

Formação AWS Cloud Foundations

Alexsandro Lechner

Arquiteto de Soluções AWS

[linkedin.com/in/alexsandrolechner](https://www.linkedin.com/in/alexsandrolechner)

Conteúdo Programático

☐ Módulo 9: Segurança na AWS

- Práticas recomendadas de segurança na nuvem
- **Criptografia de dados na AWS**
- AWS WAF: firewall de aplicativos da web

Segurança na AWS

Criptografia de Dados na AWS

Criptografia de Dados na AWS

Introdução à Criptografia de Dados

- Conceitos básicos: Criptografia em repouso e em trânsito
- Importância de proteger dados sensíveis na nuvem

Criptografia de Dados na AWS

Criptografia em repouso concentra-se na proteção dos dados quando estão armazenados em discos ou bancos de dados, garantindo sua segurança mesmo fora de movimento.

Criptografia de Dados na AWS

Em uma transmissão de dados, a segurança é fundamental. Quando falamos sobre criptografia em trânsito, estamos nos referindo às medidas que protegem os dados enquanto eles são transmitidos de um ponto a outro, como em uma comunicação pela internet.

Criptografia de Dados na AWS

Encripte os dados em trânsito ou em repouso

Encriptação de Volumes

Criptografia de
Disco (EBS)

Arquivos

Soluções de parceiros /
MarketPlace

Criptografia de Objetos

S3 Server Side
Encryption (SSE)

S3 SSE com chaves do
cliente

Criptografia do lado do
cliente

Criptografia de Bases de Dados

MSSQL

ORACLE

MYSQL

PostgreSQL

Redshift

SSL/TLS Fim-a-Fim



Criptografia de Dados na AWS

Criptografia em repouso:

Serviços como **Amazon S3** (armazenamento de objetos), **Amazon RDS** (banco de dados) e **EBS** (armazenamento de blocos) possui criptografia em repouso. Isso significa que os dados são automaticamente criptografados antes de serem gravados e descriptografados ao serem acessados.

Criptografia de Dados na AWS

Criptografia em repouso:

O AWS Key Management Service (KMS): que é um serviço que permite criar e gerenciar chaves de criptografia oferecendo controle granular sobre o uso de chaves.

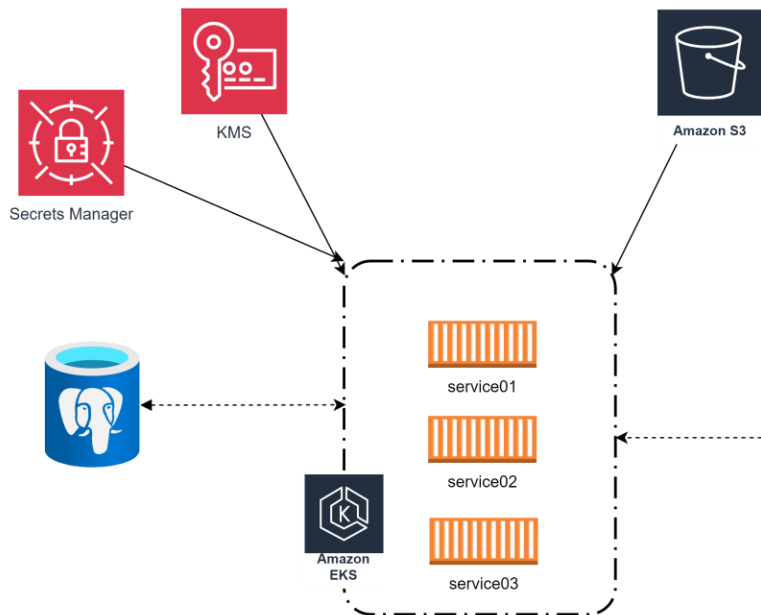
Criptografia de Dados na AWS

Criptografia em trânsito:

Os dados são protegidos enquanto são transmitidos entre clientes e serviços da AWS.

Isso garante que as informações não possam ser interceptadas ou manipuladas durante a transferência.

Criptografia de Dados na AWS



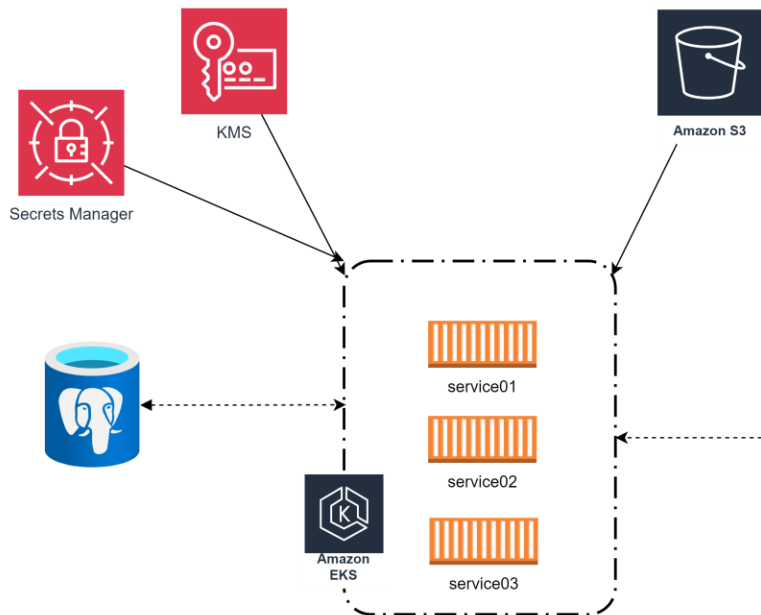
AWS KMS (Key Management Service):

Gerencia chaves de criptografia usadas para proteger dados.

Focado em criptografia de dados (em repouso ou em trânsito) e no controle de acesso às chaves.

- Quando precisamos criptografar dados em serviços como: S3, EBS (discos), DynamoDB (tabelas), RDS (bancos de dados).
- E quando desenvolvemos aplicações que exigem criptografia personalizada (usando SDK de KMS).

Criptografia de Dados na AWS



AWS Secrets Manager:

Gerencia segredos e credenciais sensíveis, como senhas, tokens de API, e strings de conexão de banco de dados.

Focado no armazenamento seguro e na rotação automática de credenciais.

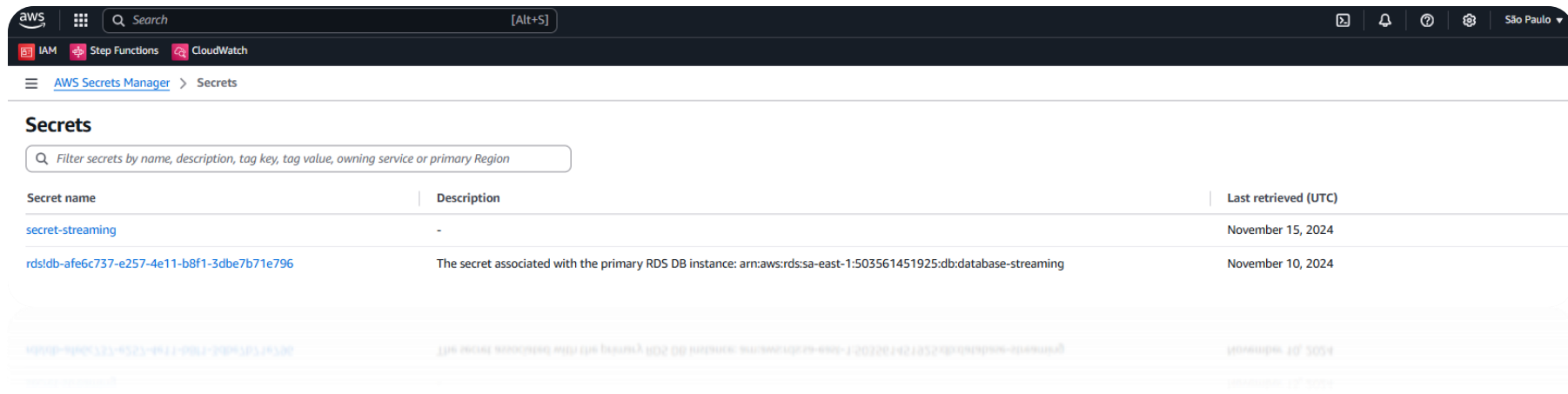
- Quando precisamos armazenar e recuperar segredos de maneira segura.
- Quando precisa automatizar a rotação de credenciais, como senhas de banco de dados ou tokens de API.
- Ideal para evitar armazenamento de credenciais em código.



API GATEWAY



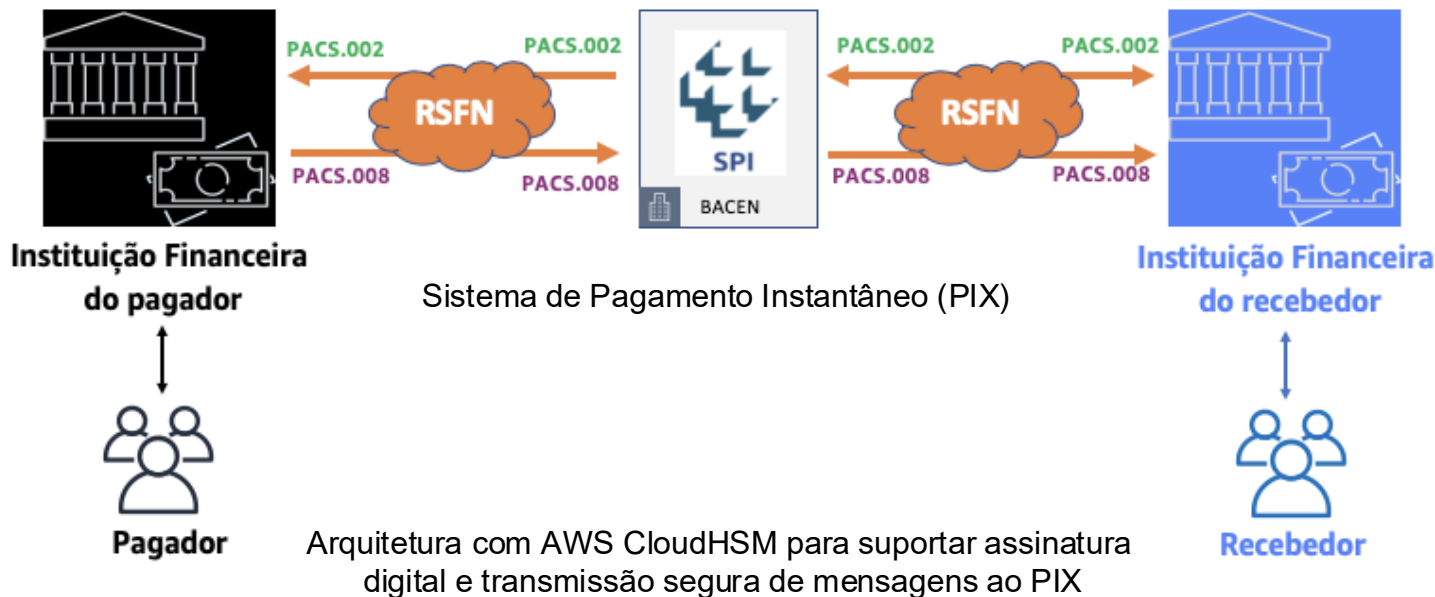
Criptografia de Dados na AWS



The screenshot shows the AWS Secrets Manager console interface. At the top, there's a navigation bar with the AWS logo, a search bar, and a region dropdown set to 'São Paulo'. Below the navigation bar, the breadcrumb trail reads 'AWS Secrets Manager > Secrets'. The main heading is 'Secrets'. Below the heading is a search filter box with the placeholder text 'Filter secrets by name, description, tag key, tag value, owning service or primary Region'. The main content area displays a table of secrets.

Secret name	Description	Last retrieved (UTC)
secret-streaming	-	November 15, 2024
rdsfdb-afe6c737-e257-4e11-b8f1-3dbe7b71e796	The secret associated with the primary RDS DB instance: arn:aws:rds:sa-east-1:503561451925:db:database-streaming	November 10, 2024

Criptografia de Dados na AWS



<https://aws.amazon.com/pt/blogs/aws-brasil/arquitetura-com-aws-cloudhsm-para-suportar-assinatura-digital-e-transmissao-segura-de-mensagens-ao-pix/>