# AWS Cloud KMS

**Topics :** AWS
**Written on** December 09, 2023

AWS Key Management Service (KMS) is a fully managed service that allows you to create, control, and manage cryptographic keys used for encrypting your data. AWS KMS makes it easier to create and control encryption keys that can be used to secure your data, both in transit and at rest.

1. **Key Creation and Management:**
    - AWS KMS enables you to create, rotate, and manage cryptographic keys used for encryption. Keys can be created in AWS KMS or imported from your own key management infrastructure.
2. **Envelope Encryption:**
    - AWS KMS uses a technique called envelope encryption. Data is encrypted with a data key, and this data key is then encrypted with a master key stored in AWS KMS. This approach provides additional security by separating data and master keys.
3. **Integrated with AWS Services:**
    - AWS KMS integrates with various AWS services, allowing you to easily encrypt and decrypt data within those services. For example, you can use AWS KMS to manage keys for Amazon S3, Amazon EBS, Amazon RDS, and more.
4. **Customer Master Keys (CMKs):**
    - In AWS KMS, cryptographic keys are referred to as Customer Master Keys (CMKs). There are two types of CMKs: Customer Managed CMKs and AWS Managed CMKs. Customer Managed CMKs offer greater control and flexibility.
5. **Key Policies and Resource-Based Policies:**
    - AWS KMS allows you to define key policies to control access to your keys. Key policies are similar to IAM policies but are specific to KMS. Additionally, you can use resource-based policies to control access to keys.
6. **Key Rotation:**
    - AWS KMS supports automatic key rotation for both Customer Managed CMKs and AWS Managed CMKs. Key rotation is a security best practice that helps limit the potential impact of a compromised key.

7. **Audit Logging:**
    - AWS KMS provides detailed audit logging through AWS CloudTrail. You can monitor and log key usage to ensure compliance with security and auditing requirements.
8. **Integration with AWS CloudTrail:**
    - AWS CloudTrail can be used to capture and log AWS KMS API calls, providing visibility into key usage and changes to key configurations.
9. **Cross-Region Replication:**
    - AWS KMS supports cross-region replication of Customer Managed CMKs. This enables you to use the same key for encryption in multiple regions.
10. **Tagging:**
    - You can use tags to label and categorize your keys. This makes it easier to organize and manage keys, especially when dealing with a large number of keys.
11. **Multi-Region Keys:**
    - AWS KMS provides a feature called Multi-Region keys, which allows you to replicate Customer Managed CMKs to multiple AWS regions. This enables you to use the same key for encryption across regions.
12. **Integration with AWS Encryption SDK:**
    - AWS KMS integrates with the AWS Encryption SDK, making it easier for developers to add encryption and decryption to their applications using a consistent set of APIs.