Reference:

FAQs

Category:

Security, Identity, and Compliance

AWS Key Management Service (AWS KMS)

Complete book:

Click Here

Created by:

Ashish Prajapati

What?

- AWS KMS is a managed service that enables you to easily create and control the keys used for cryptographic operations.
- The service provides a highly available key generation, storage, management, and auditing solution for you to encrypt or digitally sign data within your own applications or control the encryption of data across AWS services.

Why?

- AWS KMS presents a single control point to manage keys and define policies consistently across integrated AWS services and your own applications.
- It reduces your licensing costs and operational burden by providing a scalable key management infrastructure.

When?

- You want to centrally create, import, rotate, delete, and manage permissions on keys that control access to your data.
- You want to perform digital signing operations using asymmetric key pairs to ensure the integrity of your data.
- Yon need the option to store your keys in single-tenant HSMs in AWS CloudHSM instances that you control.

Where?

- AWS KMS is a regional service. KMS keys are never shared outside the AWS region in which they were created.
- AWS KMS supports multi-Region keys, which are AWS KMS keys in different AWS Regions that can be used interchangeably – as though you had the same key in multiple Regions.

Who?

- AWS KMS is a fully managed service.
- You control access to your encrypted data by defining permissions to use keys while AWS KMS enforces your permissions and handles the durability and physical security of your keys.

How?

- AWS KMS uses hardware security modules (HSM) to protect and validate your AWS KMS keys. To protect data at rest, integrated AWS services use envelope encryption, where a data key is used to encrypt data, and is itself encrypted under a KMS key. For signing and verification, integrated AWS services use a key pair from an asymmetric KMS key in AWS KMS.

How much?

- You pay US $1/month to store any key that you create. You also pay for number of API requests made to the AWS KMS.
- AWS managed keys that are created on your behalf by AWS services are free to store. You are charged per-request when you use or manage your keys beyond the free tier.