

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 (IaC) 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/1lrP5u6a0ObC3X18xwAwDY1VQYqnGrnJj/view?usp=share_link

Creación de usuario IAM en AWS para EC2

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

Step 1

Specify user details

Step 2

Set permissions

Step 3

Review and create

Step 4

Retrieve password

Specify user details

User details

User name

manzana_devops

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, =, @, _ (hyphen)

☒ Provide user access to the AWS Management Console - optional

If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type

☐ Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

☒ I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

☒ Autogenerated password

You can view the password after you create the user.

☐ Custom password

Enter a custom password for the user.

☐ Show password

☐ Users must create a new password at next sign-in - Recommended

Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

Are you creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user.

[Learn more](#)

Cancel

Next

DevOps group:

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Resource control policies

IAM Identity Center

AWS Organizations

devops

Delete

Edit

Summary

User group name

devops

Creation time

December 16, 2024, 21:53 (UTC-03:00)

ARN

arn:aws:iam:905418008126:group/devops

Users

Permissions

Access Advisor

Permissions policies (4)

Simulate

Remove

Add permissions

You can attach up to 10 managed policies.

Filter by Type

All types

Search

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	2
<input type="checkbox"/>	AmazonDynamoDBFullAccess	AWS managed	2
<input type="checkbox"/>	AmazonEC2FullAccess	AWS managed	2
<input type="checkbox"/>	AmazonS3FullAccess	AWS managed	2

aws

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

aws

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

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Resource control policies

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.

Delete

manzana_devops

Info

Delete

Summary

ARN
arn:aws:iam::905418008126:user/manzana_devops

Console access
Enabled with MFA

Access key 1
Create access key

Created
March 03, 2025, 22:54 (UTC-03:00)

Last console sign-in
Never

Permissions

Groups (1)

Tags

Security credentials

Last Accessed

Console sign-in

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

Manage console access

Multi-factor authentication (MFA) (1)

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

Remove Resync Assign MFA device

Type	Identifier	Certifications	Created on
Passkeys and security keys	arn:aws:iam::905418008126:u2f/user/manzana_devops/macOs-XG6MHUAN4VH3PC6RTE3JUXK63I		Mon Mar 03 2025

Access keys (0)

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)

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

Actions Upload SSH public key

SSH Key ID	Uploaded	Status
No SSH public keys		

Upload SSH public key

HTTPS Git credentials for AWS CodeCommit (0)

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

Actions Generate credentials

User name	Created	Status
No credentials		

Generate credentials

Credentials for Amazon Keyspaces (for Apache Cassandra) (0)

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

Actions Generate credentials

User name	Created	Status
No credentials		

Generate credentials

X.509 Signing certificates (0)

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

Actions Upload Create X.509 certificate

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
```

```
Selecting previously unselected package terraform.  
(Reading database ... 90812 files and directories currently installed.)  
Preparing to unpack ../terraform_1.11.0-1_arm64.deb ...  
Unpacking terraform (1.11.0-1) ...  
Setting up terraform (1.11.0-1) ...  
Scanning processes...  
Scanning linux images...  
  
Running kernel seems to be up-to-date.  
  
No services need to be restarted.  
  
No containers need to be restarted.  
  
No user sessions are running outdated binaries.  
  
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
manzana@devops:~$ terraform -v  
Terraform v1.11.0  
on linux_arm64  
manzana@devops:~$
```

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
```

```
manzana@devops:~$ curl -LO "https://dl.k8s.io/release/$(curl -L -s https://dl.k8s.io/release/stable.txt)/bin/linux/arm64/kubectl"  
% Total % Received % Xferd Average Speed Time Time Time Current  
Dload Upload Total Spent Left Speed  
100 138 100 138 0 0 525 0 --:--:-- --:--:-- --:--:-- 526  
100 53.2M 100 53.2M 0 0 3588K 0 0:00:15 0:00:15 --:--:-- 4294K  
manzana@devops:~$ curl -LO "https://dl.k8s.io/release/$(curl -L -s https://dl.k8s.io/release/stable.txt)/bin/linux/arm64/kubectl.sha256"  
% Total % Received % Xferd Average Speed Time Time Time Current  
Dload Upload Total Spent Left Speed  
100 138 100 138 0 0 528 0 --:--:-- --:--:-- --:--:-- 530  
100 64 100 64 0 0 176 0 --:--:-- --:--:-- --:--:-- 176  
manzana@devops:~$ echo "$(cat kubectl.sha256) kubectl" | sha256sum --check  
kubectl: OK  
manzana@devops:~$ sudo install -o root -g root -m 0755 kubectl /usr/local/bin/kubectl  
manzana@devops:~$ kubectl version --client  
Client Version: v1.32.2  
Kustomize Version: v5.5.0  
manzana@devops:~$
```

Repositorio de Github:

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

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

Inicialización y aplicación de Terraform:

`terraform init`

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS COMMENTS
manzana@devops:~/pin-final-tf$ terraform init
Initializing the backend...
Initializing modules...
- Downloading registry.terraform.io/terraform-aws-modules/eks/aws 18.31.2 for eks...
- eks in .terraform/modules/eks
- eks.eks_managed_node_group in .terraform/modules/eks/modules/eks-managed-node-group
- eks.eks_managed_node_group.user_data in .terraform/modules/eks/modules/user_data
- eks.fargate_profile in .terraform/modules/eks/modules/fargate-profile
- Downloading registry.terraform.io/terraform-aws-modules/kms/aws 1.0.2 for eks.kms...
- eks.eks in .terraform/modules/eks.kms
- eks.self_managed_node_group in .terraform/modules/eks/modules/self-managed-node-group
- eks.self_managed_node_group.user_data in .terraform/modules/eks/modules/user_data
- Downloading registry.terraform.io/terraform-aws-modules/vpc/aws 3.19.0 for vpc...
- vpc in .terraform/modules/vpc
Initializing provider plugins...
- Finding hashicorp/helm versions matching "~>= 2.0"...
- Finding hashicorp/aws versions matching "~>= 3.72.0, <= 3.73.0, <= 4.0"...
- Finding hashicorp/kubernetes versions matching "~>= 2.0, <= 2.10.0"...
- Finding hashicorp/tls versions matching "~>= 3.0.0"...
- Finding hashicorp/cloudinit versions matching "~>= 2.0.0"...
- Installing hashicorp/helm v2.17.0...
- Installed hashicorp/helm v2.17.0 (signed by HashiCorp)
- Installing hashicorp/aws v4.67.0...
- Installed hashicorp/aws v4.67.0 (signed by HashiCorp)
- Installing hashicorp/kubernetes v2.36.0...
- Installed hashicorp/kubernetes v2.36.0 (signed by HashiCorp)
- Installing hashicorp/tls v4.0.6...
- Installed hashicorp/tls v4.0.6 (signed by HashiCorp)
- Installing hashicorp/cloudinit v2.3.6...
- Installed hashicorp/cloudinit v2.3.6 (signed by HashiCorp)
Terraform has created a lock file .terraform.lock.hcl to record the provider
selections it made above. Include this file in your version control repository
so that Terraform can guarantee to make the same selections by default when
you run "terraform init" in the future.

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
manzana@devops:~/pin-final-tf$
```

```
+ tag_specifications {
+   resource_type = "instance"
+   tags = {
+     "Environment" = "Dev"
+     "Name"        = "mundose-node-group"
+     "Project"     = "PINFINAL"
+   }
+ }
+ tag_specifications {
+   resource_type = "network-interface"
+   tags = {
+     "Environment" = "Dev"
+     "Name"        = "mundose-node-group"
+     "Project"     = "PINFINAL"
+   }
+ }
+ tag_specifications {
+   resource_type = "volume"
+   tags = {
+     "Environment" = "Dev"
+     "Name"        = "mundose-node-group"
+     "Project"     = "PINFINAL"
+   }
+ }
+ }

# module.eks.module.eks_managed_node_group["mundose-node-group"].aws_security_group.this[0] will be created
+ resource "aws_security_group" "this" {
+   arn              = (known after apply)
+   description      = "EKS managed node group security group"
+   egress            = (known after apply)
+   id               = (known after apply)
+   ingress           = (known after apply)
+   name             = (known after apply)
+   name_prefix      = "mundose-node-group-eks-node-group-"
+   owner_id         = (known after apply)
+   revoke_rules_on_delete = false
+   tags             = {
+     "Environment" = "Dev"
+     "Name"        = "mundose-node-group-eks-node-group"
+     "Project"     = "PINFINAL"
+   }
+   tags_all         = {
+     "Environment" = "Dev"
+     "Name"        = "mundose-node-group-eks-node-group"
+     "Project"     = "PINFINAL"
+   }
+   vpc_id           = (known after apply)
+ }

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

Changes to Outputs:
+ cluster_endpoint = (known after apply)
+ cluster_name     = (known after apply)
+ nginx_service_endpoint = (known after apply)
```

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

```
manzana@devops:~$ aws eks --region us-east-1 update-kubeconfig --name eks-cluster-mundose
Added new context arn:aws:eks:us-east-1:905418008126:cluster/eks-cluster-mundose to /home/manzana/.kube/config
manzana@devops:~$ kubectl config current-context
arn:aws:eks:us-east-1:905418008126:cluster/eks-cluster-mundose
manzana@devops:~$ kubectl get nodes
NAME                                STATUS    ROLES    AGE   VERSION
ip-18-8-1-87.ec2.internal           Ready    <none>   20m   v1.32.1-eks-5d632ec
manzana@devops:~$ kubectl get pods -A
NAMESPACE      NAME                                READY    STATUS    RESTARTS   AGE
kube-system    aws-node-6h5sk                     2/2      Running   0           21m
kube-system    coredns-b9d75c64c-1lzyh            1/1      Running   0           23m
kube-system    coredns-b9d75c64c-nhv87            1/1      Running   0           23m
kube-system    kube-proxy-t285k                   1/1      Running   0           21m
monitoring     grafana-release-567d4456f5-5x9mx    0/1      Pending   0           6s29s
monitoring     prometheus-release-alertmanager-v   0/1      Pending   0           6m11s
monitoring     prometheus-release-kube-state-metric-59dc9d6fb-kjjc9 0/1      Pending   0           6m14s
monitoring     prometheus-release-prometheus-node-exporter-fx5dp    0/1      Pending   0           6m14s
monitoring     prometheus-release-prometheus-pushgateway-7f4f7c557-wbpzb 0/1      Pending   0           6m14s
monitoring     prometheus-release-server-796d7bd6c7-7f5d4           0/2      Pending   0           6m14s
manzana@devops:~$ kubectl cluster-info
Kubernetes control plane is running at https://4E84C37360783F207083E80A1AAE3E45.gr7.us-east-1.eks.amazonaws.com
CoreDNS is running at https://4E84C37360783F207083E80A1AAE3E45.gr7.us-east-1.eks.amazonaws.com/ap1/v1/namespaces/kube-system/services/kube-dns:proxy
To further debug and diagnose cluster problems, use 'kubectl cluster-info dump'.
```

Accedemos al cluster:

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

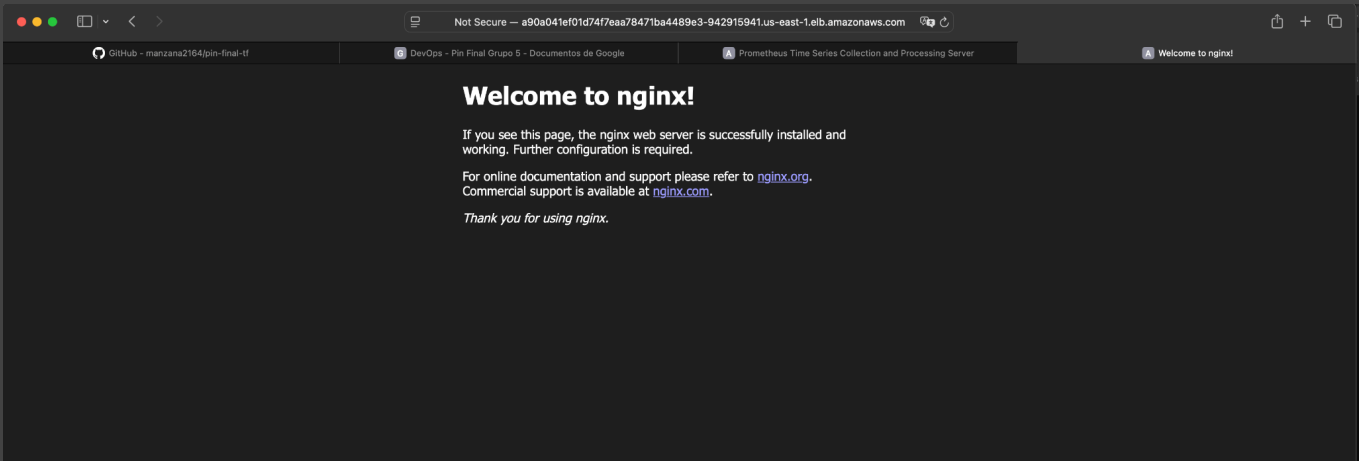
```
kubectl get pods -A
```

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     a6627b4bb066346aa895ec35f505809-1104680589.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:


```
a09e8bb22b4467baaf266910d91ab5-1015308082.us-east-1.elb.amazonaws.com
```


Grafana


Home


Bookmarks

Starred

Dashboards

Explore

Alerting

Connections

Add new connection

Data sources

Administration

Home

Welcome to Grafana

Need help? [Documentation](#) [Tutorials](#) [Community](#) [Public Slack](#)

Basic

The steps below will guide you to quickly finish setting up your Grafana installation.

TUTORIAL
DATA SOURCE AND DASHBOARDS

Grafana fundamentals

Set up and understand Grafana if you have no prior experience. This tutorial guides you through the entire process and covers the "Data source" and "Dashboards" steps to the right.

COMPLETE

Add your first data source

Learn how in the docs [🔗](#)

COMPLETE

Create your first dashboard

Learn how in the docs [🔗](#)

Remove this panel

Dashboards


Starred dashboards

Recently viewed dashboards


Kubernetes Cluster (Prometheus) ☆

Kubernetes cluster monitoring (via Prometheus) ☆


Latest from the blog



Mar 10
Grafana OnCall OSS in maintenance mode: your questions answered
At Grafana Labs, we believe in treating everyone with respect, and a core aspect of respect is clear and transparent communication. When we decided to move Grafana OnCall (OSS) into maintenance mode, we knew that along with the public announcement, there would be a lot of questions.



Mar 10
Incident response and on-call management in one app: Introducing Grafana Cloud IRM
At Grafana Labs, we're always searching for ways to develop products that give our users the best tooling to help in their day-to-day understanding of their systems.



Mar 09
Grafana Drilldown: first-class OpenTelemetry support now available for metrics
When we launched Grafana Drilldown, our queryless experience for quicker, easier insights into your telemetry, we focused first on Prometheus because it was—and is—such a great solution for storing time series data.

Accedemos a Prometheus:

a6627b4bb066346aa895ec35f5505809-1104680589.us-east-1.elb.amazonaws.com

Agregamos la source de Prometheus:

Grafana

Home

Bookmarks

Starred

Dashboards

Explore

Alerting

Connections

Add new connection

Data sources

Administration

Home > Connections > Data sources > prometheus

Q Search or jump to...

⌵

⌵

⌵

⌵

⌵

⌵

⌵

⌵

⌵

⌵

prometheus

Type: Prometheus

Type PrometheusAlertingSupportedExplore dataBuild a dashboard

SettingsDashboards

Configure your Prometheus data source below

Or skip the effort and get Prometheus (and Loki) as fully-managed, scalable, and hosted data sources from Grafana Labs with the free-forever Grafana Cloud plan.

NameprometheusDefault

Before you can use the Prometheus data source, you must configure it below or in the config file. For detailed instructions, [view the documentation](#).

Fields marked with * are required

Connection

Prometheus server URL *http://prometheus-release-server

Authentication

Authentication methods

Choose an authentication method to access the data source

Authentication method

No Authentication

TLS settings

Additional security measures that can be applied on top of authentication

Add self-signed certificate

TLS Client Authentication

Skip TLS certificate validation

HTTP headers

Pass along additional context and metadata about the request/response

Advanced settings

Additional settings are optional settings that can be configured for more control over your data source.

Advanced HTTP settings

Allowed cookiesNew cookie (hit enter to add)Add

TimeoutTimeout in seconds

Alerting

Manage alerts via Alerting UI

Interval behaviour

Scrape interval15s

Query timeout60s

Query editor

Default editorBuilder

Disable metrics lookup

Performance

Prometheus typeChoose

Cache levelLow

Incremental querying (beta)

Disable recording rules (beta)

Other

Custom query parametersExample: max_source_resolution=5m&timeout=

HTTP methodPOST

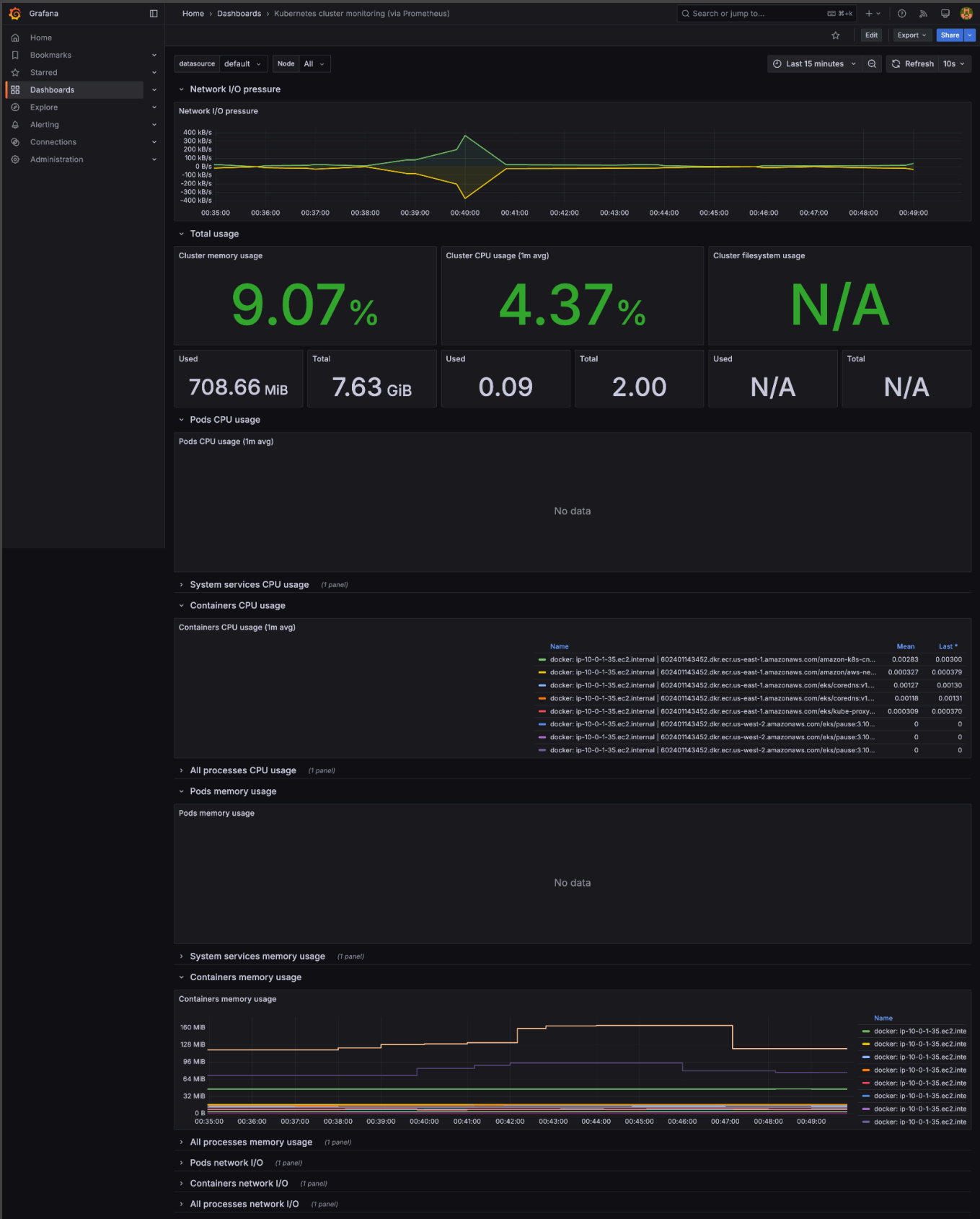
Use series endpoint

Exemplars

+ Add

DeleteSave & test

Creamos los dashboards por importación con los códigos **3119** y **6417**



Grafana

Home > Dashboards > Kubernetes Cluster (Prometheus)

Q Search or jump to...

⌵ ⌵+k ⌵+v ⌵+f ⌵+m ⌵+g ⌵+h ⌵+i ⌵+j ⌵+k ⌵+l ⌵+m ⌵+n ⌵+o ⌵+p ⌵+q ⌵+r ⌵+s ⌵+t ⌵+u ⌵+v ⌵+w ⌵+x ⌵+y ⌵+z

☆ Edit Export Share

node * namespace *

Dashboards Last 30 minutes Refresh

Cluster Health

Cluster Pod Usage	Cluster CPU Usage	Cluster Memory Usage	Cluster Disk Usage
N/A	N/A	N/A	N/A

Cluster Pod Capacity	Cluster CPU Capacity	Cluster Mem Capacity	Cluster Disk Capacity
<p>No data</p>	No data	No data	No data

Deployments

Panel plugin has no panel component

Deployment Replicas	Deployment Replicas - Updated	Deployment Replicas - Unavailable
7	7	0

Node

Number Of Nodes	Nodes Out of Disk	Nodes Unavailable
1	N/A	0

Pods

Pods Running	Pods Pending
10	0

Pods Failed	Pods Succeeded	Pods Unknown
0	0	0

Containers

Containers Running	Containers Waiting	Containers Terminated	Containers Restarts (Last 30 Minutes)
12	0	0	N/A

CPU Cores Requested by Containers	Memory Requested By Containers
N/A	N/A

Jobs

Jobs Succeeded	Jobs Succeeded	Jobs Failed
N/A		

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

```
OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS  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/sq-0334629b134ea682a" -> null
- description = "EKS Managed node group security group" -> null
- egress = [] -> null
- id = "sq-0334629b134ea682a" -> null
- ingress = [] -> null
- name = "mundose-node-group-eks-node-group-20250304061409002600000000" -> 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
}

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

Changes to Outputs:
- cluster_endpoint = "https://928407C1C365ECA877E2580C520A3E2F.gr7.us-east-1.eks.amazonaws.com" -> null
- cluster_name = "eks-cluster-mundose" -> null
- nginx_service_endpoint = "a044932d377254cdca080dcb4f117ab-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: y
SSH: 192.168.0.150 0 0 0 4

OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS  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, 60s elapsed]
module.eks.aws_eks_cluster.this[0]: Still destroying... [id=eks-cluster-mundose, 70s elapsed]
module.eks.aws_eks_cluster.this[0]: Still destroying... [id=eks-cluster-mundose, 80s elapsed]
module.eks.aws_eks_cluster.this[0]: Still destroying... [id=eks-cluster-mundose, 90s 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.module["ingress_self_coredns_tcp"]: Destroying... [id=sgrule-3848679672]
module.eks.aws_security_group_rule.module["ingress_cluster_443"]: Destroying... [id=sgrule-3813850990]
module.eks.aws_security_group_rule.module["egress_https"]: Destroying... [id=sgrule-1036271345]
module.vpc.aws_subnet.private[1]: Destroying... [id=subnet-9080bb1d37d0288f6]
module.eks.aws_iam_role_policy_attachment.this["arn:aws:iam::aws:policy/AmazonEKSClusterPolicy"]: Destroying... [id=eks-cluster-mundose-cluster-20250304061354613400000002-20250304061357077000000006]
module.eks.aws_security_group_rule.cluster["egress_nodes_kubelet"]: Destroying... [id=sgrule-2711647850]
module.eks.aws_security_group_rule.module["egress_ntp_udp"]: Destroying... [id=sgrule-282398482]
module.eks.aws_security_group_rule.module["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.module["ingress_cluster_kubelet"]: Destroying... [id=sgrule-33092393]
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 8s
module.eks.aws_security_group_rule.cluster["ingress_nodes_443"]: Destroying... [id=sgrule-283547140]
module.eks.aws_security_group_rule.module["egress_self_coredns_udp"]: Destroying... [id=sgrule-450790076]
module.eks.aws_security_group_rule.module["egress_https"]: Destruction complete after 1s
module.eks.aws_security_group_rule.cluster["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-b6f1a2a2d6619068e]
module.vpc.aws_subnet.private[1]: Destruction complete after 1s
module.eks.aws_security_group_rule.module["ingress_self_coredns_udp"]: Destroying... [id=sgrule-1094288855]
module.eks.aws_security_group_rule.module["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/AmazonEKSVPCKubernetesController"]: Destroying... [id=eks-cluster-mundose-cluster-20250304061354613400000002-20250304061357223900000007]
module.vpc.aws_subnet.private[0]: Destruction complete after 1s
module.eks.aws_security_group_rule.module["egress_ntp_tcp"]: Destroying... [id=sgrule-3793355759]
module.eks.aws_iam_role_policy_attachment.this["arn:aws:iam::aws:policy/AmazonEKSVPCKubernetesController"]: Destruction complete after 0s
module.eks.aws_iam_role.this[0]: Destroying... [id=eks-cluster-mundose-cluster-20250304061354613400000002]
module.eks.aws_security_group_rule.module["ingress_cluster_443"]: Destruction complete after 3s
module.eks.aws_iam_role.this[0]: Destruction complete after 3s
module.eks.aws_security_group_rule.module["ingress_cluster_kubelet"]: Destruction complete after 4s
module.eks.aws_security_group_rule.module["egress_ntp_udp"]: Destruction complete after 4s
module.eks.aws_security_group_rule.module["egress_cluster_443"]: Destruction complete after 5s
module.eks.aws_security_group_rule.module["egress_self_coredns_udp"]: Destruction complete after 6s
module.eks.aws_security_group_rule.module["egress_self_coredns_tcp"]: Destruction complete after 6s
module.eks.aws_security_group_rule.module["ingress_self_coredns_udp"]: Destruction complete after 7s
module.eks.aws_security_group_rule.module["egress_ntp_tcp"]: Destruction complete after 7s
module.eks.aws_security_group.cluster[0]: Destroying... [id=sg-0b10825d0240a98e]
module.eks.aws_security_group.module[0]: Destroying... [id=sg-0b10825d0240a98e]
module.eks.aws_security_group.cluster[0]: Destruction complete after 1s
module.eks.aws_security_group.module[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.
manzanadevops~/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**.