AWS Secrets Manager

SECURE STORAGE AND AUTOMATED SECRETS MANAGEMENT

AWS SECRETS MANAGER

OVERVIEW

- Fully managed secrets management service
- Store, manage, and retrieve API keys, passwords, certificates, and database credentials securely
- Automatically rotate secrets
- Integrated with AWS services like Lambda, RDS, and EC2

KEY FEATURES

- Secure storage of secrets with encryption at rest using AWS KMS
- Automatic rotation of secrets without downtime
- Fine-grained access control via AWS IAM
- Audit logging through AWS CloudTrail
- Integrated SDK/CLI/API access for applications

Security Benefits

- Secrets encrypted with KMS (Key Management Service)
-
- Controlled access with IAM policies and resource-based policies
-
- Automatic secret rotation using AWS Lambda functions
-
- Audit and monitoring using CloudWatch and CloudTrail

Use Cases

- Secure storage of database passwords
- Managing API keys, OAuth tokens, and SSH keys
- Dynamic secrets generation and rotation.
- Securely injecting secrets into Lambda functions, containers, or EC2 instances.

REAL EXAMPLE USE CASE

- Web Application needs a database password:
- Store the DB password in AWS Secrets Manager.
- Web app fetches the password dynamically via API calls (no hardcoding).
- If password rotates automatically, app uses the new secret withoutdowntime.