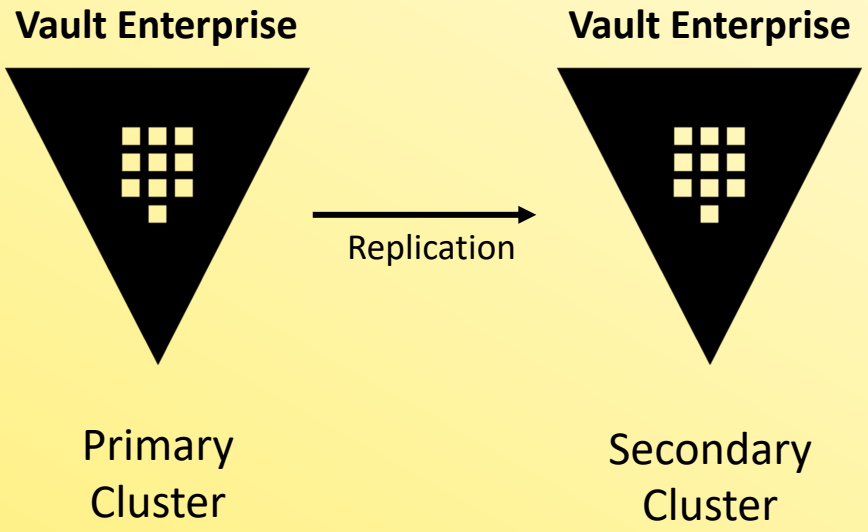
Enable and Configure Disaster Recovery (DR) Replication

What is Vault Replication?

Organizations usually have infrastructure that **spans multiple datacenters**

- Vault needs to be highly-available for application access
- Needs to scale as organizations continue to add use cases and apps
- Common set of policies that are enforced **globally**
- Consistent set of secrets and configurations available to applications that need them regardless of data center

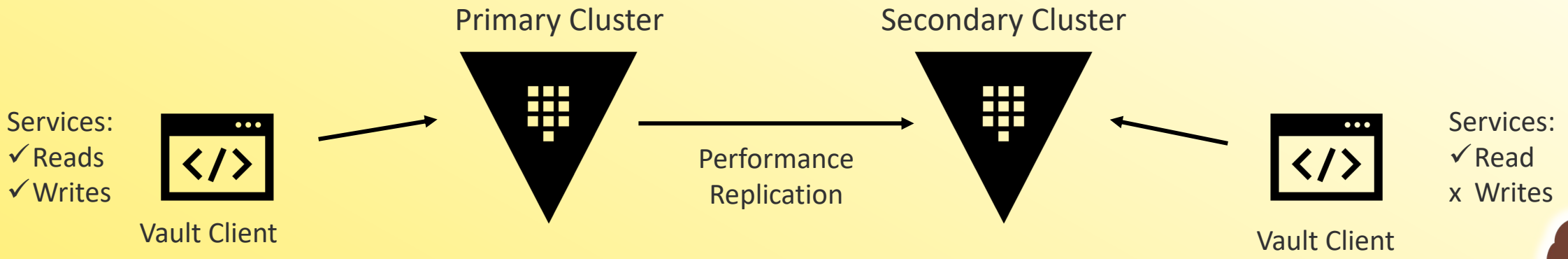
What is Vault Replication?



- **Only available in Vault Enterprise**
- Replication operates on a leader-follower model (**primaries** and **secondaries**)
- The primary cluster acts as the system of record and replicates most Vault data asynchronously
- All communication between primaries and secondaries is **end-to-end encrypted** with mutually-authenticated TLS sessions

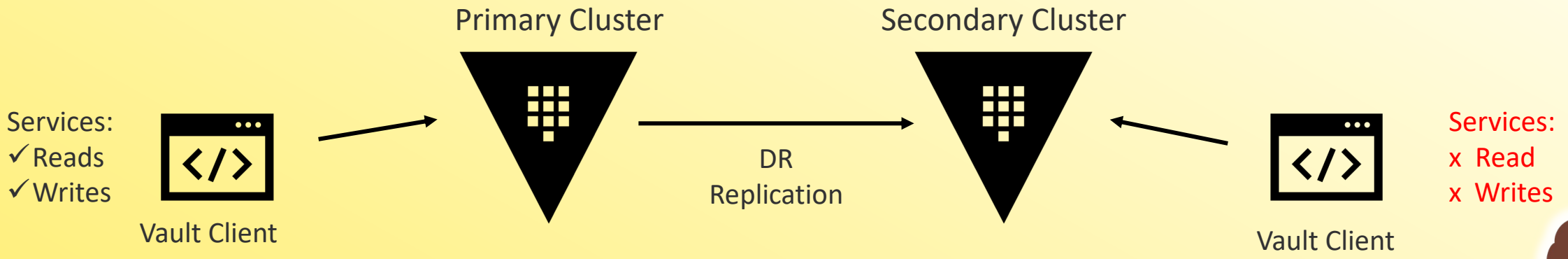
Performance Replication

- 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

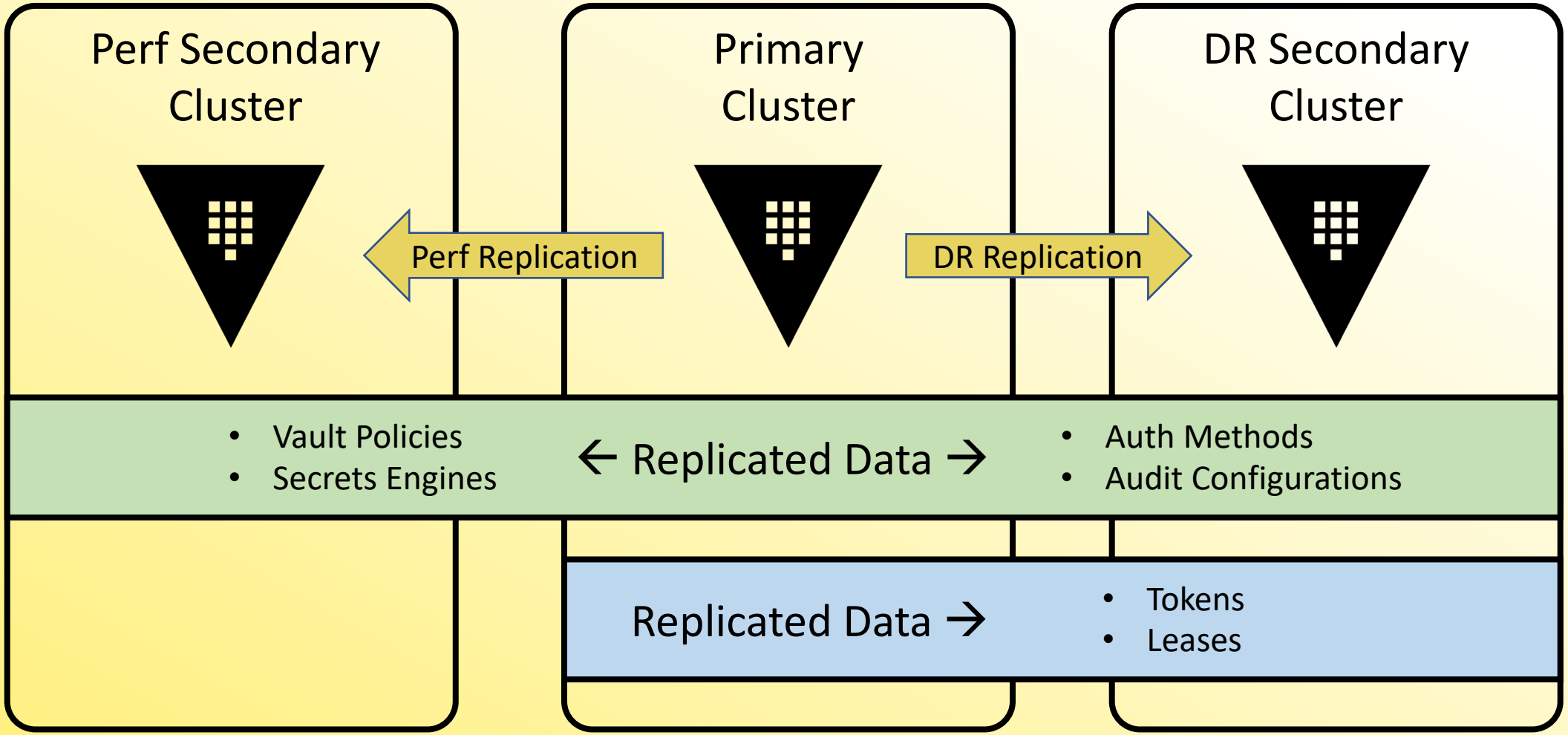


Disaster Recovery Replication

- Replicates the underlying configuration, policies, and all other data
- Cannot service reads from client requests
- Clients should authenticate with the primary cluster only (or a perf cluster)
- Will replicate tokens and leases created on the primary cluster



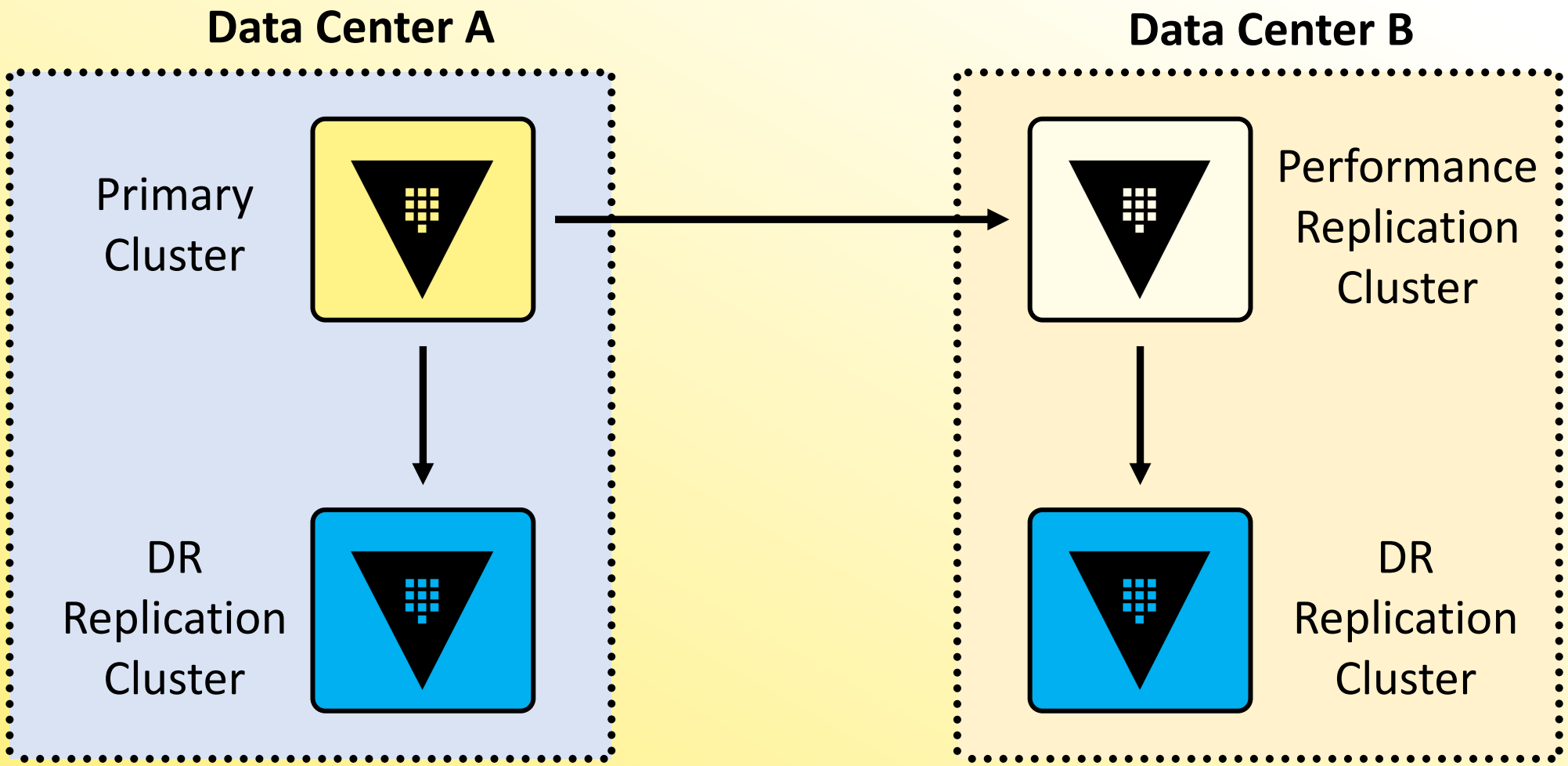
Comparison


Perf Secondary Cluster
Primary Cluster
DR Secondary Cluster
Perf Replication
DR Replication
• Vault Policies
• Secrets Engines
← Replicated Data →
• Auth Methods
• Audit Configurations
Replicated Data →
• Tokens
• Leases

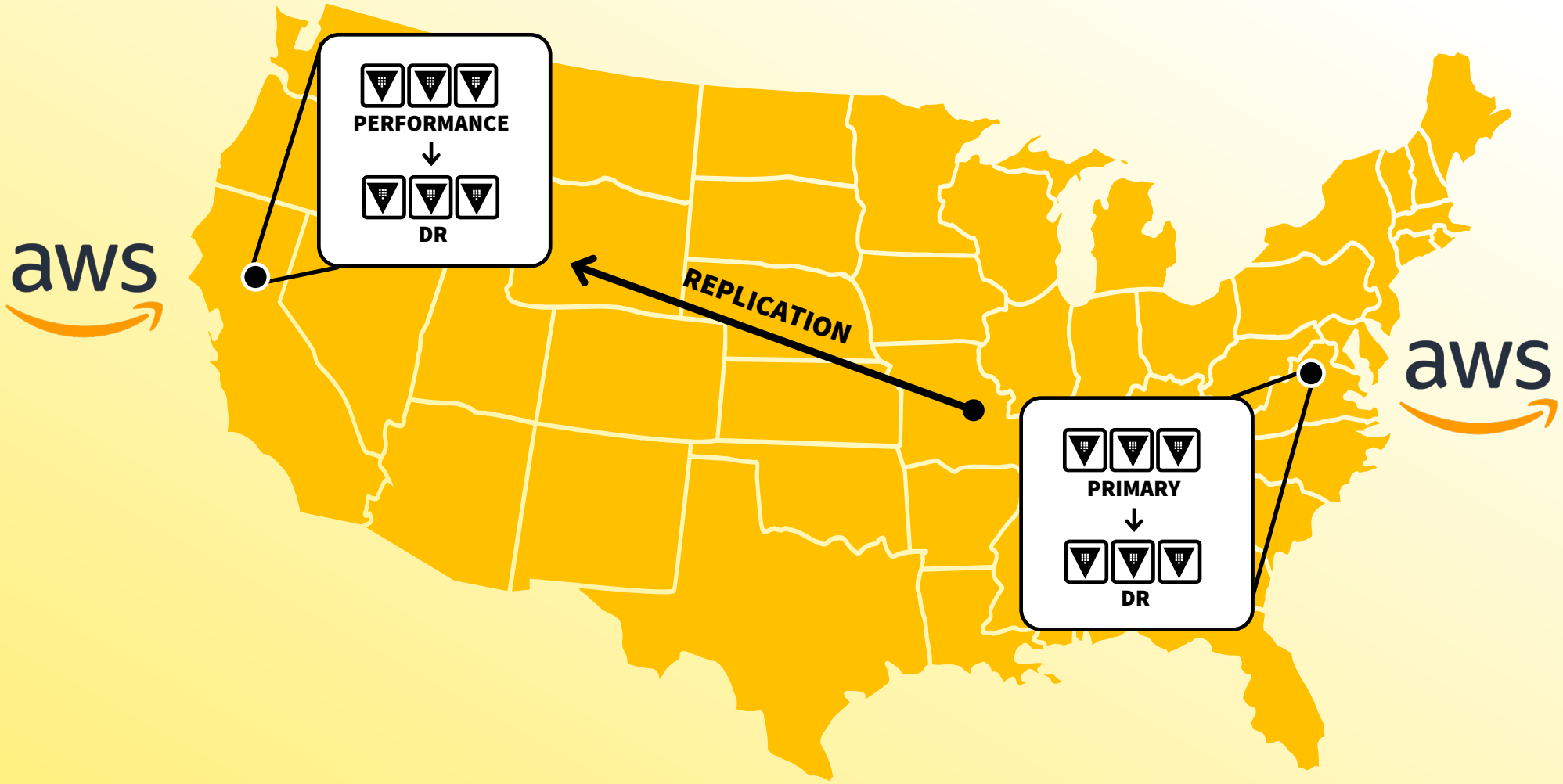
Disaster Recovery Replication

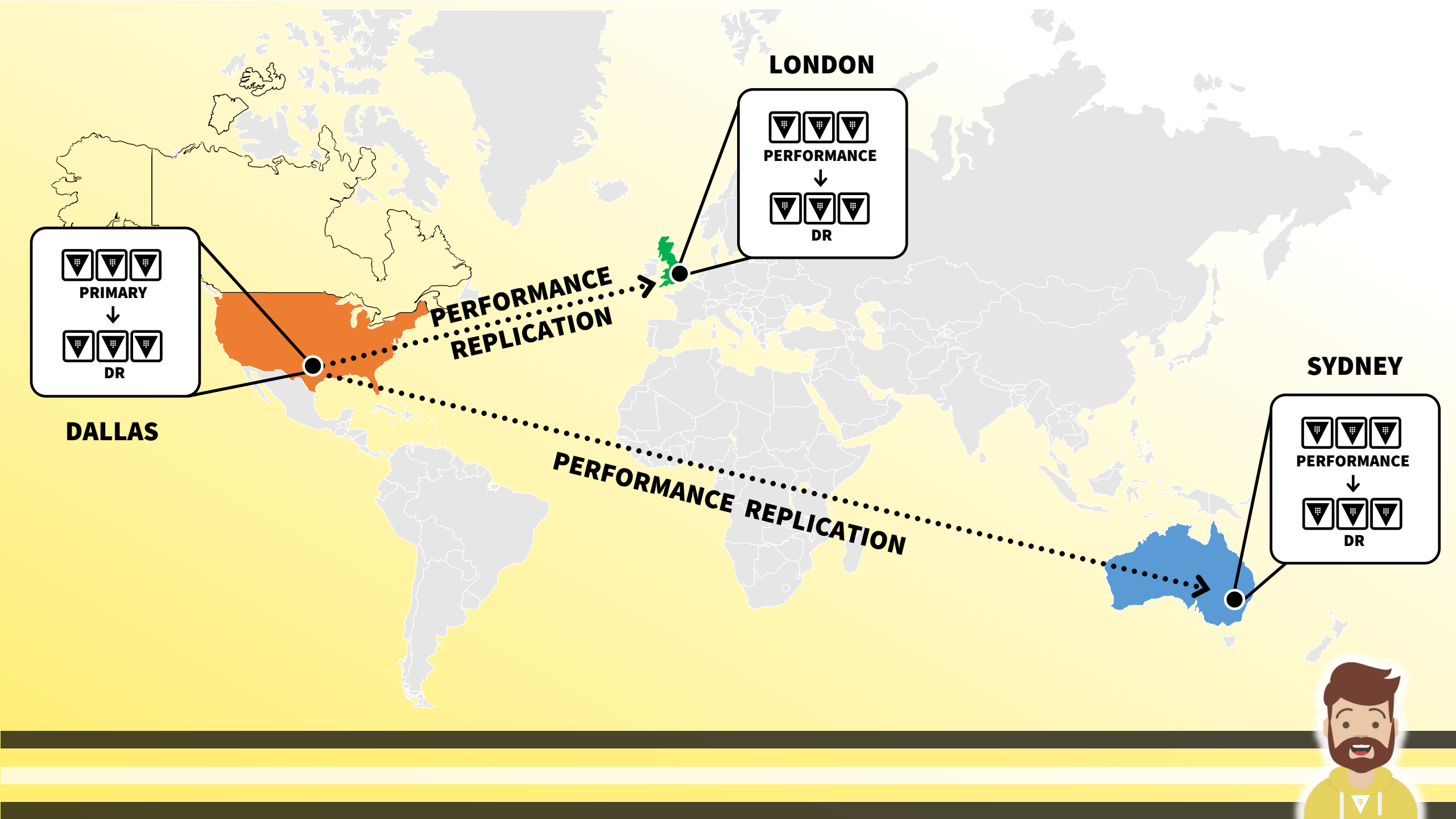
- Provides a warm-standby cluster where EVERYTHING is replicated to the DR secondary cluster(s)
- DR clusters DO NOT respond to clients unless they are promoted to a primary cluster
- Even as an admin or using a root token, most paths on a secondary cluster are disabled, meaning you can't do much of anything on a DR cluster

Replication Architecture

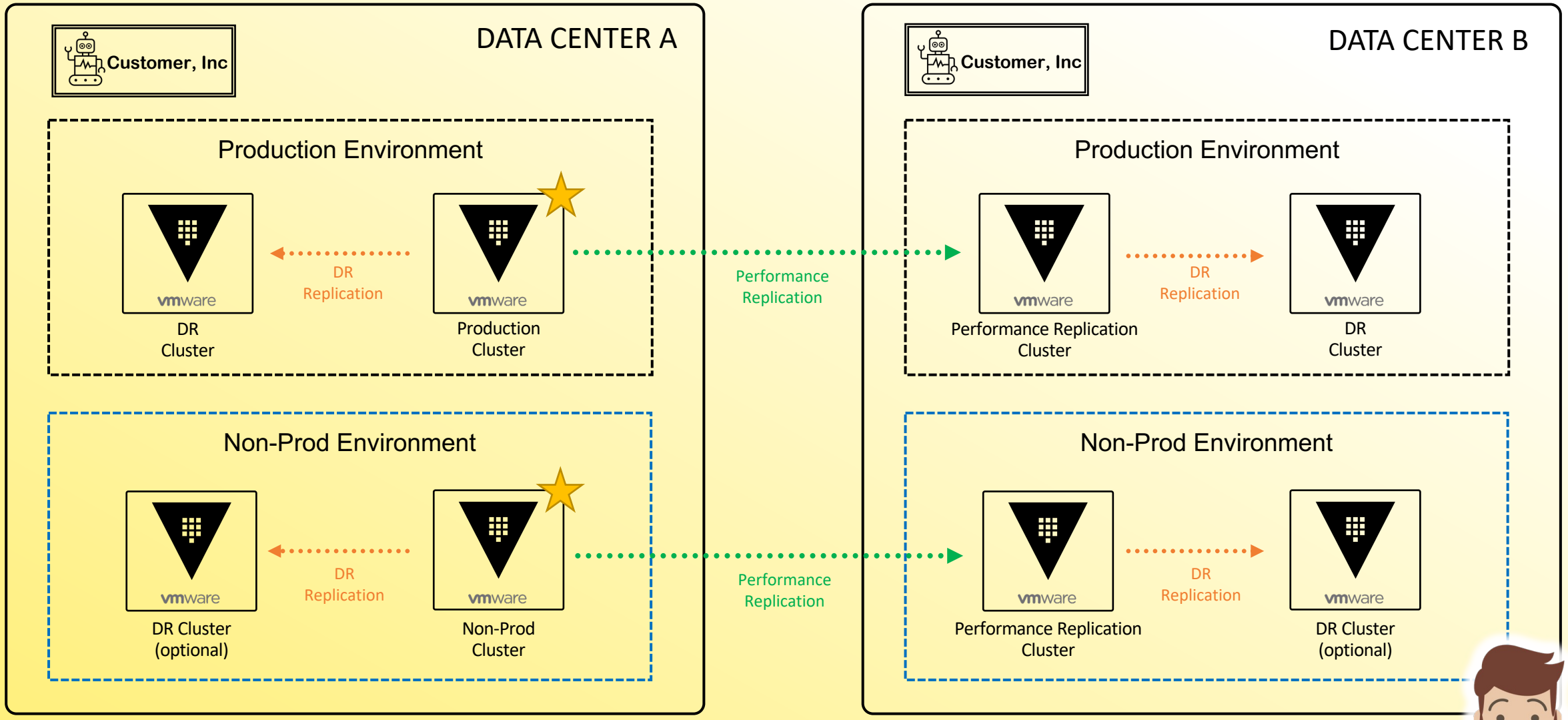


Replication Architecture



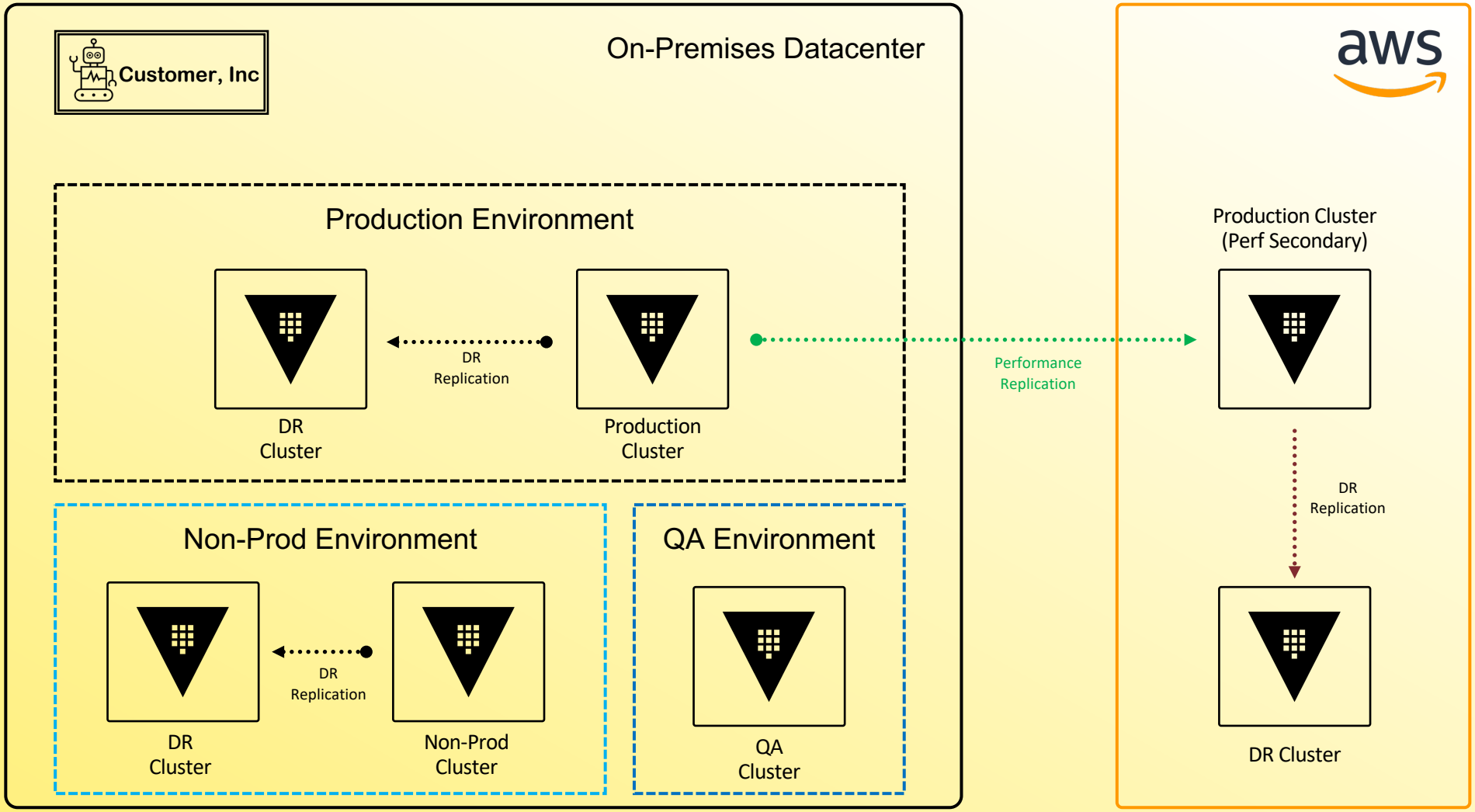

LONDON
PERFORMANCE
DR
PRIMARY
DR
DALLAS
PERFORMANCE
REPLICATION
PERFORMANCE REPLICATION
SYDNEY
PERFORMANCE
DR

Real-World Customer Example



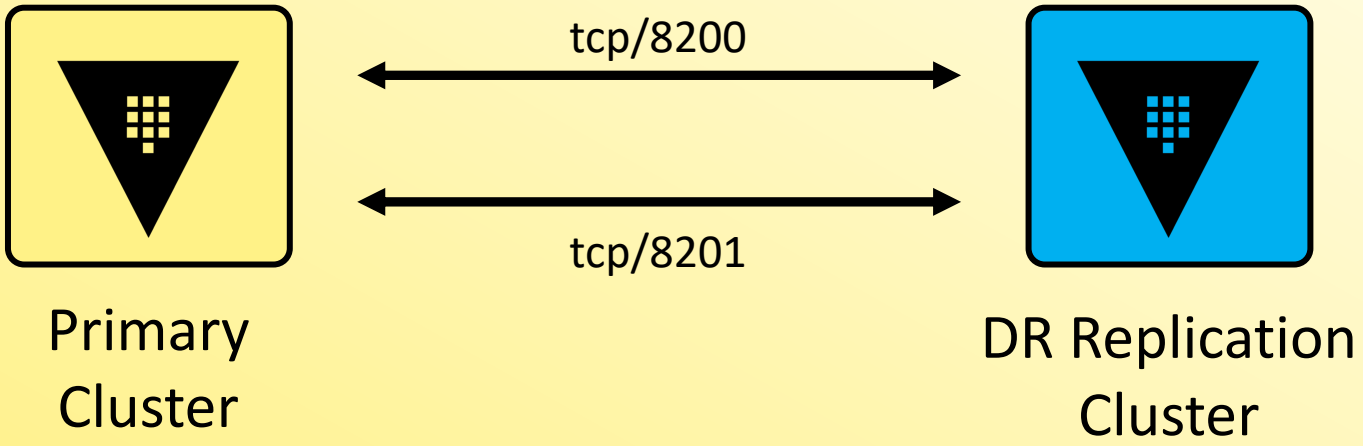
Primary Cluster in Replica Set

Real-World Customer Example



Networking Requirements

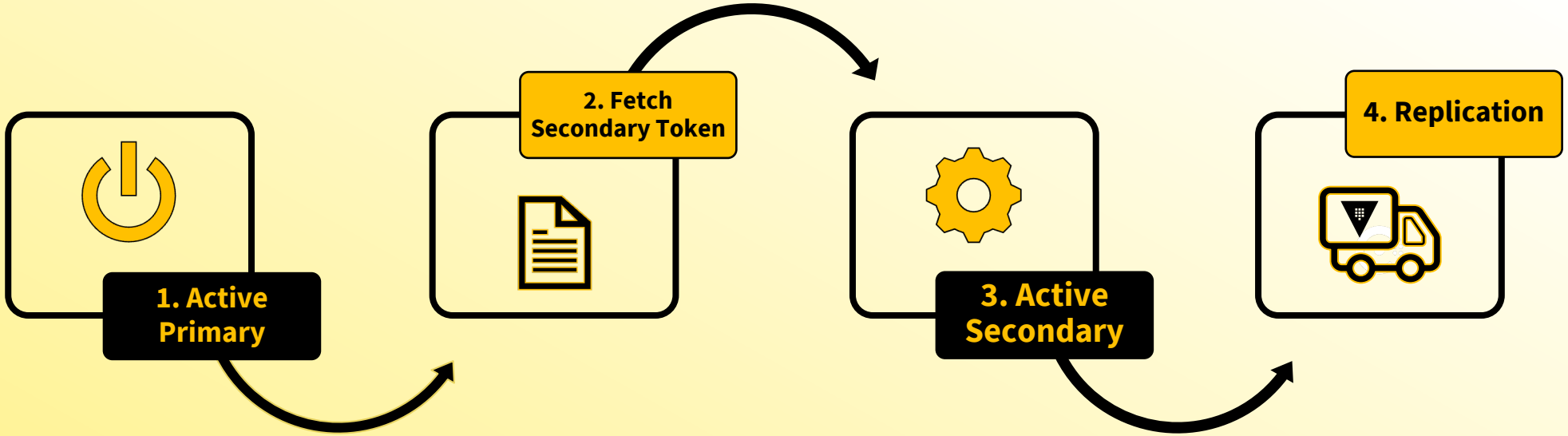
- Communication between clusters must be permitted to allow replication, RPC forwarding, and cluster bootstrapping to work as expected.
- If using DNS, each cluster must be able to resolve the name of the other cluster



Networking Ports

Source	Destination	Port	Protocol	Direction	Purpose
Client Machines	Load balancer	443	tcp	Incoming	Request distribution
Load Balancer	Vault Servers	8200	tcp	Incoming	Vault API
Vault Servers	**Vault Servers**	**8200**	**tcp**	**Bidirectional**	**Cluster bootstrapping**
Vault Servers	**Vault Servers**	**8201**	**tcp**	**Bidirectional**	**Raft, replication, request forwarding**
Vault Servers	External Systems	Various	Various	Various	External APIs

How Do We Set All of this Up?



Activate DR Replication on the Primary as a DR Primary

Create a secondary token on the Primary cluster

Activate DR Replication on the Secondary cluster as a DR secondary

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

Activating DR Replication

- Replication is NOT enabled by default, so you must enable it on each cluster that will participate in the replica set
- Enables an internal root CA on the primary Vault cluster - creates a root certificate and client cert
- Vault creates a mutual TLS connection between the nodes using self-signed certificates and keys from the internal CA – *NOT the same TLS configured for the listener*
  - If Vault sits behind a load balancer which is terminating TLS, it will break the mutual TLS between the nodes if inter-cluster traffic is forced through the load balancer

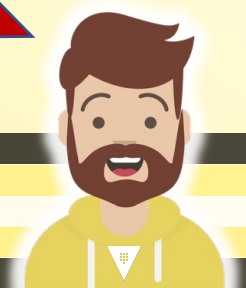
Secondary Token

- A secondary token is required to permit a secondary cluster to replicate from the primary cluster
- Due to its sensitivity, the secondary token is protected with response wrapping
- Multiple people should “have eyes” on the secondary token once it’s been issued until it is submitted to the secondary cluster
- Once the token is successfully used, it is useless (single-use token)
- The secondary token includes information such as:
  - The redirect address of the primary cluster
  - The client certificate and CA certificate

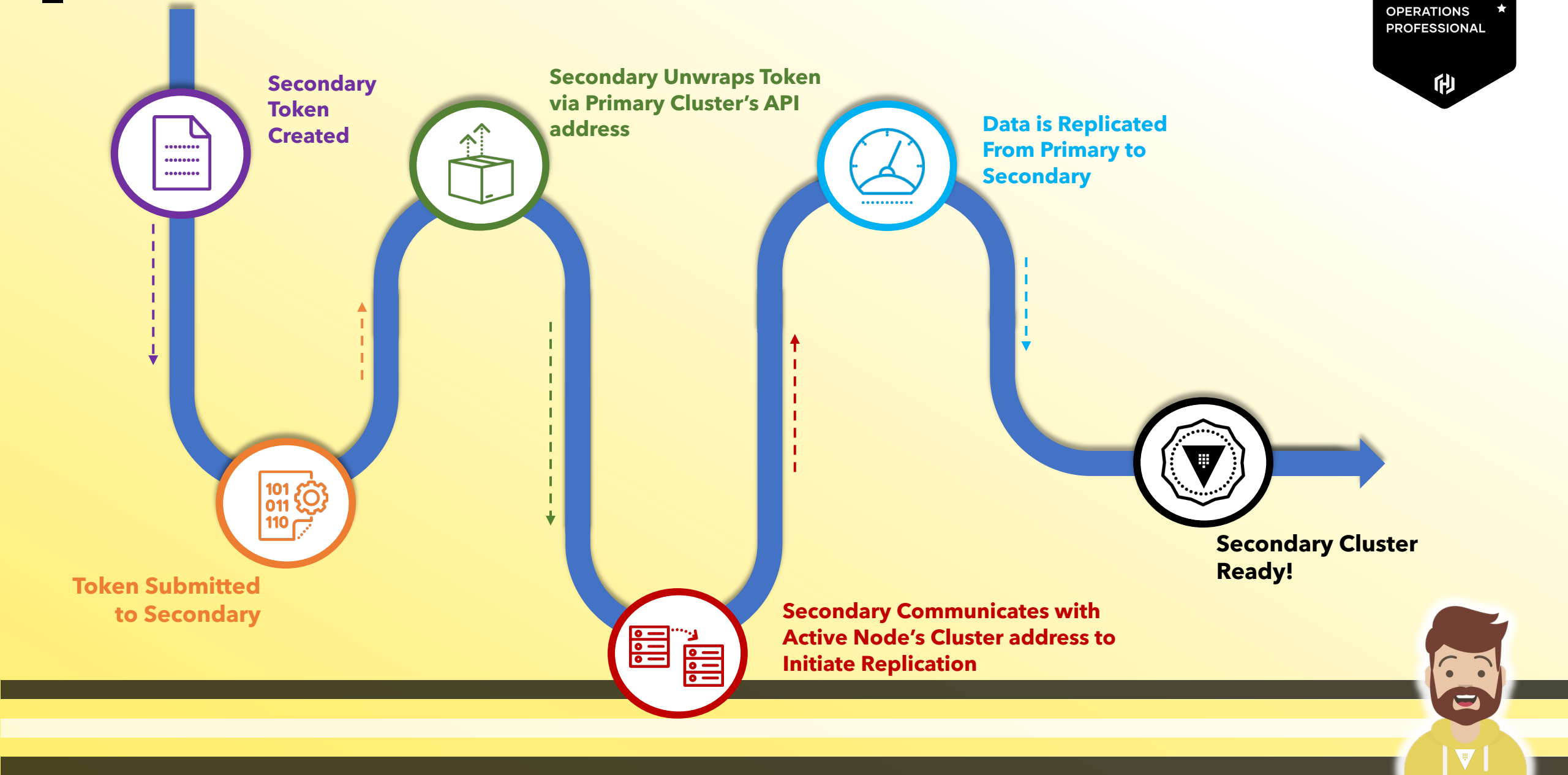
Secondary Token - Unwrapped


```
{
  "request_id": "98d4c7a5-0f00-4872-1cad-6ab8fa35694c",
  "lease_id": "",
  "lease_duration": 0,
  "renewable": false,
  "data": {
    "ca_cert":
"MIICfjCCAd+gAwIBAgIIVQciUMO14jswCgYIKoZIzj0EAwQwMzExMC8GA1UEAxMocmVwLTA3MzQyYTBiLWJhZjktNTRhZC00MjcyLWVlZTE0NTFmMGQyNDAgFw0yMjA1MjMxNzMxMTlaGA8yMDUyMD
UyMzA1MzE0OVowMzExMC8GA1UEAxMocmVwLTA3MzQyYTBiLWJhZjktNTRhZC00MjcyLWVlZTE0NTFmMGQyNDCBmzAQBgcqhkjOPQIB...",
    "client_cert":
"MIICZjCCAcigAwIBAgIIKW4DvMJIDt4wCgYIKoZIzj0EAwQwMzExMC8GA1UEAxMocmVwLTA3MzQyYTBiLWJhZjktNTRhZC00MjcyLWVlZTE0NTFmMGQyNDAgFw0yMjA1MjMxNzMzMjNaGA8yMDUyMD
UyMzA1MzM1M1owLzEtMCsGA1UEAxMkZjYwNmEwMGItMTA0Ny05...",
    "client_key": {
      "d":
100063135551708651312219621434769005305861020311916751595635823721144717769621270584557091396035214741204011866085797156614395614941293880996038154910074082 6,
      "type": "p521",
      "x":
658524146724038415139812414260046924438287594112058742800811836857332880495560891821166866953079570149591717031865169982332929869016397134936233531768630487 5,
      "y":
456334071742932065617972528983665278904799258735615931964928472922561093828333196391348485375693735165980549972782693606164075237449636858048806745513650171 7
    },
    "cluster_id": "0d127970-99ce-152f-0311-3b081d1264d3",
    "encrypted_client_key": null,
    "id": "secondary",
    "mode": 512,
    "nonce": null,
    "primary_cluster_addr": "https://vault-pri.hcvop.com:8201",
    "primary_public_key": null
  },
  "warnings": null
}
```


This is not a normal thing you would do. I simply did it to show you what information the secondary token included



How is the Secondary Token Used?



Vault
CERTIFIED OPERATIONS PROFESSIONAL

Configure Replication on the CLI

Vault
CERTIFIED OPERATIONS PROFESSIONAL

1 Activate DR Replication

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

2 Create the Secondary Token

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

Name it what you want

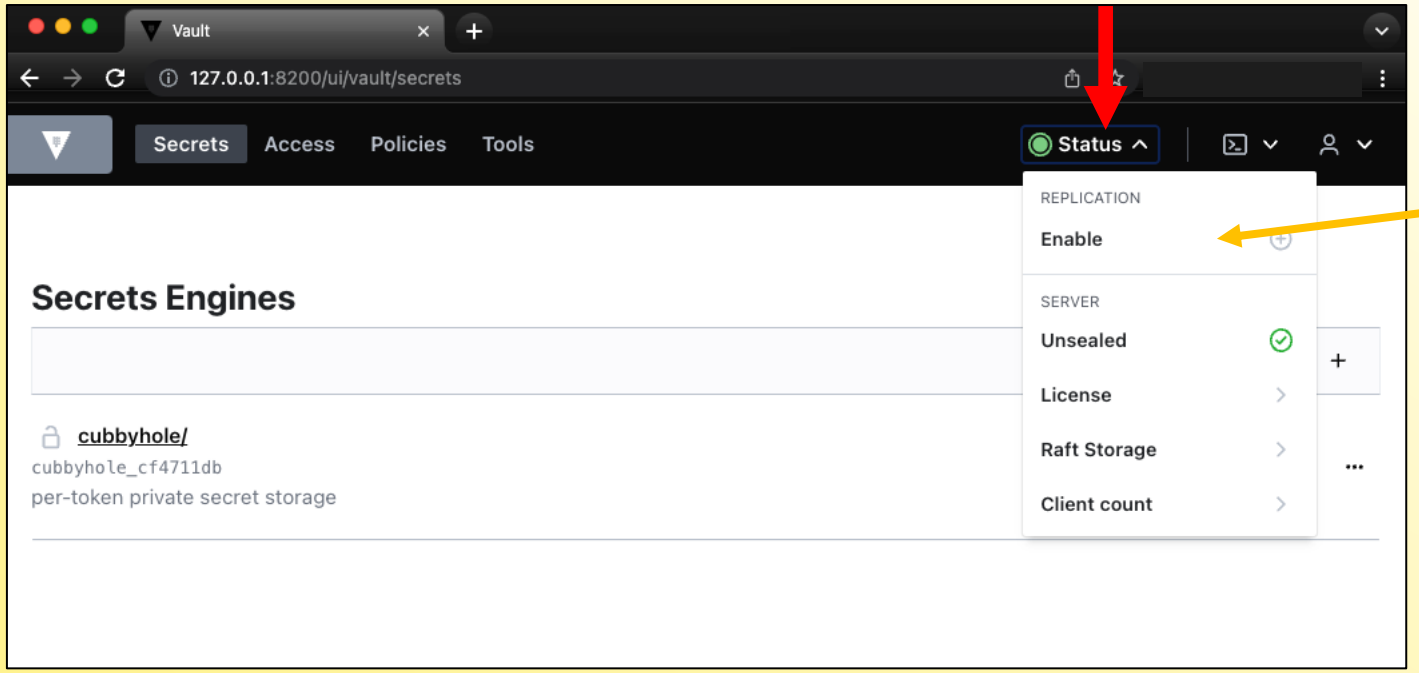
3 Activate the Secondary Cluster

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

Provide token from primary cluster (command above)

Configure Replication using the UI

Enable Replication on Primary



Enable Replication

Configure Replication using the UI

Select Type and Mode on Primary

Vault
CERTIFIED
OPERATIONS
PROFESSIONAL

Select DR Replication

Choose Primary for the DR Primary cluster

Vault

127.0.0.1:8200/ui/vault/replication

Secrets Access Policies Tools Status

Enable Replication

Type of replication

In both Performance and Disaster Recovery (DR) Replication, secondaries share the underlying configuration, policies, and supporting secrets as their primary cluster.

Disaster Recovery (DR)

Disaster Recovery Replication is designed to protect against catastrophic failure of entire clusters. Secondaries do not forward service requests until they are elected and become a new primary.

Performance

Performance Replication scales workloads horizontally across clusters to make requests faster. Local secondaries handle read requests but forward writes to the primary to be handled.

Cluster mode

primary

Primary cluster address *(optional)*

Overrides the cluster address that the primary gives to secondary nodes.

Enable Replication

Configure Replication using the UI

Add a Secondary

Vault
CERTIFIED
OPERATIONS
PROFESSIONAL

Vault

127.0.0.1:8200/ui/vault/replication/dr

Secrets Access Policies Tools Status

Replication Disaster Recovery

Disaster Recovery primary

Details Manage Secondaries

View existing Secondaries

State

The cluster's current operating state.

running

Last WAL entry

Index of last Write Ahead Logs entry written on local storage. Updates every ten seconds.

57

0 Known Secondaries

View all

No known dr secondary clusters associated with this cluster

Associated secondary clusters will be listed here.
Add your first secondary cluster to get started.

Add secondary

Add a new Secondary

primary_cluster_addr

The configuration of the cluster. This was set when

None set

Configure Replication using the UI

Name Secondary and Get Secondary Token

Vault
CERTIFIED
OPERATIONS
PROFESSIONAL

Vault

127.0.0.1:8200/ui/vault/replication/dr/secondaries/add

Secrets Access Policies Tools Status

Replication Disaster Recovery

Disaster Recovery primary

Details Manage Secondaries

Generate a secondar n

Generate a token to enable Disaster Recovery replication or change primaries on secondary cluster.

Secondary ID

my-first-dr-secondary

This will be used to identify a secondary cluster once a connection has been established with the primary.

Time to Live (TTL) for generated secondary token

If not set, the default value (30 minutes) will be used

Generate token Cancel

Give it a Name

Configure Replication using the UI

Copy New Secondary Token from Primary Cluster

Vault
CERTIFIED
OPERATIONS
PROFESSIONAL

Secondary Token

Copy your token

This token can be used to enable Disaster Recovery replication or change primaries on the secondary cluster.

Activation token

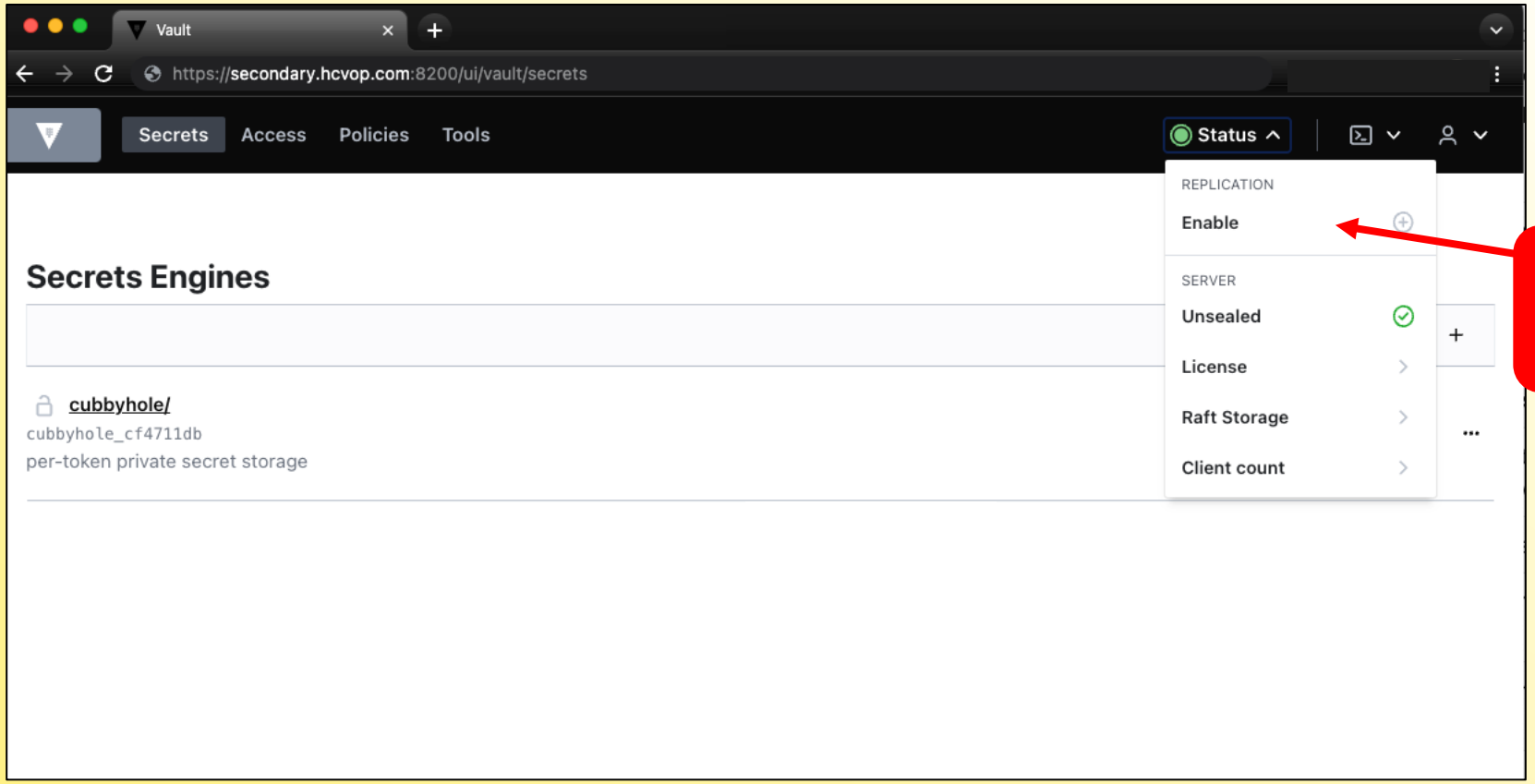
eyJhbGciOiJFUzUxMiIsInR5cCI6IkpXVCJ9.eyJhY2Nlc3NvciI6IiIsImFkZHIiOi
JodHRwOi8vYnRrLW1hY2Jvb2stcHJvOjgyMDAiLCJleHAiOjE2NTMzMzA2M
zgsImlhdCI6MTY1MzMyODgzOCwianRpIjoiaHZzLkRYSWV5ZGw3aU5TVW
RyMjlQUWZ1S0t6RyIsIm5iZiI6MTY1MzMyODgzMywidHlwZSI6IndyYXBwa

TTL	1800s
Expires	

Copy & Close

Configure Replication using the UI

Enable Replication on Secondary Cluster



Enable Replication on Secondary

Configure Replication using the UI

Configure Secondary Cluster for Replication as a Secondary

Vault
CERTIFIED
OPERATIONS
PROFESSIONAL

Vault

https://secondary.hcvop.com:8200/ui/vault/replication

Secrets Access Policies Tools Status

Enable Replication

Type of replication

In both Performance and Disaster Recovery (DR) Replication, secondaries share the underlying configuration, policies, and supporting secrets as their primary cluster.

Disaster Recovery (DR)

Disaster Recovery Replication is designed to protect against catastrophic failure of entire clusters. Secondaries do not forward service requests until they are elected and become a new primary.

Performance

Performance Replication scales workloads horizontally across clusters to make requests faster. Local secondaries handle read requests but forward writes to the primary to be handled.

Cluster mode

secondary

This will immediately clear all data in this cluster!

Secondary activation token

eyJhbGciOiJFUzUxMiIsInR5cCI6IkpXVCJ9.eyJhY2Nlc3NvciI6IiIsImFkZHIiOiJodHRwOi8vYnRrLW1hY2Jvb2stcHJvOjgyMDAiLCJleHAiOjE2NTMzMzM1ODUsIml
hdCI6MTY1MzMzMTc4NSwianRpIjoiaHZzLnh4cE5vNmZkYVh2T3R1cFA5UG5mSE9YVyIsIm5iZiI6MTY1MzMzMTc4MCwidHlwZSI6IndyYXBwaW5nIn0.ANXC0
EecO3pMCVbQrlq9SpF6cE187oJOoIltZXsUUMr-BhgeceEyaHzl2IsNE8ftmi-bThTYV-pN8aeZr6Y83-
s2AW_YSjcrrzrOY29ISMYDW1XJ6bDtsiQvB9vBBE_gphhB139bssQCGVtML_MMcZeGfL2whxs3fxGYWMGYLRWkM5k_

Primary API address *(optional)*

Select Disaster Recovery Replication

Select Secondary

Paste Secondary Token Here

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