

Servicios de encriptación y codificación en la nube

Los casos de Google Cloud Platform y Amazon Web Services



Presentación elaborada por Marcos Hidalgo Baños (GPC) y Alejandro Caro Casado (AWS)

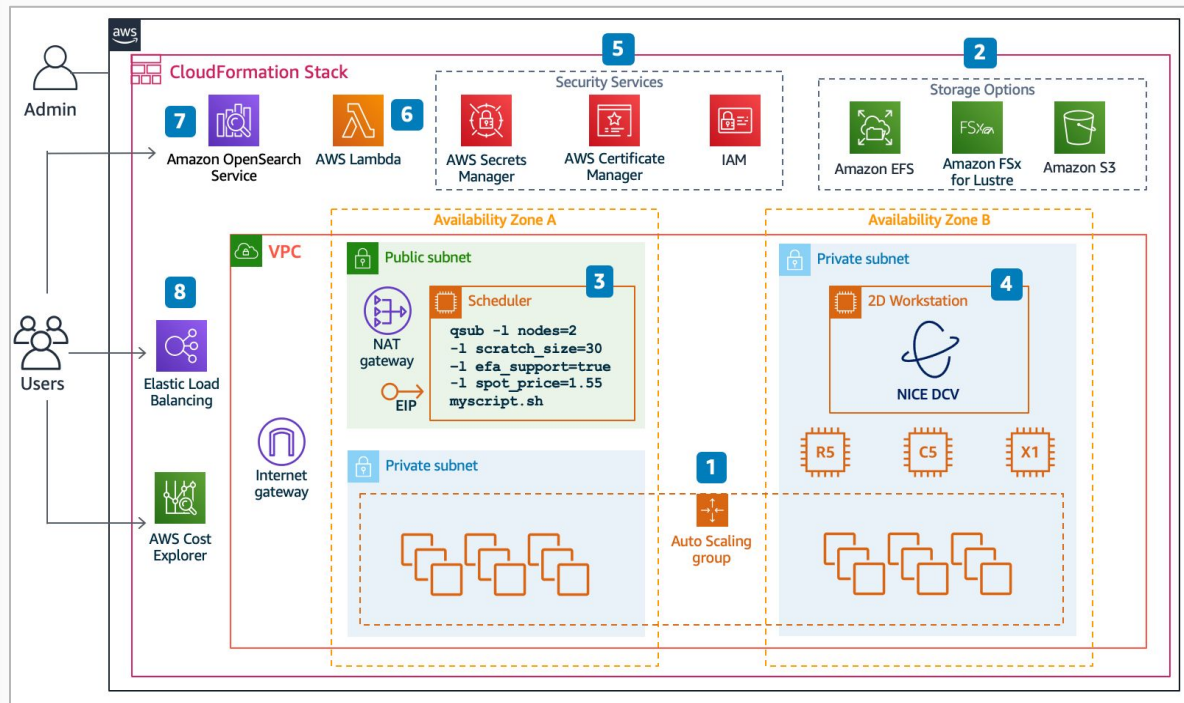
Conceptos de servicio y consola

Todo **proyecto** en la nube está compuesto por un determinado conjunto de **servicios**.

Cada servicio realiza una función concreta dentro del proyecto y deben ser independientes entre sí.

Los servicios son añadidos al proyectos mediante una **consola**, puede ser una interfaz gráfica o interfaz de línea de comandos.

Los dos servicios a presentar son [Cloud Key Management Service](#) y [Amazon Redshift](#).



Ejemplo de un proyecto en la nube de AWS

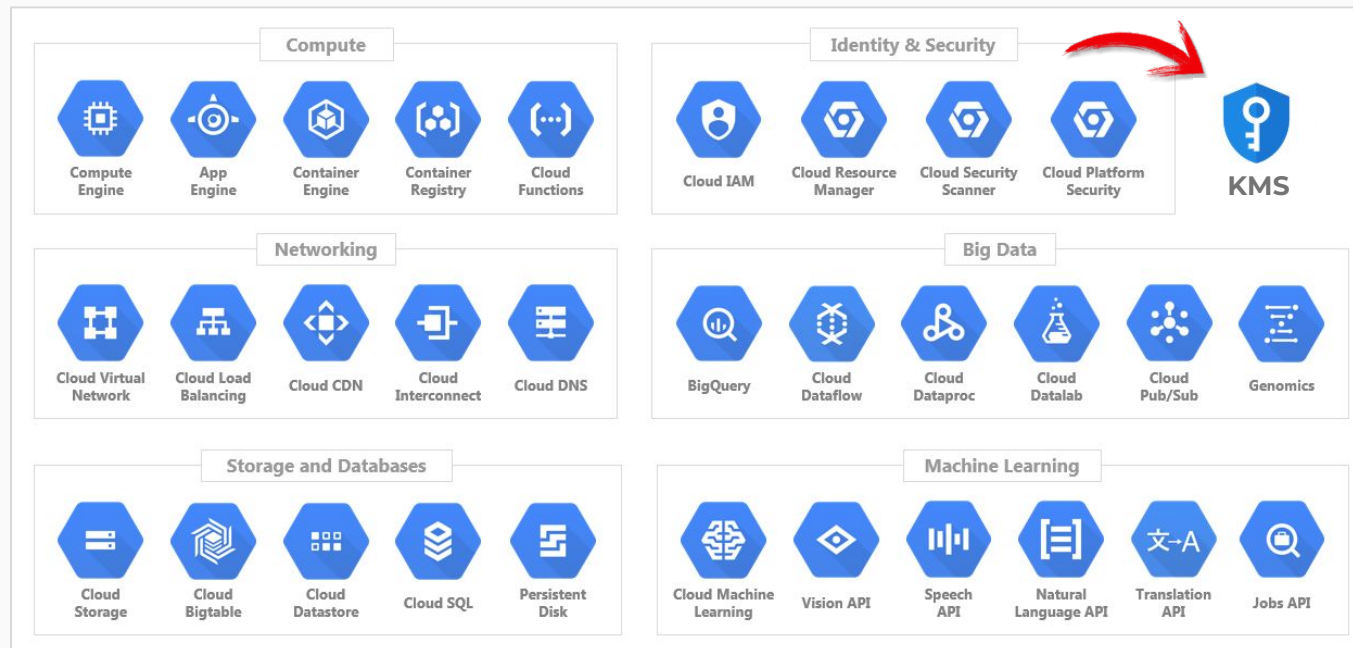
Google Cloud Platform - GCP



Cuadro resumen de las principales secciones de servicios por ámbito.

Notar que se muestran las más **representativas**, no siendo por lo tanto un listado exhaustivo.

Centraremos nuestro estudio en [KMS](#), el cual es uno de los principales servicios de Seguridad.



Google Cloud

Selecciona un proyecto

Buscar Productos, recursos, documentos (/)

Descripción general de Cl...>

Recientes>

Ver todos los productos

FIJADOS

API APIs y servicios>

Facturación

IAM y administración>

Marketplace

Compute Engine>

Kubernetes Engine>

Cloud Storage>

BigQuery>

Red de VPC>

Cloud Run>

SQL>

Seguridad>

Google Maps Platfor...>

MÁS PRODUCTOS

Comienza a utilizar Google Cloud Platform

Prueba gratuita con \$300 de crédito durante 90 días para que puedas comenzar
Acceso a productos del nivel Siempre gratuito para que puedas continuar

PROBAR GRATIS

Productos principales

Compute Engine

Máquinas virtuales escalables de alto rendimiento

Cloud Storage

Un servicio de almacenamiento de objetos potente, sencillo y económico

Cloud SQL

Un servicio de base de datos MySQL, PostgreSQL y SQL Server completamente administrado

Cloud Run

Plataforma de procesamiento completamente administrada para implementar y escalar aplicaciones en contenedores de forma rápida y

Interactúa

Blog

Comunidad

Suscripción al boletín informativo

Vínculos útiles

Descarga la app para dispositivos móviles de GCP

Instala el SDK de Cloud

Documentación

Asistencia

Enlace a la página que se muestra → console.cloud.google.com/getting-started

Servicios de encriptación de claves en la nube



Cloud Key Management Service (KMS) API

[Google Enterprise API](#)

Cloud KMS extends customer control over encryption keys

“[Google Cloud KMS](#) permite a los clientes administrar claves de encriptación y realizar operaciones criptográficas con esas claves”

¿Qué tipos de claves existen en KMS?

RSA 2048	AES256
RSA 3072	EC P256
RSA 4096	EC P384

Simétricas y Asimétricas

¿Para qué se pueden usar las claves en KMS?

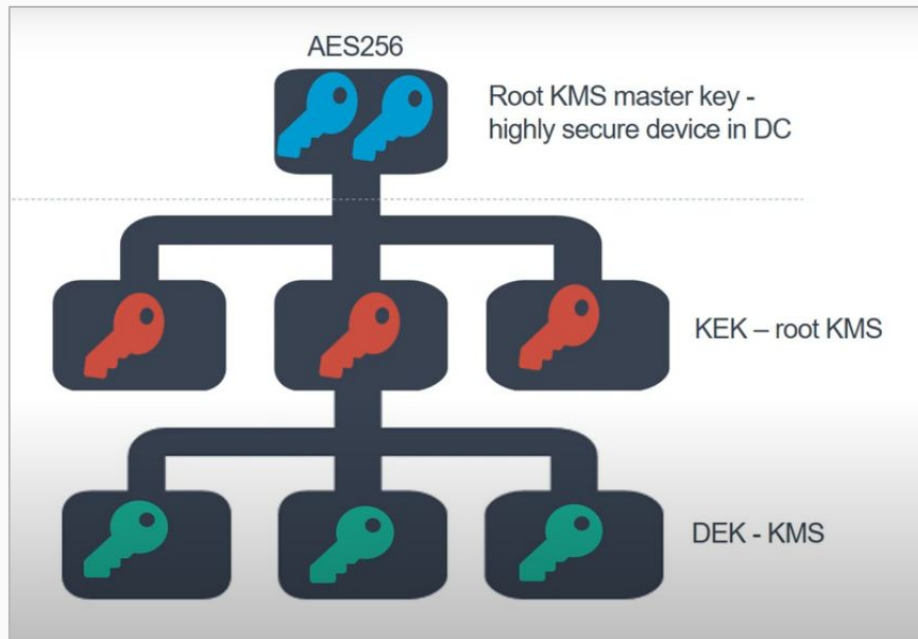
Se puede generar, usar, rotar y destruir toda clave que pertenezca a un **Keyring** (llavero), siendo agrupados según su región geográfica.

¿Hay otros servicios que extiendan a KMS?

Servicios como **EKM** (External Key Management) permiten que las claves se guarden en infraestructuras de terceros y no en los servidores de Google.

Servicios de encriptación de claves en la nube

Jerarquía de claves de encriptación por defecto en KMS.



Root KMS Master Key

Custodiadas de manera física en los centros seguros de Google, permiten desenscriptar y utilizar las KEK. Extremadamente robustas y de acceso restringido.

KEK - Key Encryption Key

Cada vez que el usuario quiere desenscriptar una DEX para utilizarla, debe llamar al servicio KMS para que su KEK correspondiente la desenvuelva. También están controladas por el propio sistema de Google.

DEK - Data Encryption Key

Son las claves que el usuario usa en sus proyectos para encriptar los datos sensibles de su aplicación.

Amazon Web Services - AWS



Una pequeña imagen de los principales servicios que nos puede llegar a ofrecer AWS.

Nos centraremos en los servicios de Base de Datos, de donde destacaremos **Redshift** puesto que utiliza codificación para realizar sus operaciones.



The screenshot shows the AWS Management Console interface. On the left is a dark navigation sidebar with the AWS logo at the top, followed by a search bar and a list of service categories: Analytics, Application Integration, AR & VR, AWS Cost Management, Blockchain, Business Applications, Compute, Containers, Customer Enablement, Database, Developer Tools, End User Computing, Front-end Web & Mobile, Game Development, Internet of Things, Machine Learning, Management & Governance, Media Services, Migration & Transfer, and Networking & Content Delivery. The main content area is titled 'All services' and features a large letter 'A' for alphabetical filtering. It lists various services with brief descriptions: 'View all services', 'Activate for Startups', 'Alexa for Business', 'AWS Amplify', 'API Gateway', 'AWS App Mesh', 'AWS App Runner', 'AWS AppConfig', 'Amazon AppFlow', and 'AWS Application Cost Profiler'. On the right, a 'Welcome to AWS' panel offers links for 'Getting started with AWS', 'Training and certification', and 'What's new with AWS?'. Below this, a section titled 'No cost and usage' states that the user hasn't configured AWS Cost Manager or lacks permission. The top of the console shows the user's location as 'London' and their name 'MarcosHidalgo'. The bottom footer contains a feedback link, a language selection notice, the copyright notice '© 2022, Amazon Web Services, Inc. or its affiliates.', and links for 'Privacy', 'Terms', and 'Cookie preferences'.

aws Services [Alt+S] London MarcosHidalgo

Recently visited Favorites All services

All services

View all services
All AWS services organized by category on a page

Activate for Startups
AWS Activate provides resources to help startups build and grow on AWS.

Alexa for Business
Alexa for Business Provides Tools to Manage Alexa in Your Organization

AWS Amplify
AWS Amplify is a complete platform—frameworks & tools and app services—for developing, building, testing, and running mobile and web apps

API Gateway
Build, Deploy and Manage APIs

AWS App Mesh
Easily monitor and control microservices

AWS App Runner
Build and run production web applications at scale

AWS AppConfig
Use feature flags, operational flags, and other runtime configuration to make changes quickly and safely on production

Amazon AppFlow
Amazon AppFlow integrates apps and automates data flows without code.

AWS Application Cost Profiler
Cost per tenant and workload

Welcome to AWS

Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.

Training and certification
Learn from AWS experts and advance your skills and knowledge.

What's new with AWS?
Discover new AWS services, features, and Regions.

No cost and usage
you haven't configured AWS Cost Manager or you do not have permission.

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Enlace a la página que se muestra → eu-west-2.console.aws.amazon.com/console

Servicios de codificación en bases de datos



“Amazon Redshift es un servicio de almacenamiento y análisis de datos que proporciona una base de datos altamente escalable que se utiliza para análisis de datos a gran escala.”

¿Qué tipos de codificación utiliza?

RAW	Diccionario de bytes	
AZ64	Delta	LZO
Mostly	Text255	Text32k
ZSTD	Run length	

¿Por qué codificamos los datos?

Redshift codifica las columnas para poder reducir el tamaño de los datos cuando se almacenen, aunque no todos los tipos de datos pueden ser codificados.

Servicios de codificación en bases de datos

Tipo de codificación	Tipos de datos
Raw (sin comprimir)	Todos
AZ64	SMALLINT, INTEGER, BIGINT, DECIMAL, DATE, TIMESTAMP, TIMESTAMPTZ
Diccionario de bytes	SMALLINT, INTEGER, BIGINT, DECIMAL, REAL, DOUBLE PRECISION, CHAR, VARCHAR, DATE, TIMESTAMP, TIMESTAMPTZ
Delta	SMALLINT, INT, BIGINT, DATE, TIMESTAMP, DECIMAL INT, BIGINT, DATE, TIMESTAMP, DECIMAL
LZO	SMALLINT, INTEGER, BIGINT, DECIMAL, CHAR, VARCHAR, DATE, TIMESTAMP, TIMESTAMPTZ, SUPER
Mostlyn	SMALLINT, INT, BIGINT, DECIMAL INT, BIGINT, DECIMAL
Run-length	SMALLINT, INTEGER, BIGINT, DECIMAL, REAL, DOUBLE PRECISION, BOOLEAN, CHAR, VARCHAR, DATE, TIMESTAMP, TIMESTAMPTZ
Texto	Solo VARCHAR Solo VARCHAR
Zstandard	SMALLINT, INTEGER, BIGINT, DECIMAL, REAL, DOUBLE PRECISION, BOOLEAN, CHAR, VARCHAR, DATE, TIMESTAMP, TIMESTAMPTZ, SUPER

Codificación AZ64

Es un algoritmo codificado de compresión que se ha diseñado para lograr una alta relación de compresión y un procesamiento mejorado de las consultas. El algoritmo comprime grupos de valores de datos más pequeños.

Codificación por Texto

Son útiles para comprimir columnas VARCHAR en las que se repiten con frecuencia las mismas palabras. Se crea un diccionario independiente de palabras únicas para cada bloque de los valores de columna del disco

Codificación Delta

La codificación Delta comprime los datos al registrar la diferencia entre los valores que se suceden en la columna. Esta diferencia se registra en un diccionario independiente para cada bloque de valores de columnas del disco.

Conclusiones de la investigación

GENERALES.

La nube puede emplearse como herramienta en contextos muy diferentes.

Los servicios en la nube son similares independientemente del proveedor.

CONCRETAS.

La administración de datos sensibles en la nube es un asunto de seguridad que no tiene una solución general para todos los casos.

- **KMS** establece una jerarquía centralizada, pero habilita alternativas.
- **Redshift** nos ofrece tipos de codificación según el tipo de datos.

Referencias bibliográficas

- cloud.google.com/security-key-management
cloud.google.com/docs/security/key-management-deep-dive
Documentación oficial y raíz de otros artículos.
- youtube.com/watch?v=GDECKM9iW0w
Vídeo sobre la arquitectura de KMS.
- docs.aws.amazon.com
aws.amazon.com/es/what-is-aws
docs.aws.amazon.com/es_es/redshift/latest/dg/welcome.html
Documentación oficial de AWS y Redshift.