DevOps

PIN FINAL

Grupo 5

Emilio Pascutti - emiliopascutti2164@gmail.com

Natalio Cardozo - nathaliocardozo@gmail.com

Julio Gonzalez - aresden113@gmail.com

Jonathan David Martino - jonamartino@gmail.com

Gonzalo Martín Montalvo - montalvog@gmail.com

Objetivos:

Terraform - EKS – AWS – Prometheus – Grafana

El objetivo de este PIN, será desarrollar una Infraestructura como Código (IaaC) de Terraform, para desplegar un clúster de kubernetes en AWS, monitoreado con Prometheus y Grafana.

Flujo de Trabajo

/PINFINAL

├── Creación de cuenta IAM con AmazonEC2FullAccess.

├── Configuración de Terraform para el Clúster EKS.

├── Deploy de Prometheus y Grafana con Helm automático.

├── Verificación de entornos

├── Configuración de Prometheus como source de Grafana y configuración de Dashboards.

├── Clean up

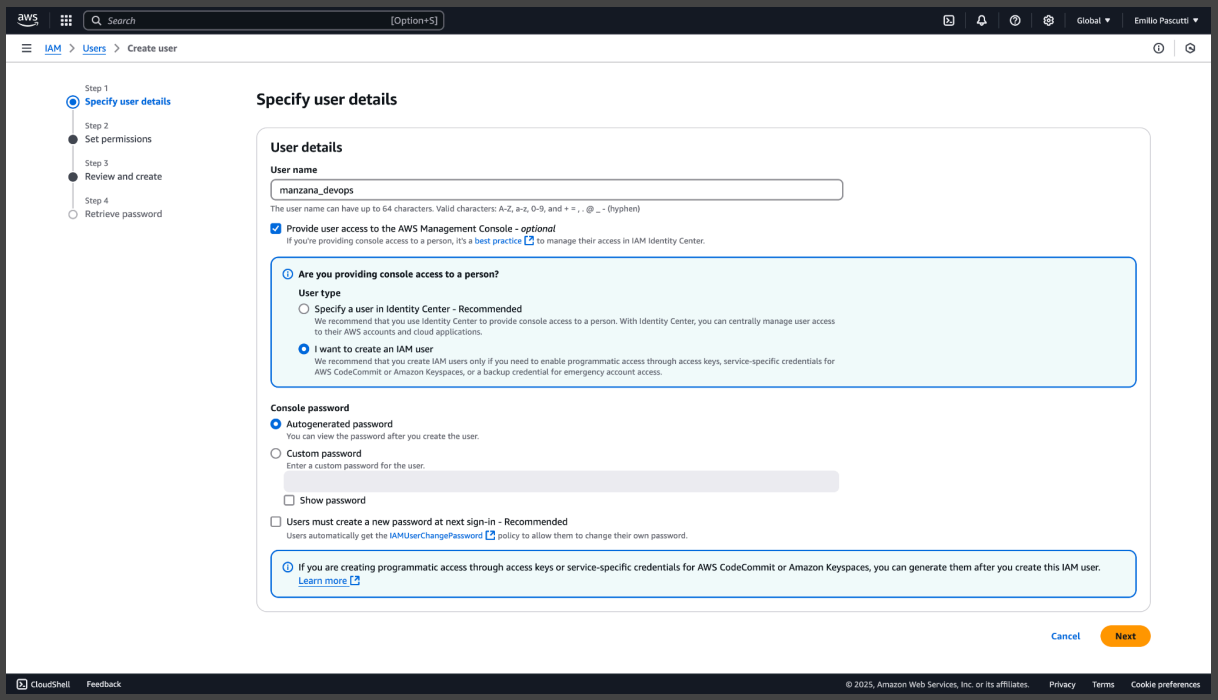
└── Análisis y conclusiones

NOTA Importante: Se adjunta link de drive para visualizar en video la configuración de Grafana de este trabajo práctico Final.

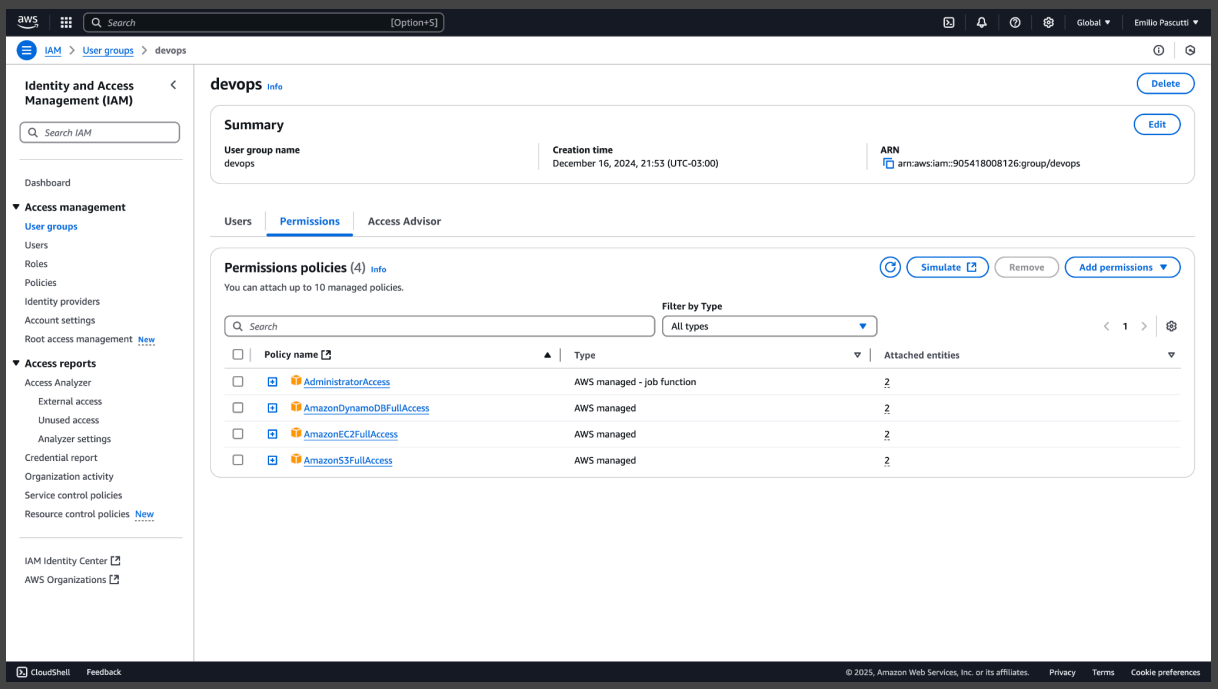
https://drive.google.com/file/d/1IrP5u6a0ObC3X18xwAwDY1VQYqnGrnJj/view?usp=share_link

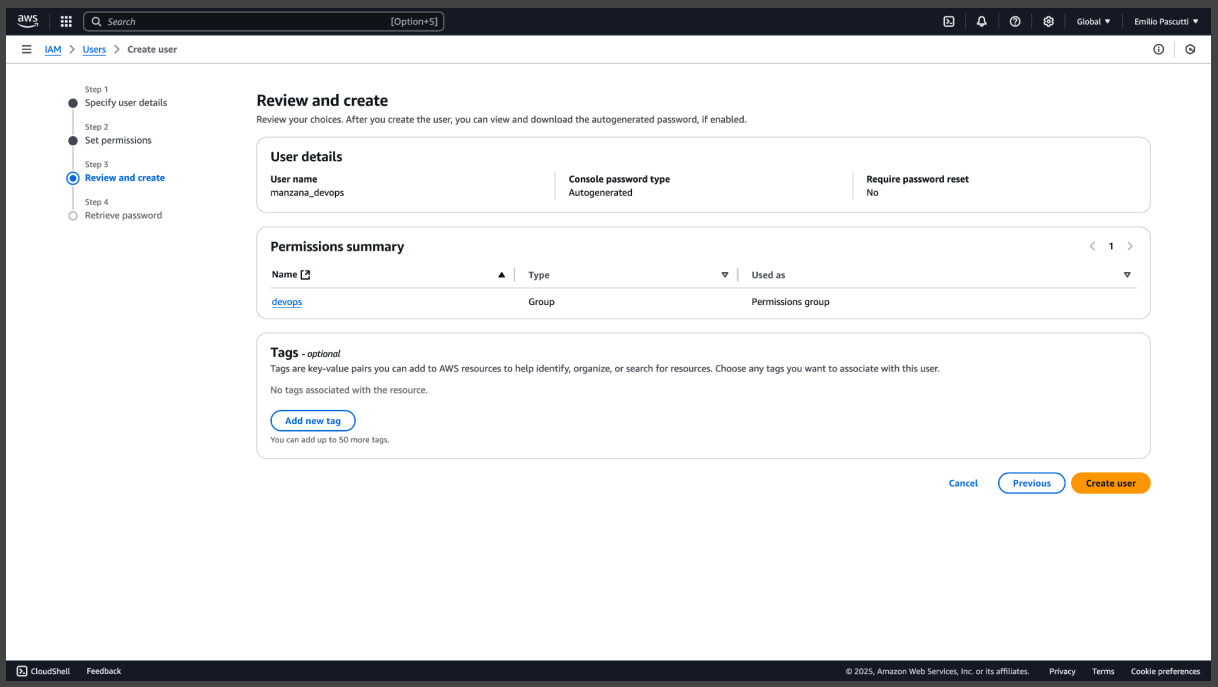
Creación de usuario IAM en AWS para EC2

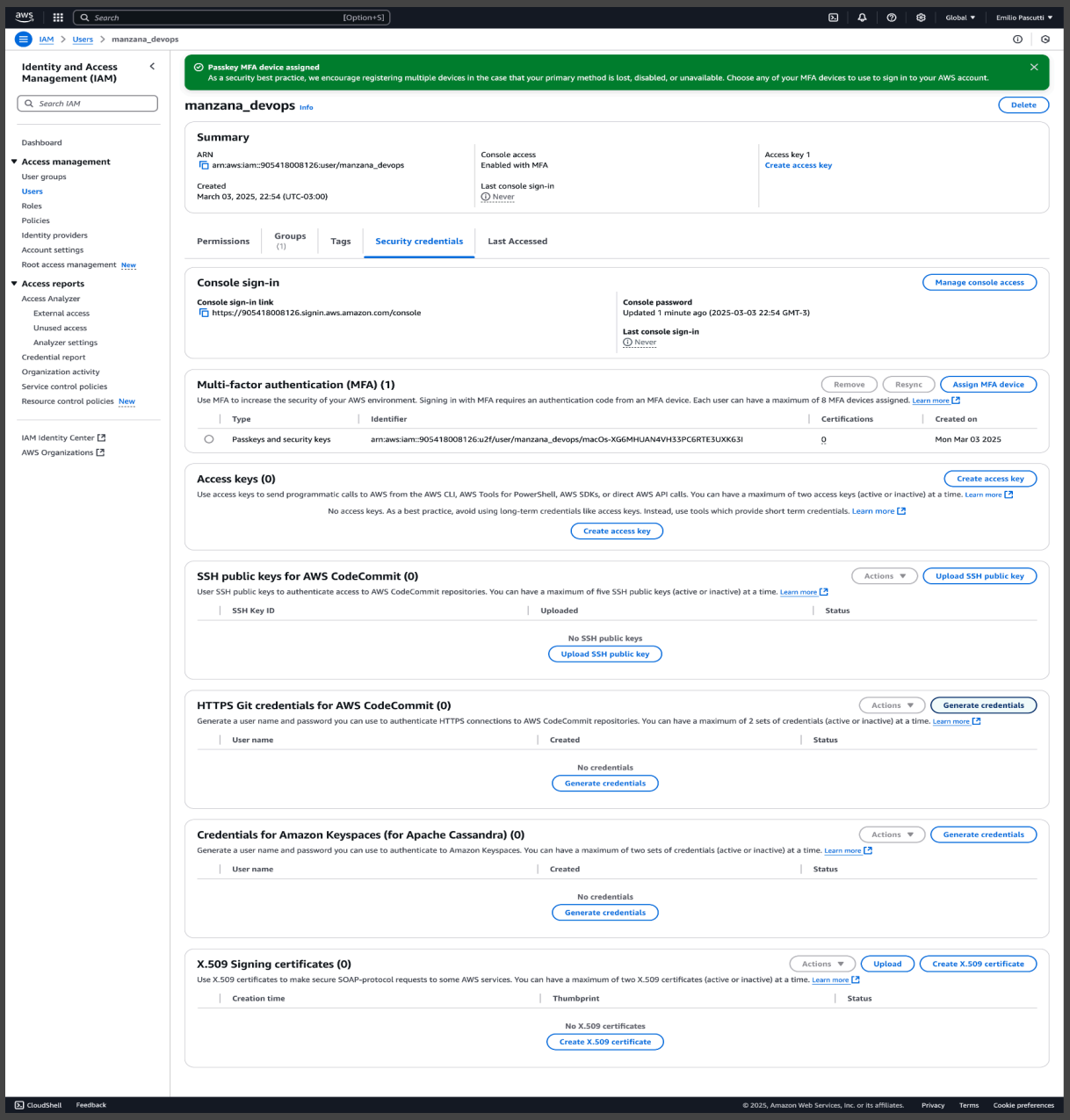
Rol IAM con policy de AmazonEC2FullAccess
Nombre de usuario IAM: manzana_devops



DevOps group:



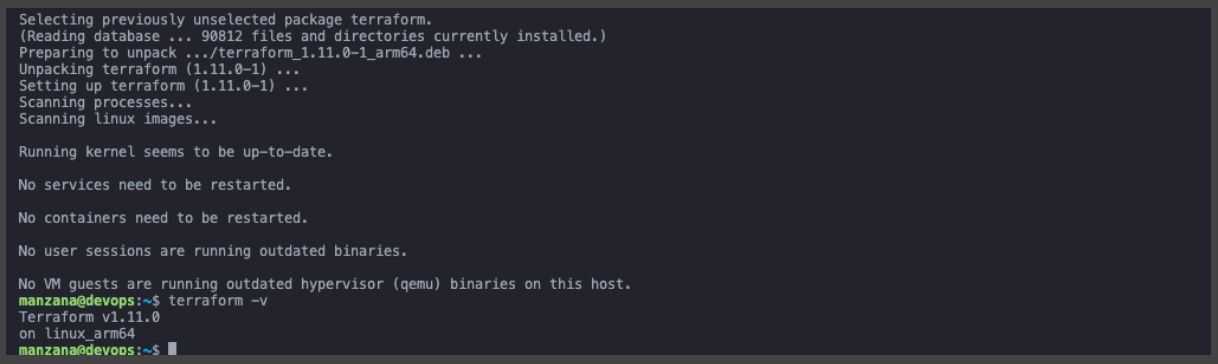

Search [Option+S]
Global
Emilio Pascutti
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
manzana_devops
Console password type
Autogenerated
Require password reset
No
Permissions summary
Name
Type
Used as
devops
Group
Permissions group
Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create user
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Option+S]
Global
Emilio Pascutti
IAM > Users > manzana_devops
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
Passkey MFA device assigned
As a security best practice, we encourage registering multiple devices in the case that your primary method is lost, disabled, or unavailable. Choose any of your MFA devices to use to sign in to your AWS account.
manzana_devops Info
Delete
Summary
ARN
arn:aws:iam::905418008126:user/manzana_devops
Created
March 03, 2025, 22:54 (UTC-03:00)
Console access
Enabled with MFA
Last console sign-in
Never
Access key 1
Create access key
Permissions
Groups (1)
Tags
Security credentials
Last Accessed
Console sign-in
Manage console access
Console sign-in link
https://905418008126.signin.aws.amazon.com/console
Console password
Updated 1 minute ago (2025-03-03 22:54 GMT-3)
Last console sign-in
Never
Multi-factor authentication (MFA) (1)
Remove
Resync
Assign MFA device
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more
Type
Identifier
Certifications
Created on
Passkeys and security keys
arn:aws:iam::905418008126:u2f/user/manzana_devops/macOs-XG6MHUAN4VH33PC6RTE3UXK63I
0
Mon Mar 03 2025
Access keys (0)
Create access key
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more
No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. Learn more
Create access key
SSH public keys for AWS CodeCommit (0)
Actions
Upload SSH public key
User SSH public keys to authenticate access to AWS CodeCommit repositories. You can have a maximum of five SSH public keys (active or inactive) at a time. Learn more
SSH Key ID
Uploaded
Status
No SSH public keys
Upload SSH public key
HTTPS Git credentials for AWS CodeCommit (0)
Actions
Generate credentials
Generate a user name and password you can use to authenticate HTTPS connections to AWS CodeCommit repositories. You can have a maximum of 2 sets of credentials (active or inactive) at a time. Learn more
User name
Created
Status
No credentials
Generate credentials
Credentials for Amazon Keyspaces (for Apache Cassandra) (0)
Actions
Generate credentials
Generate a user name and password you can use to authenticate to Amazon Keyspaces. You can have a maximum of two sets of credentials (active or inactive) at a time. Learn more
User name
Created
Status
No credentials
Generate credentials
X.509 Signing certificates (0)
Actions
Upload
Create X.509 certificate
Use X.509 certificates to make secure SOAP-protocol requests to some AWS services. You can have a maximum of two X.509 certificates (active or inactive) at a time. Learn more
Creation time
Thumbprint
Status
No X.509 certificates
Create X.509 certificate
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Configuración de Terraform para EKS:

Terraform:

```wget -O - https://apt.releases.hashicorp.com/gpg | sudo gpg --dearmor -o /usr/share/keyrings/hashicorp-archive-keyring.gpg

echo "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/hashicorp-archive-keyring.gpg] https://apt.releases.hashicorp.com $(lsb_release -cs) main" | sudo tee /etc/apt/sources.list.d/hashicorp.list

sudo apt update && sudo apt install terraform
```

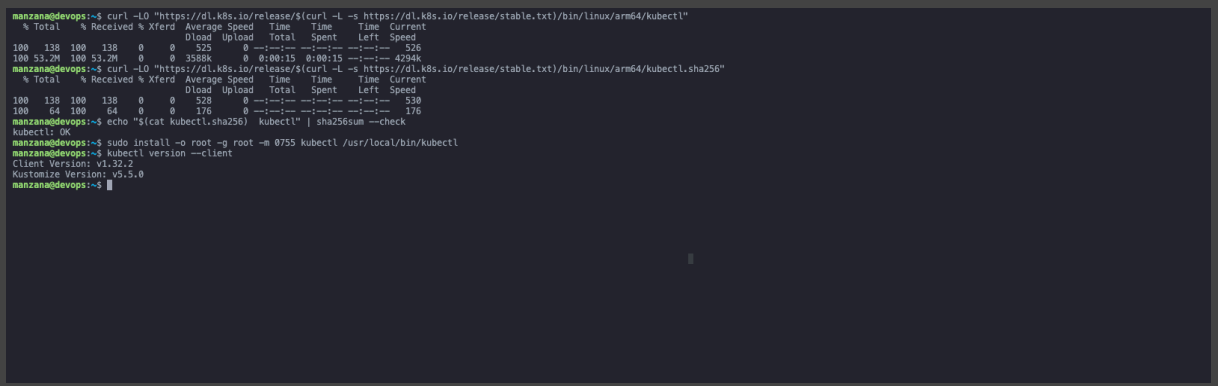


AWS CLI:

```curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install
```

kubectl para ARM:

```curl -LO "https://dl.k8s.io/release/$(curl -L -s https://dl.k8s.io/release/stable.txt)/bin/linux/arm64/kubectl"

curl -LO "https://dl.k8s.io/release/$(curl -L -s https://dl.k8s.io/release/stable.txt)/bin/linux/arm64/kubectl.sha256"

echo "$(cat kubectl.sha256)  kubectl" | sha256sum --check

sudo install -o root -g root -m 0755 kubectl /usr/local/bin/kubectl

kubectl version --client
```



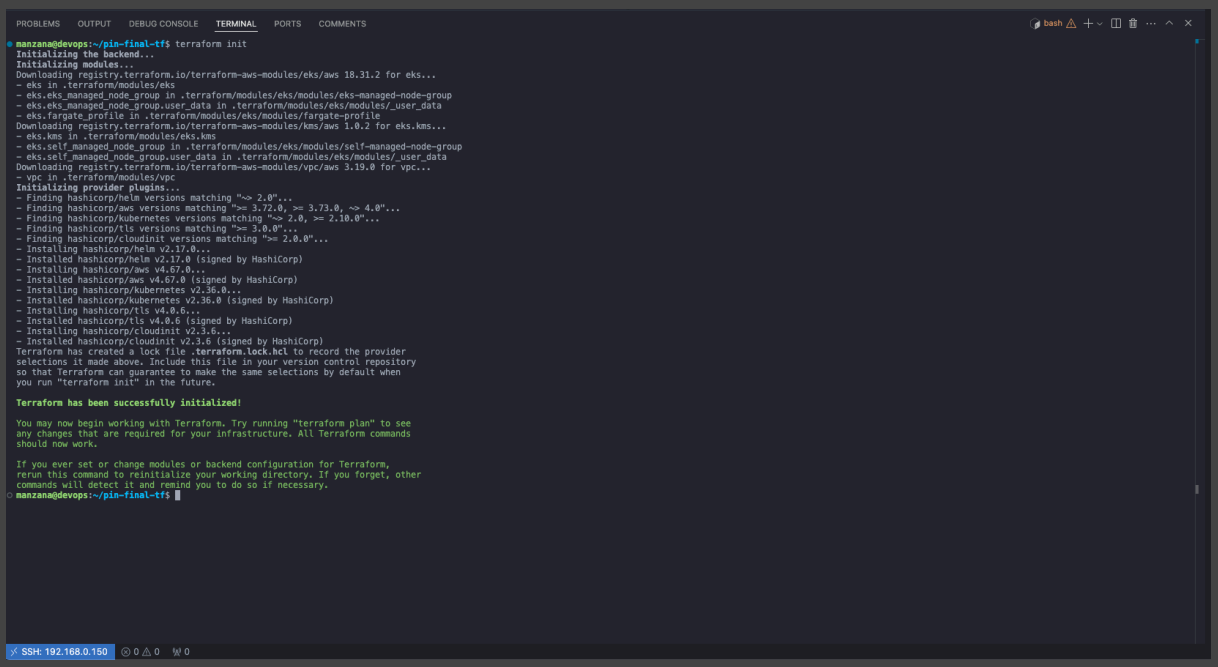
Repositorio de Github:

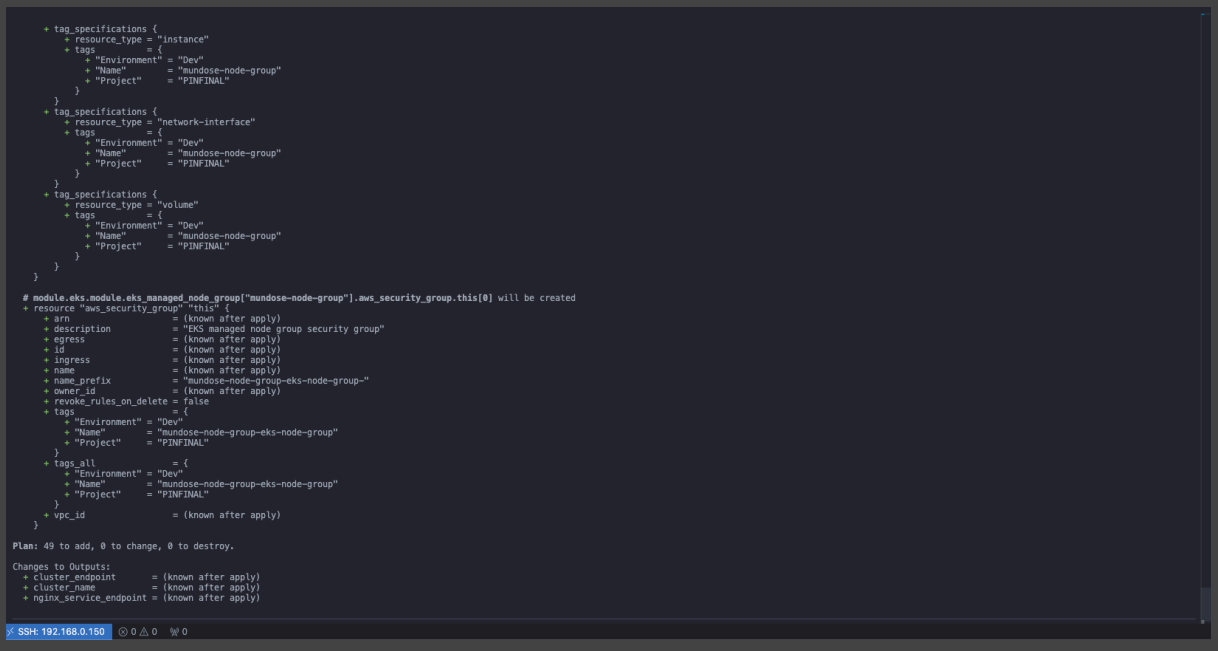
Creamos un repositorio con todas las configuraciones del IaaC donde detallamos los pasos para el despliegue del Clúster:

https://github.com/manzana2164/pin-final-tf.git

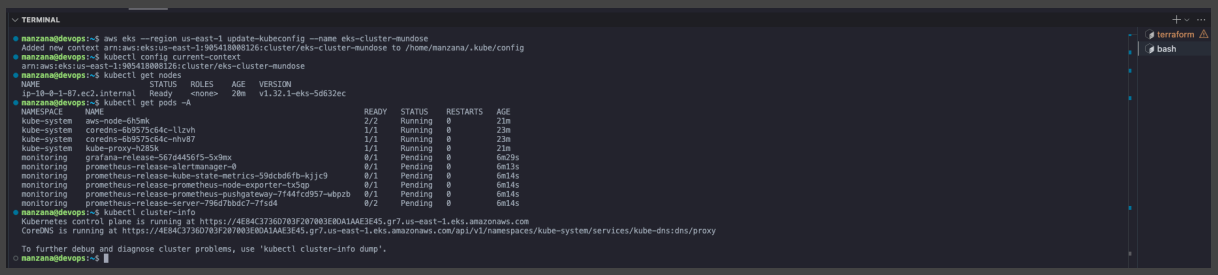
Inicialización y aplicación de Terraform:

```
terraform init
```





Después del terraform apply, chequeamos que es accesible el cluster:



Accedemos al cluster:

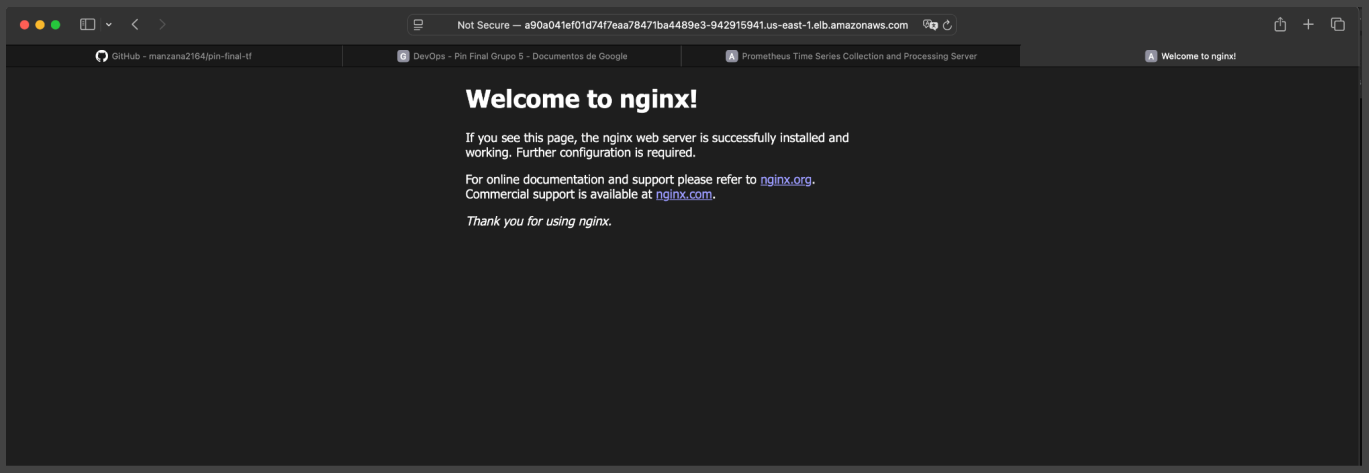
```
aws eks --region us-east-1 update-kubeconfig --name eks-cluster-mundose

kubectl get pods -A
```

Chequeamos los LoadBalancers:

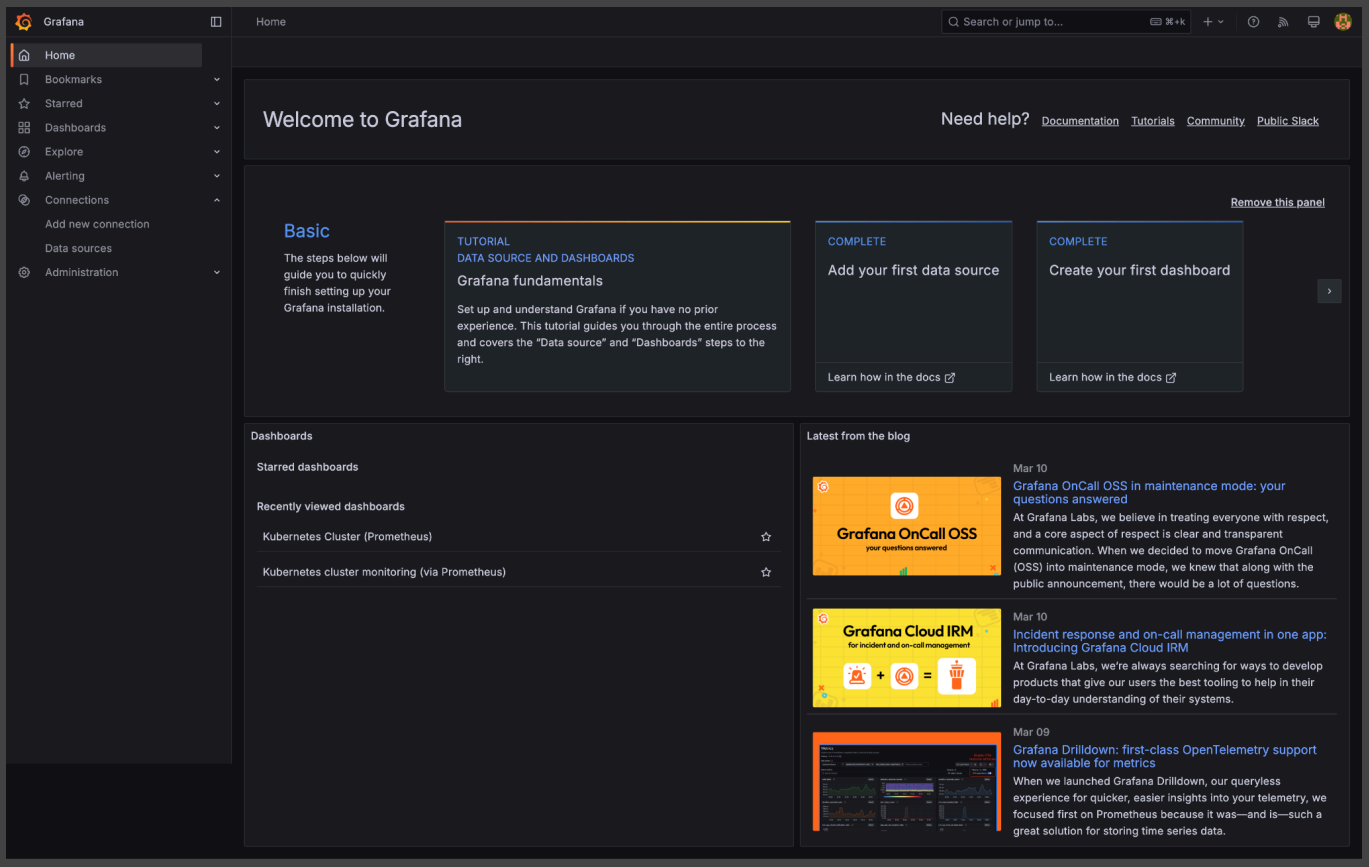
```
kubectl get svc -n monitoring
kubectl get svc -n default
```

```
manzana@devops:~$ aws eks --region us-east-1 update-kubeconfig --name eks-cluster-mundose
Updated context arn:aws:eks:us-east-1:905418008126:cluster/eks-cluster-mundose in /home/manzana/.kube/config
manzana@devops:~$ kubectl get svc -n monitoring
kubectl get svc -n default
NAME                                      TYPE           CLUSTER-IP       EXTERNAL-IP                                                                    PORT(S)          AGE
grafana-release                           LoadBalancer   172.20.39.163    afa09e8bb22b4467baaf266910d91ab5-1015308082.us-east-1.elb.amazonaws.com   80:31000/TCP     22m
prometheus-release-kube-state-metrics     ClusterIP      172.20.119.135   <none>                                                                         8080/TCP         21m
prometheus-release-prometheus-node-exporter   ClusterIP      172.20.193.46    <none>                                                                         9100/TCP         21m
prometheus-release-prometheus-pushgateway     ClusterIP      172.20.220.131   <none>                                                                         9091/TCP         21m
prometheus-release-server                 LoadBalancer   172.20.22.75     a6627b4bb066346aa895ec35f5505809-1104680589.us-east-1.elb.amazonaws.com   80:31483/TCP     21m
NAME              TYPE           CLUSTER-IP       EXTERNAL-IP                                                              PORT(S)        AGE
kubernetes        ClusterIP      172.20.0.1       <none>                                                                   443/TCP        24m
nginx-logs-service   LoadBalancer   172.20.109.110   a90a041ef01d74f7eaa78471ba4489e3-942915941.us-east-1.elb.amazonaws.com   80:31144/TCP   22m
manzana@devops:~$
```

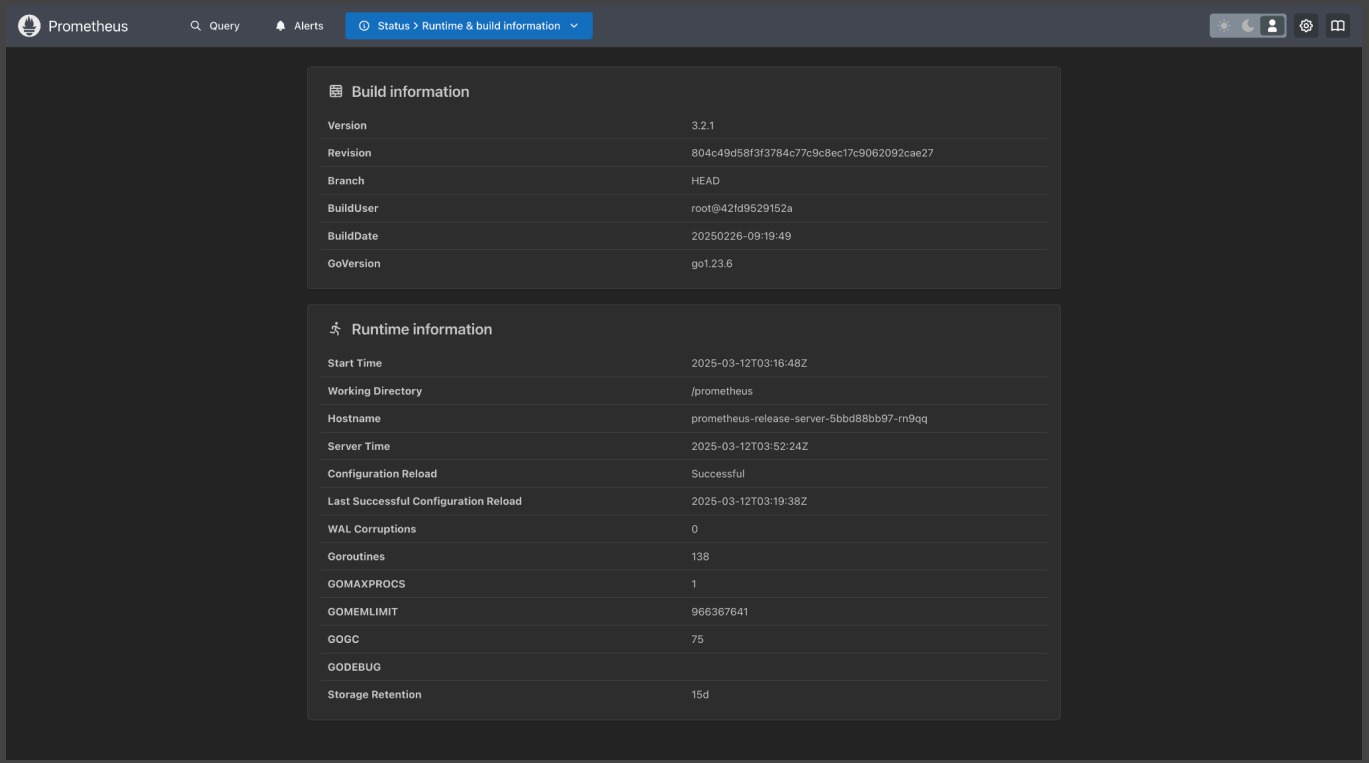
Accedemos a Nginx:
a90a041ef01d74f7eaa78471ba4489e3-942915941.us-east-1.elb.amazonaws.com



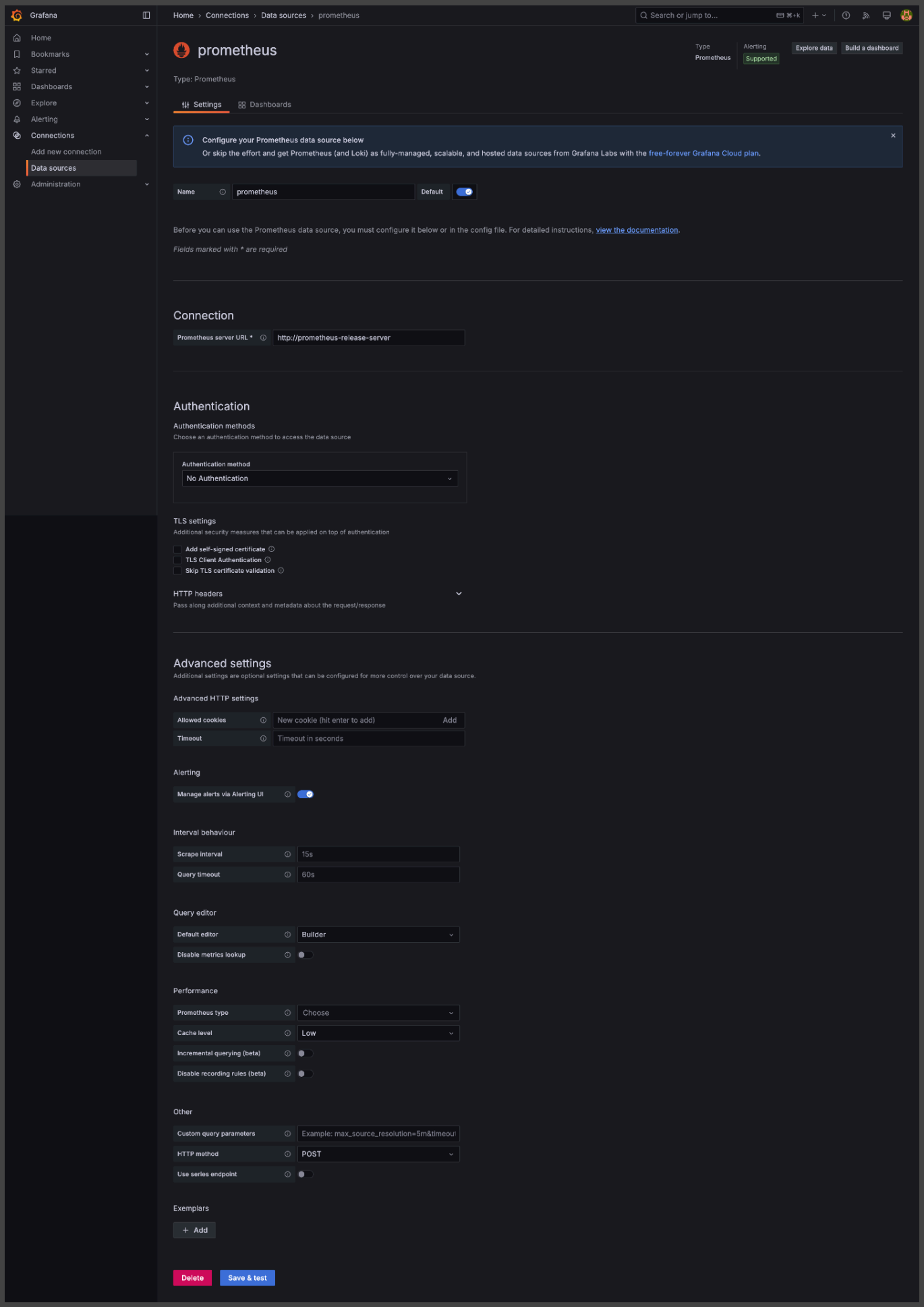
Accedemos a Grafana:
afa09e8bb22b4467baaf266910d91ab5-1015308082.us-east-1.elb.amazonaws.com



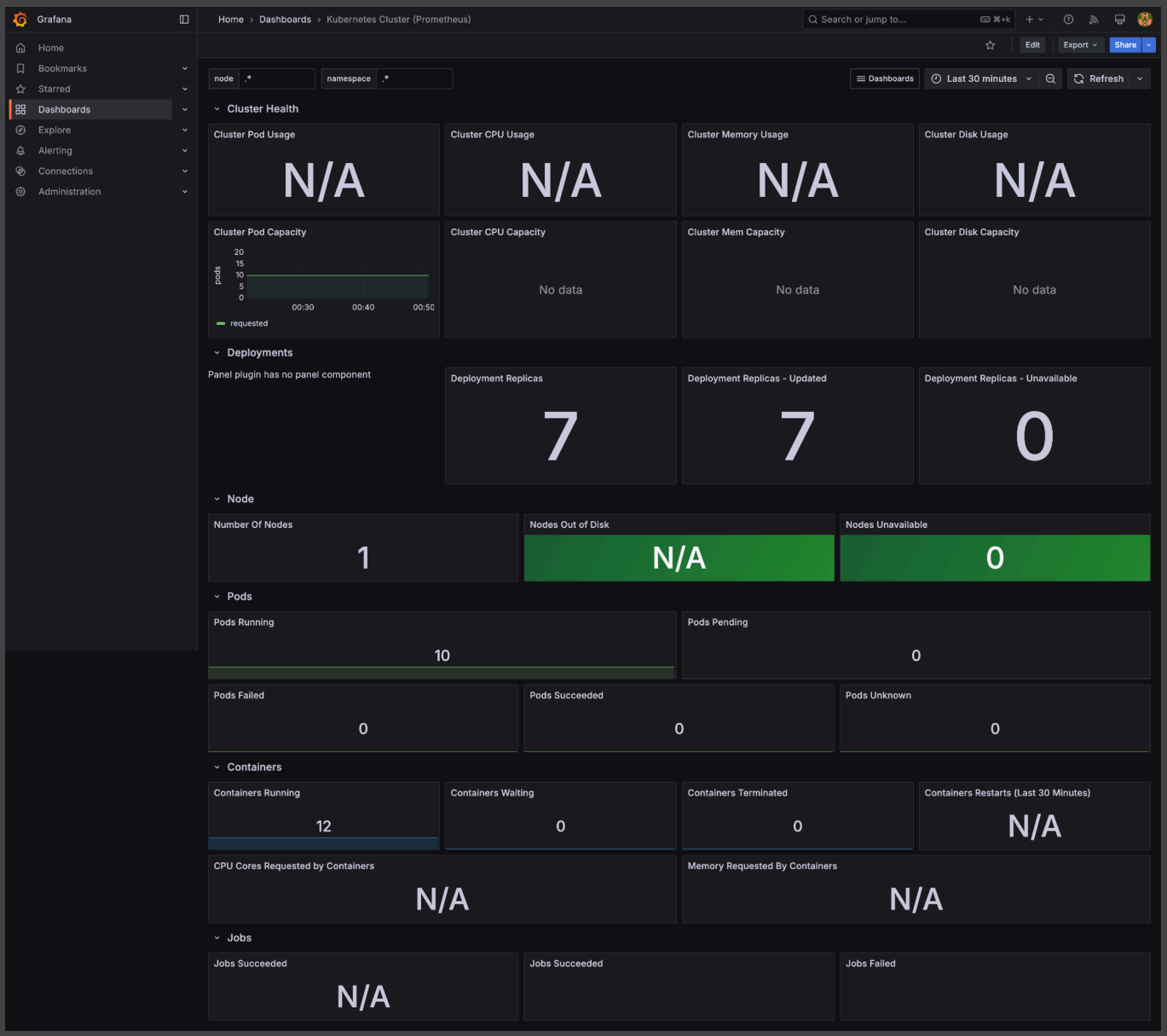
Accedemos a Prometheus:
a6627b4bb066346aa895ec35f5505809-1104680589.us-east-1.elb.amazonaws.com



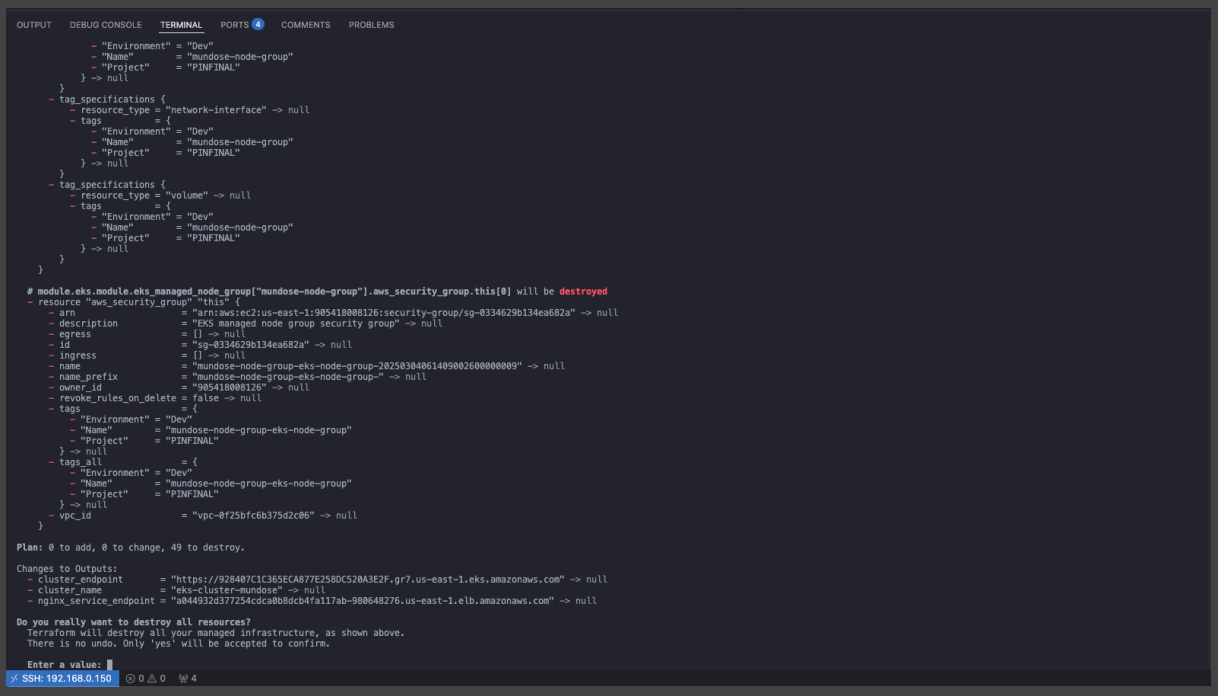
Agregamos la source de Prometheus:



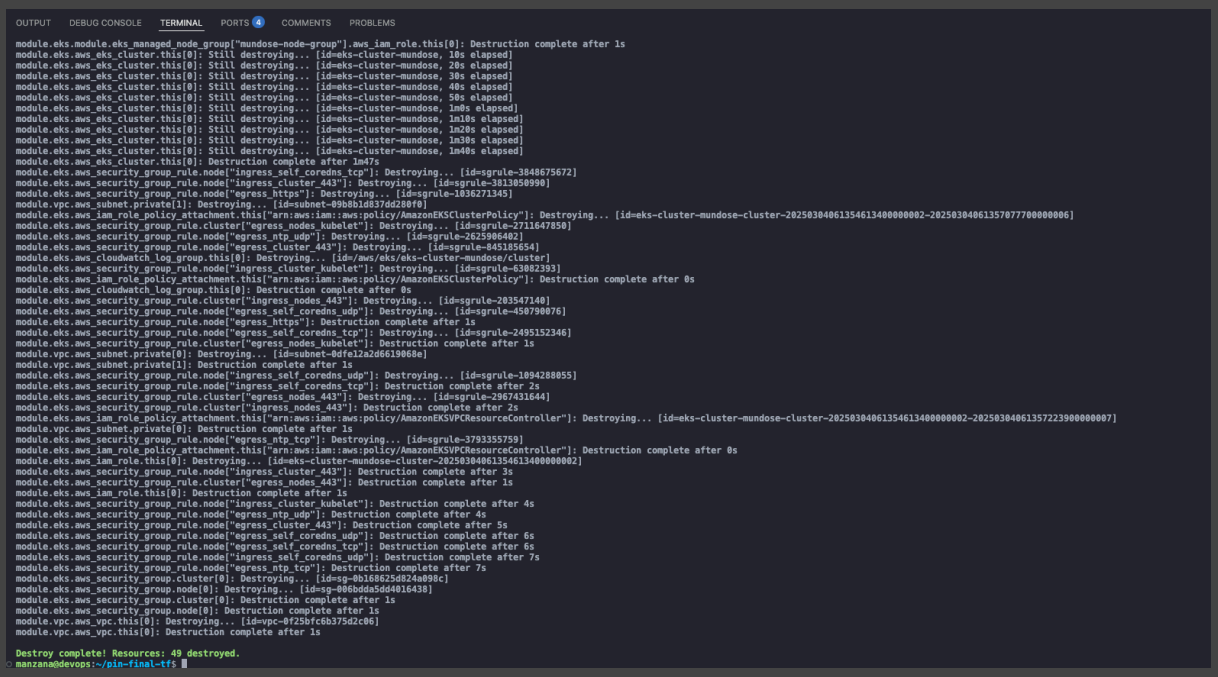
Creamos los dashboards por importación con los códigos 3119 y 6417


Grafana
Home
Bookmarks
Starred
Dashboards
Explore
Alerting
Connections
Administration
Home › Dashboards › Kubernetes Cluster (Prometheus)
Search or jump to...
Edit
Export
Share
node .*
namespace .*
Dashboards
Last 30 minutes
Refresh
Cluster Health
Cluster Pod Usage
N/A
Cluster CPU Usage
N/A
Cluster Memory Usage
N/A
Cluster Disk Usage
N/A
Cluster Pod Capacity
pods
20
15
10
5
0
00:30
00:40
00:50
requested
Cluster CPU Capacity
No data
Cluster Mem Capacity
No data
Cluster Disk Capacity
No data
Deployments
Panel plugin has no panel component
Deployment Replicas
7
Deployment Replicas - Updated
7
Deployment Replicas - Unavailable
0
Node
Number Of Nodes
1
Nodes Out of Disk
N/A
Nodes Unavailable
0
Pods
Pods Running
10
Pods Pending
0
Pods Failed
0
Pods Succeeded
0
Pods Unknown
0
Containers
Containers Running
12
Containers Waiting
0
Containers Terminated
0
Containers Restarts (Last 30 Minutes)
N/A
CPU Cores Requested by Containers
N/A
Memory Requested By Containers
N/A
Jobs
Jobs Succeeded
N/A
Jobs Succeeded
Jobs Failed

Luego de verificar los dashboards, procedemos con un `terraform destroy` a eliminar la instancia EC2



```
OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS 4  COMMENTS  PROBLEMS

            - "Environment" = "Dev"
            - "Name"        = "mundose-node-group"
            - "Project"     = "PINFINAL"
          } -> null
      }
    - tag_specifications {
        - resource_type = "network-interface" -> null
        - tags          = {
            - "Environment" = "Dev"
            - "Name"        = "mundose-node-group"
            - "Project"     = "PINFINAL"
          } -> null
      }
    - tag_specifications {
        - resource_type = "volume" -> null
        - tags          = {
            - "Environment" = "Dev"
            - "Name"        = "mundose-node-group"
            - "Project"     = "PINFINAL"
          } -> null
      }
  }

# module.eks.module.eks_managed_node_group["mundose-node-group"].aws_security_group.this[0] will be destroyed
- resource "aws_security_group" "this" {
    - arn                    = "arn:aws:ec2:us-east-1:905418008126:security-group/sg-0334629b134ea682a" -> null
    - description            = "EKS managed node group security group" -> null
    - egress                 = [] -> null
    - id                     = "sg-0334629b134ea682a" -> null
    - ingress                = [] -> null
    - name                   = "mundose-node-group-eks-node-group-20250304061409002600000009" -> null
    - name_prefix            = "mundose-node-group-eks-node-group-" -> null
    - owner_id               = "905418008126" -> null
    - revoke_rules_on_delete = false -> null
    - tags                   = {
        - "Environment" = "Dev"
        - "Name"        = "mundose-node-group-eks-node-group"
        - "Project"     = "PINFINAL"
      } -> null
    - tags_all               = {
        - "Environment" = "Dev"
        - "Name"        = "mundose-node-group-eks-node-group"
        - "Project"     = "PINFINAL"
      } -> null
    - vpc_id                 = "vpc-0f25bfc6b375d2c06" -> null
  }

Plan: 0 to add, 0 to change, 49 to destroy.

Changes to Outputs:
  - cluster_endpoint      = "https://928407C1C365ECA877E258DC520A3E2F.gr7.us-east-1.eks.amazonaws.com" -> null
  - cluster_name          = "eks-cluster-mundose" -> null
  - nginx_service_endpoint = "a044932d377254cdca0b8dcb4fa117ab-980648276.us-east-1.elb.amazonaws.com" -> null

Do you really want to destroy all resources?
  Terraform will destroy all your managed infrastructure, as shown above.
  There is no undo. Only 'yes' will be accepted to confirm.

  Enter a value:

SSH: 192.168.0.150  ⊗ 0 ⚠ 0  4
```



```
OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS 4  COMMENTS  PROBLEMS

module.eks.module.eks_managed_node_group["mundose-node-group"].aws_iam_role.this[0]: Destruction complete after 1s
module.eks.aws_eks_cluster.this[0]: Still destroying... [id=eks-cluster-mundose, 10s elapsed]
module.eks.aws_eks_cluster.this[0]: Still destroying... [id=eks-cluster-mundose, 20s elapsed]
module.eks.aws_eks_cluster.this[0]: Still destroying... [id=eks-cluster-mundose, 30s elapsed]
module.eks.aws_eks_cluster.this[0]: Still destroying... [id=eks-cluster-mundose, 40s elapsed]
module.eks.aws_eks_cluster.this[0]: Still destroying... [id=eks-cluster-mundose, 50s elapsed]
module.eks.aws_eks_cluster.this[0]: Still destroying... [id=eks-cluster-mundose, 1m0s elapsed]
module.eks.aws_eks_cluster.this[0]: Still destroying... [id=eks-cluster-mundose, 1m10s elapsed]
module.eks.aws_eks_cluster.this[0]: Still destroying... [id=eks-cluster-mundose, 1m20s elapsed]
module.eks.aws_eks_cluster.this[0]: Still destroying... [id=eks-cluster-mundose, 1m30s elapsed]
module.eks.aws_eks_cluster.this[0]: Still destroying... [id=eks-cluster-mundose, 1m40s elapsed]
module.eks.aws_eks_cluster.this[0]: Destruction complete after 1m47s
module.eks.aws_security_group_rule.node["ingress_self_coredns_tcp"]: Destroying... [id=sgrule-3848675672]
module.eks.aws_security_group_rule.node["ingress_cluster_443"]: Destroying... [id=sgrule-3813050990]
module.eks.aws_security_group_rule.node["egress_https"]: Destroying... [id=sgrule-1036271345]
module.vpc.aws_subnet.private[1]: Destroying... [id=subnet-09b8b1d837dd280f0]
module.eks.aws_iam_role_policy_attachment.this["arn:aws:iam::aws:policy/AmazonEKSClusterPolicy"]: Destroying... [id=eks-cluster-mundose-cluster-20250304061354613400000002-20250304061357077700000006]
module.eks.aws_security_group_rule.cluster["egress_nodes_kubelet"]: Destroying... [id=sgrule-2711647850]
module.eks.aws_security_group_rule.node["egress_ntp_udp"]: Destroying... [id=sgrule-2625906402]
module.eks.aws_security_group_rule.node["egress_cluster_443"]: Destroying... [id=sgrule-845185654]
module.eks.aws_cloudwatch_log_group.this[0]: Destroying... [id=/aws/eks/eks-cluster-mundose/cluster]
module.eks.aws_security_group_rule.node["ingress_cluster_kubelet"]: Destroying... [id=sgrule-63082393]
module.eks.aws_iam_role_policy_attachment.this["arn:aws:iam::aws:policy/AmazonEKSClusterPolicy"]: Destruction complete after 0s
module.eks.aws_cloudwatch_log_group.this[0]: Destruction complete after 0s
module.eks.aws_security_group_rule.cluster["ingress_nodes_443"]: Destroying... [id=sgrule-203547140]
module.eks.aws_security_group_rule.node["egress_self_coredns_udp"]: Destroying... [id=sgrule-450790076]
module.eks.aws_security_group_rule.node["egress_https"]: Destruction complete after 1s
module.eks.aws_security_group_rule.node["egress_self_coredns_tcp"]: Destroying... [id=sgrule-2495152346]
module.eks.aws_security_group_rule.cluster["egress_nodes_kubelet"]: Destruction complete after 1s
module.vpc.aws_subnet.private[0]: Destroying... [id=subnet-0dfe12a2d6619068e]
module.vpc.aws_subnet.private[1]: Destruction complete after 1s
module.eks.aws_security_group_rule.node["ingress_self_coredns_udp"]: Destroying... [id=sgrule-1094288055]
module.eks.aws_security_group_rule.node["ingress_self_coredns_tcp"]: Destruction complete after 2s
module.eks.aws_security_group_rule.cluster["egress_nodes_443"]: Destroying... [id=sgrule-2967431644]
module.eks.aws_security_group_rule.cluster["ingress_nodes_443"]: Destruction complete after 2s
module.eks.aws_iam_role_policy_attachment.this["arn:aws:iam::aws:policy/AmazonEKSVPCResourceController"]: Destroying... [id=eks-cluster-mundose-cluster-20250304061354613400000002-20250304061357223900000007]
module.vpc.aws_subnet.private[0]: Destruction complete after 1s
module.eks.aws_security_group_rule.node["egress_ntp_tcp"]: Destroying... [id=sgrule-3793355759]
module.eks.aws_iam_role_policy_attachment.this["arn:aws:iam::aws:policy/AmazonEKSVPCResourceController"]: Destruction complete after 0s
module.eks.aws_iam_role.this[0]: Destroying... [id=eks-cluster-mundose-cluster-20250304061354613400000002]
module.eks.aws_security_group_rule.node["ingress_cluster_443"]: Destruction complete after 3s
module.eks.aws_security_group_rule.cluster["egress_nodes_443"]: Destruction complete after 1s
module.eks.aws_iam_role.this[0]: Destruction complete after 1s
module.eks.aws_security_group_rule.node["ingress_cluster_kubelet"]: Destruction complete after 4s
module.eks.aws_security_group_rule.node["egress_ntp_udp"]: Destruction complete after 4s
module.eks.aws_security_group_rule.node["egress_cluster_443"]: Destruction complete after 5s
module.eks.aws_security_group_rule.node["egress_self_coredns_udp"]: Destruction complete after 6s
module.eks.aws_security_group_rule.node["egress_self_coredns_tcp"]: Destruction complete after 6s
module.eks.aws_security_group_rule.node["ingress_self_coredns_udp"]: Destruction complete after 7s
module.eks.aws_security_group_rule.node["egress_ntp_tcp"]: Destruction complete after 7s
module.eks.aws_security_group.cluster[0]: Destroying... [id=sg-0b168625d824a098c]
module.eks.aws_security_group.node[0]: Destroying... [id=sg-006bdda5dd4016438]
module.eks.aws_security_group.cluster[0]: Destruction complete after 1s
module.eks.aws_security_group.node[0]: Destruction complete after 1s
module.vpc.aws_vpc.this[0]: Destroying... [id=vpc-0f25bfc6b375d2c06]
module.vpc.aws_vpc.this[0]: Destruction complete after 1s

Destroy complete! Resources: 49 destroyed.
manzana@devops:~/pin-final-tf$
```

Análisis y Conclusiones:

Para la región **`us-east-1`**, utilizamos la versión de Kubernetes **`1.32`**, dado que la versión 1.22 no era compatible.

La instancia al ser t2.micro, le agregamos un timeout a Prometheus y Grafana de 600 segundos. Dado al tiempo de demora en el deploy Prometheus, modificamos el **`eks.tf`** para incorporar una instancia de **`T3.Large`**, y, además, limitamos los recursos de los pods en cuanto a cpu y memoria.