Introducción ECS, EKS, Kubernetes Native y re:Invent Recap

Eduardo Miranda,
Cloud Engineer, Globant

Gonzalo Vásquez
R&D Director, Waypoint

19 Diciembre, 2018

¿Qué es lo mejor de los contenedores?

Todo alrededor de los contenedores es genial!!

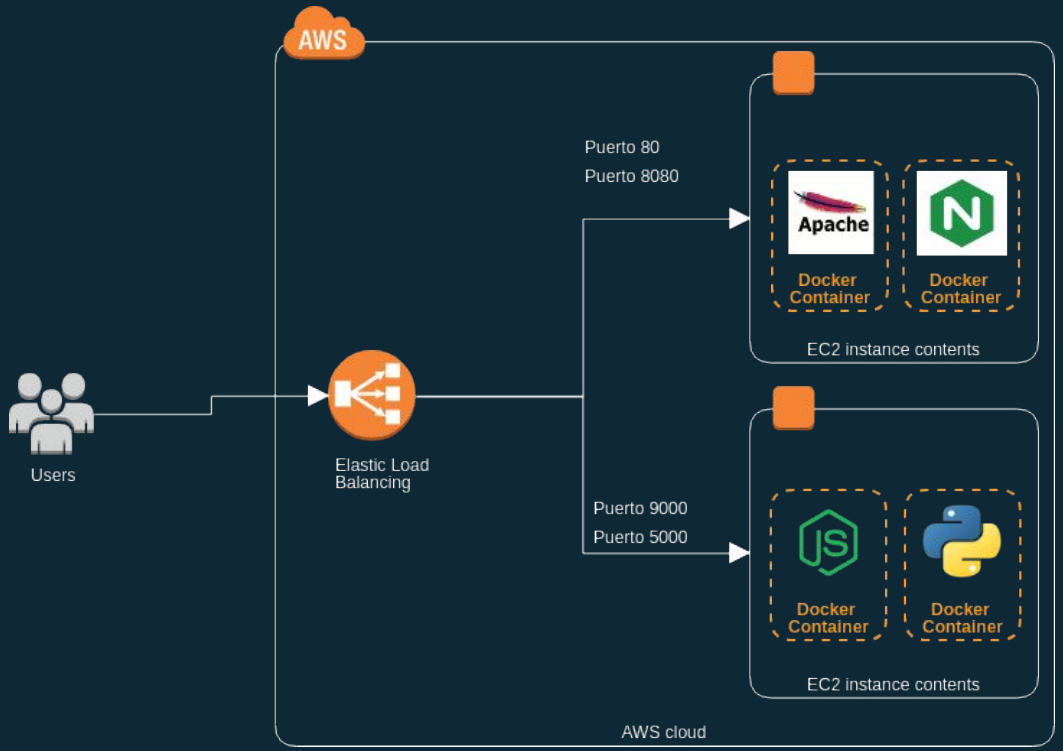
Son ligeros

Adaptables

Portable

Contenedores y microservicios van de la mano

Entonces, si tengo un contendor corriendo en mi instancia ¿Como podrá escalar?



waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

… y ¿Qué alternativas tenemos para la administración de contenedores en AWS?

Cómo puedo deployar mis contenedores sin afectar al servicio?

- Sin downtime

Cómo puedo mantener mis contenedores siempre disponibles?

- Programados, Restablecimiento

Cómo los contenedores pueden comunicarse entre ellos?

- Servicio de enlazado, descubrimiento por red

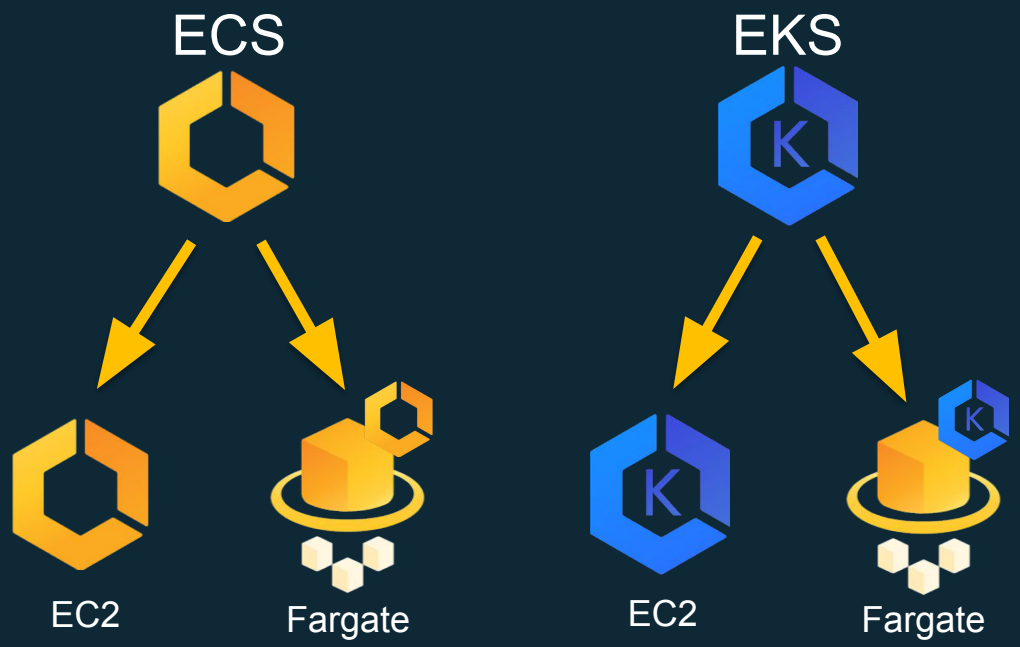
Cómo puedo configurar mis contenedores en tiempo de ejecución?

- Acceso vía consola y terminal

Cómo puedo hacer para optimizar el uso y cantidad de mis contenedores?

- Ajuste de asociación de recursos mediante el monitoreo continuo, escalamiento de contenedores por demanda

Nosotros podemos elegir:



Kubernetes Native

Kubernetes Operations
(kops)

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

Amazon EC2 Container Service (ECS)

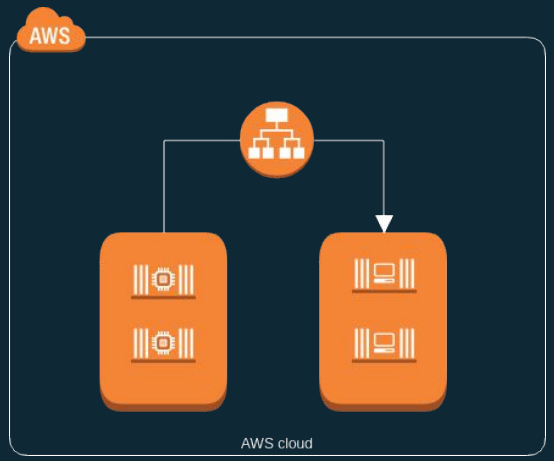
Amazon EC2 Container Service (ECS)

Instancias: cada una se registra al cluster y corre sus Task aquí.

Servicios: esta capa gestiona y asigna las tareas.

Task: contenedor envuelve y configura los procesos corriendo dentro de la instancia.

¿Cómo trabaja ECS?



Load Balancer: (ALB o ELB Classic) distribuyen el tráfico a los clusters.

Cluster: está hecho de una o más instancias EC2.

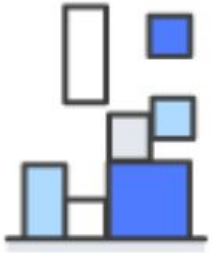
Cada **Instancia de Cluster** corre uno o más **Servicios**.

¿Qué ventajas tiene ALB sobre ELB?

Puedes definir reglas básicas para el direccionamiento del tráfico: Cuando dices enviar el tráfico a diferentes servicios basado en un endpoint, ¿no te parece genial?

Bonus: ALB permite asignar los puertos dinámicamente para la utilización de multi servicios.

Algunas características...



Amazon ECS Task Placement

IAM Roles for Tasks

Flexible scaling for performance

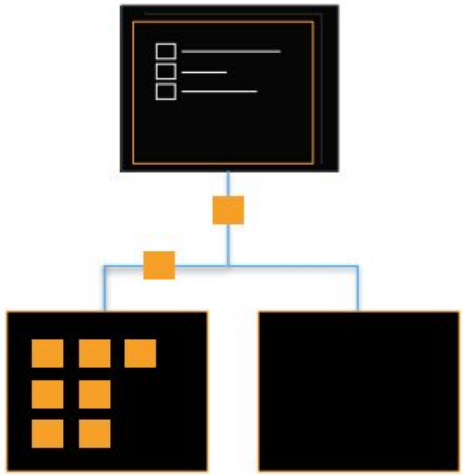
Amazon ECS Event Stream for Cloudwatch Logs

Fast, hassle-free deployments

Amazon ECS Task Placement

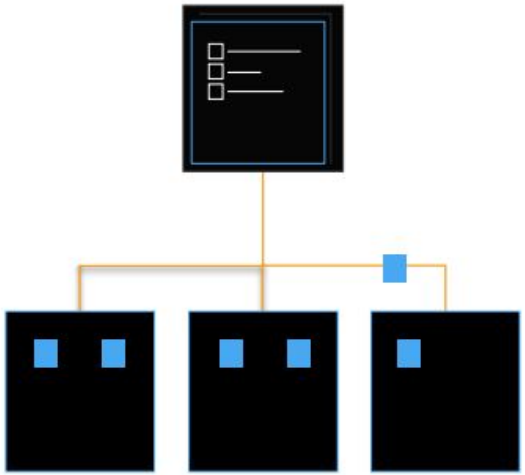
- Un task placement strategy es un algoritmo para seleccionar las instancias y la colocación de las tareas o para el término de ellas.
- un task placement constraint es una regla que se toma en consideración durante la colocación de la tarea.
- un task placement strategy y un task placement constraint puede utilizarse en conjunto.

Multiple Strategies son soportadas



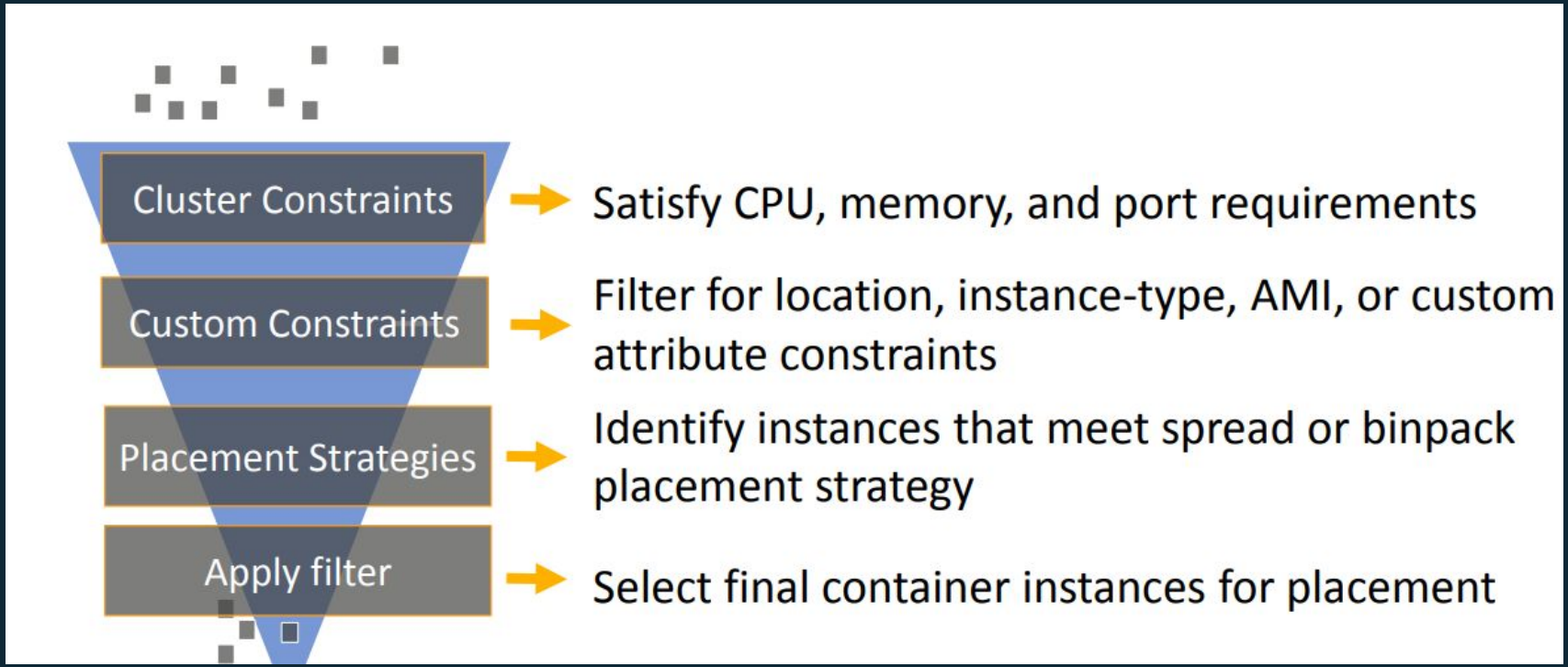
Binpacking

Random



Spread

Como trabaja..



Amazon ECS Event Stream for Cloudwatch Logs

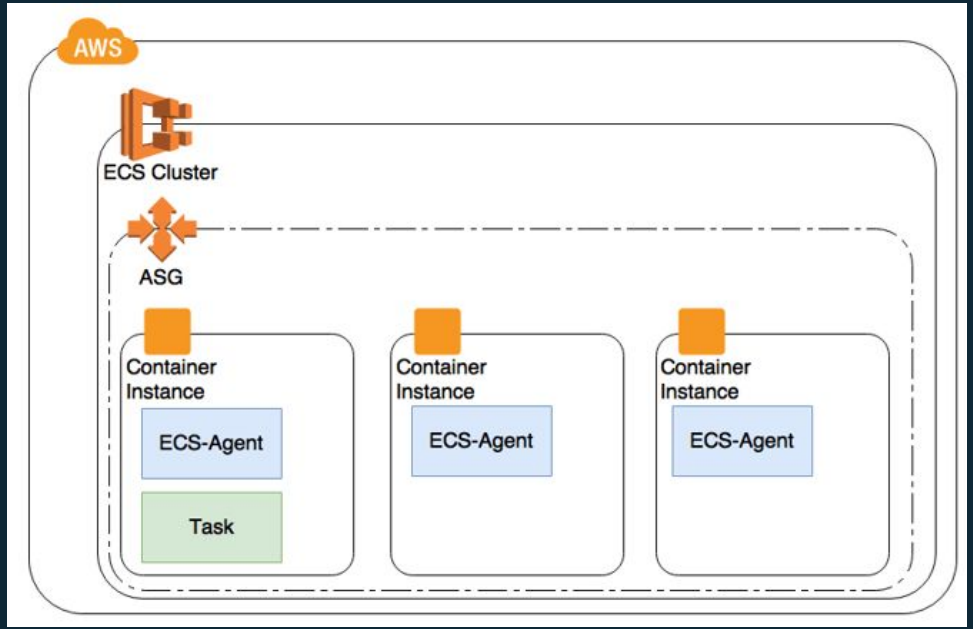
- Recibe en tiempo real las actualizaciones sobre el estado actual de los contenedores.
- Puedes programar acciones en base al estado del cluster generando eventos directamente en Lambda.

IAM Roles for ECS Tasks

- Se especifica los roles por contenedores en las tareas.
- Los contenedores pueden únicamente acceder al role que la tarea tenga asignada.
- **Autorización**: los contenedores no pueden acceder a otras credenciales definidas para otras tareas.
- **Auditabilidad**: Cloudtrail hace el trabajo por nosotros.

Flexibilidad de escalamiento

- El escalamiento de los servicios están basado en las alarmas detectadas por cloudwatch.
- EC2 Autoscaling Group nos ayuda a escalar nuestro cluster sin mayor inconveniente.



Kubernetes on AWS

Estadisticas...

57% de las cargas de trabajo en Kubernetes se Ejecutar en AWS.

— Cloud Native Computing Foundation

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

$ kubectl get tips –n meetup

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

GET api/v1/namespaces/meetup/tips/{1}

Nunca construir un cluster de kubernetes de la manera más difícil!

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

Opciones para configurar un cluster de Kubernetes en AWS.

Comunidad

- Kops – kubernetes-aws.io
- Kubeadm – Kit de Herramienta para arrancar los clusters
- Kubespray – set de herramientas para deployar K8s clusters.

Enterprise

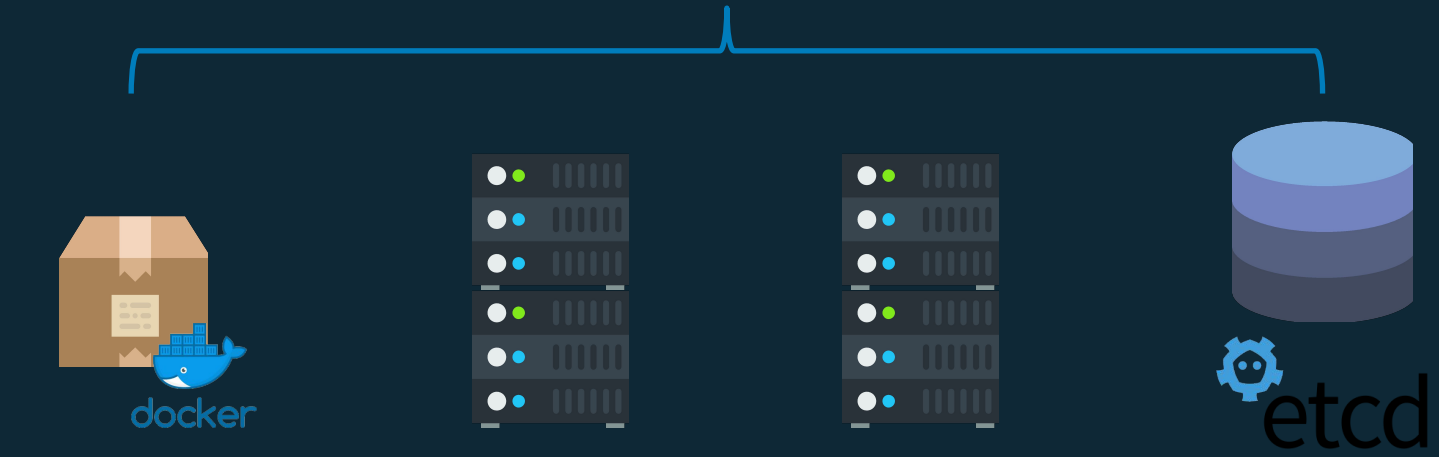
- Elastic Container Service for Kubernetes (EKS)

Otras opciones

- CloudFormation, Terraform, Ansible, Puppet

Kops

Puedes crearlo con Kops, pero la administración es tu responsabilidad.



Tus contenedores

Nodos Esclavos

Nodos Maestros

Almacenamiento del estado

waypoint®
LLEGAMOS MAS LEJOS

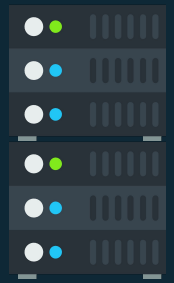
Globant
we are ready

aws

Responsabilidad basado en EKS con EC2

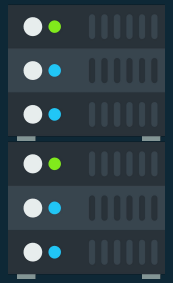
Tú

Tus contenedores

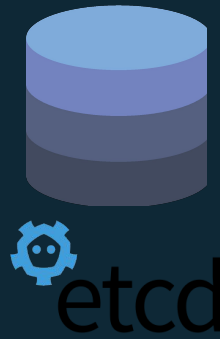


Nodos
Esclavos

Amazon EKS



Nodos
Maestros



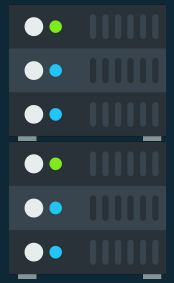
Almacenamiento
del estado

Manejo total de EKS

Tú

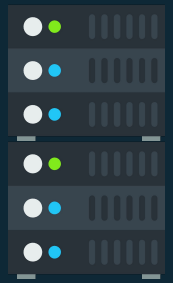
Tus contenedores

AWS Fargate



Nodos
Esclavos

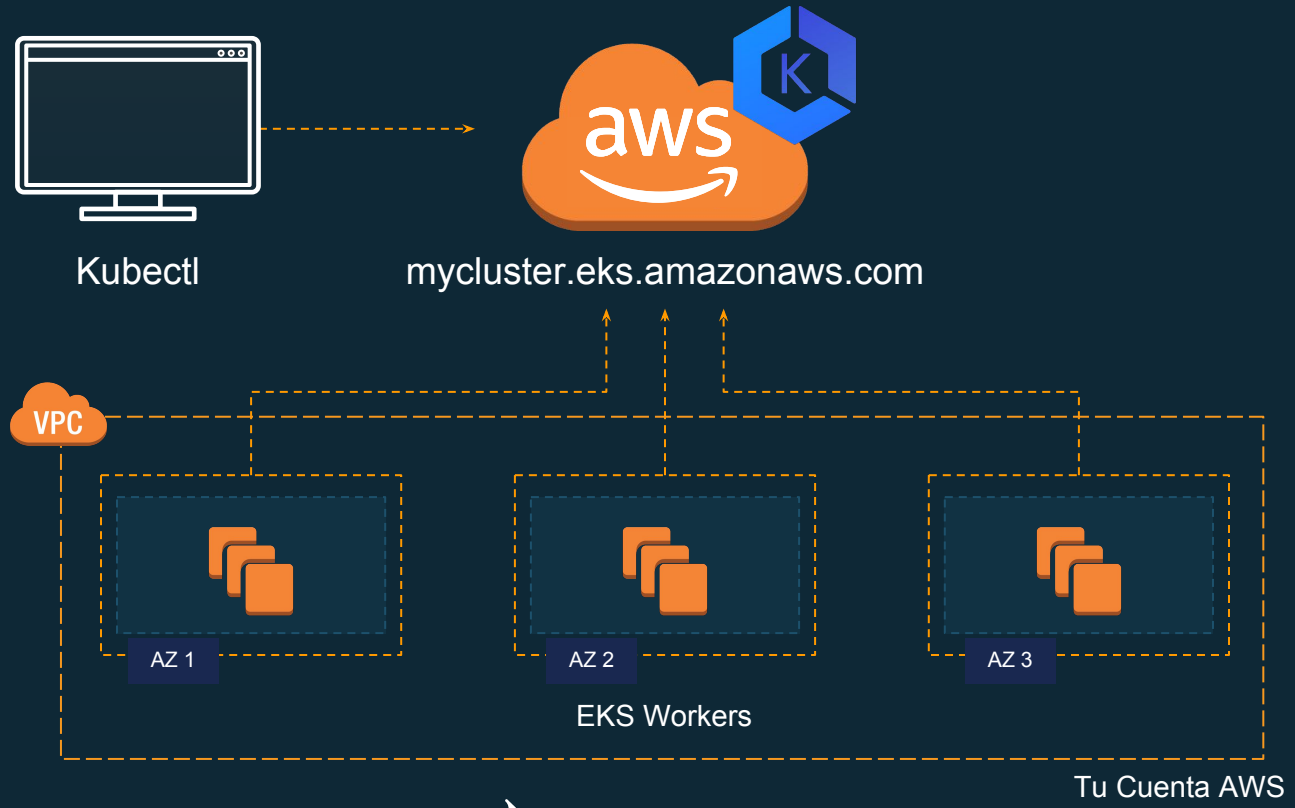
Amazon EKS



Nodos
Maestros

Almacenamiento
del estado

Amazon EKS

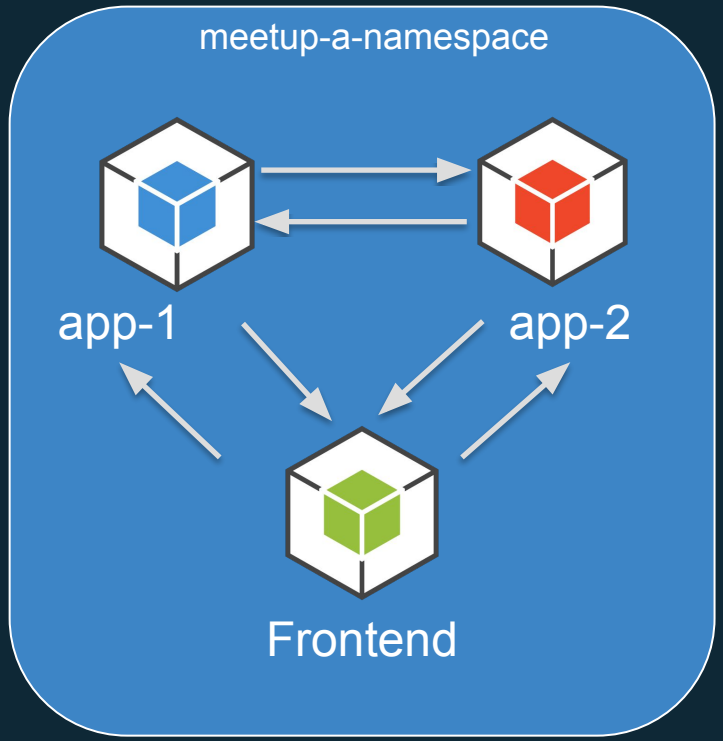

Kubectl
mycluster.eks.amazonaws.com
VPC
AZ 1
AZ 2
AZ 3
EKS Workers
Tu Cuenta AWS

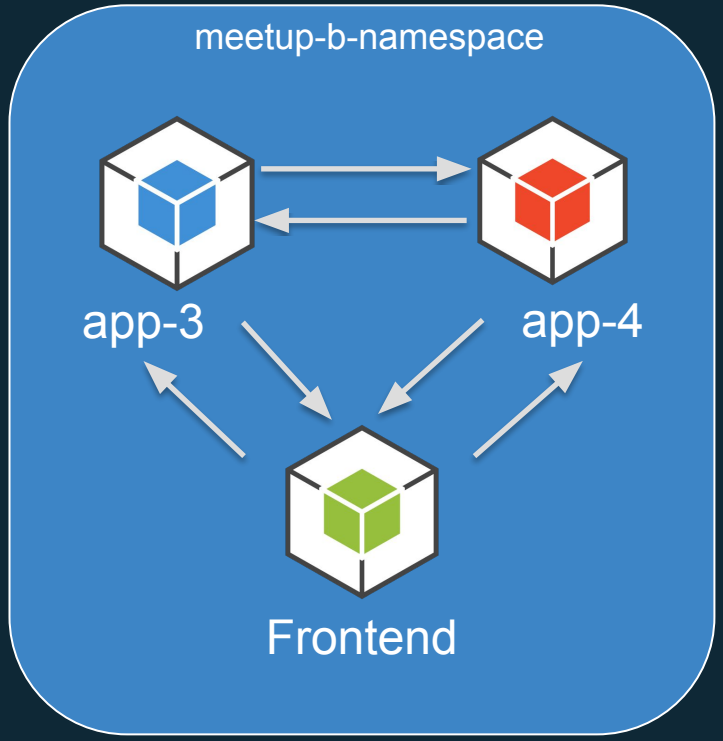
kubectl create namespace meetup

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

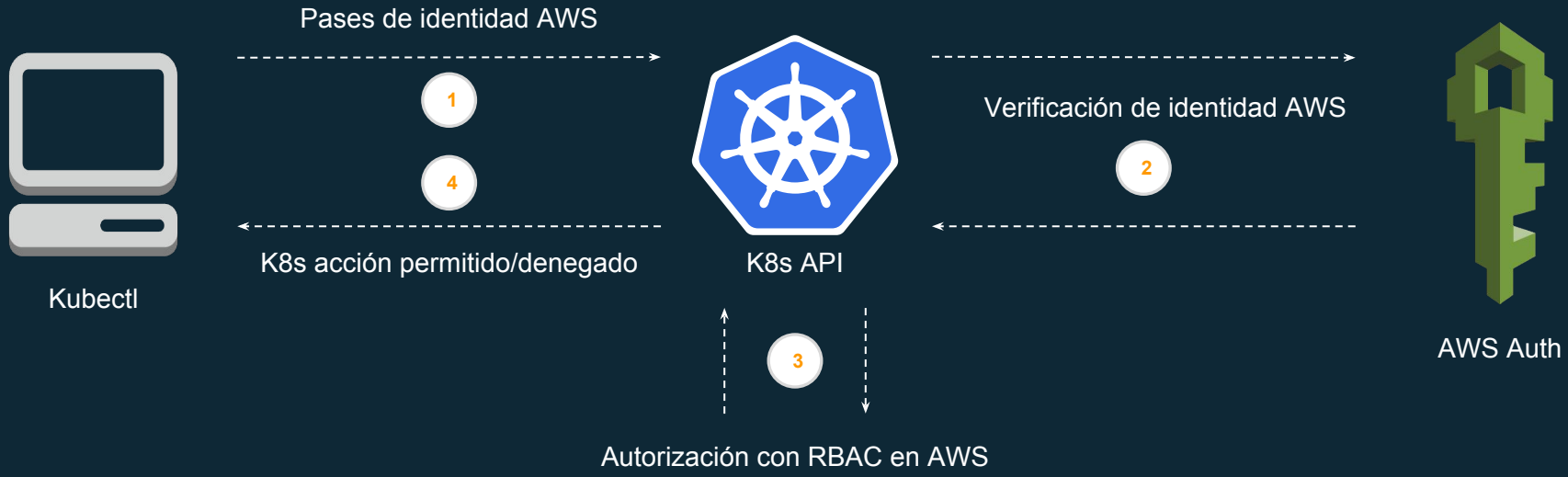




GET api/v1/namespaces/meetup/tips/{2}

Asegurar RBAC esté habilitado en tu Cluster

EKS: IAM Autentificación + Kubectl



waypoint®
LLEGAMOS MAS LEJOS

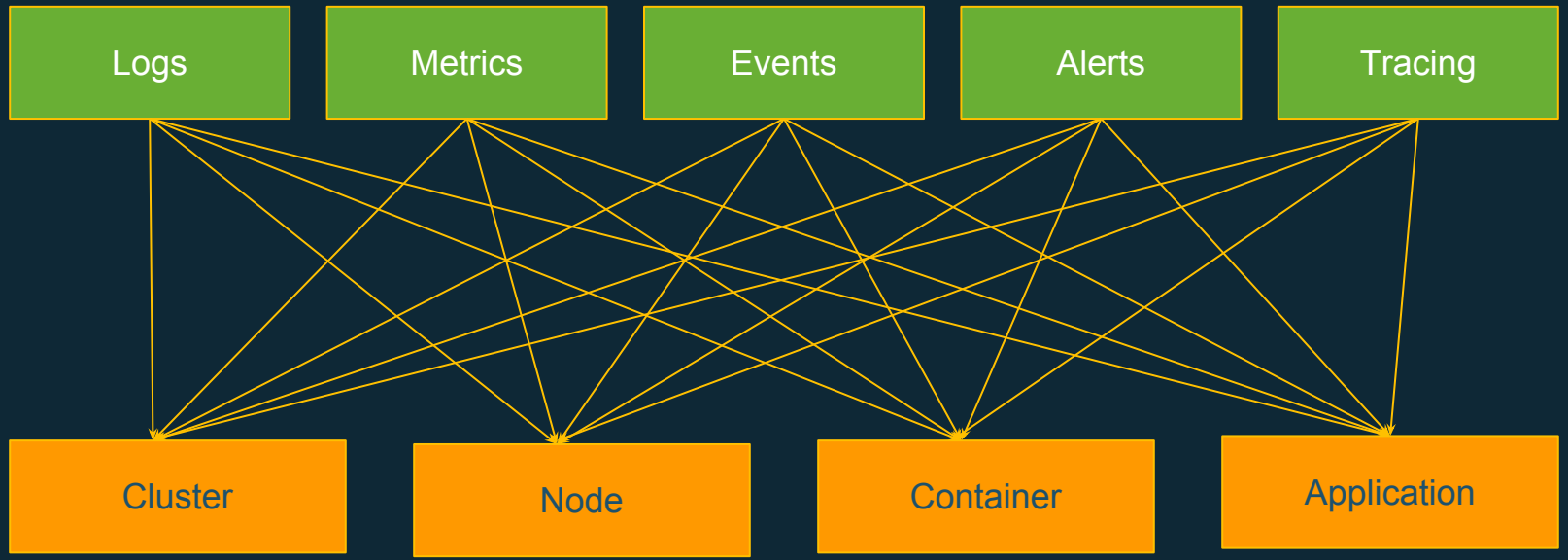
Globant
we are ready

aws

GET api/v1/namespaces/meetup/tips/{3}

Log y Monitoreo de todos los recursos!

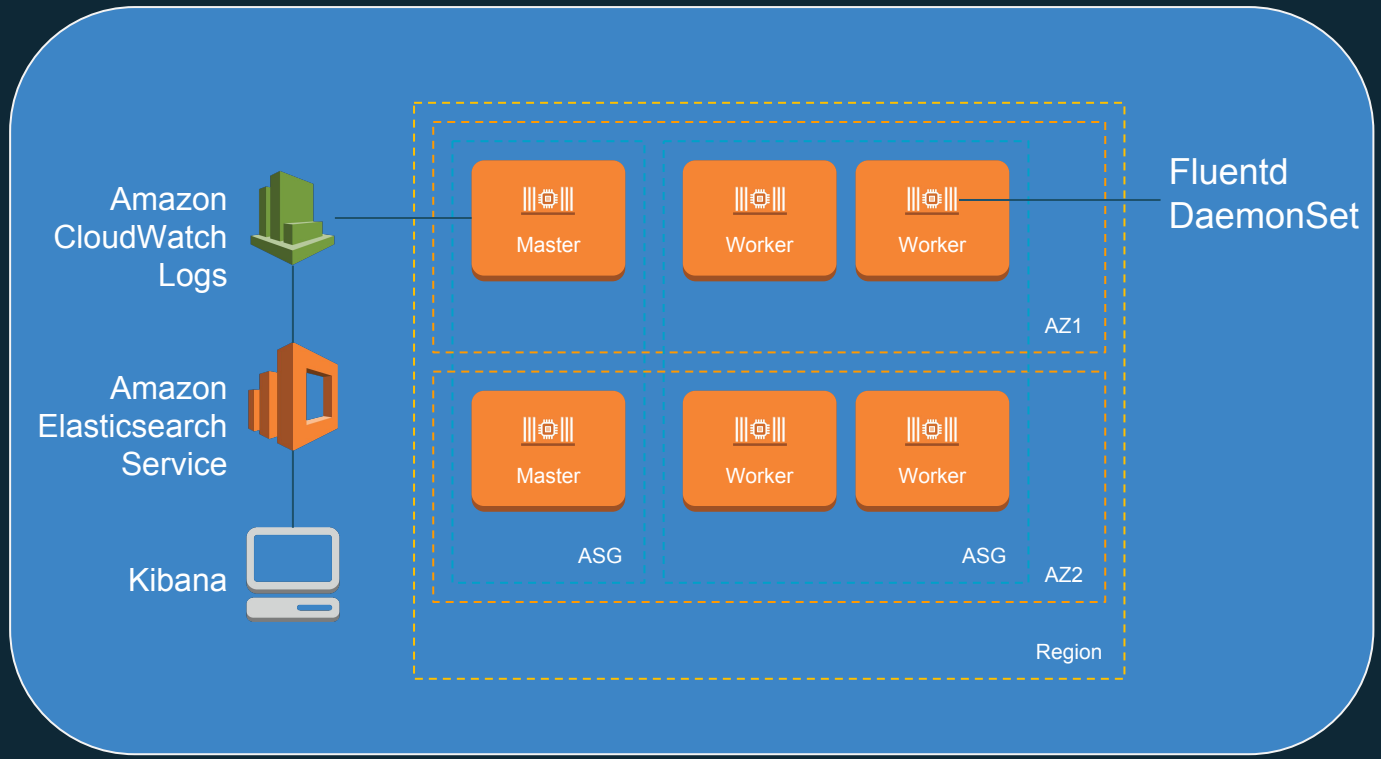
Visibilidad de tu Cluster Kubernetes



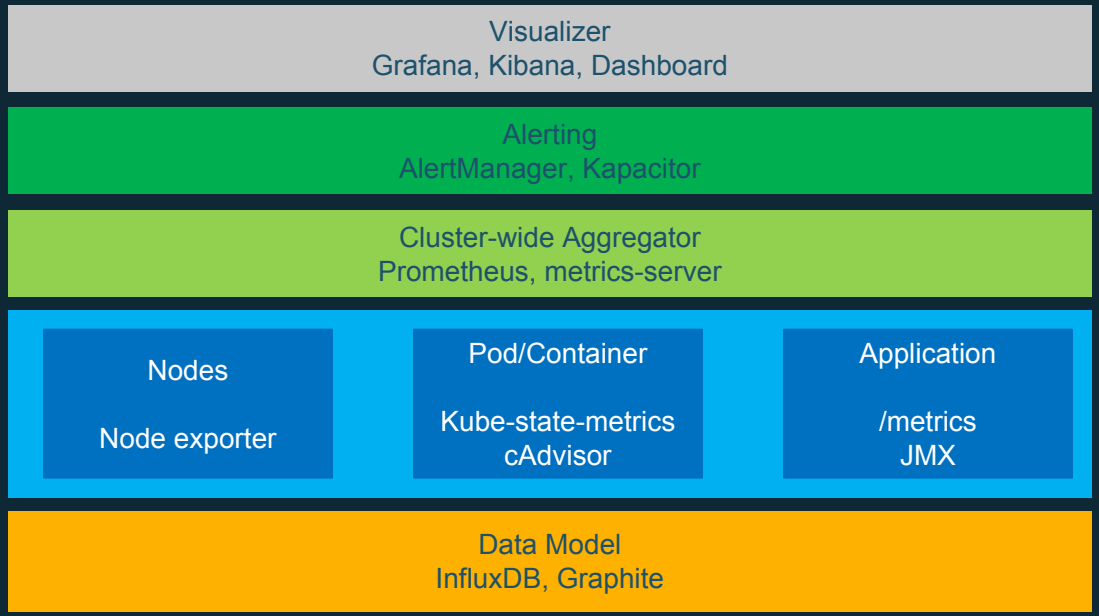
Logs

Kubectl logs

Elasticsearch (index),
Fluentd (store), and
Kibana (visualize)



Metricas

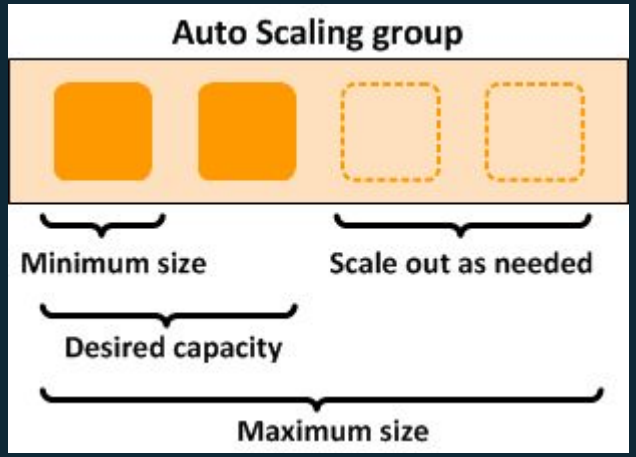


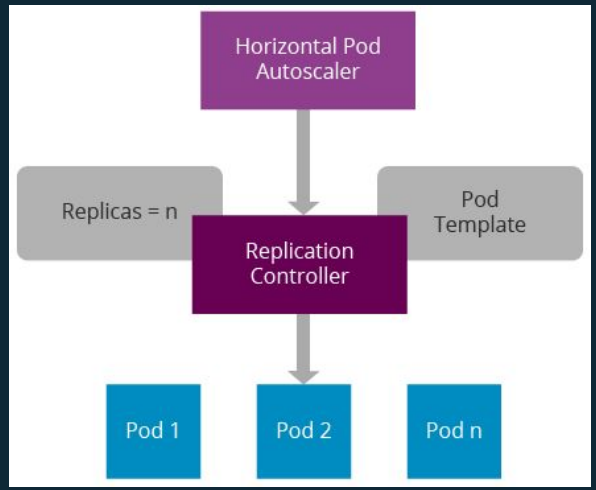
GET api/v1/namespaces/meetup/tips/{4}

Opciones de escalamiento bajo demanda con Autoscaling

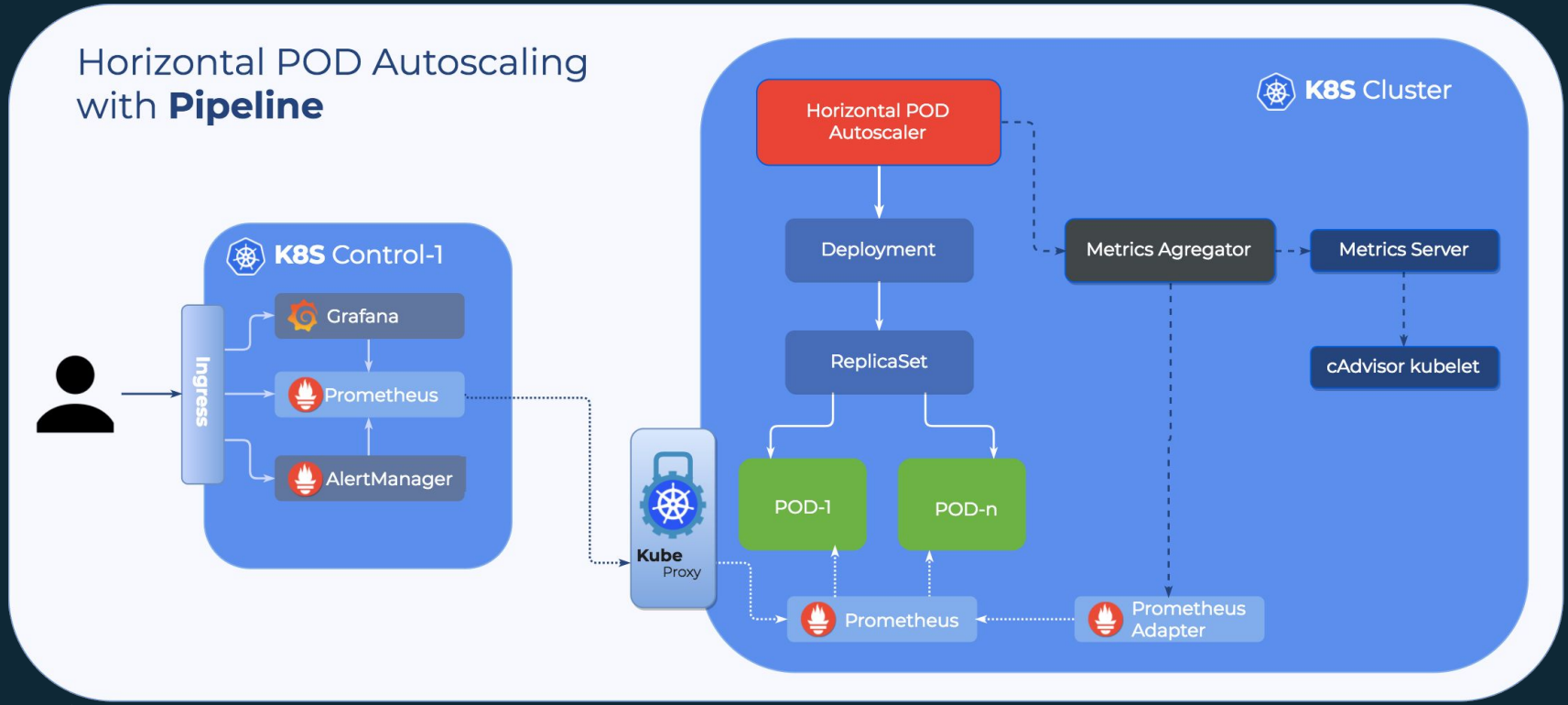
Alternativas de Autoscaling

- Nativo Autoscaling de AWS
- Autoscaler de k8s Cluster





HPA k8s Cluster



GET api/v1/namespaces/meetup/tips/{5}

Construir*, *Enviar*, *Desplegar …

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

CI/CD de aplicaciones dentro de Kubernetes

Jenkins

AWS CodePipeline, AWS CodeCommit, AWS CodeBuild

OSS: Spinnaker, Skaffold

AWS partners

- GitLab
- Shippable
- CircleCI
- Codeship

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

Es momento de...

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

Premiar a nuestros participantes!!

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

Problema N°1 - ECS

1.- Si quiero especificar la instancia en donde se deberá desplegar mi contenedor, ¿Qué tipo de **Placement Strategy** debería utilizar para lograrlo?

¿?

Problema N°2 - Kubernetes

2.- Quiero obtener los logs de mis aplicaciones corriendo en mi cluster y además los logs generados por el mismo cluster con el objetivo de visualizarlos posteriormente en Kibana, en base a la sección de logs presentada, como se llama el **Data Collector** que corre como un **DaemonSet** dentro de **Kubernetes** para la **recolección de los logs**?

¿?

re:Invent Recap

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

Calentando motores

Midnight Madness

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

Launches, Preview & Pre-Announcements

https://aws.amazon.com/es/new/reinvent/

- AWS Robomaker
- AWS DataSync
- AWS Transfer for SFTP
- S3 Intelligent-Tiering
- S3 Batch Operations
- Snowball Edge Compute Optimized
- AWS Amplify Console
- AWS Global Accelerator
- AWS Transit Gateway
- Amazon EC2 A1 Instances
- Amazon EC2 C5n Instances
- Amazon EC2 P3dn instances
- Elastic Fabric Adapter
- Dynamic Training with Apache MXNet on AWS
- Amazon Sagemaker Neo
- Firecracker
- KMS Custom Key Store
- AWS IoT SiteWise
- Amazon EBS Doubles Max

Launches, Preview & Pre-Announcements

https://aws.amazon.com/es/new/reinvent/

- Performance of io1 Volumes
- AWS IoT Events
- AWS IoT Things Graph
- S3 Object Lock
- Private Marketplace
- AWS Marketplace for Containers
- Amazon Comprehend Medical
- AWS Ground Station
- ML Insights for QuickSight
-

- Dashboard embedding in Amazon QuickSight
- DynamoDB transactions
- AWS Elemental MediaConnect
- S3 PUT to Glacier
- CodeDeploy Blue/Green Deployment Support for ECS
- CodePipeline: ECR as a source action
- Amazon Kinesis Data Analytics for Java applications

Launches, Preview & Pre-Announcements

https://aws.amazon.com/es/new/reinvent/

- CloudWatch Logs Insights
- Amazon S3 Glacier Deep Archive
- Amazon FSx for Windows File Server
- Amazon FSx for Lusre
- AWS Control Tower
- AWS Security Hub
- Amazon Lake Formation
- DynamoDB On-Demand
- Amazon Timestream
- Amazon Quantum Ledger Database
- Amazon Managed Blockchain
- Amazon Elastic Inference
- AWS Inferentia
- Amazon Sagemaker Ground Truth
- AWS Marketplace for ML
- Amazon Sagemaker RL
- AWS DeepRacer
- Amazon Textract
- Amazon Personalize

Launches, Preview & Pre-Announcements

https://aws.amazon.com/es/new/reinvent/

- AWS Well-Architected Tool
- Amazon Forecast
- AWS Outposts
- EFS Multi-VPC Access
- Amazon RDS on VMware
- On-Demand Hibernated
- AWS Cloud Map
- AWS App Mesh
- Pre-built scikit-learn container
- AWS License Manager
- Custom Runtimes for Lambda
- Ruby support for Lambda
- Lambda Layers
- Nested Applications using Serverless Application Repository
- Step Functions service integrations
- WebSocket support for API Gateway
- ALB Support for Lambda
- Amazon Managed Streaming for Kafka

AWS Transfer for SFTP

Fully managed SFTP service for Amazon S3

Seamless migration of existing workflows

Fully managed in AWS

Secure and Compliant

Native integration with AWS services

Cost-effective

Simple to use

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

Amazon S3 Object Lock—What is It?

- New S3 feature that protects data from being overwritten or deleted in order to support regulatory compliance requirements (“WORM”)
- Two modes—Governance Mode & Compliance Mode
  - For Compliance Mode, objects cannot be modified or deleted by any user, including the root account. Once this is set, it cannot be modified
  - For Governance Mode, objects can only be deleted by the AWS accounts that have explicitly been granted permission through IAM policies
- Set at the bucket level—works with lifecycle (to S3-IA/Glacier)

Amazon S3 Intelligent Tiering—What is It?

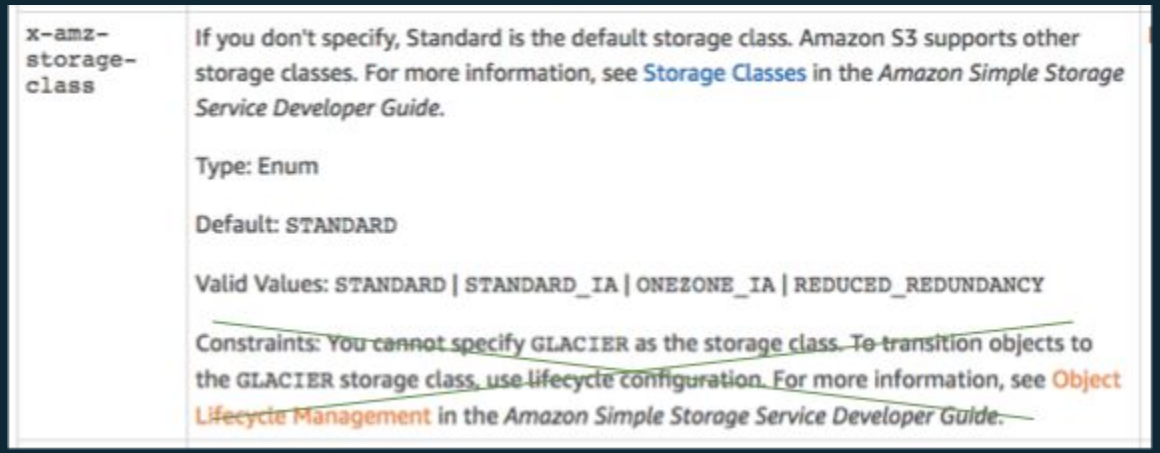
- New S3 Storage Class that automatically optimizes storage costs for data with changing access patterns
- Stores objects in two access tiers
  - One optimized for frequent access priced the same as S3-Standard
  - One optimized for infrequent access priced the same as S3-Infrequent Access
- Automatically determines which tier to use based on access patterns—no lifecycle policies needed
- Small monthly per object management fee / no per-GB access charges

S3 Glacier Deep Archive

- A pre-announcement
- Offline storage class for preservation, compliance, and DR where likelihood of recall is low and not sensitive to SLA
- Full functionality: 11 9's (3-AZ), Compliance/WORM, lifecycle, direct PUT, etc
- 8-15 hour retrieval
- Pricing targeted to be less than half of Glacier
- Targeting offsite vaulting services
- Offline tape migrations supported today via partners

S3 Glacier Direct PUT to Glacier Class

- Previously to upload to Glacier via S3...
- lifecycle policies including “0-day”
- Nondeterministic window where read method changes
- 2-layers of transaction fees



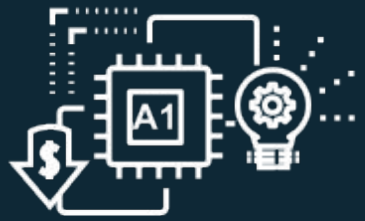
`x-amz-storage-class`	If you don't specify, Standard is the default storage class. Amazon S3 supports other storage classes. For more information, see Storage Classes in the *Amazon Simple Storage Service Developer Guide*. Type: Enum Default: `STANDARD` Valid Values: `STANDARD` | `STANDARD_IA` | `ONEZONE_IA` | `REDUCED_REDUNDANCY` Constraints: You cannot specify `GLACIER` as the storage class. To transition objects to the `GLACIER` storage class, use lifecycle configuration. For more information, see Object Lifecycle Management in the *Amazon Simple Storage Service Developer Guide*.

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

New EC2 Instances

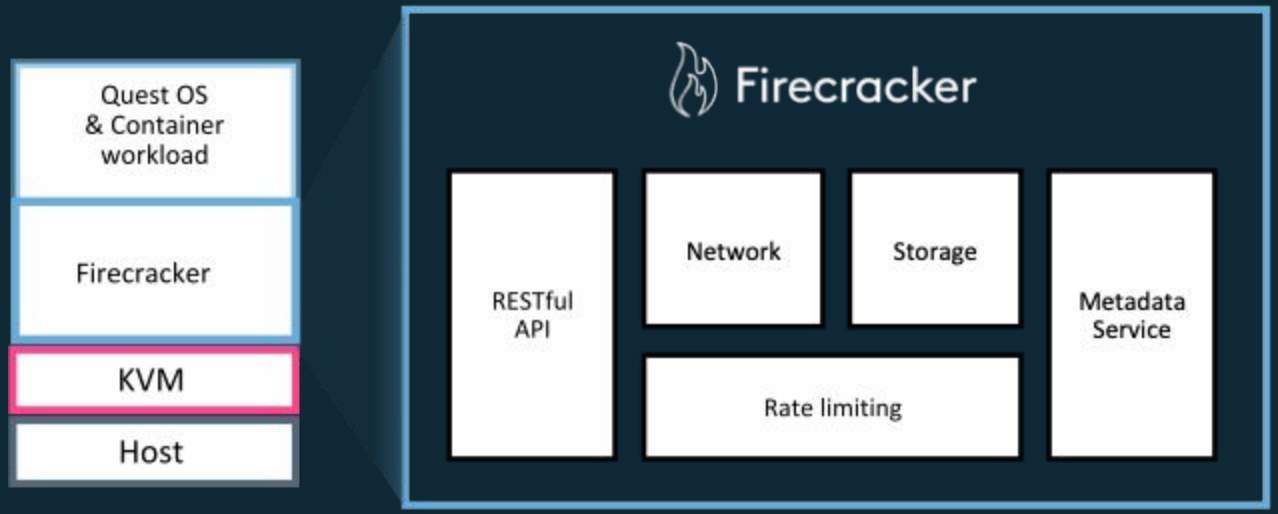


- Lower cost for scale-out workloads
- ARM-based development platform
- AWS Graviton Processor

- Faster analytics and big data workloads
- Lower costs for network-bound workloads
- 100 Gbps network throughput

- 100 Gbps network throughput
- NVMe-based SSDs
- 96 vCPUs, 768 GB RAM, 8 x Tesla V100 GPU

Firecracker
(What powers Lambda and Fargate)



Firecracker microVMs have the same security as KVM VMs

Designed for low overhead, high density, and fast start times

Built-in fair sharing

Apache 2.0 OSS
https://github.com/firecracker-microvm/firecracker

AWS Global Accelerator

Improve availability and performance for internet applications used by a global audience

- Static Anycast IP addresses
  - Never change over the lifetime of an accelerator
  - Safe to put in DNS/firewall/whitelist etc.

- Client traffic ingresses via closest available Edge location
- Route client to closest healthy Endpoint (ELB or Elastic IP)
- Traffic uses AWS Global Network from Edge to Region

AWS Control Tower

- The easiest way to set up and govern a secure, compliant, multi-account environment (Landing Zone)
  - Multi-account structure with AWS Organizations
  - Centrally-managed identities through AWS SSO or Microsoft AD
  - Centralized logging with AWS CloudTrail and AWS Config
  - Account factory through Service Catalog

Automated Landing Zone with best-practices blueprints

Guardrails for policy enforcement

Dashboard for continuous visibility

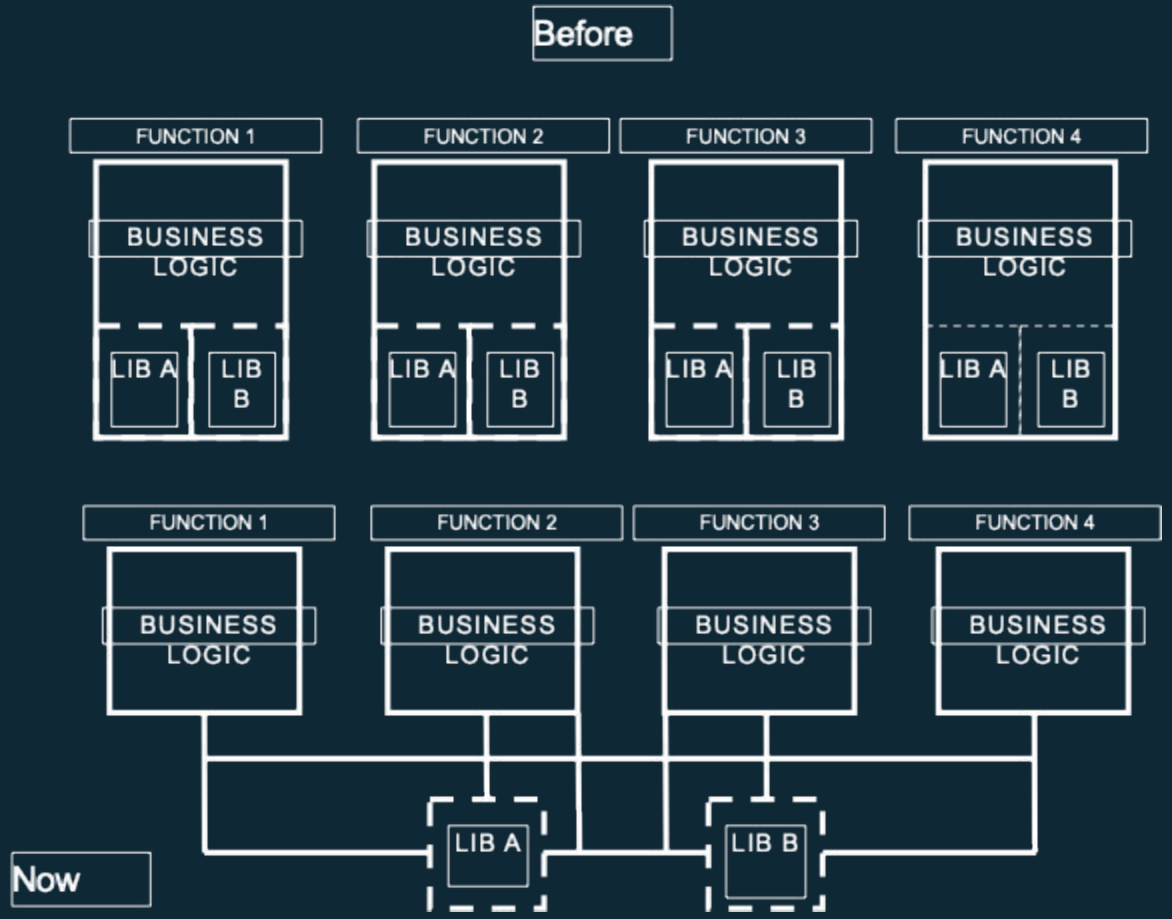
waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

Lambda Layers

Extend the Lambda execution environment with any binaries, dependencies, or runtimes



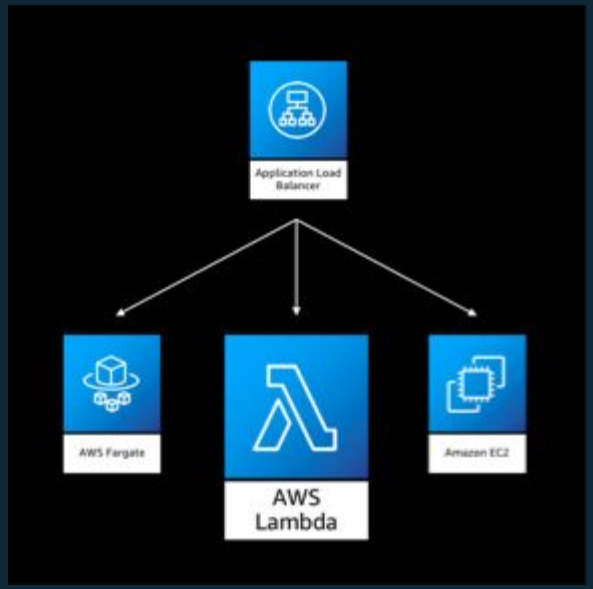
waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

ALB Support for Lambda

Integrate Lambda functions into existing web architectures



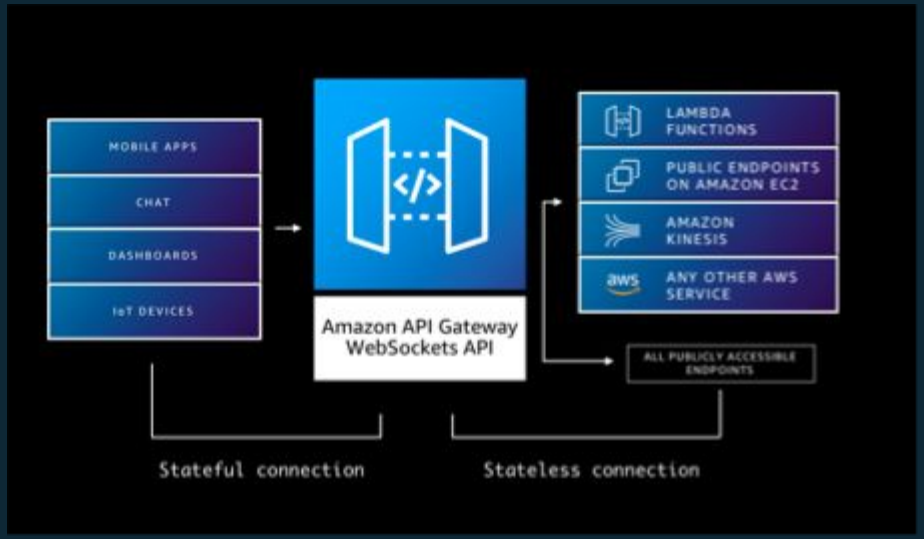
waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

WebSocket support for API Gateway

Build real-time two way communication applications



waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

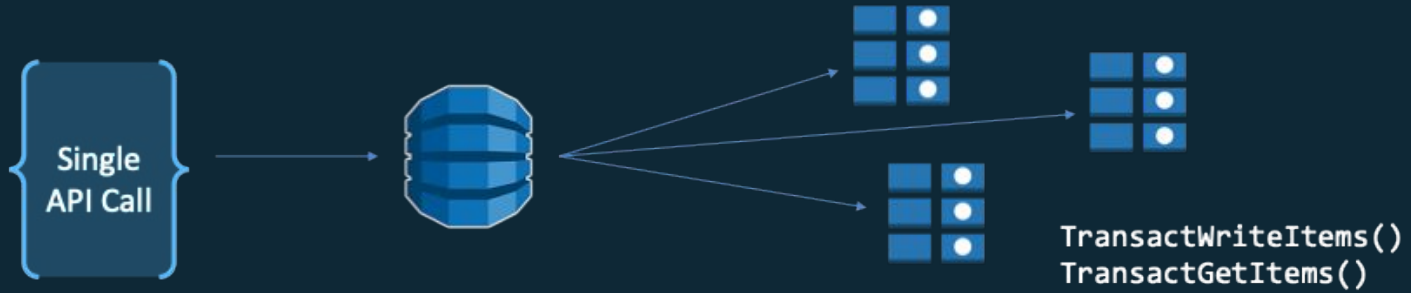
aws

Introducing AWS RoboMaker

https://twitter.com/awsreinvent/status/1066966596546060289

DynamoDB transactions

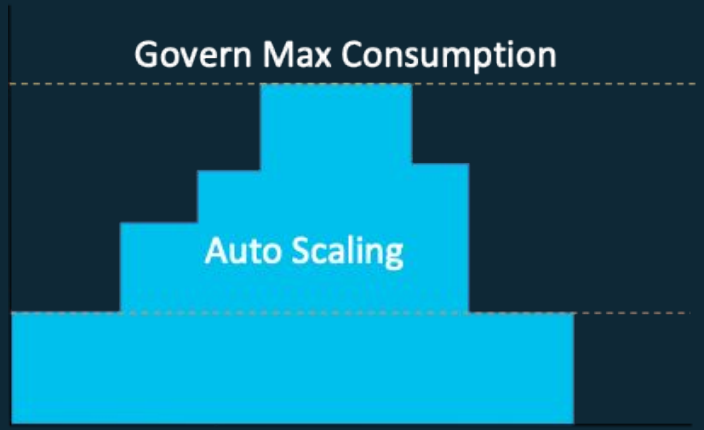
Simplify your code by executing multiple, all-or-nothing actions within and across tables with a single API call.



- Provides atomicity, consistency, isolation, and durability (ACID) in DynamoDB.
- You can perform transactions both within and across multiple DynamoDB tables.
- Native, server-side solution that provides better performance and lower costs than client-side libraries.

DynamoDB: Capacity managed for you

Provisioned



Set a Minimum

On-Demand

Start at Zero

Amazon Timestream (Preview)

- Fast, scalable, and fully managed time series database

Typical Use Cases: Application events, IoT Sensor Readings and DevOps data

1,000x faster at 1/10th the cost of relational databases

Collect fast moving time-series data from multiple sources at the rate of millions of inserts per second

Trillions of daily events

Capable of processing trillions of events daily; the adaptive query processing engine maintains steady, predictable performance

Analytics optimized for time series data

Built-in analytics for interpolation, smoothing, and approximation to identify trends, patterns, and anomalies

Serverless

No servers to manage; time-consuming tasks such as hardware provisioning, software patching, setup, & configuration done for you

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

Amazon Managed Blockchain features

Fully managed
Create a blockchain network in minutes

HYPERLEDGER
FABRIC
ethereum

Open-source variety
Support for two frameworks

Decentralized
Democratically govern the network

Reliable & scalable
Backed with Amazon QLDB technology

Low cost
Only pay for resources used

Integrated
Send data to Amazon QLDB
for secure analytics

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

QLDB (Preview)

- Fully managed ledger database
- Track and verify history of all changes made to your application's data

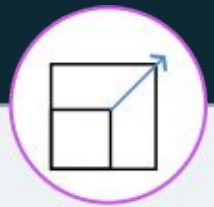
Immutable and transparent

Append-only, immutable journal tracks history of all changes which cannot be deleted or modified. Get full visibility into entire data lineage

Cryptographically verifiable

All changes are cryptographically chained and verifiable

Highly scalable



Executes 2 – 3X as many transactions than ledgers in common blockchain frameworks

Easy to use

Flexible document model, query with familiar SQL-like interface

Purpose-built databases

Relational

Key-value

Document

In-memory

Graph

Time-series

Ledger

Amazon RDS

Aurora Community Commercial

DynamoDB

ElastiCache

Neptune

Timestream

Quantum

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

Para conversar

- Amazon Lake Formation
- AWS DeepRacer
- AWS Well-Architected Tool

Eventos múltiples

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

Personajes

A Cloud Guru Founder
@KroonenburgRyan

AWS Serverless Hero
@theburningmonk

Highlights

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

Highlights

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws

Gracias!

e.miranda@globant.com
gvasquez@waypoint.cl

waypoint®
LLEGAMOS MAS LEJOS

Globant
we are ready

aws