

# Material de apoio

O AWS Certified Cloud Practitioner valida o entendimento fundamental sobre a Nuvem da AWS, serviços e terminologia. Este é um bom ponto de partida na jornada da Certificação AWS para pessoas sem experiência prévia em TI ou nuvem migrando para uma carreira em nuvem, ou para funcionários de linha de negócio que buscam alfabetização básica em nuvem.

Categoria: Fundamental

Duração do exame: 100 minutos

Formato do exame: 65 perguntas de múltipla escolha

Custo: \$100



[www.linkedin.com/in/alice-beatriz-273a60179](https://www.linkedin.com/in/alice-beatriz-273a60179)

# Ementa

O exame AWS Certified Cloud Practitioner (CLF-C02) é destinado a indivíduos que conseguem demonstrar conhecimento geral sobre a AWS Cloud, independentemente de um cargo específico.

O exame valida a capacidade do candidato de realizar as seguintes tarefas:

- Explicar o valor da AWS Cloud.
- Entender e explicar o modelo de responsabilidade compartilhada da AWS.
- Compreender o AWS Well-Architected Framework.
- Entender as melhores práticas de segurança.
- Entender os custos, economia e práticas de faturamento da AWS Cloud.
- Descrever e posicionar os serviços principais da AWS, incluindo serviços de computação, rede, banco de dados e armazenamento.
- Identificar serviços da AWS para casos de uso comuns.

Domínios de conteúdo e suas respectivas ponderações:

- Domínio 1: Conceitos de Nuvem (24% do conteúdo avaliado)
- Domínio 2: Segurança e Conformidade (30% do conteúdo avaliado)
- Domínio 3: Tecnologia e Serviços de Nuvem (34% do conteúdo avaliado)
- Domínio 4: Cobrança, Preços e Suporte (12% do conteúdo avaliado)

<https://aws.amazon.com/certification/certified-cloud-practitioner/>

# Sumário

- 1.0 que é Cloud Computing e AWS Services?
- 2.Arquitetura e ecossistema AWS
- 3.Controle de acessos, monitoramento, segurança e compliance
- 4.Pricing
- 5.Cloud Computing
- 6.Armazenamento e DataBases
7. Machine Learning
- 8.Developer Tools
- 9.VPC & Networking
- 10.Mensageria
- 11.Outros serviços



O que é Cloud Computing e  
AWS Services?

## Componentes de um computador

Um computador é composto por hardware (partes físicas) e software (programas):  
Hardware é toda a parte física do computador – aquilo que você pode tocar.  
Ex.: teclado, mouse, CPU, memória, placa-mãe, monitor.  
Software é a parte lógica, ou seja, os programas e sistemas que fazem o hardware funcionar.  
Ex.: Windows, aplicativos, jogos, navegadores, planilhas.

- CPU (Processador) – faz cálculos e processa informações.
- GPU (Placa de vídeo) – Processa gráficos e imagens.
- RAM (Memória) – Armazena dados temporários.
- Placa-mãe – Conecta todos os componentes.
- Armazenamento (HD/SSD) – Guarda arquivos e sistema.
- Fonte de alimentação – Fornece energia ao sistema.
- Router (Roteador) – Direciona o tráfego entre redes.
- Switch – Conecta dispositivos dentro da mesma rede local.
- Firewall – Controla o tráfego e protege a rede.
- Server (Servidor) – Máquina que oferece serviços a outros dispositivos.
- Protocol (Protocolo) – Regras de comunicação entre dispositivos.
- IP Address – Endereço que identifica um dispositivo na rede.
- VPN – Conexão segura para acessar uma rede remotamente.



Podemos externalizar  
tudo isso?

SIM! Com computação  
em nuvem

## Estruturas

**On-premise:** Infraestrutura dentro da empresa, com servidores físicos próprios e manutenção interna.  
**Cloud:** Infraestrutura na internet, fornecida por provedores como AWS, Azure e Google Cloud.



## O que é Cloud Computing?

Computação em nuvem é o uso de servidores e serviços pela internet, em vez de depender do armazenamento ou processamento local no seu computador.

Você acessa programas, dados e recursos (como armazenamento, banco de dados, processamento, IA) pela internet, usando infraestrutura que pertence a empresas como AWS, Google Cloud, Azure etc.

## Benefícios no uso de Cloud

- Escalabilidade – Aumenta recursos rapidamente.
- Custo menor – Paga só pelo uso.
- Alta disponibilidade – Menos risco de ficar fora do ar.
- Segurança avançada – Ferramentas integradas dos provedores.
- Manutenção reduzida – Sem gerenciar servidores físicos.
- Acesso remoto – Usável de qualquer lugar.

## Tipos de Cloud

**1. Cloud Pública:** Infraestrutura compartilhada e fornecida por empresas como AWS, Azure, Google Cloud.

Vantagem: barata, escalável, fácil de usar.

**2. Cloud Privada:** Infraestrutura exclusiva para uma única empresa (pode ser interna ou hospedada).

Vantagem: mais controle e segurança dedicada.

**3. Cloud Híbrida:** Combina on-premise + cloud pública/privada.

Vantagem: flexibilidade para usar o melhor dos dois mundos.

## Tipos de Cloud Computing

**IaaS (Infrastructure as a Service):** Você utiliza infraestrutura básica na nuvem: servidores, redes, storage.

Ex.: você monta tudo do zero.

**PaaS (Platform as a Service):** Você usa uma plataforma pronta para desenvolver e rodar aplicações.

Ex.: não precisa gerenciar servidor ou sistema operacional.

**SaaS (Software as a Service):** Você usa um software pronto, direto no navegador ou app.

Ex.: e-mail, CRM, planilhas online.

## Precificação

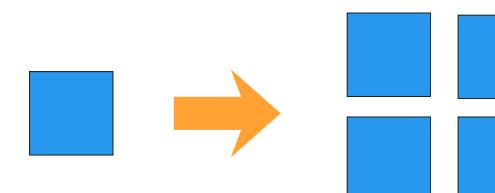
1. Pay as you go: pegue pelo uso
2. Economize quando você reservar (1 ou 3 anos)
3. Pague menos quanto mais você usar
4. Pague menos à medida que a AWS cresce

## Infraestrutura global

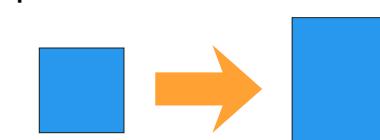
- Regions – Localizações geográficas onde a AWS opera, composta por 3 ou mais AZs, é um cluster de data centers, onde fica a infraestrutura física
- Availability Zones (AZs) – Datacenters independentes, mas conectados, dentro de cada região. Isso garante redundância em caso de falha.
- Edge Locations – Pontos de presença para entregar conteúdo com baixa latência.
- Local Zones – Infraestrutura AWS próxima do usuário para executar workloads com baixa latência
- Outposts – Equipamentos AWS instalados dentro do ambiente da empresa.

## Escalonamento

Escalonamento horizontal: adicionar ou remover mais servidores.



Escalonamento vertical: aumentar ou reduzir a potência de um único servidor



## Share responsibility

É o modelo onde AWS e cliente dividem responsabilidades de segurança  
AWS → Responsável pela segurança DA nuvem (infraestrutura, hardware, datacenters).

Cliente → Responsável pela segurança NA nuvem (dados, acessos, configurações, criptografia).



## O que é AWS Services?

Conjunto de serviços de cloud (computação, armazenamento, banco de dados, segurança, rede, IA, etc.) que você pode usar pela internet conforme a necessidade.

A AWS permite o uso normal de seus serviços para hospedar aplicações, armazenar dados, rodar sistemas e realizar integrações de forma segura e legal. No entanto, sua política de uso proíbe qualquer atividade ilegal, como fraudes, ataques cibernéticos não autorizados, envio de spam, hospedagem de malware, violações de direitos autorais, coleta indevida de dados e qualquer uso que cause prejuízo ou degradação aos serviços ou a outros clientes.

## Serviços locais VS regionais

Os serviços globais funcionam em toda a infraestrutura da AWS, sem depender de uma região específica. Um exemplo é o IAM, que gerencia identidades e permissões para toda a conta.

Já os serviços regionais operam dentro de uma região escolhida, como EC2, RDS e S3, porque precisam estar próximos dos dados ou do usuário para garantir desempenho, compliance e alta disponibilidade.

## Right Sizing

Prática de ajustar os recursos da AWS para o tamanho certo, evitando excesso ou falta de capacidade, com foco em reduzir custos e melhorar eficiência - usar o recurso certo, no tamanho certo, pelo tempo certo.

## Planos de suporte da AWS

- Basic: Sem suporte técnico (apenas conta e faturamento)
- Developer: Suporte técnico para ambientes de desenvolvimento
- Business: Suporte 24/7 para workloads em produção
- Enterprise: Suporte mission-critical com TAM (Technical Account Manager) dedicado

## Como escolher uma região?

- Latência – Escolha a região mais próxima dos usuários.
- Conformidade – Atenda leis locais de dados (ex.: manter no país).
- Serviços disponíveis – Nem todos os serviços existem em todas as regiões.
- Preço – Alguns serviços são mais baratos em certas regiões.
- Resiliência – Escolha regiões com múltiplas AZs bem distribuídas.



# Arquitetura e ecossistema AWS

# AWS Well-Architected Framework

6 pilares

## Operational Excellence (Excelência Operacional)

Capacidade de operar e monitorar sistemas para entregar valor e melhorar continuamente os processos. (AWS Cloud Formation ajuda nesse pilar).

1

- Operações como código (IAC)
- mudanças pequenas e reversíveis
- refinar procedimentos
- antecipar falhas
- aprender com falhas
- usar serviços gerenciados
- implementar observabilidade.

## Security (segurança)

Protege dados, sistemas e workloads contra acessos não autorizados e falhas, usando controle de acesso, criptografia e monitoramento.

2

- Identidade forte (IAM, MFA, menor privilégio)
- habilitar rastreabilidade (logs)
- segurança em todas as camadas
- automatizar práticas
- proteger dados em trânsito e repouso
- preparar para incidentes

## Reliability (confiabilidade)

Garante que o sistema continue funcionando mesmo com falhas, por meio de alta disponibilidade, backups e recuperação de desastres.

3

- testar procedimentos de recuperação
- recuperação automática
- escalar horizontalmente
- parar de adivinhar capacidade (auto scaling)
- gerenciar mudanças com automação

## Performance Efficiency (eficiência de performance)

Usa os recursos certos para cada carga de trabalho, garantindo desempenho eficiente e escalabilidade.  
Democratize tecnologias avançadas, go global in minutes.

4

- democratizar tecnologias avançadas
- go global fast
- usar arquiteturas serveless
- experimentar com frequência
- “mechanical sympathy” = entender serviços

## Cost Optimization (Otimização de Custos)

Busca reduzir gastos desnecessários, pagando apenas pelo que é usado e escolhendo recursos adequados.  
AWS Cost Explorer/AWS Trusted Advisor

5

- adotar modelos de consumo (pay-as-you-go)
- medir eficiência (cloudwatch)
- eliminar gastos com data center
- analisar e atribuir custos/rastreabilidade (tags)
- usar serviços gerenciados para reduzir TCO

## Sustainability (Sustentabilidade)

Reduz o impacto ambiental ao usar recursos de forma eficiente e evitar desperdícios.

6

- entender impacto e definir métricas
- estabelecer métricas de sustentabilidade
- maximizar utilização (right sizing)
- adotar hardware/software eficientes
- usar serviços gerenciados
- reduzir impacto downstream

# AWS Cloud Adoption Framework (CAF)

É um framework de orientação que ajuda organizações a planejar, preparar e executar a adoção da nuvem AWS de forma estruturada. Enquanto o Well-Architected Framework foca em arquitetura técnica, o CAF foca na jornada de adoção da nuvem (pessoas, processos e tecnologia).

## Business

A perspectiva empresarial ajuda a garantir que seus investimentos em nuvem acelerem suas ambições de transformação digital e resultados empresariais. Os stakeholders comuns incluem o CEO, CFO, COO, CIO e CTO.

## People

A perspectiva das pessoas serve como uma ponte entre Tecnologia e negócios, acelerando a jornada na nuvem para ajudar as organizações mais rapidamente evoluir para uma cultura de crescimento contínuo, aprendizado, e onde a mudança se torna o normal, com foco em cultura, estrutura organizacional, liderança e força de trabalho. Os stakeholders comuns incluem o CIO, COO, CTO, diretor de nuvem e líderes multifuncionais e empresariais.

## Governance

A perspectiva da governança foca em orquestrar seu iniciativas em nuvem enquanto maximizam os benefícios organizacionais e minimizam transformações riscos. Partes interessadas comuns Inclui diretor de transformação, CIO, CTO, CFO, CDO e CRO.

## Platform

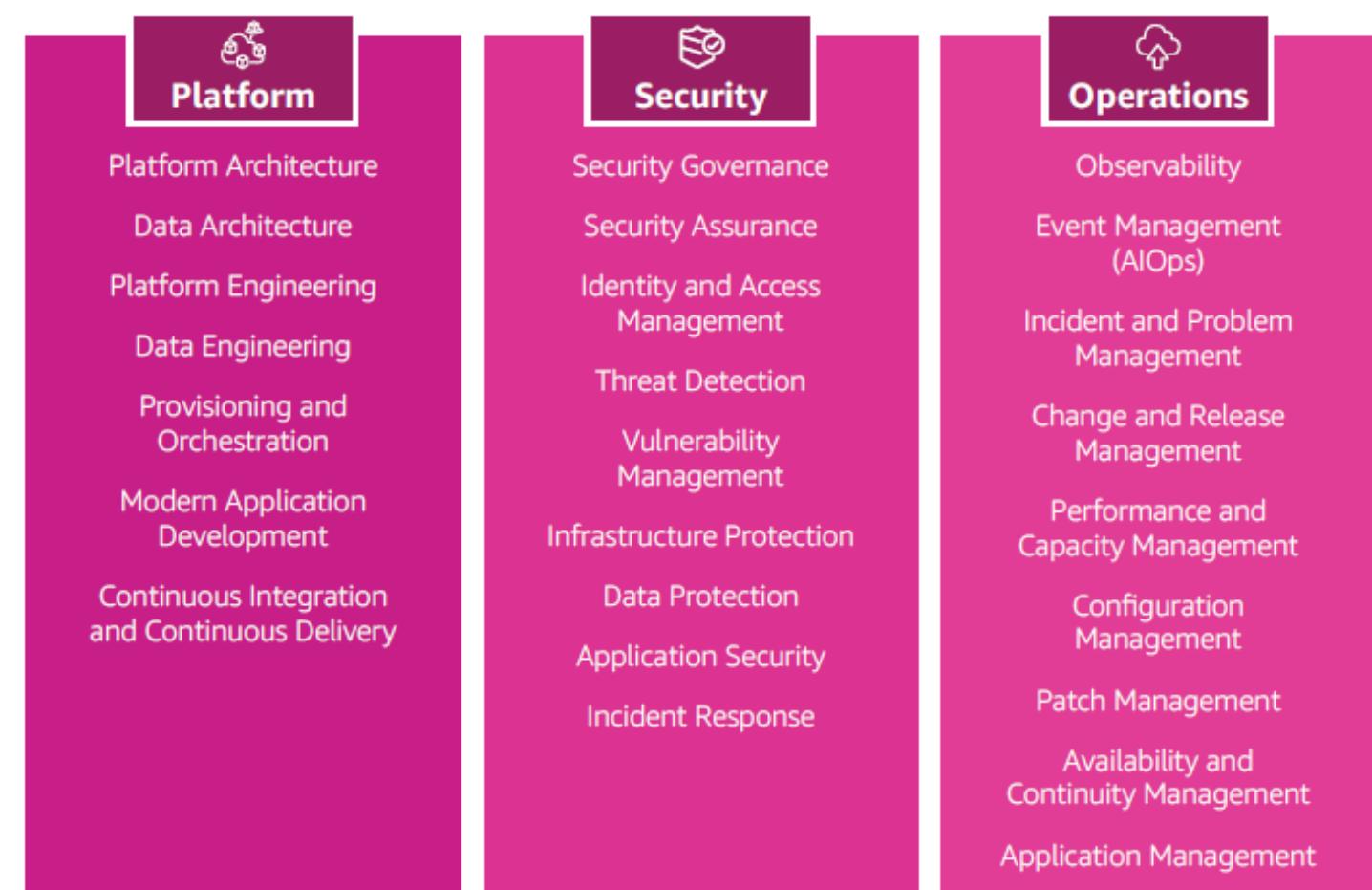
A perspectiva da plataforma foca em acelerar o Entrega das suas cargas de trabalho em nuvem por meio de um ambiente de nuvem híbrida, escalável e de nível empresarial. Os stakeholders comuns incluem o CTO, líderes tecnológicos, arquitetos e engenheiros.

## Security

A perspectiva de segurança ajuda você a alcançar o confidencialidade, integridade e disponibilidade dos seus dados e cargas de trabalho na nuvem. Ele é composto por nove Capacidades mostradas na figura a seguir. Stakeholders comuns incluem CISO, CCO, internos líderes de auditoria, arquitetos e engenheiros de segurança.

## Operations

A perspectiva operacional foca em garantir que a nuvem Os serviços são entregues em um nível acordado com os stakeholders do seu negócio. Automatizar e otimizar operações permitirá que você escala de forma eficaz enquanto melhora a confiabilidade das suas cargas de trabalho. Os stakeholders comuns incluem líderes de infraestrutura e operações, local engenheiros de confiabilidade e gerentes de serviços de tecnologia da informação.



# General Guiding Principles

Princípios Gerais de Orientação



## **Design para falhas**

Assuma que falhas podem acontecer e planeje a recuperação (ex.: múltiplas zonas de disponibilidade).

## **Automatize operações**

Use automação sempre que possível (deploy, escalabilidade, monitoramento).

## **Escale horizontalmente**

Prefira adicionar mais recursos menores (instâncias, containers) ao invés de aumentar uma única instância gigante.

## **Mantenha simplicidade**

Arquiteturas simples são mais fáceis de gerenciar, escalar e proteger.

## **Itere e aprenda**

Melhore constantemente a arquitetura com base em métricas e feedback.

## **Proteja dados e sistemas**

Use criptografia, controles de acesso e monitoramento.

## **Otimize para eficiência e custo**

Escolha recursos adequados, desligue o que não precisa e use classes de armazenamento/capacidade corretas.

# Disaster Recovery Strategies

Existem 4 abordagens, cada uma com custo e velocidade diferentes:

RTO → tempo máximo aceitável para recuperar o serviço

RPO → quantidade máxima de dados que pode ser perdida (em termos de tempo)

## Backup e restauração

Backup regulares em s3 e Glacier, restauração quando necessário.

- RTO: horas e dias
- depende da frequência do backup
- Custo baixo
- Indicado para sistemas não crítico

## Pilot light

Mantém uma versão mínima do ambiente ativa em outra região, escala quando corre desastre

- RTO: horas
- RPO: minutos
- Custo médio

## Warm Standby

Uma cópia reduzida do ambiente roda continuamente em outra região.

- RTO: minutos
- RPO: segundos
- Custo alto

## Multi-site (ativo/ativo)

Ambientes completos ativos em múltiplas regiões.

- RTO: segundos
- RPO: praticamente zero custo
- Custo muito alto



## AWS Elastic Disaster Recovery (DRS)

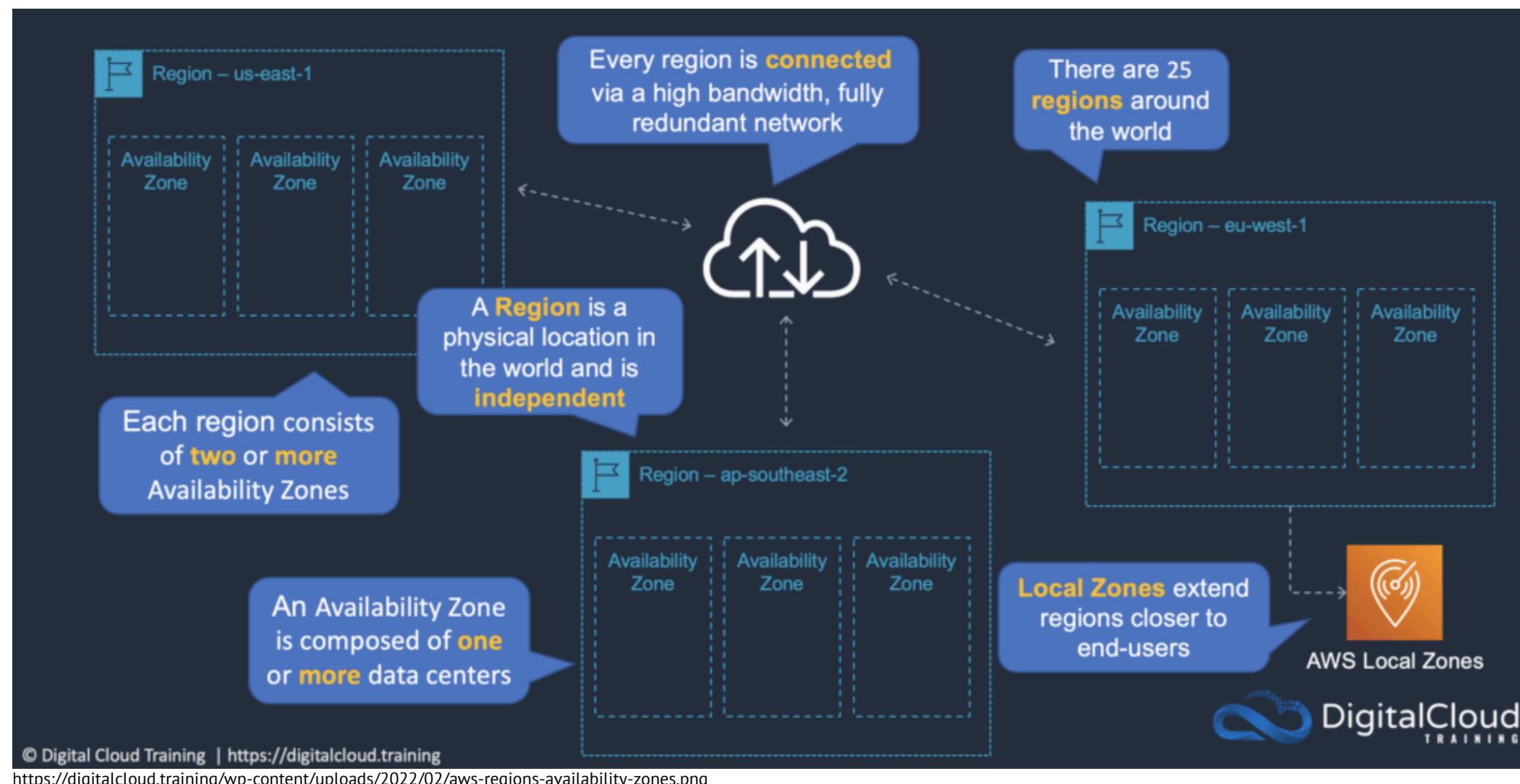
Permite recuperação rápida e confiável de aplicações on-premises, virtuais ou baseadas em nuvem para a AWS, minimizando RTO e RPO.

- Instala-se um agente leve nos servidores de origem, os dados são replicados continuamente em nível de bloco para um sub-rede de staging na sua conta AWS, usando armazenamento acessível e computação mínima para reduzir custos.

Em caso de desastre/teste, você pode lançar instâncias de recuperação na AWS em poucos minutos, no estado mais recente ou em um ponto anterior no tempo.

# Infraestrutura Global da AWS

A infraestrutura global da AWS é projetada para fornecer alta disponibilidade, baixa latência, e resiliência a desastres, permitindo que as organizações aproveitem os benefícios de uma arquitetura escalável e segura. A AWS tem uma infraestrutura distribuída mundialmente, composta por Regiões, Zonas de Disponibilidade (AZs) e Edge Locations, que são fundamentais para fornecer uma série de vantagens em termos de desempenho, recuperação de desastres, proteção contra ataques, e muito mais.



## Decreased Latency

A latência é o tempo que leva para os dados viajarem entre o usuário e o servidor. A infraestrutura global da AWS ajuda a reduzir a latência de várias maneiras:

- Distribuição de Serviços em Diversas Regiões:** A AWS tem centros de dados em diversas partes do mundo, permitindo que os serviços sejam hospedados próximos aos seus usuários.
- Amazon CloudFront e Edge Locations:** O Amazon CloudFront, a rede de CDN (Content Delivery Network) da AWS, usa Edge Locations para armazenar em cache dados mais próximos do usuário final.
- Escolha de Região Apropriada:** próxima do seu público-alvo

## Disaster Recovery

A AWS oferece um plano de recuperação de desastres (DR) robusto, que permite que as organizações garantam disponibilidade contínua e recuperação rápida de dados e serviços em caso de falhas. A infraestrutura global ajuda na disponibilidade e resiliência com as seguintes práticas:

- Zonas de Disponibilidade (AZs):** As AZs são fisicamente isoladas, mas interconectadas. Em caso de falha de uma AZ, outras AZs dentro da mesma região podem continuar a operar, garantindo alta disponibilidade e continuidade de serviços.
- Backups e Replicação:** A AWS facilita a replicação de dados entre Regiões ou AZs, permitindo backups em tempo real e a capacidade de recuperar dados rapidamente em caso de desastre.
- Armazenamento Resiliente:** Serviços como Amazon S3 e Amazon EBS oferecem armazenamento redundante, garantindo que os dados sejam preservados mesmo durante falhas de hardware.

# Global Application Architecture

A Global Application Architecture na AWS se refere à prática de projetar aplicações que operam globalmente, aproveitando a infraestrutura distribuída da AWS para oferecer alta disponibilidade, baixa latência e resiliência a falhas, atendendo usuários em qualquer lugar do mundo.

## Princípios

- Distribuição geográfica
- Balanceamento de tráfego
- Replicação e sincronização de dados
- Cache e otimização de conteúdo
- Alta disponibilidade e failover
- Segurança global

## Benefícios de uma arquitetura global

- Baixa latência para usuários em qualquer lugar.
- Alta disponibilidade e resiliência a falhas regionais.
- Escalabilidade global para atender picos de tráfego.
- Melhoria da experiência do usuário com conteúdo rápido e confiável.
- Continuidade de negócios com recuperação rápida de desastres.

Ao projetar a arquitetura de aplicações, a escolha entre Single Region Single AZ, Single Region Multiple AZs e Multi-Region impacta alta disponibilidade, tolerância a falhas e latência. Aqui está um resumo detalhado:

Arquitetura	Número de AZs/Regiões	Disponibilidade	Latência	Custo	Casos de Uso
Single Region, Single AZ	1 AZ	Baixa	Muito baixa	Baixo	Teste, desenvolvimento, protótipos
Single Region, Multiple AZs	2+ AZs na mesma região	Alta	Baixa	Médio	Produção crítica, bancos de dados, sistemas web
Multi-Region	2+ regiões	Muito alta	Global	Alto	Aplicações globais, streaming, DR, serviços

# Serviços relacionados



## AWS Well-Architected Tool

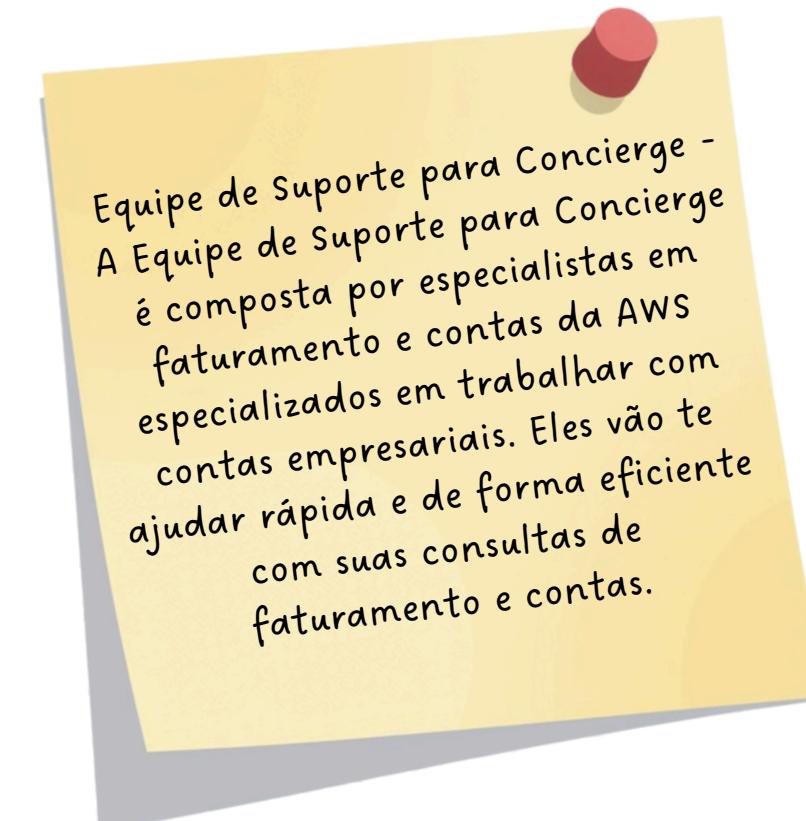
É uma ferramenta gratuita da AWS, disponível no console, usada para avaliar workloads com base no AWS Well-Architected Framework. Ela ajuda a identificar riscos arquiteturais e fornece recomendações de boas práticas.



## AWS Managed Services (AMS)

É um serviço da AWS que oferece gerenciamento contínuo e automatizado de workloads e infraestrutura na nuvem, ajudando empresas a operar ambientes complexos com segurança e confiabilidade, sem precisar de tanta intervenção manual.

Ele é voltado para organizações que querem adotar a nuvem de forma segura, mas sem aumentar muito a equipe interna.



## Support



## AWS IQ

Serviço que conecta clientes a consultores e especialistas certificados pela AWS para ajudar em projetos de nuvem.

Ele é voltado para quem precisa de suporte profissional especializado sem contratar alguém permanentemente



## AWS re:Post

É uma plataforma de Q&A comunitária para AWS, onde você pode fazer perguntas e especialistas/membros da comunidade ou até a AWS podem responder



## AWS Partner Network (APN)

É a rede de parceiros da AWS, formada por empresas e consultores que ajudam clientes a projetar, migrar, implementar e gerenciar soluções na AWS. Ele conecta clientes a empresas especializadas e certificadas, que oferecem serviços ou softwares integrados à AWS.



## AWS Marketplace

É uma loja online de softwares e serviços de terceiros que você pode usar na AWS. Ele facilita descobrir, testar, comprar e implantar aplicações prontas na nuvem.

- Ajuda a economizar tempo e simplificar implantação
- Não é um serviço de infraestrutura por si só

# Cloud Migration Strategies: The 7Rs

## Retain (reter)

- Manter aplicações no ambiente atual (on-premise) por questões de compliance ou dependências;
- Util quando não há necessidade imediata de migração.

## Retire (aposentar)

- Desativar sistemas obsoletos ou sem valor de negócio
- Reduz custos e riscos de segurança

## Relocate (relocar)

- Mover workloads para outros provedor ou região sem alterar arquitetura (ex.: VMWare Cloud on AWS)

## Rehost (Life and shift)

- Migrar aplicações “como estão” para a AWS sem mudanças significativa. Ex.: usar AWS Application Migration Service
- Vantagem: rápido e baixo risco

## Replatform (lift and reshape)

- Pequenas otimizações antes ou durante a migração
- Ex.: mover banco para Amazon RDS ou app para Elastic Beanstalk

## Repurchase (Drop and Shop)

- Substituir por uma solução SaaS
- Ex.: CRM → Salesforce ou HR → workday

## Refactor/Re-architect

- Redesenhar a aplicação para ser cloud-native
- Ex.: migrar para arquitetura serveless com AWS Lambda e S3.



## AWS Migration Evaluator

O AWS Migration Evaluator ajuda a planejar e otimizar a migração para a nuvem, fornecendo uma avaliação detalhada de custos para mover suas cargas de trabalho para a AWS.

Quando usar: Antes de começar a migração, para avaliar a viabilidade financeira e os custos operacionais da nuvem.



## AWS Migration Hub

Gerenciamento e rastreamento de migrações em andamento, fornecendo uma plataforma central para acompanhar o progresso de todas as etapas da migração de maneira coordenada.

Quando usar: Durante a migração de cargas de trabalho para a AWS, para monitorar e gerenciar o status da migração de forma eficiente.



## AWS Migration and Modernization Services

AWS MGS é um conjunto de serviços e ferramentas que oferece suporte para migrar aplicações, dados e infraestrutura para a nuvem da AWS, além de ajudar na modernização dessas aplicações para aproveitar ao máximo os recursos da nuvem. É ideal para empresas que estão movendo suas operações para a AWS e desejam modernizar suas aplicações ao longo do caminho.



# Support Plans Pricing

A AWS oferece diferentes planos de suporte que variam de acordo com o nível de suporte e os serviços incluídos, permitindo que os clientes escolham o plano mais adequado às suas necessidades e ao tamanho da sua operação. Os AWS Support Plans são essenciais para quem busca assistência técnica, consultoria em nuvem ou gerenciamento avançado de infraestrutura na AWS.

Existem 4 tipos principais de planos de suporte da AWS:

## Basic Support (Gratuito)

- Disponível para todos os clientes da AWS.
- Sem custo adicional.
- Acesso limitado à documentação, fóruns e painel de saúde (AWS Personal Health Dashboard).
- Sem suporte técnico direto (não há suporte por telefone, chat ou e-mail).
- Ideal para uso básico de AWS.

## Business Support (A partir de US\$ 100/mês)

- Suporte 24/7 (telefone, chat e e-mail).
- Tempo de resposta rápido para problemas críticos (1 hora para nível 1).
- Recomendações do AWS Trusted Advisor.
- Acesso a engenheiros especializados para questões mais complexas.
- Custo: 3% da fatura mensal da AWS, com valor mínimo de US\$ 100/mês.

## Developer Support (A partir de US\$ 29/mês)

- Suporte via e-mail durante o horário comercial.
- Tempo de resposta de 12 horas para questões de baixo impacto.
- Ideal para desenvolvedores que estão começando ou em fase de desenvolvimento de soluções.

## Enterprise Support (A partir de US\$ 15.000/mês)

- Suporte 24/7 com resposta imediata para incidentes críticos.
- Consultoria personalizada com gerentes de conta técnico (TAMs).
- Ideal para empresas grandes ou que têm infraestruturas complexas e críticas.
- Custo: 10% da fatura mensal da AWS (para faturas acima de US\$ 500.000/mês), com valor mínimo de US\$ 15.000/mês.

# Multi account strategies

Multi-Account Strategies na AWS referem-se a práticas e abordagens usadas para gerenciar várias contas AWS de forma eficiente, escalável e segura. Muitas organizações optam por adotar essa abordagem para separar ambientes (como desenvolvimento, teste, produção), melhorar a segurança, otimizar custos, ou atender a requisitos de governança. O uso de múltiplas contas é uma maneira fundamental de organizar e gerenciar recursos de forma mais controlada na AWS.

## Principais Benefícios

- Segurança: Isola ambientes (ex: produção e desenvolvimento), reduzindo riscos e melhorando o controle de permissões.
- Otimização de Custos: Facilita o controle de custos por conta e possibilita descontos por volume com a consolidação de faturas.
- Governança: Permite aplicar políticas consistentes, como SCPs, e facilita auditorias.
- Escalabilidade: Facilita o crescimento, criando novas contas conforme necessário.

## Exemplos de Estratégias

- Por ambiente: Separar contas para desenvolvimento, teste e produção.
- Por departamento: Criar contas separadas para cada área (ex: TI, Marketing, Vendas).
- Por função específica: Contas para segurança, rede, CI/CD, etc.

## Ferramentas

- AWS Organizations: Para gerenciar múltiplas contas e aplicar políticas centralizadas.
- AWS Control Tower: Automatiza a governança e a configuração inicial de contas.
- AWS IAM: Gerencia acessos de usuários por conta.
- AWS SSO: Centraliza o login para várias contas.

# Penetration testing on AWS Cloud

O Penetration Testing (Teste de Penetração) na AWS é uma prática de avaliar a segurança das suas aplicações e recursos na nuvem simulando ataques reais, de forma controlada, para identificar vulnerabilidades antes que invasores as explorem.

Na AWS, existem regras e permissões específicas para realizar esses testes com segurança e sem violar políticas.



## O que é Penetration Testing

- É um teste ético de segurança para encontrar falhas em sistemas.
- Envolve simular ataques como:
  - Exploração de vulnerabilidades de rede
  - Teste de autenticação e autorização
  - Injeção de código ou SQL injection (em aplicações)
- Ajuda a melhorar a postura de segurança e proteger dados e serviços.

## Casos de uso

- Testar aplicações web e APIs na nuvem.
- Avaliar configurações de rede e firewall.
- Identificar vulnerabilidades em instâncias EC2 e bancos de dados.
- Melhorar segurança geral e compliance.

## Destaques

- Penetration Testing é teste ético de segurança na nuvem.
- AWS permite pentests em muitos serviços sem precisar de autorização prévia.
- Ajuda a encontrar e corrigir vulnerabilidades antes que hackers explorem.
- Deve ser realizado de forma controlada e seguindo políticas AWS.

## Como funciona na AWS

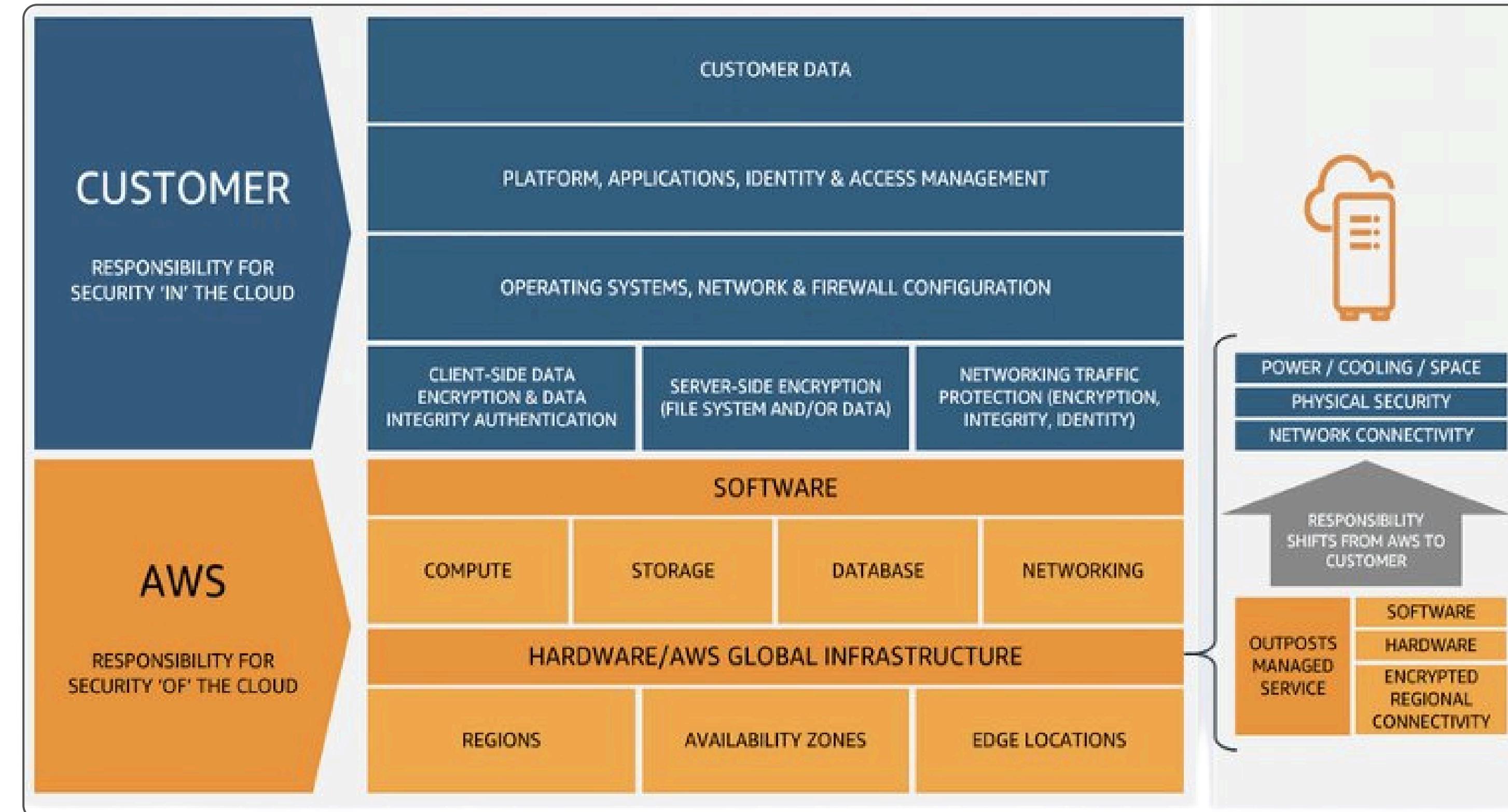
1. Serviços permitidos para teste sem autorização prévia
  - a. EC2, RDS, CloudFront, API Gateway, Lambda, Lightsail, entre outros
2. Serviços que exigem autorização prévia
  - a. Alguns serviços mais sensíveis ou gerenciados podem precisar de contato com o AWS Security Team.
3. Ferramentas e relatórios
  - a. Use ferramentas padrão de pentest (Nmap, Burp Suite, OWASP ZAP, etc.) para testar vulnerabilidades.
  - b. Documente resultados e corrija vulnerabilidades identificadas.

## Atividades proibidas

Prohibited Activities na AWS são ações que violam políticas, leis ou segurança, como ataques, abuso de recursos ou atividades ilegais, e não podem ser realizadas na plataforma.

- Têm o objetivo de proteger a infraestrutura da AWS, outros clientes e a conformidade legal.
- Estão descritas nos Termos de Serviço (AWS Acceptable Use Policy).
- Elas incluem atividades ilegais, ataques, abuso de recursos e interferência em terceiros.
- Seguir essas regras é importante para manter a conta segura e em conformidade.

# Shared responsibility model diagram



# Explicação do Modelo de Responsabilidade Compartilhada

O modelo de responsabilidade compartilhada da AWS descreve claramente o que é responsabilidade da AWS e o que é responsabilidade do cliente.

AWS é responsável pela segurança da nuvem ("Security of the Cloud"). Isso inclui proteger a infraestrutura física (hardware), a rede, os data centers e as camadas de virtualização (como a camada do sistema operacional host).

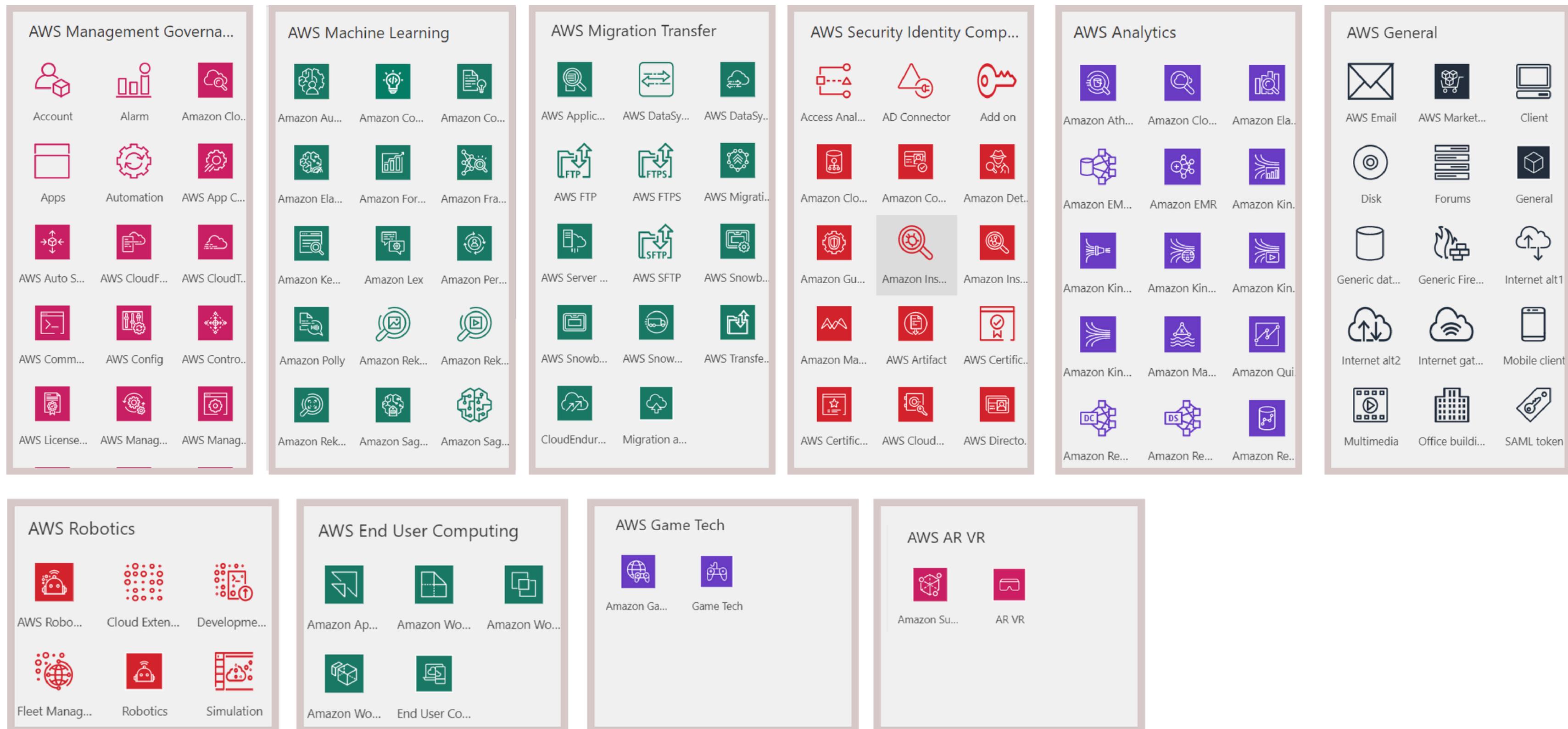
O cliente é responsável pela segurança dentro da nuvem ("Security in the Cloud"). Ou seja, o cliente precisa gerenciar e proteger o que ele coloca na AWS, como:

- Gerenciar os sistemas operacionais das instâncias EC2 (incluindo atualizações e patches de segurança),
- Gerenciar os aplicativos e software que instala nas suas instâncias EC2,
- Configurar asseguranças de rede (grupos de segurança, firewalls, etc.).

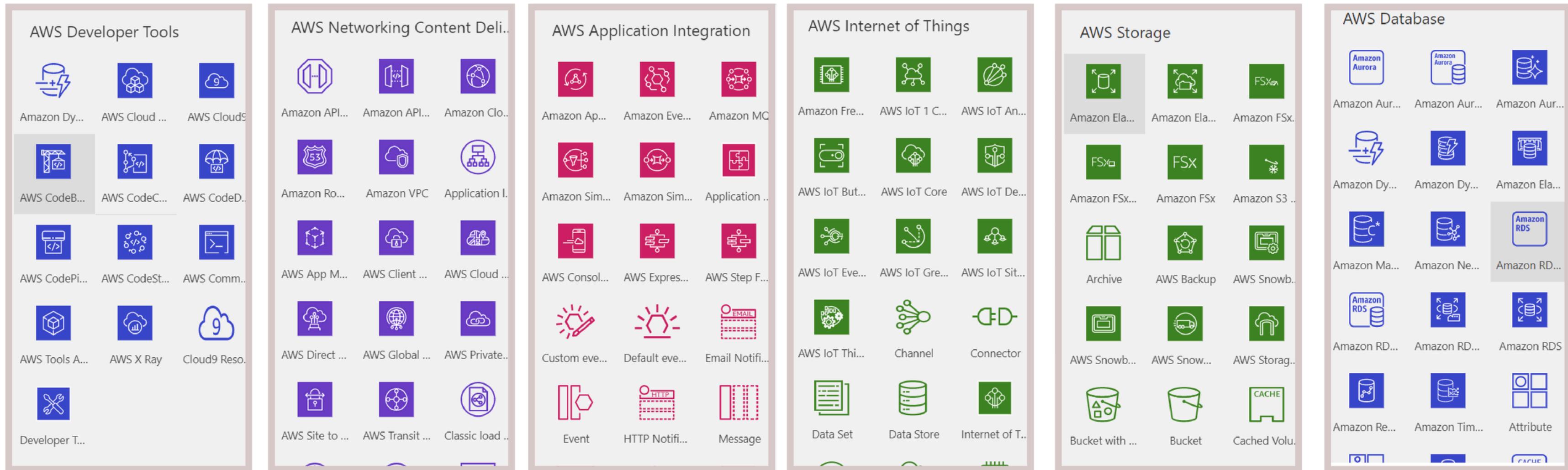
Exemplos de como pode cair na prova:

- Patching/fixing flaws within the AWS infrastructure: Esta é uma responsabilidade da AWS. Eles gerenciam a infraestrutura física, virtualização, redes e a segurança dessa infraestrutura. O cliente não precisa corrigir falhas na infraestrutura da AWS.
- Availability Zone (AZ) infrastructure management: Também é responsabilidade da AWS. Ela gerencia as zonas de disponibilidade e garante que a infraestrutura nelas seja segura e funcional.
- Managing patches of the guest operating system on Amazon EC2: Esta é a responsabilidade do cliente, como já mencionado. O cliente deve manter o sistema operacional das suas instâncias EC2 atualizado, o que inclui aplicar patches de segurança e atualizações de software.
- Configuration management for AWS global infrastructure: Novamente, é responsabilidade da AWS. A AWS gerencia a configuração e manutenção da infraestrutura global, enquanto o cliente é responsável apenas pelas configurações das suas próprias instâncias e serviços dentro da nuvem.

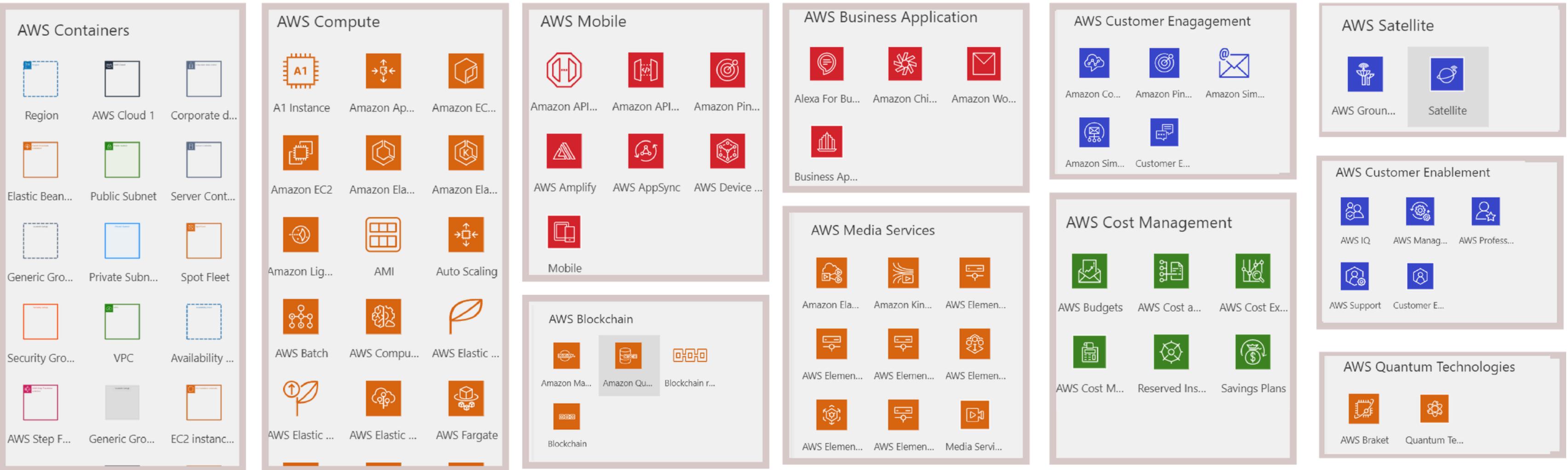
# Ícones e cores na AWS



# Ícones e cores na AWS



# Ícones e cores na AWS





Controle de acessos,  
monitoramento, segurança e  
compliance



## IAM Identity **GRATIS**

IAM (Identity and Access Management) é o serviço da AWS responsável por gerenciar identidades, acessos e permissões dentro da sua conta.

### Contexto

AWS Identity and Access Management é uma ferramenta poderosa para gerenciar o acesso com segurança a seus recursos AWS. Um dos principais benefícios de usar o IAM é a possibilidade de conceder concessões compartilhadas acesso à sua conta AWS. Além disso, o IAM permite você deve atribuir permissões granulares, permitindo controlar exatamente quais ações são diferentes Os usuários podem atuar em recursos específicos. Esse nível de controle de acesso é crucial para Manter a segurança do seu ambiente AWS. O IAM também oferece vários outros recursos de segurança. Você pode adicionar autenticação multifator (MFA) para uma camada extra de proteção e alavancagem federação de identidades para integrar de forma fluida usuários da sua rede corporativa ou de outros Provedores de identidade. O IAM também se integra ao AWS CloudTrail, fornecendo registros detalhados e informações de identidade para apoiar os requisitos de auditoria e conformidade. Por Aproveitando essas capacidades, você pode ajudar a garantir o acesso ao seu recursos críticos da AWS são rigidamente controlados e seguros.

É o serviço que controla quem pode acessar o quê na AWS.

- IAM é global – Não depende de região.
- Permissão mínima – Recomenda-se conceder apenas o necessário.
- Suporte a MFA – Autenticação de múltiplos fatores para proteger contas.
- Integração com serviços AWS – Quase tudo na AWS usa IAM.

### Conceitos

- Users (Usuários) – Identidades individuais que precisam acessar a AWS.
- Groups (Grupos) – Conjunto de usuários com permissões semelhantes.
- Roles (Funções) – Identidades sem login direto, usadas por serviços ou aplicações.
- Policies (Políticas) – Regras em JSON que definem permissões (Allow/Deny).

### Como funciona?

- Você cria usuários/grupos ou roles.
- Anexa políticas para determinar quais ações podem ser executadas (ex.: s3>ListBucket, ec2:StartInstances).
- IAM controla acesso de forma segura e granular.



### Root account

A root account é a conta principal da AWS – a primeira criada quando você abre sua conta. Ela tem acesso ilimitado a absolutamente tudo.

Por ser extremamente poderosa, ela é usada apenas para tarefas críticas, como gerenciar informações de pagamento, fechar a conta ou recuperar acessos. Justamente por ter privilégios máximos, é considerada perigosa se mal utilizada, já que nenhuma política IAM limita suas ações. Por isso, as boas práticas recomendam habilitar MFA, nunca usá-la no dia a dia e criar usuários ou roles do IAM para as operações normais. Para a certificação Cloud Practitioner, é importante entender que a root account tem controle absoluto e deve ser protegida e utilizada apenas quando necessário.

### IAM Credentials Report

Relatório gerado pela AWS que mostra o estado das credenciais de todos os usuários IAM da conta, incluindo senhas, chaves de acesso, MFA habilitado, rotação de credenciais e uso recente. Ele serve para verificar se as práticas de segurança estão sendo seguidas e identificar riscos, como usuários sem MFA ou chaves antigas demais.

### IAM Access Advisor

Mostra quais serviços da AWS um usuário, grupo ou role pode acessar e quando cada serviço foi usado pela última vez. Ele ajuda a identificar permissões excessivas e a aplicar o princípio de privilégio mínimo removendo acessos que não estão sendo utilizados.

### AWS CLI (Command Line Interface)

Ferramenta que permite gerenciar serviços da AWS pelo terminal, usando comandos em vez do console web. Com ela, você pode criar, configurar e automatizar recursos como EC2, S3, IAM e muitos outros, facilitando automação, scripts e operações repetitivas. É muito usada por desenvolvedores, administradores e equipes de DevOps para ganhar rapidez e padronização nas tarefas.

Ações como alterar informações de pagamento, fechar a conta AWS, alterar informações de segurança da conta, gerenciar permissões/usuários, gerenciar faturas e impostos, alterar configurações de regiões e AZs, modificar chaves do AWS KMS só podem ser feitas pela root account



## STS - Security token service

O AWS Security Token Service (STS) é um serviço da AWS que **permite conceder acesso temporário e seguro aos recursos da AWS, sem usar credenciais permanentes** (como access keys fixas).

Ele gera credenciais temporárias, compostas por:

- Access Key ID
- Secret Access Key
- Session Token

Com tempo de validade limitado

Essas credenciais expiram automaticamente, aumentando a segurança.



## Amazon Directory Service (AD)

O AWS Directory Service – Active Directory (AD) é um serviço gerenciado da AWS que **permite usar o Microsoft Active Directory na nuvem**, sem precisar administrar servidores AD manualmente.

Ele é usado para gerenciar usuários, grupos e permissões de forma centralizada, especialmente em ambientes Windows e corporativos.



## Amazon Cognito

O Amazon Cognito é um serviço da AWS que **fornecce autenticação, autorização e gerenciamento de usuários para aplicações web e mobile**.

Ele permite que você adicione cadastro, login e controle de acesso de usuários aos seus aplicativos web e móveis em questão de minutos. sem você precisar construir todo um sistema de identidade do zero.

- Criar e gerenciar cadastro e login de usuários
- Controlar acesso a aplicações
- Integrar login com Google, Facebook, Apple, etc.
- Usar MFA (autenticação multifator)



## Amazon IAM Identity Center

O AWS IAM Identity Center (antigo AWS Single Sign-On – SSO) é um serviço da AWS que **permite gerenciar o acesso de pessoas** (usuários) a múltiplas contas e aplicações AWS **usando login único (SSO)** - Use o IAM Identity Center para escalar o acesso de forma segura entre contas e aplicações AWS.

Ele centraliza identidades, permissões e autenticação em um único lugar.

Com ele você pode:

- Criar login único (SSO) para a AWS
- Gerenciar acesso a várias contas AWS
- Atribuir permissões por grupos
- Integrar com provedores externos (Active Directory, Okta, Azure AD)
- Controlar acesso a aplicações corporativas

1. Como funciona: o usuário faz login uma vez, escolhe a conta AWS e a role e acessa a AWS sem precisar de várias senhas

IAM é o controle de acesso técnico e detalhado dentro de uma conta AWS.  
IAM Identity Center é o gerenciador central de usuários e acessos para várias contas, focado em pessoas.



## IAM Access Analyzer

IAM Access Analyzer é um serviço da AWS que ajuda a identificar e **monitorar acessos externos aos recursos da sua conta AWS**. Ele verifica se há políticas de IAM (Identity and Access Management) ou configurações de recursos que permitem acesso de entidades externas (como usuários, grupos ou serviços de outras contas ou da internet) aos seus recursos. O IAM Access Analyzer é uma ferramenta importante para melhorar a segurança e a visibilidade da sua infraestrutura na AWS, ajudando a identificar excessos de permissões que poderiam resultar em riscos de segurança.



## AWS GuardDuty

A Amazon GuardDuty é um serviço de detecção de ameaças que monitora continuamente suas contas e cargas de trabalho AWS em busca de atividades maliciosas e entrega descobertas detalhadas de segurança para visibilidade e remediação, utilizando IA e ML com inteligência de ameaças integrada da AWS e de terceiros.

- Gera findings (alertas) quando encontra algo suspeito.



## AWS Inspector

O Amazon Inspector identifica automaticamente cargas de trabalho, como instâncias do Amazon Elastic Compute Cloud (Amazon EC2), imagens de contêineres e funções AWS Lambda, além de repositórios de código, e os analisa em busca de vulnerabilidades de software e exposição não intencional na rede. Ele ajuda a identificar possíveis falhas de segurança, configurações inadequadas e vulnerabilidades conhecidas nas instâncias da AWS, promovendo a segurança e conformidade de suas aplicações e infraestrutura.

- Ele oferece relatórios detalhados e recomendações de correção, permitindo que você corrija as falhas identificadas antes que sejam exploradas.
- Ele pode ser integrado com outros serviços de segurança da AWS, como Security Hub, CloudTrail e AWS Config, para oferecer uma abordagem de segurança mais abrangente.



## AWS Detective

O Amazon Detective coleta automaticamente dados de log dos seus recursos AWS e utiliza aprendizado de máquina (ML), análise estatística e teoria dos grafos para construir um conjunto de dados que você pode usar para conduzir investigações de segurança mais eficientes. Ele facilita a análise, investigação e identificação da causa raiz de descobertas de segurança ou atividades suspeitas.

- Ajudar a entender e investigar um incidente depois que algo suspeito foi detectado:
- Coleta e correlaciona dados de várias fontes (incluindo GuardDuty).



## AWS Abuse

AWS Abuse é um conjunto de políticas e ferramentas relacionadas à prevenção, identificação e resolução de uso indevido ou abusivo dos serviços da AWS. O termo "abuso" refere-se a comportamentos que violam os Termos de Serviço da AWS ou padrões de segurança, e pode envolver atividades como spam, ataques DDoS, uso de recursos para atividades ilegais, ou outras formas de abuso de infraestrutura da AWS.

A AWS tem uma equipe e um processo dedicado, chamada de AWS Abuse Desk, que lida com as denúncias de abuso e investiga quaisquer atividades maliciosas ou não conformes realizadas na plataforma. O objetivo da AWS é garantir que a infraestrutura seja usada de maneira ética e que todas as atividades sejam legais e seguras.

## AWS Macie

Serviço de segurança e privacidade da AWS que utiliza inteligência artificial (IA) e aprendizado de máquina (ML) para identificar, classificar e **proteger dados sensíveis**, como informações pessoais identificáveis (PII), em seus recursos da AWS, como Amazon S3. Ele ajuda as organizações a gerenciar riscos e compliance com regulamentos de privacidade de dados, como GDPR e CCPA.

O Macie é especialmente útil para empresas que precisam proteger dados sensíveis e atender a exigências regulatórias relacionadas à privacidade e proteção de dados.

## AWS Security Hub

Oferece uma **visão centralizada de segurança** da sua infraestrutura na nuvem. Ele coleta, organiza e prioriza alertas de segurança e achados de conformidade de vários serviços da AWS e ferramentas de terceiros, ajudando a simplificar o monitoramento e a gestão de riscos de segurança em ambientes AWS. A ideia é fornecer uma visão unificada dos problemas de segurança em tempo real para facilitar a resposta rápida e a automação.



## AWS RAM

AWS RAM (Resource Access Manager) é um serviço da AWS que permite o compartilhamento de recursos entre contas da AWS de maneira segura e eficiente. Com o AWS RAM, você pode compartilhar recursos como Amazon VPC subnets, AWS Transit Gateways, AWS License Manager, e outros, entre contas dentro de uma mesma organização ou até entre organizações diferentes.

Esse serviço é especialmente útil em ambientes multi-conta (como os configurados com AWS Organizations), onde você quer facilitar o compartilhamento de recursos sem a necessidade de duplicá-los em cada conta.

- Centralização: Ajuda a centralizar e simplificar a gestão de recursos em ambientes multi-conta, sem duplicar recursos entre contas.
- Economia de custos: Reduz a necessidade de provisionar recursos em múltiplas contas, o que pode gerar economia de custos.
- Segurança e controle: Fornece um controle granular sobre quem pode acessar e compartilhar os recursos, garantindo que as permissões sejam sempre respeitadas.
- Escalabilidade: Ideal para empresas que precisam escalar rapidamente suas operações e acessar recursos de maneira mais eficiente em várias contas ou regiões.
- Integra-se bem com o AWS Organizations e oferece controle de acesso via IAM.



## AWS Trusted Advisor

É uma ferramenta online que fornece **orientações em tempo real** para ajudar a provisionar seus recursos seguindo as melhores práticas da AWS em otimização de custos, segurança, tolerância a falhas, limites de serviço e melhoria de desempenho. Seja estabelecendo novos fluxos de trabalho, desenvolvendo aplicações ou como parte de uma melhoria contínua, as recomendações fornecidas pelo Trusted Advisor regularmente ajudam a manter suas soluções provisionadas de forma ideal. **Todos os clientes da AWS têm acesso às sete verificações principais do Trusted Advisor** para ajudar a aumentar a segurança e o desempenho do ambiente AWS. O Trusted Advisor não pode ser usado para migrar para a AWS e gerenciar aplicações na AWS Cloud.



## AWS Organizations

AWS Organizations é um serviço da Amazon Web Services (AWS) que permite que você gerencie múltiplas contas da AWS de forma centralizada. Com o AWS Organizations, você pode criar e gerenciar grupos de contas e aplicar políticas de gerenciamento em toda a organização, facilitando a administração e a governança de múltiplas contas da AWS.

- AWS Organizations é uma ferramenta para gerenciar várias contas AWS de forma centralizada.
- **SCPs (Service Control Policies)** ajudam a definir limites para o que pode ser feito em cada conta.
- **Você pode consolidar cobranças de várias contas e obter descontos.**
- A criação de OUs (Unidades Organizacionais) facilita a organização das contas.
- A automação e a governança de políticas e contas são facilitadas pela AWS Organizations



## AWS Control Tower

O AWS Control Tower é uma solução da AWS que ajuda a configurar e gerenciar um ambiente multi-conta com boas práticas de governança, segurança e conformidade.

- Ele facilita a criação de contas, aplica políticas de segurança e fornece ferramentas para monitoramento e auditoria.
- Ideal para organizações que precisam de uma maneira simples e escalável de gerenciar várias contas na AWS, mantendo o ambiente seguro e conforme.
- Funciona sobre o AWS Organizations
- Detecta violações de política e oferece mecanismos de correção
- Monitora conformidade via dashboard
- Integração com CloudWatch e CloudTrail.



## AWS Config

Ferramenta que permite auditar e monitorar configurações de recursos em sua conta AWS. **Ele captura alterações de configuração e registra todos os estados anteriores dos recursos**, permitindo que você entenda e recupere facilmente a configuração de qualquer recurso em sua conta a qualquer momento. Além disso, o AWS Config oferece regras de conformidade, permitindo que você verifique automaticamente se seus recursos estão em conformidade com as melhores práticas e os requisitos regulatórios.



## Amazon CloudWatch

O Amazon CloudWatch é o serviço de **monitoramento e observabilidade** da AWS. Ele permite que você cole, visualize e analise dados sobre seus recursos como CPU, memória, disco, rede etc., e aplicações na nuvem para manter tudo funcionando de forma eficiente e segura.

- Coleta métricas (CloudWatch Metrics) de recursos AWS, como EC2, RDS, Lambda, S3, etc.
- Monitora logs (CloudWatch Logs) de aplicações e sistemas.
- Permite criar dashboards para visualizar métricas e logs.
- **Permite configurar alarmes** que disparam ações automáticas se algo estiver fora do normal.
- Pode automatizar respostas a eventos com CloudWatch Events / EventBridge.

### Componentes principais

#### 1. CloudWatch Metrics

- Dados numéricos sobre recursos ou aplicações.
- Ex.: CPU, memória, latência, tráfego.

#### 2. CloudWatch Logs

- Armazena e analisa logs de servidores, aplicações e serviços.
- Pode gerar insights e alertas.

#### 3. CloudWatch Alarms

- Disparam ações quando métricas atingem limites definidos.
- Ex.: reiniciar instâncias, enviar notificação no SNS.

#### 4. CloudWatch Dashboards

- Painéis visuais com gráficos de métricas e logs.
- Útil para monitoramento em tempo real.

#### 5. CloudWatch Events / EventBridge

- Permite reagir a mudanças no ambiente AWS automaticamente.
- Ex.: iniciar funções Lambda quando uma instância para.



## Amazon EventBridge

O Amazon EventBridge é um serviço da AWS que permite **conectar aplicações usando eventos de forma totalmente gerenciada**. Ele é uma evolução do CloudWatch Events e facilita arquiteturas orientadas a eventos (**event-driven**).

- Recebe eventos de serviços AWS, aplicações SaaS ou customizados.
- Roteia eventos para destinos, como Lambda, SQS, SNS, Step Functions, etc.
- Permite automatizar fluxos de trabalho quando algo acontece na nuvem.
- Funciona em tempo real ou quase em tempo real.

### Conceitos:

#### 1. Event (Evento)

- Uma mudança ou ação que aconteceu.
- Ex.: criação de um arquivo no S3, nova linha em DynamoDB, atualização de ticket.

#### 2. Event Bus (Barramento de Eventos)

- Canal que recebe e distribui eventos.
- Pode ser: padrão (AWS), customizado (sua aplicação) ou de SaaS.

#### 3. Rule (Regra)

- Define quais eventos vão para quais destinos.
- Ex.: se o bucket S3 receber um arquivo .csv, enviar para Lambda.

#### 4. Target (Destino)

- Serviço ou recurso que recebe o evento.
- Ex.: Lambda, Step Functions, SNS, SQS, Kinesis.

### Casos de uso comuns

- Processamento de arquivos ao serem enviados para S3
- Notificações automáticas em SNS ou emails
- Disparar funções Lambda para atualizar bancos de dados
- Integração entre serviços SaaS e AWS
- Automatizar workflows em microserviços



## Amazon CloudTrail

O AWS CloudTrail é um serviço da AWS que permite registrar e monitorar todas as ações realizadas em sua conta AWS. Ele é usado para auditoria, conformidade e análise de segurança.

- Registra chamadas de API e atividades de usuários, funções e serviços AWS.
- Armazena logs de eventos detalhados (quem fez, o quê, quando, de onde).
- Facilita auditorias de segurança e conformidade.
- Pode integrar com CloudWatch para alertas em tempo real.

Conceitos:

- Trail: Registro contínuo das ações na conta AWS. Pode ser multi-região para cobrir toda a infraestrutura.
- Event (Evento): Uma ação realizada na AWS. Ex.: criação de uma instância EC2, alteração de políticas IAM, execução de Lambda.
- Management Events: Eventos de gerenciamento de recursos. Ex.: criação, modificação ou exclusão de recursos.
- Data Events: Eventos que acessam dados em serviços como S3 ou Lambda. Ex.: leitura ou gravação de objetos em S3.
- Insight Events: Detecta atividades anormais ou suspeitas automaticamente.

MOSTRA QUEM FEZ O QUÊ, QUANDO E ONDE

Os CloudTrail Insights são um recurso do AWS CloudTrail que permite detectar automaticamente atividades anormais ou incomuns na sua conta AWS.



## Amazon Health Dashboard

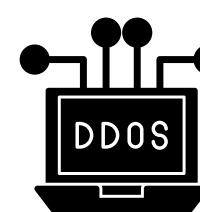
O AWS Health Dashboard é um serviço da AWS que fornece informações sobre o status e a integridade dos serviços AWS que você está usando. Ele ajuda a monitorar problemas, manutenção programada e eventos que possam afetar seus recursos.

- Mostra status em tempo real dos serviços AWS.
- Alerta sobre eventos que afetam seus recursos (interrupções, degradação de serviço, manutenção).
- Fornece detalhes personalizados para a sua conta e região.
- Permite integrar notificações com CloudWatch ou SNS.

Conceitos:

1. Service Health Dashboard (SHD)
  - Mostra status geral de todos os serviços AWS por região.
  - Ex.: OK, interrupção parcial ou completa.
2. Personal Health Dashboard (PHD)
  - Mostra eventos que afetam especificamente seus recursos.
  - Ex.: manutenção programada em uma instância EC2 que você possui.
3. Eventos
  - Notificações sobre problemas, manutenção ou ações recomendadas.
  - Pode incluir orientações para mitigação de impacto.

👉 ele avisa quando a AWS tem um problema – e se esse problema impacta você.



## DDoS

Um DDoS (Distributed Denial of Service, ou Negação de Serviço Distribuída) é um tipo de ataque cibernético que tenta tornar um serviço, site ou aplicação indisponível sobrecarregando-o com uma quantidade enorme de tráfego ou solicitações simultâneas.

## Serviços principais de DDoS Protection na AWS



### AWS Shield

"Tem tráfego demais tentando derrubar o site, vou mitigar."

- Shield Standard
  - Proteção automática e gratuita contra ataques DDoS comuns.
  - Protege serviços como CloudFront, Route 53, ELB.
- Shield Advanced
  - Proteção mais avançada, com cobertura de ataques maiores e complexos.
  - Inclui alertas, relatórios detalhados, suporte 24/7 da AWS DDoS Response Team (DRT).
  - Permite integração com WAF e proteção financeira (créditos para custos extra devido a ataques).



### AWS WAF

"Essa requisição HTTP parece maliciosa, vou bloquear."

Web Application Firewall

Bloqueia tráfego malicioso e padrões suspeitos.

Trabalha em conjunto com Shield para proteger aplicações web.

- trabalha na camada de aplicação
- tem capacidade para reconhecer requisições baseadas em filtros



## AWS CloudFront

O Amazon CloudFront é o serviço de Content Delivery Network (CDN) da AWS, usado para distribuir conteúdo (como sites, vídeos, APIs) globalmente com baixa latência e alta velocidade.

- Distribui conteúdo estático e dinâmico de forma rápida para usuários ao redor do mundo.
- Armazena cópias do conteúdo em caches (edge locations) próximas aos usuários.
- Integra com S3, EC2, API Gateway, Media Services e outros serviços AWS.
- Pode ser usado com HTTPS, WAF e Shield para segurança.



## AWS Route 53

Serviço de DNS (Domain Name System) da AWS, usado para gerenciar nomes de domínio e rotear tráfego de forma confiável para aplicações na nuvem.

- Resolve nomes de domínio (ex.: www.meusite.com) para endereços IP de servidores ou recursos AWS.
- Gerencia DNS e direciona usuários para o recurso AWS mais próximo e disponível.
- Integra com CloudFront, S3, ELB e outros serviços AWS.
- Pode ser configurado para alta disponibilidade e failover.

Tipos:

1. Simple Routing Policy: um único recurso
2. Weighted Routing Policy: distribui por peso
3. Latency Routing Policy: menor latência usuário
4. Failover Routing Policy: recurso reserva automático



## AWS Network Firewall

"Controla e filtra o tráfego de rede dentro da VPC."

O AWS Network Firewall é um serviço gerenciado da AWS que fornece proteção de rede avançada **(camadas 3, 4 e parte da 7)** para suas VPCs (Virtual Private Clouds). Ele permite criar regras de firewall para controlar o tráfego de entrada e saída, ajudando a proteger aplicações contra ameaças de rede.

Resumo das camadas (OSI)

- Camada 7 – Aplicação

O que está sendo pedido (HTTP, APIs)

conteúdo da requisição → WAF

- Camada 4 – Transporte

Por qual porta e protocolo (TCP/UDP)

portas e conexões → Shield / Network Firewall

- Camada 3 – Rede

De onde vem o tráfego (IP, roteamento)

IP e origem → Shield / Network Firewall

- Camadas 1–2 – Física / Enlace

Infraestrutura e comunicação local

hardware → AWS cuida



## AWS Firewall Manager

"Define regras uma vez e aplica em toda a organização."

O AWS Firewall Manager é um serviço da AWS que permite **gerenciar centralizadamente políticas de segurança em várias contas e VPCs**, facilitando a proteção consistente contra ameaças de rede e aplicações web. Ele funciona em conjunto com serviços como AWS WAF, AWS Shield Advanced e AWS Network Firewall.

- Cria políticas de segurança centralizadas para múltiplas contas AWS.
- Aplica automaticamente regras de WAF, Shield e Network Firewall em recursos novos e existentes.
- Facilita compliance e governança ao garantir que todas as contas sigam as mesmas regras de segurança.
- Permite auditar a aplicação das políticas em toda a organização AWS.

- Policy (Política): Conjunto de regras que define como o tráfego deve ser controlado em todos os recursos.

- Resource Types (Tipos de recurso): Define em quais recursos a política será aplicada, ex.: CloudFront, ALB, API Gateway ou VPCs.

- Account Coverage (Cobertura de contas): Aplica políticas automaticamente em todas as contas AWS da organização.



## AWS Certificate Manager (ACM)

Facilita o provisionamento, gerenciamento e implantação de certificados SSL/TLS para proteger a comunicação entre os seus clientes e os recursos da AWS. Ele ajuda a garantir a segurança das comunicações na nuvem, permitindo que você crie dados em trânsito e ofereça confiabilidade e integridade para suas aplicações e websites.

AWS gerencia a infra e você gerencia certificados para suas aplicações.



Certificados são arquivos digitais usados para autenticar a identidade de uma entidade e criar conexões seguras entre sistemas, como servidores e clientes, na internet. Eles são uma parte essencial da infraestrutura de segurança SSL/TLS, utilizada para criptografar comunicações e garantir a confidencialidade e integridade dos dados durante a transmissão.

Em termos simples, um certificado digital funciona como uma identidade digital que comprova que você é quem diz ser, de forma que as informações trocadas entre dois sistemas não sejam interceptadas ou alteradas.



## AWS Secrets Manager

É um serviço gerenciado da AWS para armazenar, gerenciar e acessar informações sensíveis, como senhas, chaves de API, tokens de autenticação e outras credenciais, de forma segura e centralizada. Ele ajuda a garantir que essas informações estejam protegidas, mas ao mesmo tempo facilmente acessíveis para aplicações e usuários autorizados, sem a necessidade de armazená-las em código ou em locais inseguros.

- O AWS Secrets Manager ajuda a armazenar e gerenciar credenciais e segredos (como senhas e chaves de API) de forma segura e acessível.
- Ele oferece armazenamento criptografado e permite que você controle o acesso aos segredos usando IAM.
- O serviço permite rotacionar automaticamente segredos, aumentando a segurança sem exigir ação manual.
- Ele se integra com muitos outros serviços AWS, como RDS, Lambda, EC2, e mais.



## AWS Artifact

Fornece documentos de conformidade e certificações de segurança para ajudar as organizações a atender a exigências regulatórias e de auditoria. Ele fornece acesso a uma biblioteca de relatórios que detalham as práticas de segurança da AWS e como a AWS atende a diferentes normas de conformidade, como ISO 27001, PCI-DSS, HIPAA, e GDPR.

Esses documentos são especialmente úteis para organizações que precisam demonstrar conformidade com padrões regulatórios ao usar a infraestrutura da AWS, bem como para aqueles que buscam realizar auditorias e garantir a segurança e privacidade dos dados.

- Ele fornece relatórios de auditoria e certificados de conformidade que podem ser usados para auditorias e demonstração de segurança.
- O AWS Artifact é uma ferramenta importante para empresas que precisam comprovar conformidade regulatória e garantir a segurança dos dados na AWS.

# Criptografia na AWS

A criptografia (encryption) na AWS é um componente fundamental para proteger dados sensíveis e garantir a privacidade e segurança dos dados enquanto estão armazenados ou sendo transmitidos. A AWS oferece várias opções de criptografia, tanto para dados em repouso (data at rest) quanto para dados em trânsito (data in transit).

Criptografia é o processo de transformar dados em uma forma ilegível para quem não tem a chave correta. Isso é feito para proteger dados confidenciais contra acessos não autorizados.

→ Criptografia de Dados em Repouso (Data at Rest) → Refere-se à criptografia de dados quando estão armazenados, ou seja, quando estão em discos, bancos de dados, buckets S3 ou outros recursos de armazenamento.

- Proteção de dados sensíveis em caso de falha de segurança, como acessos não autorizados.
- Compliance com regulamentações de segurança e privacidade, como PCI DSS, HIPAA, GDPR.

→ Criptografia de Dados em Trânsito (Data in Transit) → Refere-se à criptografia de dados enquanto estão sendo transferidos, seja entre sistemas, aplicações ou entre cliente e servidor. Isso garante que os dados não possam ser interceptados ou alterados enquanto estão sendo transmitidos pela rede.

- Proteção contra interceptação de dados enquanto transitam pela rede (evitando ataques como Man-in-the-Middle).
- Privacidade dos dados durante a transmissão, garantindo que informações sensíveis, como credenciais ou dados financeiros, não sejam expostas.

A CRIPTOGRAFIA É ESSENCIAL PARA SEGURANÇA, COMPLIANCE E PROTEÇÃO DE DADOS SENSÍVEIS.



## AWS Key Storage Manager

Serviço amplamente utilizado na AWS para gerenciar chaves de criptografia de forma segura e centralizada.

- Customer managed key
- AWS Managed key
- AWS owned key
- Cloud HSM (customer keystore)



## AWS CloudHSM

Oferece módulos de segurança de hardware (HSM) gerenciados na nuvem para gerenciar chaves de criptografia de forma altamente segura e isolada. Ao contrário do AWS KMS, que é gerenciado pela AWS, o CloudHSM fornece um controle total sobre as chaves de criptografia, ideal para empresas que precisam de controle físico sobre os dados de segurança e desejam manter suas chaves em um dispositivo HSM dedicado.

# Pricing

# Abordagens

## Pagamento por Uso (Pay-as-you-go)

- Sem custos iniciais ou compromissos: Você paga apenas pelos recursos que utiliza, sem taxas de instalação ou compromissos de longo prazo.
- Cobrança por hora ou por segundo: Muitos serviços são cobrados com base no tempo de uso (por exemplo, EC2 é cobrado por hora ou por segundo, dependendo do tipo de instância).
- Custo flexível: O custo varia dependendo de como você usa os recursos. Por exemplo, você paga mais se usar mais capacidade de processamento ou mais armazenamento, mas também pode reduzir custos ao desligar recursos quando não forem necessários.

## Descontos por compromisso e volume

A AWS oferece várias formas de descontos para incentivar o uso contínuo e em maior escala:

- Reserved Instances (RIs): Você se compromete a usar um recurso (como uma instância EC2) por 1 ou 3 anos e, em troca, recebe um desconto significativo (até 75% em relação às instâncias sob demanda).
- Savings Plans: Uma alternativa às Reserved Instances, que oferece descontos de até 72% em comparação com as tarifas sob demanda, em troca de um compromisso de uso de 1 ou 3 anos. Os Savings Plans são mais flexíveis e aplicáveis a vários serviços, como EC2, Fargate, Lambda, e mais.
- Descontos por volume: Muitos serviços (como Amazon S3 e Amazon RDS) oferecem descontos progressivos à medida que o volume de uso aumenta. Isso significa que, quanto mais você usa, menor é o custo por unidade.

## Modelo de preço por serviço

A AWS oferece diferentes modelos de cobrança para diferentes serviços. Alguns dos principais incluem:

- **Instâncias EC2:**
  - On-Demand: Você paga por hora ou segundo com base no tipo de instância e região.
  - Reserved Instances: Você pode pagar por 1 ou 3 anos de uso antecipado, com descontos de até 75% em relação ao preço sob demanda.
  - Spot Instances: Você pode aproveitar a capacidade não utilizada da AWS a preços reduzidos, mas com a possibilidade de interrupção.
- **Armazenamento (S3, EBS, etc.):**
  - Cobrança com base no volume de armazenamento utilizado e nas operações realizadas, como gravações ou leituras.
  - S3: A AWS cobra por GB armazenado e por requisições feitas (PUT, GET, etc.).
- **Transferência de Dados:**
  - A transferência de dados entre regiões ou para a internet tem custos adicionais.
  - Dentro de uma mesma região, a transferência de dados é gratuita, mas entre regiões ou para a internet é cobrada.

## Fatores de Custo Específicos para Cada Serviço

Cada serviço da AWS tem suas próprias regras de precificação, e os custos podem ser baseados em diferentes métricas, como:

- Armazenamento (em GB, operações, etc.)
- Transações (número de operações realizadas)
- Largura de banda (transferência de dados entre regiões ou para a internet)
- Número de instâncias/recursos provisionados

# Abordagens

## Preços por capacidade

- Escalabilidade: Muitos serviços são cobrados com base na capacidade ou recursos alocados, como CPU, memória, armazenamento, e largura de banda.
- Exemplo: O Amazon EC2 é cobrado com base na instância (tamanho da máquina virtual) que você escolher, enquanto o Amazon RDS é cobrado com base no tipo de banco de dados, tamanho e capacidade de armazenamento.

## Modelos de Preço por Uso Específico

Alguns serviços têm modelos de preço baseados em outras métricas específicas além do tempo ou da quantidade de dados, como:

- AWS Lambda: O preço é baseado no número de invocações e no tempo de execução (medido em milissegundos de uso de CPU).
- Amazon API Gateway: Cobrado com base no número de chamadas de API e na quantidade de dados transferidos.

## Preços regionais

Os preços podem variar de acordo com a região onde você está provisionando seus recursos. Isso é devido a fatores como custos operacionais, demanda local, e infraestrutura.

- Exemplo: O custo de uma instância EC2 pode ser diferente em regiões como US East (Norte da Virgínia) e Asia Pacific (Sydney).

# Free tier e créditos

## Free tier

A AWS oferece um nível gratuito (Free Tier) que permite que novos usuários experimentem uma série de serviços sem custos, dentro de limites mensais. Por exemplo:

- EC2: 750 horas de instâncias t2.micro por mês durante o primeiro ano.
- S3: 5 GB de armazenamento padrão, 20.000 solicitações GET e 2.000 solicitações PUT por mês.
- Lambda: 1 milhão de invocações gratuitas por mês.

Esses limites variam entre os serviços e podem ser limitados por tempo (12 meses) ou permanentes.

## Serviços sempre gratuitos:

Disponível sem limite de tempo, dentro de cotas mensais.

Principais serviços:

- IAM – usuários, grupos e permissões
- VPC – rede, subnets, route tables
- Security Groups / NACLs
- AWS CloudFormation (você paga só pelos recursos criados)
- AWS WAF (regras básicas contam, mas requests são cobrados)
- AWS Shield Standard
- Amazon CloudWatch (métricas básicas e alguns logs)
- AWS Organizations
- AWS Artifact
- AWS Health Dashboard
- Amazon Inspector (parcial, depende do uso)

## Resumo rápido

- IAM, VPC, Shield Standard, Artifact → Always Free
- EC2, S3, RDS, Lambda → 12 meses
- GuardDuty, Detective, Macie → Trial

## Créditos

Ao criar uma nova conta, você recebe automaticamente um crédito de US\$ 200 que pode ser usado para experimentar serviços da AWS. Esse crédito é válido por 30 dias a partir da ativação da sua conta. Você não precisa se comprometer a comprar nada, e os US\$ 200 são totalmente gratuitos durante o período de validade.

- Serviços comuns que você pode usar: Amazon EC2, Amazon S3, Amazon RDS, AWS Lambda, Amazon CloudFront e Amazon Glue.
- O que Não Está Incluído: Serviços pagos em maior escala - alguns serviços e recursos com custo mais alto (como instâncias EC2 muito grandes ou transferências de dados entre regiões) podem consumir rapidamente o crédito, dependendo do seu uso.
- Serviços além do Free Tier: O crédito de US\$ 200 pode ser usado junto ao Free Tier, mas se você exceder o nível gratuito em qualquer serviço, será cobrado normalmente (a menos que o crédito cubra esse custo).

## Ordem de aplicação dos créditos:

Enquanto ao tipo, a AWS usa primeiro créditos promocionais, depois créditos de suporte específicos, e só então cobra o restante do cartão registrado.

Já quanto ao vencimento, a AWS considera a seguinte prioridade:

1. Vencimento mais próximo
2. Crédito com menor número de produtos aplicáveis
3. crédito mais antigo (desempate)

# Serviços relacionados



## AWS Pricing Calculator

Estimar custos futuros antes de criar recursos

Ferramenta interativa que permite estimar o custo de usar serviços da AWS. Você pode simular a configuração de sua infraestrutura, escolher os serviços necessários e calcular o custo estimado.

Como funciona:

- Você escolhe os serviços e configura os parâmetros (ex: tipo de instância EC2, quantidade de armazenamento S3, etc.).
- O calculator mostra uma estimativa detalhada dos custos com base no uso.
- Utilização: Ideal para planejamento de novos projetos, orçamento de novas infraestruturas ou quando você precisa prever custos futuros.



## AWS Cost Explorer

Gráficos, histórico, análise

É uma ferramenta que permite visualizar e analisar os gastos com a AWS ao longo do tempo.

Como funciona:

- Você pode criar gráficos e relatórios personalizados para visualizar o histórico de custos, e entender quais serviços estão gerando mais despesas.
- Oferece funcionalidades como análise de custo por serviço, análise de custo por tag, e visualização de tendências de custos.

Utilização: Ideal para analisar os custos passados e prever despesas futuras. Permite identificar áreas onde você pode reduzir custos ou melhorar a eficiência.



## Cost & Usage Report

Detalhado, CSV/Parquet, Athena

Fornece uma visão detalhada e granular de todos os recursos e serviços da AWS que você usou, incluindo custos e o uso detalhado.

Como funciona:

- O relatório é gerado em formato CSV ou Parquet, e você pode baixá-lo ou integrá-lo com o Amazon Athena para consultas mais avançadas.
- Ele inclui dados como o custo por serviço, quantidade de recursos usados, e horas de uso.
- Utilização: Ótimo para empresas que precisam de relatórios detalhados sobre cada aspecto do uso da AWS, como para auditorias, análises financeiras ou previsões de custos.



## AWS Budgets

Orçamento, alerta, limite

Permite criar orçamentos personalizados e configurar alertas para monitorar se você está atingindo os limites de custos ou uso definidos.

Como funciona:

- Você define um orçamento com base em custos ou uso e, em seguida, configura alertas para ser notificado quando o orçamento estiver próximo de ser atingido.
- Permite monitorar custos por serviço, usuários ou até tag.
- Utilização: Ideal para controle de gastos e para evitar surpresas na fatura, especialmente para novos projetos ou quando você está operando com um orçamento limitado.

# Serviços relacionados



## Cost Anomaly Detection

Anomalia, ML, alertas

É uma ferramenta que usa machine learning para identificar anomalias de custo em sua conta AWS.

Como funciona:

- A ferramenta monitora seus custos e usa algoritmos de aprendizado de máquina para detectar padrões incomuns ou picos inesperados nos gastos.
- Você é alertado automaticamente quando um aumento de custo fora do normal é detectado.
- Utilização: Ideal para detectar problemas rapidamente, como erros de configuração ou uso excessivo que poderiam resultar em custos inesperados.

# Ferramentas relacionadas

## Cost Allocation Tag

Etiquetas que você adiciona aos recursos AWS (como EC2, S3, RDS) para atribuir custos a diferentes projetos, departamentos ou equipes.

- Como funciona:
- Você cria tags personalizadas (ex: Project: WebApp, Department: Marketing).
- No painel de faturamento da AWS, você pode usar essas tags para analisar os custos de forma granular.
- Utilização: Ideal para detalhar a alocação de custos em uma organização com múltiplos projetos ou departamentos, facilitando o controle financeiro e a atribuição de custos.

## Billing Alarms

São alertas que você configura para ser notificado caso seus custos da AWS atinjam um determinado valor.

- Como funciona:
- Você configura o alarme baseado em um limite de custo ou uso.
- Recebe notificações por e-mail ou SMS quando o limite configurado for ultrapassado.
- Utilização: Excelente para monitorar e evitar custos inesperados e garantir que seu uso da AWS fique dentro do orçamento.

## AWS Billing Dashboard

É a interface onde você pode visualizar suas faturas e gerenciar pagamentos da AWS.

- Como funciona:
- Exibe o resumo de custos e uso dos seus serviços AWS.
- Mostra a fatura atual, o custo acumulado, e as formas de pagamento.
- Permite visualizar relatórios detalhados sobre os gastos de cada serviço.
- Utilização: Essencial para monitorar a fatura e garantir que você não ultrapasse seu orçamento mensal.

## Service Quotas

Ferramenta que ajuda a monitorar e gerenciar os limites de recursos em cada serviço da AWS.

- Como funciona:
  - AWS define limites padrão para muitos serviços (como o número de instâncias EC2 ou volumes EBS).
  - Você pode solicitar aumento de quotas caso precise de mais recursos, e monitorar esses limites diretamente no painel.
- Utilização: Essencial para gerenciar os limites de uso em sua conta e garantir que você não ultrapasse as quotas padrão do serviço, evitando interrupções no uso de recursos.



# Cloud Computing

# Elastic Compute Cloud EC2

## Contexto

Serviço da AWS que fornece servidores virtuais na nuvem (instâncias). Ele é “elástico” porque você pode aumentar ou reduzir a capacidade conforme a necessidade, pagando apenas pelo uso. Permite criar e gerenciar máquinas virtuais para rodar aplicações, sites, bancos, APIs ou qualquer tipo de carga de trabalho.

## Infrastructure as a service

A AWS fornece a infraestrutura, mas você é responsável por configurar, administrar e manter tudo dentro dela – exatamente o modelo de IaaS.

## Configurações

- Tipo de instância: Escolha de CPU (núcleos), memória, rede e otimizações (ex.: t3, m5, c6g, r5).
- AMI (Imagem do Sistema Operacional)
- Tamanho da instância: ex.: t3.micro
- Tipo de armazenamento: EBS (SSD/HDD gerenciado) ou Instance Store (armazenamento físico temporário).
- Tipo de rede: VPC, Subnet, IP público/privado, Security Groups.
- Firewall keys: security groups SSH ou HTTP
- Regras de segurança: Security Groups, NACLs, portas liberadas (ex.: 22, 80, 443).
- Auto Scaling / Elasticity: Configurar para aumentar ou diminuir capacidade automaticamente.
- Tags: Identificação da instância (nome, ambiente, dono, etc.).
- Bootstrap script: script que roda automaticamente apenas ao criar a instância (instala pacotes, baixa arquivos, etc)

## Opções de compra

- **On-Demand:** paga pelo tempo de uso (segundos), preço previsível, sem compromisso. Ideal para testes ou cargas variáveis.
- **Reserved Instances:** (1 ou 3 anos) descontos significativos. Para uso longo e estável, mais barato que on-demand, permite mudar o tipo de instância durante o período.
- **Savings Plans:** (1 ou 3 anos) compromisso de gasto por hora, e não por tipo de instância. Flexível, mas exige compromisso financeiro.
- **Spot Instances:** utiliza a capacidade ociosa da AWS com preços até 90% menores, mas podem ser interrompidas a qualquer momento.
- **Dedicated Hosts:** disponibilizam servidores físicos inteiros para um único cliente - maior controle do hardware (exigências de licenciamento/compliance).
- **Dedicated Instances hardware:** não compartilhado com outros clientes, mas sem controle físico total.
- **Capacity reservations:** reserva a capacidade em uma AZ específica por qualquer duração. Garante disponibilidade.

As instâncias EC2 Linux são cobradas por segundo, mas com um tempo mínimo de cobrança de 60 segundos (1 minuto). Windows tem cobrança por hora

## Tipos de instâncias EC2

- **Instâncias de uso geral (General Purpose – T, M):** equilíbrio entre CPU, memória e rede. Uso: sites, apps comuns, servidores gerais.
- **Otimizadas para computação (Compute Optimized – C):** Alta CPU, ideal para cálculos intensos. Uso: processamento pesado, apps de alto desempenho.
- **Otimizadas para memória (Memory Optimized – R, X, Z):** R: muita RAM para bancos de dados. e X / Z: Quantidades enormes de memória. Uso: bancos de dados, big data, in-memory computing.
- **Armazenamento otimizado (Storage Optimized – I, D, H):** Foco em I/O muito rápido, SSD/NVMe local. Uso: bancos NoSQL, analytics, workloads que exigem IOPS.
- **GPU / Aceleração (Accelerated Computing – P, G, Inf, Trn):** G / P – GPU para gráficos e machine learning e Inf / Trn – Aceleradores especializados para IA. Uso: IA, deep learning, renderização 3D, vídeo.

Paga pelo que usa considerando:

- número de instâncias, região, OS, software, tipo de instância, tamanho de instância e capacidade física;
- ELB running e capacidade física
- Monitoramento detalhado
- Para on-demand instances:
  - pay per second para Linux e Microsoft, com mínimo de 60 segundos
  - pay per hour para outros OS

## EBS (Elastic Block Store)

É como um pendrive conectado pela rede à sua instância EC2  
Serve para armazenar dados de forma persistente, ou seja, mesmo que você desligue ou termine a instância, os dados continuam salvos.

- Apenas uma instância por vez
- Ligado a uma AZ: não pode ser removido para outra AZ sem copiar ou snapshot
- Armazenamento em bloco
- Para por tipo de volume, volume provisionado, tamanho dos objetos, IOPs, snapshots e transferênciaa de dados

! Um EBS não pode ser conectado a mais de um EC2, mas um EC2 pode ter vários EBS

Por padrão, ao criar um EBS volume, o root é configurado para ser deletado assim que a instância termina, mas os volumes adicionais não vêm com essa configuração default.

EBS Snapshots: são cópias de segurança (backups) dos volumes EBS, de forma incremental e salvos no S3 – persistente, pode ser copiado para outra região, camada mais barata, restaurar pode levar horas.

## EFS (Elastic File System)

Serviço de armazenamento de arquivos totalmente gerenciado e elástico.

- Escalabilidade automática (EBS não)
- pay-per-use
- mais caro que EBS, mas é escalável e permite compartilhamento de dados entre aplicações EC2
- EFS-IA é uma classe de custo menor par arquivos não acessados frequentemente

Ideal para aplicações que precisam de acesso simultâneo a arquivos por várias instâncias.

- Pode ser acessado por múltiplas instâncias EC2 simultaneamente
- Usa o protocolo NFS

## ELB (Elastic Load Balancer)

“Porteiro inteligente” que recebe requisições e distribui para servidores que estejam funcionando bem - evita servidores sobrecarregados, montem o site no ar mesmo se um servidor falhar e consegue crescer conforme a demanda.

Tipos:

- Application Load Balancer (ALB) – Camada 7; ideal para apps web, HTTP/HTTPS, roteamento avançado.
- Network Load Balancer (NLB) – Camada 4; extremamente rápido e performante; ideal para alto tráfego e baixa latência.
- Gateway Load Balancer (GLB) – Encaminha tráfego para appliances de terceiros (firewalls, inspeção de rede).
- Classic Load Balancer (CLB) – Modelo antigo, camada 4/7; legado, pouco usado hoje.

EC2 = servidor  
EBS = disco  
ELB = distribui tráfego  
EFS = acesso simultâneo  
ASG = escala automaticamente

## ASG (Auto Scaling Group)

GRÁTIS

Ajusta automaticamente a quantidade de servidores (instâncias EC2) que a aplicação usa, conforme demanda - escalabilidade horizontal.

- Escalonamento Manual: você mesmo define o número desejado de instâncias.
- Escalonamento Programado (Scheduled): horários específicos (ex.: aumentar instâncias às 18h).
- Escalonamento Dinâmico: reage automaticamente ao uso (ex.: CPU > 70%).
- Escalonamento Predictivo (Predictive Scaling): usa machine learning para prever demanda futura.
- Alta disponibilidade: substitui instâncias com falha e distribui entre múltiplas zonas de disponibilidade (AZs) - trabalha com Elastic Load Balancer, enviando tráfego para as instâncias saudáveis. (registra automaticamente novas instancias no load balancer)
- Health Checks: ASG verifica a saúde das instâncias e substitui automaticamente se estiverem com problemas, desde que sejam do mesmo tipo.

## Security Groups

São firewalls virtuais das instâncias na VPC da AWS.

Eles controlam o tráfego que entra (inbound) e sai (outbound) das suas máquinas. Filtram tráfego por porta, protocolo e IP. Permite regras de Allow apenas (não existe Deny).

## EC2 Image Builder

Automatiza a criação e manutenção de imagens de VM ou contêiner.

## EC2 Instance Store

É um disco físico dentro do servidor que hospeda sua instância EC2.

Diferente do EB2, que é um disco conectado via rede, o instance store é local, oferecendo desempenho muito alto para operações de leitura/gravação (I/O).

- alta performance, bom para dados temporários
- volátil, se você parar/terminar a instância, os dados são perdidos
- responsabilidade do backup é sua
- não persistente - armazenamento temporário em bloco para uma instância EC2.
- Não pode ser compartilhado entre várias instâncias EC2 ao mesmo tempo.

## AMI (Amazon Machine Image)

É uma imagem pré-configurada usada para criar instâncias EC2. É como um modelo/foto do sistema. A partir dela você cria quantas instâncias quiser e pode ser copiada para outras regiões.

Contém: Sistema operacional, aplicativos e configurações opcionais e permissões para quem pode usar

Opções: usar AMI públicas (fornecidas pela AWS), sua própria AMI ou comprar uma AMI que outra pessoa configurou no marketplace.

- Como criar? Inicie uma instância EC2 e personalize-a, pare a instância, crie uma AMI, lance novas instâncias a partir dessa AMI
- Uma AMI (Amazon Machine Image) existe apenas na região onde foi criada.
- Você não pode lançar uma EC2 em outra região usando diretamente a mesma AMI.
- Para usar em outra região → Copy AMI (Snapshots EBS são copiados automaticamente e a criptografia é mantida ou redefinida)



## AWS Compute Optimizer

Ferramenta que ajuda você a otimizar o desempenho e os custos de seus recursos de computação na AWS, como EC2, Auto Scaling, EBS e Lambda. Ele analisa seu uso atual e faz recomendações de instâncias e recursos mais eficientes.

- Recursos suportados: EC2, Auto Scaling, EBS, Lambda.
- Objetivo: Reduzir custos e melhorar performance sem impactar cargas de trabalho.
- Como se usa: Sem custos adicionais, integrado ao console da AWS; gera relatórios automático



## Amazon FSx

Oferece sistemas de arquivos totalmente gerenciados, otimizados para casos de uso específicos, diferente do EFS que é mais genérico.



## AWS Systems Manager Session Manager

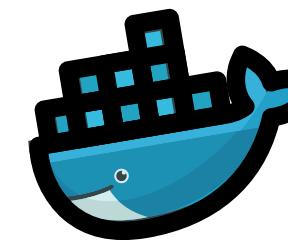
O AWS Systems Manager Session Manager é um serviço gerenciado que permite acessar instâncias EC2 de maneira interativa e segura, sem precisar abrir portas de rede ou utilizar IPs públicos. Ele permite que você conecte e gerencie instâncias EC2 sem usar o tradicional SSH ou RDP (Remote Desktop Protocol), com a vantagem de que ele é completamente gerenciado pela AWS.

A principal vantagem do Session Manager é que ele:

- Não exige abertura de portas no security group das instâncias EC2.
- Não depende de IP público.
- Proporciona um acesso seguro e auditável, facilitando o cumprimento das políticas de conformidade.
- Oferece controle centralizado e simplificado, já que você pode gerenciar várias instâncias de uma vez.

Em outras palavras, o Session Manager ajuda a aumentar a segurança e a auditabilidade do acesso às suas instâncias EC2, sem comprometer a infraestrutura de rede.

O EC2 Instance Connect também é uma forma de acessar instâncias EC2 de forma segura via SSH, mas ele requer que a porta 22 (SSH) esteja aberta no security group. A questão pede uma solução que não exija abrir portas, então essa opção não é válida.



Docker é uma plataforma que permite criar, empacotar e executar aplicações em containers.

Um container reúne a aplicação e todas as suas dependências (bibliotecas, configurações e runtime), garantindo que ela funcione da mesma forma em qualquer ambiente – no computador do desenvolvedor, em servidores ou na nuvem.

Em resumo, Docker facilita a portabilidade, padronização e escalabilidade de aplicações, sendo a base para serviços de containers como Amazon ECS e Amazon EKS.



## Amazon ECS (Elastic Container Service)

Serviço para orquestrar containers Docker de forma gerenciada, sem precisar administrar Kubernetes.

- Não usa Kubernetes (diferente do EKS).
- Pode rodar sobre EC2 ou Fargate.
- Use quando quiser containers com menos complexidade.
- Não há taxas adicionais, paga-se pelos recursos subjacentes

Você provisiona e mantém a infraestrutura (EC2) e a AWS cuida de startar/finalizar os containers.



## Fargate

Modelo serverless para containers, usado com ECS ou EKS. Você não gerencia servidores; paga apenas pelo tempo e recursos usados pelo container.

Você não precisa fornecer a infraestrutura como no ECS.

AWS roda os containers para você baseado na quantidade de CPU/RAM necessários.

- Não gerencia EC2, clusters ou servidores.
- Container sem servidor



## ECR (Elastic Container Registry)

- Repositório gerenciado para armazenar imagens Docker, garante um local seguro e integrado para armazenar imagens das aplicações.
- Armazena as imagens para serem rodadas no ECS ou fargate e é integrado com EKS e CI/CD.
- Controle de acesso via IAM.
- S3 de imagens Docker



## Amazon EKS

Serviço gerenciado de Kubernetes, usado quando você precisa do padrão Kubernetes e portabilidade entre ambientes.

- Usa o padrão K8s, muito usado no mercado.
- Mais complexo que ECS.
- Pode rodar com EC2 ou Fargate.
- Distribuir os containers entre servidores
- Criar novos containers quando um falha
- escalar sua aplicação



## AWS Lambda

Serviço de computação serverless que executa código sob demanda.

Ideal para eventos, APIs, automações e processamento em tempo real.

O código é executado apenas quando necessário, reduzindo custos e aumentando a agilidade no desenvolvimento.

- Computação serverless baseada em eventos.
- Executa código sem servidor.
- Escala automaticamente.
- Paga por execução e tempo.



## Amazon API Gateway

Serviço para criar, publicar e gerenciar APIs.

Muito usado junto com o Lambda para arquiteturas serverless.

- Cria e gerencia APIs REST, HTTP e WebSocket.
- Muito usado com Lambda.
- Controle de segurança, throttling e versionamento.



## AWS Batch

Serviço para executar jobs em lote (batch), tornam simples a execução de tarefas em lote e workloads de processamento intensivo sem a necessidade de gerenciar clusters manualmente - gerencia filas, priorização e escala automática de recursos.

- Executa jobs em lote.
- Gerencia filas e escala recursos automaticamente.
- Usa EC2 ou Fargate por trás.



## Amazon Lightsail

O Amazon Lightsail democratiza o uso da nuvem ao oferecer uma experiência simplificada para projetos menores e iniciantes.

- Plataforma simplificada de cloud.
- Ideal para iniciantes, sites simples, blogs e pequenas aplicações.
- Inclui computação, storage e rede em um pacote.
- “AWS simples”

# Resumo

Serviço	O que é	Quando usar	Palavra-chave para a prova
<b>Docker</b>	Plataforma de containers	Padronizar e empacotar aplicações	Container
<b>Amazon ECS</b>	Orquestrador de containers	Rodar containers sem Kubernetes	Containers gerenciados
<b>Amazon EKS</b>	Kubernetes gerenciado	Usar padrão Kubernetes	Kubernetes
<b>AWS Fargate</b>	Containers serverless	Rodar containers sem gerenciar servidores	Serverless containers
<b>Amazon ECR</b>	Registro de imagens Docker	Armazenar imagens de containers	Repositório Docker
<b>AWS Lambda</b>	Computação serverless	Executar código sob demanda	Código sem servidor
<b>Amazon API Gateway</b>	Gerenciamento de APIs	Criar e expor APIs	Porta de entrada
<b>AWS Batch</b>	Processamento em lote	Executar jobs batch	Batch processing
<b>Amazon Lightsail</b>	Cloud simplificada	Projetos pequenos e iniciantes	Simplicidade

- Containers: ECS / EKS
- Serverless: Lambda / Fargate
- APIs: API Gateway
- Jobs em lote: Batch
- Projetos simples: Lightsail



# Armazenamento e DataBases



# Amazon S3

## Contexto

Serviço de armazenamento de objetos (object storage), altamente durável e escalável, com diferentes classes de armazenamento, versionamento, políticas de segurança e opções de replicação. NÃO É BANCO DE DADOS, é feito para armazenar arquivos (imagens, vídeos, backups, logs, JSON, etc.), pois é altamente escalável, mas não é otimizado para acesso de baixa latência por item, como num banco de dados.

## Principais características

- “Escalabilidade infinita” de armazenamento
- Durabilidade: 99.999999999% (11 nines).
- Disponibilidade: muito alta, mas menor que a durabilidade.
- Armazenamento infinito: escala automaticamente.

## Buckets

No Amazon S3, tudo começa pelos buckets, que funcionam como contêineres onde você guarda seus arquivos. Cada bucket precisa ter um nome único no mundo inteiro, como se fosse um endereço exclusivo na internet. Dentro desses buckets ficam os objects, que são os próprios arquivos acompanhados de metadados, podendo ter até 5 TB cada. É importante entender também que cada bucket está sempre associado a uma região específica da AWS, e seus dados ficam armazenados fisicamente nela. Além disso, o S3 não funciona como um sistema de arquivos tradicional: apesar de parecer ter pastas, na verdade o que você vê são apenas prefixos usados para organizar os objetos.

## Segurança

Por padrão S3 é privado, nada fica público a menos que você altere isso. Bloqueio de Acesso Público é um recurso importante que impede exposição acidental do bucket.

Quem controla acesso?

- IAM Policies (usuários/roles)
- Bucket Policies (controle direto no bucket)
- ACLs (legado, quase não cai)

## Classes de armazenamento

- S3 Standard: uso geral, acesso frequente.
- S3 Standard-IA: acesso infrequente, mais barato.
- S3 One Zone-IA: acesso infrequente em 1 AZ.
- S3 Glacier Instant Retrieval: arquivos raramente acessados, mas com retorno rápido.
- S3 Glacier Flexible Retrieval: horas de recuperação.
- S3 Glacier Deep Archive: mais barato, recuperação em horas - ideal para arquivamento

## Custo

Você paga por:

- Armazenamento
- Requests (GET, PUT...)
- Transferência de dados pra fora da AWS
- Restauração (Glacier)

## S3 Encryption

Dois tipos importantes:

- Server-side (SSE-S3, SSE-KMS, SSE-C)
- Client-side (você criptografa antes de enviar)

## S3 Replication

- CRR: replicação entre regiões.
- SRR: replicação dentro da mesma região.
- Precisa do versionamento ativado.

## Versionamento

- Mantém múltiplas versões de um objeto.
- Ajuda a recuperar exclusões acidentais.

## S3 Transfer Acceleration

É um recurso do Amazon S3 que permite transferir arquivos para e de buckets S3 de forma mais rápida, principalmente quando os usuários estão geograficamente distantes da região onde o bucket está localizado. Ele utiliza a rede global da AWS (Edge Locations do CloudFront) para otimizar a velocidade de upload e download.

## S3 Websites

Recurso do Amazon S3 que permite hospedar sites estáticos diretamente dentro de um bucket.

## Lifecycle Rules

Moving objects automatically between classes of storage (Standard → IA → Glacier).



## Amazon Snowball

É um dispositivo físico da AWS usado para transferir grandes quantidades de dados entre o ambiente local (on-premise) e a AWS de forma rápida e segura, sem depender da internet.

- Snowball Edge (o mais comum): permite armazenar dados e até rodar computação local com AWS Lambda e EC2.
- Snowmobile: um caminhão inteiro para transferir exabytes (usado por grandes empresas).



## Amazon Managed Blockchain

É um serviço totalmente gerenciado para criar e gerenciar redes blockchain, sem precisar administrar infraestrutura.

- Suporta frameworks populares, como Hyperledger Fabric e Ethereum.
- Elimina a complexidade de configurar e manter nós blockchain.
- Oferece alta disponibilidade, segurança e escalabilidade.
- Usado para aplicações descentralizadas e registros imutáveis.



## AWS Storage Gateway

O AWS Storage Gateway é um serviço de armazenamento híbrido, que conecta ambientes on-premises (locais) à nuvem da AWS. Ele ajuda a reduzir custos, simplificar gerenciamento de dados e facilitar backup, arquivamento e recuperação de desastres.

O serviço fornece três tipos de gateways, cada um com funções específicas:

### 1. Tape Gateway

- Substitui fitas físicas para backup.
- Armazena dados de backup no Amazon S3 ou no Amazon S3 Glacier.
- Ideal para migração de backups existentes para a nuvem.

### 2. File Gateway

- Permite acessar arquivos via protocolo NFS ou SMB.
- Os arquivos ficam armazenados no Amazon S3.
- Útil para compartilhar arquivos na nuvem com baixo esforço de gerenciamento.

### 3. Volume Gateway

- Expõe volumes em bloco para servidores on-premises via iSCSI.
- Pode funcionar em modo cache (armazenando dados localmente e enviando para a nuvem) ou modo armazenado (dados primários na nuvem).
- Usado para recuperação de desastres e armazenamento de dados de alta disponibilidade.



## Amazon Neptune

Banco de dados de grafos, usado para relacionamentos complexos, como redes sociais e recomendações.



## Amazon Timestream

Banco de dados para séries temporais, usado para dados com timestamp, como IoT, métricas e monitoramento.



## Amazon Document DB

Banco de dados NoSQL compatível com MongoDB, usado para dados em documentos JSON. (documentos complexos)



## Amazon Database Migration Service

O AWS DMS é um serviço que permite migrar bancos de dados para a AWS de forma segura e com pouco ou nenhum downtime.

- Migra dados entre bancos homogêneos (ex.: Oracle → Oracle) ou heterogêneos (ex.: Oracle → Aurora).
- Permite manter o banco de origem funcionando durante a migração.
- Suporta migrações on-premise ↔ AWS ↔ entre regiões.
- Funciona com bancos relacionais e alguns NoSQL.
- Calculation Engine): motor de cálculo que acelera as consultas e permite que os dados sejam carregados na memória para análises rápidas.

Normalmente usado junto com o AWS Schema Conversion Tool (SCT) para converter esquemas quando os bancos são diferentes.



## Amazon RDS (relational database service)

Serviço gerenciado de bancos de dados relacionais. A AWS cuida da parte difícil: manutenção, backups, atualizações, patches e alta disponibilidade.

- Suporta MySQL, PostgreSQL, MariaDB, Oracle, SQL Server, Amazon Aurora, etc.
- Backups automáticos feitos pela AWS e snapshots manuais
- Monitoramento via AWS CloudWatch
- Multi-AZ
  - réplica síncrona em outra AZ para alta disponibilidade
  - em caso de falha, ocorre failover automático
  - importante: não melhora performance, apenas disponibilidade
- Escalabilidade:
  - Vertical: aumentar potência da instância (CPU, RAM).
  - Armazenamento escalável automaticamente (dependendo do engine).
- Segurança: Criptografia em repouso (KMS); Uso de VPC, subnets privadas e security groups; Controle de acesso por IAM + credenciais do DB.
- Pague pelo que usar. Custos incluem: instância, armazenamento, transferência de dados e backup.
- Réplicas assíncronas para melhorar leitura - usadas para distribuir carga, não para alta disponibilidade, e podem estar em outras regiões.

Para aplicações que precisam de consistência transacional (ACID)/sistemas legados que usam bancos relacionais.



## Amazon Aurora

Aurora é um banco relacional compatível com MySQL e PostgreSQL, mas construído pela AWS e otimizado para núvem.

- Até 5x mais rápido que MySQL e 3x mais rápido que PostgreSQL.
- Armazenamento cresce automaticamente até 128 TB.
- Alta disponibilidade nativa com réplicas distribuídas em múltiplas AZs
- Serviço gerenciado: AWS cuida de backups, patching, failover e escalabilidade.
- Criptografia em repouso e em trânsito
- É parte do RDS, mas é próprio da AWS (not open sourced)
- Custo baseado em instância, armazenamento e I/O → mais caro que RDS, mas mais eficiente.

### Aurora Serverless

Versão do banco Aurora que escala automaticamente conforme a demanda, sem precisar gerenciar instâncias manualmente.

- Escalabilidade automática: aumenta ou reduz capacidade conforme o uso.
- Pagamentos por consumo: você paga apenas pelo que usa, não por instâncias ociosas (pay per second)
- Alta disponibilidade: mantém durabilidade e replicação do Aurora tradicional.
- Sem gerenciamento de servidor: você não precisa provisionar ou parar instâncias manualmente.



## Amazon ElasticCache

Serviço que fornece cache na memória para melhorar a performance das aplicações, reduzindo a latência e a carga em bancos de dados. Ele é ideal para cenários onde se precisa acessar dados frequentemente e com muita rapidez. Compatível com dois mecanismos populares: Redis e Memcached. Pode ser usado em vários bancos de dados.



## Amazon EMR

Usado para processar grandes volumes de dados com frameworks de Big Data como Spark e Hadoop. Roda sobre clusters EC2 gerenciados, integra-se com o Amazon S3 para armazenamento dos dados e permite escalar recursos conforme a necessidade. Indicado para tarefas de larga escala, e não para aplicações transacionais ou em tempo real.

- Redshift = OLAP
- RDS/Aurora = OLTP
- EMR = Big Data com frameworks Hadoop/Spark
- DynamoDB = aplicações de baixa latência e alto escala



## DynamoDB

Banco de dados NoSQL, serverless e totalmente gerenciado, usado para aplicações que precisam de baixa latência, altaperformance e alta escala.

- Serverless: não há servidores para gerenciar.
- Escalabilidade automática: cresce conforme a demanda.
- Baixa latência: resposta em milissegundos.
- Alta disponibilidade: replicado automaticamente em várias AZs.
- Usa tabelas, mas sem esquema fixo.
- Dados são armazenados como itens e atributos.
- Possui chave primária (partition key ou partition + sort key).
- milhares de requisições por segundo
- Backups automáticos e sob demanda.
- Capacidade
  - On-Demand: paga por requisição, sem planejamento.
  - Provisioned: define leitura e escrita com antecedência.
- Segurança: Criptografia em repouso por padrão, controle de acesso via IAM, integração com VPC endpoints.

O [DAX \(DynamoDB Accelerator\)](#) é um serviço de cache em memória totalmente gerenciado para o Amazon DynamoDB, criado para reduzir ainda mais a latência de leitura, usado quando você precisa de leituras extremamente rápidas em aplicações que já utilizam DynamoDB.

[Global Tables](#) permitem replicar tabelas do DynamoDB entre várias regiões, garantindo baixa latência, alta disponibilidade e acesso global aos dados.



## Amazon RedShift

É um data warehouse totalmente gerenciado, usado para análises de grandes volumes de dados (OLAP).

- Armazena dados históricos e analíticos.
- Usa SQL para consultas.
- Armazenamento colunar: acelera consultas porque lê as colunas necessárias.
- Otimizado para analytics e BI (relatórios, dashboards) rápidas e não para operações de inserção/atualização frequentes.
- Integra com S3, RDS, DynamoDB e ferramentas de BI.
- Não é banco transacional (não é OLTP)
- Execução massivamente paralela: divide a consulta em várias partes e processa em paralelo nos nós do cluster, garantindo velocidade e alta disponibilidade.
- Modelo de cobrança pay as you go baseado em instâncias
- Carga de dados periódica. Como é um DW, você carrega dados em lote (batch), não em tempo real, como sistemas transacionais.
- Performance 10X melhor que outros DW
- Integração com o Glue
- Governança de dados: lake formation e compartilhamento de dados

## Redshift Serveless

É a versão sem servidores do Redshift.

- Não precisa provisionar clusters - sem clusters fixos.
- Escala automaticamente conforme a demanda.
- Pagamento por uso, baseado na capacidade consumida.
- Mantém os mesmos casos de uso analíticos do Redshift tradicional.

## Consultar dados facilmente



### Athena

Serviço serverless que permite consultar dados no Amazon S3 usando SQL.

- Não precisa de servidores para usar.
- Paga por consulta, baseado nos dados escaneados.
- Os dados permanecem no S3 (Athena não armazena dados).
- Ideal para análises rápidas, logs e data lakes.
- Usa SQL padrão.
- Presto (engine distribuída para consultas SQL)
- Suporta csv, json, orc, avro e parquet
- Ideal para lakes e análises rápias sem ETL complexo
- Pode ser usado junto com AWS Glue Data Catalog para metadados.
- 

Atenção: use formatos colunares (parquet, orc) e compressão para reduzir o custo, pois menos dados serão lidos.

## Visualizar dados facilmente



### QuickSight

Serviço de visualização de dados e BI (Business Intelligence) totalmente gerenciado pela AWS.

- Criação de Dashboards e Relatórios: permite criar visualizações interativas de dados, como gráficos e tabelas.
- Integra com várias fontes de dados: Redshift, S3, RDS, DynamoDB, Athena, e mais.
- Análises ad hoc: ajuda a explorar dados sem precisar de infraestrutura adicional.
- Visualizações ricas: oferece gráficos, tabelas dinâmicas, mapas geoespaciais, etc.
- Escalabilidade: é serverless e pode escalar automaticamente conforme a demanda.
- SPICE (Super-fast, Parallel, In-memory Calculation Engine): motor de cálculo que acelera as consultas e permite que os dados sejam carregados na memória para análises rápidas.

## Manipule dados facilmente



### AWS Glue

Serviço serverless de ETL (Extract, Transform, Load) usado para preparar, transformar e mover dados para análise.

- Serverless: não há servidores para gerenciar.
- Usado para ETL, não para consultas ou visualizações.
- Descobre e cataloga dados automaticamente com o Glue Data Catalog.
- Integra com S3, Athena, Redshift, RDS e outros serviços de dados.
- Automatiza limpeza, transformação e organização dos dados.

No AWS Glue, triggers, workflows e a integração com o AWS Step Functions servem para orquestrar e automatizar pipelines de dados: triggers iniciam jobs, workflows organizam pipelines dentro do Glue e o Step Functions orquestra fluxos mais complexos envolvendo vários serviços da AWS.

# Resumo

Analytics: Athena, Redshift, EMR, Quicksight  
Transacional: RDS, Aurora, DynamoDB  
Armazenamento: S3, EBS  
Migração / Integração: DMS, Snowball, Storage Gateway

Serviço	Tipo	Quando usar	Critérios principais
<b>Amazon S3</b>	Storage (objeto)	Armazenar arquivos, backups, data lake	Durável, barato, escala ilimitada
<b>Amazon EBS</b>	Storage (bloco)	Disco para EC2	Baixa latência, ligado a instância
<b>AWS Storage Gateway</b>	Híbrido	Integrar on-premise com AWS	Backup e extensão do datacenter
<b>Amazon Snowball</b>	Transferência física	Migrar grandes volumes de dados	Pouca conectividade de rede
<b>Amazon RDS</b>	Banco relacional	Aplicações transacionais	SQL, ACID, gerenciamento automático
<b>Amazon Aurora</b>	Banco relacional	Alta performance relacional	Compatível MySQL/PostgreSQL
<b>Amazon DynamoDB</b>	NoSQL	Alta escala e baixa latência	Serverless, milissegundos
<b>Amazon ElastiCache</b>	Cache	Acelerar aplicações	Cache em memória
<b>Amazon Redshift</b>	Data Warehouse	Analytics e BI	Consultas analíticas em grande escala
<b>Redshift Serverless</b>	Analytics	BI sem gerenciar cluster	Escala automática, pay-per-use
<b>Amazon EMR</b>	Big Data	Processar grandes volumes de dados	Spark, Hadoop, ETL
<b>Amazon Athena</b>	Query	Consultar dados no S3	SQL serverless, paga por consulta
<b>Amazon QuickSight</b>	BI	Criar dashboards e relatórios	Visualização de dados
<b>AWS Glue</b>	ETL	Preparar e transformar dados	ETL serverless, Data Catalog
<b>Amazon DocumentDB</b>	NoSQL (documentos)	Dados em JSON	Compatível MongoDB
<b>Amazon Neptune</b>	Banco de grafos	Relacionamentos complexos	Grafos (redes, recomendações)
<b>Amazon Timestream</b>	Time series	Dados com timestamp	IoT, métricas, monitoramento
<b>Amazon Managed Blockchain</b>	Blockchain	Ledger distribuído	Imutabilidade, descentralização
<b>AWS DMS</b>	Migração	Migrar bancos para AWS	Baixo downtime

# Machine Learning



## Amazon Comprehend

O Amazon Comprehend é um serviço de inteligência artificial (IA) da AWS que analisa textos automaticamente para extrair significado e insights.

Ele usa machine learning e funciona sem você precisar treinar modelos.

Com ele você pode:

- Detectar sentimento (positivo, negativo, neutro, misto)
- Identificar entidades (pessoas, lugares, datas, organizações)
- Extrair frases-chave
- Classificar textos por tópicos
- Identificar idioma
- Detectar informações sensíveis (PII)



## Amazon Transcribe

O Amazon Transcribe é um serviço de inteligência artificial da AWS que converte áudio em texto automaticamente (transcrição de fala).

Ele usa machine learning e funciona sem você precisar treinar modelos.

Com ele você pode:

- Converter áudio ou vídeo em texto
- Transcrever fala em tempo real ou arquivos gravados
- Identificar quem está falando (speaker identification)
- Adicionar pontuação automática

Reconhecer termos personalizados (nomes, siglas)



## Amazon Translate

O Amazon Translate é um serviço de inteligência artificial da AWS que faz tradução automática de textos entre diferentes idiomas.

Ele usa machine learning e não exige que você treine modelos.



## Amazon Lex

O Amazon Lex é um serviço de inteligência artificial para criar chatbots e voicebots.

O que ele faz:

- Entende texto e voz
- Cria chatbots conversacionais
- Reconhece intenções (intents) do usuário
- Usa a mesma tecnologia da Alexa



## Amazon Connect

O Amazon Connect é um serviço de contact center na nuvem.

O que ele faz:

- Cria call centers na AWS
- Atendimento por voz e chat
- Distribui chamadas automaticamente
- Grava e analisa chamadas
- Escala sob demanda

Lex + Connect (juntos)  
Eles são frequentemente usados em conjunto:  
Lex: entende o que o cliente diz  
Connect: gerencia a chamada ou chat



## Amazon Rekognition

O Amazon Rekognition é um serviço de inteligência artificial (IA) da AWS que permite analisar imagens e vídeos automaticamente para identificar objetos, pessoas e atividades.

Ele usa machine learning e você não precisa treinar modelos do zero.



## Amazon Polly

O Amazon Polly é um serviço de inteligência artificial da AWS que converte texto em fala (Text-to-Speech).

Ele gera voz natural a partir de texto, sem você precisar treinar modelos.

Usos: Assistentes virtuais, respostas automáticas, aplicações que precisam “falar”, e-learning e acessibilidade.



## Amazon Sagemaker IA

O Amazon SageMaker é um serviço da AWS que permite criar, treinar e implementar modelos de machine learning (IA) em escala, sem precisar gerenciar infraestrutura complexa.

Ele é mais avançado que os outros serviços de IA “prontos” (como Polly, Lex ou Comprehend), porque permite treinar modelos personalizados.

Com ele você pode:

- Preparar dados para treinamento
- Treinar modelos de Machine Learning
- Testar e validar modelos
- Implantar modelos para produzir previsões (inference)
- Automatizar tarefas de ML com AutoML



## Amazon Kendra

O Amazon Kendra é um serviço de inteligência artificial (IA) da AWS focado em busca empresarial (enterprise search).

Ele permite que organizações encontrem informações relevantes dentro de grandes volumes de dados, como documentos, intranet, sites, bancos de dados e aplicações corporativas, usando linguagem natural.

Com ele você pode:

- Fazer busca em linguagem natural (ex.: “Quais são os procedimentos de férias?”)
- Integrar dados de documentos, SharePoint, Salesforce, S3, bases SQL, etc.
- Ranquear respostas por relevância
- Permitir controle de acesso aos documentos
- Atualizar os índices automaticamente



## Amazon Personalize

O Amazon Personalize é um serviço de inteligência artificial (IA) da AWS que permite criar sistemas de recomendação personalizados para usuários, de forma rápida e sem precisar treinar modelos complexos manualmente.

Ele é o mesmo tipo de tecnologia usada pela Amazon.com para recomendar produtos.



## Amazon Textract

O Amazon Textract é um serviço de inteligência artificial (IA) da AWS que extrai texto e dados de documentos de forma automática, sem precisar de intervenção manual ou OCR tradicional complexo.

Ele consegue identificar texto, tabelas, formulários e campos estruturados em documentos digitais ou digitalizados, como pdf, imagens e outros.

# Resumo

Serviço	Tipo	Função principal	Entrada	Saída / Resultado
<b>Amazon SageMaker</b>	ML completo	Criar, treinar e implantar modelos personalizados	Dados de treino	Modelo ML treinado / Previsões
<b>Amazon Rekognition</b>	Visão computacional	Detecta objetos, rostos e atividades	Imagem ou vídeo	Objetos, rostos, texto, emoções
<b>Amazon Comprehend</b>	Processamento de linguagem	Analisa textos	Texto	Sentimento, entidades, frases-chave
<b>Amazon Textract</b>	Processamento de documentos	Extrai texto, tabelas e formulários	Documentos PDF ou imagens	Texto estruturado
<b>Amazon Translate</b>	Tradução	Tradução automática	Texto	Texto traduzido
<b>Amazon Polly</b>	Texto → Fala	Converte texto em fala	Texto	Áudio de voz natural
<b>Amazon Transcribe</b>	Fala → Texto	Converte áudio em texto	Áudio / Vídeo	Texto transscrito
<b>Amazon Lex</b>	Conversação	Chatbot e voicebot	Texto ou fala	Resposta conversacional
<b>Amazon Connect</b>	Contact center	Gerencia chamadas e chat	Voz ou chat	Atendimento centralizado
<b>Amazon Personalize</b>	Recomendação	Recomendações personalizadas	Dados de usuários	Lista de itens recomendados
<b>Amazon Kendra</b>	Busca corporativa	Busca inteligente em documentos	Documentos, intranet, bases	Resultados relevantes

# Developer Tools



## AWS CodeCommit

O AWS CodeCommit é um serviço de controle de versão gerenciado que permite armazenar código-fonte, arquivos binários e outros arquivos de projeto em repositórios Git privados na nuvem AWS. Ele funciona de forma semelhante ao GitHub ou GitLab, mas é totalmente integrado ao ecossistema AWS.

### Como funciona

1. Você cria um repositório privado no CodeCommit.
2. Os desenvolvedores podem clonar, enviar (push) e buscar (pull) alterações usando comandos Git padrão.
3. O serviço oferece controle de acesso detalhado via IAM, garantindo que apenas usuários autorizados possam acessar o repositório.
4. Integra-se com AWS CodePipeline, CodeBuild e CodeDeploy para automação de CI/CD.

### Benefícios

- Totalmente gerenciado: não é necessário configurar ou manter servidores Git.
- Alta disponibilidade e durabilidade: armazenado na infraestrutura AWS.
- Segurança integrada: controle de acesso com IAM, criptografia de dados em trânsito e em repouso.
- Escalabilidade automática: suporta repositórios de qualquer tamanho ou número de commits.
- Integração com CI/CD: facilita pipelines automáticos de build e deploy.



## AWS CodeBuild

O AWS CodeBuild é um serviço totalmente gerenciado que permite compilar código, executar testes e produzir artefatos prontos para deploy, funcionando como parte do processo de CI/CD (Integração Contínua / Entrega Contínua).

### Como funciona

1. Você conecta o repositório de código (como CodeCommit, GitHub ou S3) ao CodeBuild.
2. Cria um buildspec file (buildspec.yml) que define:
  - Comandos de build
  - Testes a serem executados
  - Artefatos a serem gerados
3. CodeBuild cria um ambiente de build isolado (container) para executar o processo.
4. Gera os artefatos finais prontos para deploy ou integração com outros serviços (como CodeDeploy ou S3).

### Benefícios

- Gerenciado e escalável: você não precisa provisionar servidores de build.
- Execução paralela: múltiplos builds podem rodar ao mesmo tempo.
- Suporte a múltiplas linguagens: Java, Python, Node.js, Ruby, Go, .NET, entre outras.
- Integração com CI/CD: funciona facilmente com CodePipeline, CodeCommit e CodeDeploy.
- Isolamento seguro: cada build roda em container separado, garantindo segurança e consistência.



## AWS CodeDeploy

O AWS CodeDeploy é um serviço que permite automatizar o deploy de aplicações em servidores EC2, instâncias on-premises ou containers, garantindo que as atualizações sejam feitas de forma rápida, segura e controlada, sem downtime (ou com downtime mínimo).

### Como funciona

1. Você prepara o código da aplicação e um arquivo de especificação de deploy (AppSpec).
2. CodeDeploy envia o código para os servidores ou ambientes alvo.
3. Ele gerencia estratégias de deploy, como:
  - o In-place deployment: atualiza a aplicação diretamente no mesmo servidor.
  - o Blue/Green deployment: cria uma nova versão em paralelo, redirecionando o tráfego gradualmente.
4. Monitora o processo e faz rollback automático se ocorrer algum problema.

### Benefícios

- Automação do deploy, reduzindo erros humanos.
- Atualizações seguras com opções de rollback automático.
- Suporte a múltiplos ambientes: EC2, Lambda, ECS e on-premises.
- Downtime mínimo com Blue/Green deployments.
- Integração com CI/CD: funciona com CodePipeline, GitHub e outras ferramentas.



## AWS CodeArtifact

O AWS CodeArtifact é um serviço gerenciado de repositório de pacotes que permite armazenar, publicar e compartilhar pacotes de software de forma segura, integrando-os facilmente em pipelines de CI/CD. Ele funciona com gerenciadores de pacotes populares, como npm, Maven, PyPI e NuGet.

### Como funciona

1. Você cria um repositório CodeArtifact para armazenar pacotes internos ou externos.
2. Desenvolvedores podem publicar pacotes de suas aplicações ou baixar dependências diretamente do CodeArtifact.
3. Pode fazer proxy de repositórios externos, armazenando em cache pacotes de terceiros para maior performance e disponibilidade.
4. Integra-se facilmente com CodeBuild, CodePipeline e outras ferramentas CI/CD.

### Benefícios

- Centralização de pacotes: gerencia dependências de forma segura e consistente.
- Segurança: controle de acesso via IAM, criptografia e políticas de repositório.
- Integração com CI/CD: facilita builds automáticos e deploys confiáveis.
- Cache de pacotes externos: reduz latência e dependência de terceiros.
- Gerenciado: não precisa manter servidores de repositório próprios.



## AWS CodePipeline

O AWS CodePipeline é um serviço de integração e entrega contínua (CI/CD) que automatiza o fluxo de build, teste e deploy de aplicações na AWS ou em outros ambientes. Ele conecta diferentes etapas do ciclo de vida do software para entrega rápida e confiável.

### Como funciona

1. Você define um pipeline, que é uma sequência de estágios (stages):
  - Source: captura o código do repositório (CodeCommit, GitHub, S3).
  - Build: compila o código e executa testes (usando CodeBuild, Jenkins, etc.).
  - Test: executa testes automatizados adicionais, se necessário.
  - Deploy: envia a aplicação para produção (usando CodeDeploy, Elastic Beanstalk, ECS, etc.).
2. Cada estágio é automatizado e monitorado, permitindo que falhas sejam detectadas rapidamente.
3. Permite integração com ferramentas de terceiros, como GitHub, Jenkins e Jira.

### Benefícios

- Automação completa do fluxo de entrega de software.
- Redução de erros manuais no deploy.
- Rapidez e frequência de deploy: permite atualizações contínuas.
- Monitoramento e visibilidade: acompanha o status de cada etapa da pipeline.
- Integração com AWS e terceiros: flexível para diferentes ferramentas.



## AWS Cloud Development Kit

O AWS Cloud Development Kit (CDK) é um framework que permite definir a infraestrutura da AWS usando linguagens de programação familiares, como Python, TypeScript, Java, C# ou Go, em vez de escrever diretamente templates JSON ou YAML do CloudFormation.

### Como funciona

1. Você escreve código na linguagem de sua escolha definindo recursos da AWS (como EC2, S3, Lambda, RDS etc.).
2. O CDK converte esse código em um template CloudFormation, que é usado para provisionar a infraestrutura automaticamente.
3. Permite programação orientada a objetos, reutilização de componentes e abstrações, facilitando a manutenção de infraestruturas complexas.

### Benefícios

- Infraestrutura como código usando linguagens de programação conhecidas.
- Abstrações e reuso de código com constructs (componentes de infraestrutura reutilizáveis).
- Integração com CloudFormation, garantindo segurança e rollback automático.
- Produtividade e manutenção facilitadas, principalmente em arquiteturas complexas.

## AWS SDK (Software Development Kit)

Conjunto de bibliotecas que permite integrar aplicações diretamente com os serviços da AWS usando linguagens de programação como Python, JavaScript, Java, C#, entre outras. Ele facilita a criação de códigos que interagem com a AWS – por exemplo, fazer upload para o S3, ler dados de um banco DynamoDB, criar instâncias EC2 ou enviar mensagens para o SQS – sem precisar escrever requisições HTTP manualmente. Em resumo, o SDK permite que sua aplicação “converse” com a AWS de forma simples e segura.



## AWS Elastic Beanstalk

O AWS Elastic Beanstalk é um serviço que permite implantar e gerenciar aplicações na AWS automaticamente, sem precisar se preocupar com a infraestrutura subjacente (como servidores,平衡adores de carga ou escalabilidade).

### Como funciona

1. Você envia o código da aplicação (em linguagens como Java, Python, Node.js, .NET, Go, Ruby etc.) para o Elastic Beanstalk.
2. O serviço automaticamente provisiona e configura os recursos necessários, incluindo:
  - EC2 (servidores)
  - Load Balancer (balanceamento de carga)
  - Auto Scaling (escalabilidade automática)
  - Banco de dados RDS (opcional)
3. Ele monitora a aplicação, realiza deploys automáticos, atualizações e ajustes de capacidade.

### Benefícios

- Fácil de usar: não é necessário gerenciar infraestrutura manualmente.
- Escalabilidade automática: ajusta recursos com base na demanda da aplicação.
- Monitoramento integrado: integra com CloudWatch para métricas e logs.
- Suporte a várias linguagens: compatível com linguagens populares de desenvolvimento.
- Controle opcional: você pode personalizar recursos quando necessário.

FOCO NO CÓDIGO, NÃO NA INFRA  
AMBIENTE GERENCIADO COMPLETO



## AWS CloudFormation

O AWS CloudFormation é um serviço da AWS que permite provisionar e gerenciar infraestrutura como código (IaC). Com ele, você pode criar recursos da AWS de forma automatizada e repetível, usando arquivos de template em JSON ou YAML.

### Como funciona

1. Você cria um template definindo todos os recursos da AWS necessários para sua aplicação (como EC2, S3, RDS, VPC, etc.).
2. O CloudFormation interpreta o template e cria os recursos na ordem correta, cuidando de dependências entre eles.
3. Permite atualizar, deletar ou replicar a infraestrutura de forma segura, controlada e versionada.

### Benefícios

- Automação: Criação e atualização de recursos sem necessidade de provisionamento manual.
- Reprodutibilidade: O mesmo template pode ser usado para criar ambientes idênticos (teste, desenvolvimento e produção).
- Consistência: Reduz erros humanos ao criar a infraestrutura.
- Controle de versão: Facilita auditoria e versionamento da infraestrutura.
- Rollback automático: Se algo der errado durante a criação ou atualização, o CloudFormation reverte as alterações para o estado anterior.

CRIAR AMBIENTES COMPLETOS



## AWS Systems Manager

O AWS Systems Manager (SSM) é um serviço que permite gerenciar, automatizar e monitorar a infraestrutura da AWS e servidores on-premises de forma centralizada e segura. Ele ajuda equipes de operações e DevOps a manter controle, visibilidade e automação em grandes ambientes.

### Como funciona

- Você registra instâncias EC2, servidores on-premises ou máquinas virtuais no Systems Manager.
- Através do SSM, é possível executar comandos remotos, aplicar patches, coletar inventário, gerenciar configurações e automatizar tarefas.
- Possui módulos (services) como:
  - Session Manager → acesso remoto seguro sem SSH ou RDP.
  - Patch Manager → aplicar atualizações de sistema automaticamente.
  - Automation → criar workflows automatizados para tarefas repetitivas.
  - Parameter Store → armazenar variáveis de configuração e segredos.

### Benefícios

- Gestão centralizada: controla instâncias e servidores on-premises em um único painel.
- Segurança: acesso remoto sem precisar abrir portas, integrado com IAM.
- Automação: tarefas repetitivas podem ser automatizadas com runbooks.
- Auditoria e compliance: logs detalhados das ações realizadas.
- Inventário e monitoramento: coleta informações sobre software, patches e configurações.



## Amazon X-Ray

O AWS X-Ray é um serviço gerenciado que permite você coletar dados de rastreamento (traces) sobre como as solicitações percorrem sua aplicação, especialmente em arquiteturas distribuídas (como microserviços), para:

### Para que serve

- Depurar aplicações distribuídas (microserviços, Serverless, contêineres)
- Encontrar gargalos de performance, falhas e latência
- Visualizar como os serviços interagem com um request através da arquitetura
- Analisar dados de produção e otimizar o desempenho

### Como funciona (visão simplificada)

#### 1. Instrumentação

- A aplicação envia dados de rastreamento de cada pedido (request) ao X-Ray.

#### 2. Traces e segmentos

- O serviço agrupa os dados em traces e segmentos para mostrar cada etapa da requisição.

#### 3. Service Map

- É criado um mapa visual dos serviços e chamadas entre eles (por exemplo, API Gateway → Lambda → DynamoDB)

### Quando é útil

- Quando sua aplicação tem múltiplos serviços colaborando (ex: Lambda, API Gateway, bancos, filas)
- Quando você precisa entender onde o tempo está sendo gasto
- Quando há erros intermitentes ou lentidão e você quer achar a raiz do problema

# Resumo

Serviço	Categoria / Função Principal
<b>CodeCommit</b>	<b>Controle de versão</b> – armazena código-fonte e arquivos de projeto (repositório Git).
<b>CodeBuild</b>	<b>Build / Integração</b> – compila código, executa testes e gera artefatos.
<b>CodeDeploy</b>	<b>Deploy / Entrega</b> – automatiza o deploy de aplicações em servidores ou serviços AWS.
<b>CodePipeline</b>	<b>Orquestração / CI/CD</b> – automatiza fluxo de build, teste e deploy.
<b>CodeArtifact</b>	<b>Gerenciamento de pacotes</b> – armazena e distribui pacotes de dependência de software.

# VPC & Networking

## Conceitos essenciais sobre VPC

- Usa-se VPN quando se precisa criar um ambiente de rede isolado e seguro dentro da AWS para hospedar seus recursos.
- Separa o tráfego, aplica políticas de segurança e integra com redes corporativas em um perímetro controlado.
- É uma rede privada dentro da AWS onde vocês pode lançar recursos (como EC2)

VPC = Virtual Private Cloud

Regional: cada VPC pertence a uma região

- Subnets (sub-redes): particionam a VPC em zonas de disponibilidade (AZ)
  - sub-rede pública: acessível pela internet
  - sub-rede privada: não acessível diretamente pela internet
- Internet Gateway (IGW): permite que recursos em sub-redes públicas tenham acesso à internet
  - NAT Gateway/NAT Instance: permite que instâncias em sub-redes privadas accessem a internet sem ficarem públicas.
- Elastic IP: IP público fixo para EC2 (custo se não estiver em uso)
- VPC Flow Logs: captura tráfego de rede para monitoramento e troubleshooting
- VPC Peering: conecta duas VPCs de forma provada (não é transitiva)
- VPC endpoints: acesso privado a serviços AWS (ex.: DynamoDB) sem usar internet
- site-to-site VPN: conexão criptografada entre data center on-premises e AWS via internet
- Direct Connect: conexão física privada entre on-premises e AWS (mais rápida e segura)
- Transit Gateway: conecta múltiplas VPCs e redes on-premises em topologia hub-and-spoke

## Segurança

Security groups: firewall no nível da instância EC2

- somente regras allow
- Statefull (mantém estabelecida conexão)

Network ACL (NACL) firewall no nível da sub-rede

- regras ALLOW e DENY
- stateless (não mantém estado)

VPC (Virtual Private Cloud)  
• É uma rede virtual isolada dentro da AWS.  
• Você pode lançar recursos (EC2, RDS etc.) dentro da VPC.  
• Você tem controle total: IPs, roteamento, gateways, regras de firewall (security groups e NACLs).  
• Importante: uma VPC não está limitada a uma AZ. Ela se estende por todas as AZs de uma região. Isso permite criar subnets em diferentes AZs dentro da mesma VPC, garantindo alta disponibilidade.

### Subnet

- É uma faixa de IPs dentro da VPC.
- Cada subnet é limitada a apenas uma AZ.
- Isso permite projetar recursos redundantes em múltiplas AZs para alta disponibilidade. Por exemplo, você pode ter:
  - Subnet A ~ AZ1
  - Subnet B ~ AZ2

## AWS VPC

É a base para criar redes privadas dentro da AWS. Não é uma conexão, mas sim o espaço onde você vai conectar outros serviços como VPN, Direct Connect ou Internet Gateway.

- Virtual Private Cloud – Cria uma rede isolada dentro da AWS.
- Criar redes privadas para recursos dentro da AWS.

## AWS VPN

- Virtual Private Network
- Conecta redes privadas em uma rede segura usando criptografia.
- Criar conexão segura entre sua VPC e uma rede on-premise ou outra VPC.
- Requer Internet como meio de transporte.

## AWS Direct Connect

Conexão privada e dedicada entre sua rede corporativa e a AWS. Ideal para grandes volumes de dados, baixa latência e maior largura de banda. Não usa a Internet.

- Conexão dedicada entre a AWS e seu datacenter ou rede corporativa.
- Conectar sua rede on-premise diretamente à AWS com baixa latência e alta largura de banda.
- Conexão privada, sem uso de internet.

## Site-to-Site VPN

- Utiliza a Internet para criar uma conexão segura entre sua rede corporativa e a VPC da AWS. Ideal para conectividade remota e flexível, mas com latência maior.
- Conexão VPN entre uma rede local e a AWS.
- Criar uma rede privada e segura entre seu ambiente on-premise e a AWS.

## Internet Gateway

A porta de entrada que permite que instâncias públicas na sua VPC acessem a Internet. Requer configuração de roteamento para permitir a comunicação.

- Ponto de entrada para tráfego de rede entre a VPC e a Internet.
- Permitir que recursos dentro da VPC se comuniquem com a Internet.
- Acesso à Internet a partir de instâncias públicas.
- Requer roteamento configurado nas tabelas de rotas da VPC.
- Permite entrada e saída de tráfego da Internet.

## AWS Endpoint

Permite conectar diretamente sua VPC a outros serviços AWS de maneira privada, sem passar pela internet pública. Através de endpoints, o tráfego entre sua VPC e os serviços da AWS ocorre totalmente dentro da rede da AWS, garantindo maior segurança, performance e confiabilidade.

## AWS Private Link

Fornece acesso privado a serviços na AWS, sem sair da rede privada da VPC. É útil para conectar a serviços de terceiros ou acessar serviços como S3 sem que o tráfego seja exposto à Internet.

- Cria conexões privadas entre a VPC e serviços na AWS ou em outras VPCs sem expor dados à Internet.
- Fornecer acesso privado e seguro a serviços da AWS ou terceiros sem tráfego na Internet.
- Conexões privadas, sem exposição à Internet.

## AWS Global Accelerator

O AWS Global Accelerator é um serviço da AWS que melhora a performance e a disponibilidade global de aplicações, usando a rede privada global da própria AWS.

Ele cria um ponto de entrada global para sua aplicação, usando:

- Endereços IP estáticos globais
- Edge locations da AWS (os mesmos usados pelo CloudFront)
- Rede privada global da AWS (em vez da internet pública)

- 👉 O usuário entra pelo ponto mais próximo geograficamente
- 👉 O tráfego percorre a rede global da AWS até a aplicação
- 👉 Resultado: menor latência e maior confiabilidade

“Um atalho global pela rede da AWS para chegar mais rápido à sua aplicação”

# Mensagería

# Mensageria

Como funciona a comunicação entre aplicações?

- Síncrono: um serviço chama e o outro que estava esperando responde - rápido e online
- Assíncrono: um serviço manda mensagem para uma fila e o outro serviço lê quando puder - escalável, mas não imediato



## Amazon Simple Queue Service

Amazon SQS é um serviço gerenciado de mensageria na nuvem que permite enviar, armazenar e receber mensagens entre componentes de uma aplicação distribuída, garantindo que eles se comuniquem de forma assíncrona e desacoplada.

- 1.Um componente da aplicação envia uma mensagem para uma fila (queue) do SQS.
- 2.Outro componente consome a mensagem da fila quando estiver pronto.
- 3.As mensagens são armazenadas temporariamente até serem processadas com sucesso.
- 4.O serviço garante entrega confiável, escalabilidade automática e resiliência.



## Amazon Simple Notification Service

Amazon SNS é um serviço gerenciado de mensageria baseado em publicação/assinatura (pub/sub) que permite enviar notificações em tempo real para múltiplos destinatários, como aplicativos, servidores, e-mails ou SMS.

- 1.Um produtor (publisher) envia uma mensagem para um tópico (topic) do SNS.
- 2.Vários consumidores (subscribers) estão assinando o tópico.
- 3.Quando uma mensagem é publicada, o SNS entrega a notificação automaticamente para todos os assinantes.
- 4.Os assinantes podem ser: HTTP/HTTPS endpoints/Filas SQS/Funções Lambda/E-mails ou SMS



## AWS Kinesis Data Streams

É projetado para processar e analisar grandes volumes de dados em tempo real. Ele permite que aplicações capturem, processem e respondam a eventos de dados contínuos, como logs, cliques de sites, sensores IoT ou transações financeiras.

- 1.Os produtores (producers) enviam dados continuamente para um stream do Kinesis.
- 2.O stream armazena os dados em shards, que permitem escalabilidade horizontal.
- 3.Os consumidores (consumers) leem os dados em tempo real para processamento, análises ou armazenamento em serviços como S3, Redshift ou Elasticsearch.
- 4.É possível reprocessar dados do stream por até 7 dias (configurável).



## AWS MQ

Serviço gerenciado de broker de mensagens que facilita a integração e comunicação entre aplicações distribuídas usando protocolos de mensageria padrão, como ActiveMQ ou RabbitMQ. Ele é ideal para quem precisa de compatibilidade com sistemas legados ou quer migrar para a nuvem sem reescrever o código de mensageria.

- 1.Você cria um broker no Amazon MQ (ActiveMQ ou RabbitMQ).
- 2.Aplicações produtoras enviam mensagens para o broker.
- 3.Aplicações consumidoras recebem as mensagens do broker, garantindo entrega confiável e ordem de mensagens.
- 4.O serviço é gerenciado, ou seja, a AWS cuida de provisionamento, patching, backup e escalabilidade.

Exemplo de uso do SNS:  
• EC2 gera métricas de CPU  
• CloudWatch monitora essas métricas  
• CloudWatch Alarm detecta CPU > 80%  
• Alarm dispara uma notificação  
• SNS envia o email ao administrador



# Outros serviços



## Amazon Global Accelerator

O AWS Global Accelerator é um serviço da AWS que melhora a disponibilidade e performance de aplicações globais, direcionando o tráfego dos usuários para os endereços IP mais próximos e saudáveis de forma inteligente, usando a rede global da AWS.



## Amazon Wavelength

O AWS Wavelength é um serviço que leva computação e armazenamento da AWS para a borda da rede de operadoras de telecomunicações, permitindo que aplicativos que exigem baixa latência extrema atendam usuários móveis ou dispositivos IoT próximos à rede 5G.



## Amazon AppStream 2.0

Serviço gerenciado de streaming de aplicativos da AWS. Ele permite entregar aplicativos desktop para usuários via navegador, sem necessidade de instalação local ou reescrita de código.

- Workspace → fornece desktops virtuais completos
- Amazon AppStream 2.0 → focado em streaming de aplicativos individuais.



## Amazon IoT Core

Permite conectar dispositivos IoT à nuvem de forma segura e escalável, sem necessidade de gerenciar servidores.

- Integração Lambda, s3, Sagemaker,...



## Amazon AppSync

Serviço totalmente gerenciados que facilita a criação e APIs GraphQL seguras e escaláveis, permitindo integrar dados de múltiplas fontes (DynamoDB, Lambda,...) em um único endpoint.

- Aplicativos móveis e web com dados em tempo real

AppSync é especializado em GraphQL e recursos em tempo real e API gateway é mais genérico, voltado para APIs restful.



## Amazon Amplify

Conjunto de ferramentas e serviços que ajuda desenvolvedores a criar e implantar aplicações web e móveis full-stack de forma rápida e escalável na nuvem AWS. (back-end para mobile).

- autenticação: cognito
- APIs (Rest e GraphQL com AppSync)
- Armazenamento: s3
- Outras integrações



## AWS Infrastructure Composer

É uma ferramenta visual que permite projetar, compor e implantar aplicações modernas na AWS usando IaC (infra as code) sem exigir conhecimento profundo de CloudFormation.



## AWS Pinpoint

Serviço voltado para engajamento com clientes, permitindo enviar mensagens direcionadas e personalizadas por múltiplos canais, com e-mail, sms, push notifications, mensagens de voz, mensagens in-app

- Ele é usadao para campanhas de marketing, notificações transacionais (ex.: confirmação de pedidos) e comunicação personalizada.
- Será descontinuado em 30/10/2026



## AWS DataSync

Serviço gerenciado de transferência de dados que simplifica, automatiza e acelera a movimentação de grandes volumes de dados entre:

- Ambientes on-premises
- Serviços de armazenamento AWS
- Outras nuvens

Replicações podem ser agendadas.



## AWS Backup

Centralizar e automatiza a proteção de dados em diversos serviços da AWS e workloads híbridas.

- criar, gerenciar e restaurar backups de forma consistente e segura, sem necessidades de scripts manuais.
- on-demand and scheduled backups
- cross-region backup (cross-account backup - using AWS organizations)



## AWS Workspaces

Serviços da AWS de virtualização de desktop totalmente gerenciados (DaaS - Desktop as a service).

- Windows ou Linux
- Elimina a necessidade de comprar hardware físico ou instalar softwares complexos localmente.
- Acesso remoto seguro

O idela é que em caso de múltiplas regiões seja feito o deploy na região mais próxima dos usuários.



## AWS Device Farm

Serviço gerenciado de teste de aplicativos que permite testar apps Android, iOs e web em dispositivos físicos reais hospedados na nuvem da AWS.

- Testes automatizados/paralelos



## AWS Ground Station

Permite controlar comunicações com satélites, processar dados e escalar operações sem precisar construir ou manter infraestrutura própria de estação terrestre.

- agendar contatos com satélites para dowlink de dados
- processar dados em tempo real usando EC2, S3 e Sagemaker
- Reduzir custos pagando apenas pelo tempo de antena usado (pay as you go)



## AWS FIS

Fault Injection Simulator

Permite executar experimentos de injeção de falhas (baseado em chaos engineering) para testar a resiliência, observabilidade e desempenho das aplicações em ambiente AWS.

Ele ajuda a simular falhas reais de forma controlada, como:

- interrupção de instâncias EC2
- latência de rede
- Sobrecarga de CPU
- Erros em APIs ou serviços

## AWS Customer Carbon Footprint Tool

É uma ferramenta gratuita disponível no AWS Billing & Cost Management Console que permite aos clientes visualizem a pegada de carbono associada ao uso dos serviços da AWS. (emissões atribuídas ao consumo do cliente)



## Step Functions

Permite orquestrar múltiplos serviços em fluxos de trabalhos visuais (state machines) sem necessidade de escrever códigos complexos para integração.

- coordenar microsserviços e componentes distribuídos
- automatizar processos e pipeline de dados
- criar workflows resilientes



## AWS Applications Discovery Service

Serviço que ajuda a planejar migrações para a nuvem AWS coletando informações detalhadas sobre servidores, aplicações e dependências em ambiente on-premises.

Tipos de migrações:

- Agentless Discovery
  - via aws agentless
  - discovery connector para VMWare VCenter
  - Inventário de servidores e VMs
  - Configuração e histórico de performance (CPU, memória, disco)
- Agent-based
  - via AWS Application Discovery Agent
  - dependência entre sistemas
  - processos em execução e conexões

Os resultados são virtualizados no AWS Migration Hub.

É possível exportar dados para análise no AWS Athena ou Excel.