A cloud-native approach for managing Kubernetes clusters in a hybrid cloud environment

Realised by: **Mouad El Haouari**

Supervised by: **Antonio Nappi**

CERN openlab

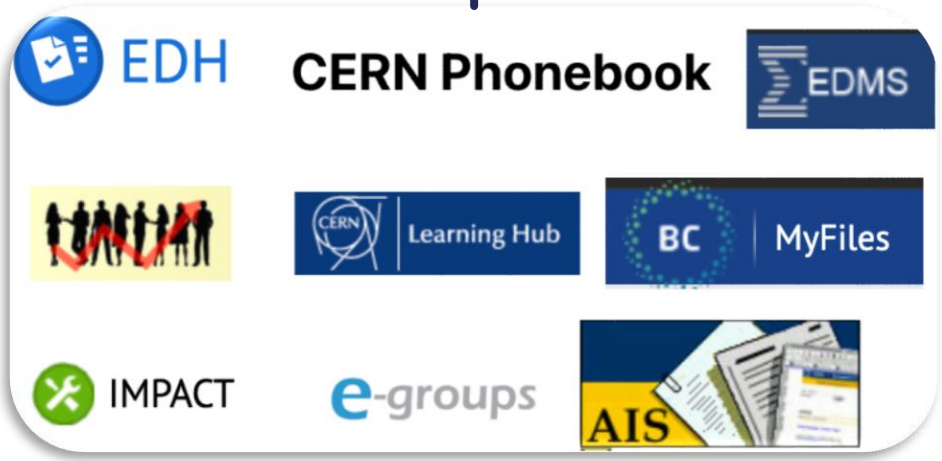
Table of Contents

Context

IT-PW-ARW
(Applications and Reusable Workflows**)**

Providing hosting infrastructure based on **Kubernetes** for:

- **SSO** (Single Sign On)
- **CERN critical java applications** for Finance and Administrative Processes (FAP) and engineering (EN) departments such as **EDH** and **EDMS**.



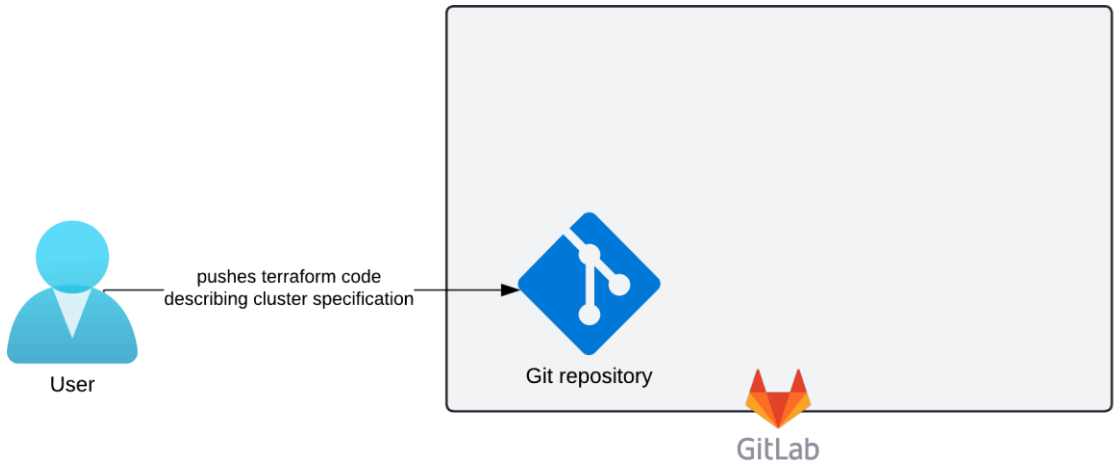
Problem Statement

Current approach

HashiCorp Terraform + CI/CD

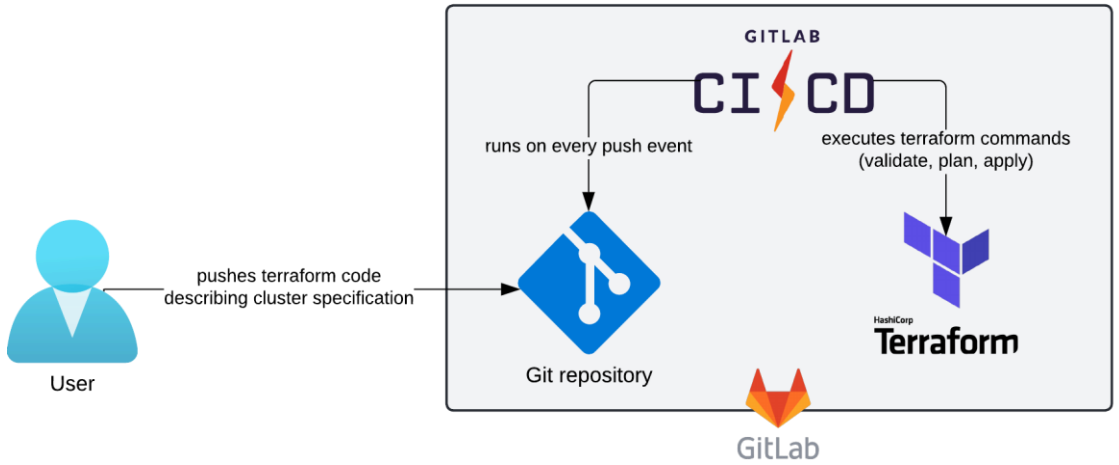
Problem Statement

Current approach



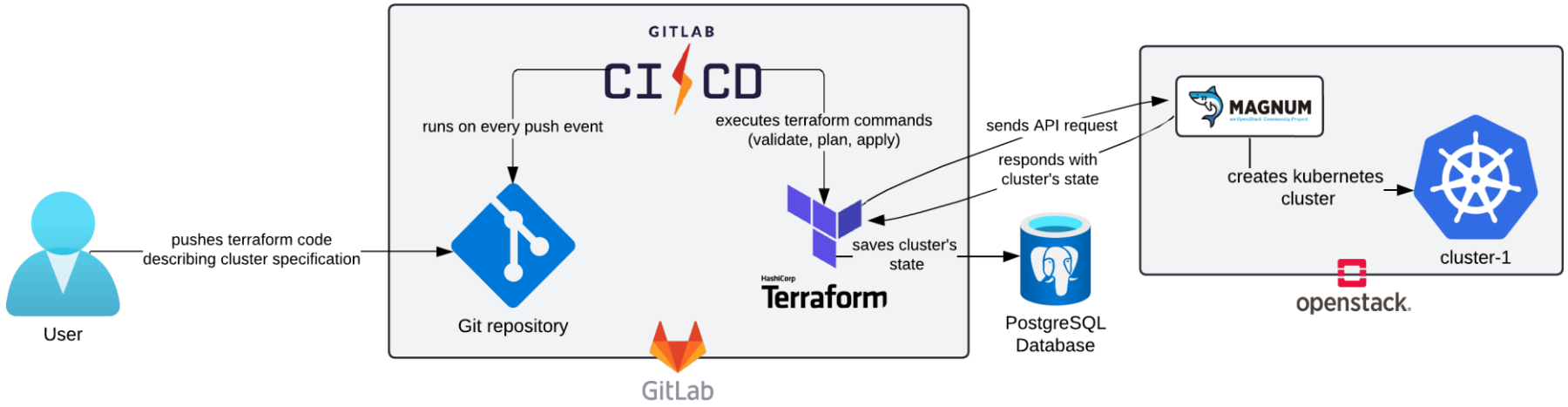
Problem Statement

Current approach



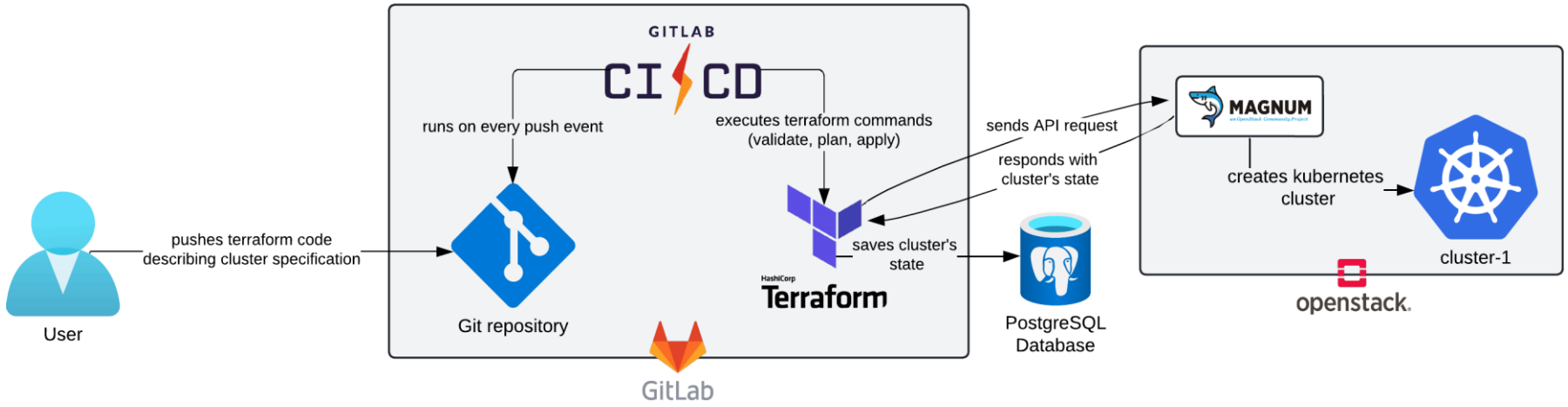
Problem Statement

Current approach



Problem Statement

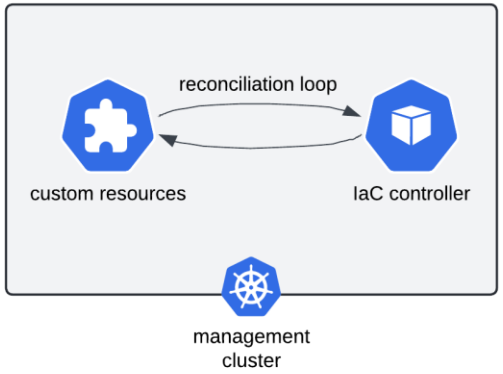
Current approach



Drawbacks

- Terraform is **not Kubernetes-native**
- **Not effective** for **disaster recovery** (strong dependency on an external CI/CD and a database)

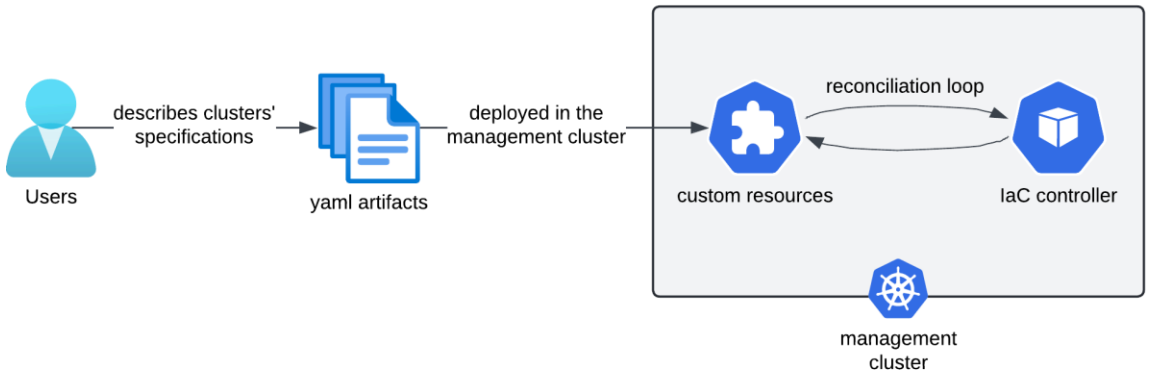
Objective



Propose a unified and cloud native approach for managing Kubernetes clusters on both on-premise (Openstack) and public cloud (Oracle Cloud Infrastructure)

*** IaC:** Infrastructure as Code

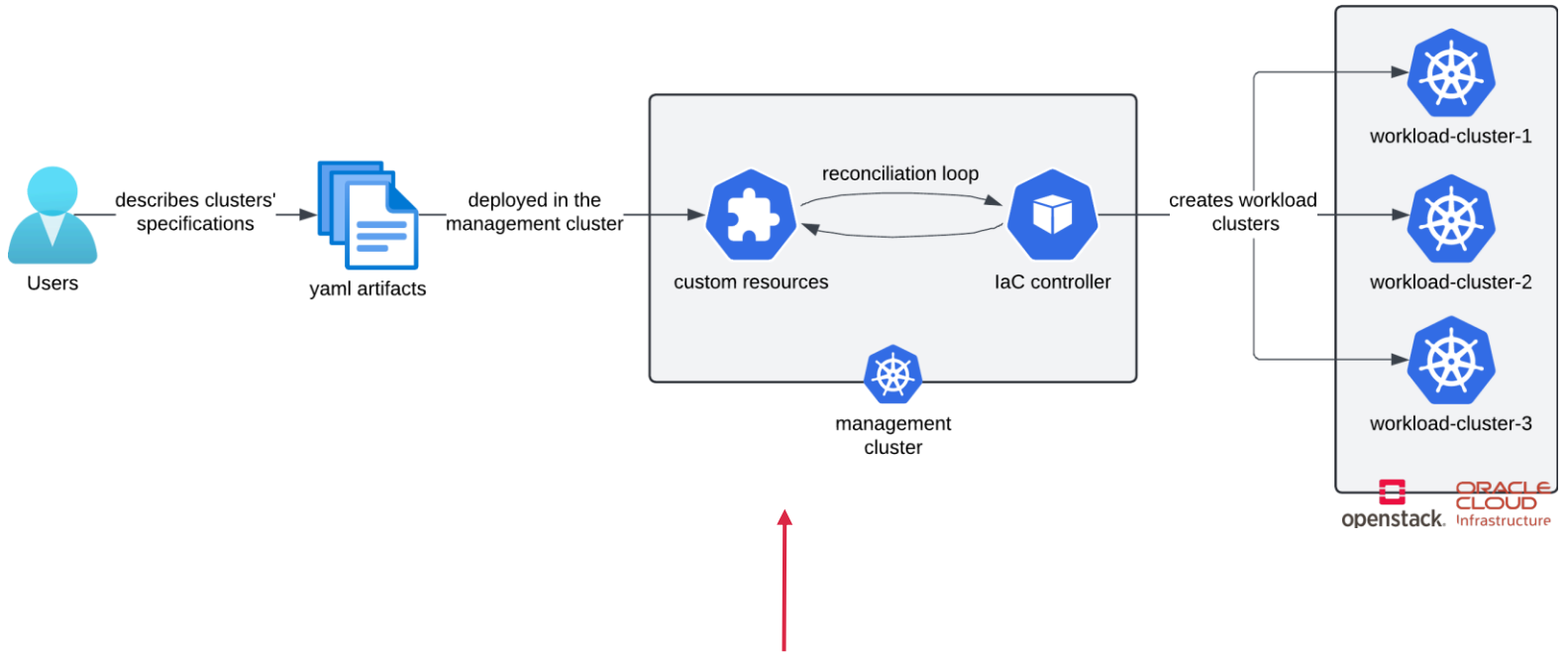
Objective



Propose a unified and cloud native approach for managing Kubernetes clusters on both on-premise (Openstack) and public cloud (Oracle Cloud Infrastructure)

*** IaC:** Infrastructure as Code

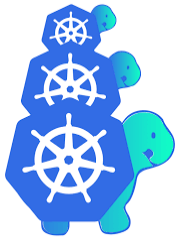
Objective



Propose a unified and cloud native approach for managing Kubernetes clusters on both on-premise (Openstack) and public cloud (Oracle Cloud Infrastructure)

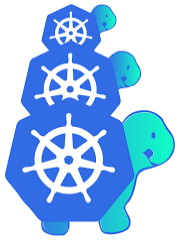
*** IaC:** Infrastructure as Code

Investigations

Cloud-native IaC tools	Overview	openstack.	ORACLE CLOUD Infrastructure
 ClusterAPI	• **focused on** the lifecycle management of **Kubernetes clusters**		
 Crossplane	• a **general purpose** IaC tool • **based on terraform** under the hood • providers are created using a code generation tool called **Upjet** that allows code generation of a crossplane provider from a terraform provider		

*** IaC:** Infrastructure as Code

Investigations

Cloud-native IaC tools	Overview	openstack.	ORACLE CLOUD Infrastructure
 ClusterAPI	• **focused on** the lifecycle management of **Kubernetes clusters**	• Does not support creating Kubernetes clusters through **Magnum** service • It can be used as a backend for **Magnum** instead of **Heat** service • Creating clusters using **Nova** service does not work with CERN Openstack cloud due to networking constraints	
 Crossplane	• a **general purpose** IaC tool • **based on terraform** under the hood • providers are created using a code generation tool called **Upjet** that allows code generation of a crossplane provider from a terraform provider		

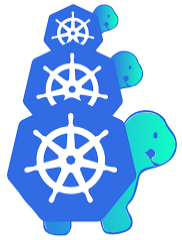
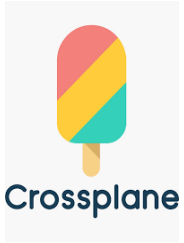
*** IaC:** Infrastructure as Code

Investigations

Cloud-native IaC tools	Overview	openstack.	ORACLE CLOUD Infrastructure
ClusterAPI	• **focused on** the lifecycle management of **Kubernetes clusters**	• Does not support creating Kubernetes clusters through **Magnum** service • It can be used as a backend for **Magnum** instead of **Heat** service • Creating clusters using **Nova** service does not work with CERN Openstack cloud due to networking constraints	• Supports creating both self-managed and managed clusters
Crossplane	• a **general purpose** IaC tool • **based on terraform** under the hood • providers are created using a code generation tool called **Upjet** that allows code generation of a crossplane provider from a terraform provider		

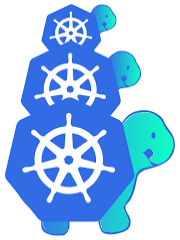
*** IaC:** Infrastructure as Code

Investigations

Cloud-native IaC tools	Overview	openstack.	ORACLE CLOUD Infrastructure
 ClusterAPI	• **focused on** the lifecycle management of **Kubernetes clusters**	• Does not support creating Kubernetes clusters through **Magnum** service • It can be used as a backend for **Magnum** instead of **Heat** service • Creating clusters using **Nova** service does not work with CERN Openstack cloud due to networking constraints	• Supports creating both self-managed and managed clusters
 Crossplane	• a **general purpose** IaC tool • **based on terraform** under the hood • providers are created using a code generation tool called **Upjet** that allows code generation of a crossplane provider from a terraform provider	• Supports creating clusters through **Magnum**	

*** IaC:** Infrastructure as Code

Investigations

Cloud-native IaC tools	Overview	openstack.	ORACLE CLOUD Infrastructure
 ClusterAPI	• **focused on** the lifecycle management of **Kubernetes clusters**	• Does not support creating Kubernetes clusters through **Magnum** service • It can be used as a backend for **Magnum** instead of **Heat** service • Creating clusters using **Nova** service does not work with CERN Openstack cloud due to networking constraints	• Supports creating both self-managed and managed clusters
 Crossplane	• a **general purpose** IaC tool • **based on terraform** under the hood • providers are created using a code generation tool called **Upjet** that allows code generation of a crossplane provider from a terraform provider	• Supports creating clusters through **Magnum**	• No provider available (there is one, but it has been abandoned by oracle and it is not officially recognized by crossplane)

*** IaC:** Infrastructure as Code

Solution

Technology Choice

+

Why ?

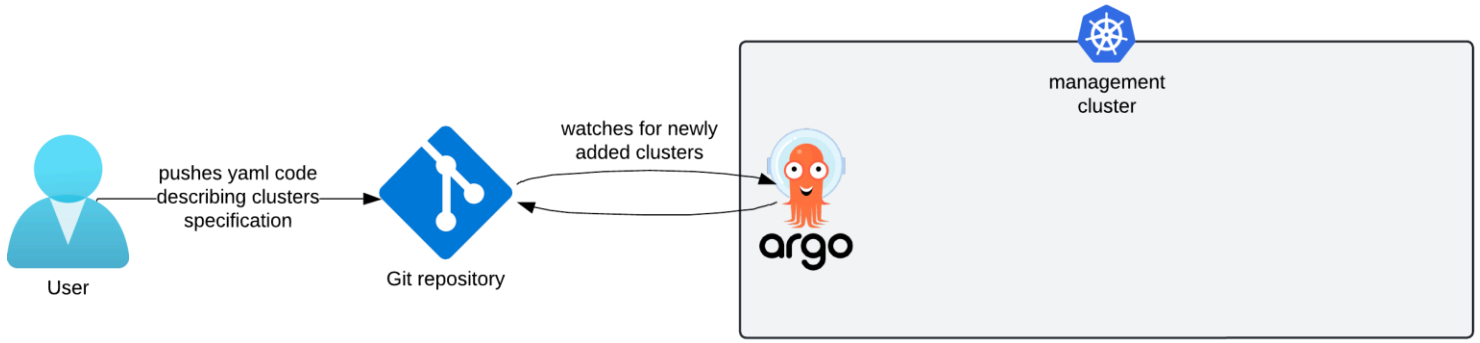
Openstack is the priority because **all our productions clusters are running on OpenStack** at the moment

Why ?

A CD pipeline that runs within Kubernetes to **automate Kubernetes objects deployment from a git repository**

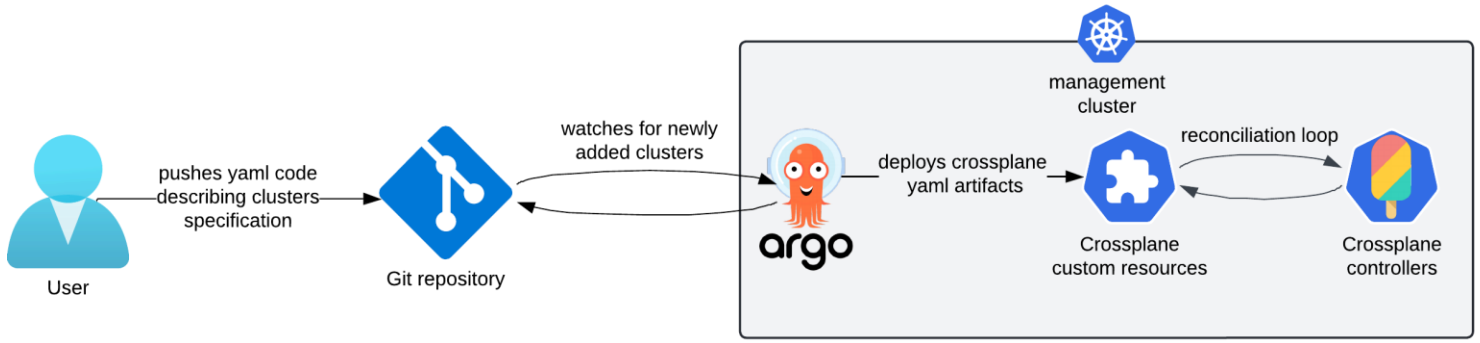
Solution

Proposed approach



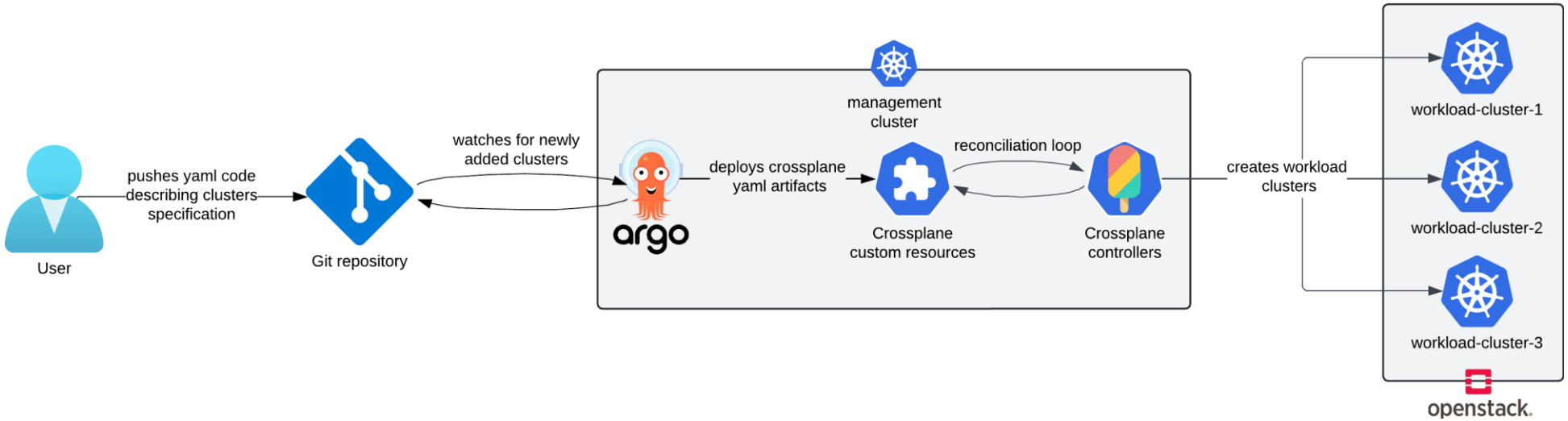
Solution

Proposed approach



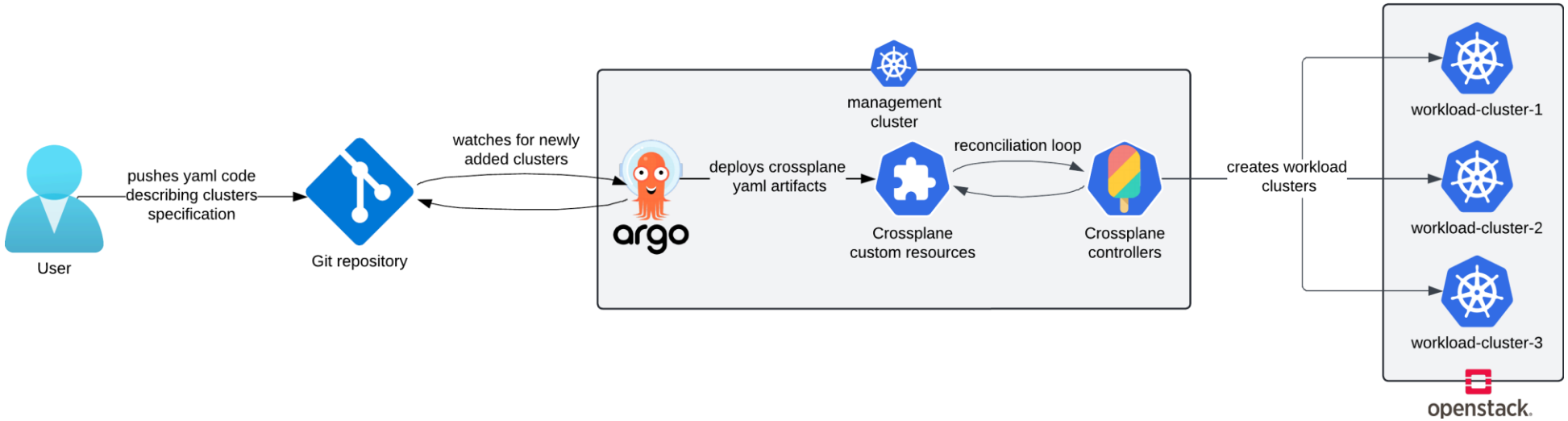
Solution

Proposed approach



Solution

Proposed approach



Advantages

- A **unified approach** for deploying applications and infrastructure
- **Faster recovery** of Kubernetes clusters (It takes only few steps)

Current vs Proposed Approach

Approach	Declarative	Version control	Requirements	Maintenance
HashiCorp Terraform Current GitLab CI/CD	Yes	Yes	• Gitlab repository • Gitlab CI/CD • PostgreSQL database	Not Straightforward (HCL - HashiCorp Configuration Language)
Crossplane Proposed argo	Yes	Yes	A Kubernetes cluster with ArgoCD installed	Easy (Kubernetes Object)

Conclusion & Perspectives

- Relying on a cloud-native IaC tool allows for both Kubernetes oriented infrastructure deployment and effective disaster recovery
- We will pass the feedback to Oracle to highlight the missing provider for Crossplane
- Integrating ClusterAPI with CERN Openstack could be possible but requires collaborative efforts between multiple teams

*** IaC:** Infrastructure as Code

Thank you!

Questions ?

mouadelhaouari1@gmail.com

mouad.el.haouari@cern.ch

CERN openlab