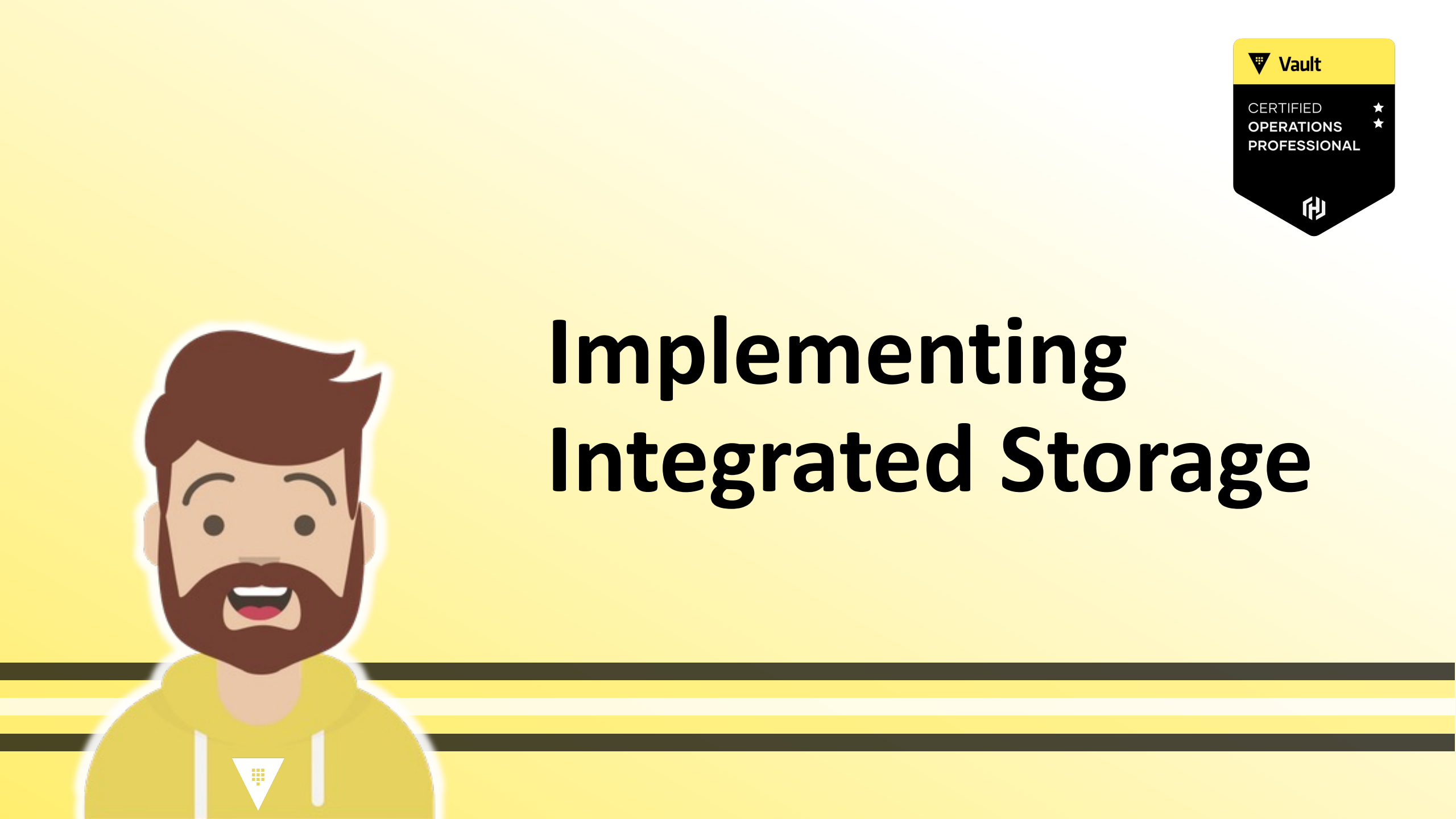
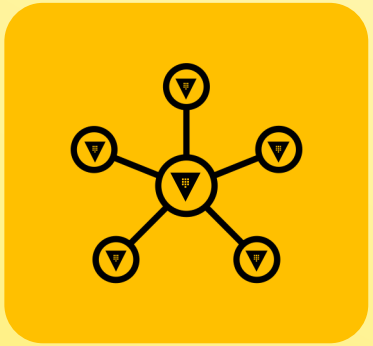


Implementing Integrated Storage

Vault Integrated Storage

Introduced in Vault 1.4, Integrated Storage provides a highly-available, durable storage backend without relying on any external systems



Uses the Raft Protocol

Integrated Storage uses the same underlying consensus protocol as Consul to handle cluster leadership and log management

Locally Stored Data

Vault data is stored locally on each node, and replicated to all other nodes in the cluster for high availability

Introduction to Integrated Storage

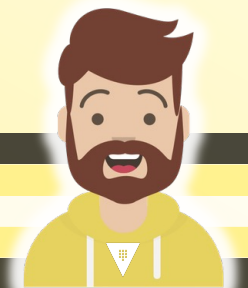
- All nodes in a Vault cluster have a replicated copy of Vault's data
- Eliminates the network hop of connecting from Vault to the external storage provider
- Also removes the administrative overhead of managing an external solution
  - When Vault has an outage, you only need to troubleshoot Vault

Introduction to Integrated Storage

- Since Integrated Storage stores all data on a local disk, it is recommended that you use storage optimized, high IOPS volumes wherever you are storing the data

Integrated Storage Features

Replication	Auto Snapshots	Cloud Autojoin	Autopilot
Integrated Storage is fully supported for Vault Enterprise environments using Performance and/or DR replication across data centers	A "Set and Forget" DR feature that schedules raft snapshots and copies them to cloud storage (Ent feature)	Stop joining clusters by hostname or IP address and discover other Vault nodes using cloud-based tags attached to your resources	Increase operational efficiency with automated features to help you manage your Vault clusters



Benefits of Integrated Storage Over Other Solutions

Reduced Complexity

All configuration is done within Vault. No external systems to provision alongside of Vault.

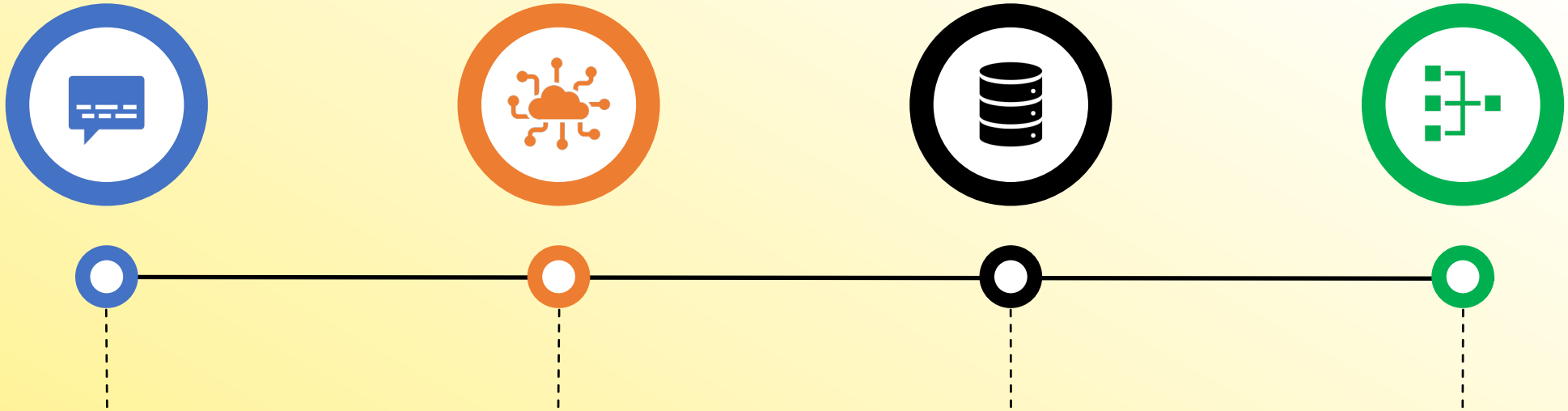
Decreased Costs

Fewer resources required for an enterprise-ready highly-available solution.

Easier to Troubleshoot

No external system to troubleshoot since Integrated Storage is a built-in solution. Storage is not memory-bound like Consul.

Integrated Storage Benefits



Similar Architecture

Same quorum requirements as Consul, so it's familiar

Fewer Networking Requirements

Raft only uses two ports for cluster operations and replication

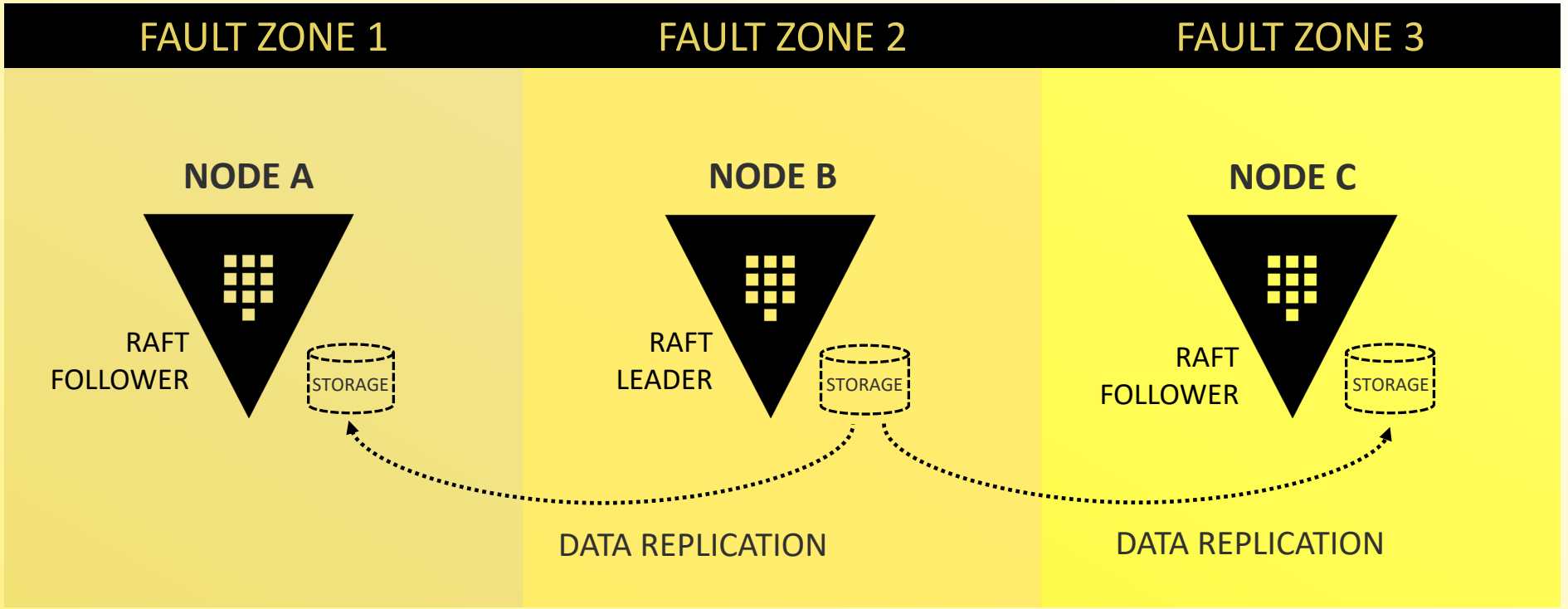
Not Memory-Bound

Stores data on local disk rather than in memory

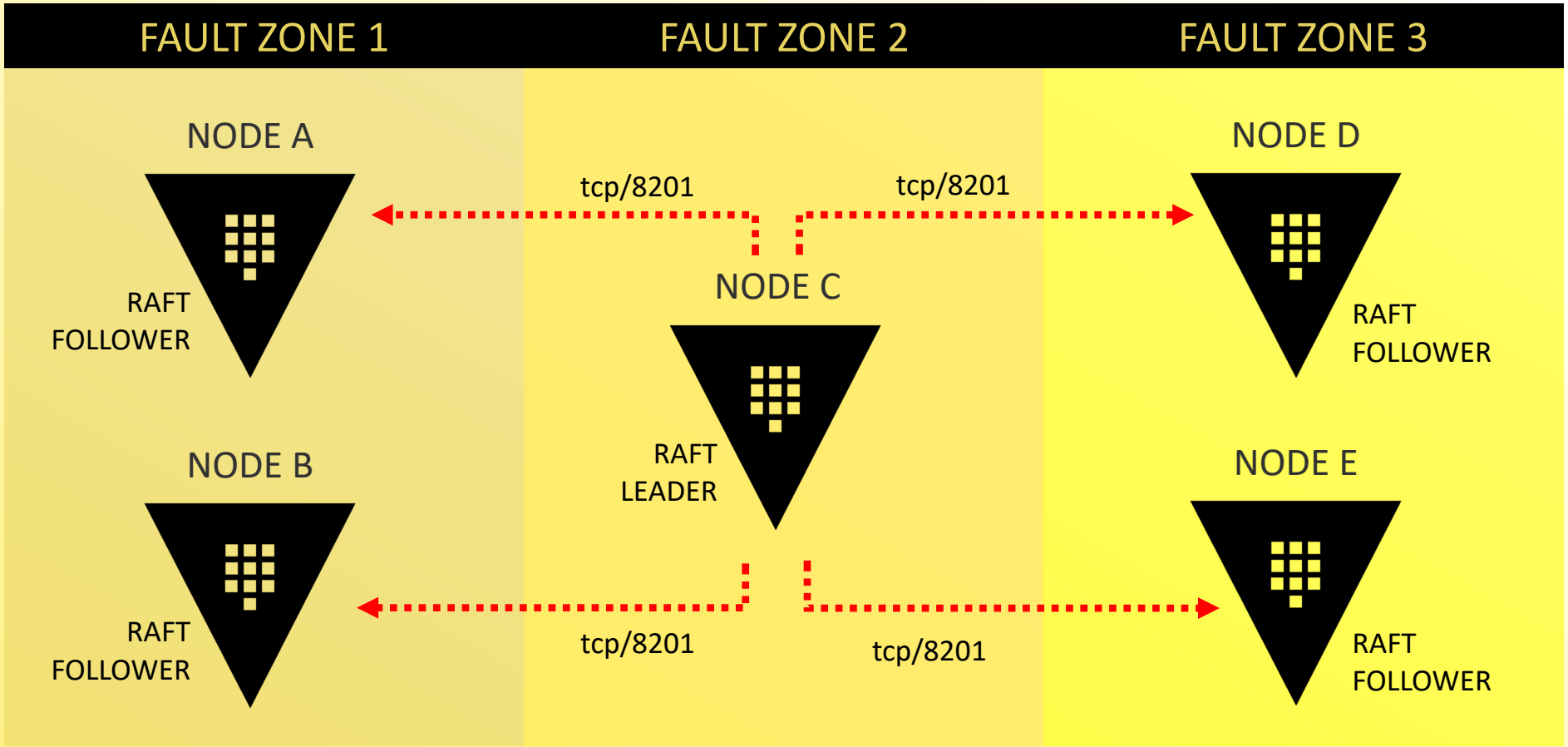
No Network Hops Required

Data is stored locally and doesn't need to be retrieved over the network

Reference Architecture – Development Cluster

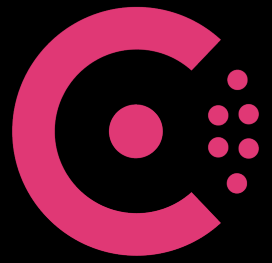


Reference Architecture – Production Cluster



Networking Requirements

CONSUL BACKEND



REQUIRED PORTS

Vault – 8200 – API
Vault – 8201 – RPC/Replication

Consul – 8500 – API
Consul – 8300 – RPC
Consul – 8301 - Serf

INTEGRATED STORAGE

REQUIRED PORTS

Vault – 8200 – API
Vault – 8201 – RPC/Replication

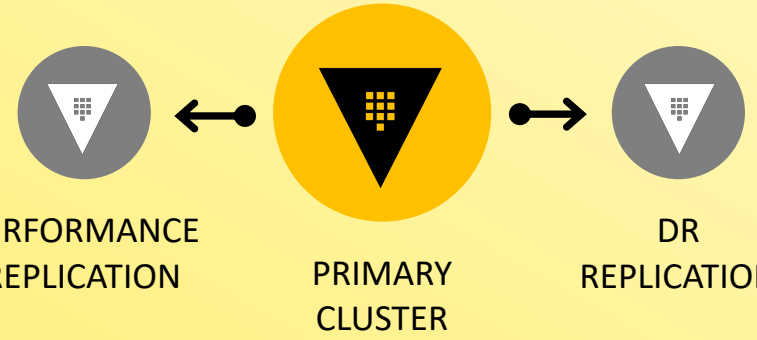
FEWER PORTS FOR COMMUNICATION

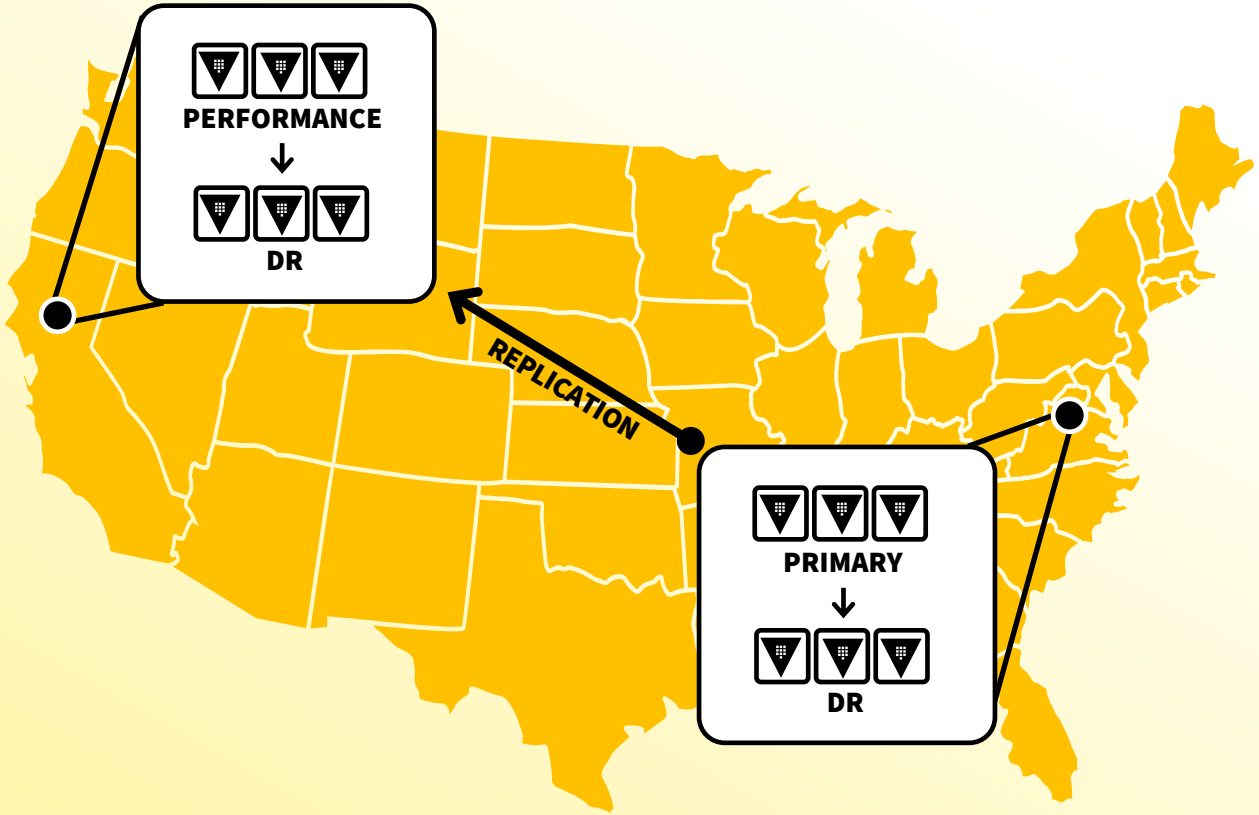
Fewer ports for communication means less attack surface for your Vault infrastructure and fewer ports required for internal firewalls.

Replicated Environment

Enterprise-Level Deployments

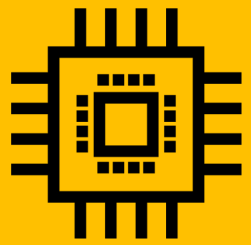
Organizations relying heavily on Vault will commonly have multiple clusters deployed in multiple data centers/cloud-based regions for high-availability and disaster recovery.





Performance Requirements

CPU & MEMORY

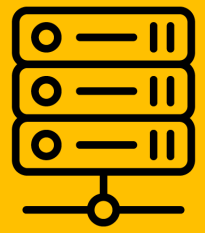


Consolidating both Vault and Consul workloads on the Vault nodes so consider increasing resources

STORAGE

Integrated Storage is disk-bound, so use high-performing disks and sufficient volume sizes

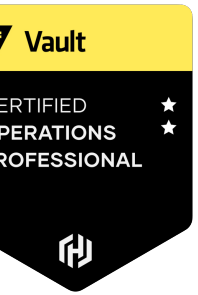
NETWORKING



Similar to Consul, replication requires low latency, high throughput connectivity

Configuring Integrated Storage

Configured in the Vault configuration file



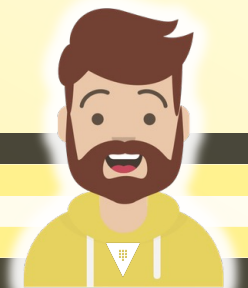
*Configuration truncated

```
...
listener "tcp" {
 address = "0.0.0.0:8200"
 cluster_address = "0.0.0.0:8201"
...
}
storage "raft" {
 path = "/opt/vault/data"
 node_id = "vault-node-a.hcvop.com"
 retry_join {
  auto_join = "provider=aws region=us-east-1 tag_key=vault tag_value=us-east-1"
 }
 performance_multiplier = 1
}
api_addr = "https://vault.hcvop.com:8200"
cluster_addr = " https://vault-node-a.hcvop.com:8201"
```

Configuring Integrated Storage

Common Configurations

- `storage "raft"` = use integrated storage for the node/cluster
- `path` = local directory to store data
- `node_id` = name of the local node – cannot be duplicated within a cluster
- `retry_join` = Vault nodes to communicate with and join a cluster
- `performance_multiplier` = configure the time it takes Vault to detect leader failures and to perform leader elections



Configuring Integrated Storage

Retry Join Block

- `leader_api_addr` = address of a potential leader in the cluster (IP or DNS)

  or

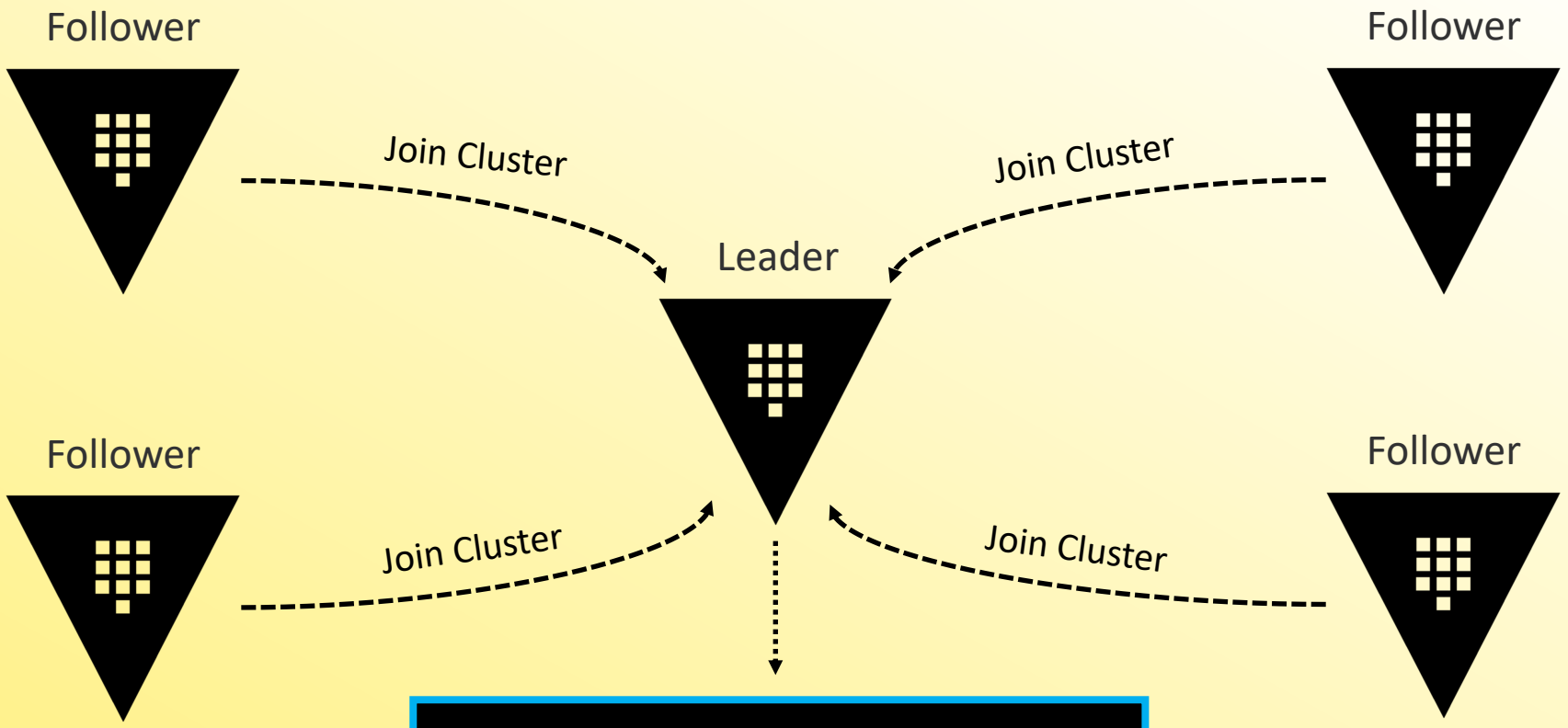
- `auto_join` = use cloud auto-join config using tags assigned to Vault nodes
- `leader_ca_cert_file` = file path of the CA cert of possible leader node
- `leader_client_cert_file` = file path to the client cert to establish client auth with the possible leader node
- `leader_client_key_file` = file path to the client key to establish client auth with the possible leader node

Configuring Integrated Storage

Retry Join Blocks


```
storage "raft" {
  path = "/opt/vault/data"
  node_id = "vault-node-a.hcvop.com"
  retry_join {
    leader_api_addr = https://vault-node-b.hcvop.com:8200
    leader_ca_cert_file = "/opt/vault.d/ca.pem"
    leader_client_cert_file = "/opt/vault.d/cert.pem"
    leader_client_key_file = "/opt/vault.d/pri.key"
  }
  retry_join {
    leader_api_addr = https://vault-node-c.hcvop.com:8200
    leader_ca_cert_file = "/opt/vault.d/ca.pem"
    leader_client_cert_file = "/opt/vault.d/cert.pem"
    leader_client_key_file = "/opt/vault.d/pri.key"
  }
}
```

Cluster Configuration Workflow



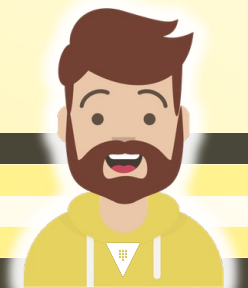

```
$ vault operator init
$ vault operator unseal
```

Managing Integrated Storage

Vault CLI:

```
vault operator raft <subcommand> [options] [arguments]
```

Subcommand	Description
`list-peers`	Returns the raft cluster member information
`join`	Joins a node to the cluster
`remove-peer`	Removes a node from the cluster
`snapshot`	Save or restore a raft snapshot from the cluster



Raft Operations


```
# Join a Node to an existing (or new) Cluster
$ vault operator raft join https://vault-0.hcvop.com:8200


# Remove a Node from a cluster
$vault operator raft leave vault-4
Peer removed successfully!
```

Name of the node to be removed

Raft Operations


```
# List the cluster members
$ vault operator raft list-peers

Node       Address                State      Voter
----       -------                -----      -----
vault-0    vault-0.hcvop:8201     leader     true
vault-1    vault-1.hcvop:8201     follower   true
vault-2    vault-2.hcvop:8201     follower   true
vault-3    vault-3.hcvop:8201     follower   true
vault-4    vault-4.hcvop:8201     follower   true
```

Raft Snapshots

Integrated Storage includes the ability to create a snapshot manually or on a scheduled configuration (Ent only)

Snapshot is a point-in-time backup that includes configuration data and data contained within the KV stores

Create a Raft Snapshot


```
# Save a snapshot
$ vault operator raft snapshot save daily.snap


# Log Entries after snapshot
2022-04-18T16:41:09.545-0400 [INFO]  storage.raft: starting snapshot up to: index=389
2022-04-18T16:41:09.585-0400 [INFO]  storage.raft: snapshot complete up to: index=389
```

Restore Raft Snapshot


```
# Restore a snapshot
$ vault operator raft snapshot restore daily.snap


# Log Entries after snapshot
2022-12-18T16:42:26.298-0400 [INFO]  core: applying snapshot
2022-12-18T16:42:26.298-0400 [INFO]  storage.raft.snapshot: creating new snapshot:
path=/opt/vault/data/raft/snapshots/6-422-1654546298.tmp
2022-12-25T16:42:26.466-0400 [INFO]  storage.raft: copied to local snapshot: bytes=54038
2022-12-25T16:42:26.482-0400 [INFO]  storage.raft.fsm: installing snapshot to FSM
2022-12-25T16:42:26.504-0400 [INFO]  storage.raft.fsm: snapshot installed
2022-12-25T16:42:26.586-0400 [INFO]  storage.raft: restored user snapshot: index=1
2022-12-25T16:42:31.708-0400 [INFO]  core: running post snapshot restore invalidations
```