# SKYLINES

ACADEMY

# Vault Clustering and Replication

Bryan Krausen
Sr. Solutions Architect
@btkrausen

SKYLINES ACADEMY

# Vault Clustering and Replication

- Types of Vault Nodes
- Vault Clustering
- Vault Replication
- Vault Ports and Protocols
- Vault Deployment Strategies

# Types of Vault Nodes

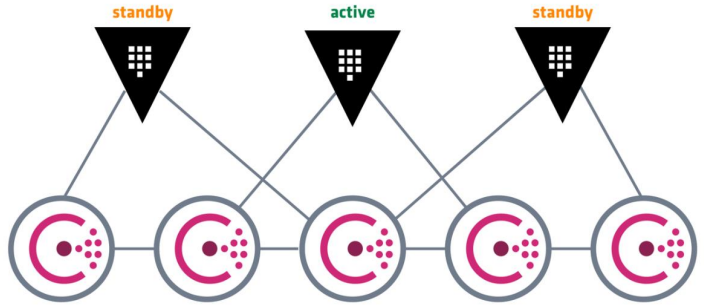
SKYLINES ACADEMY

- Three types of nodes:
  - **Active Node**: Responsible for all reads and writes in a basic Vault cluster configuration
  - **Standby Node**: Will forward ALL requests to the Active Node in a basic cluster configuration
  - **Performance Standby**: Can process read requests for clients without forwarding to Active Node. Will still forward write requests to Active node [Enterprise license required]

# Vault Clustering

SKYLINES ACADEMY

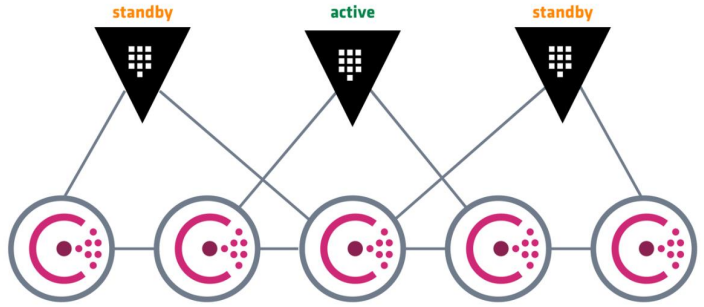
- Vault provides built-in high-availability in the form of clustering
- Multiple Vault instances form a cluster when sharing a storage backend without additional configuration
- The storage backend must support high-availability
- Clustering is available in both Open Source and Enterprise



# Vault Clustering (continued)

SKYLINES ACADEMY

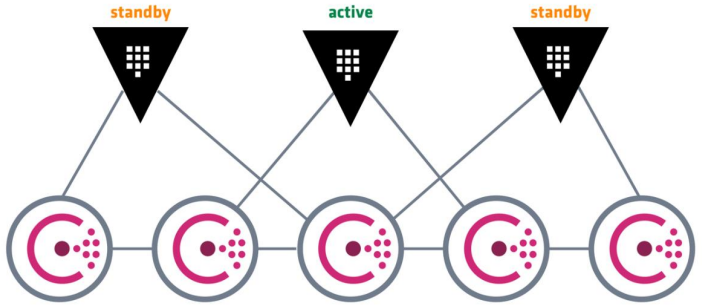
- Cluster consists of Active node and Standby node(s)
- How is the cluster leader determined?
- The first Vault node who grabs a lock in storage backend
- The successful node becomes the Active node; all others become Standby nodes



# Vault Clustering (continued)

SKYLINES ACADEMY

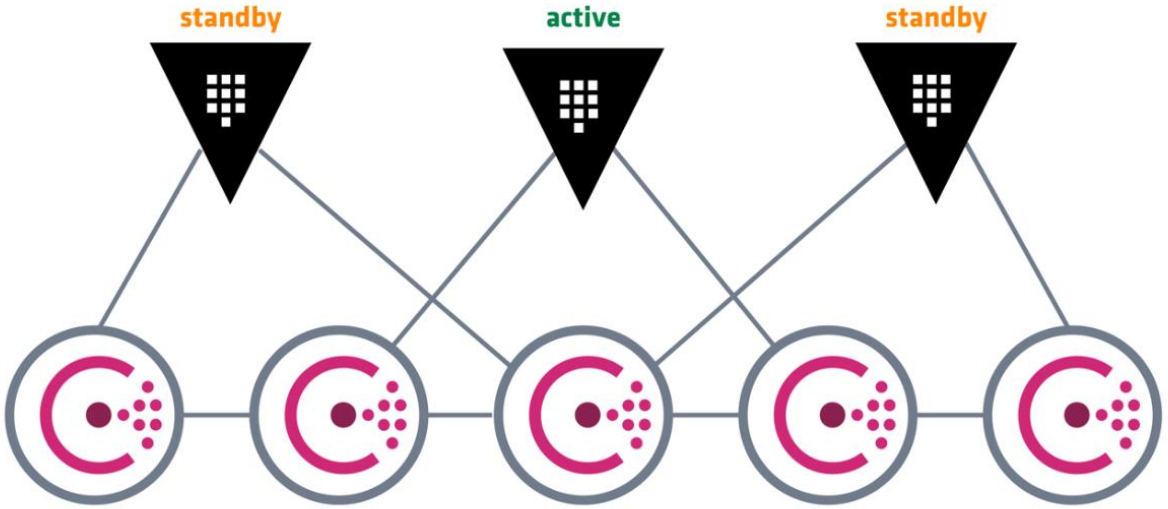
- Vault is generally front-ended with a load-balancer or Consul
- In this case, the load-balancer is for high-availability, not load balancing traffic
- Health checks on the load balancer can determine which node is the active node
- curl https://<ipaddress>:8200/v1/sys/health
  - HTTP Response 200 = initialized, unsealed, and active
  - HTTP Response 429 = unsealed and standby



# Vault Clustering (continued)

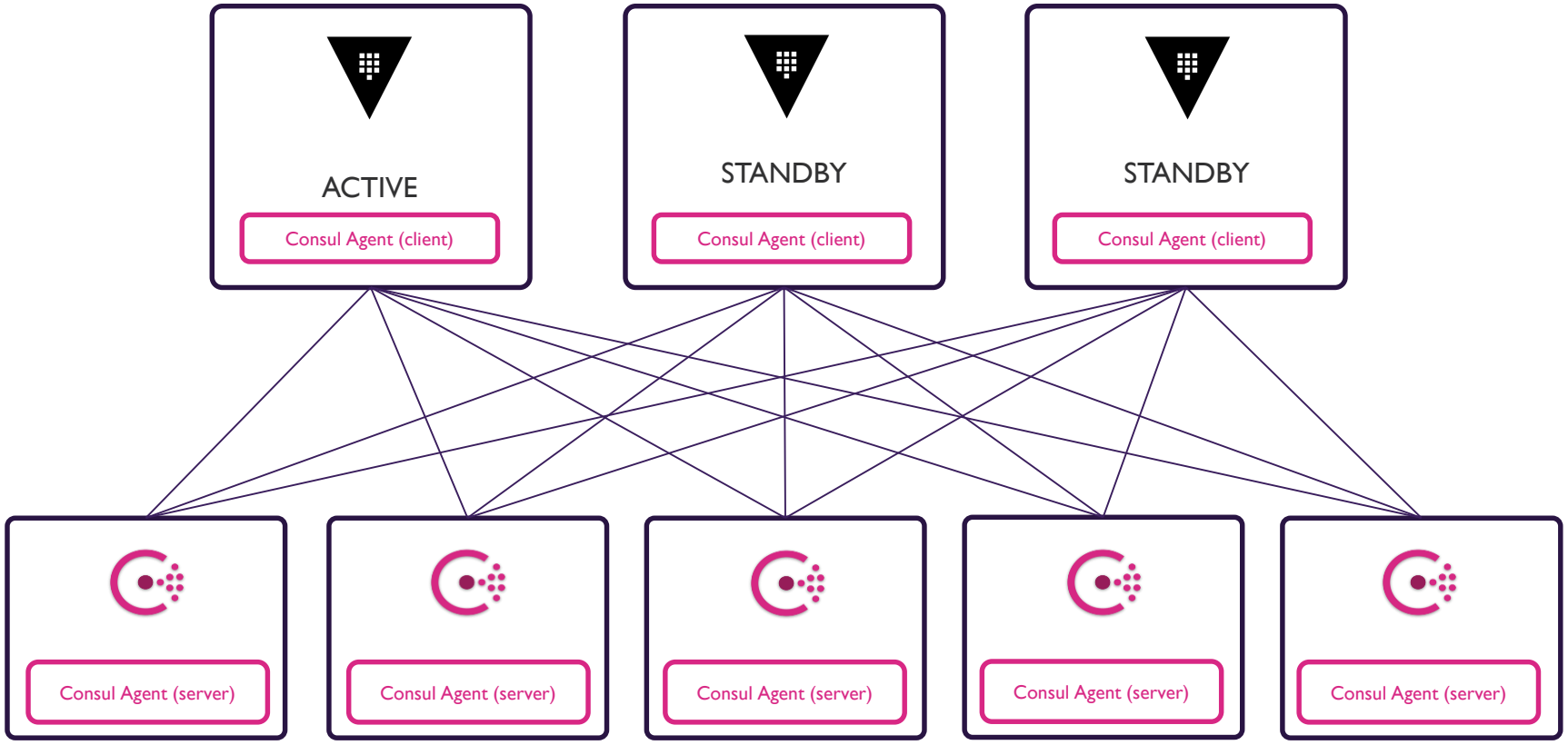
SKYLINES ACADEMY

- Vault can be tightly integrated into Consul as well
  - **Active Node**: active.vault.service.consul
  - **Standby Node:** standby.vault.service.consul



# Vault Clustering

SKYLINES ACADEMY

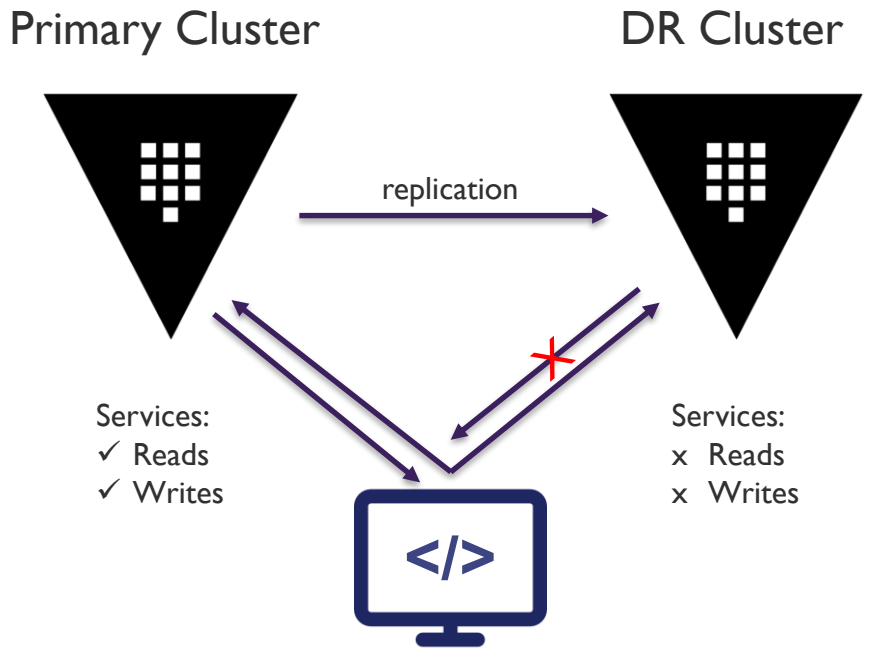


# Vault Replication [Enterprise Feature]

SKYLINES ACADEMY

## Disaster Recovery Replication

- Replicates the following data:
  - K/V store
  - Policies
  - Tokens
- Warm Standby
- Does Not Serve Client Requests

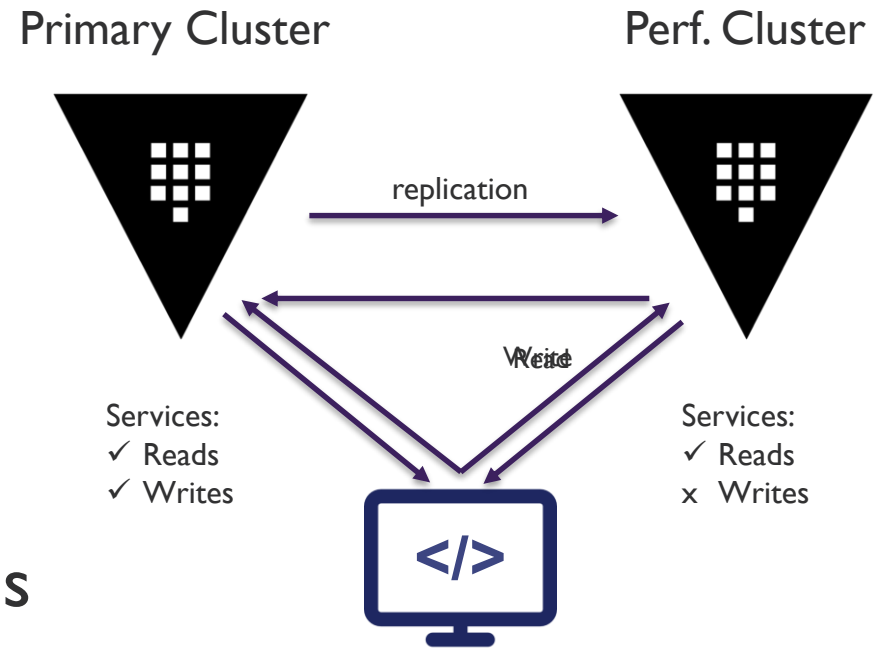


# Vault Replication [Enterprise Feature]

SKYLINES ACADEMY

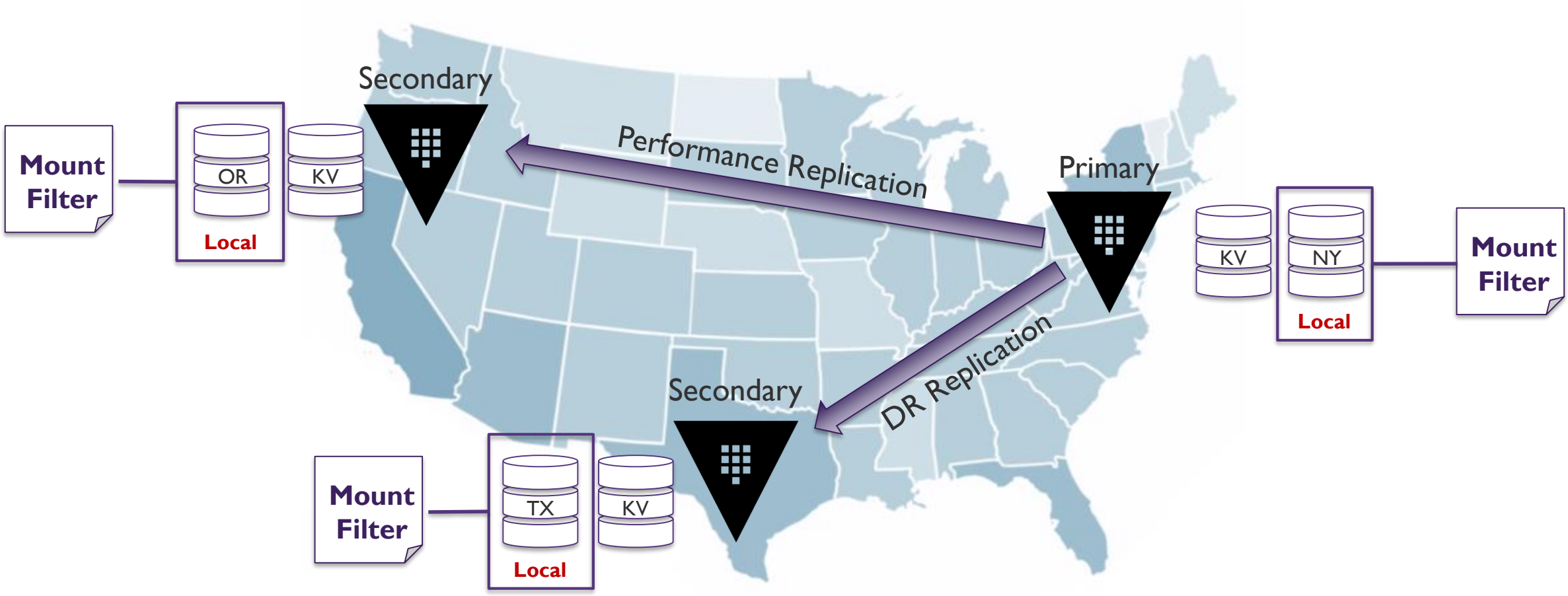
**Performance Replication**

- Replicates the following data:
  - K/V store
  - Policies
  - Does NOT replicate tokens
- Will Serve Client Requests (reads)
- Used to 'extend' Vault across data centers or provide multi-cloud access



# Replication & Filters

SKYLINES ACADEMY



# Vault Ports and Protocols

SKYLINES ACADEMY

- All communication for Vault uses TLS

TCP/8200 – general port for UI and API

TCP/8201 – Used for server to server communication

- Consul client requires additional ports

TCP/8500 – Consul client to server communication

TCP/UDP 8301 – Serf LAN for LAN gossip

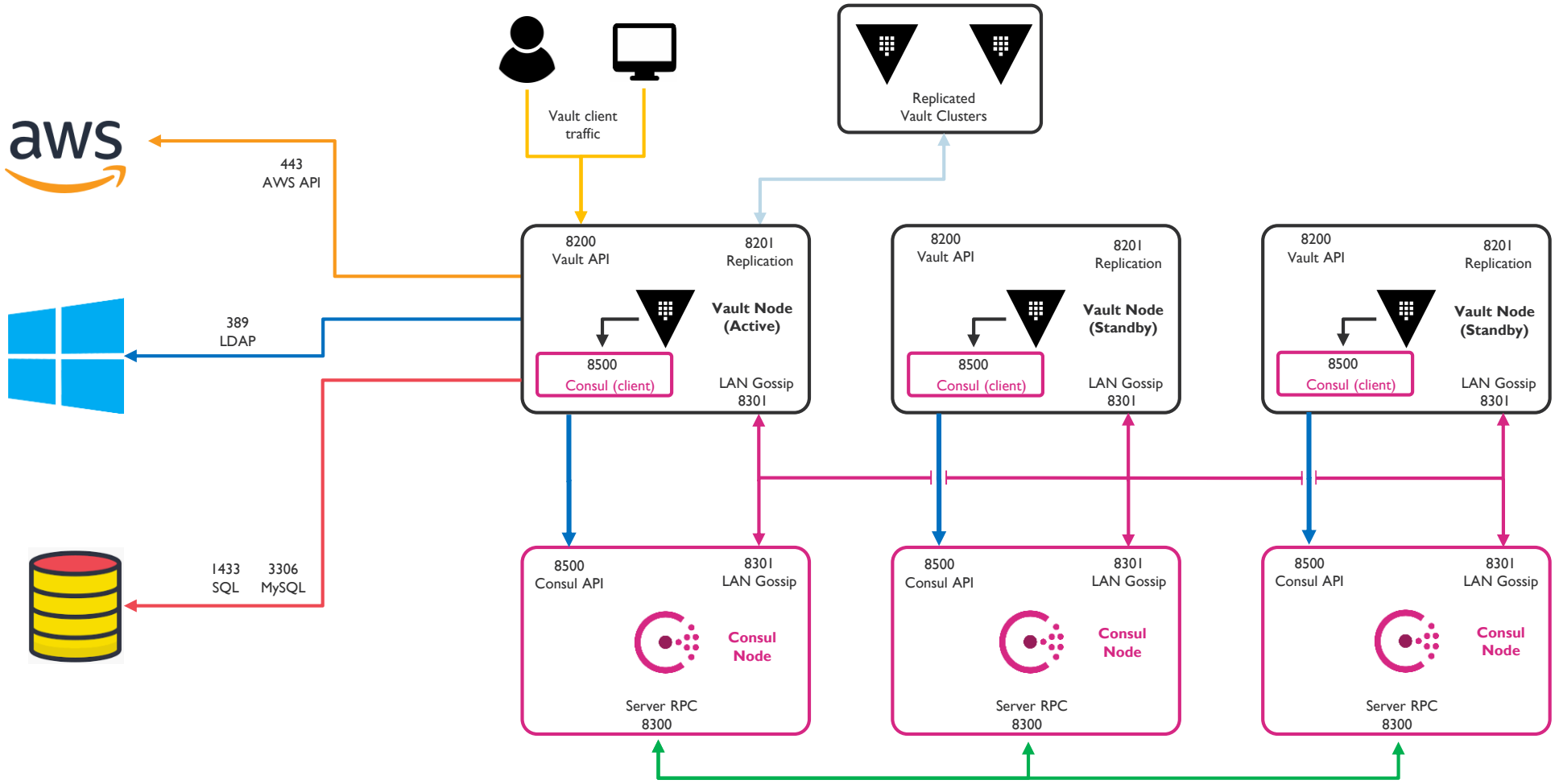
# Communication Requirements

SKYLINES ACADEMY

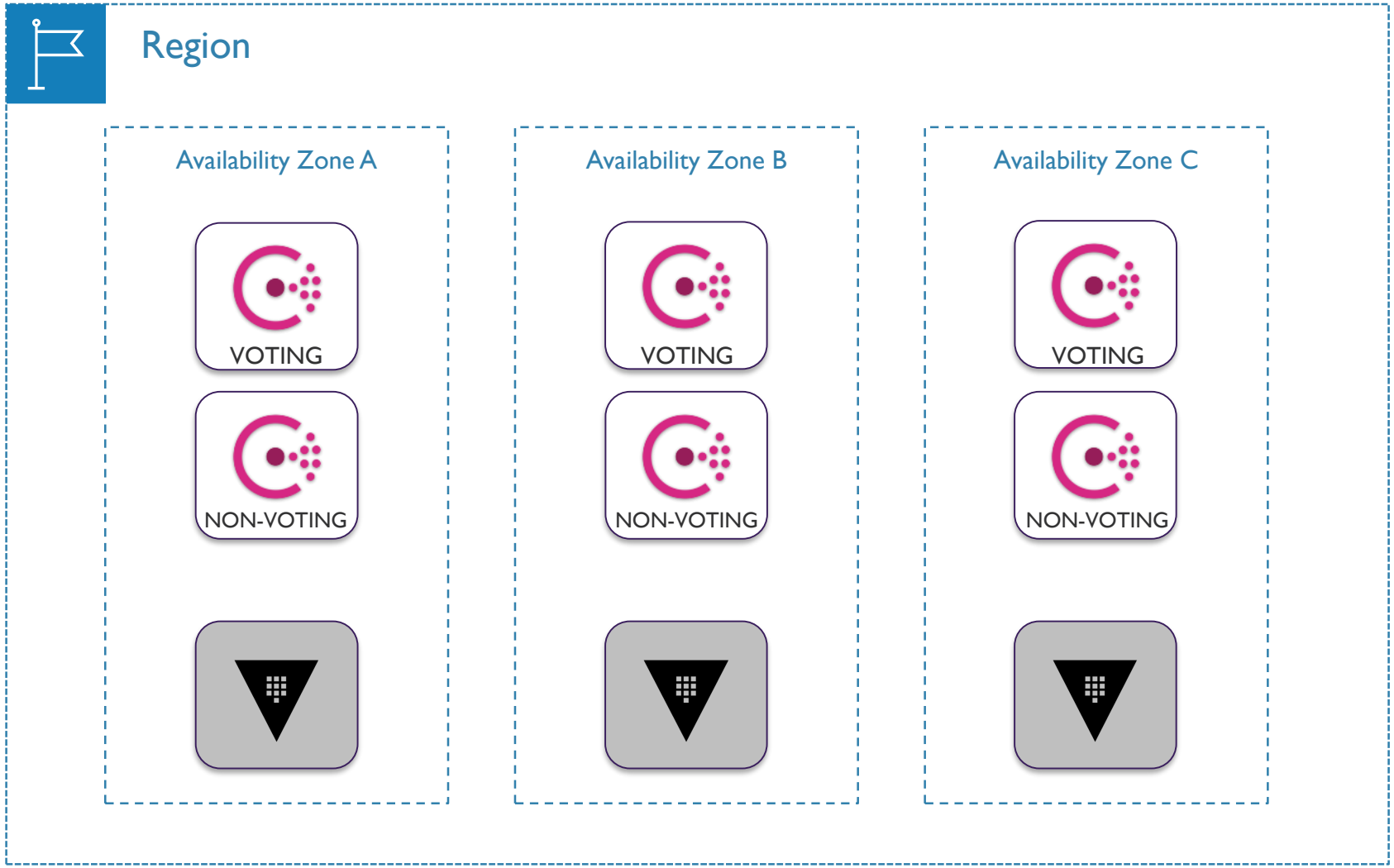
| Source | Target | Port | Protocol | Direction | Description |
|---|---|---|---|---|---|
| Vault Clients | Vault Load Balancer | 8200 | tcp | ingress | Vault Interface (API) |
| Vault Load Balancer | Vault Nodes | 8200 | tcp | ingress | Vault Interface (API) |
| Vault Nodes | Vault Nodes | 8201 | tcp | bidirectional | Request Forwarding |
| Vault Nodes | Vault Nodes | 8301 | tcp/udp | bidirectional | LAN Gossip Communication |
| Vault Nodes | Consul Nodes | 8301 | tcp/udp | bidirectional | LAN Gossip Communication |
| Consul Nodes | Consul Nodes | 8300 | tcp/udp | bidirectional | Server RPC |
| Consul Nodes | Consul Nodes | 8301 | tcp/udp | bidirectional | LAN Gossip Communication |
| Vault Nodes | Consul Nodes | 8500 | tcp | ingress | Consul Interface (API) |
| Vault Primary Cluster | Secondary Cluster | 8201 | tcp | bidirectional | Vault Replication |

# Traffic Flow

SKYLINES ACADEMY



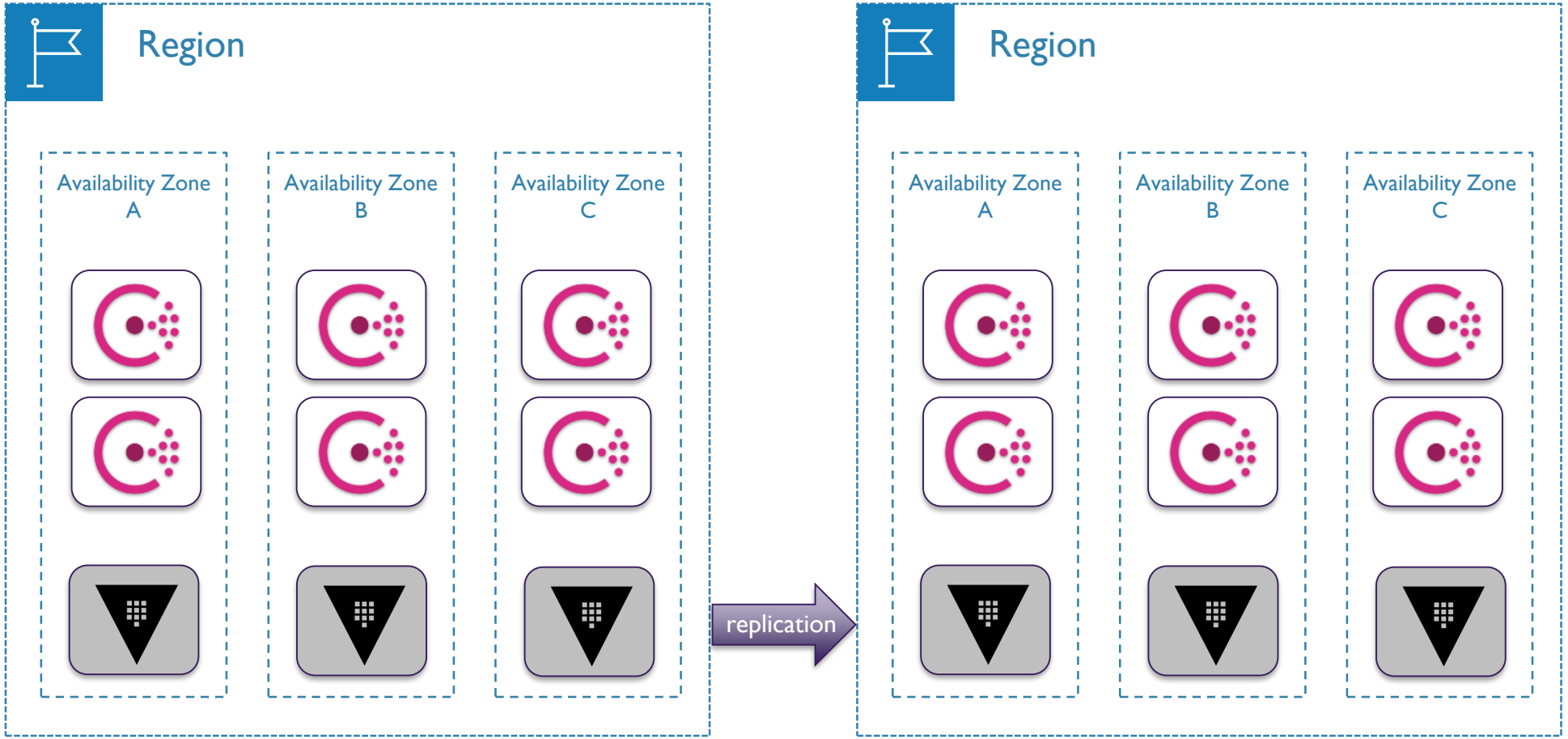
# Vault Deployment Strategy – Single Cluster




- Standard 3 x 6 Deployment
  - Formerly 3 x 5
  - Provides n+2 redundancy
- Takes advantage of Consul Autopilot features
- Could lose 3 Consul servers and 2 Vault clusters and still be online
- Use Spread Placement Groups (AWS) or VMware Anti-Affinity Rules
- Don't stretch Consul across data center boundaries

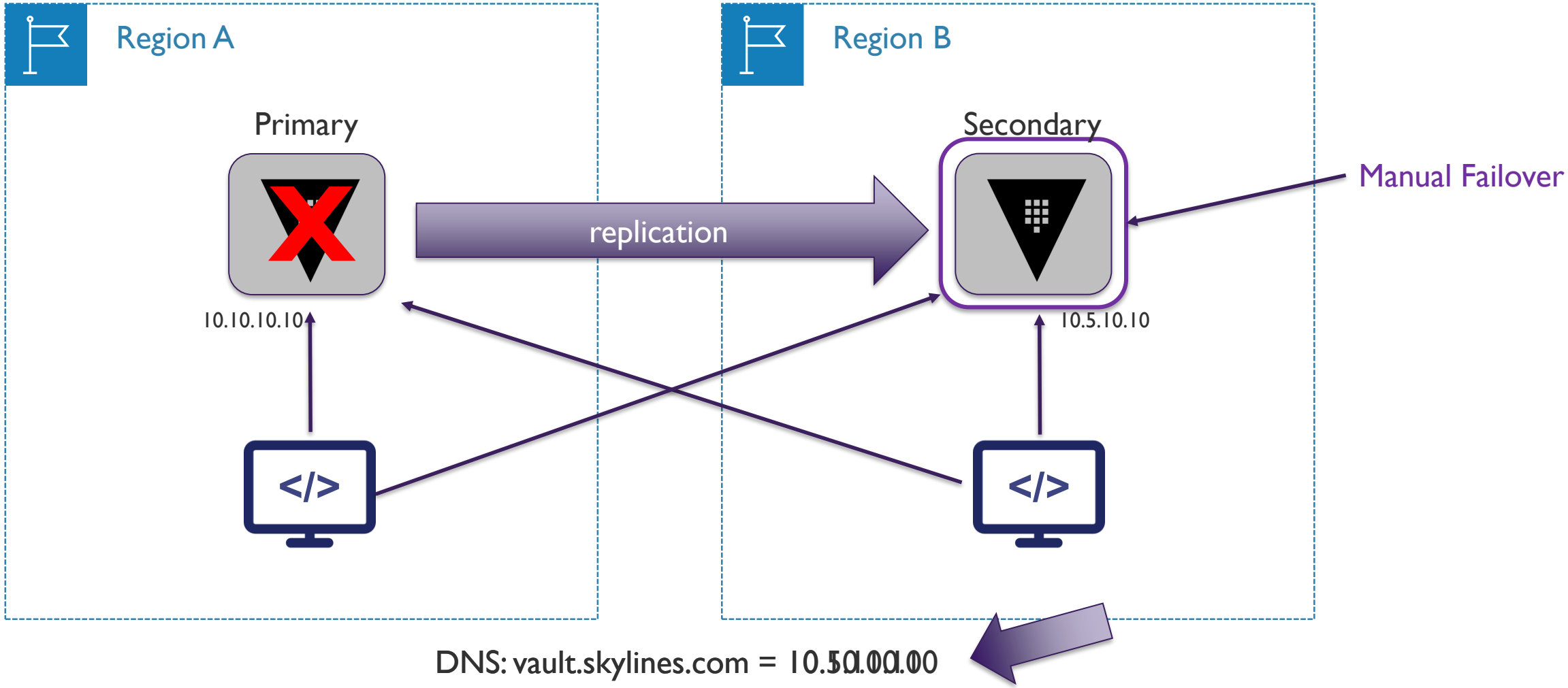
# Vault Deployment Strategy – DR Cluster

SKYLINES ACADEMY

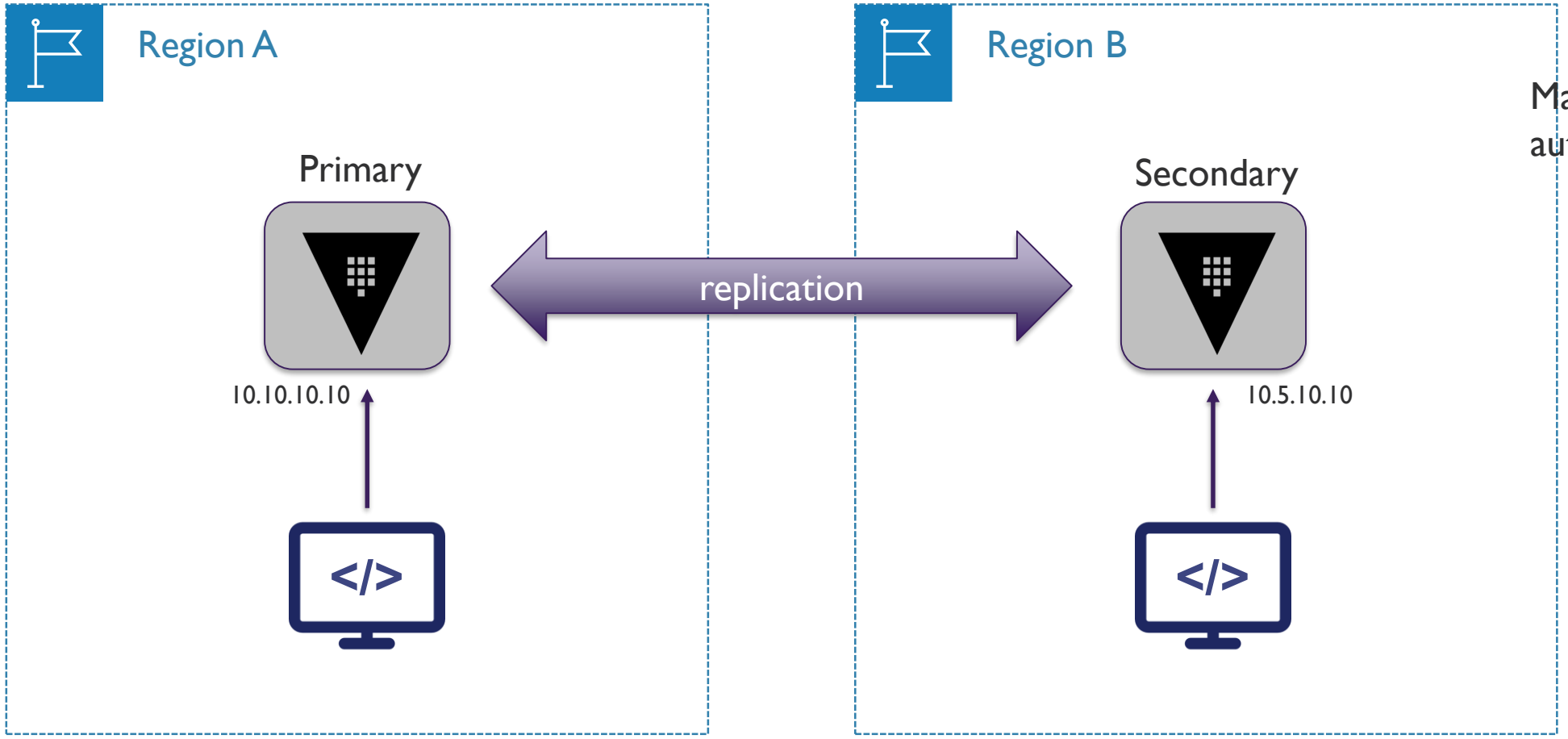



- Provides warm-standby
- Protects against regional/data center failure
- Replicates everything
- Design each cluster for high-availability per region/data center

# Vault Deployment Strategy – DR Cluster



# Vault Deployment Strategy – Performance Replication



# Vault Clustering and Replication

- Types of Vault Nodes
- Vault Clustering
- Vault Replication
- Vault Ports and Protocols
- Vault Deployment Strategies

SECTION RECAP

# SKYLINES

ACADEMY