HashiCorp Nomad at Allianz

Roman Pogribnyi,
Allianz Technology

HashiCorp

ABA at Allianz

Goal: Create Business Value and improve processes using AI and new data technologies

Share knowledge between OEs

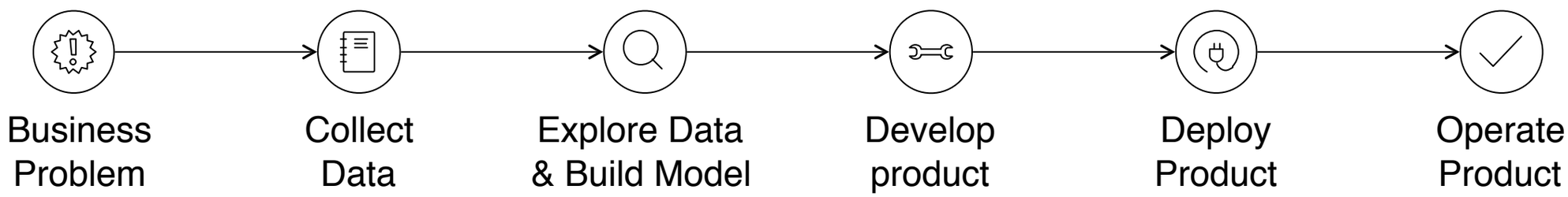
Facilitate processes

HashiCorp

DSP Platform at Allianz

- Provides infrastructure ABA
- Basically: **developing, deploying, and operating data driven products end to end**.

Lifecycle of a data-driven product



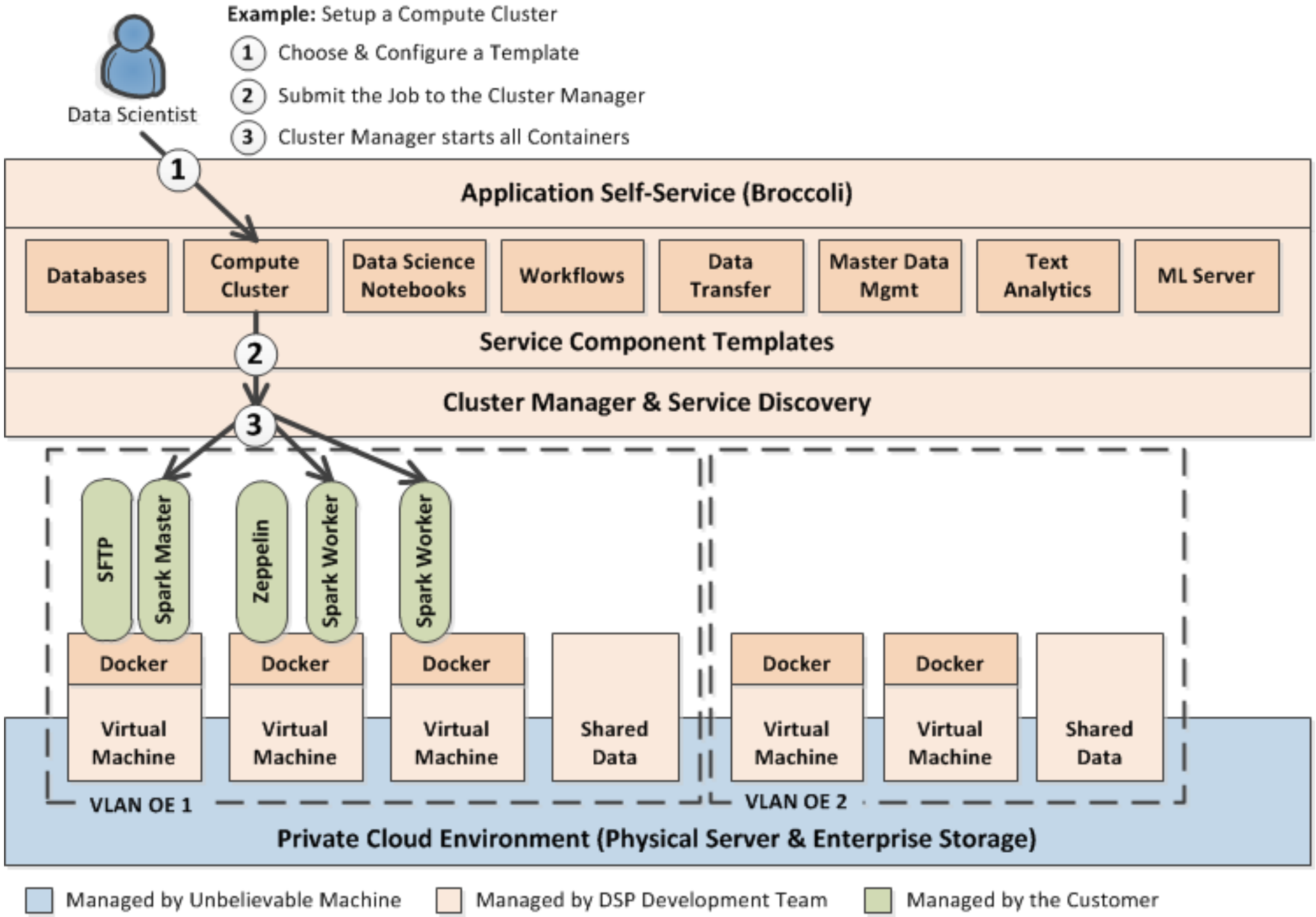
HashiCorp

Use Cases of DSP

- Explore data from OEs and 3rd parties
- Quickly prototype a model
- Create an API based on this model

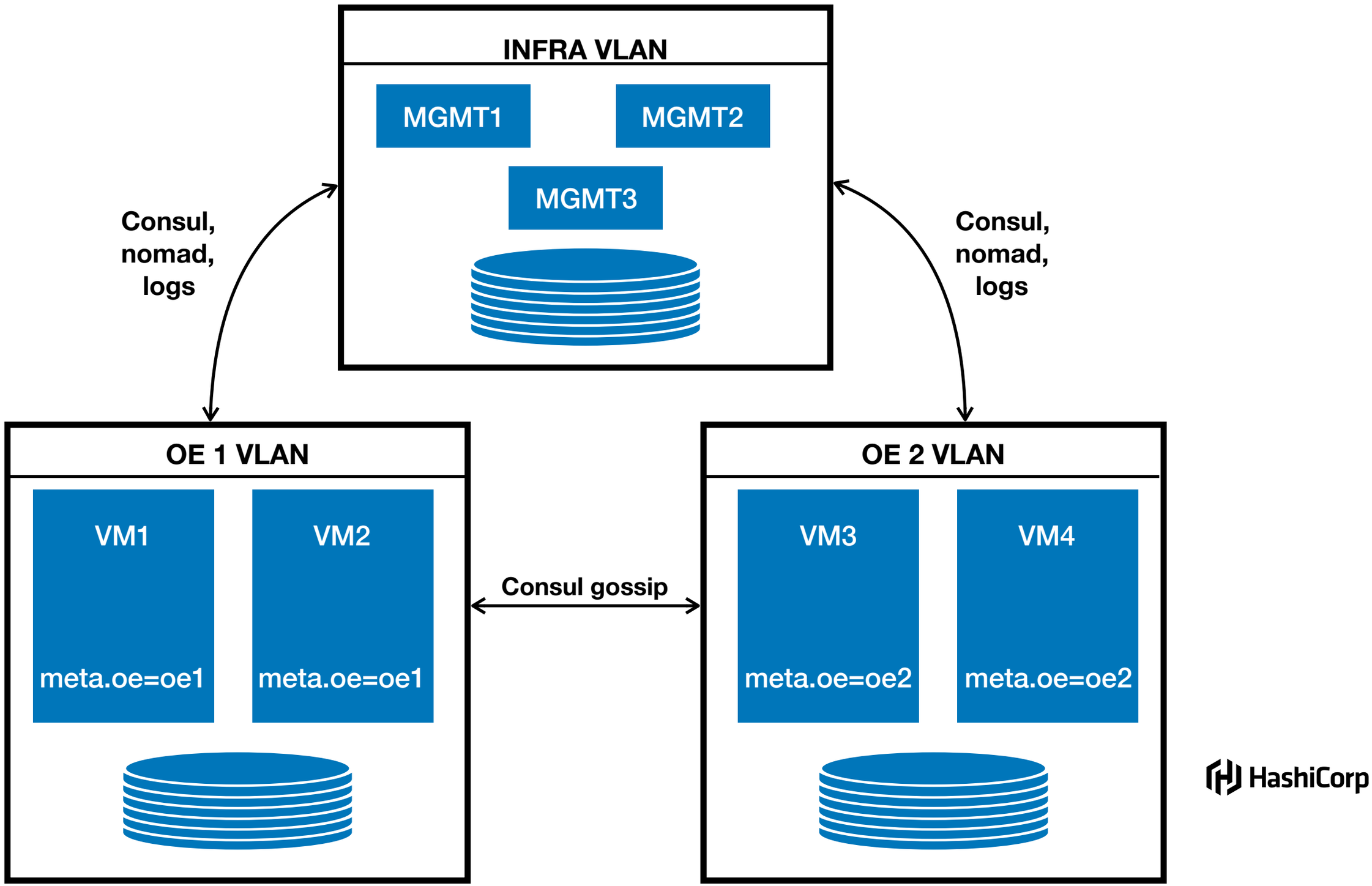
HashiCorp

Current Setup



HashiCorp

Old Network Structure



HashiCorp

Usage of Consul & Vault

Consul:

- Service Discovery
- Health checks of services
- Health checks of VMs

Vault:

- Intermediate CA
- Secrets for CI/CD

HashiCorp

Self-service for Nomad: Cluster Broccoli

- Create / configure / monitor Nomad jobs
- https://github.com/Data-Science-Platform/cluster-broccoli

HashiCorp

Broccoli: list jobs

Cluster Broccoli ▾ Instances Resources Template Filter nooe admin

anaconda-manager d4514dd7 2

Deploy and manage shared Python environments across the cluster.

New Start Stop Delete

	#			
nooe-anaconda2	-	1d0f8bbc	stopped	
nooe-anaconda3	nooe-anaconda3-ssh	acb83c71	running	

HashiCorp

Broccoli: inspect jobs

nooe-anaconda3 — nooe-anaconda3-ssh — acb83c71 — running

Template

Unchanged: anaconda-manager (acb83c7107a4fc07786c85b5813bbbc5)

Parameters

Anaconda Installation Path(Raw)	/misc/anaconda3	OE(Raw)	nooe
Anaconda Version(Raw)	Anaconda3-4.4.0	CPU (MHz)(Raw)	100
Deployment Environment(Raw)	default	Memory (MB)(Raw)	512
Authorized Group(Raw)	AZDE1_USERS		

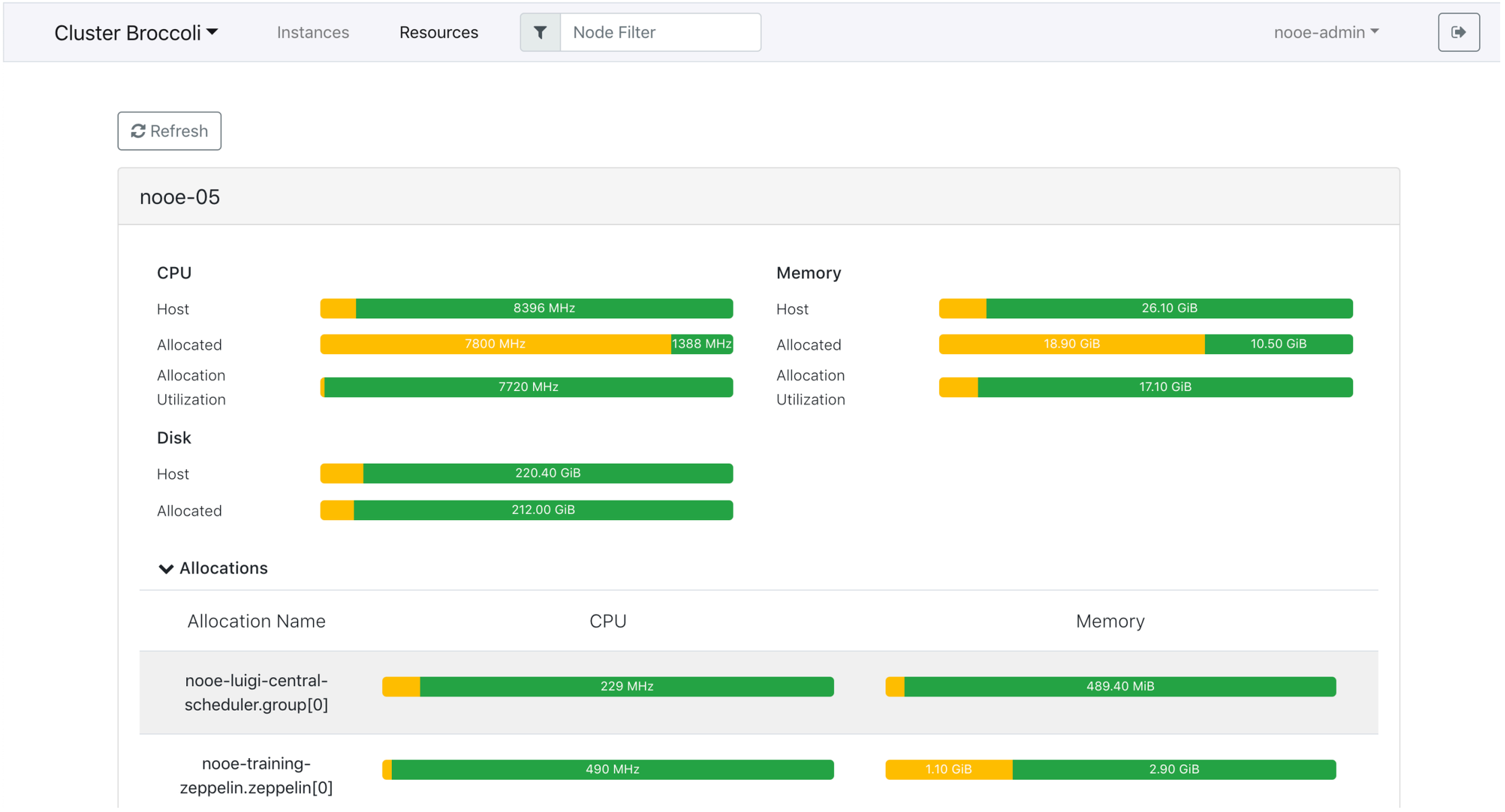
Apply Discard

Allocated Tasks

Allocation	State	Task	CPU	Memory	Task Logs
674dbfc3	running	nooe-anaconda3	0%	0%	stdout stderr

HashiCorp

Broccoli: host resources



HashiCorp

Broccoli: job definition

Broccoli job definition

```
{
  "Job": {
    "Region": "global",
    "ID": "{{id}}",
. . .

“TaskGroups”:[
  {
. . .

    “Tasks”:[{
. . .
      "Resources": {
        "CPU": {{resources_cpu}},
        "MemoryMB": {{resources_memory_mb}},
. . .
```

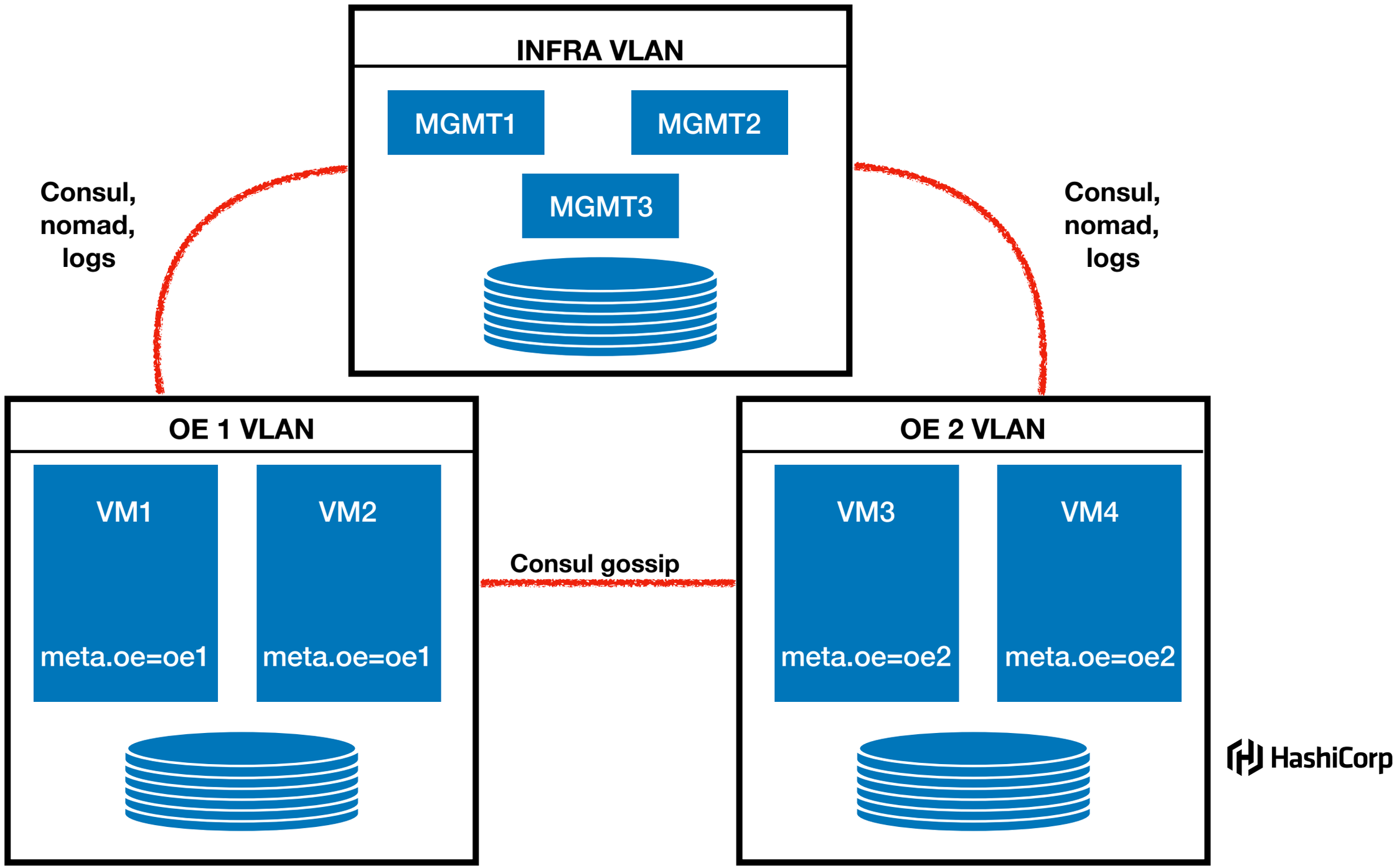
HashiCorp

Why we needed a change

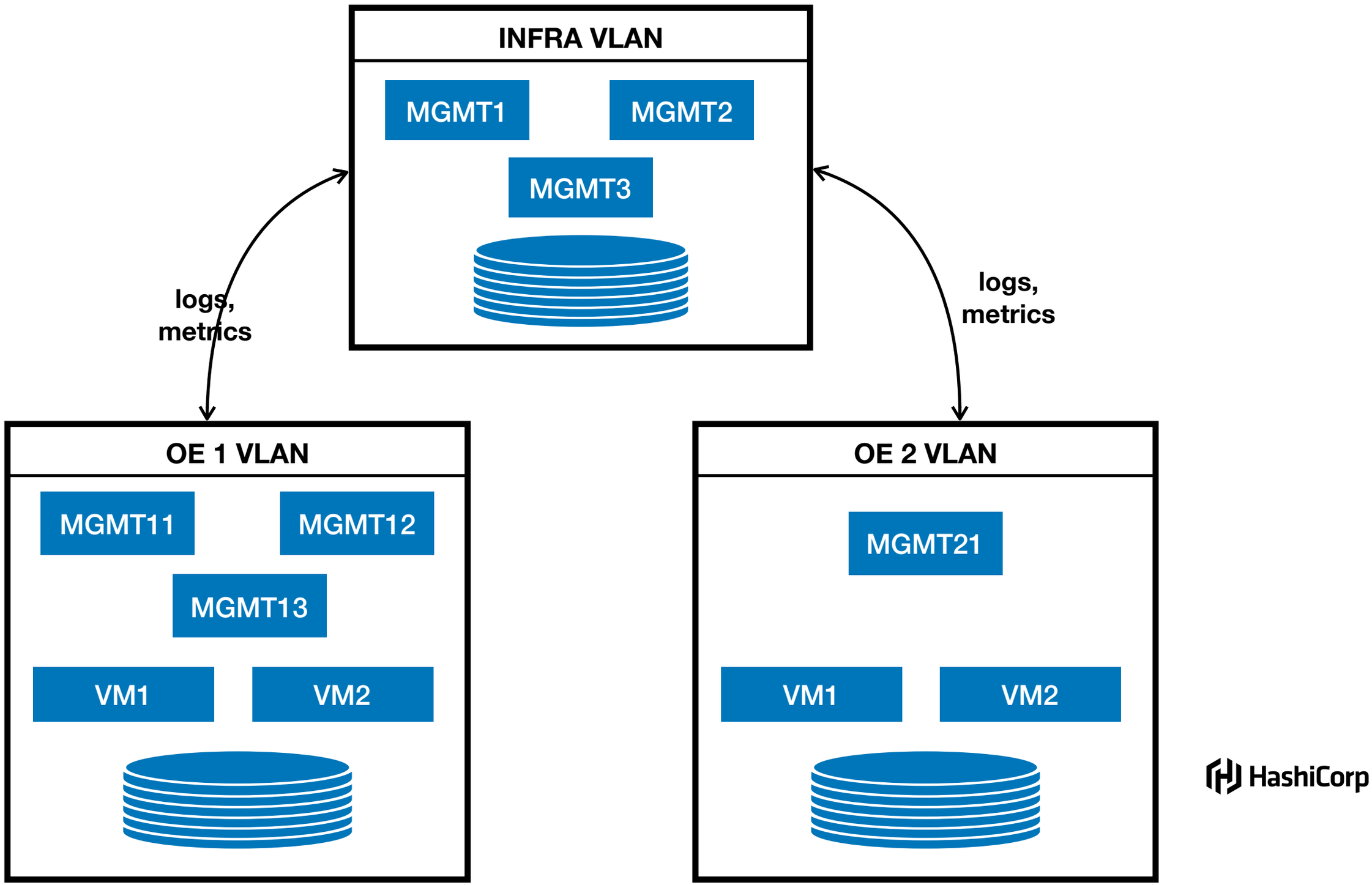
- No ACLs in place(redundant anyways)
- *Full* self-service for customer
- Allow VCs in client VLANs

HashiCorp

Option 1: Introduce ACLs



Option 2: Dedicated Nomad



HashiCorp

Option 3: Centralised Nomad(EE)

- Define ACLs on namespaces
- Resource quotas(if needed)
- Sentinel policies for allocation checks

HashiCorp

Nomad EE: Namespace isolation

```
{
    "namespace": {
        "default": {
            "policy": "read"
        },
        "azde": {
            "policy": "write"
        }
    },
}
```

Nomad EE: Resource quotas

- Each Namespace uses 100% of resources
- Split only within teams

Nomad EE: Resource quotas

```
$ cat azde-project1-quota.hcl
name = “azde-project1-quota“
description = “Project 1 of AZDE OE"

# Create a limit for the global region. Additional limits may
# be specified in-order to limit other regions.
limit {
    region = "global"
    region_limit {
        cpu = 40000
        memory = 100000
    }
}

$ nomad namespace apply -quota azde-project1-quota azde-project1-ns
```

HashiCorp

Nomad EE: Sentinel policies

```
$ cat allocation.sentinel
get_constraint_for_oe = func(oe){
 return {
    "LTarget": "${meta.oe_tag}",
    "RTarget": oe,
    "Operand": “=",
  }
}

check_namespace_alloc = func() {
  ns = job.namespace
  return job.constraints contains get_constraint_for_oe(ns)
}

main = rule { check_namespace_alloc() }
```

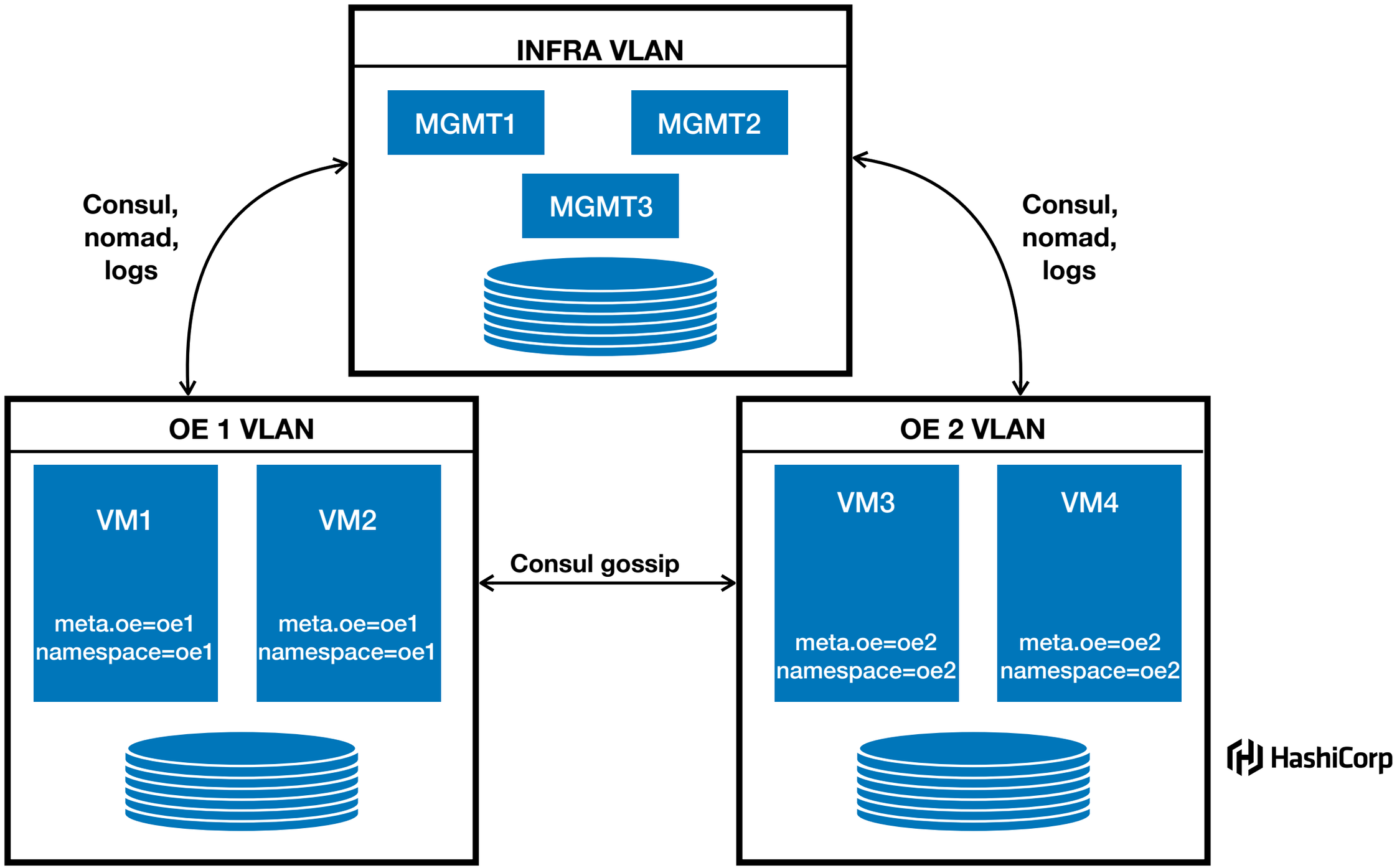
HashiCorp

Final Design

- Single namespace per OE
- Sentinel checks for customer-created jobs
- Introduce ACLs to Broccoli

HashiCorp

Option 3: Centralised Nomad(EE)



Thank you

HashiCorp