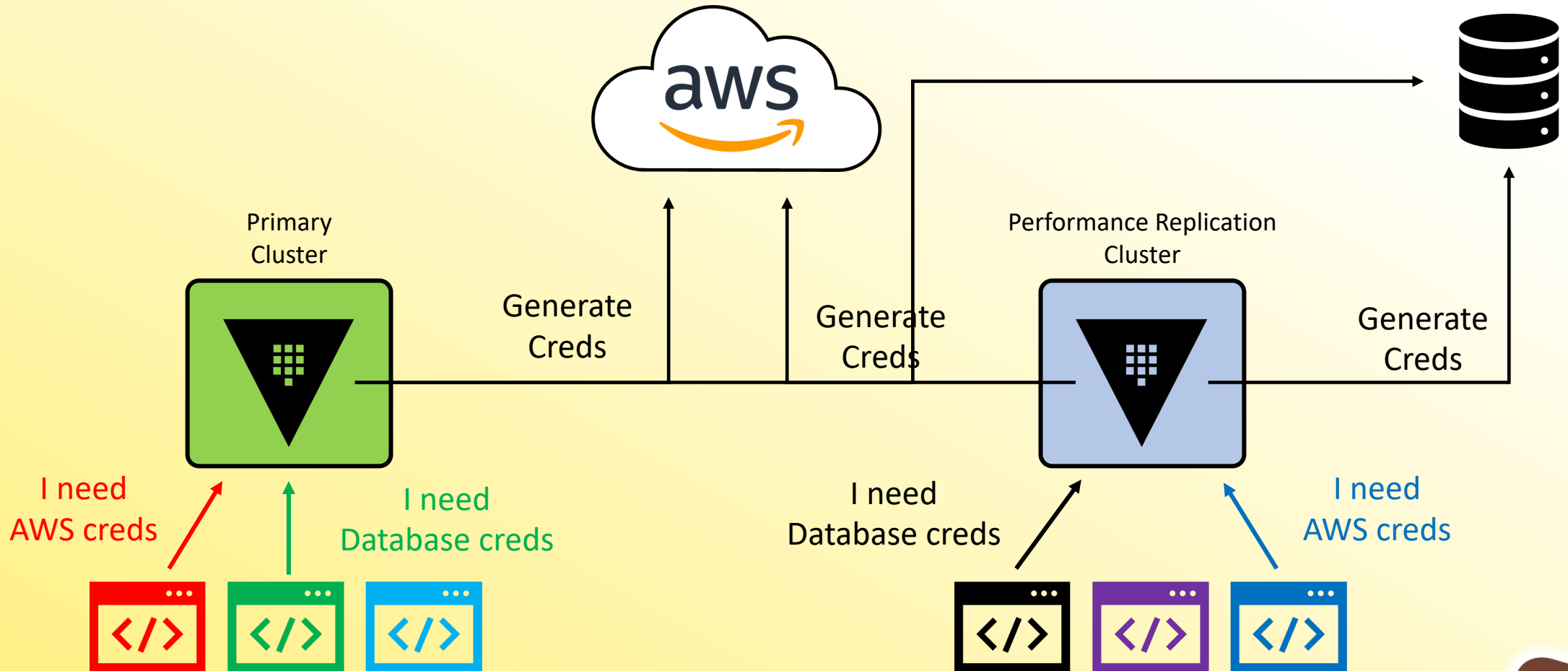
Performance Replication

- Performance replicated clusters handle the retrieval of secrets and the generation of dynamic credentials for local clients

- These requests are handled locally and tokens/leases not replicated to the primary cluster
  - This helps offload some WRITE operations from the primary because the local cluster handles and doesn't forward to the primary cluster

- Any request to write data to the KV, write/updates Vault policies, make Vault configuration changes, etc. WILL be forwarded to the primary
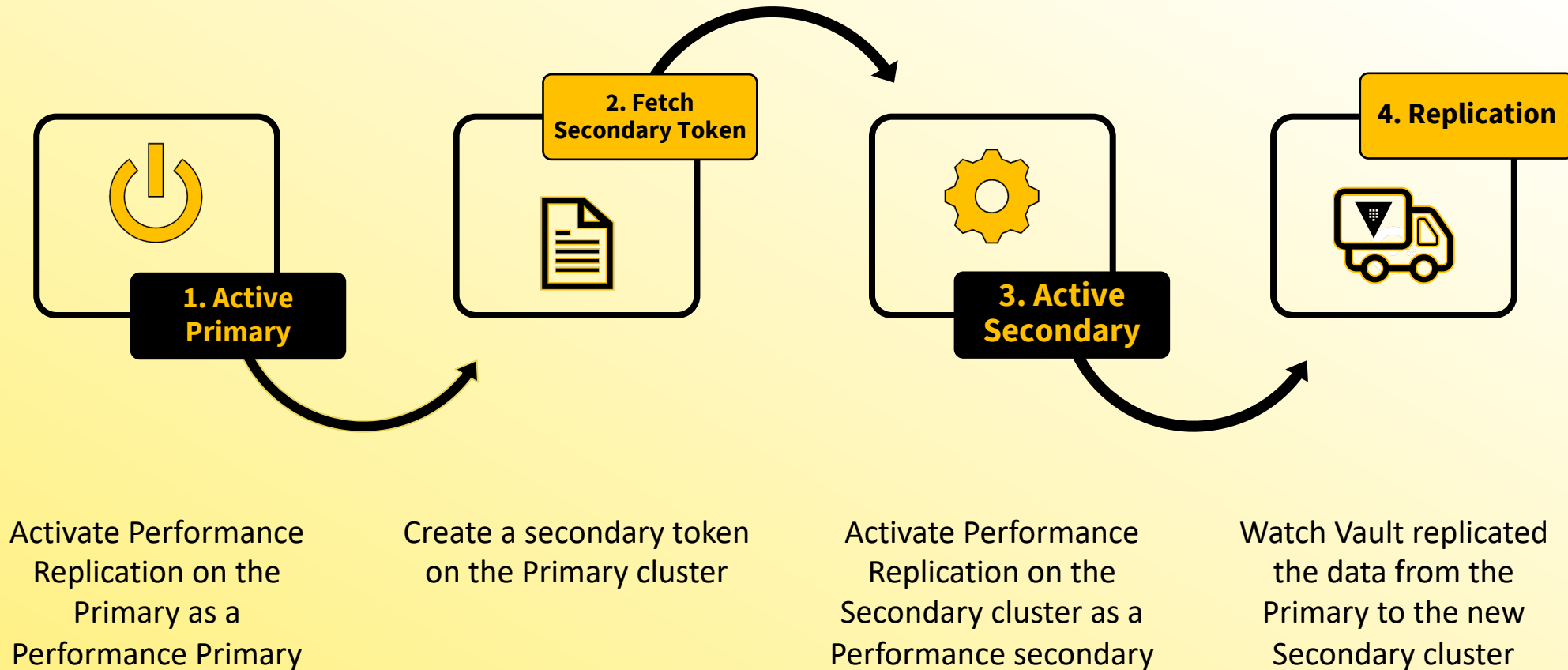
Interaction with External Services

How Do We Set All of this Up?

1. Active Primary

Activate Performance Replication on the Primary as a Performance Primary

2. Fetch Secondary Token

Create a secondary token on the Primary cluster

3. Active Secondary

Activate Performance Replication on the Secondary cluster as a Performance secondary

4. Replication

Watch Vault replicated the data from the Primary to the new Secondary cluster

Configure Replication

1 **Activate Performance Replication**

```
primary$ vault write -f sys/replication/performance/primary/enable
```

2 **Create the Secondary Token**

Name it what you want

```
primary$ vault write sys/replication/performance/primary/secondary-token id=<id>
```

3 **Activate the Secondary Cluster**

Provide token from primary cluster (command above)

```
secondary$ vault write sys/replication/performance/secondary/enable token=<token>
```

Monitor Replication

Check Status of ALL Replication

```
$ vault read -format=json sys/replication/status
```

Check Status of Performance Replication

```
$ vault read -format=json sys/replication/performance/status
```

Performance Replication Only

Check Status of DR Replication

```
$ vault read -format=json sys/replication/dr/status
```

DR Replication Only