

AWS Key Management Service (KMS)

AWS Key Management Service (KMS) is a managed encryption service provided by Amazon Web Services (AWS). It allows you to create and manage encryption keys for your applications and workloads. KMS helps you protect sensitive data and meet compliance requirements by providing robust encryption capabilities.

Key Features:

1. **Centralized Key Management:** KMS allows you to create, import, and manage cryptographic keys in a secure and scalable manner.
2. **Integration with AWS Services:** KMS seamlessly integrates with various AWS services like S3, RDS, EBS, and others, allowing you to encrypt your data at rest.
3. **Granular Access Control:** You can define fine-grained access policies to control who can use and manage encryption keys.
4. **Hardware Security Modules (HSM) backed:** KMS is designed to be highly secure, using dedicated HSMs to protect keys.
5. **Key Versioning and Rotation:** KMS supports key versioning and automatic key rotation, ensuring that your data remains secure over time.
6. **Audit Trails:** KMS provides detailed logs of all key usage, allowing you to track who accessed which keys and when.

Use Cases:

Data Encryption: Encrypting data at rest in services like S3, EBS, and RDS.

Application-Level Encryption: Encrypting data before storing it in your applications.

Compliance Requirements: Meeting regulatory and compliance requirements that mandate encryption.