Proyecto Integrador DevOps 2203

El repositorio del proyecto se encuentra aquí.

Grupo 7 - DevOps2203

- Luis Miguel Mamani Humpiri
- Carlos Ruiz de la Vega
- Reynaldo Capia Capia

Instrucciones

El proyecto CDK para el aprovisionamiento del nodo bastión se encuentra en cdk-bastion.

Despliegue desde bastión

Desde bastión sólo es necesario desplegar el pipeline. Por defecto, el pipeline será disparado por cambios en la rama definida en `core.common.PIPELINE_GITHUB_BRANCH`. Antes de realizar el despliegue se requiere acceder a la consola y configurar la conexión a Github aquí.

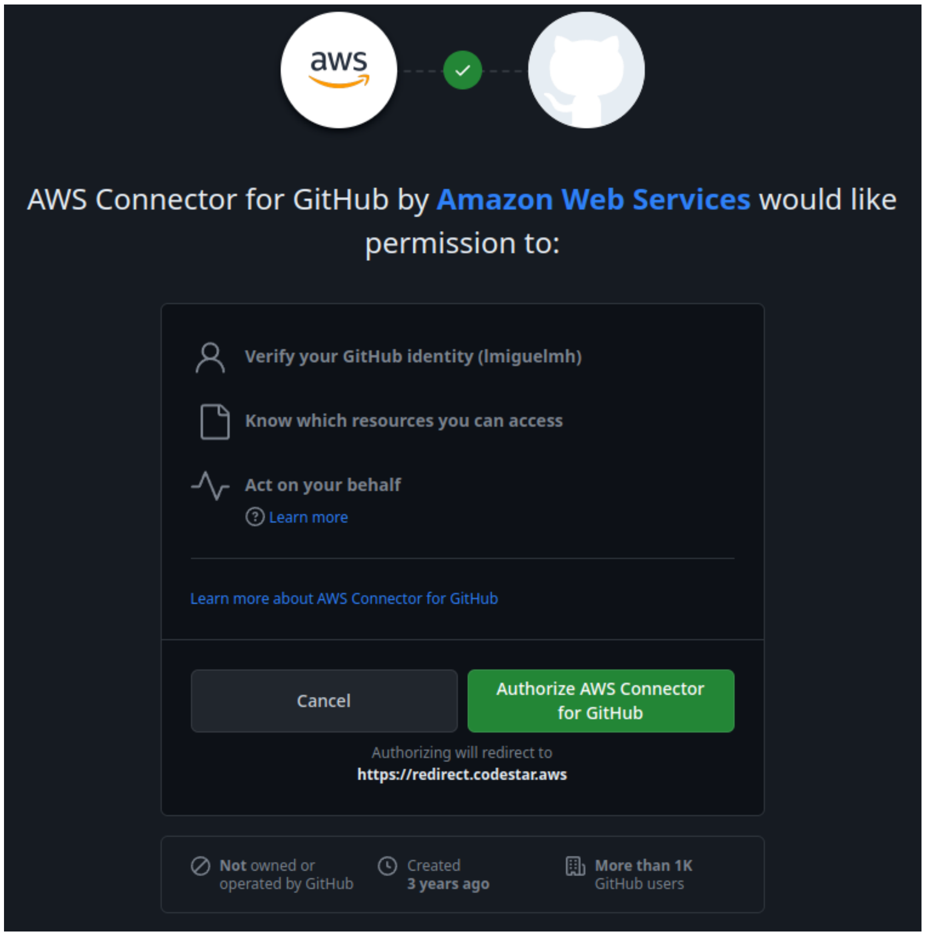
Al finalizar, completar la información en el archivo de configuración `core.conf.{ENV}`.

```
# set the environment/configuration
# on this case we will use the configuration defined on `core.conf.common` and `core.conf.de
export ENV=dev

# deploy the pipeline
cdk deploy eks-toolchain
```

Despliegue desde local

El despliegue desde local permite el desarrollo ágil y el despliegue de uno o varios stacks sin necesidad de desplegar toda la aplicación.

```
# set the environment/configuration
export ENV=sandbox

# here we deploy the EKS cluster
cdk deploy eks-cluster

# update kube configuration to access the EKS cluster
# run the command located on the output of ClusterStack
aws eks update-kubeconfig ...

# test kubectl
```



AWS Connector for GitHub by **Amazon Web Services** would like permission to:

Verify your GitHub identity (lmiguelmh)

Know which resources you can access

Act on your behalf

Learn more

Learn more about AWS Connector for GitHub

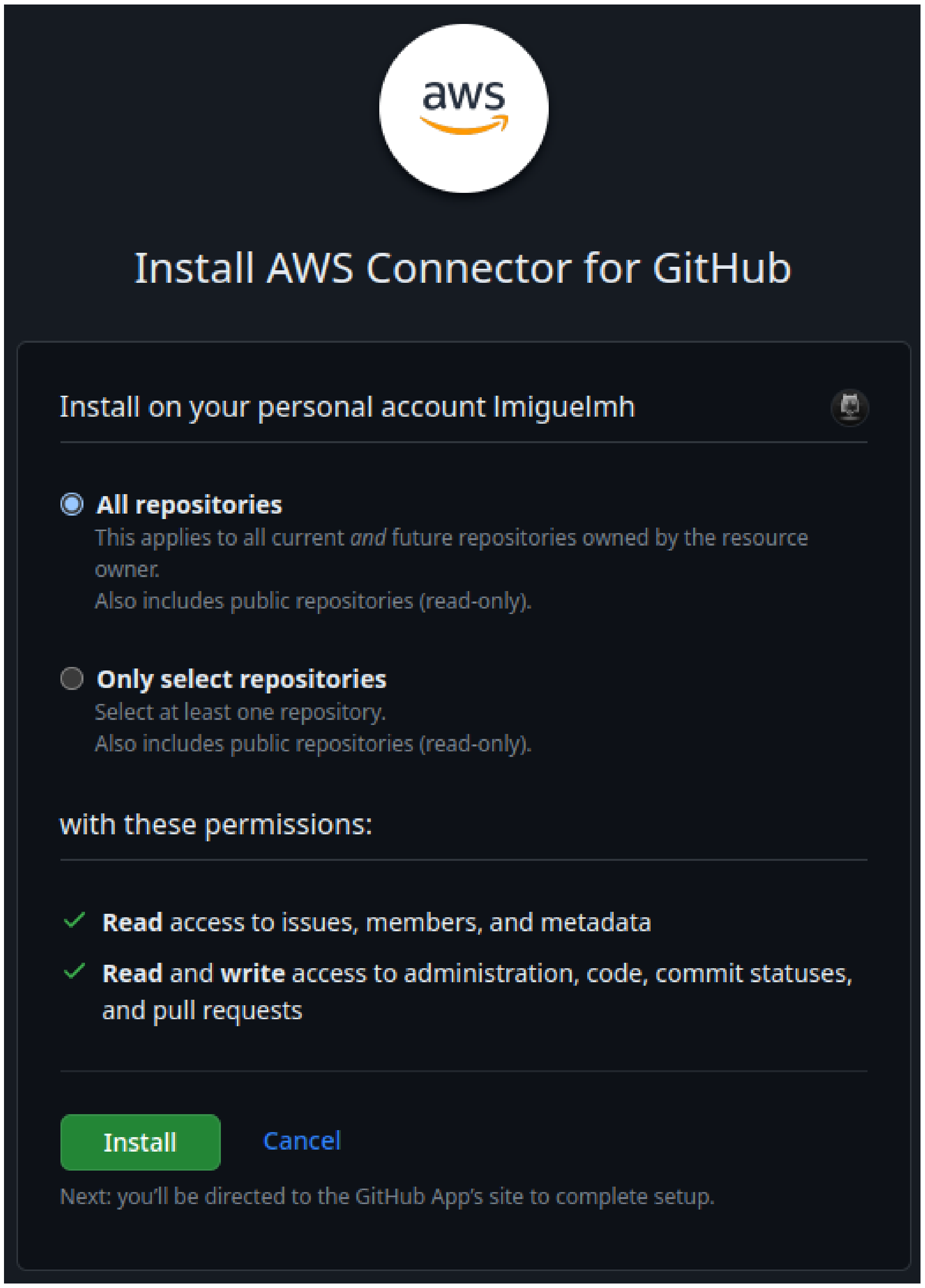
Authorizing will redirect to **https://redirect.codestar.aws**

Not owned or operated by GitHub

Created **3 years ago**

More than 1K GitHub users

Figure 1: img_28.png



Install AWS Connector for GitHub

Install on your personal account lmiguelmh

[✓ **All repositories**]
This applies to all current *and* future repositories owned by the resource owner.
Also includes public repositories (read-only).

Only select repositories
Select at least one repository.
Also includes public repositories (read-only).

with these permissions:

✓ **Read** access to issues, members, and metadata

✓ **Read** and **write** access to administration, code, commit statuses, and pull requests

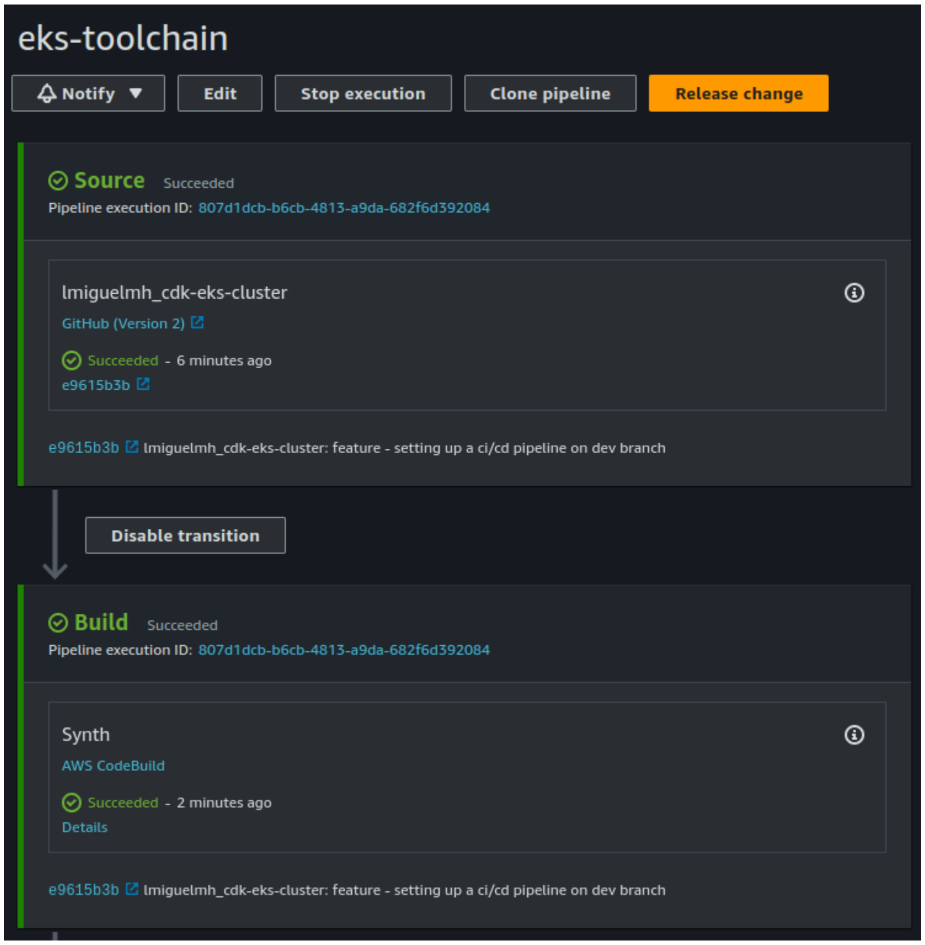
Next: you'll be directed to the GitHub App's site to complete setup.

Figure 2: img_29.png

```
kubectl get all

# beware that resources created by kubectl need to be deleted manually (ie. load balancers)
kubectl apply -f pod.yml
kubectl get pods
kubectl delete -f pod.yml
```

Despliegue desde pipeline

El despliegue desde el pipeline se dispara automáticamente cuando se realizan cambios en la rama configurada. En entorno `dev` la rama configurada es `dev`.



Source Succeeded
Pipeline execution ID: 807d1dcb-b6cb-4813-a9da-682f6d392084

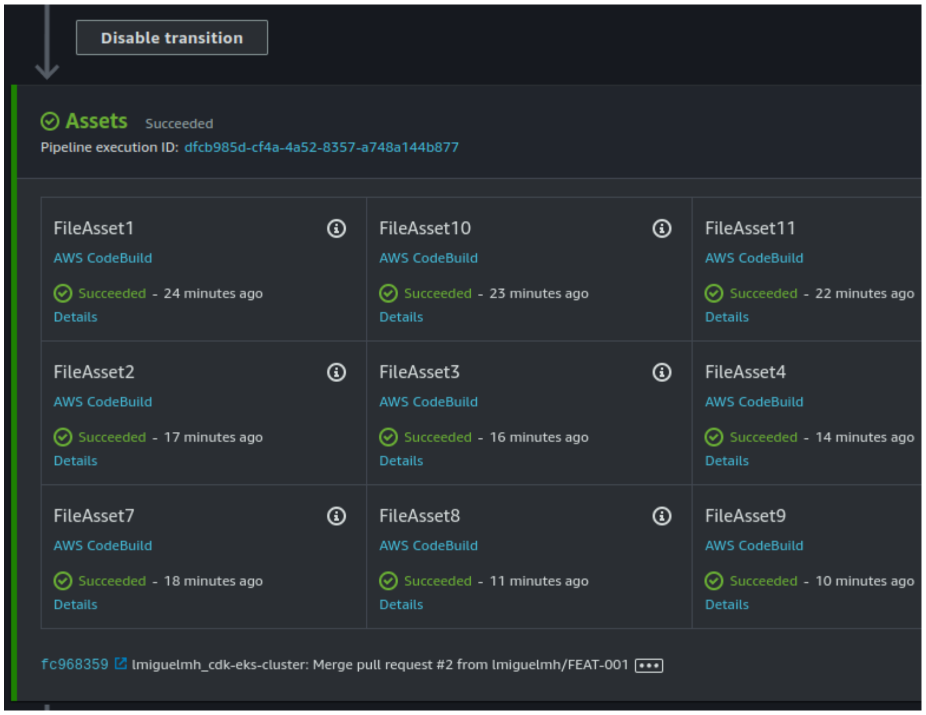
lmiguelmh_cdk-eks-cluster
GitHub (Version 2)
Succeeded - 6 minutes ago
e9615b3b

e9615b3b lmiguelmh_cdk-eks-cluster: feature - setting up a ci/cd pipeline on dev branch

Build Succeeded
Pipeline execution ID: 807d1dcb-b6cb-4813-a9da-682f6d392084

Synth
AWS CodeBuild
Succeeded - 2 minutes ago
Details

e9615b3b lmiguelmh_cdk-eks-cluster: feature - setting up a ci/cd pipeline on dev branch



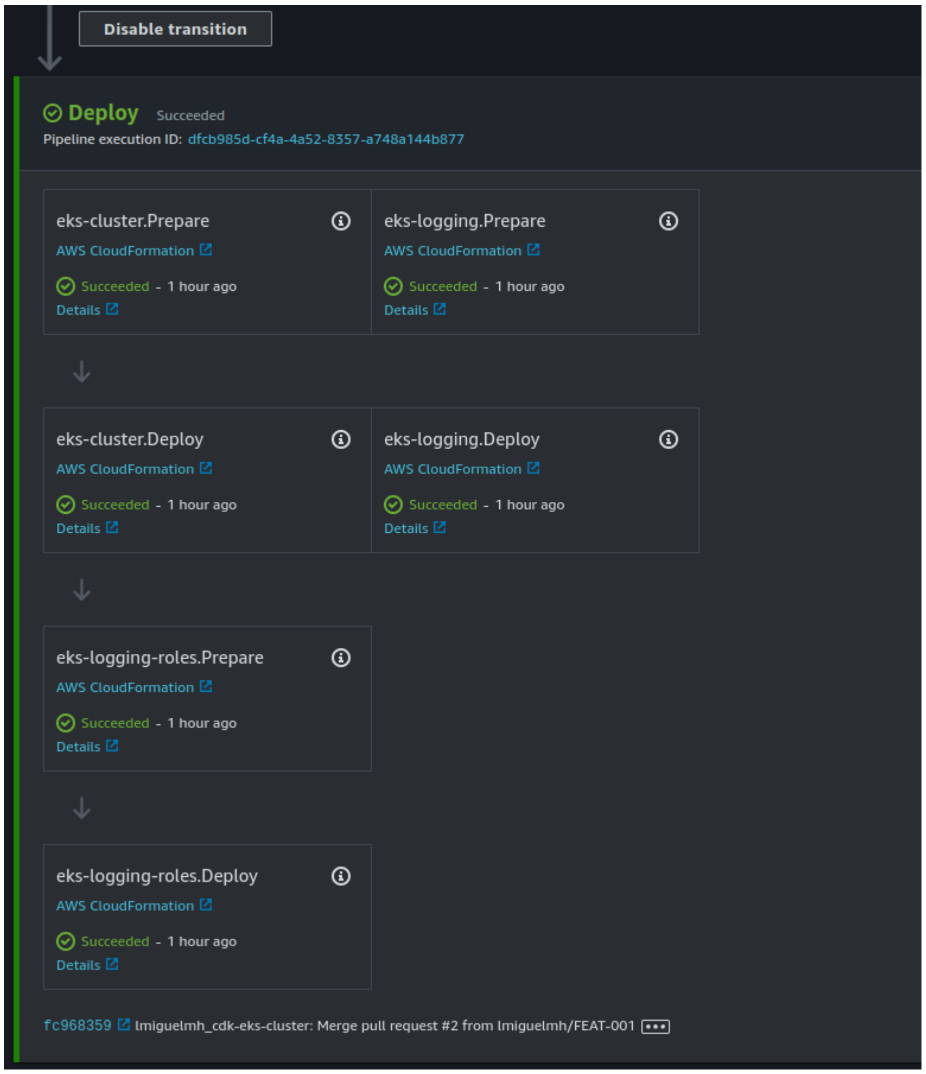
Disable transition

Assets Succeeded

Pipeline execution ID: dfcb985d-cf4a-4a52-8357-a748a144b877

FileAsset1 AWS CodeBuild Succeeded - 24 minutes ago Details	FileAsset10 AWS CodeBuild Succeeded - 23 minutes ago Details	FileAsset11 AWS CodeBuild Succeeded - 22 minutes ago Details
FileAsset2 AWS CodeBuild Succeeded - 17 minutes ago Details	FileAsset3 AWS CodeBuild Succeeded - 16 minutes ago Details	FileAsset4 AWS CodeBuild Succeeded - 14 minutes ago Details
FileAsset7 AWS CodeBuild Succeeded - 18 minutes ago Details	FileAsset8 AWS CodeBuild Succeeded - 11 minutes ago Details	FileAsset9 AWS CodeBuild Succeeded - 10 minutes ago Details

fc968359 lmiguelmh_cdk-eks-cluster: Merge pull request #2 from lmiguelmh/FEAT-001


Disable transition

Deploy Succeeded
Pipeline execution ID: dfcb985d-cf4a-4a52-8357-a748a144b877

eks-cluster.Prepare
AWS CloudFormation
Succeeded - 1 hour ago
Details

eks-logging.Prepare
AWS CloudFormation
Succeeded - 1 hour ago
Details

eks-cluster.Deploy
AWS CloudFormation
Succeeded - 1 hour ago
Details

eks-logging.Deploy
AWS CloudFormation
Succeeded - 1 hour ago
Details

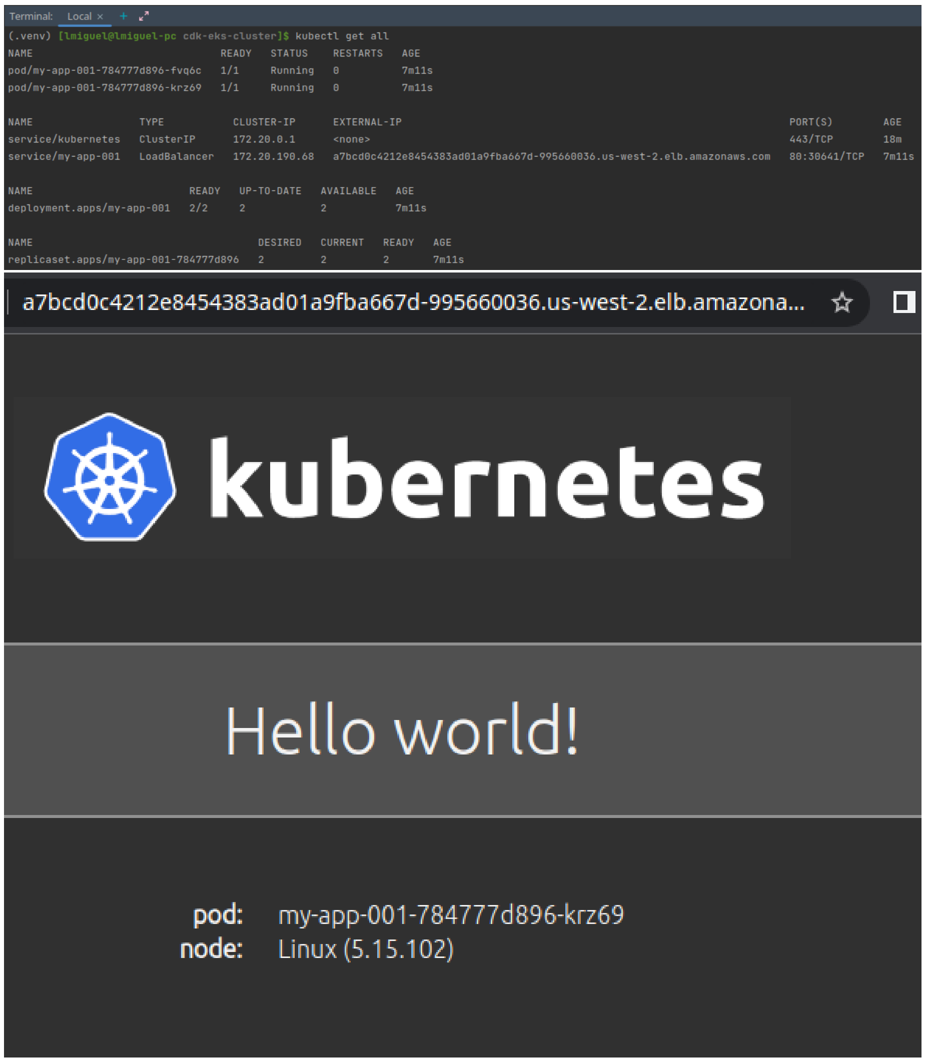
eks-logging-roles.Prepare
AWS CloudFormation
Succeeded - 1 hour ago
Details

eks-logging-roles.Deploy
AWS CloudFormation
Succeeded - 1 hour ago
Details

fc968359 lmiguelmh_cdk-eks-cluster: Merge pull request #2 from lmiguelmh/FEAT-001

Configuración del Cluster EKS

- La definición del cluster se encuentra en ClusterStack.
- Se usó CDK para la creación de la infraestructura.
  - El aprovisionamiento de los nodos se realiza con un ASG.
  - Otros recursos son aprovisionados
- La definición del servicio y el despliegue de la aplicación de ejemplo también se encuentra en ClusterStack.



```
(.venv) [lmiguel@lmiguel-pc cdk-eks-cluster]$ kubectl get all
NAME                             READY   STATUS    RESTARTS   AGE
pod/my-app-001-784777d896-fvq6c   1/1     Running   0          7m11s
pod/my-app-001-784777d896-krz69   1/1     Running   0          7m11s

NAME                 TYPE           CLUSTER-IP      EXTERNAL-IP                                                                 PORT(S)        AGE
service/kubernetes   ClusterIP      172.20.0.1      <none>                                                                      443/TCP        18m
service/my-app-001   LoadBalancer   172.20.190.68   a7bcd0c4212e8454383ad01a9fba667d-995660036.us-west-2.elb.amazonaws.com   80:30641/TCP   7m11s

NAME                         READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/my-app-001   2/2     2            2           7m11s

NAME                                    DESIRED   CURRENT   READY   AGE
replicaset.apps/my-app-001-784777d896   2         2         2       7m11s
```

a7bcd0c4212e8454383ad01a9fba667d-995660036.us-west-2.elb.amazona...

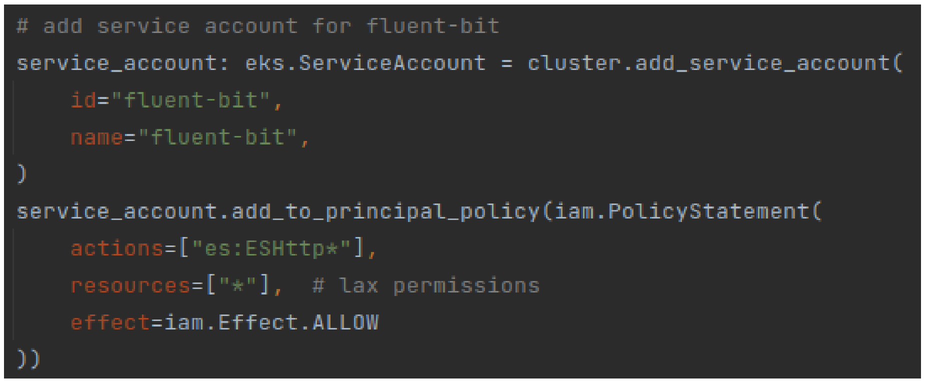
kubernetes

Hello world!

pod: my-app-001-784777d896-krz69
node: Linux (5.15.102)

Configuración de OpenSearch + Fluent Bit

- La definición del cluster se encuentra en ClusterLoggingStack.
- Se usó CDK para la creación de la infraestructura.
- Se usó autenticación por Cognito User Pools en vez de un Master password.
- Así mismo, se creó un serviceAccount para permitir que los pods puedan acceder al API de ES.
    –
- El mapping de los roles de ES/fluent-bit se encuentra en ClusterLogginRolesStack.
    – Importante. Incluir el rol creado en el paso anterior.



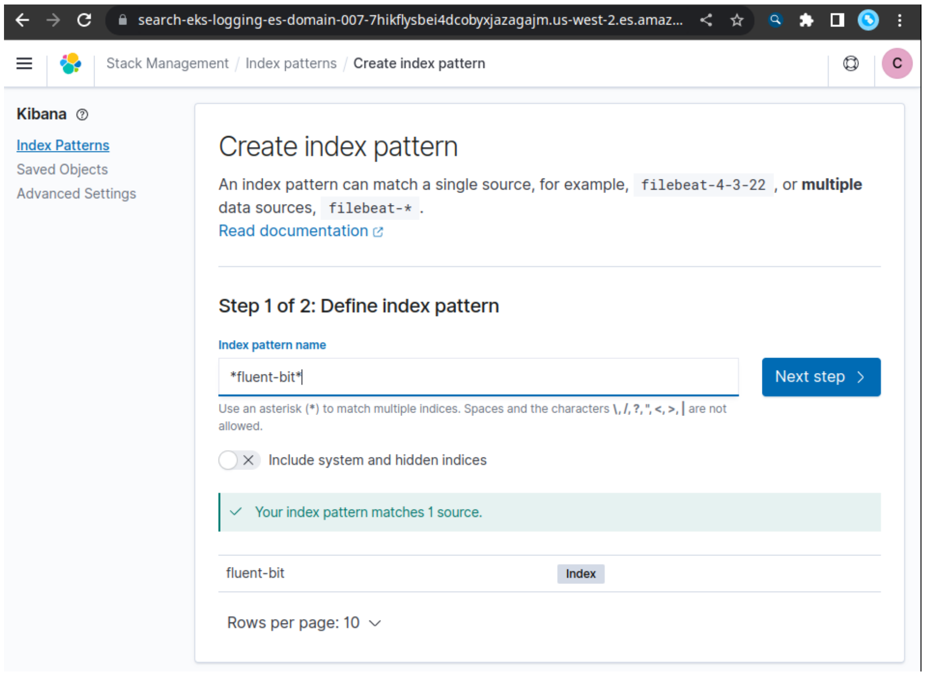
```
# add service account for fluent-bit
service_account: eks.ServiceAccount = cluster.add_service_account(
    id="fluent-bit",
    name="fluent-bit",
)
service_account.add_to_principal_policy(iam.PolicyStatement(
    actions=["es:ESHttp*"],
    resources=["*"],  # lax permissions
    effect=iam.Effect.ALLOW
))
```

Figure 3: img_23.png

```
# create fluent-bit
# before, edit the file an change the namespace, cluster endpoint and aws region
kubectl apply -f fluentbit.yaml

# there should be 3 pods for fluent-bit
kubectl get pods

# cleanup
kubectl delete -f fluentbit.yaml
```

Configuración de Prometheus + Grafana

```
# install helm
# helm 3.9+ breaks some packages, awscliv2 should solve this but in my case didn't
# curl -sSL https://raw.githubusercontent.com/helm/helm/master/scripts/get-helm-3 | bash
# installing helm 3.8.2
curl -L https://git.io/get_helm.sh | bash -s -- --version v3.8.2
helm version --short
helm repo add stable https://charts.helm.sh/stable
helm search repo stable

# add prometheus repo
helm repo add prometheus-community https://prometheus-community.github.io/helm-charts
# add grafana repo
helm repo add grafana https://grafana.github.io/helm-charts
# add support for volumes on EBS
#helm repo add aws-ebs-csi-driver https://kubernetes-sigs.github.io/aws-ebs-csi-driver
#helm repo update
#helm upgrade --install aws-ebs-csi-driver --namespace kube-system aws-ebs-csi-driver/aws-eb
# install eksctl - https://github.com/weaveworks/eksctl/releases/
```



Create index pattern

An index pattern can match a single source, for example, `filebeat-4-3-22` , or **multiple** data sources, `filebeat-*` .

Read documentation

Step 1 of 2: Define index pattern

Index pattern name

fluent-bit

Use an asterisk (*) to match multiple indices. Spaces and the characters \, /, ?, ", <, >, | are not allowed.

Include system and hidden indices

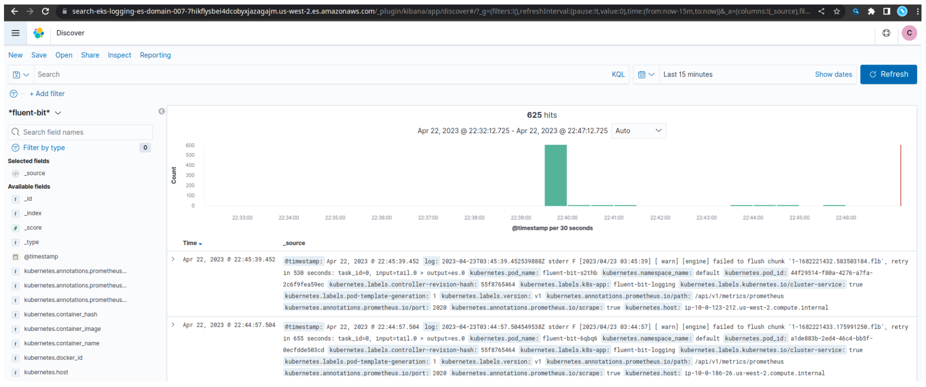
Your index pattern matches 1 source.

fluent-bit	Index

Rows per page: 10

search-eks-logging-es-domain-007-7hikflysbei4dcobyxjazagajm.us-west-2.es.amaz...
Stack Management / Index patterns / Create index pattern
Kibana
Index Patterns
Saved Objects
Advanced Settings
Next step

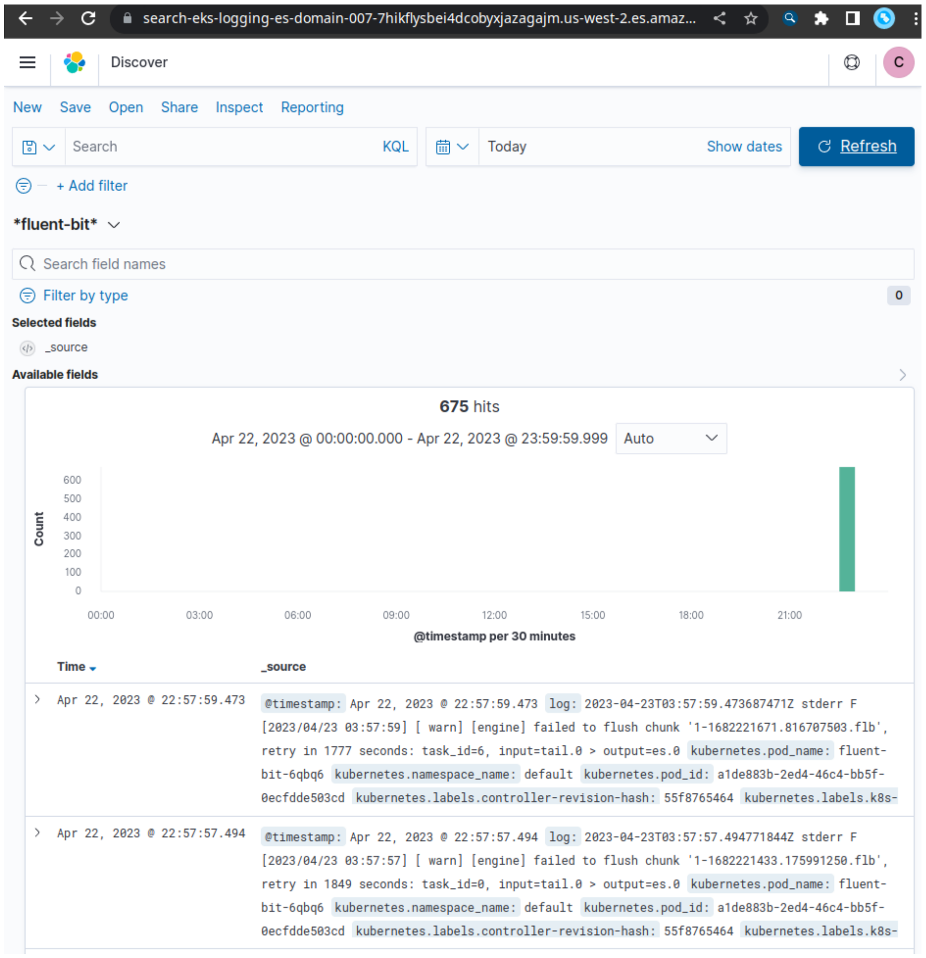
Figure 4: img_9.png



search-eks-logging-es-domain-007-7hikflysbei4dcobyxjazagajm.us-west-2.es.amazonaws.com/_plugin/kibana/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))&_a=(columns:!(_source),fil...
Discover
New Save Open Share Inspect Reporting
Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
fluent-bit
Search field names
Filter by type 0
Selected fields
_source
Available fields
_id
_index
_score
_type
@timestamp
kubernetes.annotations.prometheus...
kubernetes.annotations.prometheus...
kubernetes.annotations.prometheus...
kubernetes.container_hash
kubernetes.container_image
kubernetes.container_name
kubernetes.docker_id
kubernetes.host
625 hits
Apr 22, 2023 @ 22:32:12.725 - Apr 22, 2023 @ 22:47:12.725
Auto
Count
@timestamp per 30 seconds

```
Time      _source
> Apr 22, 2023 @ 22:45:39.452  @timestamp: Apr 22, 2023 @ 22:45:39.452 log: 2023-04-23T03:45:39.452539888Z stderr F [2023/04/23 03:45:39] [ warn] [engine] failed to flush chunk '1-1682221432.583503184.flb', retry in 530 seconds: task_id=0, input=tail.0 > output=es.0 kubernetes.pod_name: fluent-bit-s2thb kubernetes.namespace_name: default kubernetes.pod_id: 44f29514-f80a-4276-a7fa-2c6f9fea59ec kubernetes.labels.controller-revision-hash: 55f8765464 kubernetes.labels.k8s-app: fluent-bit-logging kubernetes.labels.kubernetes.io/cluster-service: true kubernetes.labels.pod-template-generation: 1 kubernetes.labels.version: v1 kubernetes.annotations.prometheus.io/path: /api/v1/metrics/prometheus kubernetes.annotations.prometheus.io/port: 2020 kubernetes.annotations.prometheus.io/scrape: true kubernetes.host: ip-10-0-123-212.us-west-2.compute.internal
> Apr 22, 2023 @ 22:44:57.504  @timestamp: Apr 22, 2023 @ 22:44:57.504 log: 2023-04-23T03:44:57.504549538Z stderr F [2023/04/23 03:44:57] [ warn] [engine] failed to flush chunk '1-1682221433.175991250.flb', retry in 655 seconds: task_id=0, input=tail.0 > output=es.0 kubernetes.pod_name: fluent-bit-6qbq6 kubernetes.namespace_name: default kubernetes.pod_id: a1de883b-2ed4-46c4-bb5f-0ecfdde503cd kubernetes.labels.controller-revision-hash: 55f8765464 kubernetes.labels.k8s-app: fluent-bit-logging kubernetes.labels.kubernetes.io/cluster-service: true kubernetes.labels.pod-template-generation: 1 kubernetes.labels.version: v1 kubernetes.annotations.prometheus.io/path: /api/v1/metrics/prometheus kubernetes.annotations.prometheus.io/port: 2020 kubernetes.annotations.prometheus.io/scrape: true kubernetes.host: ip-10-0-186-26.us-west-2.compute.internal
```

Figure 5: img_10.png



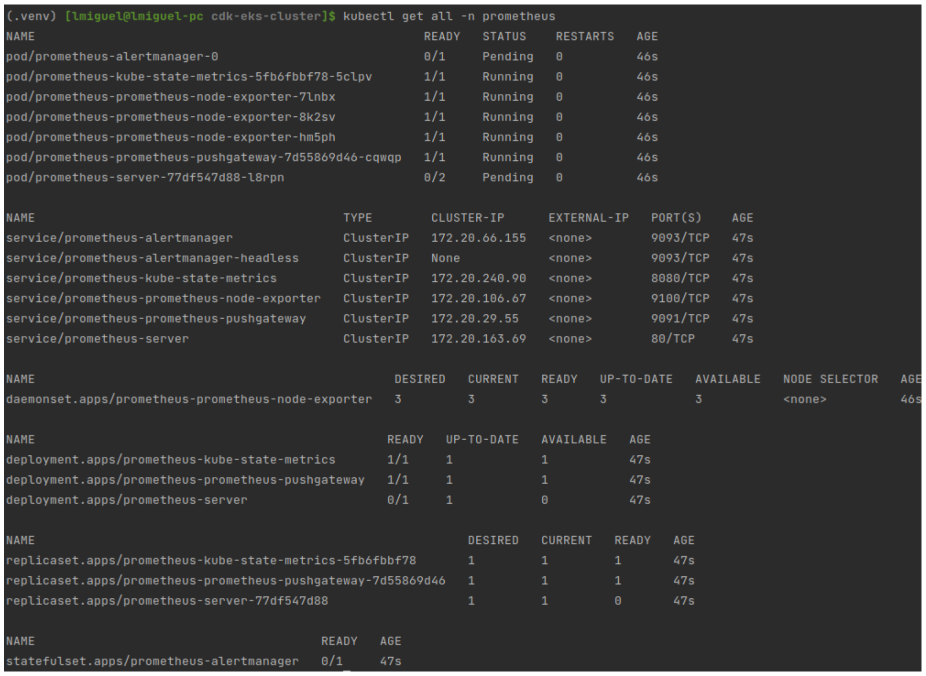
Time	_source
Apr 22, 2023 @ 22:57:59.473	@timestamp: Apr 22, 2023 @ 22:57:59.473 log: 2023-04-23T03:57:59.473687471Z stderr F [2023/04/23 03:57:59] [warn] [engine] failed to flush chunk '1-1682221671.816707503.flb', retry in 1777 seconds: task_id=6, input=tail.0 > output=es.0 kubernetes.pod_name: fluent-bit-6qbq6 kubernetes.namespace_name: default kubernetes.pod_id: a1de883b-2ed4-46c4-bb5f-0ecfdde503cd kubernetes.labels.controller-revision-hash: 55f8765464 kubernetes.labels.k8s-
Apr 22, 2023 @ 22:57:57.494	@timestamp: Apr 22, 2023 @ 22:57:57.494 log: 2023-04-23T03:57:57.494771844Z stderr F [2023/04/23 03:57:57] [warn] [engine] failed to flush chunk '1-1682221433.175991250.flb', retry in 1849 seconds: task_id=0, input=tail.0 > output=es.0 kubernetes.pod_name: fluent-bit-6qbq6 kubernetes.namespace_name: default kubernetes.pod_id: a1de883b-2ed4-46c4-bb5f-0ecfdde503cd kubernetes.labels.controller-revision-hash: 55f8765464 kubernetes.labels.k8s-

Figure 6: img_11.png

```
# test EBS CSI driver
# by creating a StorageClass, a PersistentVolumeClaim (PVC) and a pod
# all at once
#kubectl apply -f dynamic-provisioning/
#kubectl get pods
#kubectl delete -f dynamic-provisioning/
# or step by step
kubectl apply -f gp3-sc.yaml
kubectl apply -f pvc-csi.yaml
kubectl apply -f pod-csi.yaml
# pod status should be RUNNING after 60s
kubectl get pod
# pvc status should be BOUND
kubectl get pvc
# check more details of PVC
kubectl describe pvc
# cleanup
kubectl delete -f pod-csi.yaml
kubectl delete -f pvc-csi.yaml
kubectl delete -f gp3-sc.yaml

# install helm
kubectl create namespace prometheus
helm install prometheus prometheus-community/prometheus \
    --namespace prometheus \
    --set alertmanager.persistentVolume.storageClass="gp2" \
    --set server.persistentVolume.storageClass="gp2"

# check pods
kubectl get pods -n prometheus

# cleanup
helm uninstall prometheus --namespace prometheus
kubectl delete ns prometheus
```

Configuración manual

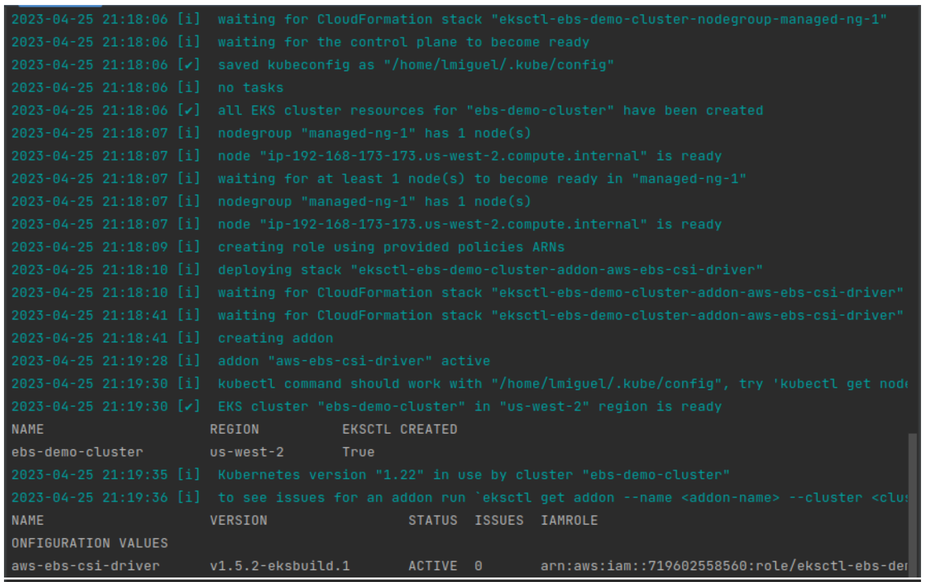
```
eksctl create cluster -f config.yaml
kubectl config current-context
kubectl apply -f gp3-sc.yaml
kubectl apply -f pvc-csi.yaml
# check resources
eksctl get cluster
eksctl get addon --name aws-ebs-csi-driver --cluster ebs-demo-cluster
kubectl get sc
```



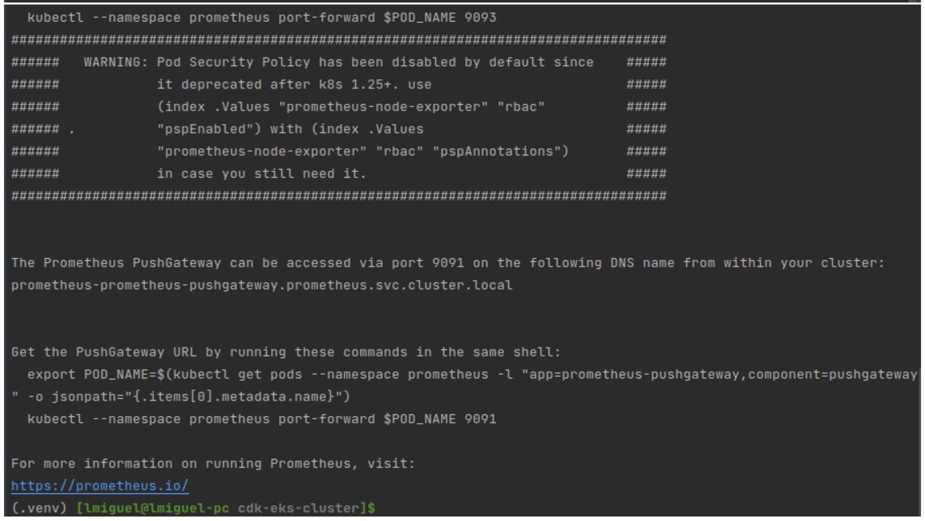
```
(.venv) [lmiguel@lmiguel-pc cdk-eks-cluster]$ kubectl get all -n prometheus
NAME                                                     READY   STATUS    RESTARTS   AGE
pod/prometheus-alertmanager-0                            0/1     Pending   0          46s
pod/prometheus-kube-state-metrics-5fb6fbbf78-5clpv       1/1     Running   0          46s
pod/prometheus-prometheus-node-exporter-7lnbx            1/1     Running   0          46s
pod/prometheus-prometheus-node-exporter-8k2sv            1/1     Running   0          46s
pod/prometheus-prometheus-node-exporter-hm5ph            1/1     Running   0          46s
pod/prometheus-prometheus-pushgateway-7d55869d46-cqwqp   1/1     Running   0          46s
pod/prometheus-server-77df547d88-l8rpn                   0/2     Pending   0          46s

NAME                                          TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)    AGE
service/prometheus-alertmanager               ClusterIP   172.20.66.155   <none>        9093/TCP   47s
service/prometheus-alertmanager-headless      ClusterIP   None            <none>        9093/TCP   47s
service/prometheus-kube-state-metrics         ClusterIP   172.20.240.90   <none>        8080/TCP   47s
service/prometheus-prometheus-node-exporter   ClusterIP   172.20.106.67   <none>        9100/TCP   47s
service/prometheus-prometheus-pushgateway     ClusterIP   172.20.29.55    <none>        9091/TCP   47s
service/prometheus-server                     ClusterIP   172.20.163.69   <none>        80/TCP     47s

NAME                                                 DESIRED   CURRENT   READY   UP-TO-DATE   AVAILABLE   NODE SELECTOR   AGE
daemonset.apps/prometheus-prometheus-node-exporter   3         3         3       3            3           <none>          46s

NAME                                                READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/prometheus-kube-state-metrics       1/1     1            1           47s
deployment.apps/prometheus-prometheus-pushgateway   1/1     1            1           47s
deployment.apps/prometheus-server                   0/1     1            0           47s

NAME                                                           DESIRED   CURRENT   READY   AGE
replicaset.apps/prometheus-kube-state-metrics-5fb6fbbf78       1         1         1       47s
replicaset.apps/prometheus-prometheus-pushgateway-7d55869d46   1         1         1       47s
replicaset.apps/prometheus-server-77df547d88                   1         1         0       47s

NAME                                      READY   AGE
statefulset.apps/prometheus-alertmanager   0/1     47s
```

Figure 7: img_13.png

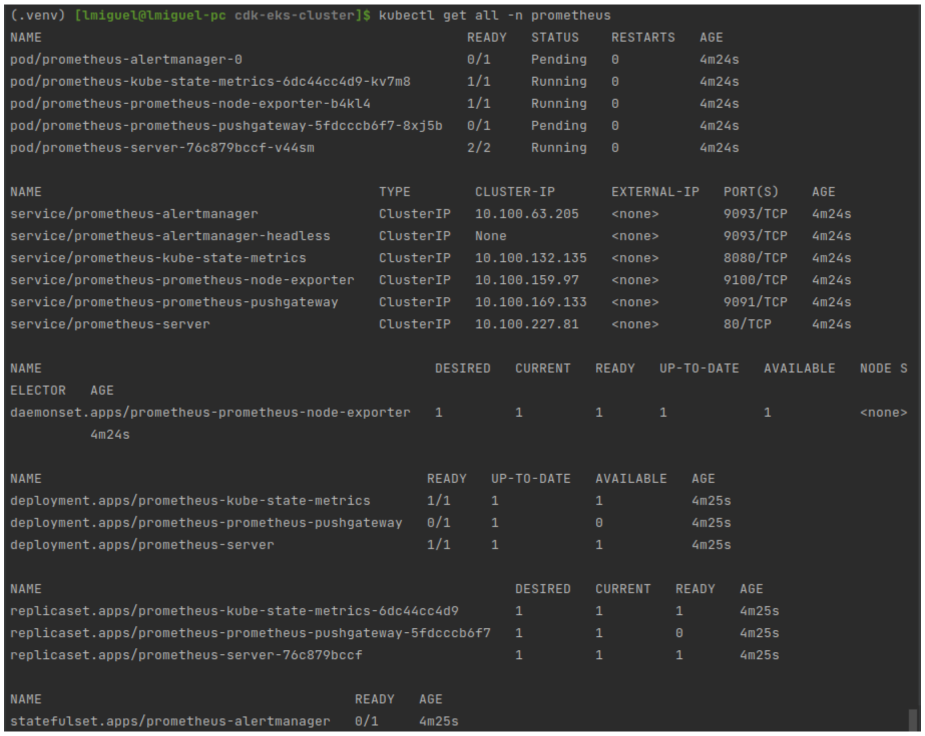
```
# install
helm install prometheus prometheus-community/prometheus \
    --namespace prometheus \
    --set alertmanager.persistentVolume.storageClass="gp3" \
    --set server.persistentVolume.storageClass="gp3"
# check prometheus
kubectl get all -n prometheus

# cleanup
helm uninstall prometheus --namespace prometheus
kubectl delete -f pvc-csi.yaml
kubectl delete -f gp3-sc.yaml
eksctl delete addon --name aws-ebs-csi-driver --cluster ebs-demo-cluster
```



```
2023-04-25 21:18:06 [i]  waiting for CloudFormation stack "eksctl-ebs-demo-cluster-nodegroup-managed-ng-1"
2023-04-25 21:18:06 [i]  waiting for the control plane to become ready
2023-04-25 21:18:06 [✔]  saved kubeconfig as "/home/lmiguel/.kube/config"
2023-04-25 21:18:06 [i]  no tasks
2023-04-25 21:18:06 [✔]  all EKS cluster resources for "ebs-demo-cluster" have been created
2023-04-25 21:18:07 [i]  nodegroup "managed-ng-1" has 1 node(s)
2023-04-25 21:18:07 [i]  node "ip-192-168-173-173.us-west-2.compute.internal" is ready
2023-04-25 21:18:07 [i]  waiting for at least 1 node(s) to become ready in "managed-ng-1"
2023-04-25 21:18:07 [i]  nodegroup "managed-ng-1" has 1 node(s)
2023-04-25 21:18:07 [i]  node "ip-192-168-173-173.us-west-2.compute.internal" is ready
2023-04-25 21:18:09 [i]  creating role using provided policies ARNs
2023-04-25 21:18:10 [i]  deploying stack "eksctl-ebs-demo-cluster-addon-aws-ebs-csi-driver"
2023-04-25 21:18:10 [i]  waiting for CloudFormation stack "eksctl-ebs-demo-cluster-addon-aws-ebs-csi-driver"
2023-04-25 21:18:41 [i]  waiting for CloudFormation stack "eksctl-ebs-demo-cluster-addon-aws-ebs-csi-driver"
2023-04-25 21:18:41 [i]  creating addon
2023-04-25 21:19:28 [i]  addon "aws-ebs-csi-driver" active
2023-04-25 21:19:30 [i]  kubectl command should work with "/home/lmiguel/.kube/config", try 'kubectl get node
2023-04-25 21:19:30 [✔]  EKS cluster "ebs-demo-cluster" in "us-west-2" region is ready
NAME                    REGION          EKSCTL CREATED
ebs-demo-cluster        us-west-2       True
2023-04-25 21:19:35 [i]  Kubernetes version "1.22" in use by cluster "ebs-demo-cluster"
2023-04-25 21:19:36 [i]  to see issues for an addon run `eksctl get addon --name <addon-name> --cluster <clu
NAME                    VERSION                 STATUS  ISSUES  IAMROLE
ONFIGURATION VALUES
aws-ebs-csi-driver      v1.5.2-eksbuild.1       ACTIVE  0       arn:aws:iam::719602558560:role/eksctl-ebs-de
```



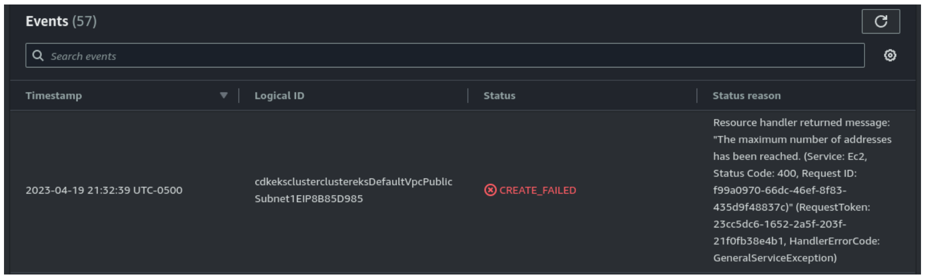
```
  kubectl --namespace prometheus port-forward $POD_NAME 9093
#################################################################################
######   WARNING: Pod Security Policy has been disabled by default since    #####
######            it deprecated after k8s 1.25+. use                        #####
######            (index .Values "prometheus-node-exporter" "rbac"          #####
###### .          "pspEnabled") with (index .Values                         #####
######            "prometheus-node-exporter" "rbac" "pspAnnotations")       #####
######            in case you still need it.                                #####
#################################################################################



The Prometheus PushGateway can be accessed via port 9091 on the following DNS name from within your cluster:
prometheus-prometheus-pushgateway.prometheus.svc.cluster.local


Get the PushGateway URL by running these commands in the same shell:
  export POD_NAME=$(kubectl get pods --namespace prometheus -l "app=prometheus-pushgateway,component=pushgateway
" -o jsonpath="{.items[0].metadata.name}")
  kubectl --namespace prometheus port-forward $POD_NAME 9091

For more information on running Prometheus, visit:
https://prometheus.io/
(.venv) [lmiguel@lmiguel-pc cdk-eks-cluster]$
```



```
(.venv) [lmiguel@lmiguel-pc cdk-eks-cluster]$ kubectl get all -n prometheus
NAME                                                    READY   STATUS    RESTARTS   AGE
pod/prometheus-alertmanager-0                           0/1     Pending   0          4m24s
pod/prometheus-kube-state-metrics-6dc44cc4d9-kv7m8      1/1     Running   0          4m24s
pod/prometheus-prometheus-node-exporter-b4kl4           1/1     Running   0          4m24s
pod/prometheus-prometheus-pushgateway-5fdcccb6f7-8xj5b  0/1     Pending   0          4m24s
pod/prometheus-server-76c879bccf-v44sm                  2/2     Running   0          4m24s

NAME                                          TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)    AGE
service/prometheus-alertmanager               ClusterIP   10.100.63.205    <none>        9093/TCP   4m24s
service/prometheus-alertmanager-headless      ClusterIP   None             <none>        9093/TCP   4m24s
service/prometheus-kube-state-metrics         ClusterIP   10.100.132.135   <none>        8080/TCP   4m24s
service/prometheus-prometheus-node-exporter   ClusterIP   10.100.159.97    <none>        9100/TCP   4m24s
service/prometheus-prometheus-pushgateway     ClusterIP   10.100.169.133   <none>        9091/TCP   4m24s
service/prometheus-server                     ClusterIP   10.100.227.81    <none>        80/TCP     4m24s

NAME                                                 DESIRED   CURRENT   READY   UP-TO-DATE   AVAILABLE   NODE S
ELECTOR   AGE
daemonset.apps/prometheus-prometheus-node-exporter   1         1         1       1            1           <none>
          4m24s

NAME                                                READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/prometheus-kube-state-metrics       1/1     1            1           4m25s
deployment.apps/prometheus-prometheus-pushgateway   0/1     1            0           4m25s
deployment.apps/prometheus-server                   1/1     1            1           4m25s

NAME                                                           DESIRED   CURRENT   READY   AGE
replicaset.apps/prometheus-kube-state-metrics-6dc44cc4d9       1         1         1       4m25s
replicaset.apps/prometheus-prometheus-pushgateway-5fdcccb6f7   1         1         0       4m25s
replicaset.apps/prometheus-server-76c879bccf                   1         1         1       4m25s

NAME                                      READY   AGE
statefulset.apps/prometheus-alertmanager   0/1     4m25s
```

Problemas

- El despliegue falló porque se llegó al límite de 5 IPs por región.
  - Se solicitó el incremento de número de IPs.



Events (57)

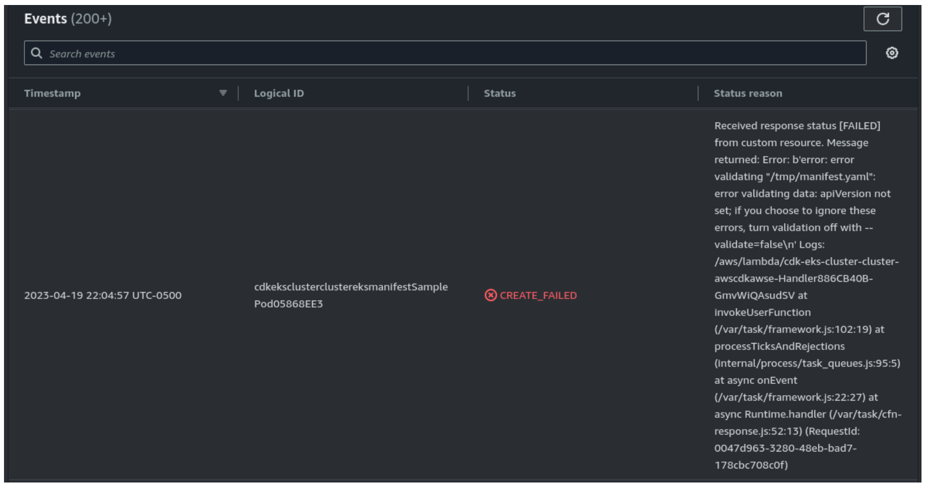
Search events

Timestamp	Logical ID	Status	Status reason
2023-04-19 21:32:39 UTC-0500	cdkeksclusterclustereksDefaultVpcPublicSubnet1EIP8B85D985	⊗ CREATE_FAILED	Resource handler returned message: "The maximum number of addresses has been reached. (Service: Ec2, Status Code: 400, Request ID: f99a0970-66dc-46ef-8f83-435d9f48837c)" (RequestToken: 23cc5dc6-1652-2a5f-203f-21f0fb38e4b1, HandlerErrorCode: GeneralServiceException)

Figure 8: img.png

  -

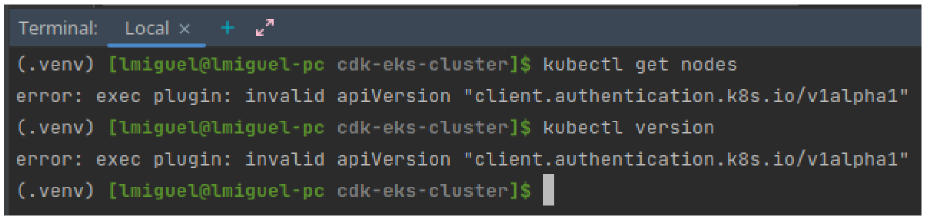
- El despliegue falló por un error en el manifest.
  - Se eliminó el manifest para culminar el despliegue.
  -
- No se pudo usar kubectl desde local.
  - Se eliminó la versión de kubectl 1.26.3-1.



Timestamp	Logical ID	Status	Status reason
2023-04-19 22:04:57 UTC-0500	cdkeksclusterclustereksmanifestSamplePod05868EE3	CREATE_FAILED	Received response status [FAILED] from custom resource. Message returned: Error: b'error: error validating "/tmp/manifest.yaml": error validating data: apiVersion not set; if you choose to ignore these errors, turn validation off with --validate=false\n' Logs: /aws/lambda/cdk-eks-cluster-cluster-awscdkawse-Handler886CB40B-GmvWiQAsudSV at invokeUserFunction (/var/task/framework.js:102:19) at processTicksAndRejections (internal/process/task_queues.js:95:5) at async onEvent (/var/task/framework.js:22:27) at async Runtime.handler (/var/task/cfn-response.js:52:13) (RequestId: 0047d963-3280-48eb-bad7-178cbc708c0f)

Figure 9: img_1.png

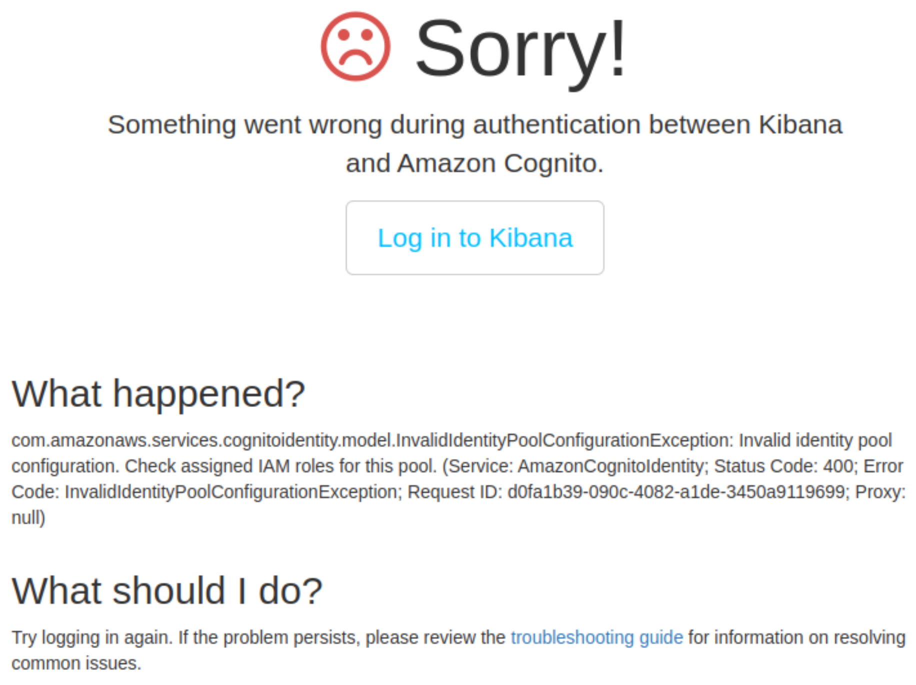
  - Se recreó la carpeta ~/.kube/
  - Se probó con la versión 1.27, 1.26, 1.25, 1.24, finalmente la versión 1.23.17



```
(.venv) [lmiguel@lmiguel-pc cdk-eks-cluster]$ kubectl get nodes
error: exec plugin: invalid apiVersion "client.authentication.k8s.io/v1alpha1"
(.venv) [lmiguel@lmiguel-pc cdk-eks-cluster]$ kubectl version
error: exec plugin: invalid apiVersion "client.authentication.k8s.io/v1alpha1"
(.venv) [lmiguel@lmiguel-pc cdk-eks-cluster]$
```

Figure 10: img_2.png

  -
- No se puede acceder a Kibana con el usuario de Cognito.
  - Posiblemente un error de integración entre UserPool y el IdentityPool. Se añadieron roles y redesplegó.
  -
- El despliegue de un manifiesto (service + deployment) falla.
  - Errores de versión de manifiesto. Se corrigió y cambiaron algunos nombres.
  -
- Problemas al eliminar el Cluster EKS, al parecer algunas VPCs, IGs y subnets no pueden eliminarse.
  - Un balanceador de carga creado con kubectl (manualmente) no podía ser eliminado. Se identificó el balanceador y tuvo que ser eliminado manualmente, luego el stack pudo ser eliminado.



Sorry!

Something went wrong during authentication between Kibana and Amazon Cognito.

Log in to Kibana

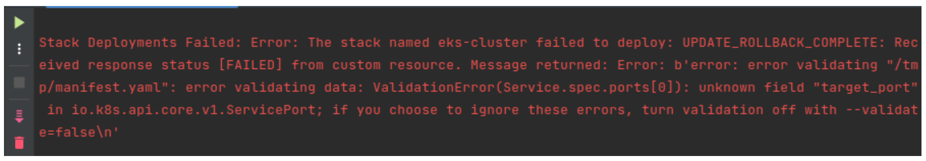
What happened?

com.amazonaws.services.cognitoidentity.model.InvalidIdentityPoolConfigurationException: Invalid identity pool configuration. Check assigned IAM roles for this pool. (Service: AmazonCognitoIdentity; Status Code: 400; Error Code: InvalidIdentityPoolConfigurationException; Request ID: d0fa1b39-090c-4082-a1de-3450a9119699; Proxy: null)

What should I do?

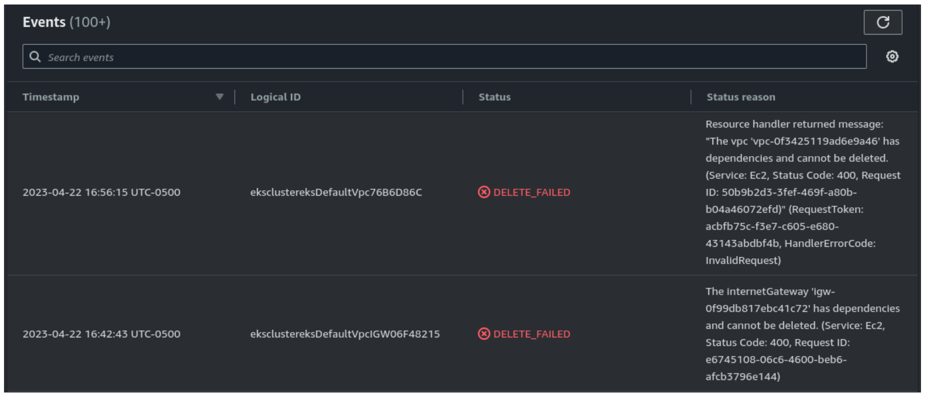
Try logging in again. If the problem persists, please review the troubleshooting guide for information on resolving common issues.

Figure 11: img_3.png



```
Stack Deployments Failed: Error: The stack named eks-cluster failed to deploy: UPDATE_ROLLBACK_COMPLETE: Rec
eived response status [FAILED] from custom resource. Message returned: Error: b'error: error validating "/tm
p/manifest.yaml": error validating data: ValidationError(Service.spec.ports[0]): unknown field "target_port"
 in io.k8s.api.core.v1.ServicePort; if you choose to ignore these errors, turn validation off with --validat
e=false\n'
```

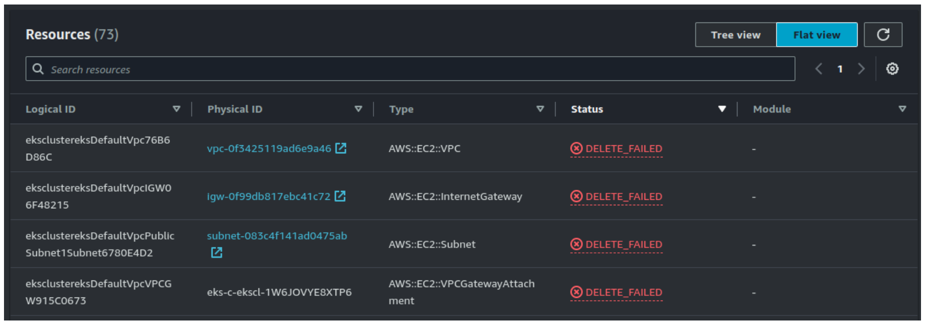
Figure 12: img_4.png



Timestamp	Logical ID	Status	Status reason
2023-04-22 16:56:15 UTC-0500	eksclustereksDefaultVpc76B6D86C	DELETE_FAILED	Resource handler returned message: "The vpc 'vpc-0f3425119ad6e9a46' has dependencies and cannot be deleted. (Service: Ec2, Status Code: 400, Request ID: 50b9b2d3-3fef-469f-a80b-b04a46072efd)" (RequestToken: acbfb75c-f3e7-c605-e680-43143abdbf4b, HandlerErrorCode: InvalidRequest)
2023-04-22 16:42:43 UTC-0500	eksclustereksDefaultVpcIGW06F48215	DELETE_FAILED	The internetGateway 'igw-0f99db817ebc41c72' has dependencies and cannot be deleted. (Service: Ec2, Status Code: 400, Request ID: e6745108-06c6-4600-beb6-afcb3796e144)

Figure 13: img_8.png

–

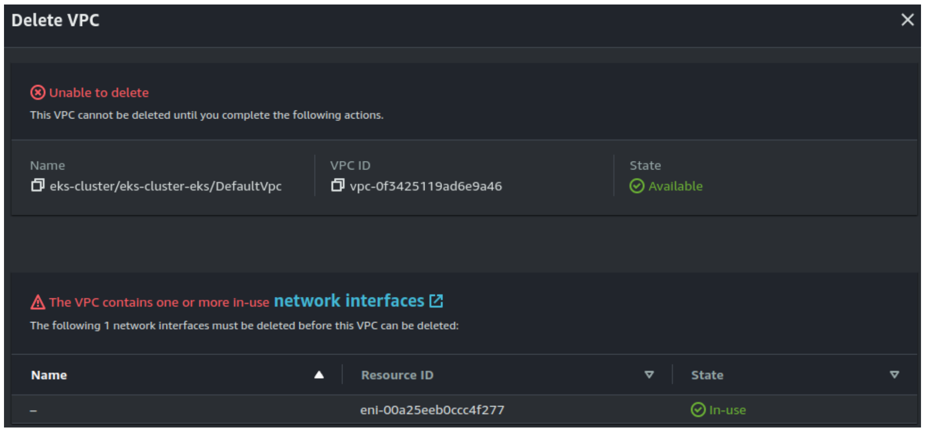


Logical ID	Physical ID	Type	Status	Module
eksclustereksDefaultVpc76B6D86C	vpc-0f3425119ad6e9a46	AWS::EC2::VPC	DELETE_FAILED	-
eksclustereksDefaultVpcIGW06F48215	igw-0f99db817ebc41c72	AWS::EC2::InternetGateway	DELETE_FAILED	-
eksclustereksDefaultVpcPublicSubnet1Subnet6780E4D2	subnet-083c4f141ad0475ab	AWS::EC2::Subnet	DELETE_FAILED	-
eksclustereksDefaultVpcVPCGW915C0673	eks-c-ekscl-1W6JOVYE8XTP6	AWS::EC2::VPCGatewayAttachment	DELETE_FAILED	-

Figure 14: img_7.png

  –
  –
  –

- Error al desplegar Prometheus: INSTALLATION FAILED: Kubernetes cluster unreachable: exec plugin: invalid apiVersion "client.authentication.k8s.io/v1alpha1"
  - Al parecer es un problema de Helm 3.9 + AWS cli v1.
  - Instalando AWS cli v2 no funcionó (https://github.com/helm/helm/issues/10975#issuecomment-1132139799)
  - Tuve que revertir y usar la v3.8.2 de Helm.
  –
- El pod de helm se queda en *Pending*.
  –
  - No hay logs en `kubectl logs -n prometheus pod/prometheus-server-77df547d88-l8rpn -c prometheus-server`.
  - `kubectl describe -n prometheus pods/prometheus-server-77df547d88-bxtdc`



Delete VPC

Unable to delete

This VPC cannot be deleted until you complete the following actions.

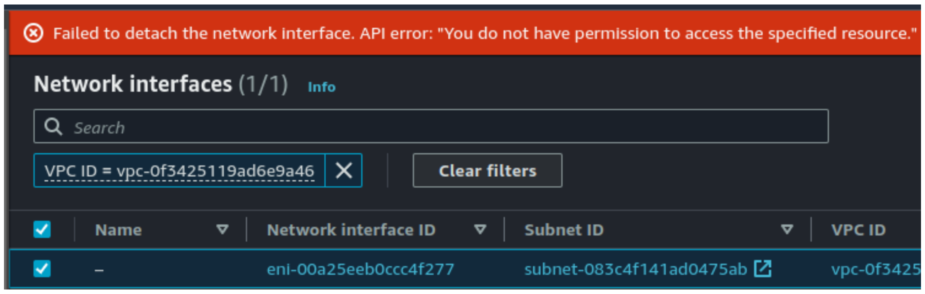
Name	VPC ID	State
eks-cluster/eks-cluster-eks/DefaultVpc	vpc-0f3425119ad6e9a46	Available

The VPC contains one or more in-use network interfaces

The following 1 network interfaces must be deleted before this VPC can be deleted:

Name	Resource ID	State
–	eni-00a25eeb0ccc4f277	In-use

Figure 15: img_6.png



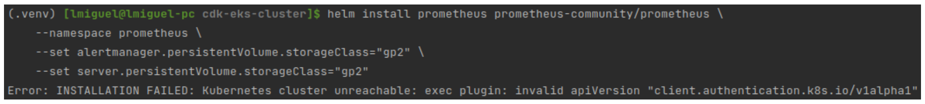
Failed to detach the network interface. API error: "You do not have permission to access the specified resource."

Network interfaces (1/1) Info

VPC ID = vpc-0f3425119ad6e9a46

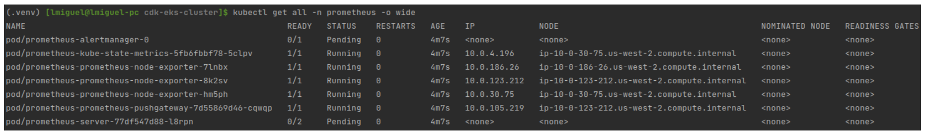
Name	Network interface ID	Subnet ID	VPC ID
–	eni-00a25eeb0ccc4f277	subnet-083c4f141ad0475ab	vpc-0f3425

Figure 16: img_5.png



```
(.venv) [lmiguel@lmiguel-pc cdk-eks-cluster]$ helm install prometheus prometheus-community/prometheus \
    --namespace prometheus \
    --set alertmanager.persistentVolume.storageClass="gp2" \
    --set server.persistentVolume.storageClass="gp2"
Error: INSTALLATION FAILED: Kubernetes cluster unreachable: exec plugin: invalid apiVersion "client.authentication.k8s.io/v1alpha1"
```

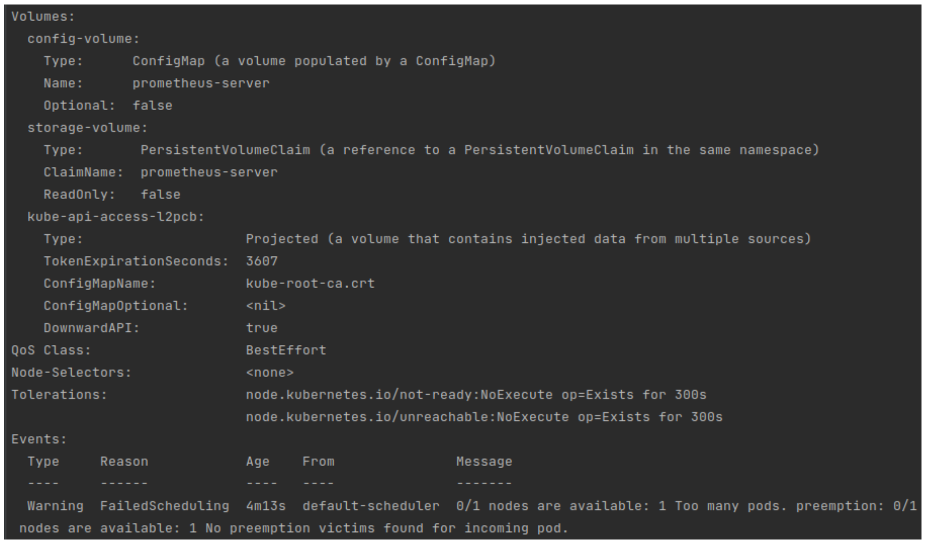
Figure 17: img_12.png



```
(.venv) [lmiguel@lmiguel-pc cdk-eks-cluster]$ kubectl get all -n prometheus -o wide
NAME                                                  READY   STATUS    RESTARTS   AGE    IP             NODE                                          NOMINATED NODE   READINESS GATES
pod/prometheus-alertmanager-0                         0/1     Pending   0          4m7s   <none>         <none>                                        <none>           <none>
pod/prometheus-kube-state-metrics-5fb6fbbf78-5clpv    1/1     Running   0          4m7s   10.0.4.196     ip-10-0-30-75.us-west-2.compute.internal      <none>           <none>
pod/prometheus-prometheus-node-exporter-7lnbx         1/1     Running   0          4m7s   10.0.186.26    ip-10-0-186-26.us-west-2.compute.internal     <none>           <none>
pod/prometheus-prometheus-node-exporter-8k2sv         1/1     Running   0          4m7s   10.0.123.212   ip-10-0-123-212.us-west-2.compute.internal    <none>           <none>
pod/prometheus-prometheus-node-exporter-hm5ph         1/1     Running   0          4m7s   10.0.30.75     ip-10-0-30-75.us-west-2.compute.internal      <none>           <none>
pod/prometheus-prometheus-pushgateway-7d55869d46-cqwqp   1/1  Running   0          4m7s   10.0.105.219   ip-10-0-123-212.us-west-2.compute.internal    <none>           <none>
pod/prometheus-server-77df547d88-l8rpn                0/2     Pending   0          4m7s   <none>         <none>                                        <none>           <none>
```

Figure 18: img_14.png

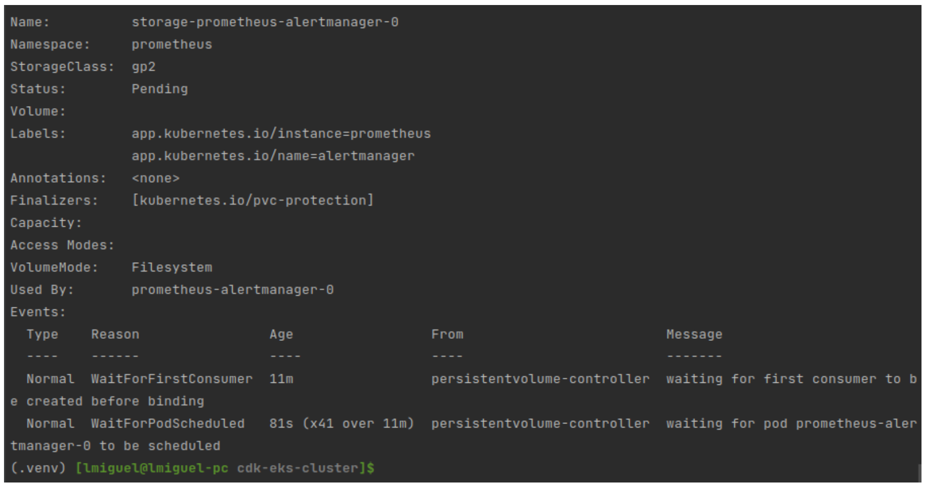
no ayuda:



```
Volumes:
  config-volume:
    Type:      ConfigMap (a volume populated by a ConfigMap)
    Name:      prometheus-server
    Optional:  false
  storage-volume:
    Type:       PersistentVolumeClaim (a reference to a PersistentVolumeClaim in the same namespace)
    ClaimName:  prometheus-server
    ReadOnly:   false
  kube-api-access-l2pcb:
    Type:                    Projected (a volume that contains injected data from multiple sources)
    TokenExpirationSeconds:  3607
    ConfigMapName:           kube-root-ca.crt
    ConfigMapOptional:       <nil>
    DownwardAPI:             true
QoS Class:                   BestEffort
Node-Selectors:              <none>
Tolerations:                 node.kubernetes.io/not-ready:NoExecute op=Exists for 300s
                             node.kubernetes.io/unreachable:NoExecute op=Exists for 300s
Events:
  Type     Reason            Age    From               Message
  ----     ------            ----   ----               -------
  Warning  FailedScheduling  4m13s  default-scheduler  0/1 nodes are available: 1 Too many pods. preemption: 0/1
 nodes are available: 1 No preemption victims found for incoming pod.
```

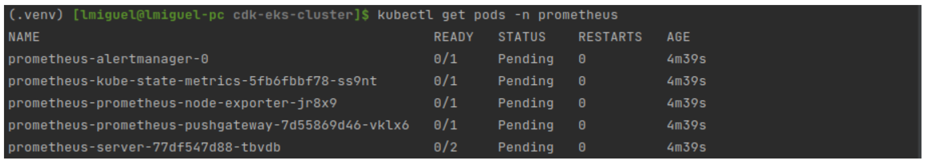
Figure 19: img_17.png

  *
- `kubectl describe pvc -n prometheus` parece un problema de volúmenes. Al parecer no puede crear algun volumen.
  *
- Se instaló aws-ebs-csi-driver, ahora todos los pods en *Pending*.
  *
- Se siguió el siguiente post para habilitar el almacenamiento persistente en EKS
- Se encontró un problema al crear el ServiceAccount y realizar el despliegue. Solucionado al desinstalar `aws-ebs-csi-driver`, instalado previamente.
  *
- Se intentó la configuración del despliegue usando el add-on de EKS para el driver EBS CSI. Pero el pod de prueba de AWS se queda en *Pending*.
  *
- Se intentó la instalación del driver EBS CSI usando helm
  *
- Se volvió a reintentar, esta vez siquiendo este blog de AWS para usar el EBS CSI driver como un add-on de EKS
  * Repitiendo los pasos se encontró que el Service Account fue creado en el namespace `default` cuando debió ser creado en el namespace `kube-system`.
  * Así mismo se encontró algunas otras herramientas para diagnos-



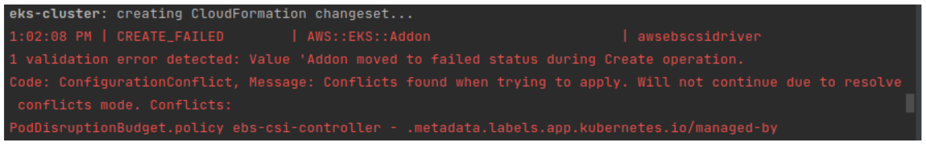
```
Name:          storage-prometheus-alertmanager-0
Namespace:     prometheus
StorageClass:  gp2
Status:        Pending
Volume:
Labels:        app.kubernetes.io/instance=prometheus
               app.kubernetes.io/name=alertmanager
Annotations:   <none>
Finalizers:    [kubernetes.io/pvc-protection]
Capacity:
Access Modes:
VolumeMode:    Filesystem
Used By:       prometheus-alertmanager-0
Events:
  Type    Reason                Age                 From                         Message
  ----    ------                ----                ----                         -------
  Normal  WaitForFirstConsumer  11m                 persistentvolume-controller  waiting for first consumer to b
e created before binding
  Normal  WaitForPodScheduled   81s (x41 over 11m)  persistentvolume-controller  waiting for pod prometheus-aler
tmanager-0 to be scheduled
(.venv) [lmiguel@lmiguel-pc cdk-eks-cluster]$
```

Figure 20: img_18.png



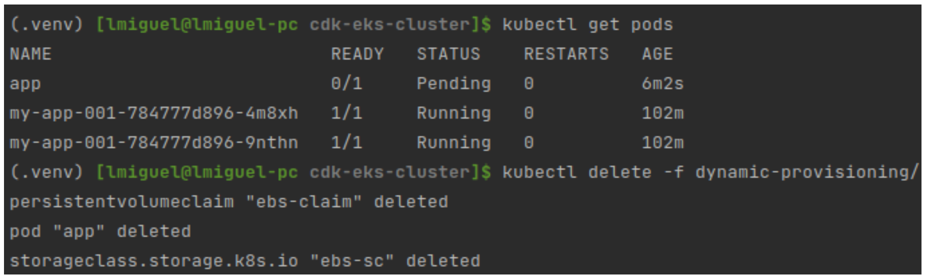
```
(.venv) [lmiguel@lmiguel-pc cdk-eks-cluster]$ kubectl get pods -n prometheus
NAME                                                 READY   STATUS    RESTARTS   AGE
prometheus-alertmanager-0                            0/1     Pending   0          4m39s
prometheus-kube-state-metrics-5fb6fbbf78-ss9nt       0/1     Pending   0          4m39s
prometheus-prometheus-node-exporter-jr8x9            0/1     Pending   0          4m39s
prometheus-prometheus-pushgateway-7d55869d46-vklx6   0/1     Pending   0          4m39s
prometheus-server-77df547d88-tbvdb                   0/2     Pending   0          4m39s
```

Figure 21: img_19.png



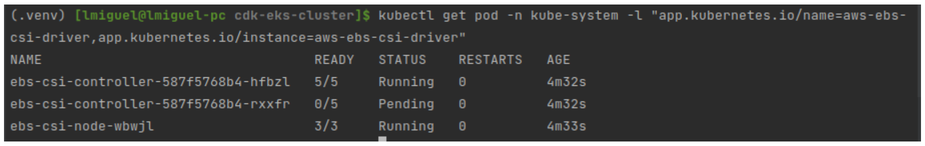
```
eks-cluster: creating CloudFormation changeset...
1:02:08 PM | CREATE_FAILED        | AWS::EKS::Addon                        | awsebscsidriver
1 validation error detected: Value 'Addon moved to failed status during Create operation.
Code: ConfigurationConflict, Message: Conflicts found when trying to apply. Will not continue due to resolve
 conflicts mode. Conflicts:
PodDisruptionBudget.policy ebs-csi-controller - .metadata.labels.app.kubernetes.io/managed-by
```

Figure 22: img_20.png



```
(.venv) [lmiguel@lmiguel-pc cdk-eks-cluster]$ kubectl get pods
NAME                          READY   STATUS    RESTARTS   AGE
app                           0/1     Pending   0          6m2s
my-app-001-784777d896-4m8xh   1/1     Running   0          102m
my-app-001-784777d896-9nthn   1/1     Running   0          102m
(.venv) [lmiguel@lmiguel-pc cdk-eks-cluster]$ kubectl delete -f dynamic-provisioning/
persistentvolumeclaim "ebs-claim" deleted
pod "app" deleted
storageclass.storage.k8s.io "ebs-sc" deleted
```

Figure 23: img_21.png



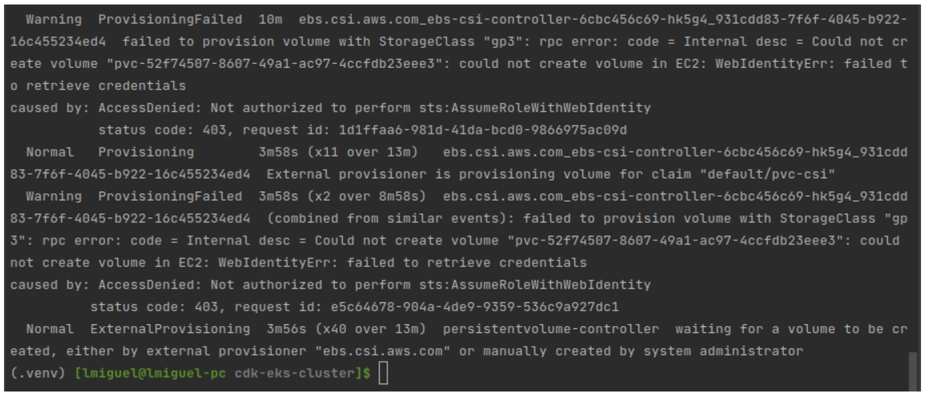
```
(.venv) [lmiguel@lmiguel-pc cdk-eks-cluster]$ kubectl get pod -n kube-system -l "app.kubernetes.io/name=aws-ebs-
csi-driver,app.kubernetes.io/instance=aws-ebs-csi-driver"
NAME                               READY   STATUS    RESTARTS   AGE
ebs-csi-controller-587f5768b4-hfbzl   5/5     Running   0          4m32s
ebs-csi-controller-587f5768b4-rxxfr   0/5     Pending   0          4m32s
ebs-csi-node-wbwjl                 3/3     Running   0          4m33s
```

Figure 24: img_22.png

ticar los componentes del add-on:

- `kubectl get deploy,ds -l=app.kubernetes.io/name=aws-ebs-csi-driver -n kube-system`
- `kubectl get po -n kube-system -l 'app in (ebs-csi-controller,ebs-csi-node)'`
- `kubectl get -n kube-system pod/ebs-csi-controller-CHANGE_ME -o jsonpath='{.spec.containers[*].name}'`

∗ El problema persiste, pero ahora al hacer describe del PersistentVolumeClaim (PVC) obtenemos varios errores.



```
  Warning  ProvisioningFailed  10m  ebs.csi.aws.com_ebs-csi-controller-6cbc456c69-hk5g4_931cdd83-7f6f-4045-b922-
16c455234ed4  failed to provision volume with StorageClass "gp3": rpc error: code = Internal desc = Could not cr
eate volume "pvc-52f74507-8607-49a1-ac97-4ccfdb23eee3": could not create volume in EC2: WebIdentityErr: failed t
o retrieve credentials
caused by: AccessDenied: Not authorized to perform sts:AssumeRoleWithWebIdentity
           status code: 403, request id: 1d1ffaa6-981d-41da-bcd0-9866975ac09d
  Normal   Provisioning        3m58s (x11 over 13m)   ebs.csi.aws.com_ebs-csi-controller-6cbc456c69-hk5g4_931cdd
83-7f6f-4045-b922-16c455234ed4  External provisioner is provisioning volume for claim "default/pvc-csi"
  Warning  ProvisioningFailed  3m58s (x2 over 8m58s)  ebs.csi.aws.com_ebs-csi-controller-6cbc456c69-hk5g4_931cdd
83-7f6f-4045-b922-16c455234ed4  (combined from similar events): failed to provision volume with StorageClass "gp
3": rpc error: code = Internal desc = Could not create volume "pvc-52f74507-8607-49a1-ac97-4ccfdb23eee3": could
not create volume in EC2: WebIdentityErr: failed to retrieve credentials
caused by: AccessDenied: Not authorized to perform sts:AssumeRoleWithWebIdentity
          status code: 403, request id: e5c64678-904a-4de9-9359-536c9a927dc1
  Normal  ExternalProvisioning  3m56s (x40 over 13m)  persistentvolume-controller  waiting for a volume to be cr
eated, either by external provisioner "ebs.csi.aws.com" or manually created by system administrator
(.venv) [lmiguel@lmiguel-pc cdk-eks-cluster]$ 
```

Figure 25: img_24.png

·

∗ Redesplegando el stack, para acelerar las cosas se puede usar otra región para el despliegue, y no esperar a que el cluster se elimine por completo.

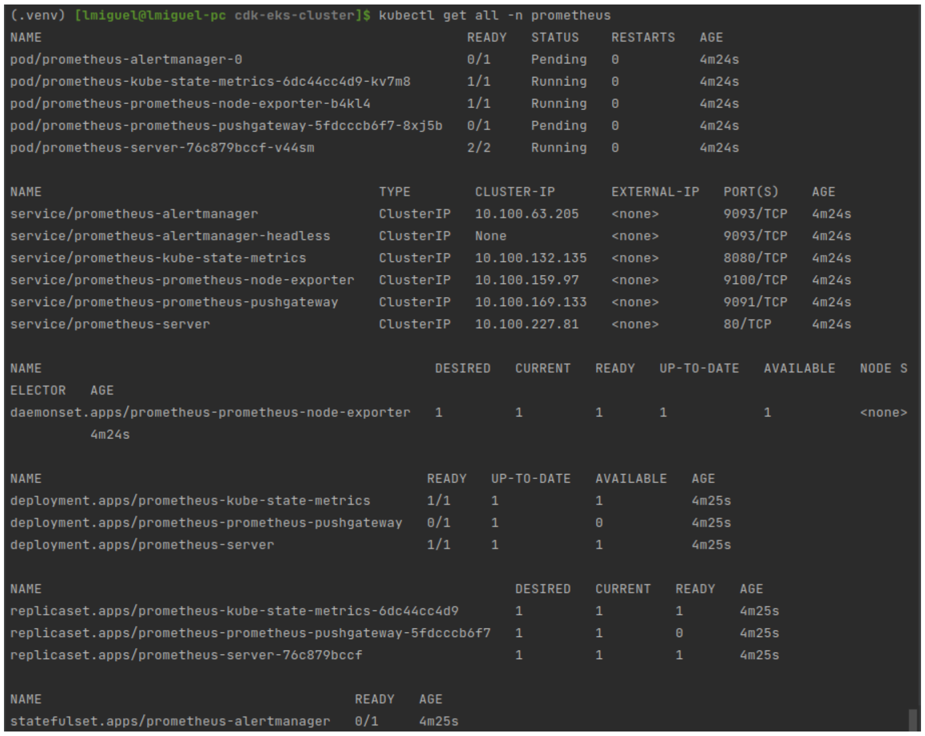
∗ Problema persiste.

– Creando el cluster con kubectl según el blog, el PVC llega a estado BOUND, y el pod a RUNNING! El problema debe estar en la forma en cómo CDK crea el cluster EKS o algún policy o recurso fallido.

  ∗ Se crea el storageClass "gp3".
  ∗ Se reintenta el comando usando "gp3" como storageClass. Algunos recursos funcionan y otros ya no.

    ·

  ∗ No se puede obtener mayor detalle de porqué los pods fallaron.



```
(.venv) [lmiguel@lmiguel-pc cdk-eks-cluster]$ kubectl get all -n prometheus
NAME                                                   READY   STATUS    RESTARTS   AGE
pod/prometheus-alertmanager-0                          0/1     Pending   0          4m24s
pod/prometheus-kube-state-metrics-6dc44cc4d9-kv7m8     1/1     Running   0          4m24s
pod/prometheus-prometheus-node-exporter-b4kl4          1/1     Running   0          4m24s
pod/prometheus-prometheus-pushgateway-5fdcccb6f7-8xj5b 0/1     Pending   0          4m24s
pod/prometheus-server-76c879bccf-v44sm                 2/2     Running   0          4m24s

NAME                                        TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)    AGE
service/prometheus-alertmanager             ClusterIP   10.100.63.205    <none>        9093/TCP   4m24s
service/prometheus-alertmanager-headless    ClusterIP   None             <none>        9093/TCP   4m24s
service/prometheus-kube-state-metrics       ClusterIP   10.100.132.135   <none>        8080/TCP   4m24s
service/prometheus-prometheus-node-exporter ClusterIP   10.100.159.97    <none>        9100/TCP   4m24s
service/prometheus-prometheus-pushgateway   ClusterIP   10.100.169.133   <none>        9091/TCP   4m24s
service/prometheus-server                   ClusterIP   10.100.227.81    <none>        80/TCP     4m24s

NAME                                                DESIRED   CURRENT   READY   UP-TO-DATE   AVAILABLE   NODE S
ELECTOR   AGE
daemonset.apps/prometheus-prometheus-node-exporter   1         1         1       1            1           <none>
          4m24s

NAME                                                READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/prometheus-kube-state-metrics       1/1     1            1           4m25s
deployment.apps/prometheus-prometheus-pushgateway   0/1     1            0           4m25s
deployment.apps/prometheus-server                   1/1     1            1           4m25s

NAME                                                           DESIRED   CURRENT   READY   AGE
replicaset.apps/prometheus-kube-state-metrics-6dc44cc4d9       1         1         1       4m25s
replicaset.apps/prometheus-prometheus-pushgateway-5fdcccb6f7   1         1         0       4m25s
replicaset.apps/prometheus-server-76c879bccf                   1         1         1       4m25s

NAME                                       READY   AGE
statefulset.apps/prometheus-alertmanager   0/1     4m25s
```

Figure 26: img__27.png