

## Contents

|  |    |
|--|----|
| Módulo 1: Introdução a Nuvem AWS                   | 3  |
| Core Services                                      | 4  |
| Compute: EC2 (Elastic Compute Cloud)               | 4  |
| Compute: ECS (Elastic Container Service)           | 5  |
| Storage: EBS (Elastic Block Store)                 | 5  |
| Storage: Amazon S3 (Simple Storage Service)        | 6  |
| Storage: S3 Glacier                                | 7  |
| Storage: EFS (Elastic File System)                 | 7  |
| Storage: AWS Storage Gateway                       | 8  |
| Infra Global AWS                                   | 8  |
| Network: VPC (Virtual Private Cloud)               | 9  |
| Network: AWS Direct Connect                        | 10 |
| Segurança da AWS                                   | 10 |
| Integrated Services                                | 11 |
| Application Load Balancer                          | 11 |
| Auto Scaling                                       | 12 |
| Network: Route 53                                  | 13 |
| Database: RDS (Relational Database Service)        | 13 |
| Compute: Lambda                                    | 15 |
| Elastic Beanstalk                                  | 16 |
| Simple Notification Service (SNS)                  | 16 |
| Management: Amazon CloudWatch                      | 17 |
| Amazon CloudTrail                                  | 18 |
| Storage: CloudFront CDN (Content Delivery Network) | 19 |
| Storage: Snowball Edge                             | 19 |
| Management: Amazon CloudFormation                  | 20 |
| Arquitetura  | 21 |
| Segurança  | 22 |
| Modelo de responsabilidade compartilhada           | 22 |
| IAM (Identity and Access Management)               | 23 |
| Amazon Inspector                                   | 23 |

|  |    |
|--|----|
| AWS Shield                                     | 24 |
| Segurança e conformidade                       | 24 |
| AWS Personal Health Dashboard                  | 25 |
| AWS Config                                     | 25 |
| Definição de preço e suporte                   | 27 |
| Detalhes da definição de preço                 | 27 |
| Trusted Advisor                                | 29 |
| AWS Support                                    | 30 |
| TCO (Total cost ownership)                     | 31 |
| Consolidated billing for AWS Organizations     | 32 |
| Outros serviços (podem ser abordados na prova) | 33 |
| Compute  | 33 |
| Database                                       | 33 |
| Security & Identity                            | 34 |
| Analytics                                      | 34 |
| Application Services                           | 34 |
| Enterprise Applications                        | 35 |
| Artificial Intelligence                        | 35 |
| AWS Developer Tool                             | 35 |

## Módulo 1: Introdução a Nuvem AWS

Abordagem de alterações de gerenciamento, testes, confiabilidade e planejamento de capacidade é mais ágil e eficiente.

Reduzir **riscos**:

- Por ser capaz de aprender e **adaptar-se rapidamente as mudanças** (reduz o custo da mudança)
- Riscos de **segurança** por permitir testar com frequência e efetuar correções rápidas

Escalabilidade

- Redimensionar seus recursos conforme necessário

Confiabilidade

- Capacidade de um sistema se recuperar de falhas de infraestrutura ou serviço
- Capaz de adquirir recursos computacionais para atender à demanda e mitigar interrupções
- Data Centers em todo o mundo (AWS Regions) que estão em locais isolados (Availability Zones)
- Availability Zones são DCs separados com alimentação redundante, redes e conectividade

Segurança dos dados

- Clientes mantém propriedade total sobre seus dados (incluindo região que os armazena, como lida com criptografia e quem mantém as chaves de criptografia)

### Interfaces AWS

Os usuários AWS podem criar e gerenciar recursos de três maneiras:

- **Console de Gerenciamento AWS**: interface gráfica para acessar recursos da AWS
- **Interface de linha de comando (CLI)**: permite controlar os serviços da AWS
- **SDKs**: permite acessar AWS utilizando linguagens de programação

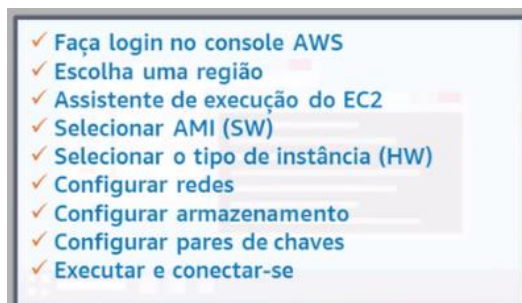
Os três utilizam como referência a API da AWS. Com as Interfaces AWS, há mais flexibilidade de criar e acessar os recursos em qualquer lugar.

## Core Services

### Compute: EC2 (Elastic Compute Cloud)

É um serviço que disponibiliza **capacidade computacional** segura e redimensionável na nuvem. A interface permite que você obtenha e configure a capacidade com o mínimo de esforço. Ele oferece controle total de seus recursos e permite trabalhar no ambiente das AWS.

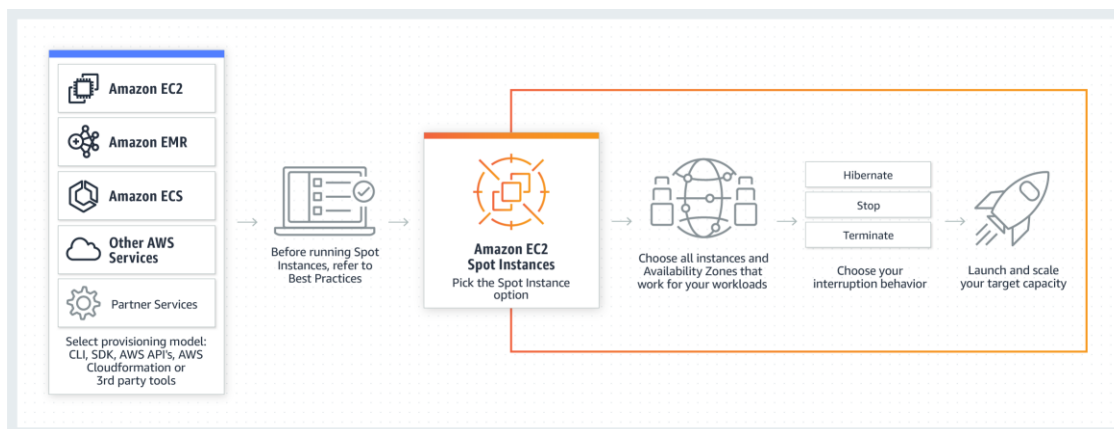
Instâncias do EC2 são *Pay as you go* (pelas instâncias em execução). Ampla seleção de hw/sw e hospedagem global.



As **instâncias spot** do Amazon EC2 permitem aproveitar a capacidade não utilizada do EC2 na Nuvem AWS. Em comparação com a definição de preço sob demanda, as instâncias spot oferecem descontos de até 90%. Elas podem ser usadas para vários aplicativos *stateless*, tolerantes a falhas e flexíveis como big data, cargas de trabalho containerizadas, CI/CD, servidores web, computação de alta performance e outras cargas de trabalho de teste e desenvolvimento.

Como as instâncias spot são estreitamente **integradas a outros serviços** da AWS como Auto Scaling, EMR, ECS, CloudFormation, Data Pipeline e AWS Batch, você pode escolher como iniciar e manter os aplicativos em execução nas instâncias spot.

Além disso, você pode **combinar facilmente instâncias spot com instâncias sob demanda e reservadas** para otimizar ainda mais o custo e a performance das cargas de trabalho. Você também tem a opção de hibernar, parar ou encerrar as instâncias spot quando o EC2 solicitar a devolução da capacidade, com dois minutos de aviso prévio. Somente a AWS oferece acesso à capacidade computacional não utilizada em uma escala tão massiva, e com um desconto de até 90%.



## Diferenças entre Spot Instances x On-Demand Instances

|                       | Spot Instances  | On-Demand Instances  |
|-----------------------|---|--|
| Launch time           | Can only be <b>launched immediately</b> if the Spot Request is active and capacity is available.  | Can only be launched immediately if you make a <b>manual launch</b> request and capacity is available.             |
| Available capacity    | If capacity is not available, the Spot Request continues to automatically make the launch <b>request until capacity becomes available</b> .   | If capacity is not available when you make a launch request, you get <b>an insufficient capacity error (ICE)</b> . |
| Hourly price          | The hourly price for Spot Instances varies <b>based on demand</b> .   | The hourly price for On-Demand Instances is <b>static</b> .  |
| Instance interruption | You can stop and start an Amazon EBS-backed Spot Instance. In addition, the Amazon EC2 Spot service can <u>interrupt</u> an individual Spot Instance if capacity is no longer available, the Spot price exceeds your maximum price, or demand for Spot Instances increases. | You determine when an On-Demand Instance is interrupted (stopped, hibernated, or terminated).                      |

\* AMI = snapshot para recriação de instância; EC2 Snapshot = ponto para novos volumes ou backup

## Compute: ECS (Elastic Container Service)

É um serviço de **gerenciamento de contêineres** altamente dimensionável e rápido **que facilita a execução, a interrupção e o gerenciamento de contêineres do Docker em um cluster**. Você pode hospedar seu cluster em uma infraestrutura sem servidor gerenciada pelo Amazon ECS ao iniciar seus serviços ou tarefas usando o tipo de inicialização Fargate. Para obter mais controle, você pode hospedar suas tarefas em um cluster de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) gerenciado usando o tipo de inicialização EC2.

## Storage: EBS (Elastic Block Store)

É um serviço de **armazenamento de blocos** de alta performance, projetado para o uso com as instâncias do EC2, para *workloads* com alta taxa de transferência de dados e com transações em qualquer escala.

*Workloads* como BD relacionais e não relacionais, aplicativos corporativos, aplicativos em contêiner, mecanismos de análise de big data, sistemas de arquivos e fluxos de trabalho de mídia são amplamente empregados no Amazon EBS.



- Escolha entre os tipos HDD e SSD
- Armazenamento em bloco persistente e personalizável para instâncias do EC2
- Replicado na mesma zona de disponibilidade
- Backup usando snapshots
- Criptografia fácil e transparente
- Volumes elásticos

Você pode escolher entre quatro tipos de volume diferentes para equilibrar preço e desempenho ideais:

- **Latência** abaixo de 10 ms para *workloads* de BD de alta performance, como o SAP HANA.
- **Transferência de dados** de 1 GB/s para *workloads* sequenciais grandes, como o Hadoop.
- Alterar **os tipos de volume** (com suporte a SSD incluem um volume projetado para aplicativos de alta performance e um volume de uso geral; com suporte a HDD são projetados para grandes *workloads* sequenciais como mecanismos de análise de big data DW).
- Ajustar a **performance** ou aumentar o tamanho do volume sem interromper seus aplicativos essenciais, assim terá armazenamento econômico quando precisar.

Os **volumes EBS** são replicados em uma zona de disponibilidade (AZ) e podem ser facilmente escalonados para petabytes de dados. Além disso, é possível usar o **EBS Snapshots** com políticas de ciclo de vida automatizadas para fazer backup de seus volumes no Amazon S3 e, ao mesmo tempo, garantir a proteção geográfica de seus dados e da continuidade de negócios.

### Storage: Amazon S3 (Simple Storage Service)

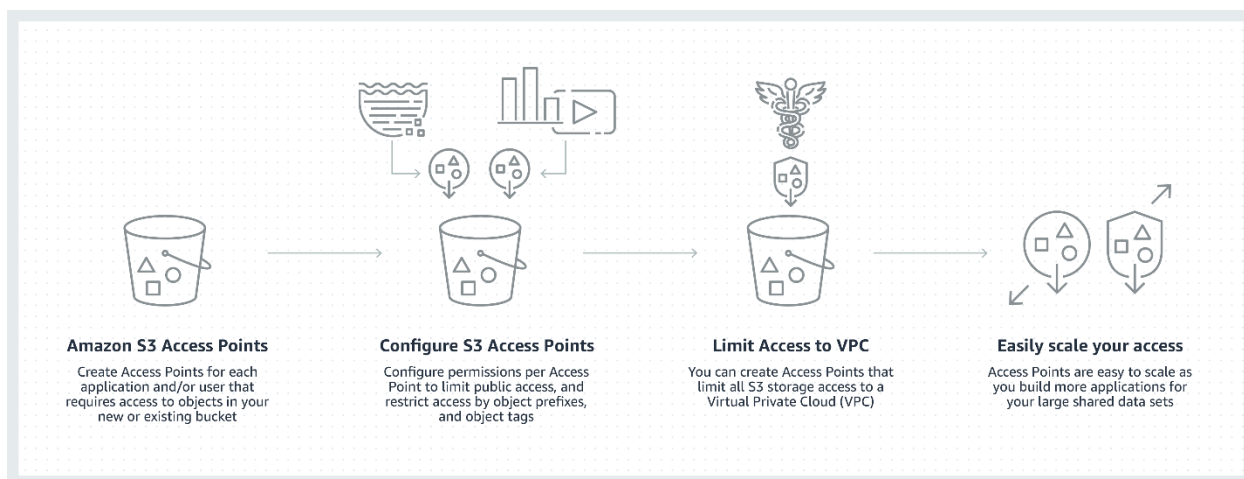
É um serviço **gerenciado de armazenamento na nuvem** que utiliza APIs (ou *endpoints* de VPCs) para armazenar e recuperar dados. Armazena um número praticamente **ilimitado** de objetos (imagens, vídeos, logs, etc.). Também oferece acesso de baixa latência por HTTP ou HTTPS.



O S3 pode ser acessado pelo Console, CLI e SDKs da AWS. O **uso mais comum** do S3 é para armazenamento de ativos de aplicativos, hospedagem de sites estáticos, recuperação de desastre e backup (possui **alta durabilidade**) e área de preparação para Big Data (pelo armazenamento escalável e performance do S3).

Os **pontos de acesso** do S3 simplificam o gerenciamento do acesso de dados para aplicativos que usam conjuntos de dados compartilhados no S3. Os pontos de acesso fornecem um caminho personalizado em

um bucket, com um hostname e uma política de acesso únicos, que aplica as permissões e os controles de rede específicos para qualquer solicitação feita por meio do ponto de acesso.



### Storage: S3 Glacier

O Amazon S3 Glacier e o S3 Glacier Deep Archive são classes de armazenamento em nuvem do Amazon S3 seguro, resiliente e de custo extremamente baixo para **arquivamento de dados e backups de longa duração**. Essas classes foram projetadas para oferecer resiliência de 99,999999999% e disponibilizar recursos abrangentes de segurança e conformidade que podem ajudar a cumprir até mesmo os requisitos normativos mais rigorosos.

A classe de armazenamento Amazon S3 Glacier disponibiliza três opções de recuperação:

- **Recuperações aceleradas:** retornam dados em 1 a 5 minutos; excelentes p/ arquivamento ativo.
- **Recuperações padrão:** são concluídas em 3 a 5 horas e funcionam bem para atividades em que o tempo não é tão crucial, como dados de backup, edição de mídia ou análises de longo prazo.
- **Recuperações em massa:** são a opção de recuperação mais barata, e retornam grandes quantidades de dados em 5 a 12 horas.

A classe de armazenamento **Amazon S3 Glacier Deep Archive** oferece duas opções de recuperação, variando de 12 a 48 horas.

### Storage: EFS (Elastic File System)

Fornece um **sistema de arquivos NFS** (Network File System) elástico, simples, escalável e totalmente gerenciado para uso com os serviços de nuvem AWS e os recursos locais. Ele foi desenvolvido para escalar sob demanda até petabytes sem interromper os aplicativos, aumentando e diminuindo automaticamente à medida que você adiciona e remove arquivos, eliminando a necessidade de provisionar e gerenciar a capacidade com base no crescimento.

O Amazon EFS oferece duas classes de armazenamento:

- **Standard**
- **Infrequent Access (EFS IA):** fornece preço/performance com custo otimizado para arquivos que não são acessados todos os dias.

|                 |                              | File<br>Amazon EFS   | Object<br>Amazon S3   | Block<br>Amazon EBS   |
|-----------------|------------------------------|--|---|---|
| Performance     | Per-operation latency        | Low, consistent  | Low, for mixed request types, and integration with CloudFront                                       | Lowest, consistent  |
|                 | Throughput scale             | Multiple GBs per second  | Multiple GBs per second   | Single GB per second  |
| Characteristics | Data Availability/Durability | Stored redundantly across multiple AZs   | Stored redundantly across multiple AZs  | Stored redundantly in a single AZ                                       |
|                 | Access                       | One to thousands of EC2 instances or on-premises servers, from multiple AZs, concurrently  | One to millions of connections over the web   | Single EC2 instance in a single AZ                                      |
|                 | Use Cases                    | Web serving and content management, enterprise applications, media and entertainment, home directories, database backups, developer tools, container storage, big data analytics | Web serving and content management, media and entertainment, backups, big data analytics, data lake | Boot volumes, transactional and NoSQL databases, data warehousing & ETL |

O Amazon EFS foi criado para fornecer **acesso compartilhado** massivamente paralelo para milhares de instâncias do Amazon EC2, permitindo que seus aplicativos alcancem altos níveis em taxas de transferências agregadas e IOPS com latências baixas e consistentes.

### Storage: AWS Storage Gateway

É um serviço de **armazenamento na nuvem híbrida** que oferece acesso local a armazenamento na nuvem praticamente ilimitado. Os clientes usam o Storage Gateway para simplificar o gerenciamento de armazenamento e reduzir os custos de casos de uso de armazenamento na nuvem híbrida. Esses casos de uso incluem a mudança de backups de fita para a nuvem, a redução do armazenamento local com compartilhamentos de arquivo baseados na nuvem, a disponibilização de acesso de baixa latência a dados na AWS para aplicativos locais, bem como vários casos de uso de migração, arquivamento, processamento e recuperação de desastres.

Para oferecer suporte a esses casos de uso, o serviço oferece três tipos diferentes de gateway: **gateway de fitas, gateway de arquivos e gateway de volumes**. Esses gateways conectam de forma transparente aplicativos locais ao armazenamento na nuvem, armazenando dados em caches locais para oferecer acesso de baixa latência. Os aplicativos se conectam ao serviço por meio de uma máquina virtual ou um dispositivo de gateway de hardware usando protocolos de armazenamento padrão, como NFS, SMB e iSCSI. O gateway é conectado a serviços de armazenamento da AWS, como S3, S3 Glacier, S3 Glacier Deep Archive, EBS e AWS Backup, o que disponibiliza armazenamento para arquivos, volumes, snapshots e fitas virtuais na AWS. O serviço inclui um mecanismo de transferência de dados altamente otimizado, com gerenciamento de largura de banda, resiliência de rede automatizada e transferência de dados eficiente.

### Infra Global AWS

Pode ser separado em três tópicos:

#### AWS Regions



São regiões que hospedam uma ou mais Availability Zones. Ao escolher região, considere latência, minimizar custos e cumprir requisitos normativos. Pode ser implementado recursos em várias regiões (para melhor atender a sua empresa). Exemplo: servidor de *deploy* em uma região e base de clientes em outra. Ou os mesmos recursos em várias regiões, permitindo uma experiência global consistente (independente da localização do cliente).

As regiões são entidades completamente separadas. Os recursos em uma região não são replicados automaticamente a outras (e nem todos os serviços estão disponíveis em todas as regiões).

### Availability Zones

Conjunto de DCs dentro de uma região. São isoladas uma da outra, mas conectadas por uma rede rápida e de baixa latência. Cada uma possui sua própria infraestrutura (alimentação, geradores de backup, redes e conectividade). O isolamento das zonas garante proteção de falhas em outras zonas (alta disponibilidade e redundância de dados em uma região).

### Edge locations (pontos de presença)

Hospedam CDNs (redes de entrega de conteúdos) – Amazon Cloudfront, que é utilizado para entregar conteúdo aos clientes, através de roteamentos ao ponto de presença mais próximo.

### Network: VPC (Virtual Private Cloud)

O VPC **permite provisionar uma seção da Nuvem AWS isolada** logicamente na qual é possível executar recursos da AWS em uma rede virtual que você mesmo define. Você tem controle total sobre seu ambiente de redes virtuais, incluindo a seleção do seu próprio intervalo de endereços IP, a criação de sub-redes e a configuração de tabelas de rotas e gateways de rede. Você pode usar IPv4 e IPv6 na VPC para acessar recursos e aplicativos com segurança e facilidade.

|  |   |
|--|---|
| <ul style="list-style-type: none"><li>📦 Uma rede virtual privada na Nuvem AWS<ul style="list-style-type: none"><li>• Usa os mesmos conceitos que as redes locais</li></ul></li><li>📦 Permite controle completo da configuração de rede<ul style="list-style-type: none"><li>• Capacidade de isolar e expor recursos dentro da VPC</li></ul></li><li>📦 Oferece várias camadas de controles de segurança<ul style="list-style-type: none"><li>• Capacidade de permitir e negar tráfego interno e específico da Internet</li></ul></li><li>📦 Outros produtos da AWS implantam na VPC<ul style="list-style-type: none"><li>• Serviços de segurança inerente à rede</li></ul></li></ul> | <ul style="list-style-type: none"><li>- Boa parte da complexidade da configuração de uma rede foi abstraída sem prejudicar o controle, a segurança e a usabilidade.</li><li>- Clientes podem definir itens de configuração de rede, endereço IP, sub-redes e tabelas roteamento</li><li>- Personalizar regras de roteamento e controle de tráfego de e/s.</li><li>- Há vários produtos AWS que herdam e aproveitam a segurança incorporadas a VPC</li></ul> |
|--|---|

Amazon VPC é um serviço fundamental e se integra a vários serviços da AWS. Por exemplo, instâncias EC2 são implantadas na VPC.



E possuo as seguintes configurações:

- ❏ Criação com base na alta disponibilidade das regiões e zonas de disponibilidade (AZ) da AWS
  - A Amazon VPC reside em uma região
  - Várias VPCs por conta
- ❏ Sub-redes
  - Usadas para dividir a Amazon VPC
  - Permitem que a Amazon VPC abranja várias AZs
- ❏ Tabelas de rotas
  - Controlar o tráfego que sai das sub-redes
- ❏ Gateway de Internet (IGW)
  - Permite acesso à Internet por meio da Amazon VPC
- ❏ NAT Gateway
  - Permite que recursos de sub-rede privada acessem a Internet
- ❏ Listas de controle de acesso de rede (NACL)
  - Controlar o acesso a sub-redes, sem estado



## Network: AWS Direct Connect

Permite **conectar o seu ambiente da AWS ao DC** (ou escritório local) através de uma conexão dedicada de alta velocidade e baixa latência, que *bypass* os provedores de serviços de Internet em seu caminho de rede.

Um local do AWS Direct Connect fornece acesso ao AWS na região à qual está associado e também a outras regiões dos EUA. Permite particionar logicamente as conexões de fibra ótica em várias conexões lógicas chamadas **VLAN** (Virtual Local Area Networks). Você pode tirar proveito dessas conexões lógicas para melhorar a segurança, diferenciar o tráfego e alcançar os requisitos de conformidade.

## Segurança da AWS

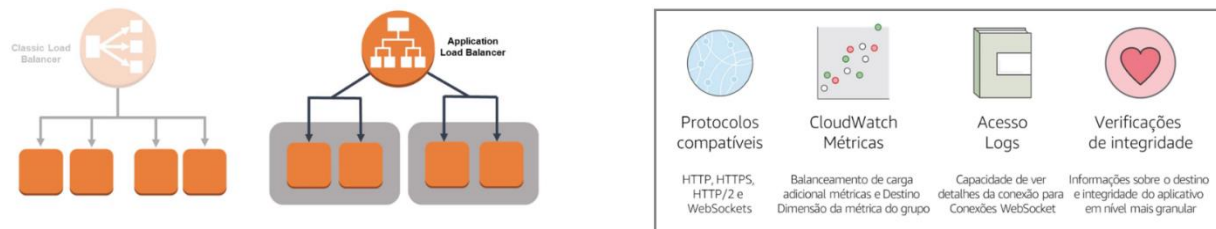
Os grupos de segurança funcionam como um *firewall* integrado para seus servidores virtuais. Com isso, você tem total controle sobre o nível de acesso das suas instâncias.

- Método para filtrar o tráfego das suas instâncias
- As instâncias podem ser totalmente privada até totalmente pública
- Regras para arquiteturas multicamadas

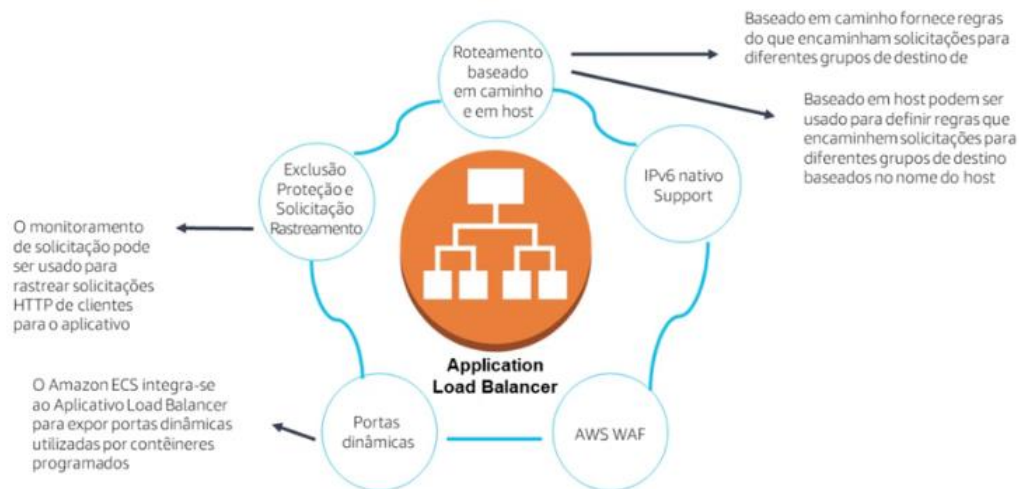
## Integrated Services

### Application Load Balancer

É o um tipo de *load balancer* como parte do serviço Elastic Load Balancer (ELB). Adiciona recursos importantes em relação ao *classic load balancer*, tais como protocolos compatíveis etc.

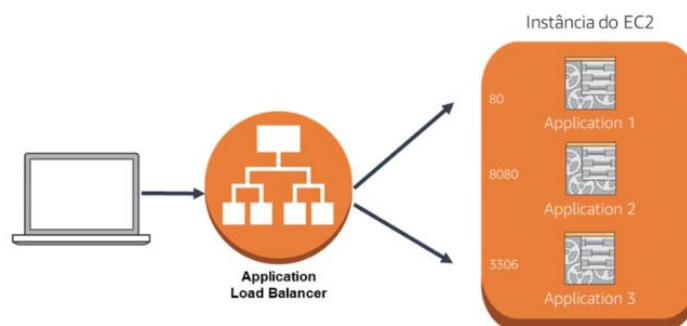


Outros recursos adicionais do Application Load Balancer:

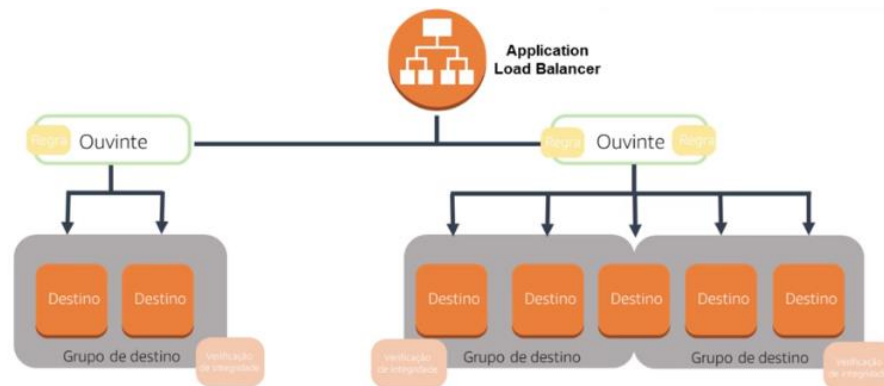


Onde utilizar:

- Capacidade de usar contêineres para hospedar microsserviços e rotear para esses aplicativos de um único *load balancer*
- Permite rotear solicitações diferentes para a mesma instância (diferencia o caminho baseado na porta)



Um grupo de destino é como os destinos são registrados no *load balancer*. O desenho abaixo mostra como o ALB roteia e organiza destinos de back-end. As regras para direcionar solicitações são configuradas nos *listeners*.



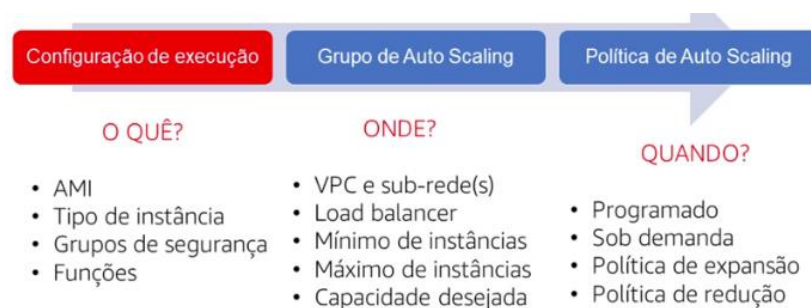
## Auto Scaling

Ajuda a garantir o número correto de instâncias do Amazon EC2 disponíveis para processar a carga dos aplicativos. Permite adicionar/remover instâncias de acordo com as condições especificadas.

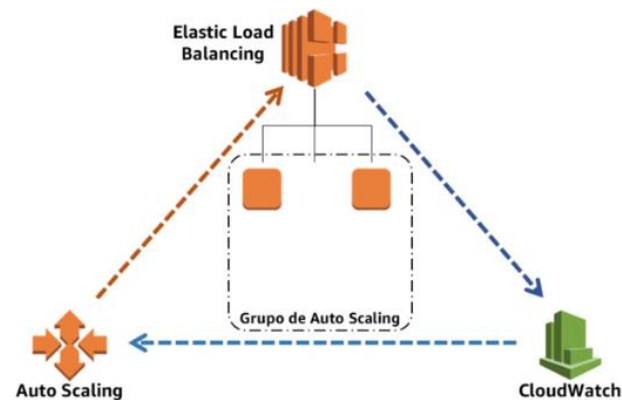
- Como posso garantir que meus *workloads* tenham recursos suficientes do EC2 para atender a requisitos dinâmicos de performance? **Escalabilidade.**
- Como posso dimensionar o provisionamento de recursos do EC2 para que ocorra sob demanda? **Automação.**



Os componentes do Auto Scaling são:



No **Auto Scaling dinâmico**, pode criar alarmes no CloudWatch, com base nas informações de performance de suas instâncias EC2 ou de um *load balancer*.



Load Balancing = Distributing load

Auto scaling = Changing/Adjusting loads

Network: Route 53

É um serviço de DNS projetado para rotear usuários finais a *endpoints* (que pode ser uma aplicação que precisa converter o nome de domínio em IP).



Entre as principais funções do Route 53: registro de domínio, DNS global e altamente disponível, nomes DNS públicos e privados, vários algoritmos de roteamento, IPv4 e IPv6, integrado a outros serviços AWS.

Database: RDS (Relational Database Service)

É um serviço gerenciado que configura e opera um **BD relacional** na nuvem. Permite que você se concentre em performance, alta disponibilidade, segurança e compatibilidade necessárias.

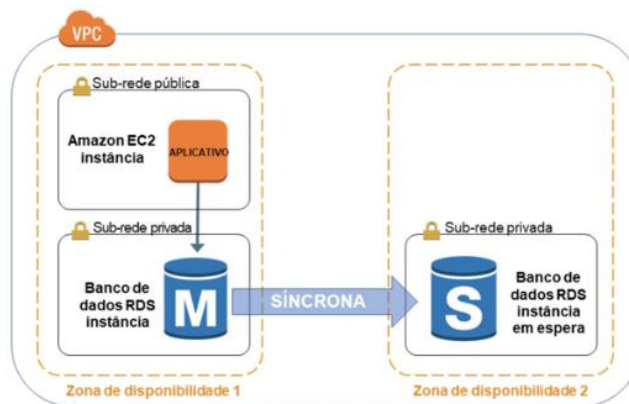
Entre os principais desafios em manter um BD relacional: manutenção do servidor e energia, instalação do software e *patches*, backups, alta disponibilidade, limites de escalabilidade, segurança de dados, instalação de SO e *patches*.



Você pode executar uma instância de BD usando o Amazon VPC. Ao usar VPC, você tem controle do seu ambiente de rede virtual (intervalo de endereços IP, sub-redes, roteamento e listas de controle de acesso).

Geralmente, a instância do BD é isolada em uma sub-rede privada e só está acessível às instâncias de aplicativos indicados. As sub-redes são associadas a uma única *availability zone*.

A configuração de **alta disponibilidade com Multi-AZ** gera uma cópia *stand by* da instância do BD em outra *availability zone* (dentro da mesma VPC). Os dados são replicados de forma síncrona. Ajuda na manutenção e falhas nas instâncias de BD.



O uso de **Réplicas de leituras** do Amazon RDS:



- 📌 Método de replicação assíncrona
- 📌 Descarregar consultas de leitura da instância de banco de dados mestra
- 📌 Ideal para cargas de trabalho do banco de dados com uso intensivo de leitura
- 📌 A réplica de leitura pode ser promovida a Mestra, se necessário

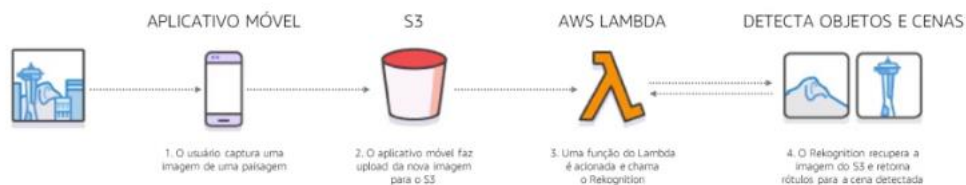
Os **principais benefícios** do RDS: altamente escalável, alta performance, fácil de administrar (console de gerenciamento AWS, CLI ou chamadas API), disponível e durável, seguro e compatível (controle e segurança via VPC ou não).

### Compute: Lambda

É um serviço que permite executar código sem provisionar ou gerenciar recursos. Executa seu código somente quando necessário (orientada a eventos) e dimensiona automaticamente as solicitações.

O AWS Lambda está em uma infraestrutura altamente disponível (inclui manutenção de servidor e SO), com provisionamento de capacidade, Auto Scaling, monitoramento e registro de log.

Oferece suporte a diversas linguagens de programação: Node .JS, Java, C# e Python. O CloudWatch Events é onde configura os *triggers*.



O AWS Lambda pode ser usado em quase qualquer aplicativo, tais como backup automatizados, objetos de processamento enviados para o S3, IoT, etc.

### Exemplo: criação de miniatura da imagem





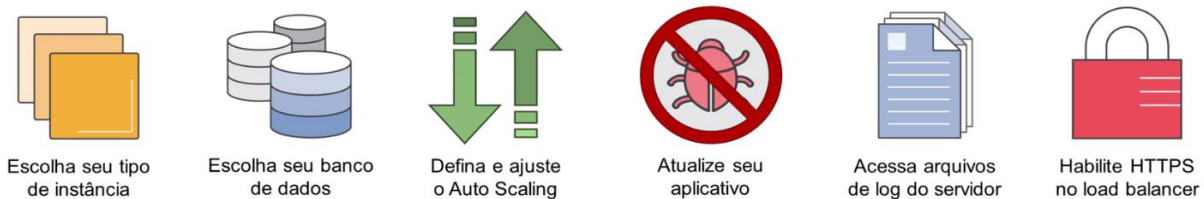
### Exemplo: análise de streaming de dados de mídia social



### Elastic Beanstalk

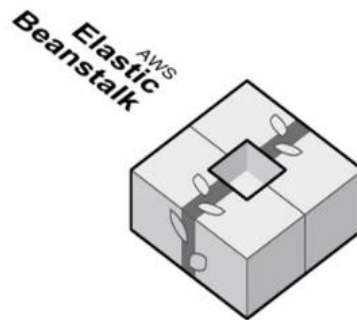
É um PaaS, ou seja, você possui toda a infraestrutura e plataforma criada para você, de modo a colocar o código da aplicação, conforme necessário. Permite a implementação rápida de seus aplicativos e reduz a complexidade de gerenciamento.

Basta fazer o upload de seu código e o Elastic Beanstalk se encarrega automaticamente da implementação, desde o provisionamento de capacidade, o balanceamento de carga e a escalabilidade automática até o monitoramento da saúde do aplicativo.



Oferece suporte a plataformas:

- Packer Builder
- Contêiner único, vários contêineres ou Docker pré-configurado
- Go
- Java SE
- Java com Tomcat
- .NET no Windows Server com IIS
- Node.js
- PHP
- Python
- Ruby



### Simple Notification Service (SNS)

É um serviço de mensagens e comunicações móveis de publicação/assinatura (pub/sub) flexível e totalmente gerenciado. Também coordena a entrega de mensagens para *endpoints* e clientes assinantes.



Permite desacoplar e ajustar a escala de microsserviços, sistemas distribuídos e aplicativos *serverless*.



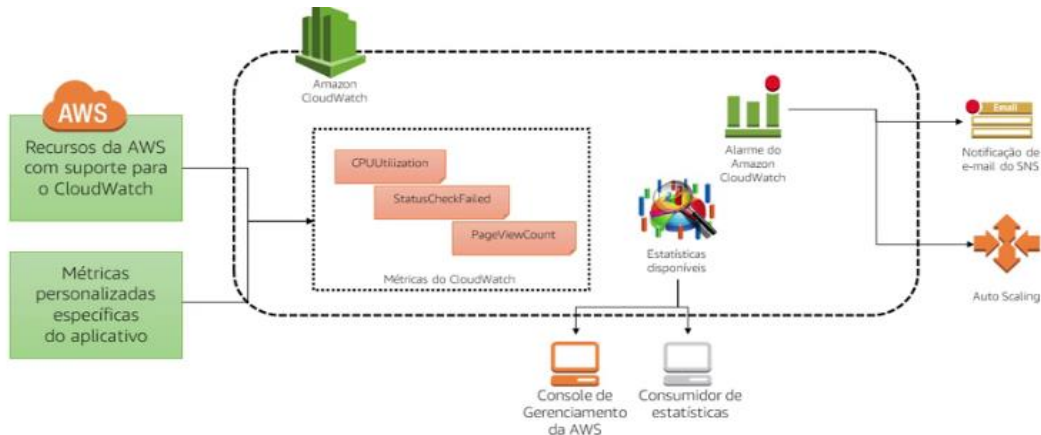
Eventos que precisam disparar e-mail ao administrador, microsserviços que precisam se comunicar entre si, etc.

#### Management: Amazon CloudWatch

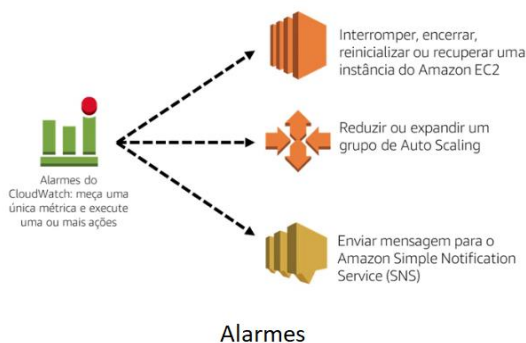
**Monitorea seus recursos** AWS e os aplicativos que você executa em tempo real (métricas como utilização de CPU, transferência de dados, etc.). O CloudWatch fornece dados e *insights* para monitorar aplicativos, responder às alterações de performance em todo o sistema, otimizar a utilização de recursos e obter uma visualização unificada da integridade operacional.

O CloudWatch coleta dados de monitoramento e operações na **forma de logs, métricas e eventos**, oferecendo uma visualização unificada dos recursos, dos aplicativos e dos serviços da AWS executados na AWS e em servidores locais. Você pode usar o CloudWatch para detectar comportamento anômalo em seus ambientes, definir alarmes, visualizar logs e métricas lado a lado, executar ações automatizadas, resolver problemas e descobrir insights para manter seus aplicativos em perfeita execução.

A **capacidade de automaticamente reagir às mudanças** é o principal recurso do CloudWatch.



Os principais componentes do CloudWatch são: métricas, alarmes, eventos, logs e *dashboards*.

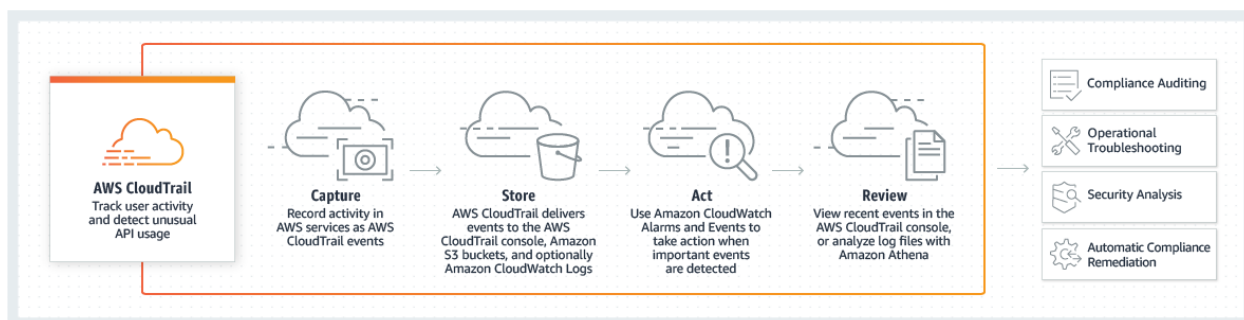


Como detectar e revogar automaticamente o acesso não intencional do IAM com o Amazon CloudWatch Events.



## Amazon CloudTrail

É um serviço que possibilita **governança, conformidade, auditoria e de riscos** em sua conta da AWS. Permite registrar, monitorar continuamente e reter a atividade da conta relacionada às ações executadas na infraestrutura da AWS.



Disponibiliza o **histórico de eventos** da atividade da conta da AWS (inclusive ações via Console de Gerenciamento, SDKs, CLIs e de outros Serviços da AWS). É usado para simplificar as auditorias de compatibilidade ao registrar e armazenar automaticamente **logs de evento de ações executadas em sua conta da AWS**.

**P: Qual é a diferença entre o CloudWatch Events e o AWS CloudTrail?**

Com o CloudWatch, você pode definir regras para **monitorar eventos** específicos e **executar ações** de maneira automática. O AWS CloudTrail é um serviço que **registra chamadas de API** e entrega arquivos de log contendo chamadas de API para seu bucket do Amazon S3 ou um grupo de log do CloudWatch Logs, com o intuito de **conformidade, auditoria e gestão de riscos**.

## AWS Artifact

Os relatórios de **System & Organization Control (SOC)** da AWS são relatórios de exame de terceiros independentes que demonstram como a AWS atende aos principais controles e objetivos de conformidade. O propósito desses relatórios é ajudar você e os seus auditores a entenderem os controles estabelecidos na AWS para apoiar as operações e a conformidade.

O relatório SOC 1 e SOC 2 da AWS estão disponíveis para clientes da AWS por meio do **AWS Artifact**. Relatório de segurança, disponibilidade e confidencialidade SOC 3 da AWS, disponível publicamente como um whitepaper.

#### Storage: CloudFront CDN (Content Delivery Network)

É uma **rede de entrega de conteúdo**. Ao utilizar o CloudFront, você aproveita diversos *edge locations* espalhados pelo mundo para entregar conteúdo, garantido baixa latência na interação com os usuários (através do uso de caches).

Está integrado a outros serviços AWS, tais como AWS Web Application Firewall, Route 53, etc. Pode ser usado para conteúdos estáticos e dinâmicos.

Os tipos de CDN: o RTMP é usado para *streaming* de vídeo e Web para entrega de conteúdo habitual (que não é *streaming*).

- Armazenamento em cache de ativos estáticos
- Streaming de vídeo ao vivo e sob demanda
- Segurança e proteção contra DDoS
- Conteúdo dinâmico e personalizável
- Aceleração de APIs
- Distribuição de software

#### Storage: Snowball Edge

É um dispositivo de **borda de computação e migração de dados** que vem com duas opções:

- **Snowball Edge Storage Optimized:** fornece armazenamento de blocos e armazenamento de objetos compatível com o Amazon S3 e 24 vCPUs. Ele é ideal para armazenamento local e transferência de dados em larga escala.
- **Snowball Edge Compute Optimized:** fornece 52 vCPUs, armazenamento de blocos e objetos e uma GPU opcional para casos de uso, como machine learning avançado e análise de vídeos animados em ambientes desconectados.

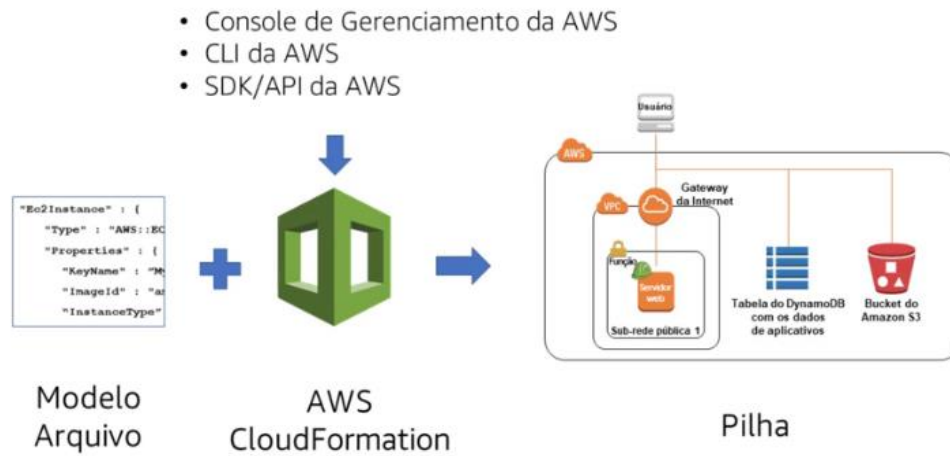
Os clientes podem usar essas duas opções para coleta de dados, machine learning e processamento e armazenamento em ambientes com conectividade intermitente (como fabricação, indústria e transporte), ou em locais extremamente remotos (como operações militares e marinhas) antes de enviá-los de volta à AWS. Esses dispositivos também podem ser montados em rack e agrupados em cluster para criar instalações temporárias maiores.

O Snowball Edge tem suporte para tipos de instância específicos do Amazon EC2, bem como funções AWS Lambda; assim, os clientes podem desenvolver e testar na AWS e então implantar aplicativos em dispositivos em locais remotos para coletar, pré-processar e retornar os dados. Casos de uso comuns incluem migração de dados, transporte de dados, comparação de imagem, captura de fluxo de sensor de IoT e machine learning.

## Management: Amazon CloudFormation

Simplifica a tarefa de criar grupos de recursos relacionados a seus aplicativos. O foco é a **automação do provisionamento de recursos**.

O CloudFormation lê o arquivo modelo (JSON ou YAML) e o *output* é o provisionamento de recursos (conhecido como pilha). Você pode criar, atualizar e excluir pilhas (*stacks*).



## Arquitetura

Os cinco pilares são:

- **Segurança:** IAM, controles de detecção, resposta a incidentes, proteção de infraestrutura e dados. Aplica o princípio de privilégio mínimo e segurança em todas as camadas. Com o modelo de responsabilidade compartilhada, você foca na proteção dos dados da aplicação e SO (e a AWS oferece infraestrutura e serviços seguros).
- **Confiabilidade:** recuperar problemas/falhas (automaticamente), gerenciamento de alterações, previsão, resposta e prevenção de falhas.
- **Eficiência de performance:** selecionar soluções personalizáveis para inovar continuamente (tecnologias avançadas, alcance global em minutos, arquitetura *serverless*, etc.) .
- **Otimização de custos:** refinamento e aprimoramento contínuo dos sistemas. Usar recursos econômicos, combinar oferta e demanda, conscientização sobre despesas e otimizar ao longo do tempo.
- **Excelência operacional:** gerenciar e automatizar alterações, responder a eventos e definir os padrões.

### Tolerância a falhas

- Capacidade de um sistema permanecer operacional
- Redundância integrada do componente de um aplicativo

## Segurança

Uma infraestrutura resiliente, projetada para alta segurança e proteções fortes (*safe guards*) para ajudar a proteger a privacidade dos clientes.

- Atenda aos **requisitos de conformidade** (automação centralizada, controle de segurança e supervisão adicional)
- Modelo de **responsabilidade compartilhada**: herde controles de segurança na AWS. Coloque em camadas seus controles
- **Segurança de rede**: firewalls integrados, criptografia em trânsito, conexões privadas/dedicadas, mitigação de DDoS.
- **Gerenciamento de inventário e configuração**: ferramentas de definição e gerenciamento de modelos
- **Criptografia de dados**: recursos de criptografia, gerenciamento e armazenamento de chaves
- Monitoramento e registro em log
- **AWS Marketplace**: parceiros qualificados que se integram com os controles

Os cinco pilares AWS Well-Architected Framework são:

- **Operational Excellence**: perform operations as code, annotate documentation, make frequent, small, reversible changes, refine operations procedures frequently, anticipate failure e Learn from all operational failures
- **Security**: implement a strong identity foundation, enable traceability, apply security at all layers, automate security best practices, protect data in transit and at rest e prepare for security events
- **Reliability**: test recovery procedures, automatically recover from failure, scale horizontally to increase aggregate system availability, stop guessing capacity e manage change in automation
- **Performance Efficiency**: democratize advanced technologies, go global in minutes, use serverless architectures, experiment more often e mechanical sympathy
- **Cost Optimization**: adopt a consumption model, measure overall efficiency, stop spending money on data center operations, analyze and attribute expenditure e use managed services to reduce cost of ownership

### Modelo de responsabilidade compartilhada

|                    |  |         |
|--------------------|--|---------|
| <b>User Data</b>   | Chave de acesso e métodos de criptografia são criados pelo cliente | Cliente |
| <b>Application</b> | AWS não controla a sua aplicação                                   | Cliente |
| <b>Guest OS</b>    | AWS não interfere na escolha. Pode ser windows, linux, etc.        | Cliente |
| <b>Hypervisor</b>  | AWS usa Hypervisor baseado em Xex. É seguro e escalável            | AWS     |
| <b>Network</b>     | Protocolos de rede proprietários (VPC, etc.) para prover segurança | AWS     |
| <b>Physical</b>    | Gerenciamento físico (acesso restrito a DCs, etc.)                 | AWS     |

Os clientes que implantam uma instância do EC2 são responsáveis pelo gerenciamento do SO convidado (o que inclui atualizações e *patches* de segurança), por qualquer utilitário ou software de aplicativo instalado pelo cliente nas instâncias, bem como pela configuração do firewall disponibilizado pela AWS (chamado de grupo de segurança) em cada instância.

## IAM (Identity and Access Management)

Trabalha com os conceitos de **Group** – **User** (credenciais permanentes; pode ser usuário e senha, chave de acesso, chave secreta, etc.) – **Role** (método de autenticação; não são permissões).

A **permissão** ocorre na *Policy Docs* que é um objeto separado. Esse JSON pode ser anexado a um grupo, usuário ou role. Cada ação ocorrida em APIs (maioria dos serviços é utilizada por APIs) é registrada no CloudTrail.

IAM - casos de uso:

- Controle acesso aos recursos AWS: controle de acesso às APIs de serviços e recursos específicos da AWS. Permite adicionar condições (horário de uso para um usuário, seu IP de origem, se estão usando SSL ou autenticação multifator).
- Autenticação multifator
- Analisar o acesso
- Integração ao diretório corporativo (como o MSFT AD)
- Gerencie permissões com grupo; configure uma política de senha forte

## Amazon Inspector

É um serviço de avaliação de segurança automatizado. Avalia **vulnerabilidades** e desvios das melhores práticas. Produz relatórios com descobertas de segurança e etapas priorizadas para a correção. É baseado em agentes e orientado por API.



- ❗ Inclui uma base de conhecimento com centenas de regras que são mapeadas para:
  - ✓ Padrões comuns de segurança e conformidade
  - ✓ Definições de vulnerabilidade
- ❗ Atualizadas regularmente pelos pesquisadores de segurança da AWS

Exemplos de regras integradas



## AWS Shield

É um serviço gerenciado contra DDoS que protege aplicações em execução na AWS.



Protege outros recursos da AWS: Route 53 (proteção zonas hospedadas do Route 53 contra DDoS ataques – inundações, ataques de reflexão, etc.), CloudFront (proteções nas camadas 3 e 4 de infraestrutura, usando engenharia de tráfego) e VPC.

## Segurança e conformidade

AWS compartilha informações de segurança: obtenções de certificado do setor, publicação de práticas de segurança e controle, relatórios de conformidade.

Programas de garantia – a AWS fornece informações e recursos de conformidade para suporte jurídico/normativo, certificações/declarações e alinhamentos/estruturas.

### Ajude os clientes a:

- ✓ Documentar uma estrutura completa de controle e governança
- ✓ Implantar soluções que atendam a vários padrões específicos do setor



Serviços de Informação da Justiça Criminal (CJIS)

Cloud Security Alliance (CSA)

Family Educational Rights and Privacy Act (FERPA – Lei de direitos educacionais e privacidade da família)

Health Insurance Portability and Accountability Act (HIPAA – Lei de portabilidade e responsabilidade do seguro de saúde)

Motion Picture Association of America (MPAA)












- Inclui políticas, processos e atividades de controle para proteger a entrega de ofertas de produtos da AWS
- Oferece suporte à eficácia operacional da estrutura de controle da AWS
- Integra controles específicos da nuvem
- Aplica as melhores práticas do setor



## AWS Personal Health Dashboard

Fornece alertas e orientações de remediação quando a AWS enfrenta **eventos** que podem afetá-lo. Também há uma exibição personalizada do desempenho e da disponibilidade dos serviços da AWS subjacentes aos seus recursos da AWS. O painel exibe informações relevantes e oportunas para ajudar a gerenciar eventos em andamento e fornece notificações proativas para ajudar a planejar atividades programadas.

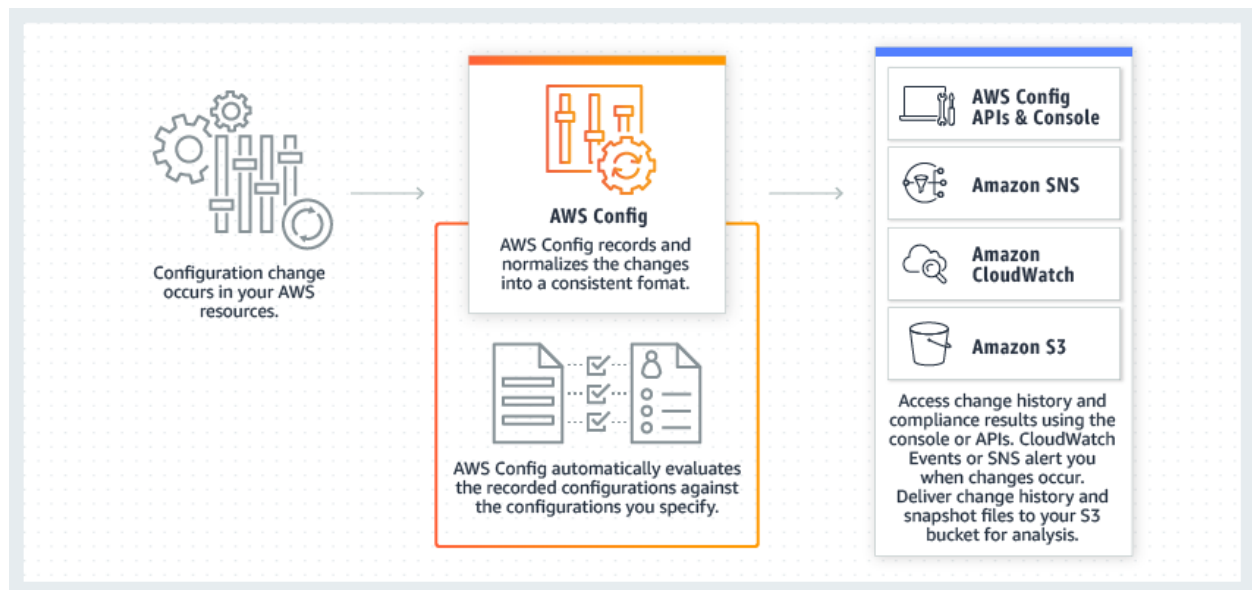
AWS **Service Health Dashboard** é aquele que exibe o **status** dos serviços (*service availability*) no Dashboard.

|  |               |                               |        |              |             |   |
|--|---------------|-------------------------------|--------|--------------|-------------|---|
| North America  | South America | Europe                        | Africa | Asia Pacific | Middle East | Contact Us  |
| Recent Events  |               | Details                       |        |              |             | RSS   |
|  No recent events.                  |               |                               |        |              |             |   |
| Remaining Services   |               | Details                       |        |              |             | RSS   |
|  Alexa for Business (N. Virginia)   |               | Service is operating normally |        |              |             |  |
|  Amazon API Gateway (Montreal)      |               | Service is operating normally |        |              |             |  |
|  Amazon API Gateway (N. California) |               | Service is operating normally |        |              |             |  |
|  Amazon API Gateway (N. Virginia)   |               | Service is operating normally |        |              |             |  |

## AWS Config

É um serviço que permite **acessar, auditar e avaliar as configurações** dos recursos da AWS. O Config monitora e grava continuamente registros das configurações de recursos da AWS e lhe permite automatizar a avaliação das configurações registradas com base nas configurações desejadas.

Com o Config, você pode analisar alterações feitas nas configurações e relacionamentos entre os recursos da AWS, aprofundar-se de forma detalhada no histórico de configuração de recursos e determinar a conformidade geral em relação às configurações especificadas em suas diretrizes internas. Dessa forma, você pode simplificar a **auditoria de conformidade, a análise de segurança, o gerenciamento de mudanças e a solução de problemas operacionais.**



## Definição de preço e suporte

### Detalhes da definição de preço

Possui as seguintes modalidades:

- **Pay as you go:** serviços pagos conforme o uso (sem penalização de saída)
- **Capacidade reservada:** pode economizar até 75% em relação à capacidade sob demanda equivalente. Estão disponíveis em três opções: AURI (tudo adiantado), PURI (parcialmente adiantado) e NURI (nenhum pagamento adiantado). Quanto maior o pagamento adiantado, maior será o desconto.

Sua organização pode minimizar riscos, gerenciar orçamentos de forma mais previsível e cumprir políticas que exigem compromissos a longo prazo. Serviços como EC2 e RDS podem utilizar capacidade reservada.

Pague por:

- Capacidade computacional
- Armazenamento
- Transferência de dados de saída (agregada)

Não há cobrança para:

- Transferência de dados de entrada

### Capacidade reservada

As instâncias reservadas proporcionam um **desconto significativo** (até 75%) em comparação com a definição de preço das instâncias por demanda e podem ser compradas por um **período de 1 ou 3 anos**. Ao serem atribuídas a uma zona de disponibilidade específica, elas disponibilizam uma reserva de capacidade, podendo executar instâncias quando for necessário.

Os clientes têm a **flexibilidade** de alterar a zona de disponibilidade, o tamanho da instância e o tipo de rede de suas instâncias reservadas padrão. O nível gratuito da AWS inclui 750 horas de instâncias t2.micro Linux e Windows por mês por um ano.

Compre **instâncias reservadas conversíveis** se precisar de flexibilidade adicional, como SO, famílias de instâncias, ou locações diferentes durante o período de vigência. As instâncias reservadas conversíveis oferecem um desconto considerável (até 54%) em comparação às instâncias sob demanda e podem ser compradas por um período de vigência de 1 ou 3 anos.

As três opções de reserva que a AWS oferece:

- **All Upfront:** o cliente opta por pagar pelo custo total da instância em uma única vez de acordo com o período escolhido (1 ano ou 3 anos). O custo é à vista e englobará o valor total do período, não haverá cobranças mensais adicionais sobre a instância reservada. Nesse modelo o desconto pode chegar à 60%.

- **Partial Upfront:** o cliente opta por pagar um valor menor à vista (se compararmos ao modelo All Upfront) e as cobranças mensais terão um grande desconto. No geral, o desconto gira em torno de 35%.
- **No Upfront:** o cliente não pagará nenhum valor à vista, porém o desconto será aplicado da mesma forma nas cobranças mensais. Lembre-se que ao efetuarmos uma reserva estamos fechando um contrato com AWS e as cobranças mensais pela instância serão realizadas nos meses decorrentes do contrato. Nesse modelo, o desconto gira em torno de 30%.

#### Faturamento por segundo/hora:

- Os recursos geram cobranças somente quando estão em execução

#### Configuração da instância:

- Capacidade física da instância
- A definição de preço varia de acordo com:
  - ✓ Região da AWS
  - ✓ SO
  - ✓ Tipo de instância
  - ✓ Tamanho da instância



Amazon EC2

#### Base de definição de preço em:

- Solicitações:
  - ✓ Número de solicitações
  - ✓ Tipo de solicitações – taxas diferentes para solicitações GET
- Transferência de dados:
  - ✓ Quantidade de dados transferidos para fora da região do Amazon S3



Amazon S3

- Volumes: todos os tipos cobrados pela quantidade provisionada por mês
- IOPS:
  - ✓ Uso geral (SSD): incluído no preço
  - ✓ Magnético: cobrado pelo número de solicitações
  - ✓ IOPS provisionadas (SSD): cobradas pela quantidade provisionada em IOPS



Amazon EBS

- Snapshots: custo adicional por GB-mês de dados armazenados
- Transferência de dados:
  - ✓ A transferência de dados de entrada não tem cobrança.
  - ✓ Faixas de cobrança para transferência de dados de saída.



Amazon EBS

- Faturamento por hora: os recursos incorrem em cobranças durante a execução.
- Características do banco de dados: modelo, tamanho e classe de memória afetam o custo.
- Tipo de compra de banco de dados:
  - ✓ As instâncias de banco de dados sob demanda são cobradas por hora.
  - ✓ Instâncias de banco de dados reservadas exigem pagamento adiantado para instâncias de banco de dados reservadas.
  - ✓ Provisione várias instâncias de banco de dados para lidar com picos de carga.



Amazon RDS

- Armazenamento provisionado:
  - ✓ Gratuito para armazenamento de backup de até 100% do armazenamento de banco de dados
  - ✓ Armazenamento de backup para instâncias de banco de dados encerradas cobrando a GB/mês
- Armazenamento adicional: armazenamento de backup além do armazenamento provisionado cobrado a GB/mês



Amazon RDS

- A definição de preço varia entre regiões geográficas
- Com base em:
  - ✓ Solicitações
  - ✓ Transferência de dados para fora



Amazon CloudFront

- Instâncias sob demanda:
  - ✓ Capacidade computacional por hora e segundo
  - ✓ Mínimo de 60 segundos
- Instâncias reservadas:
  - ✓ Instâncias de pagamento antecipado baixas ou não reservadas
  - ✓ Desconto na cobrança por hora para essa instância
- Instâncias spot:
  - ✓ Você faz ofertas pela capacidade não utilizada do Amazon EC2



Amazon EC2

- Preços de SO incluídos nos preços de instância
- Software:
  - ✓ Parceria com outros fornecedores
  - ✓ Licenças de fornecedor necessárias
  - ✓ Licenças existentes aceitas por meio de programas específicos de fornecedores



Amazon EC2

- **AWS Cost Explorer:** permite uma análise detalhada dos dados de custos e uso para identificar tendências, indicar os fatores determinantes dos custos e detectar anomalias. Também criar relatórios de uso e custos (ambos em um nível mais resumido) ou para solicitações altamente

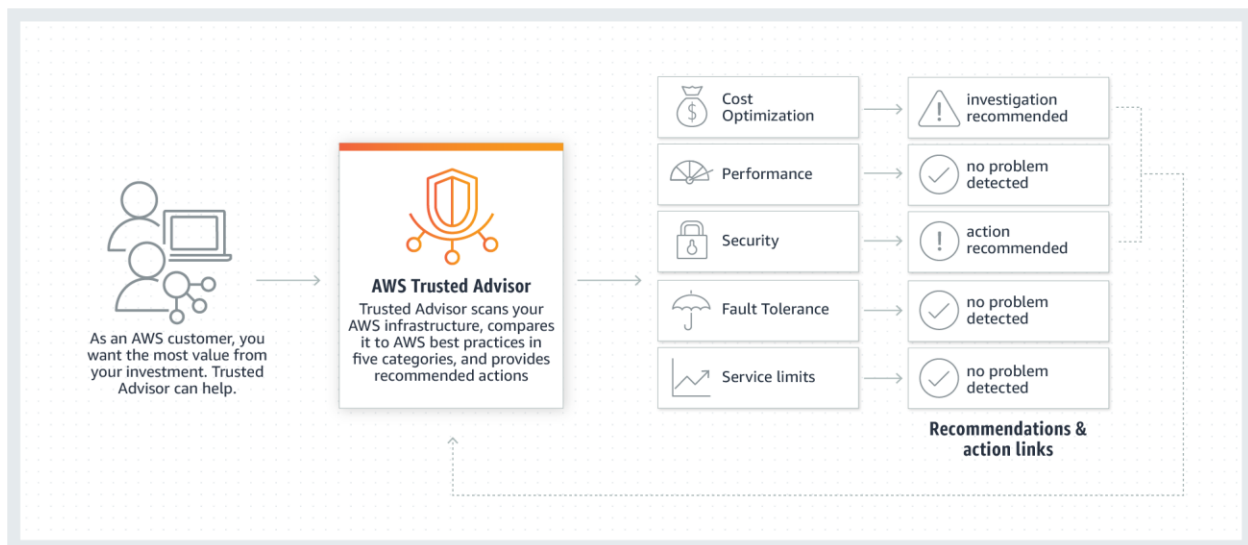
específicas (por exemplo, os custos da m2.2xlarge na conta Y marcados como “projeto: secretProject”).

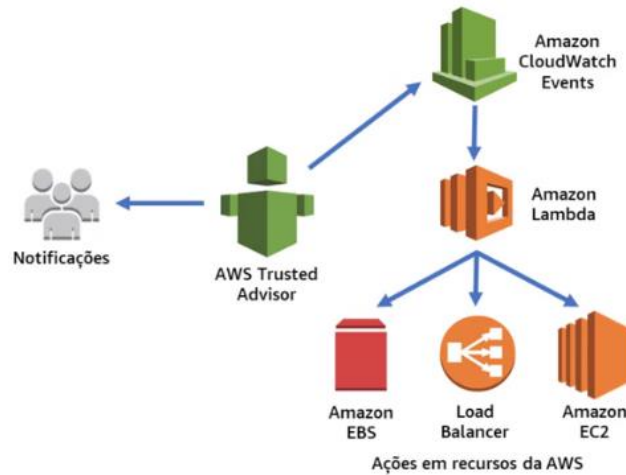
- **AWS Budgets:** permite definir orçamentos personalizados que enviam alertas quando o uso ou os custos excedem (ou tendem a exceder) o valor orçado. Também pode ser usado para definir metas de utilização ou cobertura de reservas e receber alertas quando a utilização cair abaixo do limite definido. Os alertas de reservas são compatíveis com reservas dos serviços Amazon EC2, Amazon RDS, Amazon Redshift, Amazon ElastiCache e Amazon Elasticsearch.

### Trusted Advisor

É uma ferramenta que fornece orientações em tempo real para ajudar a provisionar recursos de acordo com as melhores práticas da AWS (que podem ser usadas em novos fluxos de trabalho, desenvolver aplicativos, aprimoramentos contínuos, etc.).

Casos indicam que o Trusted Advisor ajudou ao destacar: Instâncias do EC2 não utilizadas, Instâncias reservadas do Amazon EC2, volumes não utilizados do Amazon EBS, etc.





## AWS Support

O suporte é fornecido para:

- Testar com a AWS
- Usar a AWS em produção
- Usar essencialmente para os negócios da AWS
- Orientações proativas (gerente técnico de conta – TAM)
- Melhores práticas (Trusted Advisor)
- Assistência à conta (AWS Support Concierge)

O AWS Support oferece quatro planos de suporte:

- Suporte básico
- Developer Support
- Business Support
- Enterprise Support

|   | Desenvolvedor   | Business   | Empresarial  |
|---|---|--|--|
|   | <i>Recomendado se você está experimentando ou testando a AWS.</i>   | <i>Recomendado se você tem cargas de trabalho de produção na AWS.</i>  | <i>Recomendado se você tem cargas de trabalho empresariais e/ou de missão crítica na AWS.</i>  |
| Verificação de melhores práticas do AWS Trusted Advisor | Sete verificações principais  | Conjunto completo de verificações  | Conjunto completo de verificações  |
| Suporte técnico aprimorado                              | Acesso aos associados do Cloud Support pelo e-mail em horário comercial**<br>Casos ilimitados/um contato primário | Acesso aos engenheiros do Cloud Support por telefone, e-mail e chat 24 horas por dia, 7 dias por semana<br>Casos ilimitados/contatos ilimitados (com suporte do IAM)                                   | Acesso aos engenheiros do Cloud Support por telefone, e-mail e chat 24 horas por dia, 7 dias por semana<br>Casos ilimitados/contatos ilimitados (com suporte do IAM)   |
| Severidade do caso/tempo de resposta*                   | Orientações gerais:<br>< horário comercial**<br><br>Falha no sistema:<br>< horário comercial**                    | Orientações gerais:<br>Menos de 24 horas<br><br>Falha no sistema:<br>Menos de 12 horas<br><br>Falha no sistema de produção:<br>Menos de 4 horas<br><br>Sistema de produção inativo:<br>Menos de 1 hora | Instruções gerais:<br>Menos de 24 horas<br><br>Falha no sistema:<br>Menos de 12 horas<br><br>Falha no sistema de produção:<br>Menos de 4 horas<br><br>Sistema de produção inativo:<br>Menos de 1 hora<br><br>Sistema inativo essencial para as atividades da empresa:<br>Menos de 15 minutos |
| Orientações de arquitetura                              | Geral   | Contextual em relação ao seus casos de uso   | Revisão consultiva e orientações de acordo com os aplicativos  |
| Gerenciamento programático de casos                     |   | API do AWS Support   | API do AWS Support   |
| Suporte a software de terceiros                         |   | Orientações de interoperabilidade e configuração, e solução de problemas   | Orientações de interoperabilidade e configuração, e solução de problemas   |
| Programas proativos                                     |   | Acesso ao gerenciamento de eventos de infraestrutura mediante taxa adicional.  | Gerenciamento de eventos de infraestrutura<br>Análises do Well-Architected<br>Revisões de operações<br><br>Gerente técnico da conta (TAM) coordena o acesso a programas e outros especialistas da AWS, conforme a necessidade.   |
| Gerente técnico da conta                                |   |  | Gerente técnico da conta (TAM) designado para monitorar proativamente o ambiente e auxiliar na otimização.   |
| Treinamento   |   |  | Acesso a laboratórios autoguiados online   |

## TCO (Total cost ownership)

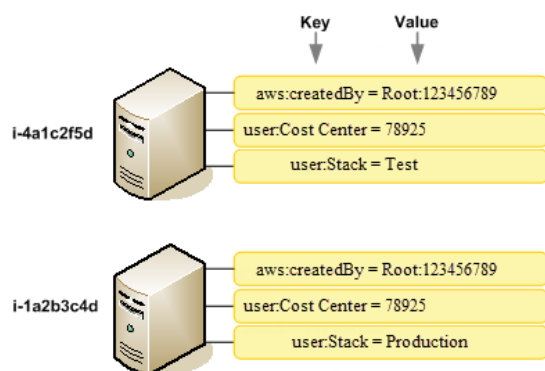
As calculadoras de TCO permitem estimar a **redução de custo** ao usar a AWS e oferecem um conjunto de relatórios detalhados (*server hw, network hw, hw maintenance, power and cooling, data center space, personnal/staff and aws instances*). As calculadoras também permitem modificar as suposições de acordo com suas necessidades empresariais.

## Estimate your AWS billing

- To estimate the costs of migrating on-premises infrastructure to AWS, use **the AWS Total Cost of Ownership (TCO) Calculator**.
- If you plan to migrate significant infrastructure to AWS, use the **AWS Sales & Business Development** contact form, and then choose I need to speak to someone in sales.
- To estimate a bill, use the **AWS Pricing Calculator**. Enter your planned resources by service, and the AWS Pricing Calculator provides an estimated cost per month.
- To forecast your costs, use the **AWS Cost Explorer**. Use cost allocation tags to divide your resources into groups, and then estimate the costs for each group.

Use esta calculadora para comparar o custo da execução das aplicações em um ambiente local ou de hospedagem tradicional com o custo da execução na AWS. Descreva sua configuração de ambiente local ou hospedado para produzir uma comparação detalhada de custos com a AWS.

Uma **tag** é um rótulo que você ou a AWS atribui a um recurso da AWS. Cada tag consiste em uma chave e um valor. Você pode usar tags para organizar os seus recursos e tags de alocação de custos para acompanhar os custos da AWS em um nível detalhado. Depois de ativar as tags de alocação de custos, a AWS as utiliza para organizar seus custos de recursos no cost allocation report, facilitando a categorização e o controle dos custos da AWS.



### Consolidated billing for AWS Organizations

Usado para **consolidar o faturamento e o pagamento de várias contas** da AWS ou da Amazon Internet Services Pvt. Ltd (AISPL). Todas as organizações possuem uma conta mestra (pagante) que paga as cobranças de todas as contas-membro (vinculadas). O uso em conjunto permite compartilhar os descontos de preços por volume, de instância reservada e os Savings Plans.

Isso pode resultar em um custo mais baixo para o seu projeto, departamento ou empresa do que com contas independentes individuais. O faturamento consolidado é oferecido sem qualquer custo adicional.



## Outros serviços (podem ser abordados na prova)

### Compute

- **Lambda:** permite executar código sem provisionar ou gerenciar servidores. Você paga apenas pelo tempo de computação consumido. Ele pode ser acionado automaticamente por meio de outros serviços da AWS ou diretamente usando qualquer aplicativo móvel / web.
- **Fargate:** é um mecanismo *serverless* para contêineres que funciona com o Amazon Elastic Container Service (ECS) e com o Amazon Elastic Kubernetes Service (EKS). O Fargate elimina a necessidade de provisionar e gerenciar servidores, permite que você pague pelos recursos por aplicativo. Executa cada tarefa ou pod no próprio kernel do serviço.

### Database

- **DynamoDB (noSQL):** é um BD de valor-chave e documento que oferece desempenho de milissegundos com um dígito em qualquer escala. Se estende por várias regiões e armazenamento em cache na memória para aplicativos em escala. Pode processar mais de 10 trilhões de solicitações por dia e picos de mais de 20 milhões de solicitações por segundo. Muito usado em aplicativos móveis e web e aplicativos para jogos, tecnologia de anúncios, IoT e de outras áreas que precisam de acesso a dados com baixa latência.
- **Aurora:** é um BD **relacional** compatível com MySQL e PostgreSQL e criado para a nuvem que combina a performance e a disponibilidade de BD comerciais com a simplicidade e a economia de BD *open source*. É até cinco vezes mais rápido que bancos de dados MySQL padrão e três vezes mais rápido que bancos de dados PostgreSQL padrão. Oferece um sistema de armazenamento distribuído, tolerante a falhas e com recuperação automática que escala automaticamente para até 64 TB por instância de banco de dados. O Amazon Aurora é gerenciado pelo Amazon Relational Database Service (RDS).
- **MariaDB:** é um BD **relacional** de *open source*, que foi criado pelos desenvolvedores originais do MySQL. O Amazon RDS facilita a configuração, a operação e a escalabilidade de implantações do servidor MariaDB na nuvem. Com o Amazon RDS, você pode implantar bancos de dados na nuvem escaláveis do MariaDB em minutos, com capacidade de hardware redimensionável e econômica.
- **Redshift:** é um produto de DW que faz parte da AWS. Com o Redshift, você pode consultar petabytes de dados estruturados e semiestruturados em DW e data lakes usando SQL padrão. O Redshift permite salvar facilmente os resultados das consultas de volta no data lake do S3 usando formatos abertos, como o Apache Parquet, para análises adicionais de outros serviços analíticos como Amazon EMR, Amazon Athena e Amazon SageMaker.
- **DMS (migração):** ajuda você a migrar BD para a AWS de modo rápido e seguro. O BD de origem permanece totalmente operacional durante a migração, minimizando o tempo de inatividade de aplicativos que dependem do BD. O DMS viabiliza migrações homogêneas, como de Oracle para Oracle, além de migrações heterogêneas entre plataformas de BD diferentes, como de Oracle ou de Microsoft SQL Server para Amazon Aurora. Ao migrar BD para o Amazon Aurora, o Amazon Redshift, o Amazon DynamoDB ou o Amazon DocumentDB (com compatibilidade com o MongoDB), você pode usar o DMS grátis por seis meses.

(DB2 não é suportado na AWS)

## Security & Identity

- **WAF (Web Application Firewall):** é um firewall que ajuda a proteger os aplicativos ou APIs contra exploits comuns na web. Fornece controle sobre como o tráfego atinge seus aplicativos, permitindo criar regras de segurança que bloqueiam padrões de ataque comuns, como injeção de SQL ou scripts entre sites, e regras que filtram padrões de tráfego específicos. As Regras gerenciadas do WAF abordam questões como os 10 principais riscos de segurança da OWASP. Essas regras são atualizadas regularmente conforme surgem novos problemas. O AWS WAF inclui uma API multifuncional que você pode usar para automatizar a criação, a implantação e a manutenção de regras de segurança.

A definição de preço baseia-se em quantas regras você implanta e em quantas solicitações o seu aplicativo recebe. Você pode implantar o AWS WAF no Amazon CloudFront como parte de uma solução de CDN, no Application Load Balancer que fica na frente dos servidores web ou de origem executados no EC2 ou no Amazon API Gateway para suas APIs.

## Analytics

- **EMR (Elastic Map Reduce):** é a plataforma de big data em Cloud para processar grandes quantidades de dados usando ferramentas de código aberto, como Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi e Presto. Com o EMR, você pode executar análises em escala de Petabytes a menos da metade do custo das soluções tradicionais locais e 3x mais rápido que o Apache Spark padrão.

Analisa dados sem precisar gerenciar Hadoop clusters. Para trabalhos de execução curta, você pode aumentar e diminuir os clusters e pagar por segundo pelas instâncias usadas. Para cargas de trabalho de longa execução, você pode criar clusters altamente disponíveis que são dimensionados automaticamente para atender à demanda.

- **Kinesis:** permite consumir dados em tempo real como vídeo, áudio, logs de aplicativos, clickstreams de sites e dados de telemetria de IoT para machine learning, análises e outros aplicativos. Ainda processar e analisar dados assim recebidos e responder instantaneamente, em vez de aguardar a conclusão da coleta de dados para poder iniciar o processamento.

## Application Services

- **API Gateway:** é um serviço gerenciado que permite que desenvolvedores criem, publiquem, mantenham, monitorem e protejam APIs em qualquer escala com facilidade. Usando o API Gateway, você pode criar APIs do RESTful e APIs do WebSocket que habilitam aplicativos de comunicação bidirecionais em tempo real. O API Gateway dá suporte a cargas de trabalho containerizadas e sem servidor, além de aplicativos da web.

O API Gateway administra todas as tarefas envolvidas no recebimento e processamento de até centenas de milhares de chamadas de API simultâneas, inclusive gerenciamento de tráfego, suporte de CORS, controle de autorização e acesso, com fluxo controlado, monitoramento e

gerenciamento de versões de API. Você paga apenas pelas chamadas de API recebidas e pela quantidade transferida de dados de saída.

- **SQS (Simple Queue Service):** é um serviço de filas de mensagens gerenciado que permite o desacoplamento e a escalabilidade de microsserviços, sistemas distribuídos e aplicativos sem servidor. O SQS elimina a complexidade e a sobrecarga associadas ao gerenciamento e à operação de middleware orientado a mensagens, além de permitir que os desenvolvedores se dediquem a criar diferenciais.

O SQS oferece dois tipos de filas de mensagens. As filas padrão oferecem throughput máximo, o melhor esforço de classificação e entrega pelo menos uma vez. As filas FIFO do SQS são criadas para garantir que as mensagens serão processadas exatamente uma vez, na ordem exata em que forem enviadas.

### Enterprise Applications

- **Workspaces:** é uma solução de desktop como serviço (DaaS) gerenciada e segura. Provisiona desktops Windows ou Linux em minutos e escala rapidamente para oferecer milhares de desktops a funcionários em todo o mundo. O pagamento pode ser feito mensalmente ou por hora e apenas pelos WorkSpaces executados, ajudando você a economizar dinheiro em comparação aos desktops tradicionais e às soluções de Virtual Desktop Infrastructure (VDI – Infraestrutura de desktop virtual) no local.

### Artificial Intelligence

- **Machine Learning:** o Amazon SageMaker é o serviço de ML para criar, treinar e implantar modelos de ML rapidamente. Ele remove a complexidade que atrapalha a implementação bem-sucedida do ML desde a execução de modelos para detecção de fraudes em tempo real, passando pela análise virtual de impactos biológicos de medicamentos em potencial, até a previsão de êxito no roubo de bases no baseball.

### AWS Developer Tool

- **CodePipeline:** automatize pipelines de CI/CD para oferecer atualizações rápidas e confiáveis.
- **CodeCommit:** hospede com segurança repositórios Git privados altamente escaláveis.
- **CodeBuild:** compile e teste código com escalabilidade contínua.
- **CodeDeploy:** automatize implantações de código para manter a disponibilidade dos aplicativos.
- **X-ray:** analise e depure aplicações distribuídas em produção.
- **Codestar:** desenvolva, crie e implante aplicativos na AWS. Com o AWS CodeStar, é possível configurar toda a sua cadeia de ferramentas de entrega contínua, possibilitando que você comece o lançamento de códigos mais rapidamente.
- **OpsWorks:** é um serviço de gerenciamento de configurações que oferece instâncias gerenciadas do Chef e do Puppet, permitindo automatizar a forma como os servidores são configurados, implantados e gerenciados em instâncias do Amazon EC2 ou ambientes de computação no local. O OpsWorks tem três ofertas, AWS OpsWorks for Chef Automate, AWS OpsWorks for Puppet Enterprise e AWS OpsWorks Stacks.