SILIN

Jikkosoft
Innovating your world

ARQUITECTURA COMO SERVICIO DE SILIN

312 282 2189
info@jikkosoft.com
www.jikkosoft.com

CONTENIDO

Introducción: 3
- Propósito 3
- Alcance 3
- Definiciones, abreviaturas y acrónimos 3
- Definiciones 3
- Acrónimos 4
- Referencias 5
  - Amazon Elastic Container Service - User Guide 5
  - Amazon Virtual Private Cloud - User Guide 5
  - Elastic Load Balancing - Application Load Balancers 5
  - Amazon Simple Storage Service API Reference 5
  - Terraform Documentation 5
  - Gitlab CI/CD 5
  - Referencia y Glosario de AWS 5
- Descripción: 6

Representación de la arquitectura: 6

Metas y restricciones de la arquitectura: 6
- Metas 6
- Restricciones del Sistema 6

Modelo conceptual de la arquitectura como servicio SILIN: 7
- Vista General Infraestructura Cloud. 8

Modelo conceptual de la arquitectura de micro servicios: 8
- Vista infraestructura de micro servicios. 9

Modelo detallado de la arquitectura para SILIN. 9
- Vista detallada de la arquitectura para SILIN. 10

Rendimiento y respaldo. 11
- Rendimiento 11
- Respaldo 12

Introducción:

Propósito

El siguiente documento pretende dar una visión general de la arquitectura desplegada para el sistema SILIN 2.0, representado a través de una serie de vistas arquitectónicas con base en el diseño lógico de la infraestructura.

Alcance

En este documento se detallan dos vistas lógicas de la arquitectura para el sistema SILIN 2.0 soportadas en el proveedor de nube **Amazon Web Services** como actor principal. Para la elaboración del mismo se contempló una arquitectura multicapa y multistage para asegurar el perímetro de red del sistema y despliegues continuos versionados para registros y control.

Definiciones, abreviaturas y acrónimos

Se proveen definiciones y acrónimos de términos utilizados en este documento que aseguran la correcta interpretación del lector.

Definiciones

Amazon EC2	Servicio web para iniciar y administrar instancias de Linux/UNIX y Windows.
Amazon ECS	Servicio de administración de microservicios docker en un clúster nativo de AWS.
Amazon RDS	Servicio web que facilita la configuración, el funcionamiento y el escalado de una base de datos relacional en AWS.
Amazon S3	Almacenamiento lógico que se puede usar para almacenar y recuperar cualquier cantidad de datos en AWS.

Zona de Disponibilidad	Ubicación distinta dentro de una región que está aislada de los errores que se producen en otras zonas de disponibilidad.
Amazon Cloud Map	Servicio utilizado para crear y mantener un mapa de los recursos y servicios de backend.
Terraform	Software de infraestructura como código para despliegues en la arquitectura como servicio SILIN.
API Gateway	Proporciona punto de acceso para la creación y la implementación de sus propias API HTTP y de WebSocket.
Repositorio	Espacio centralizado donde se almacena, organiza, mantiene y difunde información digital, habitualmente archivos informáticos.
Docker	Es un sistema operativo para contenedores
CNAME	Es un tipo de registro DNS que asigna un alias a un nombre de dominio auténtico o canónico.
CloudFront	Agiliza la distribución de contenido web estático y dinámico, como archivos .html, .css, .php, imágenes y archivos multimedia.
CloudFlare	Red de entrega de contenido, servicios de seguridad y servicios de servidores de nombres de dominio distribuidos.

Acrónimos

ECS	Elastic Container Services
EC2	Elastic Compute Cloud
VPC	Virtual Private Cloud
VPN	Virtual Private Network
ACL	Control Access List
CDN	Content Delivery Network
ALB	Application Load Balancer
CNAME	Canonical Name
IaC	Infrastructure as Code

Referencias

La arquitectura desplegada sigue los lineamientos de buenas prácticas de los siguientes documentos:

Amazon Elastic Container Service - User Guide
https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ecs-dg.pdf

Amazon Virtual Private Cloud - User Guide
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ug.pdf

Elastic Load Balancing - Application Load Balancers
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/elb-ag.pdf

Amazon Simple Storage Service API Reference
https://docs.aws.amazon.com/AmazonS3/latest/API/s3-api.pdf

Terraform Documentation
https://www.terraform.io/docs/index.html

Gitlab CI/CD
https://docs.gitlab.com/ee/ci/

Referencia y Glosario de AWS
https://docs.aws.amazon.com/es_es/general/latest/gr/glos-chap.html

Descripción:

Este documento se compone principalmente de tres secciones que consisten en dos vistas arquitectónicas de la infraestructura desplegada, y una vista funcional detallada de la arquitectura de SILIN, adicional en cada sección se incluyen descripciones conceptuales para su correcta interpretación.

Representación de la arquitectura:

Este documento presenta la arquitectura del sistema mediante tres vistas. La primera abarca la arquitectura como servicio SILIN de una manera macro, la segunda vista describe el funcionamiento de los micro servicios bajo docker y la tercera sección detalla la arquitectura desplegada de SILIN desde un punto de vista técnico.

Metas y restricciones de la arquitectura:

Se tomaron en cuenta las siguientes metas y restricciones para el diseño de la arquitectura:

Metas

- Brindar una visión general del sistema mediante vistas lógicas de diseño. Se pretende disponer de un panorama claro del sistema a nivel de arquitectura como servicio SILIN y correlacionando las funcionalidades entre los componentes que lo conforman.
- Proveer una infraestructura que cumpla los pilares de la seguridad, integridad confidencialidad y disponibilidad de los sistemas y datos presentes en la arquitectura como servicio SILIN integrando procesos de CI/CD.

Restricciones del Sistema

- El proceso de despliegue para los componentes actuales y futuros se realizará mediante el proceso de IaC generando respaldo, versionamiento y

auditorías sobre los diferentes entornos de la arquitectura como servicio SILIN.

- El proceso de liberación de nuevas versiones permite enviar cambios a los diferentes entornos de manera controlada mediante el sistema de control de versiones y procesos de CI/CD controlados por el área de software.
- El sistema funciona con bases de datos en RDS con replicación de datos en al menos 1 zona de disponibilidad diferente, asegurando su disponibilidad, protección e integridad. Adicionalmente se establecen planes de copias de seguridad con cifrado sobre las bases de datos de los ambientes productivos de SILIN.
- Se establecen subredes para segmentar el despliegue de entornos controlados y aseguramiento mediante ACLs para restringir el acceso a zonas core del sistema.
- La conexión a los recursos de la infraestructura de AWS se controla mediante conexiones VPN Cliente – Servidor que proporcionan comunicaciones seguras mediante certificados a las redes de los entornos core del sistema.
- La funcionalidad y privilegios de los componentes de la arquitectura como servicio SILIN dependen de políticas y roles IAM en formato JSON definidos mediante el proceso IaC. Su afinamiento controla los accesos y niveles de ejecución presente en la arquitectura que soporta el sistema.

Modelo conceptual de la arquitectura como servicio SILIN:

La arquitectura como servicio SILIN que se utiliza para el sistema, funciona bajo el proceso de IaC, esto quiere decir que los despliegues iniciales y futuros son escritos como código y desplegados en el proveedor de nube predefinido, permitiendo generar una arquitectura versionada, protegida e inmutable.

Las subredes que se utilizan dentro de un VPC y entre cada una de ellas como ACL son utilizadas para filtrar y regular el tráfico entrante y saliente acorde al modelo de

seguridad implementado. Por otro lado, la arquitectura es capaz de conectar mediante su perímetro, redes externas tipo VPN punto a punto, cliente-Servidor, logrando de esta manera integración con entornos remotos y aseguramiento en las conexiones.

Vista General Infraestructura Cloud.

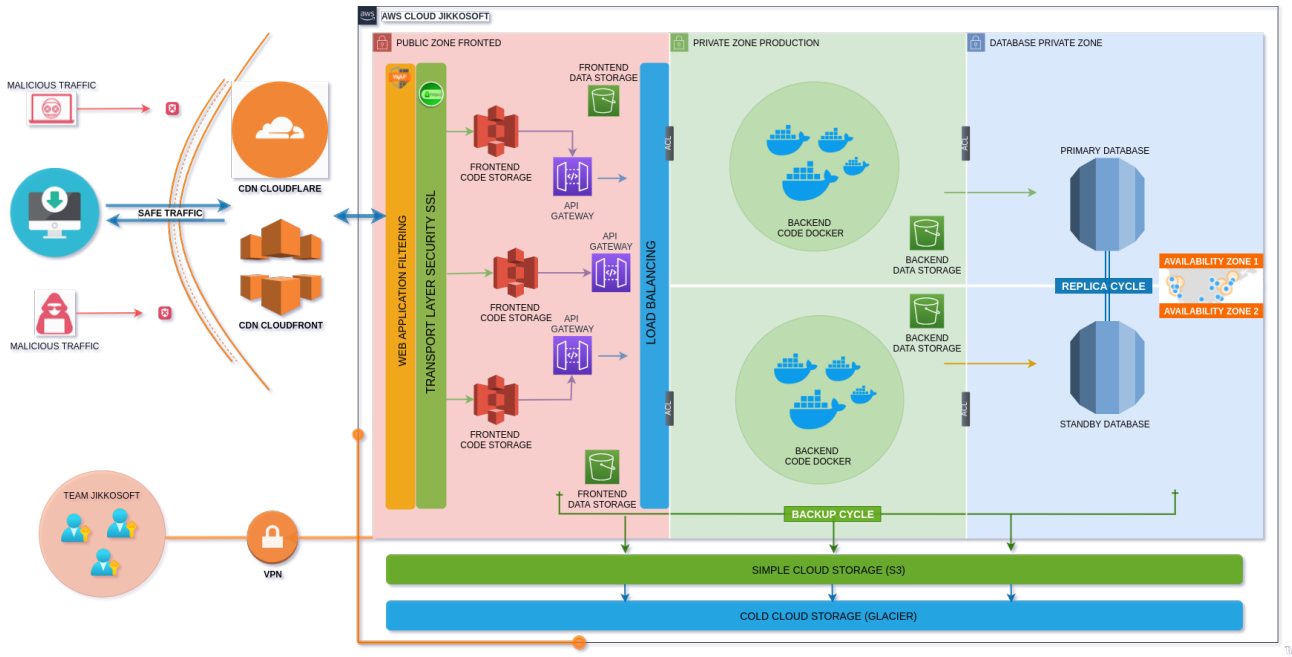


Ilustración 1. Diagrama Infraestructura Cloud

Modelo conceptual de la arquitectura de micro servicios:

La arquitectura como servicio SILIN comprende diferentes clústeres de micro servicios bajo ECS que soportan los diferentes entornos productivos y pre-productivos del sistema. Los despliegues de las funcionalidades actuales y futuras, se realizan mediante el proceso de integración continua, esto quiere decir que el sistema está en la capacidad de realizar integraciones de nuevas funcionalidades de manera continua y progresiva, monitoreando los diferentes estados que implica un correcto despliegue sin afectar la interacción del usuario.

Vista infraestructura de micro servicios.

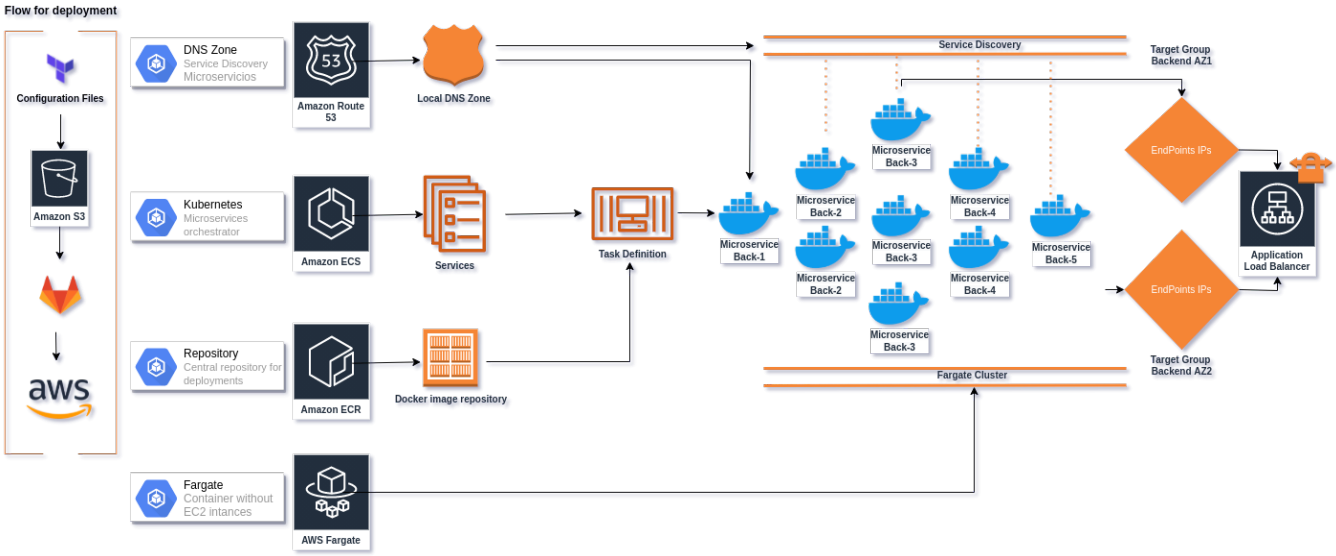


Ilustración 2. Diagrama Infraestructura de Micro Servicios

Modelo detallado de la arquitectura para SILIN.

La arquitectura desplegada para SILIN se divide en diferentes entornos, algunos productivos y otros pre-productivos, aislando recursos de acuerdo al core del sistema y los entes que interactúan con la plataforma.

El componente "Frontend" arquitectado mediante SPA (single-page application) es soportado por sistemas CDN de distribución geolocalizada que optimizan las peticiones web de usuario final.

El componente "Backend" arquitectado principalmente mediante Application Load Balancer (ALB), permite escalar horizontalmente de acuerdo al volumen de peticiones y aumento de recursos en el cluster de microservicios.

El componente de "Databases" arquitectado permite conexiones seguras de los recursos de su propio entorno.

El componente “CI/CD” permite entregas de nuevas versiones de manera controlada, versionada y segura desde los repositorios privados del código fuente del sistema SILIN. Los procedimientos para los despliegues se ejecutan en cómputo preinstalado de Jikkosoft garantizando la seguridad del código fuente del sistema SILIN.

Vista detallada de la arquitectura para SILIN.

Fronted

```
resource "aws_cloudfront_distribution" "service-silin-com-co" {
  origin {
    origin_id   = "service-dev"
  s3_origin_config {
     origin_access_identity = aws_cloudfront_origin_access_identity.aoi}
```

API Gateway

```
resource "aws_api_gateway_rest_api" "silin-api-staging-proxy" {
  api_key_source = "HEADER"
  binary_media_types = [
    "multipart/form-data",
  ]
```

Load Balancing

IaC - Terraform

```
resource "aws_lb_listener_rule" "service_rule_prod" {
  listener_arn = aws_alb_listener.https.arn
priority     = 200
  action {
    type             = "forward"
    target_group_arn = aws_lb_target_group.service-prod.arn}
}
```

ECS Cluster Microservices

```
resource "aws_ecs_cluster" "cluster-service" {
  name               = name.services
  capacity_providers = ["FARGATE"]
  setting {
    name  = "containerInsights"
    value = "enabled"
  }
```

Relational Databases

```
resource "aws_db_instance" "db-services" {
  auto_minor_version_upgrade = false
  availability_zone          = "us-services"
  backup_retention_period    = 0
  copy_tags_to_snapshot      = true
  db_subnet_group_name       = aws_db_subnet_group.subnet-services
  deletion_protection        = true
}
```

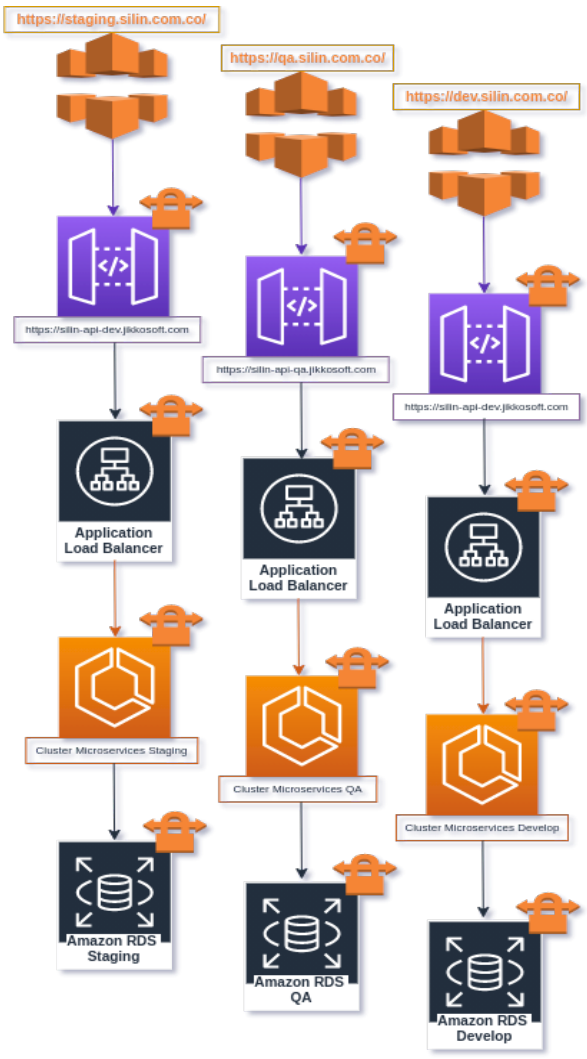


Ilustración 3. Diagrama detallado Infraestructura IaC de SILIN

Rendimiento y respaldo.

Rendimiento

- El sistema permite el acceso concurrente de varios usuarios mediante su balanceador de carga de aplicaciones. Adicionalmente, el CDN optimiza el acceso a la información, puesto que el usuario llegará a aquellas copias de datos que se encuentren más próximas a su posición geográfica.
- La capa de seguridad detiene la mayor parte del tráfico malicioso antes de que llegue a los servidores de aplicaciones. En esta fase se analizan las amenazas potenciales en las solicitudes de los visitantes en función de una serie de características:

    - Dirección IP del visitante
    - Recursos solicitados.
    - Carga y frecuencia de solicitudes.
    - Reglas de firewall definidas previamente.

- Los micro servicios escalan horizontalmente, es decir, que con base en diferentes criterios se tienen predefinidos grupos de escalamiento, que detectan si algún parámetro sobrepasa el umbral definido en cuanto a memoria, costo en CPU o conexiones entrantes.
- Las bases de datos del sistema están ubicadas dentro del mismo backbone de red de los micro servicios permitiendo una mayor eficiencia en las transacciones.

Respaldo

- La información persistente se almacena en buckets de S3 con ciclo de vida, generando un sistema de copias de seguridad.
- Según los criterios de Retención y Rotación de las copias de seguridad, estas se van moviendo hacia almacenamiento frío tipo S3 Glacier para posteriormente eliminarse al cumplir su ciclo de retención.
- Cada componente computacional trabaja en paralelo en al menos dos zonas de disponibilidad y dos subredes del mismo VPC garantizando el acceso continuo al sistema.

Firma,

Juan David Lopez
CEO
Jikkosoft S.A.S