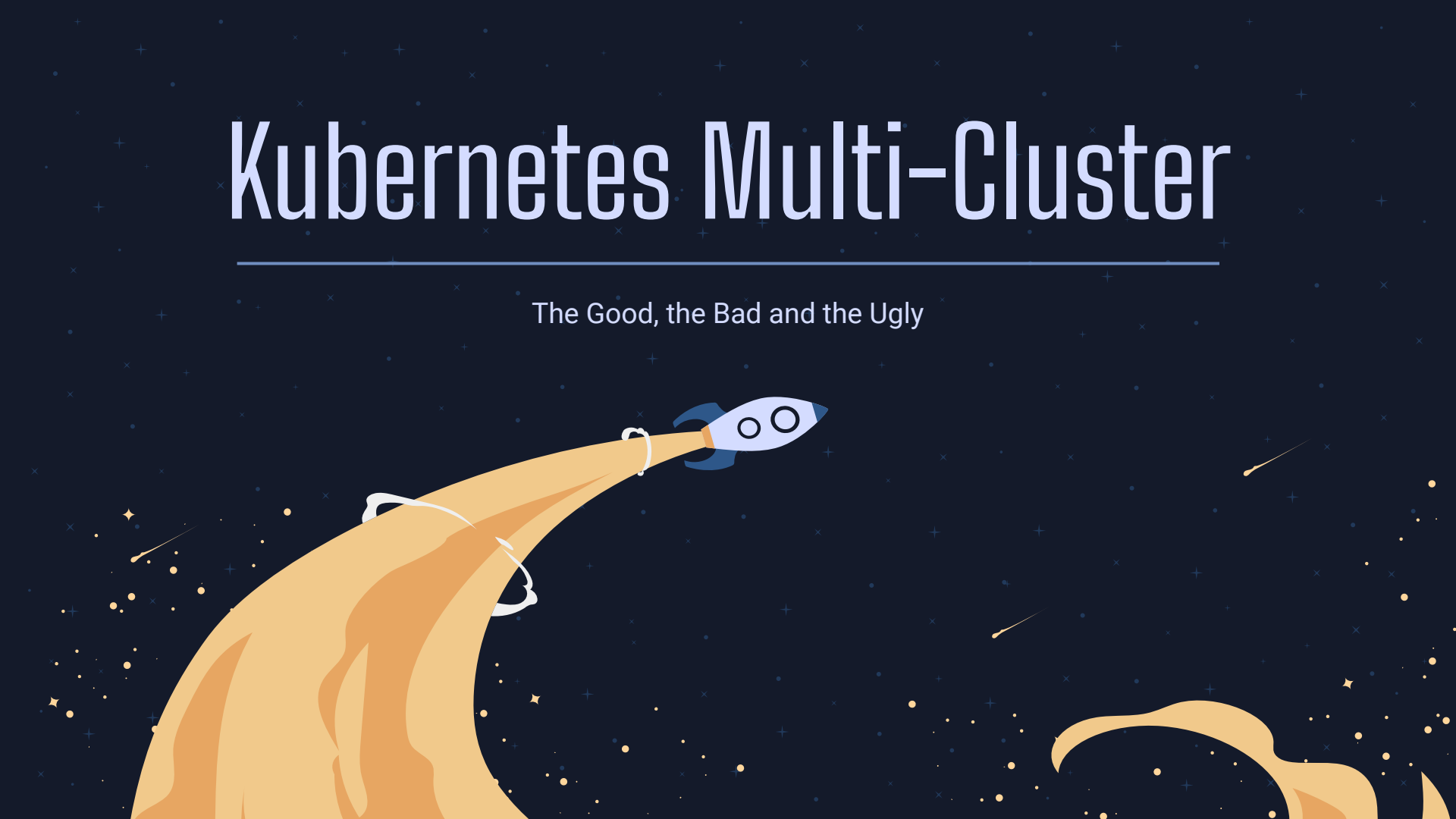
Kubernetes Multi-Cluster

The Good, the Bad and the Ugly



Hello!

I am smalltown

MaiCoin Group Lead SRE

Taipei HashiCorp UG Organizer

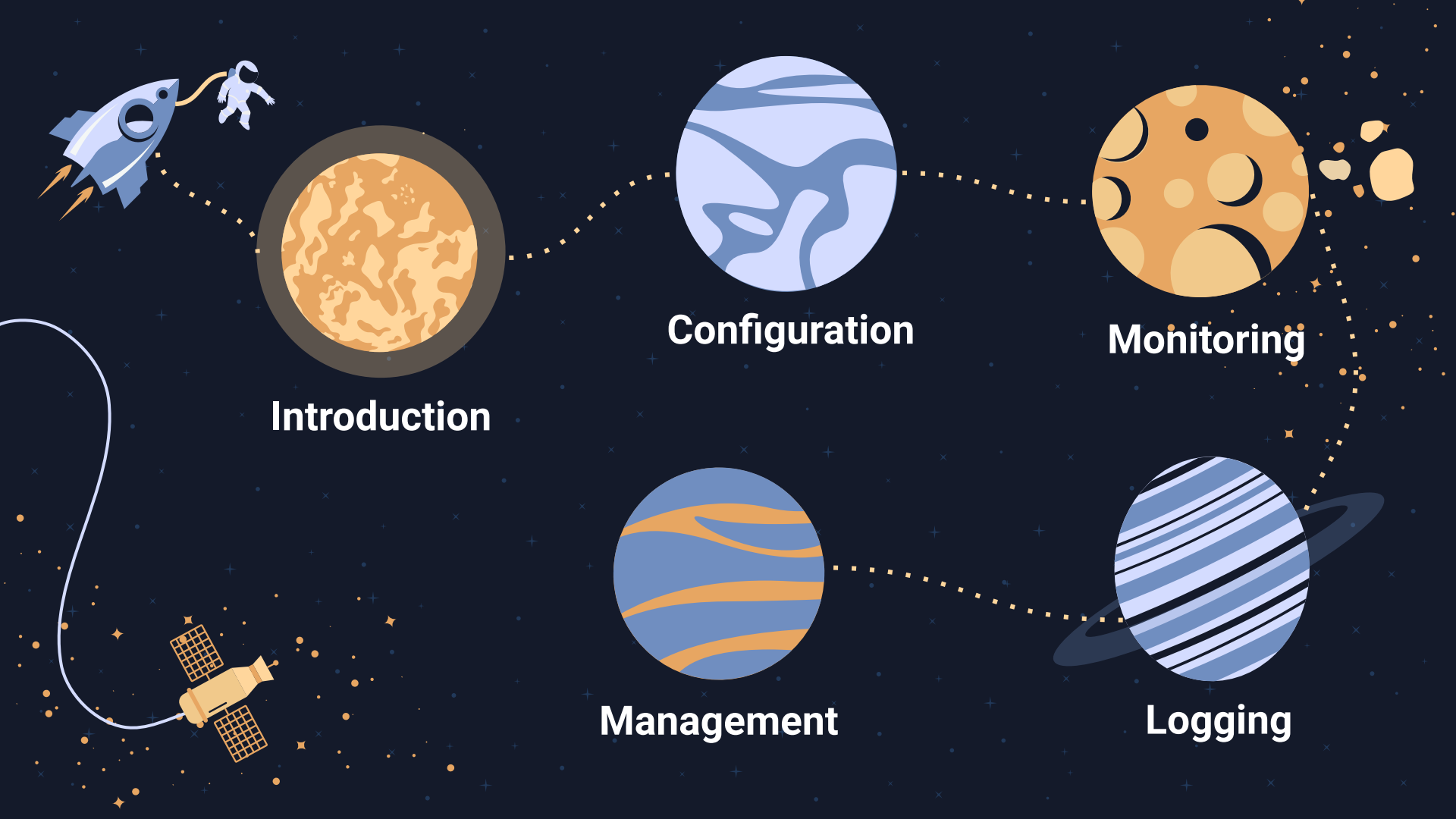
AWS UG Taiwan Staff

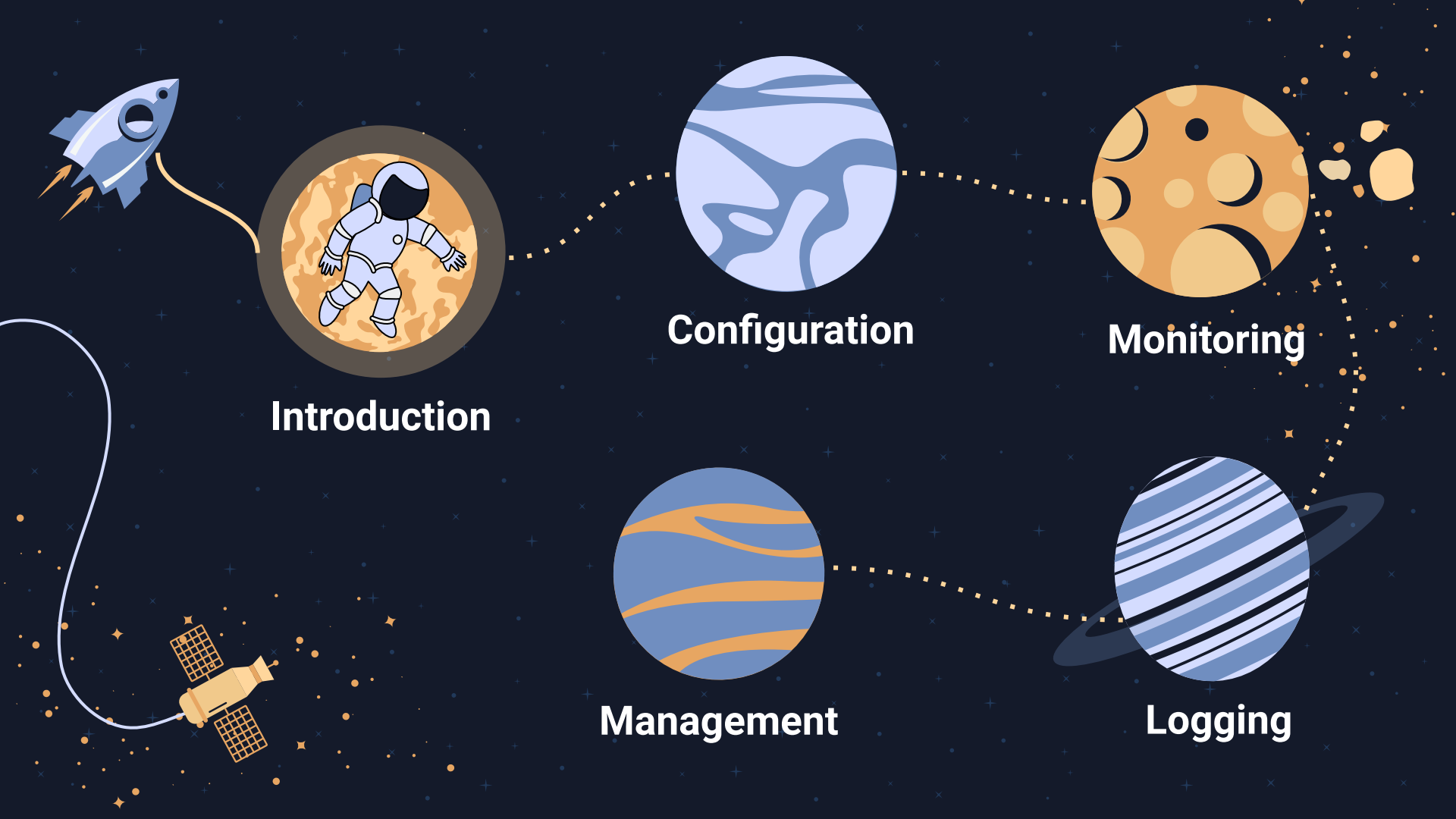
HashiCorp

MaiCoin

aws

How Many K8s Clusters Do you Need to Take Care?


Introduction
Configuration
Monitoring
Management
Logging


Introduction
Configuration
Monitoring
Management
Logging

What We Care?

Security

Availability

What We Want?

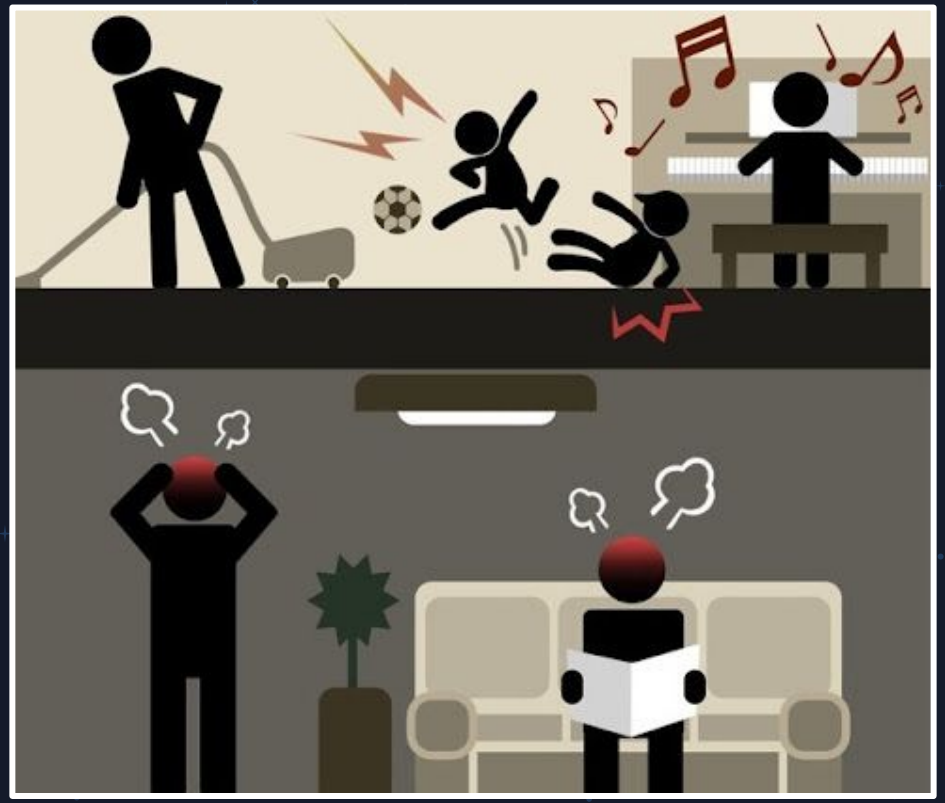
我只想維運一個 K8s Cluster 就好

How About Multi-Tenancy ?

- A Software Architecture
- A Single Instance of Software Runs on a Server (**K8s Cluster**) and Serves Multiple Tenants (**Namespaces**)
- A Tenant is a Group of Users who Share a Common Access with Specific Privileges to the Software Instance

Ref

Soft V.S. Hard Multi-Tenancy



Kubernetes Only Provides Weak Soft Multi-Tenancy

- Use **Namespace** to Implement Logical Isolation
- RBAC
- Limit Ranges
- Resource Quotas
- Network Policies
- Pod Security Policies (Deprecated V1.25)

Enhanced Kubernetes Weak Soft Multi-Tenancy

- User Management
  - dex
- Resource Sharing & Isolation
  - Argo CD: Use casbin Implement RBAC Management, Collocation with Project CRD
  - loft.sh: kiosk - Multi-Tenancy Extension For Kubernetes
  - Flux 2: Leverage CRD and Folder Structure
- Policy as Code
  - Kyverno or OPA Gatekeeper

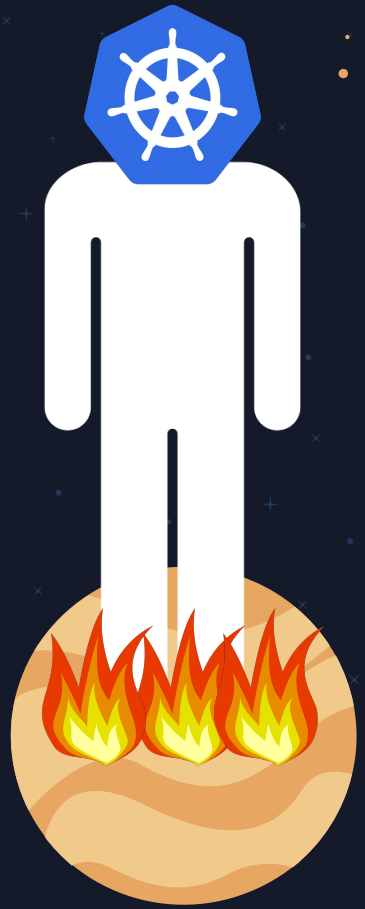
Hard Multi-Tenancy Kubernetes on the Way

- Kubernetes Working Group for Multi-Tenancy (Ref)
  - Benchmarks
  - Hierararchical namespaces (aka HNC)
  - Tenant Operator
  - Virtual clusters
- Multi-Tenancy SIG Virtual Cluster
- loft vClusters

No Hard Multi-Tenancy Now !

What Single-Tenancy Achieve ?

True Isolation



Single-Tenancy Shortcoming

- Setup, Configuration, Upgrade, Backup, Disaster Recovery … for **Multiple Clusters**
- Manage Authentication and Authorization for User & Application Across **Multiple Clusters**
- Collect and Analysis Logging & Metrics Management Across **Multiple Clusters**
- Cannot Share Resource Across **Multiple Clusters**

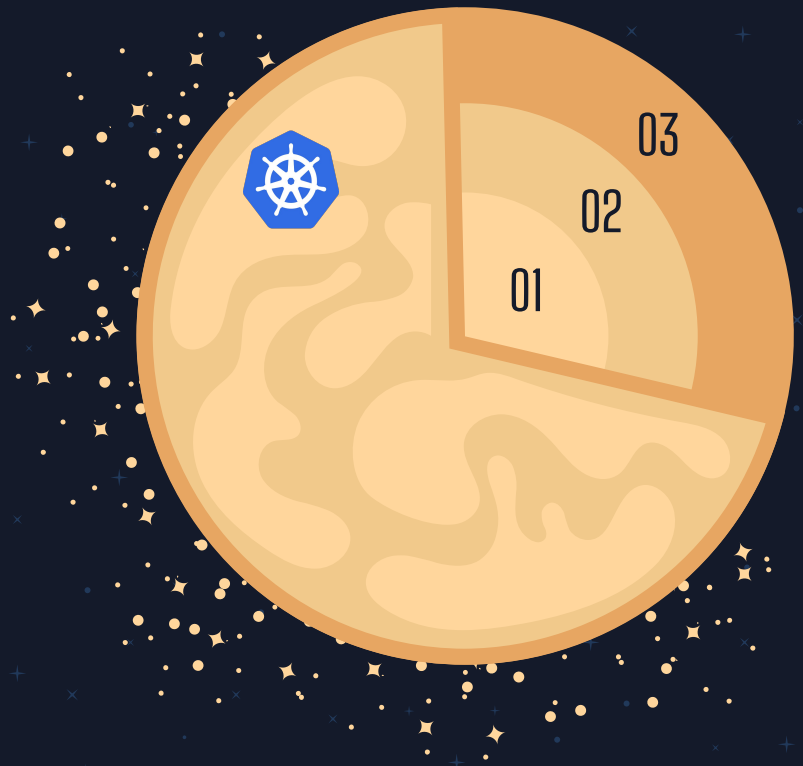
Enhanced Weak Soft Multi-Tenancy + Multi-Cluster

Planetary System

Multi-Tenancy Cluster

Center Cluster

Center Cluster Functionality



01

Configuration Management

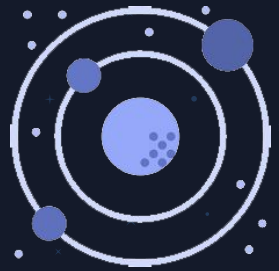
02

Monitoring and Alarm

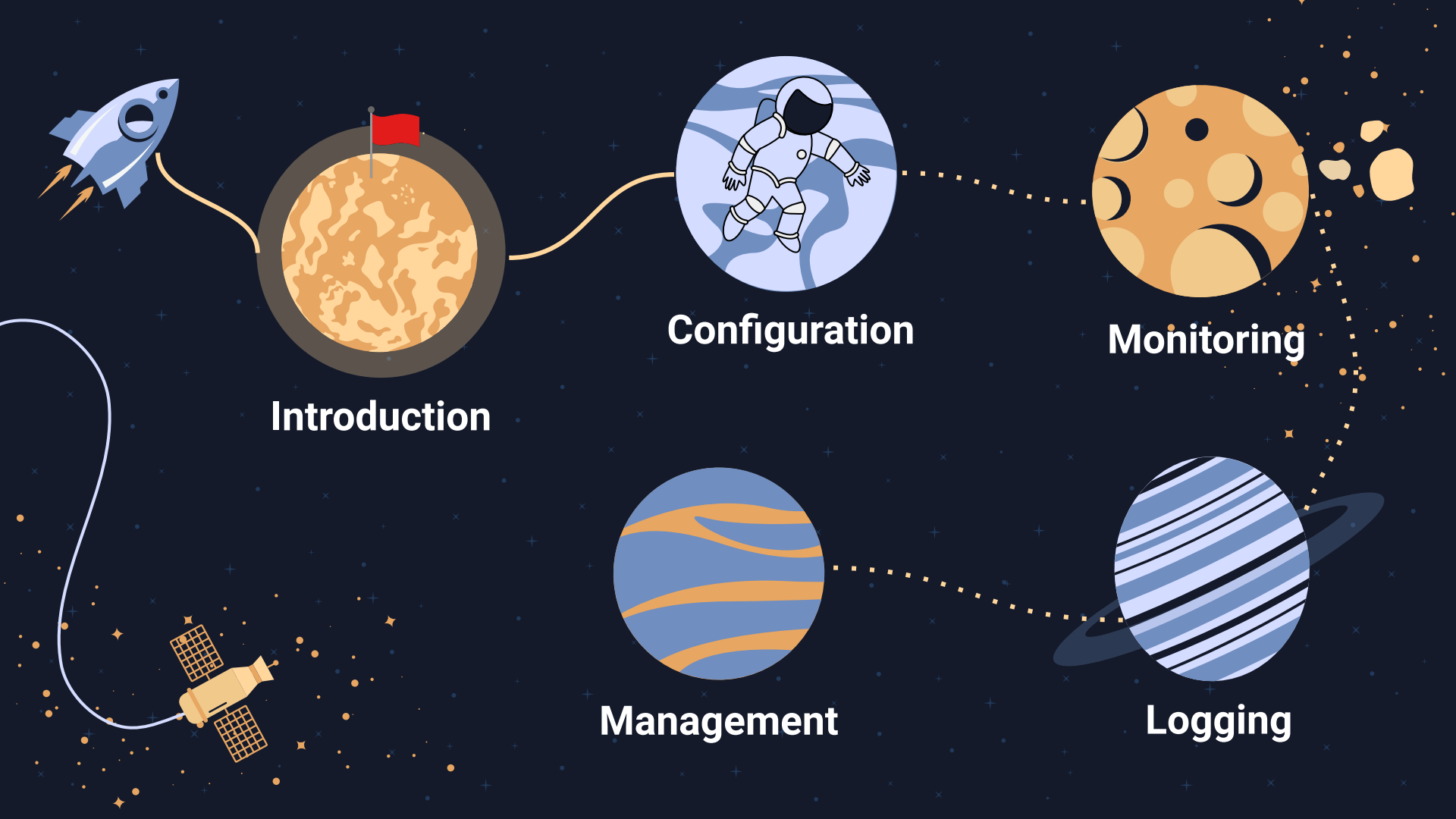
03

Logging and Analysis

Separation Decision Example



Non Production Environment	Production Environment
Whether Service Critical Or Not?	
Whether System Sensitive Or Not?	


Introduction
Configuration
Monitoring
Management
Logging

Why Kubernetes Need Configuration Management ?

Hey, John Wick, If You Want to Save Trinity, Helping Me to Patch Log4j Security Vulnerability

I’m Neo! Not John Wick! And Please Don’t Disclosed More Log4j Security Vulnerability T_T

Why Kubernetes Need Configuration Management ?

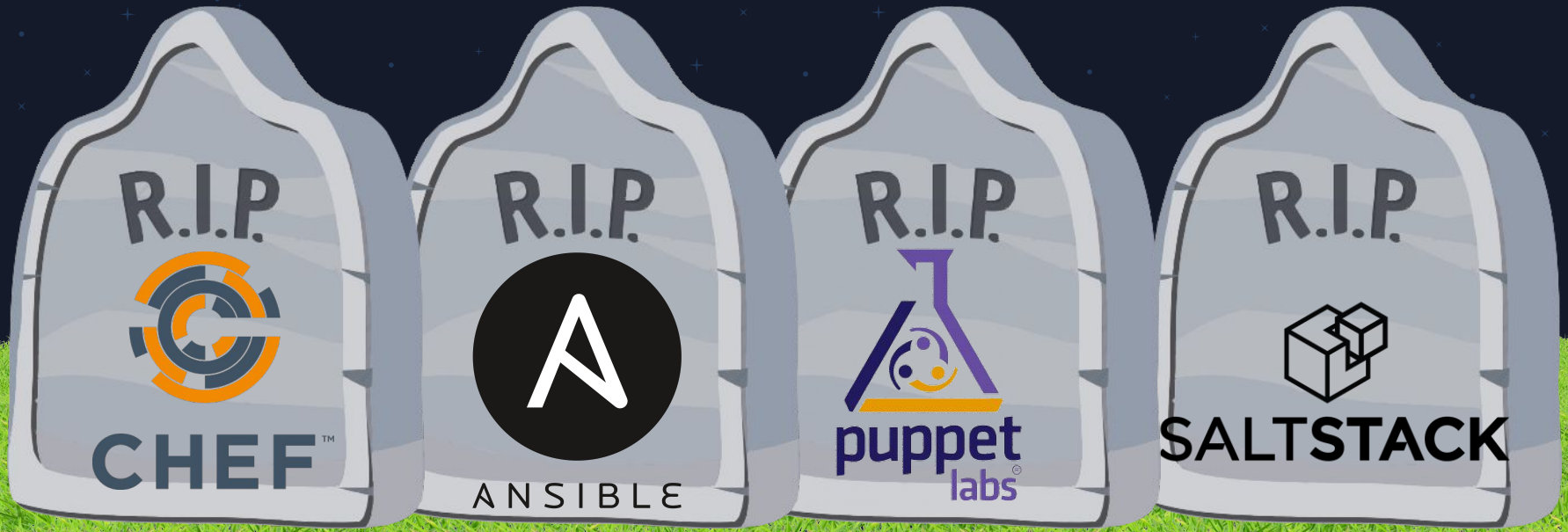
想救崔妮蒂的話，就幫宏爸刪除所有人腦裡關於宏宏不優質的記憶～

我是救世主，不是奇異博士啊 ！蕾神請停止更新不然刪不完 T_T

Configuration Management Benefits

- No Out of Date Document Anymore
- Increased Efficiency
- Reliability
- Cost Reduction and Risks
- ...

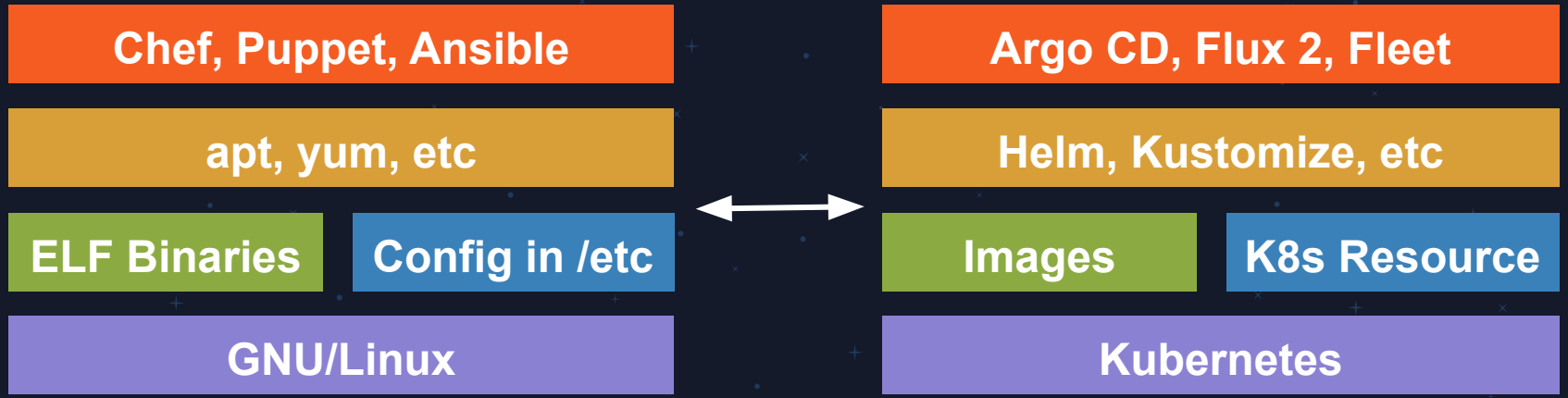
R.I.P. Configuration Management



~~Welcome Configuration Management~~ ⬅️ 這樣不潮

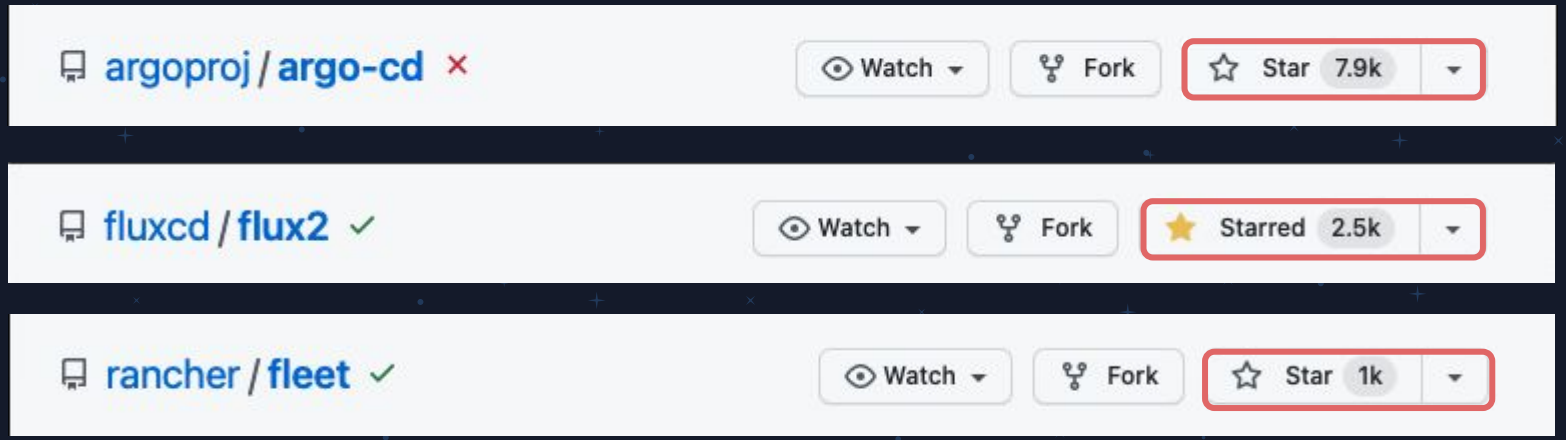
Welcome GitOps ⬅️ 這樣比較潮比較好行銷

Tradition Server VS Kubernetes



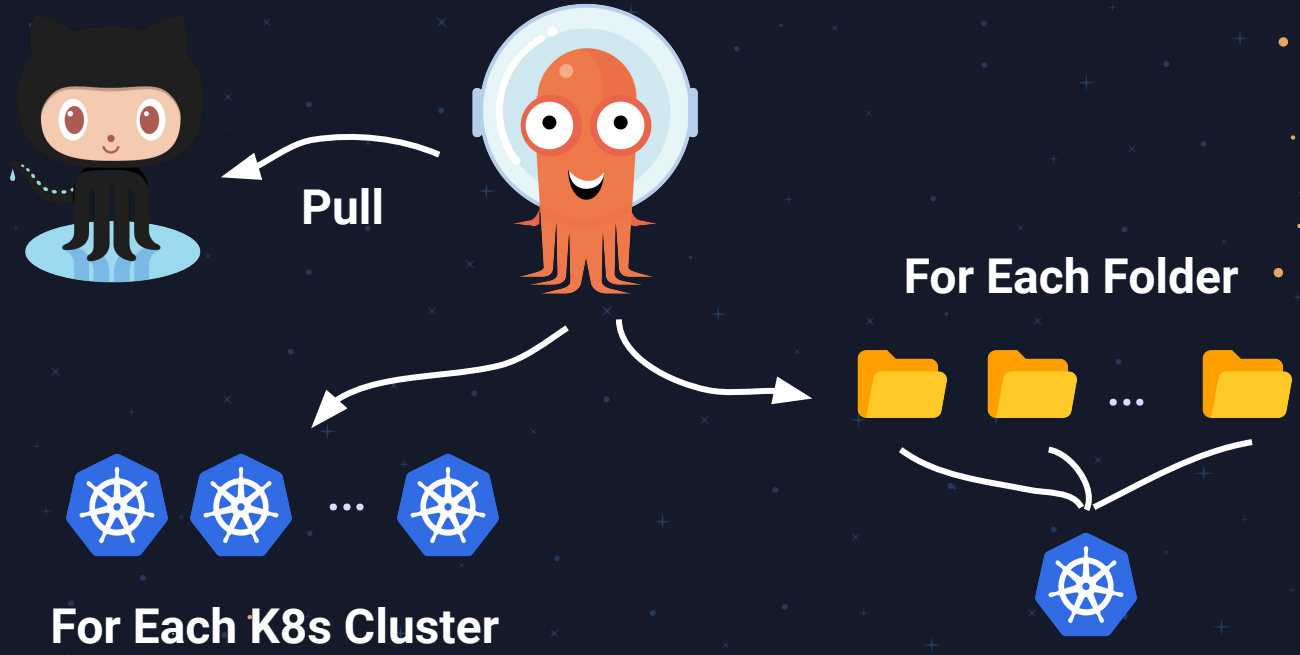
GitOps Solution Selection

- Multi-Cluster & Multi-Tenancy
- Pure CRD to Define Configuration
- Active Community



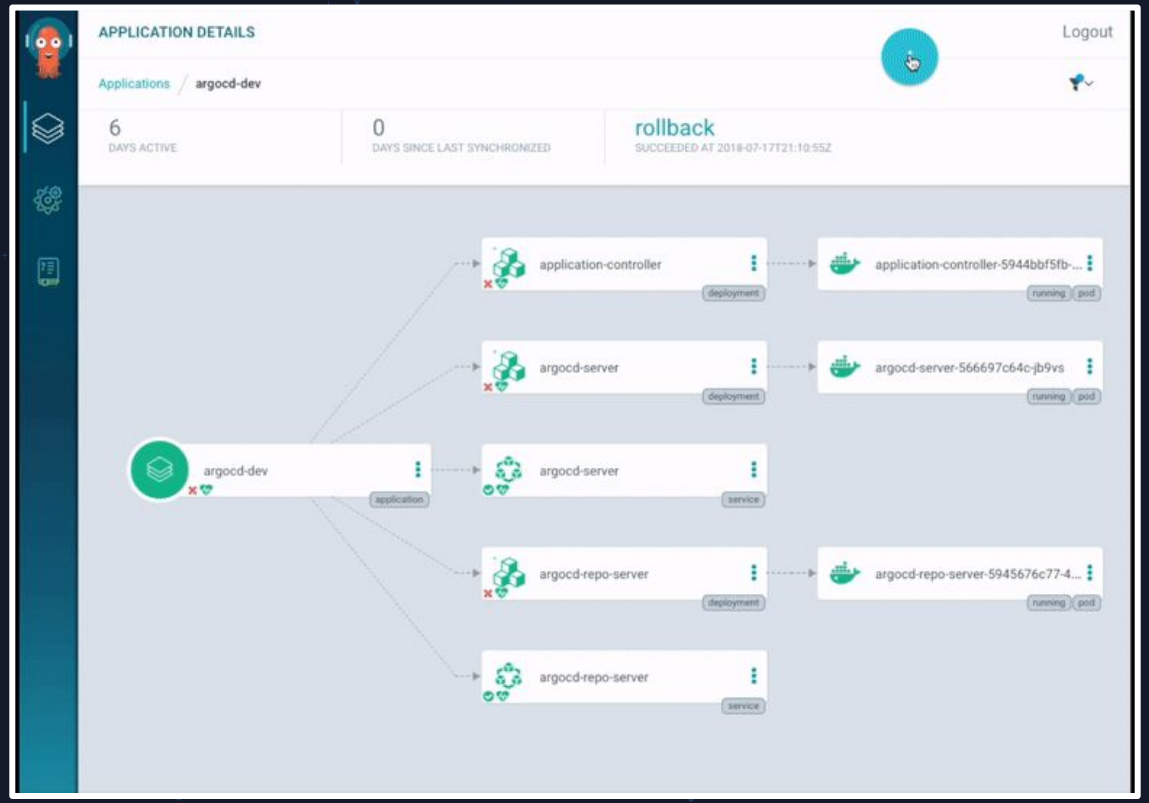
Ref

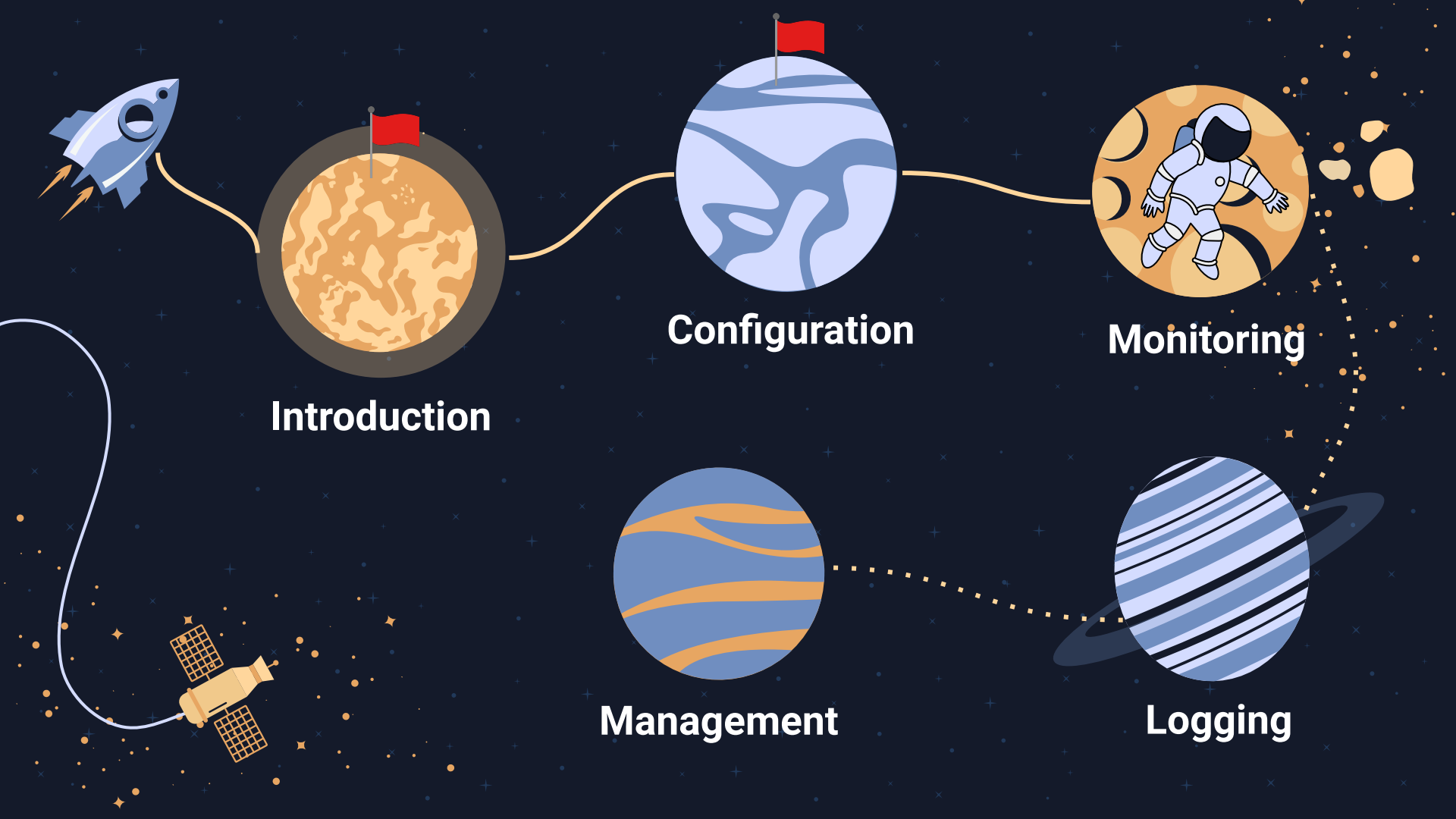
Use Argo CD With ApplicationSet Controller



Ref

Friendly UI


APPLICATION DETAILS
Logout
Applications
argocd-dev
6
DAYS ACTIVE
0
DAYS SINCE LAST SYNCHRONIZED
rollback
SUCCEEDED AT 2018-07-17T21:10:55Z
application-controller
deployment
application-controller-5944bbf5fb-...
running
pod
argocd-server
deployment
argocd-server-566697c64c-jb9vs
running
pod
argocd-dev
application
argocd-server
service
argocd-repo-server
deployment
argocd-repo-server-5945676c77-4...
running
pod
argocd-repo-server
service


Introduction
Configuration
Monitoring
Management
Logging

No Doubt! Prometheus With Operator

K8s Service
(Exporter)

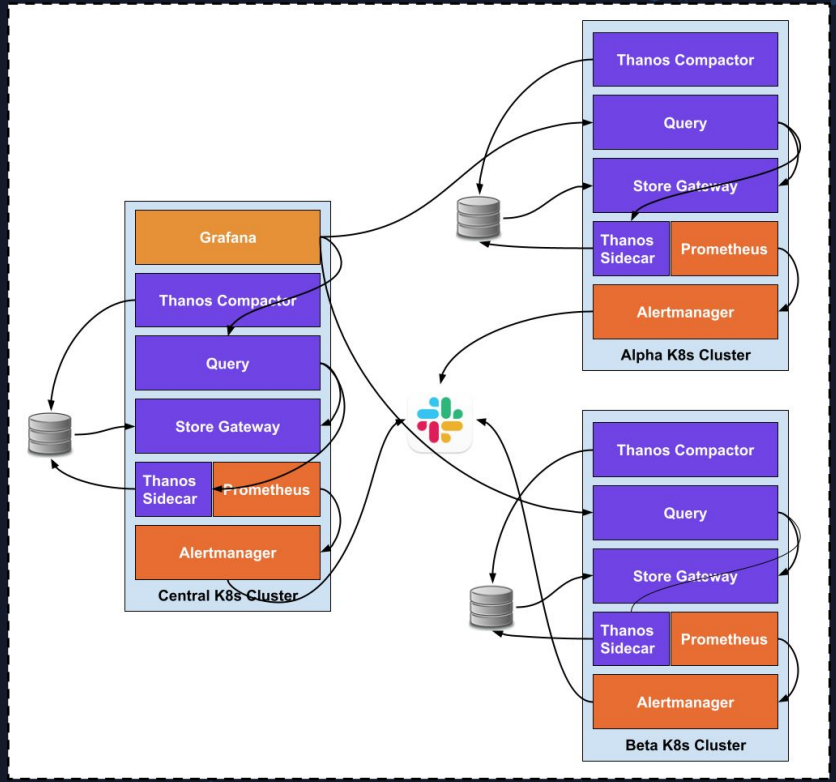
K8s ServiceMonitor
(CRD)

Prometheus

Alertmanager

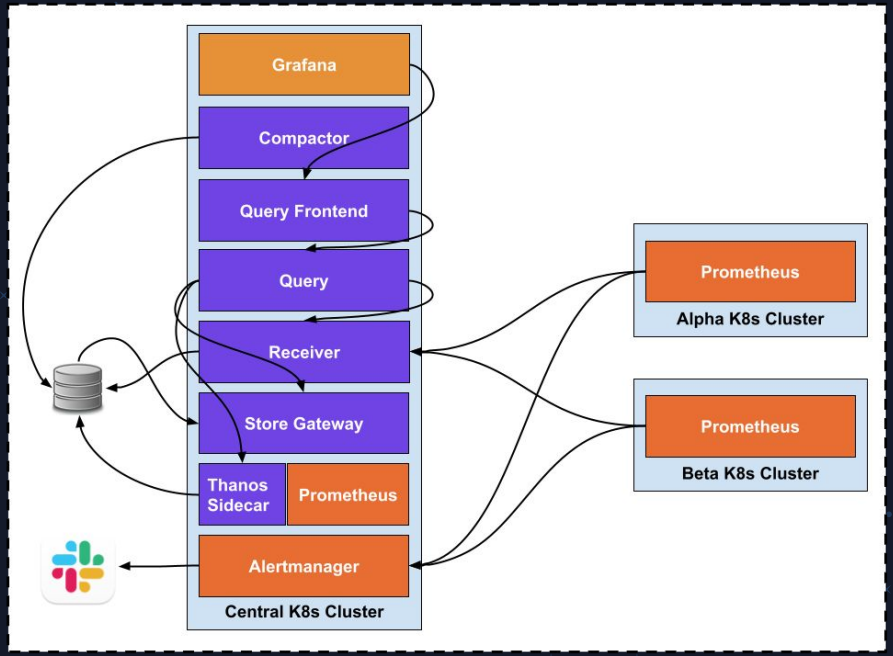
Ref

Pure Prometheus Stack With Thanos



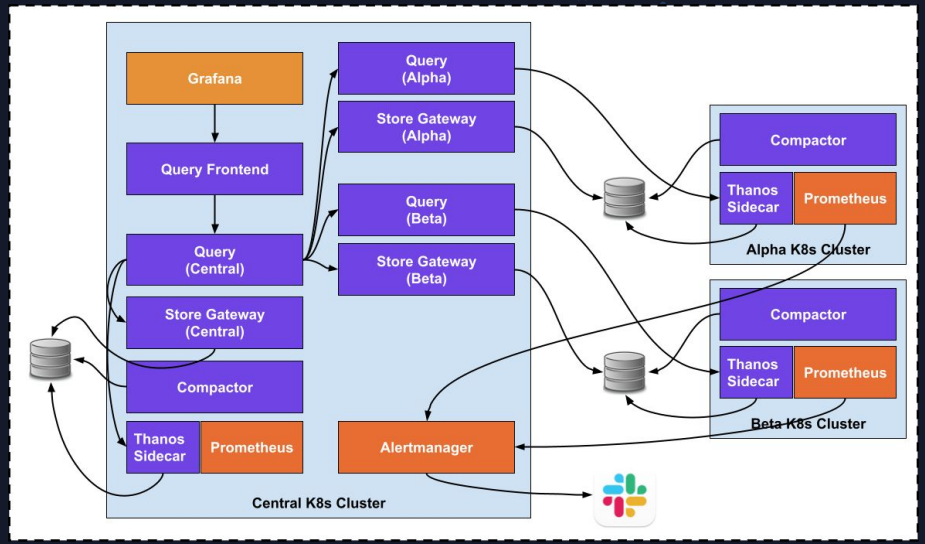
- Pros
  - Stable
  - Separate Metric Lifecycle
  - Highly Isolation
- Cons
  - Different Data Source
  - Query Performance
  - Manage Effort

Prometheus Remote Write With Thanos

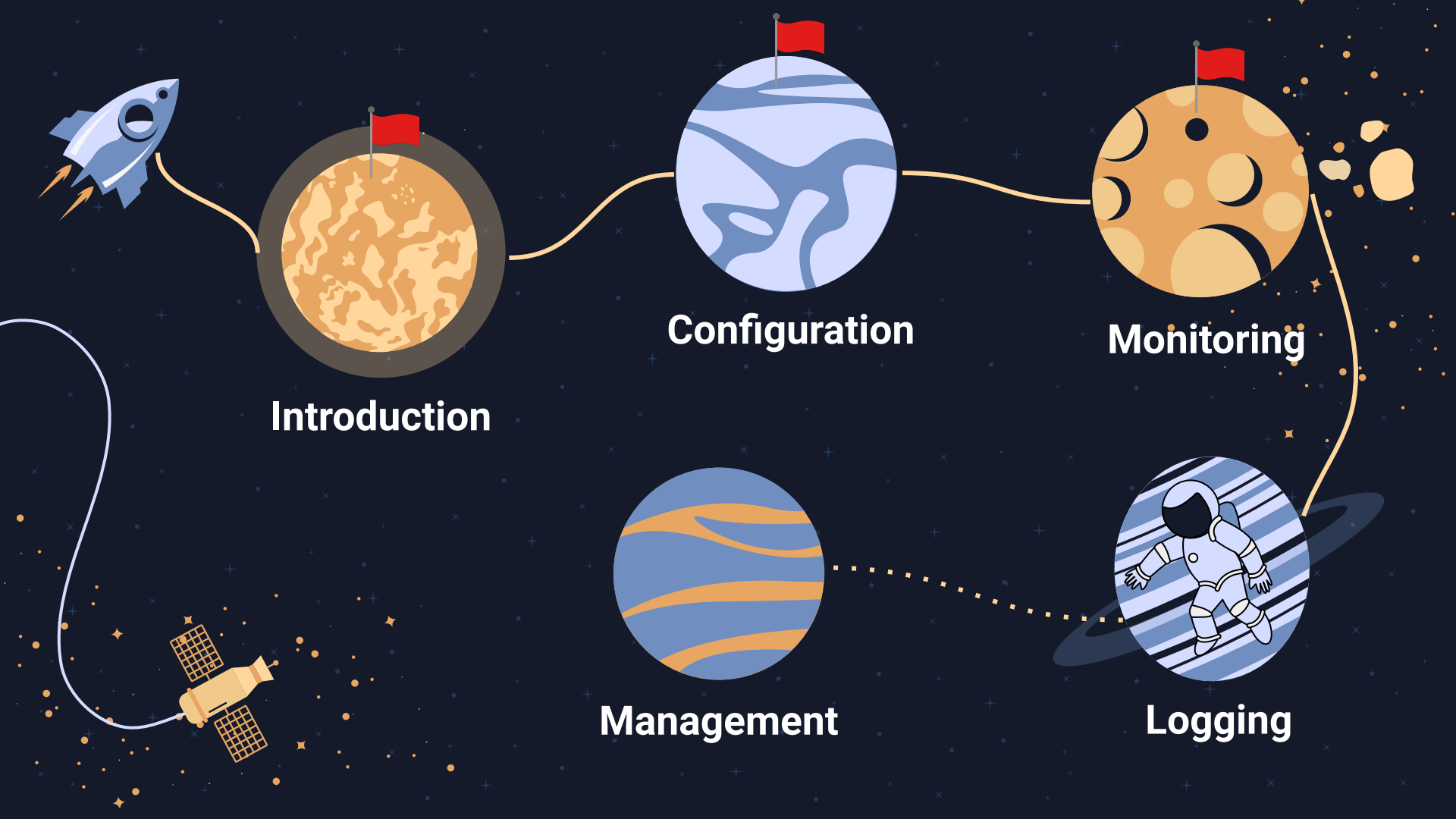


- Pros
  - Central Query View
  - Cost Efficiency
  - Less Manage Effort
- Cons
  - No Separate Metric Lifecycle
  - Single Point of Failure

Remote Query Prometheus With Thanos



- Pros
  - Central Query View
  - Separate Metric Lifecycle
  - Less SPOF
- Cons
  - Complicated Setup
  - Less Resource Sharing


Introduction
Configuration
Monitoring
Logging
Management

ElasticSearch VS Loki

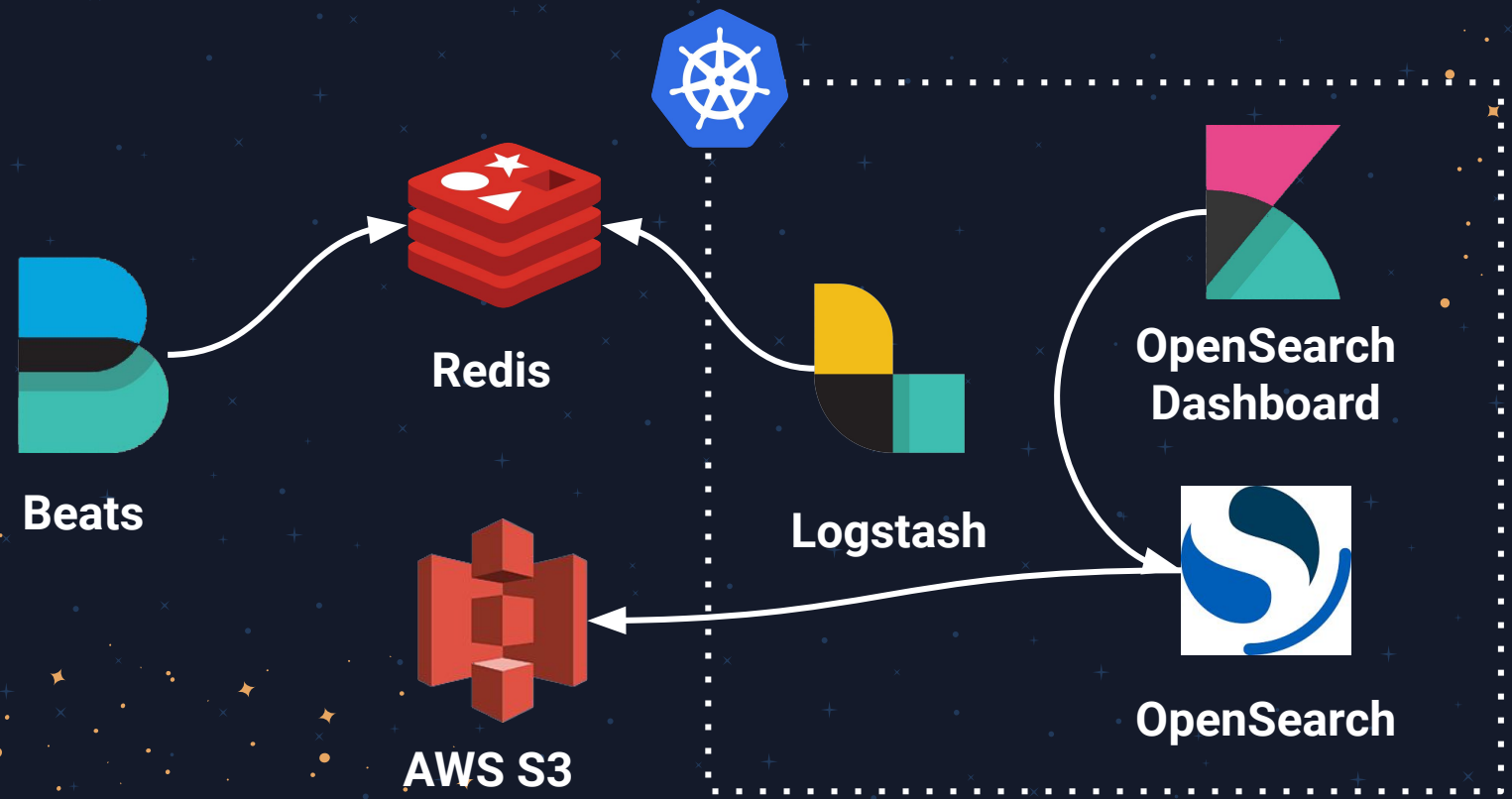
Criteria	ELFK	PLG
Resource Usage	High	Low ✌️
Data Processing	Logs Content Processing ✌️	Metadata Processing
Search	Complex Queries and Filter ✌️	Simple Search, No Filter
Scalability	Highly Configurable ✌️	Not Well-Documented
Access	Paid Subscription	Grafana OSS Feature ✌️
Alerting	Complex Alerts Through Third-Party Tools	Promtail -> Log-Based Metrics ✌️
Performance	Can Make Complex Selections ✌️	Not Recommended to Select More Than 5-10k Entries
Dashboards	Kibana Can Build Rich Dashboards ✌️	Simple Tables W/ Log Data

Ref

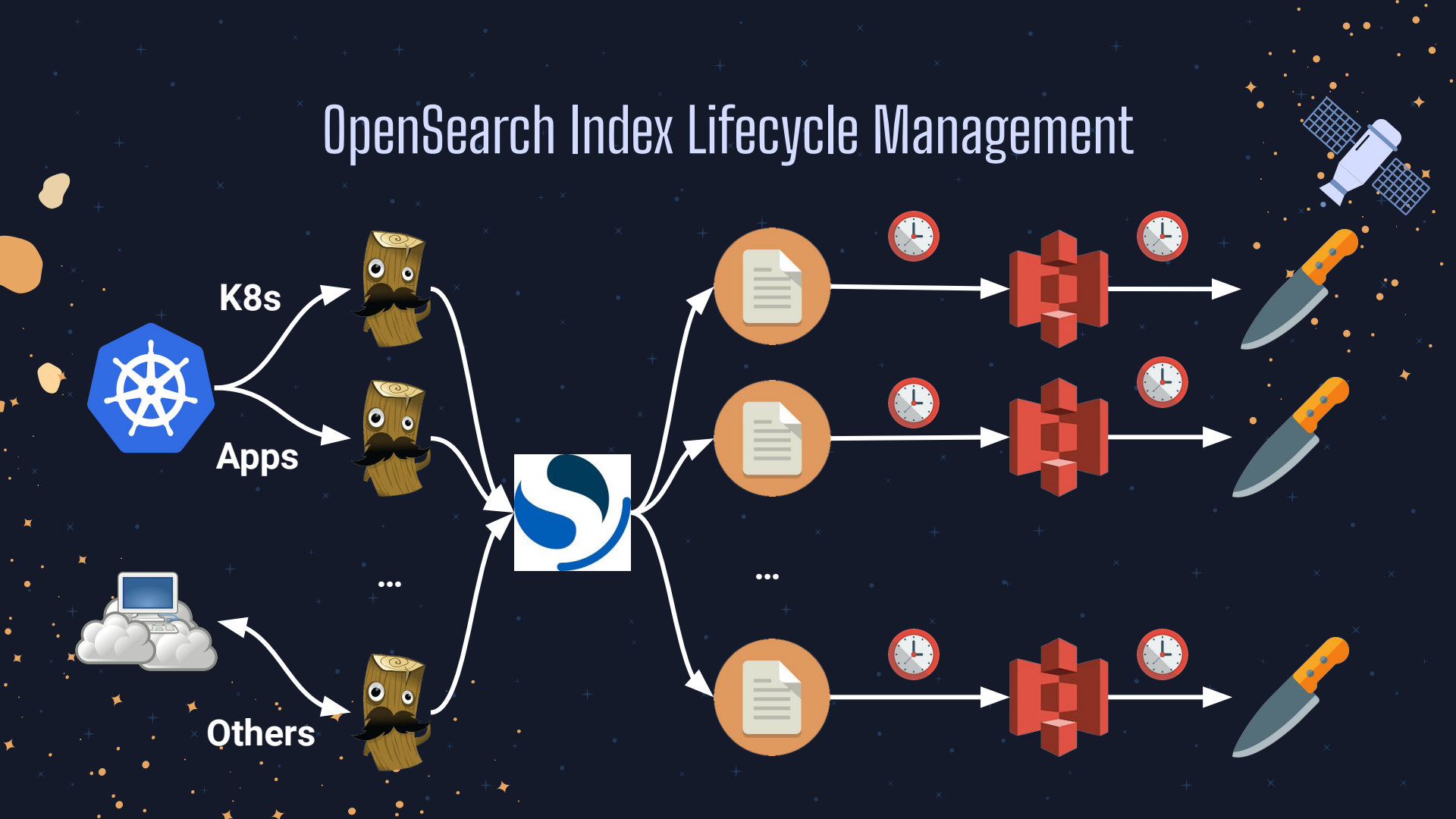
ElasticSearch □ OpenSearch

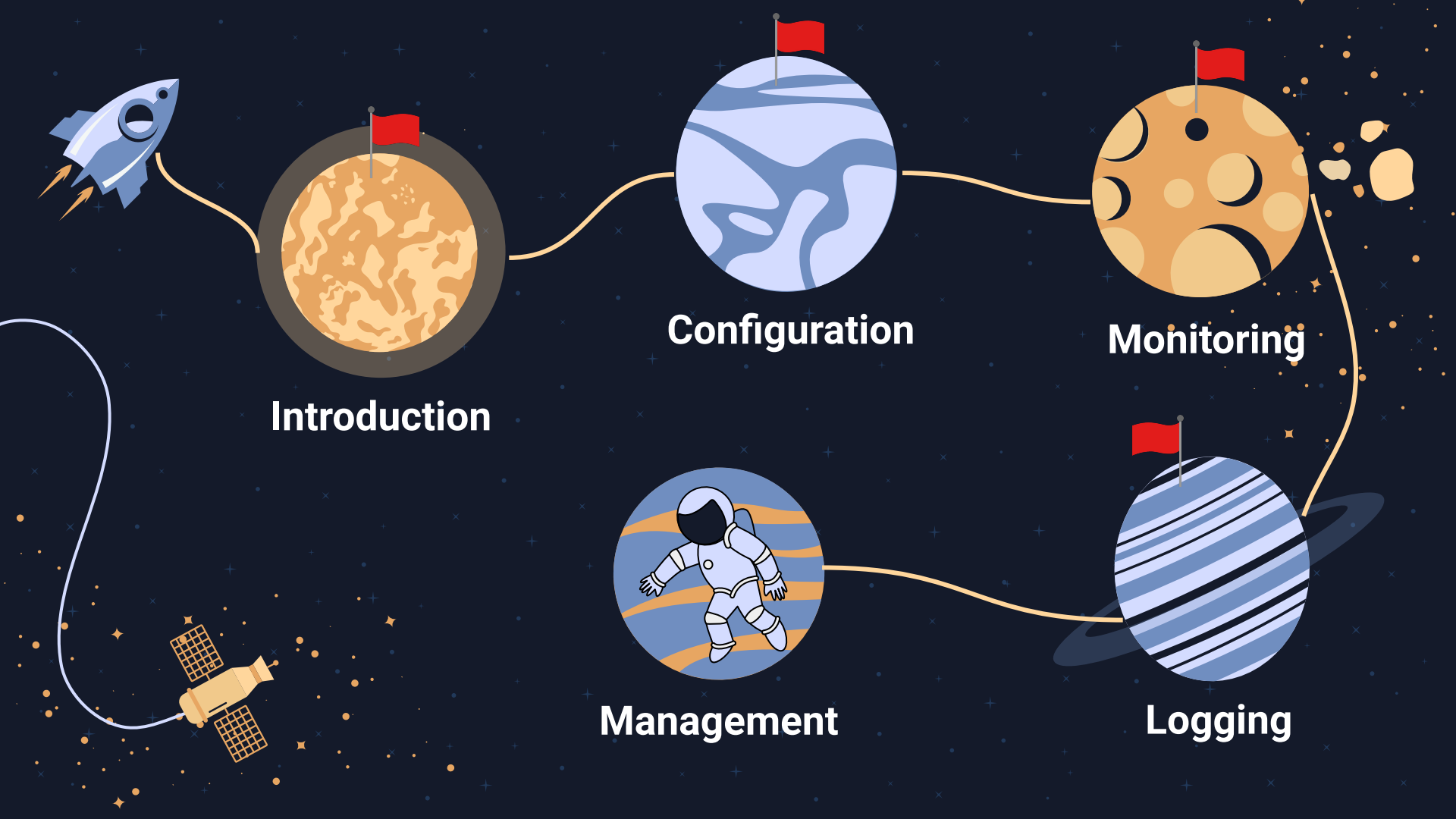
- Authentication & Authorization in OSS Version
- The Most Important Little Thing
  - Customized From ElasticSearch 7.10.2
  - Install OpenSearch Output Plugin in Logstash
  - No UltraWarm Feature in OSS Version
- Reference
  - ElasticSearch Evolution: Cost ⬇️
  - ElasticSearch Tuning: Performance ⬆️

Central Logging Service Architecture



OpenSearch Index Lifecycle Management




Introduction
Configuration
Monitoring
Logging
Management

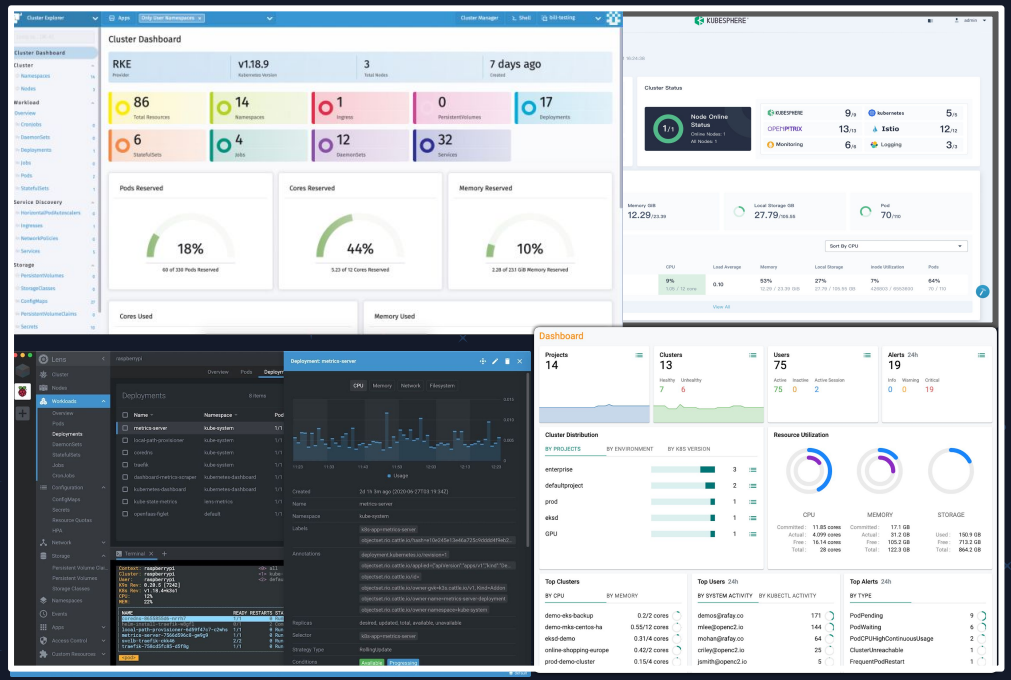
A Centralized Place to Manage K8s Multi-Cluster

What Feature Required in The Platform

- Configuration & Provision
- Manage
  - Visualize K8s Resource
  - Monitoring & Logging
  - Simplified Service Mesh
- Secure
  - Authentication
  - Authorization
- Upgrades
- ...

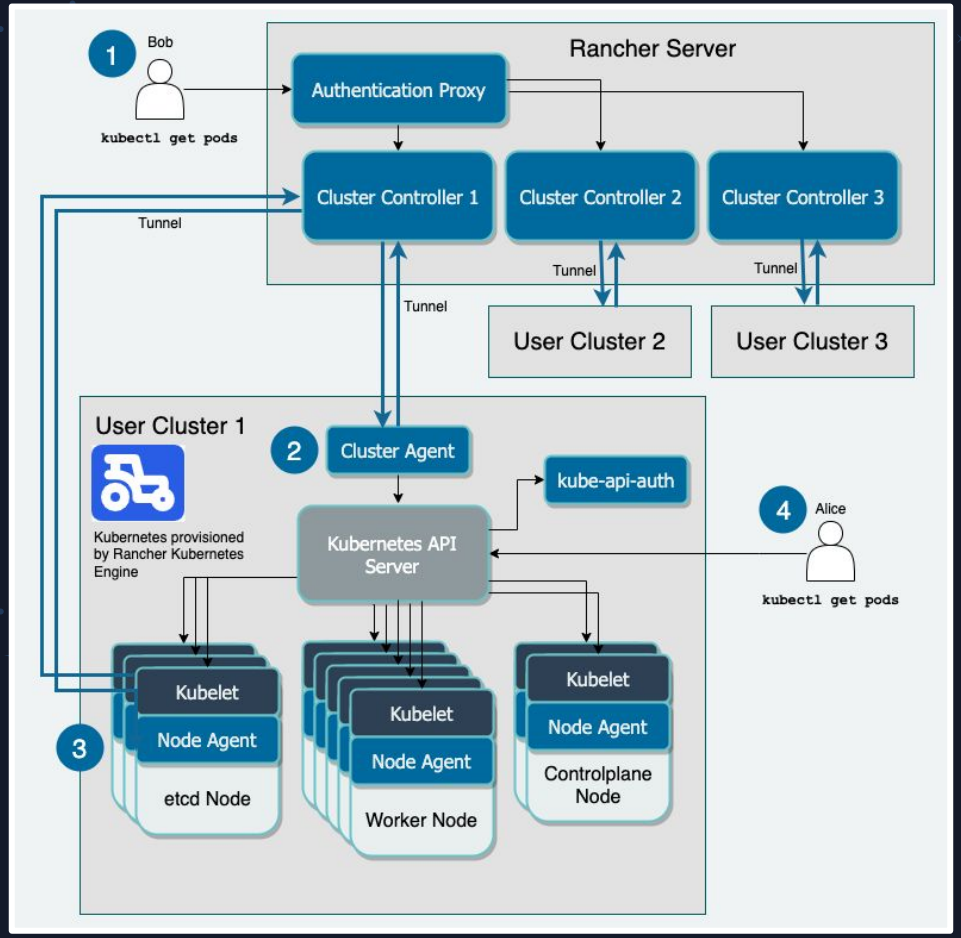
Solutions

- Server Side
  - Rancher ✌️
  - KubeSphere
  - Rafay
- Client Side
  - Lens ✌️

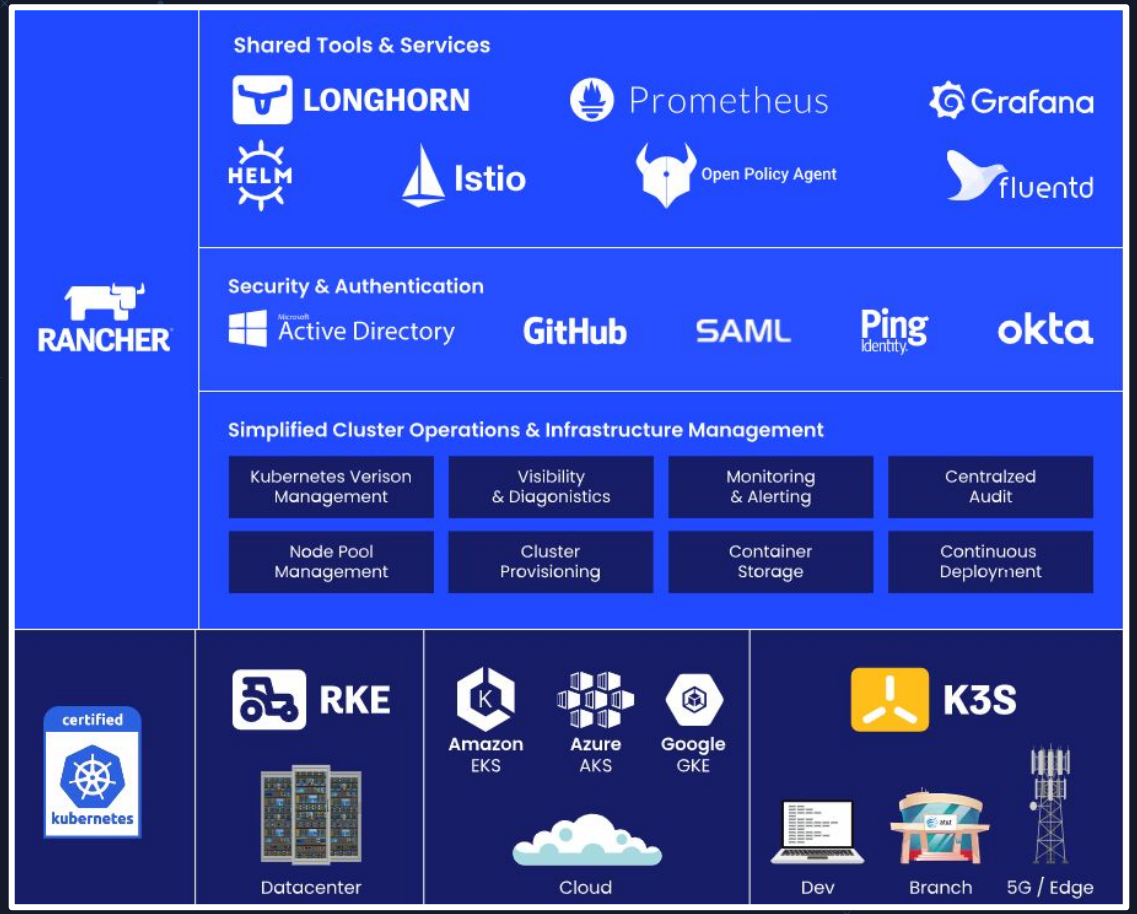


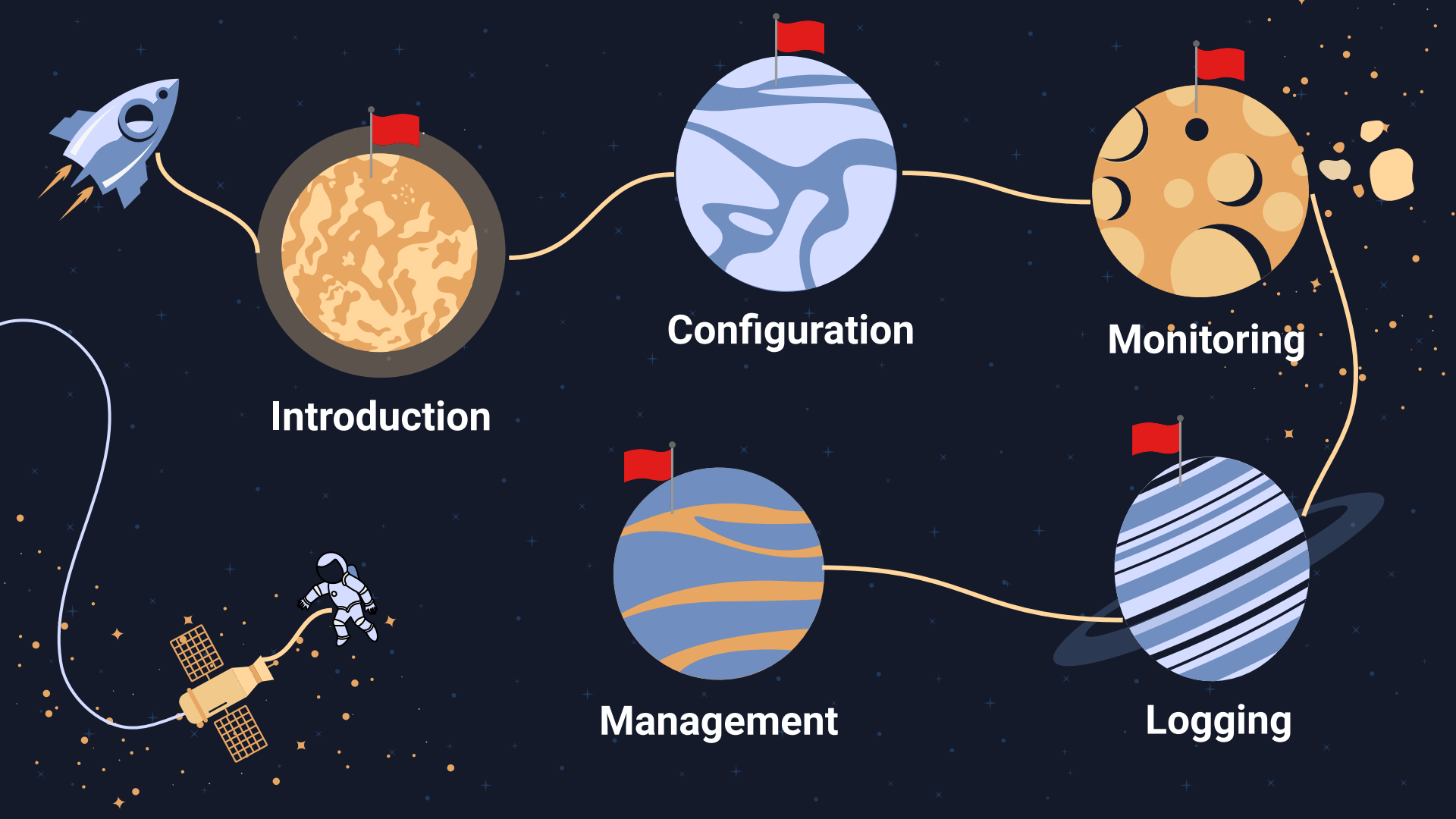
Ref

Rancher Server Architecture



Rancher Ecosystem




Introduction
Configuration
Monitoring
Logging
Management

THANKS!

ANY QUESTIONS?

You can find me at my office:

- Blockchain Engineer
- Backend Engineer
- Frontend Engineer
- ...