



Managing Kubernetes Clusters in a multicloud environment

CERN openlab summer student Lightning talks

Author: Daniel Vera Nieto

Supervisor: Antonio Nappi

07/09/2021

The problem

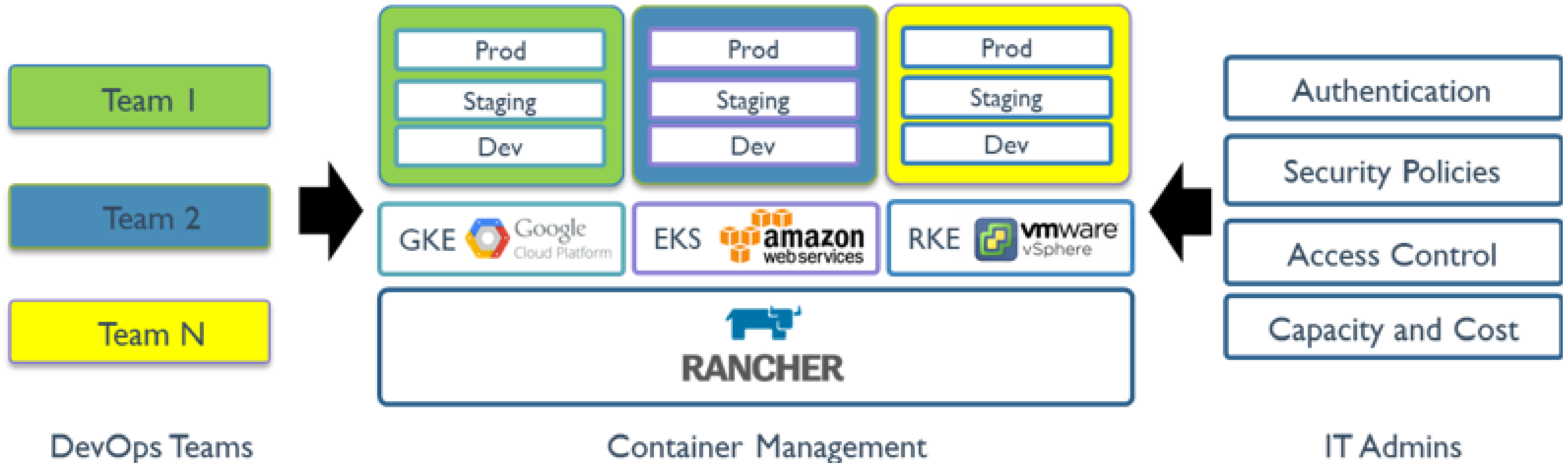


kubernetes

- Migration to Kubernetes
- Hybrid Cloud multi-clusters environment: Openstack & OCI
 - Overall idea of what is being used
 - Provide read-only access to the teams of the applications

How can we manage clusters running in different places using just a tool?

Solution: Rancher



Project steps

1. Run Rancher locally
2. Run Rancher on a k8s cluster
3. Webhook Issue
4. Import some clusters

Imported clusters

<input type="checkbox"/>	State ▾	Name ▾	Version ▾	Provider ▾	Machines/Nodes	Age ▾	
<input type="checkbox"/>	Active	ais-cluster	v1.18.6	Imported	86	5 mins	Explore ⋮
<input type="checkbox"/>	Active	edms-cluster	v1.18.6	Imported	7	10 mins	Explore ⋮
<input type="checkbox"/>	Active	ims-cluster	v1.18.6	Imported	8	14 mins	Explore ⋮
<input type="checkbox"/>	Active	local	v1.21.1	Imported	5	2.7 hours	Explore ⋮

Imported clusters

The screenshot displays the OpenLab Cluster Dashboard for a local cluster. The interface includes a sidebar with navigation options: Cluster, Projects/Namespaces, Nodes (1), Workload, Apps & Marketplace, Service Discovery, Storage, RBAC, and More Resources. The main content area is titled "Cluster Dashboard" and provides the following information:

- Provider:** K3s
- Kubernetes Version:** v1.21.2
- Created:** 13 days ago
- [Install Monitoring](#)

Key metrics are displayed in three cards:

- Total Resources:** 35
- Node:** 1
- Deployments:** 8

Capacity usage is shown in three cards with progress bars:

- Pods:** Used 9 / 110 (8.18%)
- Cores:** Reserved 0.1 / 2 (5.00%)
- Memory:** Reserved 0.07 / 3.84 GiB (1.82%)

At the bottom, there is a "Cluster Tools" button and an "Events" section.

Project steps

1. Run Rancher locally
2. Run Rancher on a k8s cluster
3. Webhook Issue
4. Import some clusters
5. Enable SSO Authentication
 1. SAML
 2. OIDC -> Rancher dev version
 3. The "Groups" problem

Auth
API

App
Portal

...

CERN SSO

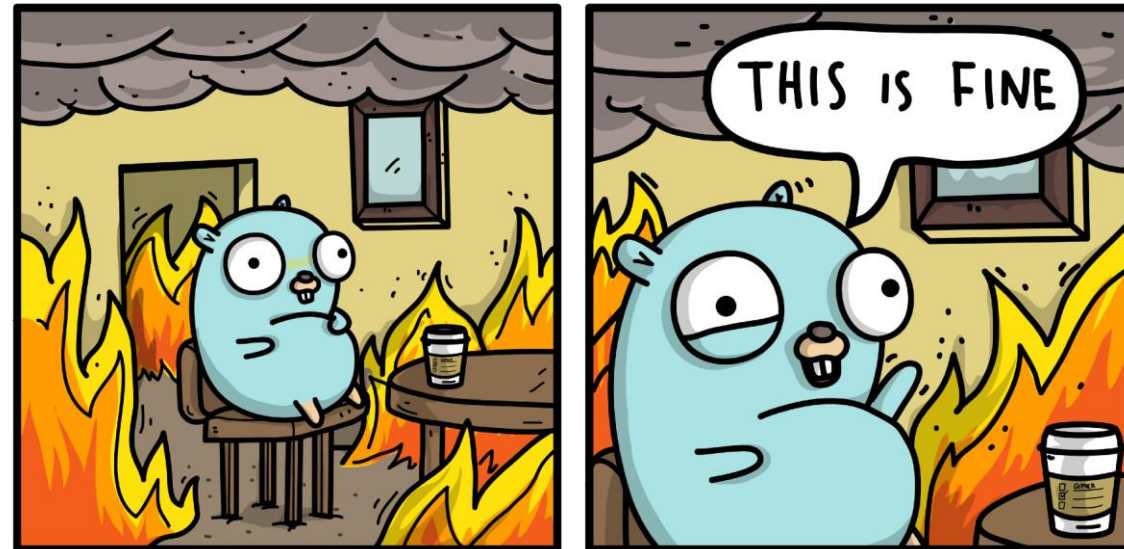


What's the problem then?

1. Rancher queries the IDP to retrieve the groups
2. It assumes it can access directly to the keycloak server
3. CERN SSO does not allow that, you must use the Auth API (different endpoint)
4. You need an API access token first
5. Rancher was looking for "Users" and "Groups" resources, SSO has "Identity" and "Group" resources.

Solution: Modify Rancher

1. Written in Go language (Never used it before)
2. Set up a local Rancher dev env
3. Request API Access Token
4. Query the SSO API endpoint
5. Request the correct resource
6. Get CERN groups!



Assign Global Roles To Group

Select Member

Start typing to search for principals

Your Groups:

- cern-computing
Keycloak Group
- lxadm-authorized-users
Keycloak Group
- cern-active-users
Keycloak Group
- SC-IT-DEP
Keycloak Group
- pacS-egroup-test-cernpriv
Keycloak Group

Future work

1. Refactor my code modifications to support other organizations
2. Make a Pull Request
3. Integrate my code modifications into Rancher
4. Deploy Rancher in production



QUESTIONS?

daveni@protonmail.com

@daveni_