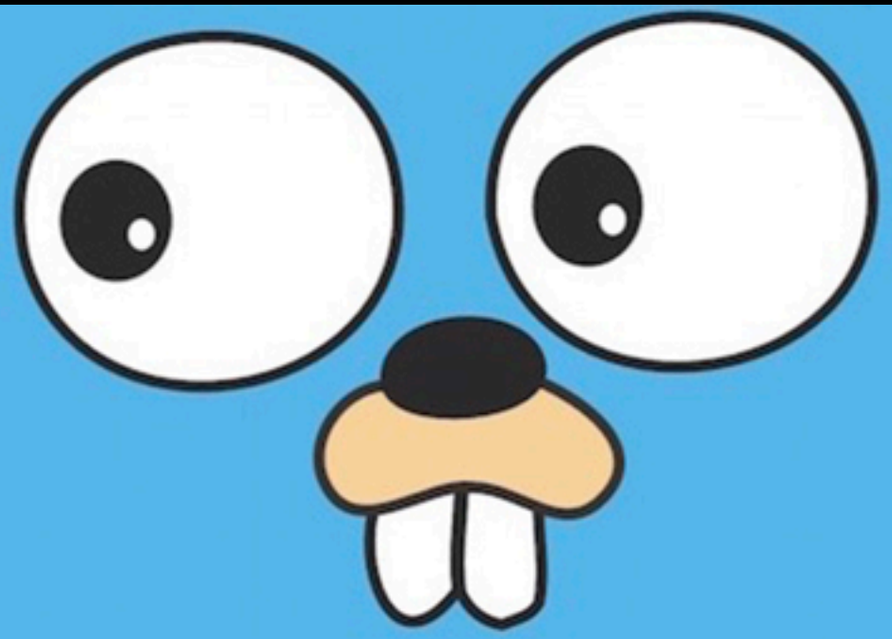
How to make OSS Vault HA

backed by NFS



What is Vault

According to vaultproject.io

What is Vault?

Vault is a tool for securely accessing *secrets*. A secret is anything that you want to tightly control access to, such as API keys, passwords, or certificates. Vault provides a unified interface to any secret, while providing tight access control and recording a detailed audit log.

Problem Statement

Vault doesn't support the NFS File system for High Availability. The OpenSource version of Vault also doesn't form a cluster for making the vault service HA. We are going to see a hacky way of implementing the Vault cluster backed by NFS Servers as the persistent store and making it Highly Available.

vaultproject

Word of advice

- Definitely not recommended for Production Environment.

Who am I

Karthikeyan Govindaraj
OpenSource Enthusiast | Writer | CNCF Speaker

In community, Active contributor, Kubernetes;
Member of SIG ContribEx & WG Naming

Cloud Native Developer @ BlackRock

Know more about me!!

Technologies and tools we will discuss in this presentation are.,

- >_ Vault
- >_ Consul
- >_ Kubernetes
- >_ GoLang
- >_Helm
- >_ Vault initializer
- >_ VLB

Consul Intro

>_ Vault without persistent storage is not recommended in production

>_ NFS Doesn't support leader election

ref: https://github.com/hashicorp/vault/issues/4236

>_ Consul can be deployed on top of NFS

Consul Intro

>_ A DNS based service discovery solution

>_ Integrated health-checking, securing network traffics

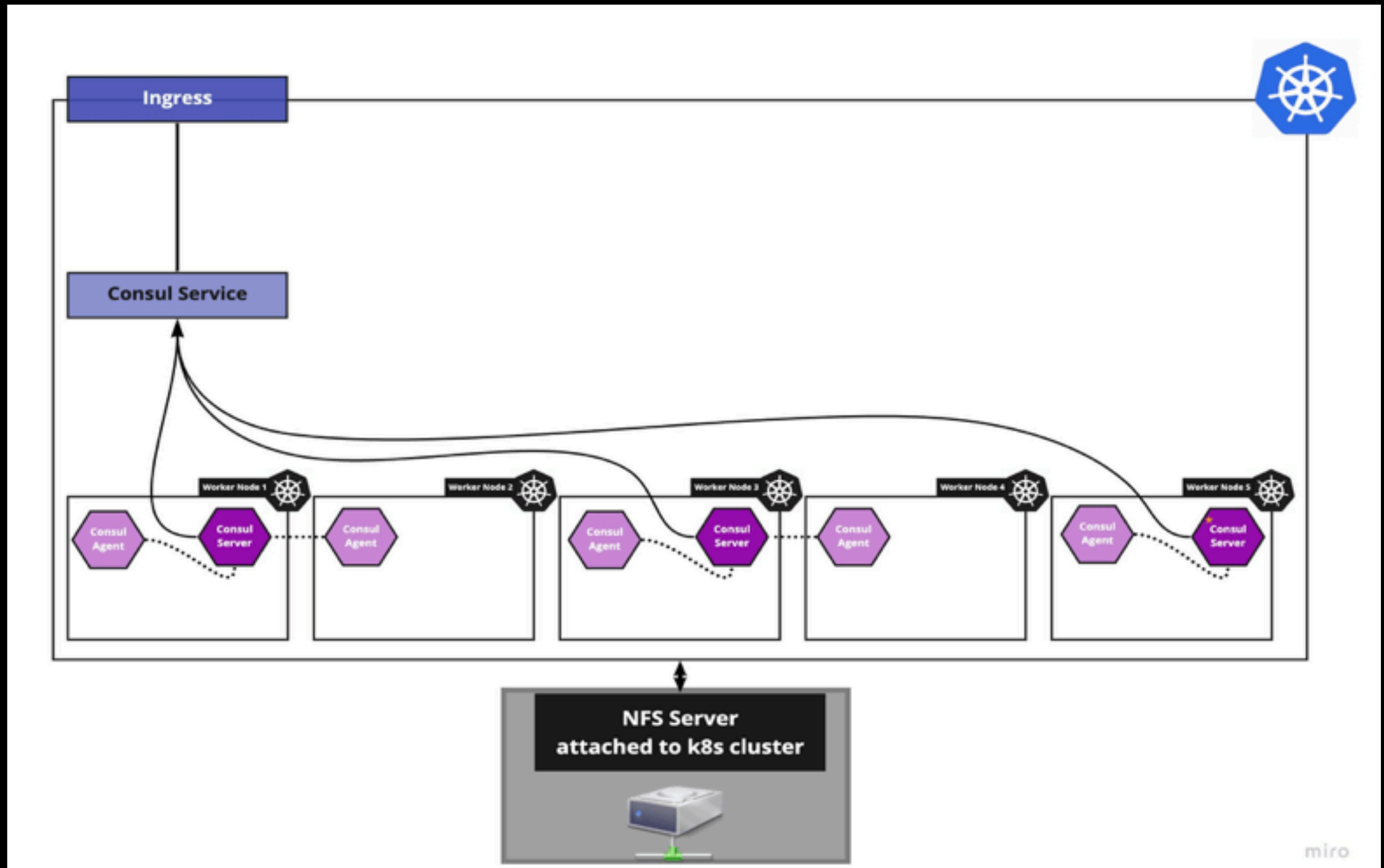
>_ A distributed key-value storage

>_ Manage leader election/ backend store for Vault naturally

Consul Docs

Deploy Consul to K8s

>_ Deploy using official consul helm chart



Deploy Vault to K8s

>_ Deploy using official Vault helm chart

>_ Use the community version of Hashicorp Vault

>_ Make three replicas at least

Hashicorp Helm Charts

...contnd.,

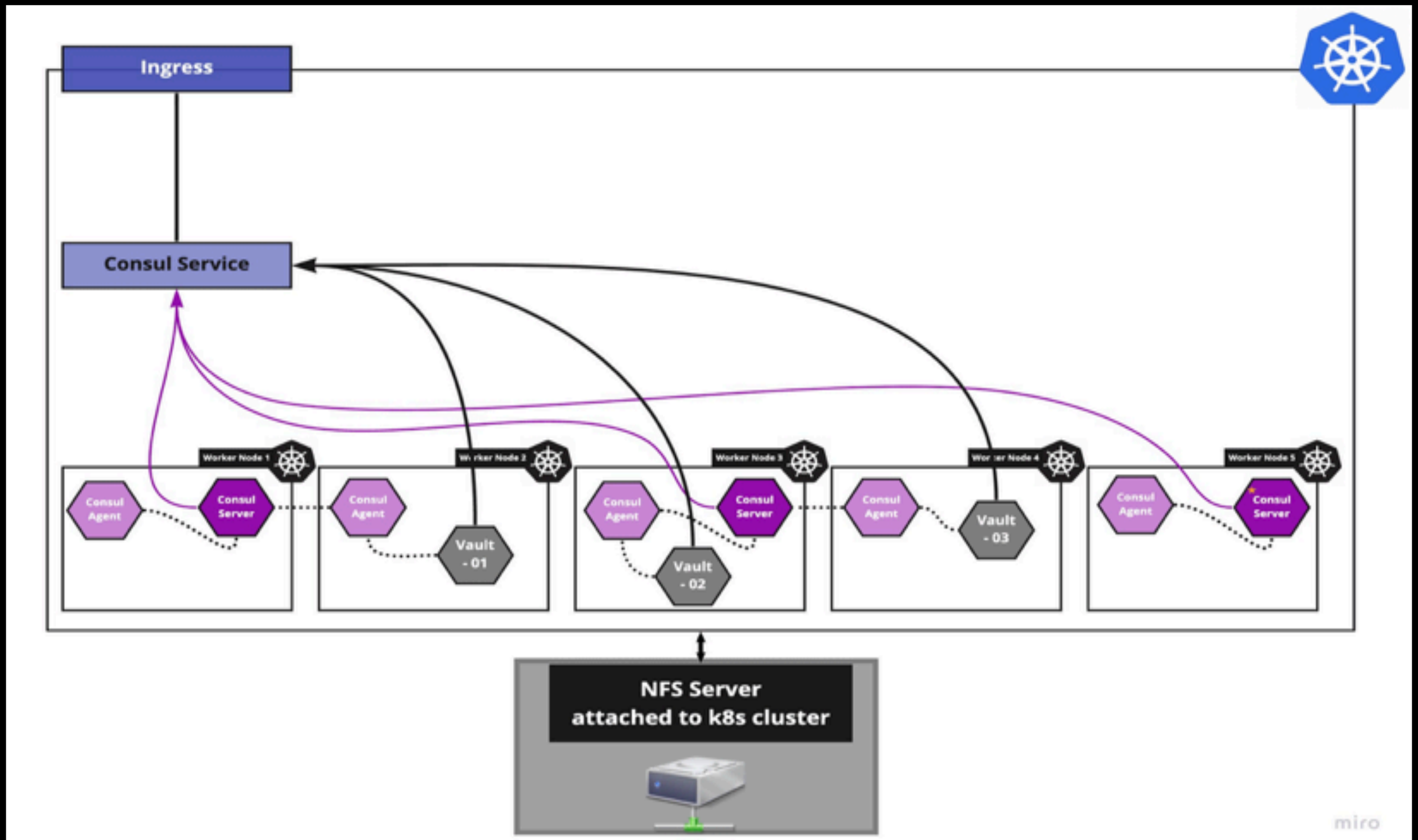
>_ Configure to use Consul as storage

>_ Consul takes care of Leader election

```
storage "consul" {
   address = "consul.default.svc:8500"
   path    = "vault"
}
```

HCL

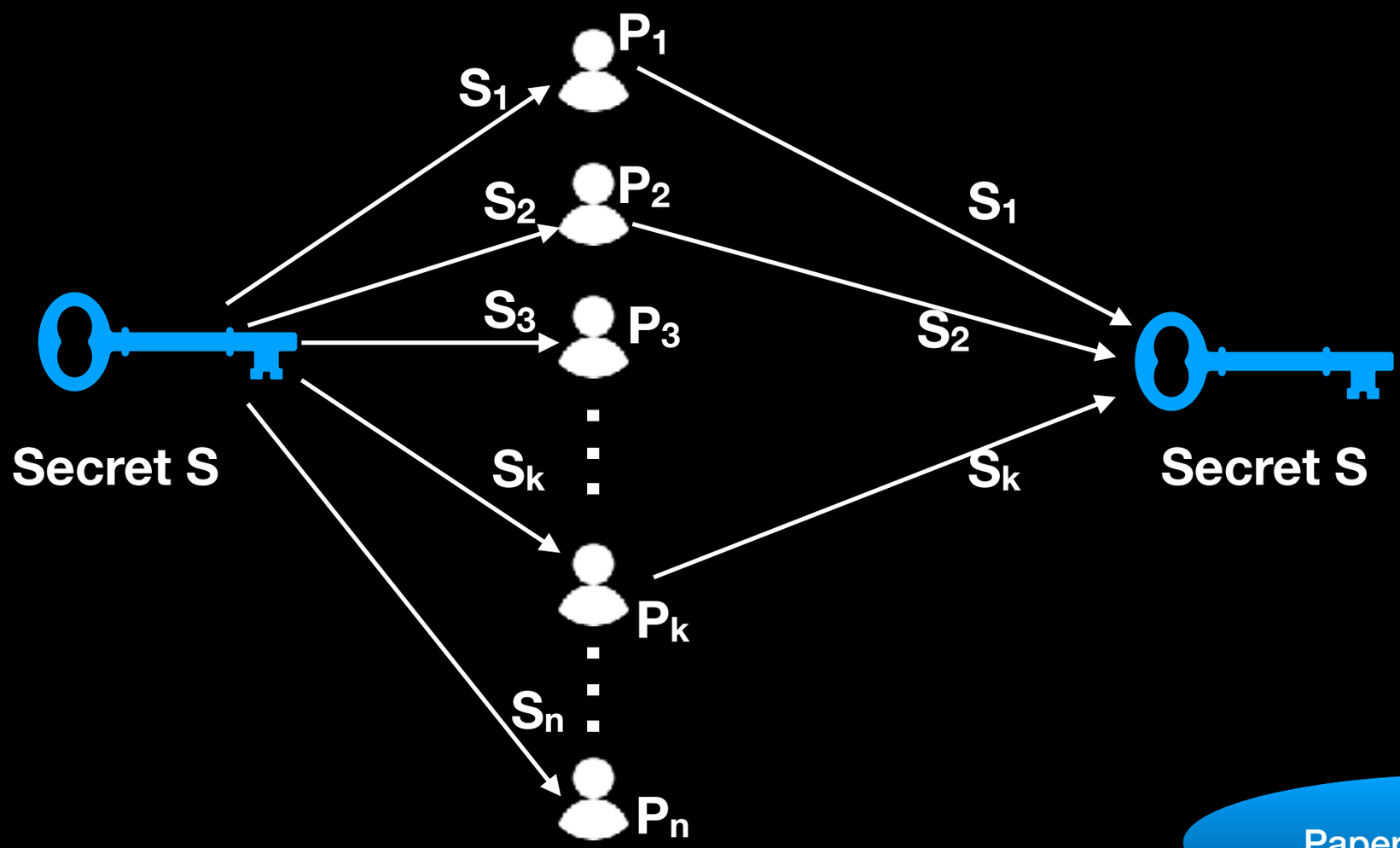
...contnd.,


Ingress
Consul Service
Worker Node 1
Worker Node 2
Worker Node 3
Worker Node 4
Worker Node 5
Consul Agent
Consul Server
Vault - 01
Vault - 02
Vault - 03
NFS Server
attached to k8s cluster
miro

Initialize Vault

>_ Vault is very secure and doesn't allow leakage

>_ uses *shamir* algorithm for key distribution



Paper by Adi Shamir

...contnd.,

>_ automatically seals if started/restarted at any time in its lifecycle

>_ simply store somewhere

https://github.com/gkarthiks/vault-initializer

ref: https://github.com/kelseyhightower/vault-init

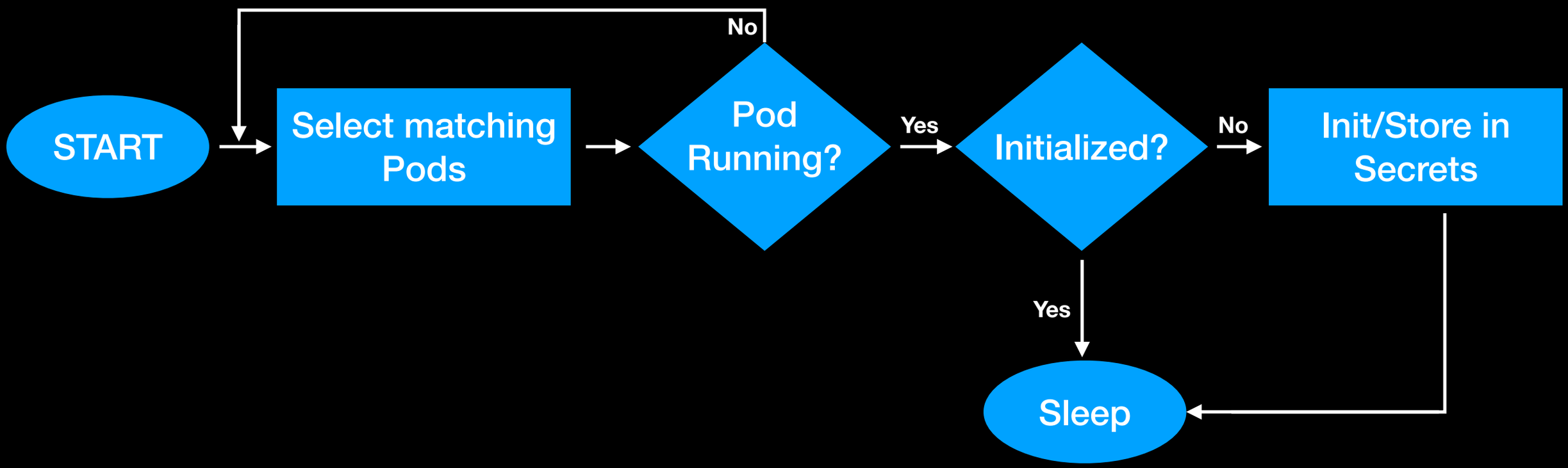
GH Repo: vault-init

What does it do?

>_ Simply checks for the available vault pods

>_ uses the HTTP API to check the status

>_ Initializes if not initialized and stores the key in secrets



…contnd.,

>_ doesn’t need to be in the secrets, you can store wherever you want

>_ not via bash script, as its complex and needs access for keys’ location

>_ always good to have as an independent deployment alongside vault pods

Did we achieve the High Availability yet??? ***Nope!!***

Kubernetes and its Services

>_ Probes
- readiness
- liveness
- startup

Probe describes a health check to be performed against a container to determine whether it is alive or ready to receive traffic.

>_ vault's status is checked using the "vault status" command

>_ soon after the vault container is started, status will return *200OK*

>_ still unsealed and may be even not initialized

>_ according to k8s probes, container is ready to accept traffics

>_ results in false status and user gets no response

>_ not a problem of k8s, but not really a HA cluster of Vault yet

>_ solve via VLB

Distribute load via VLB

https://github.com/gkarthiks/vault-balancer

>_ Vault Load Balance, a simplest load-balancer in k8s

>_ frequently checks for the matched vault pods

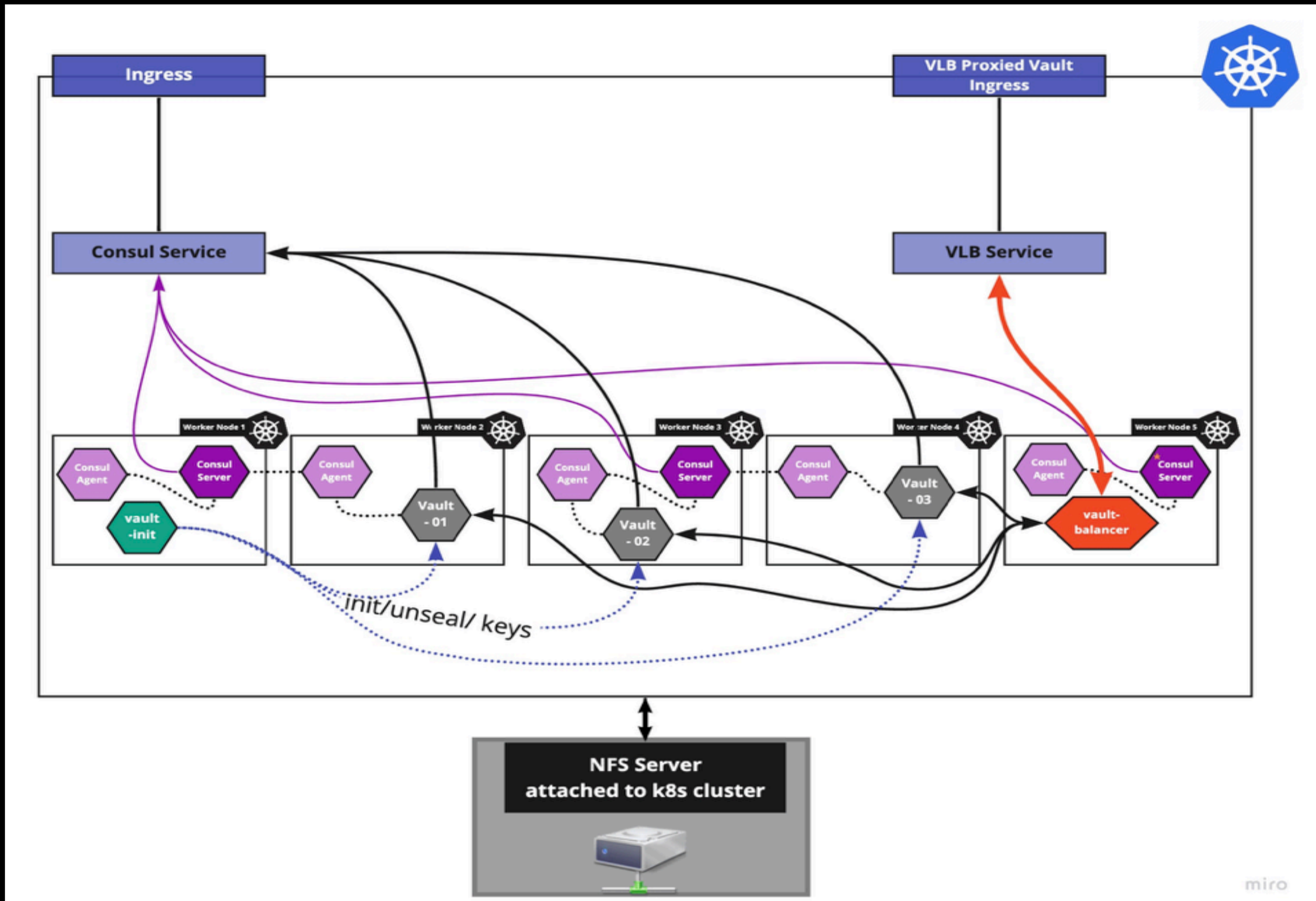
>_ executes the HTTP Health check api

>_ stores the healthy pod’s IP address for round robin

>_ Deploy it alongside the vault pods

>_ route traffic via VLB instead of k8s service

Finally cluster looks like...



is it HA yet?

>_ May be yes from where it was ;-)

Medium article

Know me!!

Questions?