

# Atalhos

[IAM](#)

[IAM Identity Center](#)

[Access Advisor ou Consultor de Acesso](#)

[AWS IAM Credentials Report](#)

[AWS Organizations](#)

[Infra Global](#)

[Tipos de Ec2](#)

[BBS](#)

[EFS](#)

[FSx](#)

[Amazon Auto Scaling](#)

[S3](#)

[RDS](#)

[Amazon Neptune](#)

[AWS Glue](#)

[VPC](#)

[ALC](#)

[VPC Peering](#)

[VPC Flow Logs](#)

[Client e Site to Site VPN](#)

[AWS PrivateLink](#)

[AWS Direct Connect](#)

[AWS Transit Gateway](#)

[Route53](#)

[Route53 Policies](#)

[AWS CloudFront AWS CloudFront](#)

[S3 Transfer Acceleration](#)

[AWS Global Accelerator](#)

[Amazon Elastic Container Registry \(Amazon ECS\)](#)

[Amazon Elastic Kubernetes Service \(Amazon EKS\)](#)

[AWS Kinesis](#)

[AWS SQS \(Simple Queue Service\)](#)

[AWS SNS \(Simple Notification Service\)](#)

[AWS Batch](#)

[AWS LightSail](#)

[AWS Lambda](#)

[AWS Fargate](#)

[AWS Well-Architected Framework](#)

[AWS Cloud Adoption Framework \(CAF\)](#)

[AWS EcoSystem](#)

[AWS IQ](#)

[AWS Serviços Gerenciados](#)

[Amazon Cognito](#)

[Amazon Security Token Service \(STS\)](#)

[AWS Device Farm](#)

[AWS AppSync](#)

[AWS Amplify](#)

[AWS IoT Core](#)

[AWS Step Functions](#)

[Amazon AppFlow](#)

[AWS Backup](#)

[AWS Disaster Recovery Strategy](#)

[AWS WorkSpaces](#)

[AWS AppStream 2.0](#)

## **AWS IAM (Identity and Access Management)**

- **Propósito:** IAM é usado para gerenciar o **acesso granular** e as permissões dentro de uma conta AWS. Ele permite que você crie políticas que controlam quais ações usuários, grupos e funções podem executar em recursos específicos da AWS.
- **Uso:** Gerenciar identidades e permissões de recursos AWS dentro de **uma conta**. Com IAM, você pode criar usuários IAM, grupos, políticas de acesso e funções que permitem que serviços da AWS e usuários autorizados acessem recursos.
- **Exemplo:** Criar um usuário com acesso apenas ao Amazon S3 e negar acesso a outras partes da AWS.
- **Público-Alvo:** Administradores que precisam definir políticas detalhadas para permissões e recursos em uma única conta AWS ou quando configurando permissões entre serviços da AWS.

## **IAM Identity Center (anteriormente AWS SSO)**

- **Propósito:** IAM Identity Center é projetado para simplificar o gerenciamento de identidades e permissões em **múltiplas contas AWS** ou para facilitar o acesso centralizado a **aplicativos externos** usando o mesmo login. Ele oferece um **Single Sign-On (SSO)** para acessar várias contas AWS e aplicativos.
- **Uso:** IAM Identity Center permite que os usuários usem suas credenciais empresariais (como as de um diretório corporativo ou Azure AD) para acessar várias contas AWS e até mesmo serviços de terceiros de forma centralizada.
- **Exemplo:** Permitir que um usuário de uma organização faça login com credenciais de diretório (como Active Directory) e acesse várias contas AWS ou aplicativos SaaS com um único login.
- **Público-Alvo:** Organizações que têm várias contas AWS e querem centralizar o gerenciamento de identidades ou facilitar o acesso para usuários que precisam alternar entre contas e serviços.

## **Access Advisor ou Consultor de Acesso**

O **Access Advisor** é uma funcionalidade do **AWS IAM** que ajuda a gerenciar e otimizar permissões de acesso dos usuários, grupos e funções na AWS. Ele fornece informações sobre o uso real de permissões associadas a uma política IAM, permitindo que administradores ajustem as permissões para seguir o princípio do **menor privilégio**.

#### **Principais Características do Access Advisor:**

1. **Avaliação do Uso de Permissões:**
  - O Access Advisor mostra quando um serviço AWS foi **usado pela última vez** por uma entidade (usuário, grupo ou função). Isso ajuda a identificar permissões desnecessárias que nunca ou raramente são usadas.
2. **Otimização de Permissões:**
  - Com base nas informações de uso fornecidas, os administradores podem ajustar as políticas de IAM para **revogar permissões** desnecessárias, melhorando a segurança e limitando o acesso a apenas o que é necessário.
3. **Princípio do Menor Privilégio:**
  - O Access Advisor facilita a aplicação do princípio do menor privilégio, que consiste em garantir que cada identidade tenha o mínimo de permissões necessárias para executar seu trabalho. Isso é crucial para reduzir a **superexposição de permissões** e mitigar riscos de segurança.
4. **Análise por Serviço AWS:**
  - Ele mostra uma lista de serviços AWS aos quais a entidade tem permissão de acesso, indicando se essas permissões foram **efetivamente utilizadas** ou não.
5. **Uso em Funções, Usuários e Grupos:**
  - O Access Advisor pode ser utilizado para **analisar permissões de usuários individuais**, grupos de usuários, ou funções de IAM (como aquelas usadas para instâncias do EC2 ou Lambda). Ele também é útil para verificar o uso de permissões associadas a funções cross-account ou a funções de confiança.

## **AWS IAM Credentials Report**

O **AWS IAM Credentials Report** é uma ferramenta que fornece um relatório detalhado sobre o estado das credenciais de segurança associadas a todas as identidades (usuários IAM) em sua conta da AWS. Esse relatório é útil para auditoria e para garantir que as práticas de segurança relacionadas às credenciais estejam sendo seguidas, como a rotação de senhas e a desativação de chaves de acesso não utilizadas.

#### **Principais Características do Credentials Report:**

## 1. Relatório de Segurança de Credenciais:

- O Credentials Report fornece uma visão consolidada das credenciais de segurança (como senhas, chaves de acesso e MFA) para **todos os usuários IAM** em uma conta da AWS.

## 2. Informações Fornecidas:

- O relatório contém informações como:
  - **Nome do Usuário:** Identificação do usuário IAM.
  - **Status da Senha:** Se uma senha de console está habilitada ou não.
  - **Último Uso da Senha:** Data e hora do último uso da senha.
  - **Chaves de Acesso:** Informações sobre chaves de acesso, incluindo data de criação, status (ativo/inativo) e última vez que foram utilizadas.
  - **Autenticação Multifator (MFA):** Indica se a MFA está habilitada para o usuário.
  - **Data de Criação:** Quando o usuário, senha, ou chaves foram criados.
  - **Último Uso das Credenciais:** Para senhas e chaves de acesso, mostra a última vez que foram usadas.

## AWS Organizations

AWS Organizations é um serviço da AWS que permite a você centralizar e gerenciar de forma unificada várias contas AWS. Com o AWS Organizations, você pode criar uma organização para administrar suas contas da AWS a partir de um único local.

Aqui estão algumas características principais do AWS Organizations:

1. **Gerenciamento Centralizado de Contas:** O AWS Organizations permite agrupar e gerenciar todas as suas contas AWS de um único local centralizado. Isso facilita o gerenciamento de contas e recursos em uma organização.
2. **Controle de Acesso Hierárquico:** Com o AWS Organizations, você pode criar uma estrutura hierárquica de Unidades Organizacionais (OUs) para agrupar suas contas. Isso ajuda a organizar suas contas em uma estrutura que melhor se alinhe com o uso dos recursos em sua organização.
3. **Políticas de Controle de Serviço:** O AWS Organizations oferece políticas de controle de serviço (SCPs) que permitem que você controle as permissões para as contas em sua organização. Isso permite que você aplique regras de acesso uniformes em todas as suas contas.
4. **Consolidação de Cobrança:** O AWS Organizations também oferece a capacidade de consolidar sua cobrança em todas as suas contas AWS, o que

pode simplificar a gestão de custos e permitir um melhor rastreamento e controle dos gastos da AWS.

5. **Automação:** Com o AWS Organizations, você pode automatizar a criação e o gerenciamento de contas por meio de APIs e integrações com outras ferramentas da AWS, como o AWS CloudFormation.

## Infra Global

1. **Regiões:** Uma região da AWS é uma área geográfica que contém pelo menos duas Zonas de Disponibilidade. Cada região é completamente independente das outras regiões, o que ajuda a isolar falhas e evitar a propagação de problemas de uma região para outra. Em setembro de 2021, a AWS tinha 25 regiões geográficas ao redor do mundo.
2. **Zonas de Disponibilidade (AZs):** Cada região da AWS é dividida em Zonas de Disponibilidade. Cada AZ é um centro de dados separado dentro de uma região, mas todas as AZs dentro de uma região estão conectadas através de redes de alta velocidade, de baixa latência e totalmente redundantes. As AZs fornecem uma maneira de construir aplicativos altamente disponíveis e tolerantes a falhas.
3. **Zonas Locais:** As zonas locais da AWS aproximam a computação, o armazenamento, o banco de dados e outros produtos da AWS selecionados dos usuários finais. Com as zonas locais da AWS, você pode executar facilmente aplicativos altamente exigentes que exigem latências em milissegundos de um dígito para seus usuários finais, como criação de conteúdo de mídia e entretenimento, jogos em tempo real, simulações de reservatórios, automação de projetos eletrônicos e machine learning.
4. **Wavelength:** O AWS Wavelength permite que os desenvolvedores criem aplicações com latências de um dígito para dispositivos móveis e usuários finais. Os desenvolvedores da AWS podem implantar seus aplicativos nas Zonas do Wavelength, implantações de infraestrutura da AWS que incorporam serviços de computação e armazenamento da AWS aos datacenters dos provedores de telecomunicações na borda das redes 5G e acessam facilmente a variedade de serviços da AWS na região. Isso permite que os desenvolvedores forneçam aplicativos que exigem latências inferiores a 10 milissegundos, como streaming de jogos e vídeos ao vivo, inferência de machine learning na borda e realidade aumentada e virtual (AR/VR).
5. **OutPosts:** O AWS Outposts leva produtos, infraestrutura e modelos operacionais nativos da AWS a praticamente qualquer datacenter, espaço de colocalização ou instalações on-premises. Você pode usar as mesmas APIs, ferramentas e infraestrutura da AWS no local e na Nuvem AWS para oferecer uma experiência híbrida verdadeiramente consistente. O AWS Outposts foi projetado para ambientes conectados e pode ser usado para oferecer suporte a workloads que precisam permanecer on-premises devido à baixa latência ou às necessidades de processamento de dados locais.

## Tipos de EC2

O Amazon EC2 oferece uma variedade de tipos de instâncias otimizados para atender diferentes casos de uso. Os tipos de instâncias compreendem combinações variadas de capacidade de CPU, memória, armazenamento e rede e proporcionam a flexibilidade para escolher a combinação apropriada de recursos para seus aplicativos. Os principais tipos de instâncias do Amazon EC2 incluem:

1. **Instâncias de Uso Geral (A, T, M):** Essas instâncias proporcionam um bom equilíbrio de computação, memória e rede e são uma boa escolha para muitas cargas de trabalho que não requerem especificações de hardware específicas.
2. **Instâncias Otimizadas para Computação (C):** Essas instâncias são otimizadas para cargas de trabalho que exigem alta performance de CPU, como computação científica, modelagem e análise financeira, e renderização de mídia.
3. **Instâncias Otimizadas para Memória (R, X, Z):** Essas instâncias são projetadas para cargas de trabalho que processam grandes conjuntos de dados na memória, como bancos de dados em memória, caches distribuídos, análise em memória e aplicações de big data.
4. **Instâncias Otimizadas para Armazenamento (D, I, H):** Essas instâncias são projetadas para cargas de trabalho que requerem alto desempenho de armazenamento local, como bancos de dados escalonáveis, processamento de dados em escala de petabytes e aplicações de data warehousing.
5. **Instâncias Otimizadas para GPU (P, G, F, Inf):** Essas instâncias são projetadas para cargas de trabalho de computação gráfica, como aprendizado de máquina, mineração de criptomoedas, renderização 3D, e aplicações de streaming de jogos.
6. **Instâncias Arm (A1, M6g, C6g, R6g):** Essas instâncias são baseadas na arquitetura Arm e são uma opção de baixo custo para cargas de trabalho que requerem um bom desempenho de CPU e suportam a arquitetura Arm.

Os tipos de instâncias do Amazon EC2 são constantemente atualizados e ampliados para suportar uma gama cada vez maior de casos de uso. É importante verificar a documentação mais recente da AWS para obter as informações mais atualizadas.

## EBS

O Amazon Elastic Block Store (EBS) é um serviço de armazenamento de alto desempenho oferecido pela AWS para uso com Amazon Elastic Compute Cloud (EC2). Ele foi projetado para aplicativos que exigem armazenamento de baixa latência para ler e escrever dados em blocos.

Aqui estão algumas características principais do EBS:

1. **Desempenho de Armazenamento:** EBS fornece armazenamento em bloco de alto desempenho que pode ser anexado a uma instância EC2. Os volumes EBS são otimizados para cargas de trabalho que exigem operações de E/S de baixa latência, como bancos de dados e aplicativos que exigem muita E/S.
2. **Durabilidade:** O EBS é projetado para durabilidade. Os volumes EBS são automaticamente replicados em sua zona de disponibilidade para proteger contra falhas de componentes, proporcionando alta disponibilidade e durabilidade.
3. **Tipos de Volume:** EBS oferece vários tipos de volume para atender às necessidades de armazenamento e desempenho. Isso inclui os volumes SSD-backed para cargas de trabalho transacionais de uso geral (gp2 e gp3) e de alto desempenho (io1 e io2), e os volumes HDD-backed para cargas de trabalho throughput intensivas (st1 e sc1).
4. **Backup com Snapshots:** O EBS oferece a capacidade de criar snapshots (cópias) dos seus volumes, que são armazenados no Amazon S3 para durabilidade. Esses snapshots podem ser usados para criar novos volumes EBS ou para aumentar o tamanho do volume.
5. **Criptografia:** O EBS oferece a opção de criar volumes criptografados e controlar as chaves de criptografia usando o AWS Key Management Service (KMS). Isso ajuda a atender aos requisitos de conformidade e segurança.
6. **Integração com a AWS:** EBS é profundamente integrado com outros serviços da AWS, como Amazon CloudWatch para monitoramento, AWS Identity and Access Management (IAM) para controle de acesso, e AWS Snapshot Scheduler para automação de backup.

## EFS

O Amazon Elastic File System (EFS) é um serviço de armazenamento de arquivos totalmente gerenciado que facilita a configuração e o dimensionamento de sistemas de arquivos em nuvem na AWS. O EFS foi projetado para ser altamente disponível, durável e seguro, e pode ser usado com uma ampla gama de serviços da AWS e aplicações on-premise.

Aqui estão alguns pontos-chave sobre o Amazon EFS:

1. **Escalabilidade:** O EFS é projetado para escalar automaticamente para acomodar o crescimento dos dados, de alguns gigabytes a petabytes, sem a necessidade de provisionar o armazenamento.
2. **Alta Disponibilidade e Durabilidade:** O EFS armazena automaticamente os arquivos em vários dispositivos dentro e entre várias zonas de disponibilidade para garantir a disponibilidade e durabilidade dos dados.



3. **Compartilhamento de Arquivos:** O EFS suporta o compartilhamento de arquivos entre várias instâncias do Amazon EC2, permitindo que múltiplos servidores acessem um sistema de arquivos simultaneamente.
4. **Integração com AWS:** O EFS pode ser integrado a outros serviços da AWS, como o AWS Backup para backups automatizados e o AWS IAM para controle de acesso.
5. **Tipos de armazenamento:** O EFS oferece várias classes de armazenamento, incluindo Standard e Infrequent Access (IA), permitindo que você otimize os custos com base em seus padrões de acesso aos arquivos.
6. **Segurança:** O EFS inclui suporte para criptografia de dados em repouso e em trânsito, bem como integração com o AWS Key Management Service (KMS) para gerenciamento de chaves de criptografia.

## **FSx**

O Amazon FSx é um serviço de armazenamento de arquivos totalmente gerenciado da AWS que facilita o lançamento e a execução de sistemas de arquivos de terceiros. O FSx fornece o rico conjunto de recursos e a rápida performance que esses tipos de aplicativos precisam, e atualmente suporta dois sistemas de arquivos: Windows File Server para aplicações baseadas em Windows, e Lustre para cargas de trabalho de computação intensiva.

Aqui estão alguns pontos chave sobre o Amazon FSx:

1. **FSx para Windows File Server:** Ele fornece um sistema de arquivos nativamente compatível com o Windows, permitindo que você mova com facilidade as aplicações baseadas em Windows que exigem o sistema de arquivos do Windows para a AWS. É construído sobre o Windows Server e oferece suporte a recursos como deduplicação de dados, criptografia de dados em repouso, e acesso via SMB (Server Message Block) e NFS (Network File System).
2. **FSx para Lustre:** O Lustre é um sistema de arquivos popular para cargas de trabalho de computação intensiva, como análise de big data, modelagem de machine learning e processamento de mídia. O FSx para Lustre é totalmente gerenciado pela AWS, simplificando o processo de criação e execução de um sistema de arquivos Lustre.
3. **Desempenho:** O Amazon FSx foi projetado para oferecer o desempenho rápido necessário para suportar aplicações exigentes. Ele fornece baixa latência e altas taxas de transferência de dados.
4. **Compatibilidade e Integração:** O Amazon FSx é totalmente compatível com os sistemas de arquivos que suporta, o que significa que você pode usar suas ferramentas e aplicações existentes sem modificação. Além disso, o FSx se integra com uma série de outros serviços AWS para coisas como backup, monitoramento e acesso seguro a arquivos.

5. **Segurança:** O Amazon FSx oferece várias funcionalidades de segurança, como a capacidade de armazenar dados em redes virtuais privadas da Amazon (VPCs), suporte a redes de acesso (ACLs) para o Windows File Server, criptografia de dados em repouso e em trânsito, e integração com AWS Key Management Service (KMS) para gerenciamento de chaves de criptografia

## Amazon Auto Scaling

O Amazon Auto Scaling é um serviço da AWS que permite o dimensionamento automático de recursos para manter a performance e a disponibilidade de suas aplicações. Ele funciona monitorando continuamente suas aplicações e ajustando a capacidade para manter a performance estável e previsível ao menor custo possível.

Aqui estão algumas características principais do Amazon Auto Scaling:

1. **Dimensionamento Automático:** O Auto Scaling permite que você defina políticas de dimensionamento que ajustam automaticamente a capacidade de recursos com base nas condições definidas. Por exemplo, você pode dimensionar automaticamente o número de instâncias do Amazon EC2 para atender à demanda de tráfego.
2. **Otimização de Custo e Performance:** Ao ajustar continuamente a capacidade, o Auto Scaling ajuda a melhorar a disponibilidade e minimizar os custos. Quando a demanda aumenta, o Auto Scaling adiciona automaticamente mais recursos. Quando a demanda diminui, ele remove os recursos desnecessários para economizar dinheiro.
3. **Balanceamento de Carga:** O Auto Scaling pode ser usado junto com o Elastic Load Balancing (ELB) para distribuir o tráfego de aplicações entre várias instâncias EC2 para melhorar a disponibilidade e a tolerância a falhas.
4. **Saúde da Aplicação:** O Auto Scaling realiza verificações de saúde em suas instâncias EC2 e substitui automaticamente as instâncias que não estão saudáveis.
5. **Integração AWS:** O Auto Scaling está integrado com uma série de serviços da AWS, incluindo Amazon CloudWatch, Amazon SNS, AWS CloudFormation, entre outros.
6. **Flexibilidade:** O Auto Scaling permite dimensionar vários recursos, não se limitando apenas às instâncias EC2. Você também pode dimensionar serviços como Amazon DynamoDB, Amazon Aurora, Amazon ECS, e Amazon RDS.

## S3

O **Amazon S3 (Simple Storage Service)** é um serviço de armazenamento de objetos altamente escalável e durável oferecido pela AWS. Ele é amplamente utilizado para armazenar e recuperar grandes volumes de dados, sendo uma solução flexível que atende a uma variedade de casos de uso, como backup, armazenamento de arquivos, distribuição de conteúdo e armazenamento de dados para análises.

## Principais Características do Amazon S3:

### 1. Armazenamento de Objetos:

- O Amazon S3 armazena **objetos** (arquivos) em "buckets", que funcionam como contêineres onde você pode organizar e gerenciar os arquivos. Cada arquivo é armazenado como um objeto, que inclui dados e metadados associados.
- Os objetos podem variar de pequenos arquivos de texto a grandes vídeos e backups de dados, com um tamanho de até **5 TB** por objeto.

### 2. Buckets:

- Um **bucket** é o contêiner de armazenamento no S3. Cada bucket tem um nome global exclusivo e é onde você armazena seus objetos. Os buckets podem ser configurados para diferentes regiões da AWS para melhorar a latência e atender aos requisitos de conformidade de dados.
- Os buckets também podem ser configurados com políticas de segurança detalhadas para controlar o acesso aos objetos.

### 3. Escalabilidade e Durabilidade:

- O S3 é altamente escalável, o que significa que ele pode lidar com grandes volumes de dados e um número praticamente ilimitado de objetos.
- Ele oferece uma durabilidade de **99.999999999% (11 noves)**, o que significa que os dados armazenados são extremamente resilientes a falhas. O S3 automaticamente replica os dados entre múltiplos dispositivos e em diferentes locais dentro de uma região AWS.

### 4. Modelos de Armazenamento:

- O S3 oferece diferentes **classes de armazenamento** para atender a necessidades específicas:
  - **S3 Standard:** Projetado para armazenamento frequente de dados e oferece baixa latência e alta durabilidade.
  - **S3 Intelligent-Tiering:** Move automaticamente objetos entre níveis de armazenamento com base em padrões de acesso.
  - **S3 Standard-IA (Infrequent Access):** Para dados acessados com menos frequência, mas que ainda precisam de rápida recuperação.
  - **S3 Glacier:** Para arquivamento de longo prazo com custos reduzidos, com opções de recuperação de dados em minutos ou horas.
  - **S3 Glacier Deep Archive:** Oferece o armazenamento de menor custo para dados que raramente são acessados, com tempos de recuperação mais longos.

### 5. Políticas de Acesso e Segurança:

- O Amazon S3 oferece **controle detalhado de acesso** aos seus dados, com suporte para:
  - **Políticas de bucket:** Controle de acesso no nível do bucket.
  - **Políticas baseadas em identidade (IAM):** Gerenciamento de permissões específicas para usuários ou funções.
  - **Controles de ACL (Access Control Lists):** Controle de permissões no nível do objeto.
  - **Logs de Acesso:** Você pode habilitar logs para monitorar quem acessa os dados armazenados no S3.
- O S3 também oferece **criptografia em repouso** (armazenamento) e **em trânsito** para proteger seus dados. A criptografia pode ser gerenciada pela AWS (SSE-S3), por chaves fornecidas pelo cliente (SSE-C), ou por chaves gerenciadas pelo AWS KMS (SSE-KMS).

#### 6. Versionamento e Backup:

- O **versionamento** permite que você mantenha várias versões de um objeto dentro de um bucket, o que é útil para recuperação de erros humanos ou backups.
- O **cross-region replication** permite replicar objetos entre diferentes regiões para redundância e recuperação de desastres.

#### 7. Acesso a Dados e Integração:

- Os dados no S3 podem ser acessados diretamente pela internet (com URLs pré-assinados) ou integrados a outros serviços da AWS, como **Amazon CloudFront** para distribuição de conteúdo, **Amazon Lambda** para processamento de arquivos, **Amazon Athena** para consultas SQL diretas em dados S3, entre outros.

#### 8. Custo:

- O S3 utiliza um modelo de **pagamento por uso**, onde você paga apenas pelo que usa. Os principais fatores que influenciam o custo incluem:
  - Volume de dados armazenados.
  - Número de requisições de leitura e gravação.
  - Transferência de dados (saída de dados para fora da AWS tem custos).

## RDS

O **Amazon RDS (Relational Database Service)** é um serviço gerenciado da AWS que facilita a configuração, operação e escalabilidade de bancos de dados relacionais na nuvem. Ele automatiza tarefas administrativas complexas, como provisionamento de hardware, backups, atualizações de software, e configuração de alta disponibilidade,

permitindo que os usuários se concentrem no desenvolvimento de suas aplicações em vez de gerenciar a infraestrutura de banco de dados.

### **Principais Características do Amazon RDS:**

#### **1. Bancos de Dados Suportados:**

- O Amazon RDS suporta vários **motores de banco de dados** populares:
  - **Amazon Aurora** (compatível com MySQL e PostgreSQL)
  - **MySQL**
  - **PostgreSQL**
  - **MariaDB**
  - **Oracle Database**
  - **Microsoft SQL Server**
- Com essas opções, o Amazon RDS oferece flexibilidade para escolher o banco de dados mais adequado às suas necessidades.

## **Amazon Neptune**

O **Amazon Neptune** é um serviço de banco de dados gerenciado, otimizado para trabalhar com **gráficos** (ou grafos), que oferece suporte aos principais modelos de dados em grafos, como **Property Graph** e **RDF (Resource Description Framework)**. Ele é projetado para armazenar e consultar grandes volumes de relacionamentos altamente conectados, proporcionando desempenho otimizado para aplicações que utilizam esses tipos de dados, como redes sociais, motores de recomendação e detecção de fraudes.

### **Principais Características do Amazon Neptune:**

#### **1. Suporte a Grafos:**

- O Neptune suporta dois modelos de grafos amplamente utilizados:
  - **Property Graph**: Utilizado com o framework **Gremlin**, da Apache TinkerPop, que é uma linguagem de consulta para navegar e manipular grafos de propriedade.
  - **RDF (Resource Description Framework)**: Usado com o padrão de consulta **SPARQL**, que é uma linguagem W3C padrão para consultas em grafos RDF. É amplamente utilizado na web semântica para modelar dados de forma que possam ser entendidos por máquinas.

#### **2. Consultas Otimizadas para Grafos:**

- O Neptune permite realizar consultas complexas em dados de grafos. Graças à sua estrutura otimizada, ele consegue navegar rapidamente em grafos e identificar relações entre os dados.
- **Gremlin** é utilizado para realizar consultas em Property Graph, permitindo operações como encontrar todos os vértices conectados a um nó ou calcular a distância mínima entre dois nós.
- **SPARQL** é utilizado para RDF, permitindo consultas sofisticadas em triplets RDF (sujeito, predicado, objeto) para inferir relações entre entidades.

## AWS GLUE

O **AWS Glue** é um serviço totalmente gerenciado de **extração, transformação e carregamento (ETL)** da AWS. Ele facilita a preparação e integração de dados para análises, machine learning ou outras finalidades. Com o Glue, você pode descobrir, catalogar, limpar e transformar dados provenientes de várias fontes, como bancos de dados relacionais, armazenamentos de dados no Amazon S3, entre outros, de forma fácil e automática.

### Principais Características do AWS Glue:

1. **ETL (Extração, Transformação e Carregamento):**
  - O AWS Glue ajuda a **extrair** dados de diferentes fontes, **transformá-los** conforme suas necessidades e depois **carregá-los** em destinos, como **data warehouses** ou **data lakes**, sem precisar gerenciar infraestrutura.
  - Você pode criar scripts ETL automaticamente com base em suas fontes de dados. O Glue gera código em **Python** ou **Scala**, que pode ser personalizado conforme necessário.

## VPC (Virtual Private Cloud)

A **VPC (Virtual Private Cloud)** da AWS é um serviço que permite criar uma rede virtual privada isolada dentro da infraestrutura da Amazon Web Services (AWS). Essa rede é altamente personalizável e dá controle total sobre o ambiente de rede, permitindo a configuração de sub-redes, tabelas de roteamento, gateways de internet e muito mais. Com a VPC, você pode definir como os seus recursos, como instâncias EC2, irão se comunicar entre si e com a internet ou outras redes.

### Principais Conceitos da VPC:

1. **Sub-redes (Subnets):**

- Uma VPC é dividida em **sub-redes**, que são segmentos da rede onde os recursos são implantados. Cada sub-rede é associada a uma **zona de disponibilidade (Availability Zone)** da região AWS.
- As sub-redes podem ser **públicas** ou **privadas**:
  - **Sub-rede Pública:** Tem acesso à internet através de um **Internet Gateway (IGW)**.
  - **Sub-rede Privada:** Não tem acesso direto à internet, geralmente usada para recursos que precisam ser isolados da internet pública, como bancos de dados.
- Cada sub-rede deve ter um intervalo de IPs (CIDR block) dentro do espaço da VPC.

## 2. Bloco CIDR (Classless Inter-Domain Routing):

- Ao criar uma VPC, você define um **bloco CIDR**, que determina o intervalo de endereços IP que serão usados na rede.
- Exemplo: Um bloco CIDR típico seria **10.0.0.0/16**, o que oferece até 65.536 endereços IP.
- Você pode dividir esse intervalo em sub-redes menores, como **10.0.1.0/24** para uma sub-rede e **10.0.2.0/24** para outra.

## 3. Tabela de Roteamento (Route Tables):

- As **tabelas de roteamento** determinam como o tráfego será encaminhado dentro da VPC. Elas contêm regras para rotear tráfego para diferentes destinos.
- Cada sub-rede é associada a uma tabela de roteamento. Por exemplo, uma tabela pode ter uma rota padrão (default route) que envia tráfego para o **Internet Gateway (IGW)**, permitindo que os recursos na sub-rede pública se comuniquem com a internet.

## 4. Internet Gateway (IGW):

- Um **Internet Gateway** permite que as instâncias dentro da sua VPC tenham comunicação com a internet pública. Ele é associado à VPC e atua como um ponto de saída para tráfego de internet.
- Para uma sub-rede ser pública, ela precisa ter uma rota na tabela de roteamento apontando para o IGW.

## 5. NAT Gateway / NAT Instance:

- O **NAT Gateway** ou **NAT Instance** permite que instâncias em sub-redes privadas façam **saída para a internet** (por exemplo, para baixar atualizações ou pacotes) sem estarem diretamente acessíveis de fora.
- O NAT traduz os endereços IP privados em endereços IP públicos para permitir a saída, sem expor esses recursos para conexões de entrada da internet.

## 6. VPN Gateway e Direct Connect:

- O **VPN Gateway** permite conectar a VPC à sua infraestrutura local via uma **VPN segura** sobre a internet.
- O **AWS Direct Connect** oferece uma conexão privada, dedicada e de alta largura de banda entre sua rede local e a AWS, sem passar pela internet pública.

## ACL

Uma **ACL (Access Control List)**, ou **Lista de Controle de Acesso**, na AWS é um mecanismo de segurança que atua no nível de sub-rede dentro de uma VPC (Virtual Private Cloud). As ACLs controlam o tráfego que entra e sai das sub-redes por meio de regras configuradas, aplicando-se tanto ao tráfego de entrada quanto ao de saída. Elas funcionam como **firewalls de rede**, proporcionando uma camada adicional de controle de segurança, complementando os **Security Groups**.

### Características Principais das ACLs:

#### 1. Aplicação a Sub-redes:

- As ACLs são aplicadas a **sub-redes inteiras**, enquanto os **Security Groups** são aplicados diretamente às **instâncias** individuais (por exemplo, instâncias EC2). Isso significa que as ACLs afetam todo o tráfego que entra ou sai de uma sub-rede, independentemente do recurso específico dentro dessa sub-rede.

#### 2. Regras Numeradas:

- Cada ACL é composta por um conjunto de **regras numeradas**, e essas regras são avaliadas em ordem crescente (do número mais baixo ao mais alto). A primeira regra que corresponder ao tráfego é aplicada.
- Cada regra define se o tráfego deve ser **permitido (allow)** ou **negado (deny)**, além de especificar o tipo de tráfego (porta, protocolo, IP de origem/destino).

## VPC Peering

**VPC Peering** na AWS é um recurso que permite a conexão direta entre duas **VPCs (Virtual Private Clouds)**, permitindo que o tráfego seja roteado entre elas usando endereços IP privados, sem a necessidade de passar pelo tráfego público da Internet ou criar conexões VPN. Esse tipo de conexão é feito por meio de uma **conexão de peering**, que cria um canal privado entre as duas VPCs, seja na mesma região da AWS ou entre regiões diferentes (peering inter-regional).

### Características do VPC Peering:

#### 1. Comunicação Direta via IP Privado:

- As instâncias em uma VPC podem se comunicar com instâncias em outra VPC diretamente usando endereços IP privados, sem a



necessidade de IPs públicos ou NAT. Isso facilita a comunicação segura e de baixa latência entre VPCs.

## VPC Flow Logs

Os VPC Flow Logs capturam informações sobre o tráfego IP que entra e sai de suas interfaces de rede em uma VPC (Virtual Private Cloud). Esses logs podem ser úteis para monitoramento de segurança, solução de problemas de conectividade de rede e análise de desempenho.

## Client e Site to Site VPN

Esses dois tipos de VPNs são usados para conectar redes locais ou dispositivos remotos à sua VPC:

- **Client VPN:** Permite que dispositivos individuais, como laptops, se conectem à sua VPC de forma segura usando um cliente VPN.
- **Site-to-Site VPN:** Conecta a rede local (on-premises) diretamente à sua VPC por meio de uma conexão VPN, criando um túnel criptografado para o tráfego de rede.

## AWS PrivateLink

PrivateLink permite acessar serviços da AWS de maneira privada, dentro da rede da AWS, sem expor o tráfego à internet. Ele usa endpoints de interface dentro da VPC para garantir comunicação segura com serviços da AWS ou de terceiros.

## AWS Direct Connect

O Direct Connect oferece uma conexão física privada entre a rede local (on-premises) e a AWS. Isso é útil para grandes volumes de dados, fornecendo uma conexão de alta largura de banda e baixa latência entre sua infraestrutura e a AWS, sem passar pela internet.

## AWS Transit Gateway

O Transit Gateway atua como um hub central para conectar várias VPCs, redes locais e até mesmo conexões com outras regiões da AWS. Ele facilita a interconexão de redes complexas ao simplificar a gestão de múltiplas conexões, criando uma infraestrutura de rede mais escalável.

## **Route53**

O Amazon Route 53 é um serviço de DNS (Domain Name System) escalável e altamente disponível. Ele faz o roteamento de usuários finais para aplicativos da internet, traduzindo nomes de domínio em endereços IP. Route 53 também oferece balanceamento de carga, monitoramento de integridade e roteamento de tráfego baseado em geografia.

### **Route53 Policies**

As políticas de roteamento do Route 53 determinam como o tráfego é distribuído para diferentes endpoints com base em critérios como latência, localização geográfica, integridade e peso (para dividir a carga). As principais políticas incluem:

- **Roteamento Simples**
- **Roteamento de Latência**
- **Roteamento Failover**
- **Roteamento Geográfico**

### **Configurando Route53**

Envolve a criação de zonas hospedadas para o domínio, onde você configura registros DNS que mapeiam nomes de domínio para recursos da AWS, como instâncias EC2, buckets S3, ou balanceadores de carga. Também é possível configurar verificações de integridade para monitorar o desempenho e a disponibilidade dos endpoints.

## **AWS CloudFront**

O CloudFront é uma rede de distribuição de conteúdo (CDN) que entrega dados, vídeos, aplicativos e APIs a clientes globalmente, com baixa latência e altas velocidades de transferência. Ele distribui o conteúdo a partir de servidores cache localizados em várias regiões, otimizando a entrega para os usuários com base em sua localização.

## **S3 Transfer Acceleration**

Esse recurso do Amazon S3 acelera as transferências de dados para e de um bucket S3, aproveitando a rede de borda distribuída do CloudFront. Ele melhora a velocidade de upload em longas distâncias geográficas, permitindo que os dados sejam transferidos de maneira mais rápida de diferentes locais do mundo.

## **AWS Global Accelerator**

O AWS Global Accelerator melhora a performance e a disponibilidade de aplicativos globais, utilizando a rede global da AWS para direcionar o tráfego do usuário para o endpoint mais próximo e de menor latência. Ele usa dois endereços IP Anycast estáticos para encaminhar o tráfego por rotas otimizadas, aumentando a resiliência e performance.

## **Amazon Elastic Container Registry (Amazon ECS)**

O Amazon ECS (Elastic Container Service) é um serviço gerenciado de orquestração de contêineres que permite executar, parar e gerenciar contêineres Docker em clusters de servidores gerenciados pela AWS. Ele é altamente integrado com outros serviços da AWS, como o IAM para controle de acesso e o CloudWatch para monitoramento.

### **Amazon Elastic Kubernetes Service (Amazon EKS)**

O Amazon EKS (Elastic Kubernetes Service) é um serviço gerenciado para executar o Kubernetes na AWS. Ele permite que você implemente, gerencie e escale aplicativos baseados em contêiner usando Kubernetes. O EKS automatiza a gestão da infraestrutura subjacente, como a configuração do cluster e upgrades de versão, enquanto mantém a compatibilidade com ferramentas e plug-ins nativos do Kubernetes.

### **AWS Kinesis**

O Amazon Kinesis é um serviço para coletar, processar e analisar dados em tempo real em grande escala. Ele é usado para trabalhar com fluxos de dados em tempo real, como logs de aplicativos, cliques em sites ou dados de dispositivos IoT. O Kinesis Streams permite que você capture e armazene dados de streaming, enquanto o Kinesis Firehose e o Kinesis Data Analytics oferecem maneiras de carregar dados e realizar análises em tempo real.

### **AWS SQS (Simple Queue Service)**

O Amazon SQS é um serviço de enfileiramento de mensagens gerenciado que facilita o desacoplamento de componentes de sistemas distribuídos. Ele oferece uma fila de mensagens para enviar, armazenar e receber mensagens entre diferentes componentes de uma aplicação sem perder dados. Ele suporta duas filas principais: Standard (com entrega em ordem, mas sem garantias de duplicidade) e FIFO (ordem garantida e sem duplicação).

### **AWS SNS (Simple Notification Service)**

O Amazon SNS é um serviço de mensagens push totalmente gerenciado que permite enviar notificações para endpoints ou dispositivos distribuídos, como e-mails, SMS, e sistemas de mensagens. Ele é comumente usado para publicar mensagens de sistemas ou aplicativos para vários assinantes simultaneamente. SNS também se integra com SQS, permitindo que mensagens enviadas pelo SNS sejam entregues em filas SQS.

### **AWS Batch**

AWS Batch é um serviço gerenciado que permite rodar trabalhos de computação em lote na nuvem. Ele organiza a execução de tarefas em clusters de instâncias EC2 gerenciadas, otimizando a alocação de recursos com base no volume e nas necessidades dos trabalhos. É ideal para processar grandes quantidades de dados ou executar tarefas intensivas de computação de forma escalável e eficiente.

### **AWS LightSail**

O AWS LightSail é uma solução simples para lançar e gerenciar servidores virtuais privados. Ele oferece uma interface amigável e recursos integrados para usuários que precisam de uma infraestrutura básica, como máquinas virtuais, bancos de dados, armazenamento e rede, sem a complexidade do EC2. Ele é voltado para desenvolvedores, pequenas empresas e pessoas que buscam uma alternativa mais simples ao EC2 para cargas de trabalho pequenas.

### **AWS Lambda**

O AWS Lambda é um serviço de computação sem servidor que permite executar código em resposta a eventos sem a necessidade de gerenciar servidores. Ele

funciona com base em eventos gerados por serviços da AWS (como S3, DynamoDB ou API Gateway) ou por invocações diretas. O Lambda escala automaticamente e cobra apenas pelo tempo de execução do código, tornando-o ideal para automação de tarefas, microsserviços e processamento de dados sob demanda.

### **AWS Fargate**

O AWS Fargate é uma tecnologia de computação serverless para contêineres, usada com Amazon ECS e EKS. Ele permite que você execute contêineres sem gerenciar instâncias de servidores ou clusters de máquinas. O Fargate cuida do provisionamento, escalabilidade e gerenciamento da infraestrutura necessária para rodar contêineres, liberando os desenvolvedores de tarefas operacionais e permitindo que se concentrem apenas nas aplicações.

### **AWS Well-Architected Framework**

O AWS Well-Architected Framework é um guia para ajudar a construir infraestruturas seguras, resilientes e eficientes na nuvem. Ele é baseado em seis pilares fundamentais para avaliar a arquitetura de qualquer aplicação.

#### **Pilar 1 - Excelência Operacional:**

Foca em operações que sustentam o desenvolvimento e a execução de workloads de maneira eficiente. Isso inclui automação, monitoramento e otimização de processos.

#### **Pilar 2 - Segurança:**

Concentra-se na proteção de dados, sistemas e ativos da empresa. Inclui a aplicação de controles de segurança, como criptografia, gerenciamento de identidade e conformidade com normas de segurança.

#### **Pilar 3 - Confiabilidade:**

Visa garantir que os sistemas possam se recuperar de falhas e cumprir as expectativas de disponibilidade. Isso envolve práticas de resiliência, como recuperação de desastres e replicação.

#### **Pilar 4 - Eficiência de Desempenho:**

Foca no uso eficiente de recursos computacionais para atender aos requisitos de desempenho e responder às demandas de forma eficaz.

#### **Pilar 5 - Otimização de Custos:**

Enfatiza a economia, otimizando o uso de recursos para evitar desperdícios. Esse pilar encoraja o uso eficiente de serviços e a escalabilidade conforme necessário para controlar gastos.

#### **Pilar 6 - Sustentabilidade:**

Introduzido mais recentemente, este pilar foca no impacto ambiental das arquiteturas. A sustentabilidade busca minimizar o consumo de recursos e maximizar a eficiência de energia em soluções na nuvem.

### **AWS Cloud Adoption Framework (CAF)**

O AWS Cloud Adoption Framework fornece diretrizes e boas práticas para facilitar a transição para a nuvem, considerando aspectos de negócios, governança e infraestrutura. Ele ajuda a alinhar estratégias de TI com os objetivos de negócios.

### **AWS EcoSystem**

Refere-se ao conjunto de serviços, ferramentas, parceiros e práticas oferecidos pela AWS que formam um ecossistema coeso para construir, gerenciar e otimizar soluções na nuvem.

### **AWS IQ**

AWS IQ é uma plataforma que conecta clientes com especialistas certificados da AWS para obter ajuda personalizada em projetos, como arquitetura, implementação e consultoria.

### **AWS Serviços Gerenciados**

Os AWS Managed Services são serviços da AWS que automatizam tarefas de gerenciamento de infraestrutura, como monitoramento, backups e segurança. Eles permitem que as empresas se concentrem em suas aplicações em vez de gerenciar a infraestrutura subjacente.

### **Amazon Cognito**

O Amazon Cognito facilita o gerenciamento de autenticação, autorização e sincronização de dados de usuários em dispositivos móveis e web. Ele oferece autenticação de usuários por meio de credenciais sociais ou corporativas, além de permitir login através de provedores de identidade.

### **Amazon Security Token Service (STS)**

O Amazon STS permite que você crie credenciais de segurança temporárias para usuários federados ou funções IAM. Essas credenciais temporárias podem ser usadas para acessar recursos da AWS de maneira segura e por um tempo limitado.

### **AWS Device Farm**

O AWS Device Farm é um serviço que permite testar e interagir com aplicações móveis e web em uma ampla variedade de dispositivos reais em tempo real. Ele ajuda a identificar problemas antes do lançamento, simulando diversos ambientes e condições.

### **AWS AppSync**

O AWS AppSync facilita a construção de APIs GraphQL que sincronizam dados em tempo real entre aplicativos móveis e web. Ele também gerencia automaticamente o acesso aos dados e a execução de resoluções em backends escaláveis.

### **AWS Amplify**

O AWS Amplify é uma plataforma que simplifica o desenvolvimento de aplicativos móveis e web, oferecendo ferramentas para backend, autenticação, armazenamento de dados, e hospedagem. Ele ajuda os desenvolvedores a criar aplicações escaláveis rapidamente.

### **AWS IoT Core**

O AWS IoT Core é uma plataforma gerenciada que permite a conexão de dispositivos de Internet das Coisas (IoT) à nuvem. Ele oferece suporte a milhões de dispositivos e pode processar grandes quantidades de mensagens enviadas por dispositivos conectados.

### **AWS Step Functions**

AWS Step Functions facilita a coordenação de vários serviços da AWS em fluxos de

trabalho automatizados. Ele permite o design visual de processos complexos como uma série de passos, coordenando a execução de funções Lambda e outros serviços.

### **Amazon AppFlow**

O Amazon AppFlow permite transferir dados de maneira segura entre serviços de SaaS (Software as a Service) e a AWS, sem a necessidade de desenvolver integração personalizada. Ele automatiza fluxos de dados entre aplicações como Salesforce, Zendesk e Slack.

### **AWS Backup**

AWS Backup é um serviço que centraliza e automatiza o backup de dados entre vários serviços da AWS, como Amazon EBS, RDS, DynamoDB e EFS. Ele oferece backup seguro, políticas de retenção e recuperação de desastres.

### **AWS Disaster Recovery Strategy**

Essa estratégia envolve a implementação de medidas e soluções que ajudam a recuperar a operação de sistemas e dados em casos de falha, desastre ou interrupção, garantindo a continuidade dos negócios com o mínimo de downtime.

### **AWS WorkSpaces**

O AWS WorkSpaces é um serviço que fornece desktops virtuais na nuvem, permitindo que usuários acessem seus ambientes de trabalho de qualquer lugar. Ele oferece um ambiente seguro e escalável para trabalho remoto ou híbrido.

### **AWS AppStream 2.0**

O AWS AppStream 2.0 permite o streaming de aplicações de desktop para qualquer navegador, sem a necessidade de instalação ou infraestrutura local. É ideal para aplicações pesadas que precisam ser acessadas de forma remota.