Contents

[**TIPO DE CLOUD** 3](#_Toc131248380)

[**AWS** 4](#_Toc131248381)

[**Região e Zona de disponibilidade** 4](#_Toc131248382)

[**Amazon Cloudfront.** 5](#_Toc131248383)

[**IAM (Identity and Access Managemen)** 5](#_Toc131248384)

[**AWS Compute** 6](#_Toc131248385)

[**1 Amazon EC2** 6](#_Toc131248386)

[**2 Amazon EC2 auto scaling** 6](#_Toc131248387)

[**3 Amazon Elastic load balancing** 7](#_Toc131248388)

[**4 Amazon Elasitic contanainer service (ECS)** 8](#_Toc131248389)

[**5 Amazon Elastic Kubernetes Service (Amazon EKS)** 8](#_Toc131248390)

[**6 Amazon Elasitic Beanstalk** 8](#_Toc131248391)

[**7 AWS CloudFormation** 9](#_Toc131248392)

[**8 AWS Fargate** 9](#_Toc131248393)

[**9 AWS Lambda** 9](#_Toc131248394)

[**Outros serviços** 10](#_Toc131248395)

[**Qual serviço usar** 10](#_Toc131248396)

[**AWS NETWORKING** 11](#_Toc131248397)

[**Amazon Virtual Private Cloud (Amazon VPC)** 11](#_Toc131248398)

[**AWS Direct Connect** 15](#_Toc131248399)

[**Domain Name System (DNS)** 17](#_Toc131248400)

[**Amazon Route 53** 17](#_Toc131248401)

[STORAGE 18](#_Toc131248402)

[**Amazon Elastic Block Store (Amazon EBS)** 18](#_Toc131248403)

[**Amazon Elastic File System (Amazon EFS)** 19](#_Toc131248404)

[**O Amazon Simple Storage Service (Amazon S3)** 20](#_Toc131248405)

[**Amazon Relational Database Service (Amazon RDS)** 21](#_Toc131248406)

[**Amazon Aurora** 22](#_Toc131248407)

[**Monitoramento** 24](#_Toc131248408)

[**AWS CloudTrail** 24](#_Toc131248409)

[**CloudTrail Insights.** 25](#_Toc131248410)

[**AWS Trusted Advisor** 25](#_Toc131248411)

[**Segurança** 26](#_Toc131248412)

[**Modelo de responsabilidade compartilhada** 26](#_Toc131248413)

[**AWS Organizations** 26](#_Toc131248414)

[**AWS Artifact** é um serviço que fornece acesso sob demanda a relatórios de segurança e conformidade da AWS e a contratos on-line selecionados. O AWS Artifact tem duas seções principais: AWS Artifact Agreements e o AWS Artifact Reports. 27](#_Toc131248415)

[**DDoS ou DDoS. Negação de serviço distribuída.** 28](#_Toc131248416)

[**AWS Key Management Service (AWS KMS)** 28](#_Toc131248417)

[**AWS WAF** 29](#_Toc131248418)

[Planos do AWS Support 30](#_Toc131248419)

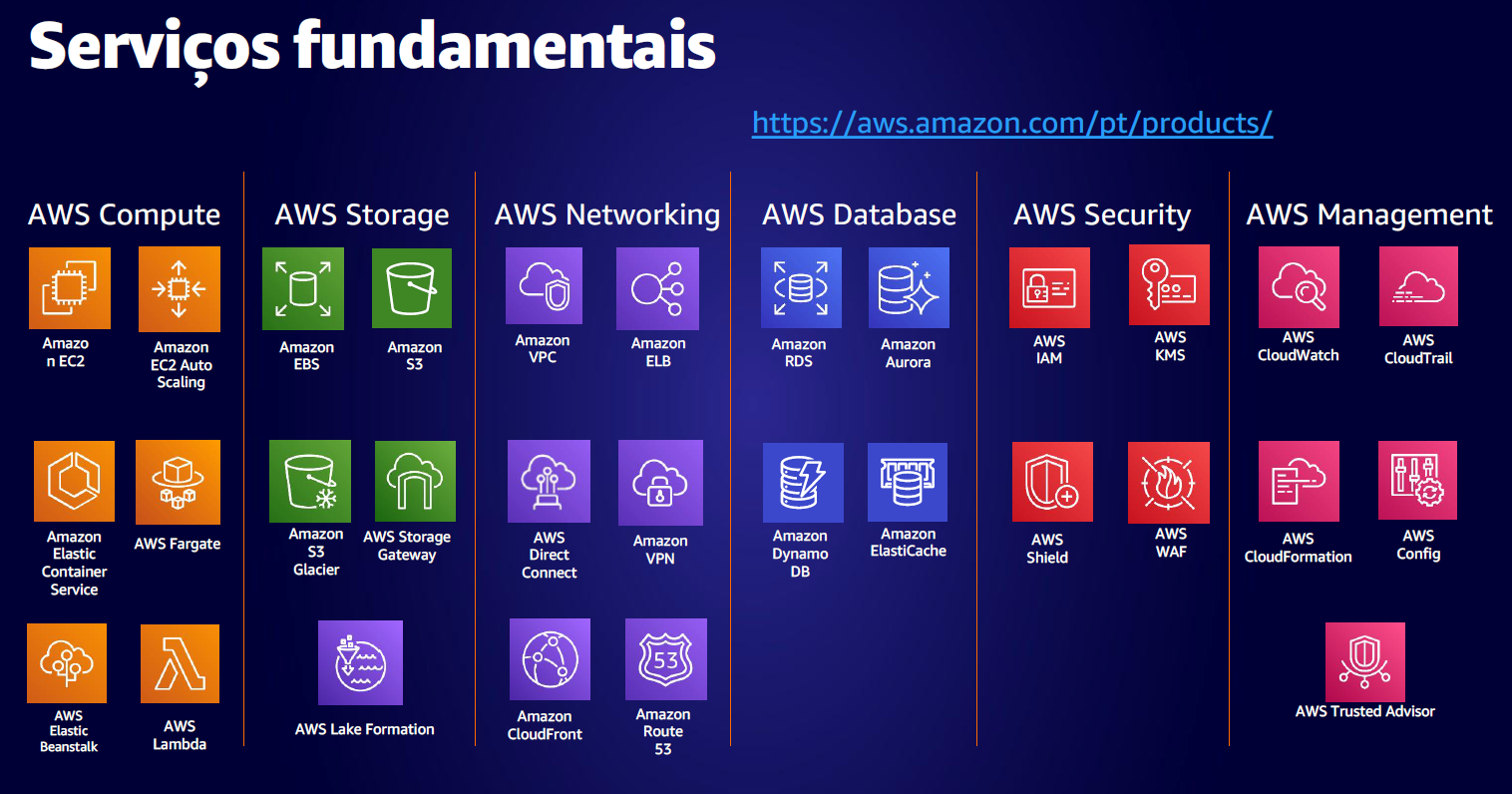
[**MIGRAÇÃO E INOVAÇÃO** 31](#_Toc131248420)

[**AWS Cloud Adoption Framework (AWS CAF)** 31](#_Toc131248421)

[**AWS Snow Family** 34](#_Toc131248422)

[**Recursos adicionais** 36](#_Toc131248423)

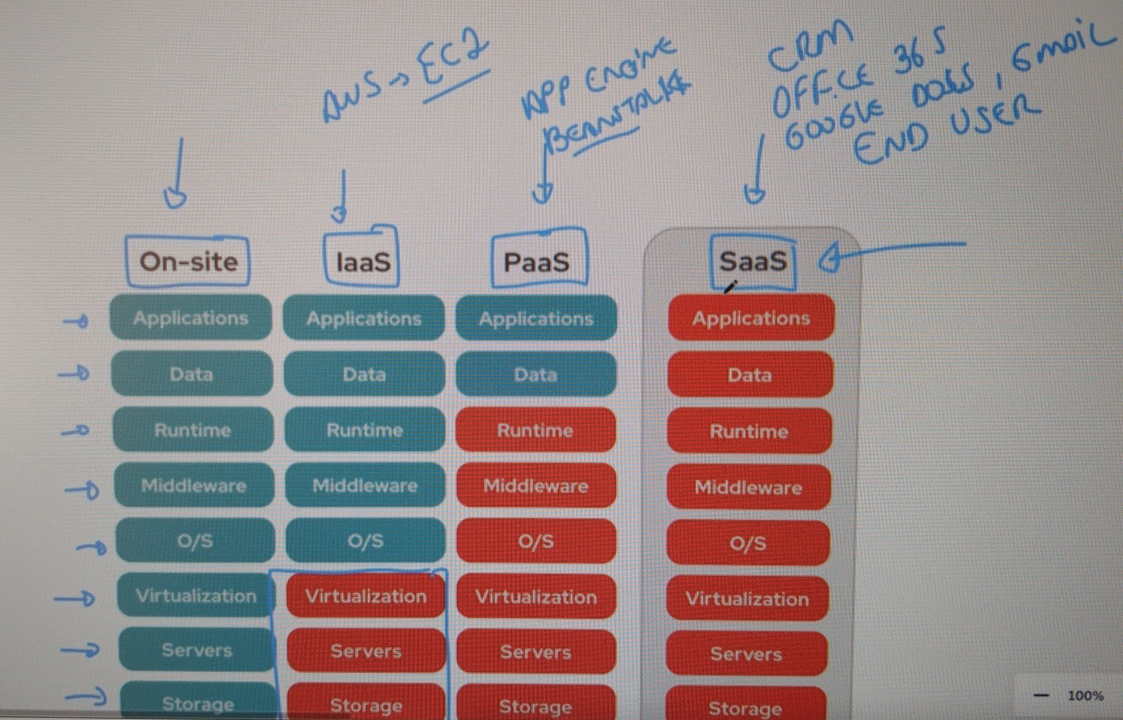
[**Recursos adicionais** 37](#_Toc131248424)



<https://aws.amazon.com/es/products/>

# **TIPO DE CLOUD**

Infraestrutura como um serviço (IaaS)  
Plataforma como um serviço (PaaS)  
Software como um serviço (SaaS)



# **AWS**

Os cinco pilares consistem nas seguintes áreas:

1. Segurança
2. Eficiência de performance
3. Confiabilidade
4. Excelência operacional
5. Otimização de custos

## **Região e Zona de disponibilidade**

Uma **Região** é uma área geográfica que contém recursos AWS

**Zonas de Disponibilidade** é um único data center ou grupo de data centers em uma Região.

O **AWS Outposts** é um serviço da AWS que roda dentro de empresas. AWS basicamente vai instalar e configurar uma mini-região totalmente operacional direto no datacenter do cliente. Toda responsabilidade e propriedade é da AWS. Ela que vai operar e administrar tudo, mas de forma isolada, dentro próprio prédio do cliente

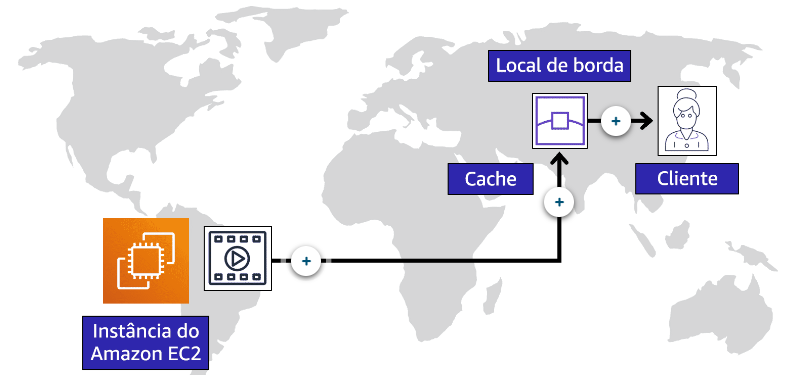
* 31 regiões lançadas cada uma com várias zonas de disponibilidade (AZs)
* 99 zonas de disponibilidade
* Mais de 410 pontos de presença Mais de 400 locais da borda e 13 caches da borda regionais

## **Amazon Cloudfront.**

Quando você armazena em cache uma cópia dos seus dados para ficar mais perto dos seus clientes em todo o mundo, você está usando o conceito de Redes de entrega de conteúdo, ou CDNs. na AWS, A nossa CDN se chama Amazon Cloudfront.

O Amazon Cloudfront é um serviço que ajuda a fornecer dados, vídeos, aplicações e APIs para os clientes em todo o mundo, com baixa latência e alta velocidade de transferência. O Amazon Cloudfront usa que nós chamamos de Edge Locations, pontos de presença espalhados pelo mundo para ajudar a acelerar a comunicação com os usuários, Não importa onde eles estejam.

O **local de borda** é o lugar onde o serviço Amazon Cloudfront está.



## **IAM (Identity and Access Managemen)**

IAM é o serviço responsável por monitorar identidades e acessos no sistema Componentes fundamentais em uma política do IAM:

* PRINCIPAL especifica QUEM recebe permissões
* AÇÃO especifica O QUÊ está sendo executado
* RECURSO especifica QUAIS propriedades estão sendo acessadas

**Função do IAM** é uma identidade que você pode assumir para obter acesso temporário a permissões. Quando alguém assume uma função do IAM, ele abandona todas as permissões que tinha em uma função anterior e assume as permissões da nova função. As funções do IAM são ideais para situações em que o acesso a serviços ou recursos precisa ser concedido temporariamente em vez de longo prazo

**usuário-raiz** da conta AWS é estabelecido quando se cria uma conta AWS pela primeira vez. Como prática recomendada, não use o usuário-raiz para tarefas cotidianas.

As **políticas de controle de serviço (SCPs)** permitem que você controle de forma centralizada as permissões para as contas em sua organização

# **AWS Compute**



## **1 Amazon EC2**

O Amazon Elastic Compute Cloud (Amazon EC2) é um serviço Web que disponibiliza capacidade computacional segura e redimensionável na nuvem. O EC2 oferece muitas opções que permitem criar e executar virtualmente qualquer aplicativo.

* as instâncias EC2 são flexíveis confiáveis e escaláveis
* O Amazon EC2 requer que você configure e gerencie sua frota de instâncias. Você é responsável por aplicar os testes de suas instâncias quando novos pacotes de software forem lançados
* É responsável também por configurar a escalabilidade dessas instâncias arquitetando as suas soluções para serem hospedadas de uma maneira altamente disponível

Com os serviços **Serverless** vc não consegue ver e nem acessar as infraestruturas subjacente. ( **lambda** é serverles)

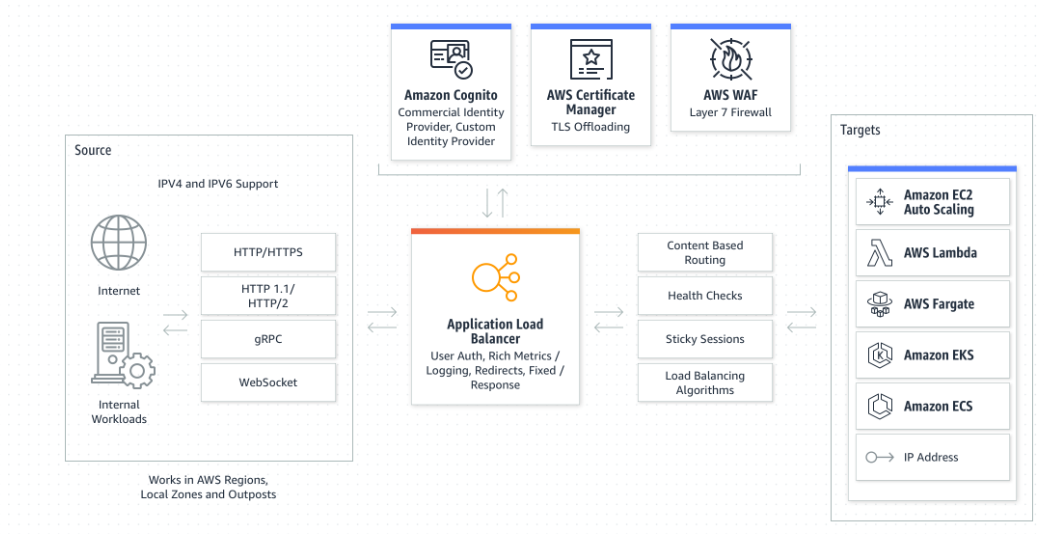
## **2 Amazon EC2 auto scaling**

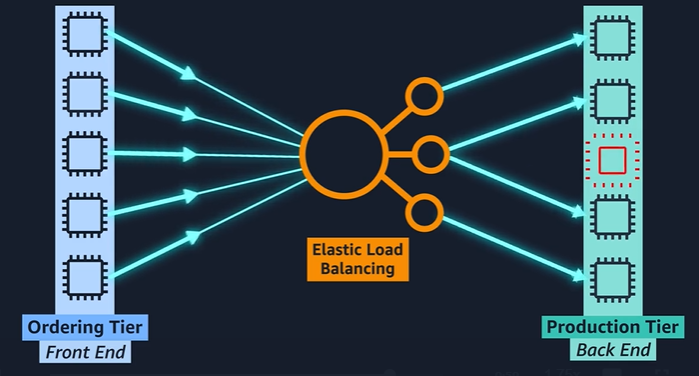
O Amazon EC2 Auto Scaling permite que você adicione ou remova automaticamente instâncias do Amazon EC2 em resposta à alteração da demanda do aplicativo. Ao fazer auto scaling de suas instâncias, aumentando ou reduzindo conforme a necessidade, você consegue manter uma sensação maior de disponibilidade de aplicativos.  
  
No Amazon EC2 Auto Scaling, há duas abordagens disponíveis: scaling dinâmico e scaling preditivo.

* O *scaling dinâmico* responde às alterações na demanda.
* O *scaling preditivo*programa automaticamente o número correto de instância do Amazon EC2 com base na demanda prevista.

## **3 Amazon Elastic load balancing**

O Elastic Load Balancing é o serviço AWS que distribui automaticamente o tráfego de entrada de aplicativos entre vários recursos, como instâncias do Amazon EC2. Isso ajuda a garantir que nenhum recurso único seja usado em excesso.





## **4 Amazon Elasitic contanainer service (ECS)**

O Amazon ECS é um serviço de orquestração de contêineres totalmente gerenciado que facilita a implantação, o gerenciamento e a escala de aplicações em contêineres.



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

O Amazon EKS é um serviço totalmente gerenciado do Kubernetes. O Kubernetes é um software de código aberto que permite implantar e gerenciar aplicativos em contêineres em grande escala.

## **6 Amazon Elasitic Beanstalk**

O AWS Elastic Beanstalk é um serviço que ajuda você a provisionar ambientes baseados no Amazon EC2. Em vez de clicar pela console ou escrever vários comandos para criar sua rede, instâncias EC2, escalabilidade e os load balances, você vai fornecer o seu código da aplicação com as configurações desejadas no Beanstalk e, em seguida, ele cria o seu ambiente e faz o seu deploy. O Elastic Beanstalk também permite salvar as configurações do ambiente para que elas possam ser implantadas novamente. O AWS Elastic Beanstalk fornece a conveniência de não ter que provisionar e gerenciar todos esses componentes separadamente e ainda te provê a visibilidade e o controle dos recursos que compõem o seu ambiente. Você irá focar, então, na sua aplicação e não na infraestrutura.

Com o **AWS Elastic Beanstalk,** você fornece definições de código e configuração, e o Elastic Beanstalk implanta os recursos necessários para executar as seguintes tarefas:

* Ajustar capacidade
* Balancear carga
* Dimensionar de forma automática
* Monitorar a integridade do aplicativo

## **7 AWS CloudFormation**

O AWS CloudFormation é uma ferramenta que trata a infraestrutura como código, permitindo que você defina uma ampla variedade de recursos da AWS usando JSON ou Yaml, chamados de Templates do CloudFormation. Um formato declarativo como esse permite definir o que você deseja criar sem especificar o passo a passo exatamente de como fazer essa criação. Portanto, o CloudFormation te permite definir o que você deseja e o mecanismo dele vai se preocupar com os detalhes sobre como chamar as APIs para fazer essa criação.  
  
Também não é limitado apenas para soluções básicas que contemplem instâncias EC2. O CloudFormation é compatível com diversos recursos diferentes da AWS, como armazenamento, banco de dados, machine learning e muito mais. Depois de definir os seus recursos em um template do CloudFormation, o serviço vai analisar o template e começar a provisionar todos os recursos que você definiu em paralelo. O CloudFormation gerencia todas as chamadas de API para o back end da AWS para você. Você pode executar o mesmo template do CloudFormation em várias contas ou em várias regiões e ele criará ambientes idênticos em todos eles. Há menos espaço para erro humano uma vez que é um processo totalmente automatizado.

## **8 AWS Fargate**

O AWS Fargate é um mecanismo de computação sem servidor para contêineres.

## **9 AWS Lambda**

é um serviço que permite executar código sem provisionar ou gerenciar servidores.

O Lambda é um serviço que permite que você faça o upload do seu código no que chamamos de função lambda, configure um trigger, ou seja, um evento que vai iniciar a execução da sua função Lambda e o serviço vai aguardar o trigger. Quando o Trigger é detectado, o código é automaticamente executado em um ambiente gerenciado

O Lambda foi projetado para executar um código em até 15 minutos, então, não foi criado para o processamento de longa execução, como o Deep learning, por exemplo.

## **Outros serviços**

* O Amazon Simple Queue Service (Amazon SQS) é um serviço que permite enviar, armazenar e receber mensagens entre componentes de software por uma fila.
* O Amazon Simple Notification Service (Amazon SNS) é um serviço de publicação/assinatura. Usando tópicos do Amazon SNS, um editor publica mensagens para assinantes.

## **Qual serviço usar**

Se você ainda não está pronto para trabalhar de forma serverless ou precisa acessar e gerenciar o seu ambiente mas ainda assim quer eficiência e portabilidade deve olhar para serviços de contêiner, como, por exemplo, o Amazon Elastic Container Service, também conhecido como ECS, ou o Amazon Elastic Kubernetes Service, também conhecido como EKS.  
  
Ambos os serviços são ferramentas de orquestração de container

**Se você estiver tentando hospedar suas aplicações tradicionais e desejar sucesso total o sistema operacional como Linux ou Windows, você vai optar por instâncias EC2.**

**Se você deseja trabalhar com processamento de curta duração, orientados a eventos e serviços ou aplicações e não deseja gerenciar o seu ambiente, cheque a AWS Lambda.**

**Se você deseja executar workloads baseados em containers Docker na AWS, primeiro precisa escolher a sua ferramenta de orquestração. O que você prefere: o ECS ou o EKS? Depois de escolher a sua ferramenta, você precisa escolher a sua plataforma. Você prefere executar seus containers em instâncias do EC2 que você gerencia ou utilizando o Fargate que é gerenciado pra você?**

Escalabilidade

Você pode redimensionar as instâncias EC2 verticalmente, aumentando o tamanho da instância, ou horizontalmente, adicionando novas instâncias no grupo. Você pode configurar a escalabilidade horizontal automatizada utilizando o Amazon EC2 Auto Scaling.  
  
**Depois de redimensionar as suas instâncias EC2 horizontalmente, Você precisa de algo para distribuir o tráfego de entrada entre todas as instâncias. E é ai que entra o Elastic Load Balancing. As instâncias EC2 têm diferentes modelos de preços: há o sob demanda, que é on demand, que é mais flexível e não tem um compromisso. Tem um Modelo spot, que permite a utilização da capacidade computacional que não está sendo utilizada no momento por um valor inferior ao on demand. Saving plans em instâncias reservadas, que permitem que você obtenha um desconto ao se comprometer a um determinado nível de uso, e Compute Savings plans que se aplicam ao AWS Lambda, Fargate, bem como às instâncias EC2.**

**ambém abordamos os serviços de mensageria, o Amazon Simple Queue Service, ou SQS. Esse serviço permite deaacoplar componentes do seu sistema. As mensagens permanecem na fila até que sejam consumidas ou excluídas. Vimos também o Amazon Simple Notification Service, ou SMS, que e é usado para enviar mensagens para assinantes de e-mails, mensagens de texto, notificações push ou até mesmo endpoints HTTP e HTTPS. Depois que uma mensagem é publicada em um tópico, ela é enviada para todos esses assinantes.**

Os **armazenamentos de instâncias** são ideais para dados temporários que não precisam ser mantidos a longo prazo

Quando uma instância do Amazon EC2 é interrompida ou encerrada, todos os dados que foram gravados no armazenamento de instâncias anexado são excluídos.

# **AWS NETWORKING**

## **Amazon Virtual Private Cloud (Amazon VPC)**

 VPC, Virtual Private Cloud, é o serviço que você utiliza para criar a sua própria rede privada na AWS. A VPC permite que você defina o seu intervalo de preços privados para fazer a alocação de recursos, como instâncias EC2 e Load Balancing dentro da sua rede.

Mas você não pode simplesmente jogar os seus recursos em uma VPC e seguir em frente. Você precisa colocá los em sub-redes. Cada sub-rede possui uma porção dos endereços de IP da sua VPC e permite que você faça o deploy de diversos recursos. Sub-redes, juntamente com as regras de redes, que abordaremos mais tarde, controlam se os recursos estarão disponíveis de forma pública ou privada

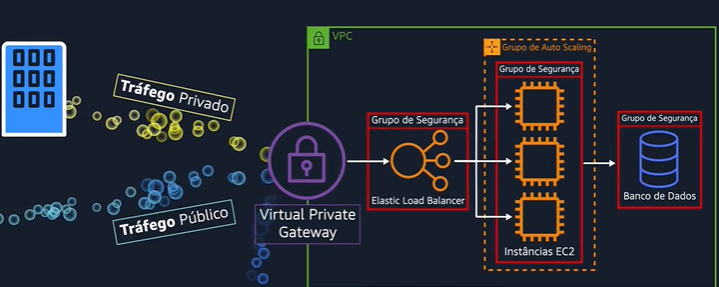
Existem cenários onde você pode ter recursos que deseja que sejam acessíveis apenas se alguém estiver conectado à sua rede privada. Por exemplo, aplicações internas como uma aplicação de RH ou um banco de dados.

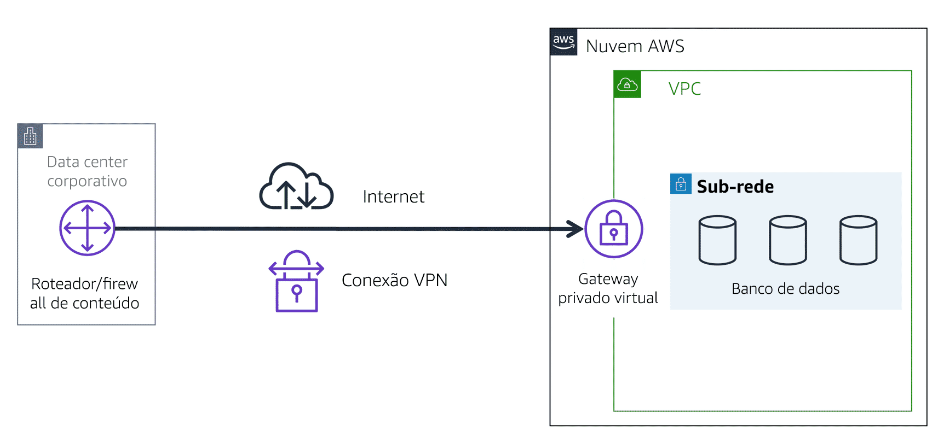
**Publico**: Para permitir a comunicação de tráfego que vem da internet para sua VPC, você deve associar um recurso que chamamos de internet Gateway, ou GW, a sua VPC

Um internet gateway é como se fosse uma porta aberta para o público.



**privados internos:** Não queremos que qualquer um, de qualquer lugar, seja capaz de alcançar esses recursos. Então, nós não queremos o Internet Gateway conectado à nossa VPC. Em vez disso, queremos um gateway privado, que vai permitir somente a entrada de pessoas que estiverem vindo de uma rede privada, não da Internet pública. Esse Gateway privado é chamado de Virtual Private Gateway, que é um recurso que permite que você crie uma conexão VPN entre uma rede privada que pode ser, por exemplo, seu data center ou uma rede corporativa interna com sua VPC.



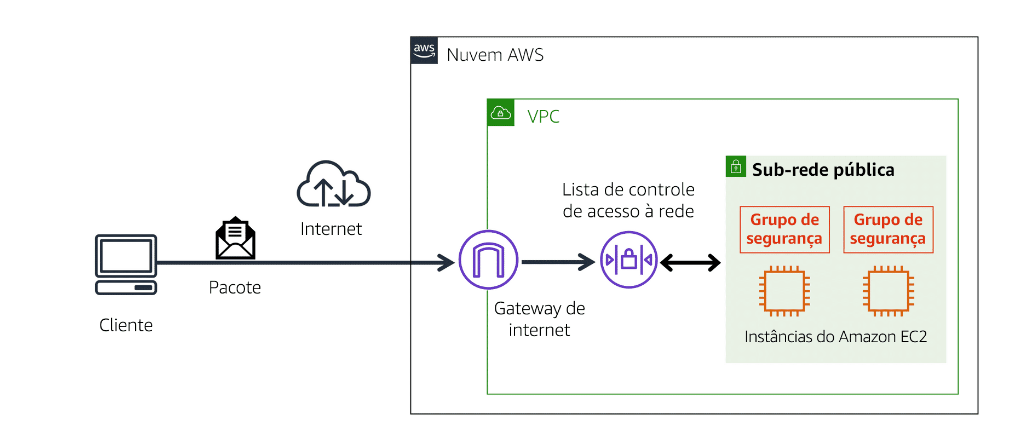


O AWS Direct Connect fornece uma linha física que conecta sua rede do datacenter à sua VPC. Isso pode ajudar você a atender às necessidades regulamentares e de conformidade bem como contornar potenciais problemas de largura de banda.

A AWS tem uma ampla variedade de serviços que cobre cada uma das camadas de segurança. Proteção de rede, segurança de aplicações identidades de usuário, autorização, autenticação, proteção contra ataques de negação de serviço distribuído, ou DDoS, integridade dos dados criptografia e muito mais.

**O principal motivo para usar subnets em uma VPC é controlar o acesso aos gateways**

**Pacotes** são mensagens na internet e cada pacote que cruza os limites de uma subnet é verificado por um recurso chamado de **Lista de controle de acesso à rede**, ou **network ACL.**



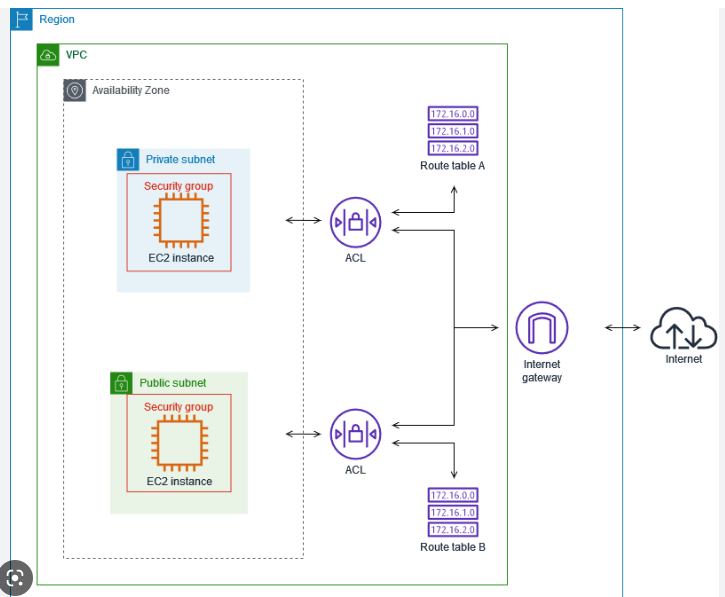
 E essa verificação é necessária para validar se o pacote tem permissões para sair ou entrar na subnet com base em quem enviou e como ele está tentando se comunicar. As network ACLs verificam o fluxo de dados que entram e saem de uma subnet. Da mesma forma que o controle de passaportes. O fluxo de dados que foi aprovado pode passar até o seu destino e o fluxo de dados potencialmente prejudicial, como tentativas de obter o controle de um sistema através das requisições na central de administração, são bloqueados antes de chegarem no alvo. Você não pode hackear o que não pode alcançar.

A network ACL somente pode controlar se um pacote cruza o limite de uma subnet tentando entrar ou sair. Ela não avalia se o pacote pode ir até uma instância EC2 específica ou não. Às vezes, você vai ter várias instâncias EC2 na mesma subnet mas pode precisar de regras diferentes relacionadas a quem pode enviar os pacotes para qual porta esses pacotes podem ser enviados. Então, você precisa de uma segurança de rede no nível da instância também.

Para resolver questões de acesso no nível da instância, podemos adicionar aqui os grupos de segurança.

**o grupo de segurança é Stateful**, o que quer dizer que ele tem uma espécie de memória quando se trata de permitir a entrada ou saída. Se um pacote for verificado uma vez, na próxima vez não será verificado

**o network ACL é Stateless,** ou seja, ele não se lembra de nada e verifica cada pacote que cruza sua fronteira, independentemente da situação.



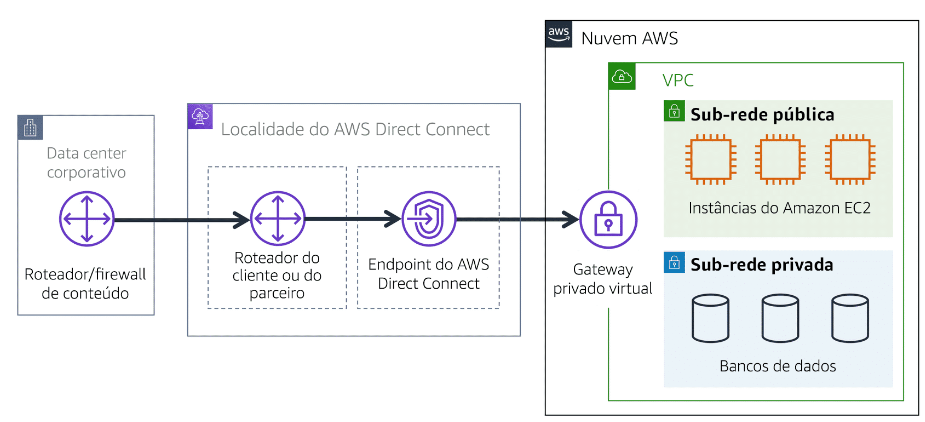
As ACLs de rede (listas de controle de acesso de rede) fazem a filtragem de pacotes stateless . Elas não se lembram de nada e verificam os pacotes que atravessam a fronteira da sub-rede em todos os sentidos: entrada e saída.  
  
Cada conta AWS tem uma ACL de rede comum. Ao configurar a VPC, você pode usar a ACL de rede comum da conta ou criar ACLs de rede personalizadas.  
  
Por padrão, a ACL de rede comum da conta permite todo o tráfego de entrada e saída, mas você pode modificá-la adicionando suas próprias regras. Para ACLs de rede personalizadas, todo o tráfego de entrada e saída é negado até que você adicione regras para especificar qual tráfego deve ser permitido. Além disso, todas as ACLs de rede têm uma regra de negação explícita. Essa regra garante que, se um pacote não corresponder a nenhuma das outras regras na lista, ele será negado.

## [**AWS Direct Connect**](https://aws.amazon.com/directconnect/)

é um serviço que permite estabelecer uma conexão privada dedicada entre seu data center e uma VPC.

Suponha que haja um prédio com um corredor que liga o prédio diretamente à cafeteria. Somente os moradores do prédio podem passar por esse corredor.  
Esse corredor privado fornece o mesmo tipo de conexão dedicada que o AWS Direct Connect. Os moradores conseguem entrar na cafeteria sem precisarem usar a estrada pública compartilhada com outros clientes.

A conexão privada que o AWS Direct Connect fornece ajuda você a reduzir os custos de rede e a aumentar a quantidade de largura de banda que pode trafegar pela sua rede.



Sub-rede privada : Isola bancos de dados contendo informações pessoais dos clientes.

Sub-rede pública : É compatível com o site voltado para o cliente.

Gateway privado virtual: Cria uma conexão VPN entre a VPC e a rede corporativa interna.

AWS Direct Connect: Estabelece uma conexão dedicada entre o data center local e a VPC.

1 - Exercicio  
Sua empresa tem um aplicativo que usa instâncias do Amazon EC2 para executar o site voltado para o cliente e instâncias de banco de dados do Amazon RDS para armazenar informações pessoais dos clientes. Como o desenvolvedor deve configurar a VPC de acordo com as práticas recomendadas?

Resposta:   
Colocar as instâncias do Amazon EC2 em uma sub-rede pública e as instâncias de bancos de dados do Amazon RDS em uma sub-rede privada.

Uma **sub-rede** é uma seção de uma VPC na qual você pode agrupar recursos com base em necessidades operacionais ou de segurança. As sub-redes podem ser públicas ou privadas.  
  
As sub-redes públicas têm recursos que precisam ser acessíveis pelo público, como o site de uma loja on-line.  
  
As sub-redes privadas têm recursos que devem ser acessíveis apenas pela sua rede privada, como um banco de dados contendo informações pessoais dos clientes e históricos de pedidos.

2-

Qual declaração descreve melhor a lista de controle de **acesso de rede comum de uma conta AWS**?

a) Ela é stateless e nega todo o tráfego de entrada e saída.

b) Ela é stateful e permite todo o tráfego de entrada e saída.

c) Ela é stateless e permite todo o tráfego de entrada e saída.

d) Ela é stateful e nega todo o tráfego de entrada e saída.

As ACLs de rede (listas de controle de acesso de rede) fazem a filtragem de pacotes **stateless**. Elas não se lembram de nada e verificam os pacotes que atravessam a fronteira da sub-rede em todos os sentidos: entrada e saída.  
  
Cada conta AWS tem uma ACL de rede comum. Ao configurar a VPC, você pode usar a ACL de rede comum da conta ou criar ACLs de rede personalizadas.  
  
Por padrão, a ACL de rede comum da conta permite todo o tráfego de entrada e saída, mas você pode modificá-la adicionando suas próprias regras. Para ACLs de rede personalizadas, todo o tráfego de entrada e saída é negado até que você adicione regras para especificar qual tráfego deve ser permitido. Além disso, todas as ACLs de rede têm uma regra de negação explícita. Essa regra garante que, se um pacote não corresponder a nenhuma das outras regras na lista, ele será negado.

Qual declaração descreve melhor os grupos de segurança?

1. Eles são stateful e negam todo o tráfego de entrada por padrão.
2. Eles são stateful e permitem todo o tráfego de entrada por padrão.
3. Eles são stateless e negam todo o tráfego de entrada por padrão.
4. Eles são stateless e permitem todo o tráfego de entrada por padrão.

Grupos de segurança são stateful. Isso significa que eles usam padrões e fluxos de tráfego anteriores ao avaliar novas solicitações para uma instância.  
  
Por padrão, os grupos de segurança negam todo o tráfego de entrada, mas você pode adicionar regras personalizadas para atender às suas necessidades operacionais e de segurança.

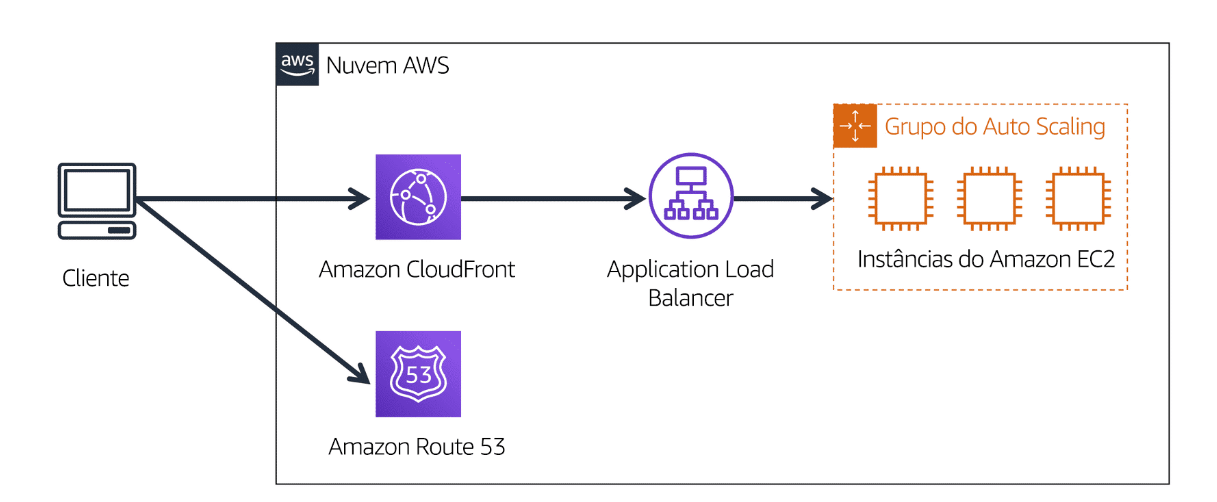
* O Amazon Virtual Private Cloud (Amazon VPC) é um serviço que permite provisionar uma seção isolada da nuvem AWS. Nesta seção isolada, é possível iniciar recursos em uma rede virtual definida por você.
* O AWS Direct Connect é um serviço que permite estabelecer uma conexão privada dedicada entre o seu data center e a VPC.
* O Amazon CloudFront é um serviço de entrega de conteúdo. Ele usa uma rede de locais de borda para armazenar conteúdo em cache e entregar conteúdo para clientes em todo o mundo.

## **Domain Name System (DNS)**

traduz nomes de sites para endereços IP (Internet Protocol). Os servidores DNS (Domain Name System, ou Sistema de Nomes de Domínios) são os responsáveis por localizar e traduzir para números [IP (Internet Protocol)](https://canaltech.com.br/software/o-que-e-ip/) os endereços dos sites que digitamos nos navegadores

## [**Amazon Route 53**](https://aws.amazon.com/route53)

é um serviço web de DNS. Oferece aos desenvolvedores e empresas uma maneira confiável de rotear os usuários finais para aplicativos da internet hospedados na AWS



# STORAGE



# **[Amazon Elastic Block Store (Amazon EBS)](https://aws.amazon.com/ebs" \t "_blank)**

é um serviço que fornece volumes de armazenamento a nível de bloco que você pode usar com instâncias do Amazon EC2. Se você interromper ou encerrar uma instância do Amazon EC2, todos os dados no volume do EBS anexo permanecerão disponíveis.

Para criar um volume do EBS, defina a configuração (como tamanho e tipo do volume) e a provisão. Depois de criar um volume do EBS, ele pode ser anexado a uma instância do Amazon EC2.

Como os volumes do EBS são para dados que precisam perdurar, é importante fazer backup dos dados. Você pode fazer backups complementares de volumes do EBS criando snapshots do Amazon EBS.

Um [**snapshot do EBS**](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html) é um backup incremental. Isso significa que o primeiro backup de um volume copia todos os dados. Nos backups subsequentes, somente os blocos de dados que foram alterados desde o snapshot mais recente são salvos.

Os backups complementares são diferentes dos backups completos, nos quais todos os dados em um volume de armazenamento são copiados cada vez que ocorre um backup. O backup completo inclui dados que não foram alterados desde o backup mais recente.

Os volumes de armazenamento a nível de bloco se comportam como discos rígidos físicos.   
Um armazenamento de instância é o armazenamento em disco fisicamente anexo ao computador host para uma instância do EC2 e, portanto, tem a mesma vida útil da instância. Quando a instância é encerrada, todos os dados no armazenamento de instâncias são perdidos.

Portanto, a AWS recomenda armazenamentos de instâncias para casos de uso que envolvam dados temporários que você não precisa a longo prazo.

# [**Amazon Elastic File System (Amazon EFS)**](https://aws.amazon.com/efs/)

é um sistema de arquivos **automaticamente** **escalável** usado com os serviços de nuvem AWS e recursos locais. À medida que você adiciona e remove arquivos, o Amazon EFS expande e retrai automaticamente. Ele pode dimensionar sob demanda para petabytes sem interromper os aplicativos.

|  |  |
| --- | --- |
| **EBS** | **EFS** |
| Um volume do Amazon EBS armazena dados em uma **única** Zona de Disponibilidade.   Para anexar uma instância do Amazon EC2 a um volume do EBS, tanto a instância do Amazon EC2 quanto o volume do EBS devem residir na mesma Zona de Disponibilidade. | O Amazon EFS é um serviço regional. Ele armazena dados em **várias** Zonas de Disponibilidade e entre elas.   O armazenamento duplicado permite que você acesse dados simultaneamente de todas as Zonas de Disponibilidade na Região em que um sistema de arquivos está localizado. Além disso, os servidores locais podem acessar o Amazon EFS usando o AWS Direct Connect. |

# [**O Amazon Simple Storage Service (Amazon S3)**](https://aws.amazon.com/s3/)

é um serviço que fornece armazenamento a nível do objeto. O Amazon S3 armazena dados como objetos em buckets.

 S3 Standard e vem com 11 noves de durabilidade. Isso significa que um objeto armazenado no S3 tem uma porcentagem de 99,99999999%

**S3 Standard**

* Projetado para dados acessados com frequência
* Armazena dados em um mínimo de três Zonas de Disponibilidade

O S3 Standard fornece alta disponibilidade para objetos. Isso o torna uma boa escolha para diversos casos de uso, como sites, distribuição de conteúdo e análise de dados. O S3 Standard tem um custo mais alto do que outras categorias de armazenamento para dados acessados com pouca frequência e armazenamento de arquivamento.

**S3 Standard-Infrequent Access (S3 Standard-IA)**

* Ideal para dados com pouca frequência de acesso
* Semelhante ao S3 Standard, mas com um preço de armazenamento mais baixo e um preço de recuperação mais alto

O S3 Standard-IA é ideal para dados acessados com pouca frequência, mas que precisam ter alta disponibilidade para quando necessário.

O S3 Standard e o S3 Standard – IA armazenam dados em um mínimo de três Zonas de Disponibilidade. O S3 Standard – IA fornece o mesmo nível de disponibilidade do S3 Standard, mas com um preço de armazenamento mais baixo e um preço de recuperação mais alto.

Perfeito para armazenar backups, arquivos de recuperação de desastres ou qualquer objeto que exija armazenamento a longo prazo.

**S3 One Zone-Infrequent Access (S3 One Zone – IA)**

* Armazena dados em uma única Zona de Disponibilidade
* Tem um preço de armazenamento menor do que o S3 Standard – IA

Comparado com o S3 Standard e o S3 Standard – IA, que armazenam dados em um mínimo de três Zonas de Disponibilidade, o S3 One Zone – IA armazena em uma única Zona de Disponibilidade. Isso o torna uma boa categoria de armazenamento nas seguintes condições:

* Você quer economizar custos com armazenamento.
* Você pode reproduzir facilmente seus dados em caso de falha na Zona de Disponibilidade.

**S3 Intelligent-Tiering**

* Ideal para dados com padrões de acesso desconhecidos ou em alteração
* Requer uma pequena taxa mensal de monitoramento e automação por objeto

Na categoria de armazenamento S3 Intelligent-Tiering, o Amazon S3 monitora os padrões de acesso dos objetos. Se você não acessou um objeto por 30 dias consecutivos, o Amazon S3 o move automaticamente para o nível de acesso pouco frequente S3 Standard – IA. Se você acessar um objeto no nível de acesso pouco frequente, o Amazon S3 o move automaticamente para o nível de acesso frequente S3 Standard.

**S3 Glacier**

* Armazenamento de baixo custo projetado para arquivamento de dados
* Capaz de recuperar objetos em **poucos minutos a horas**

O S3 Glacier é uma categoria de armazenamento de baixo custo, ideal para o arquivamento de dados. Por exemplo, você pode usar essa categoria para armazenar registros de clientes arquivados ou arquivos de fotos e vídeos mais antigos.

Ideal para arquivos que não precisamos que eles sejam recuperados muito rapidamente

**S3 Glacier Deep Archive**

* Categoria de armazenamento de objetos com menor custo, ideal para arquivamento
* Capaz de recuperar objetos em **12 horas**

Ao decidir entre o Amazon S3 Glacier e o Amazon S3 Glacier Deep Archive, considere a prontidão com que você precisa recuperar objetos arquivados. É possível recuperar objetos armazenados na categoria de armazenamento S3 Glacier de alguns minutos a algumas horas. Em comparação, é possível recuperar objetos armazenados na categoria de armazenamento S3 Glacier Deep Archive em até 12 horas.

# **Amazon Relational Database Service (Amazon RDS)**

 é um serviço que permite executar bancos de dados relacionais na nuvem AWS.  
  
O Amazon RDS é um serviço **gerenciado que automatiza tarefas como provisionamento de hardware, configuração de banco de dados, patch e backups**.

O Amazon RDS fornece inúmeras opções de segurança diferentes. Muitos mecanismos de banco de dados do Amazon RDS oferecem criptografia em repouso (protegendo os dados enquanto estão armazenados) e criptografia em trânsito (protegendo os dados enquanto estão sendo enviados e recebidos).

O Amazon RDS está disponível em seis mecanismos de banco de dados, que otimizam memória, desempenho ou entrada/saída (E/S). Os mecanismos de banco de dados compatíveis são:

* Amazon Aurora
* PostgreSQL
* MySQL
* MariaDB
* Oracle Database
* Microsoft SQL Server

Ao armazenar dados em um banco de dados do Amazon Aurora.

# [**Amazon Aurora**](https://aws.amazon.com/rds/aurora/)

é um banco de dados relacional de nível empresarial. É compatível com os bancos de dados relacionais MySQL e PostgreSQL. É até cinco vezes mais rápido do que os bancos de dados MySQL comuns e até três vezes mais rápido do que os bancos de dados PostgreSQL comuns.

O Amazon Aurora ajuda a reduzir os custos do banco de dados reduzindo operações desnecessárias de entrada/saída (E/S), garantindo que os recursos do banco de dados permaneçam confiáveis e disponíveis.

Considere o Amazon Aurora se suas cargas de trabalho exigem alta disponibilidade. Ele replica seis cópias de seus dados em três Zonas de Disponibilidade e faz backup contínuo de seus dados para o Amazon S3.

Ela vem em duas formas: MySQL e PostgreSQL. E seu preço é 1/10 do custo de banco de dados de nível comercial. É um banco de dados bastante econômico. Outros benefícios são coisas como seus dados serem replicados entre instalações. Então você tem seis cópias a qualquer momento. É possível implantar até 15 réplicas de leitura para que você possa descarregar as suas leituras e dimensionar a performance.

[**Amazon DynamoDB**](https://aws.amazon.com/dynamodb/)

é um serviço de banco de dados **de chave-valor (NoSQL)** **e serveless** Ele oferece um desempenho de um dígito de milissegundo em qualquer scaling.

é totalmente gerenciado e altamente escalável.

 o DynamoDB é um banco de dados NoSQL, num modelo não relacional. Ele é um banco de propósito específico, com tempo de resposta de milissegundos, é totalmente gerenciado e altamente escalável.

À medida que o tamanho do banco de dados expande ou retrai, o DynamoDB é dimensionado automaticamente para ajustar as alterações na capacidade e, ao mesmo tempo, manter o desempenho consistente.

O DynamoDB é:

* **sem servidor**: o que significa que você não precisa provisionar, aplicar patches ou gerenciar servidores. Você também não precisa instalar, manter ou operar o software.
* **Auto scaling**: À medida que o tamanho do banco de dados expande ou retrai, o DynamoDB é dimensionado automaticamente para ajustar as alterações na capacidade e, ao mesmo tempo, manter o desempenho consistente.  Isso o torna uma escolha adequada para casos de uso que exigem alto desempenho durante o scaling.
* Amazon Relational Database Service (Amazon RDS) e Amazon Aurora usam linguagem de consulta estruturada (SQL) para armazenar e consultar dados. Eles não são bancos de dados de chave-valor.
* O Amazon DocumentDB é um serviço de banco de dados de documentos compatível com cargas de trabalho do MongoDB.

[**Amazon Redshift**](https://aws.amazon.com/redshift)

é serviço de data warehouse que você pode usar para análise de big data. Ele oferece a capacidade de coletar dados de muitas fontes além de ajudar a entender relações e tendências em todos os seus dados.

[**AWS Database Migration Service (AWS DMS)**](https://aws.amazon.com/dms/)

Permite migrar bancos de dados relacionais e não relacionais e outros tipos de armazenamentos de dados

**Migrações homogêneas** (bancos de dados que são do mesmo tipo): exemplo: do  MySQL para o Amazon RDS for MySQL, do Microsoft SQL Server para o Amazon RDS for SQL Server ou até mesmo do Oracle para o Amazon RDS para Oracle

**heterogêneas :** origem e de destino são de diferentes tipos. Duas etapas: converter usando o AWS Schema Conversion Tools depois  usar o DNS para migrar os dados do banco de dados de origem para o banco de dados de destino.

**Outros usos**: incluem migrações de banco de dados de desenvolvimento e teste, consolidação de banco de dados e até mesmo a replicação contínua de banco de dados.

**Outros serviços de banco de dados**

* [**Amazon DocumentDB**](https://aws.amazon.com/documentdb) é um serviço de banco de dados de documentos compatível com cargas de trabalho do MongoDB. (MongoDB é um programa de banco de dados de documentos.).  falamos sobre o DynamoDB e ele é ótimo para bancos de dados chave-valor. Mas se você precisar ir além de apenas armazenar pequenos atributos e se você precisar de um sistema completo de gerenciamento de conteúdo, é aí que entra o Amazon DocumentDB, ideal para gerenciamento de conteúdo, catálogos, perfis de usuário.
* [**Amazon Neptune**](https://aws.amazon.com/neptune) é um serviço de banco de dados de grafo.  
  Você pode usar o Amazon Neptune para criar e executar aplicativos que funcionam com conjuntos de dados altamente conectados, como mecanismos **de recomendação, redes sociais, detecção de fraudes e gráficos de conhecimento.**
* [**Amazon Quantum Ledger Database (Amazon QLDB)**](https://aws.amazon.com/qldb) é um serviço de banco de dados ledger. Você pode usar o Amazon QLDB para revisar um histórico completo de todas as alterações feitas nos dados do aplicativo. um sistema imutável de registros onde nenhum dado inserido pode ser removido das auditorias.
* O [**Amazon Managed Blockchain**](https://aws.amazon.com/managed-blockchain) é um serviço para criar e gerenciar redes de blockchain com estruturas de código aberto.   
  O Blockchain é um sistema de registro distribuído que permite que várias partes executem transações e compartilhem dados sem uma autoridade central.
* O [**Amazon ElastiCache**](https://aws.amazon.com/elasticache) é um serviço que adiciona camadas de cache sobre seus bancos de dados para ajudar a melhorar os tempos de leitura de solicitações comuns.  
  Ele é compatível com dois tipos de armazenamentos de dados: Redis e Memcached.
* [**Amazon DynamoDB Accelerator (DAX)**](https://aws.amazon.com/dynamodb/dax/) é um cache em memória para o DynamoDB. Ele ajuda a melhorar os tempos de resposta de milissegundos para microssegundos.

<https://explore.skillbuilder.aws/pages/59/subscriptions?trk=e6d86b22-90b3-487c-bac9-3603075dbf69&sc_channel=el>

<https://aws.amazon.com/pt/training/digital/aws-builder-labs/?dt=sec&sec=isf>

# **Monitoramento**

## [**AWS CloudTrail**](https://aws.amazon.com/cloudtrail/)

* O [AWS CloudTrail](https://aws.amazon.com/cloudtrail/) registra as chamadas de API realizadas na sua conta.  Faz a auditoria, grava as log.



os eventos são atualizados no CloudTrail dentro de 15 minutos após uma chamada de API.

## [**CloudTrail Insights**](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-insights-events-with-cloudtrail.html)**.**

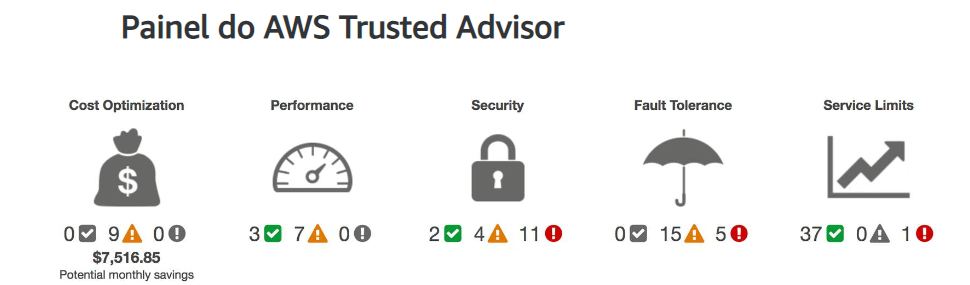
No CloudTrail, você também pode ativar o [CloudTrail Insights](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-insights-events-with-cloudtrail.html" \t "_blank). Esse recurso opcional permite que o CloudTrail detecte automaticamente atividades de API incomuns em sua conta AWS.

## [**AWS Trusted Advisor**](https://aws.amazon.com/premiumsupport/technology/trusted-advisor/)

É um serviço web que inspeciona seu ambiente AWS e faz recomendações em tempo real de acordo com as práticas recomendadas da AWS.

 cinco categorias:

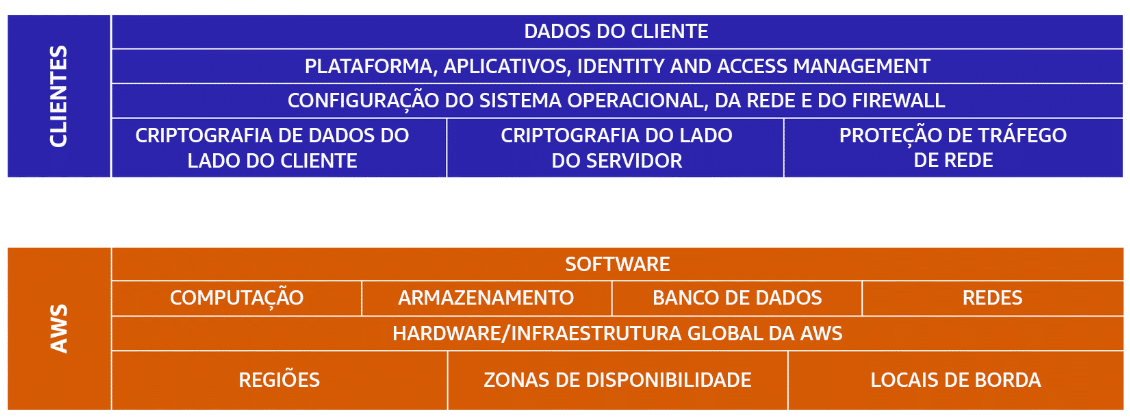
1. otimização de custos
2. desempenho
3. segurança
4. tolerância a falhas
5. limites de serviço.



* A marca de verificação verde indica o número de itens para os quais **não foram detectados problemas**.
* O triângulo laranja representa o número de investigações recomendadas.
* O círculo vermelho representa o número de ações recomendadas.

# **Segurança**

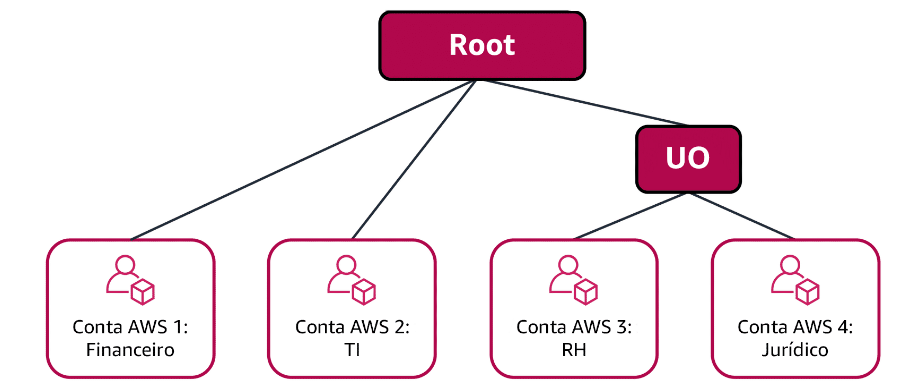
## **Modelo de responsabilidade compartilhada**



## **AWS Organizations**

A maneira mais fácil de pensar no Organizations é como um local central para gerenciar várias contas da AWS.

principais recursos:

* gerenciamento centralizado de todas as suas contas na AWS. Outra vantagem do faturamento consolidado é o desconto em massa.
* agrupamento hierárquico de suas contas para atender a requisitos de segurança, conformidade ou necessidades orçamentais, Isso significa que você pode agrupar contas em unidades organizacionais, ou OUs, tipos de negócios ou business units. 
* faturamento consolidado de todas as contas de membros.  você pode usar a conta principal da sua organização para consolidar e pagar todas as contas de outros membros.
* controle sobre serviços da WS e as ações de API. Cada conta pode acessar como administrador da conta principal de uma organização.

cobrança consolidada é outro recurso do AWS Organizations

## [**AWS Artifact**](https://aws.amazon.com/artifact) é um serviço que fornece acesso sob demanda a relatórios de segurança e conformidade da AWS e a contratos on-line selecionados. O AWS Artifact tem duas seções principais: AWS Artifact Agreements e o AWS Artifact Reports.

Vc pode **Acessar relatórios de conformidade da AWS sob demanda. Analisar, aceitar e gerenciar seus contratos com a AWS.**

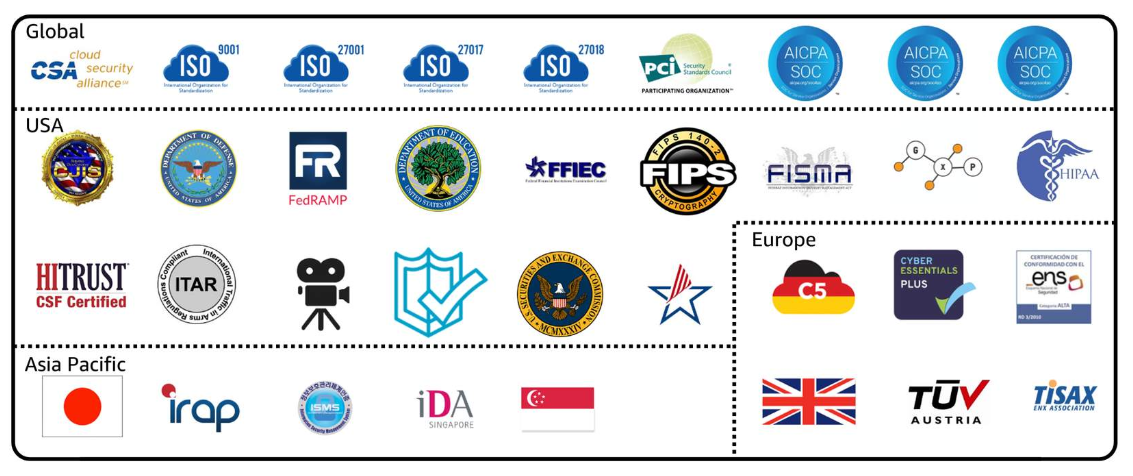
* **AWS Artifact Agreements**

Suponha que sua empresa precise assinar um contrato com a AWS em relação ao uso de determinados tipos de informações em todos os serviços AWS. Você pode fazer isso pelo **AWS Artifact Agreements**.  
No AWS Artifact Agreements, você pode revisar, aceitar e gerenciar contratos para uma conta individual e para todas as suas contas no AWS Organizations. Diferentes tipos de acordos são oferecidos para atender às necessidades dos clientes sujeitos a regulamentações específicas, como a Lei de Portabilidade e Responsabilidade dos Provedores de Saúde dos EUA (HIPAA).

* **AWS Artifact Reports**

Suponha que um membro da equipe de desenvolvimento da sua empresa esteja criando um aplicativo e precise de mais informações sobre a responsabilidade em cumprir determinados padrões regulatórios. Você pode recomendar o acesso a essas informações em **AWS Artifact Reports**.  
O AWS Artifact Reports fornece relatórios de conformidade por auditores terceirizados. Esses auditores testaram e verificaram se a AWS está em conformidade com diversas normas e regulamentações de segurança globais, regionais e específicas do setor. O AWS Artifact Reports se mantém atualizado com os relatórios publicados mais recentes. Você pode fornecer os artefatos de auditoria da AWS aos auditores ou reguladores como evidência dos controles de segurança da AWS.

O [**Centro de conformidade para o cliente**](https://aws.amazon.com/compliance/customer-center/) contém recursos que ajudam você a saber mais sobre a conformidade da AWS.



## **DDoS ou DDoS. Negação de serviço distribuída.**

Em um ataque DDoS, o agente mal-intencionado tenta sobrecarregar a capacidade da sua aplicação para que qualquer outra requisição que ocorra nos seus serviços seja negada.

**AWS Shield Standard** protege automaticamente todos os clientes AWS sem nenhum custo. Ele protege seus recursos AWS contra os tipos de ataques DDoS mais comuns e frequentes.  
À medida que o tráfego de rede ingressa em seus aplicativos, o AWS Shield Standard usa diversas técnicas de análise para detectar tráfego mal-intencionado em tempo real e mitigá-lo automaticamente.

O **AWS Shield Advanced** é um serviço pago que fornece diagnósticos detalhados de ataques e a capacidade de detectar e mitigar ataques elaborados de DDoS.  
Ele também se integra a outros serviços, como o Amazon CloudFront, o Amazon Route 53 e o Elastic Load Balancing. Além disso, você pode integrar o AWS Shield ao AWS WAF escrevendo regras personalizadas para mitigar ataques complexos de DDoS.

## [**AWS Key Management Service (AWS KMS)**](https://aws.amazon.com/kms)

permite que você execute operações de criptografia pelo uso de **chaves de criptografia**. Uma chave de criptografia é uma cadeia aleatória de dígitos usada para bloquear (criptografar) e desbloquear (descriptografar) dados. Você pode usar o AWS KMS para criar, gerenciar e usar chaves de criptografia. Você também pode controlar o uso de chaves em uma ampla gama de serviços e em seus aplicativos.

você deve garantir que os dados de seus aplicativos estejam protegidos durante o armazenamento **(criptografia em repouso)** e sendo transmitidos **(criptografia em trânsito)**.

## [**AWS WAF**](https://aws.amazon.com/waf)

é um firewall de aplicativo web que permite monitorar solicitações de rede que entram em seus aplicativos web.

O AWS WAF trabalha em conjunto com o Amazon CloudFront e um balanceador de carga de aplicativo. Lembre-se das listas de controle de acesso de rede que você aprendeu em um módulo anterior. O AWS WAF funciona de forma semelhante para bloquear ou permitir o tráfego. No entanto, ele faz isso usando uma [**lista de controle de acesso (ACL) da web**](https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html) para proteger seus recursos AWS.

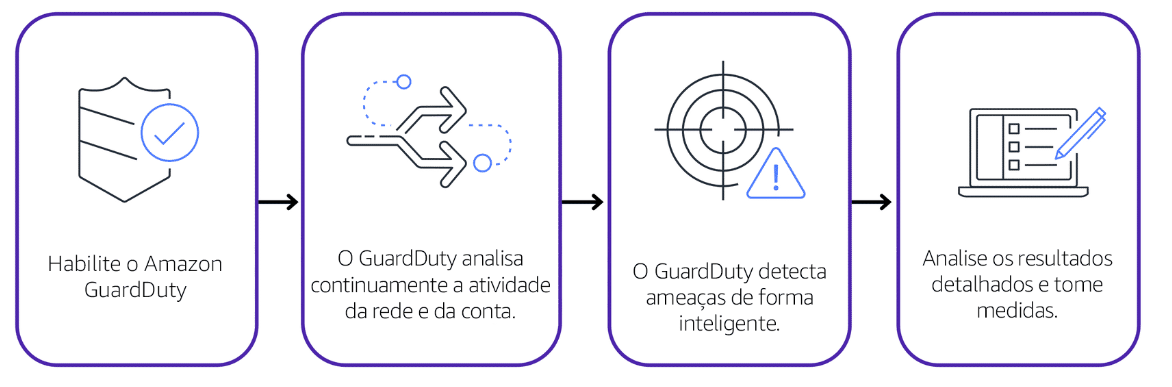
Veja um exemplo de como você pode usar o AWS WAF para permitir e bloquear solicitações específicas.

Suponha que o aplicativo tenha recebido solicitações de rede mal-intencionadas de vários endereços IP. Você quer impedir que essas solicitações continuem a acessar seu aplicativo, mas também deseja garantir que usuários legítimos ainda possam acessá-lo. Você configura a ACL da web para permitir todas as solicitações, exceto aquelas dos endereços IP que você especificou.

Quando uma solicitação entra no AWS WAF, ele confere a lista de regras configurada na ACL da web. Se uma solicitação não for proveniente de um dos endereços IP bloqueados, o AWS WAF permite o acesso ao aplicativo.

[**Amazon GuardDuty**](https://aws.amazon.com/guardduty)

é um serviço que fornece detecção inteligente de ameaças para sua infraestrutura e seus recursos AWS. Ele identifica ameaças monitorando continuamente a atividade da rede e o comportamento da conta no seu ambiente AWS.



Depois de habilitar o GuardDuty para sua conta AWS, ele começa a monitorar sua atividade de rede e conta. Você não precisa implantar ou gerenciar nenhum outro software de segurança. O GuardDuty analisa continuamente dados de várias fontes da AWS, incluindo logs de fluxo de VPC e logs de DNS.

Se ele detectar ameaças, você poderá revisar as descobertas detalhadas no AWS Management Console. As descobertas incluem etapas recomendadas para a correção. Você também pode configurar as funções do AWS Lambda para executar as etapas de correção automaticamente em resposta às descobertas de segurança do GuardDuty.

Sempre gratuito

[https://aws.amazon.com/pt/free/?all-free-tier.sort-by=item.additionalFields.SortRank&all-free-tier.sort-order=asc&awsf.Free%20Tier%20Types=\*all&awsf.Free%20Tier%20Categories=\*all](https://aws.amazon.com/pt/free/?all-free-tier.sort-by=item.additionalFields.SortRank&all-free-tier.sort-order=asc&awsf.Free%20Tier%20Types=*all&awsf.Free%20Tier%20Categories=*all)

<https://aws.amazon.com/pt/premiumsupport/plans/>

# Planos do AWS Support

**Developer**

Os clientes com um plano de suporte **Developer** têm acesso a recursos como:

* Orientação de práticas recomendadas
* Ferramentas de diagnóstico do lado do cliente
* Suporte à arquitetura de componentes fundamentais, que consiste em orientações sobre como usar as ofertas, recursos e serviços AWS combinados

Por exemplo, suponha que sua empresa esteja explorando os serviços AWS. Você já ouviu falar sobre alguns serviços diferentes da AWS. No entanto, você não tem certeza de como usá-los combinados para criar aplicativos que possam atender às necessidades de sua empresa. Nesse cenário, o suporte à arquitetura de componentes fundamentais incluído no plano de suporte Developer pode ajudar você a identificar oportunidades para combinar serviços e recursos específicos.

**Business**

Os clientes com um plano de suporte **Business** têm acesso a recursos adicionais, incluindo:

* Orientação de caso de uso para identificar ofertas, recursos e serviços AWS que podem atender melhor às suas necessidades específicas
* Todas as verificações do AWS Trusted Advisor
* Suporte limitado para software de terceiros, como sistemas operacionais comuns e componentes de pilha de aplicativos

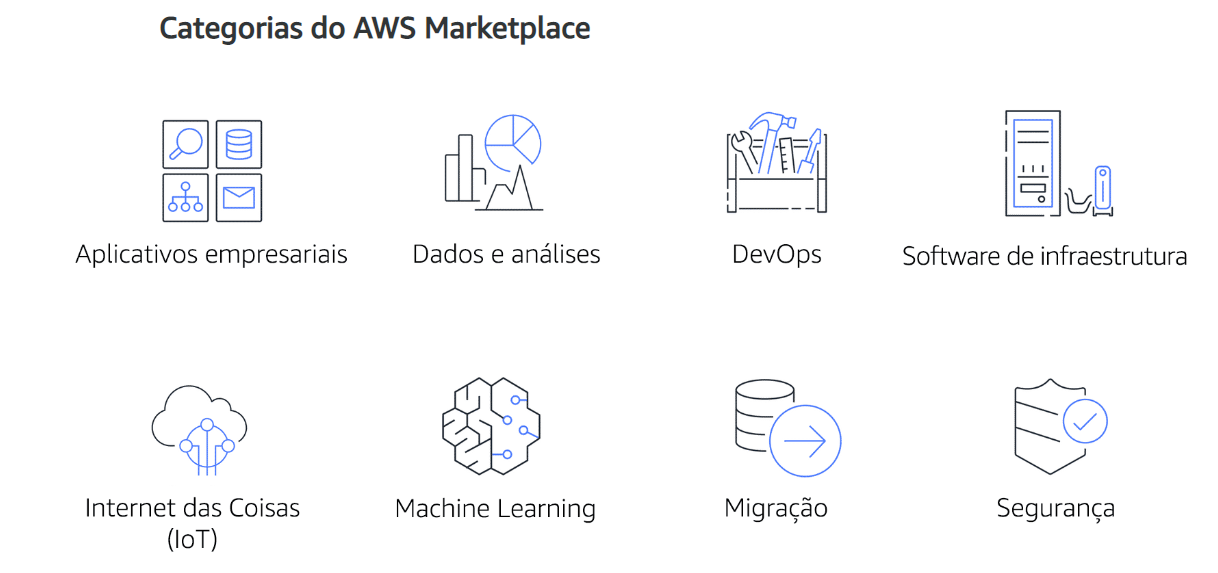
Suponha que sua empresa tenha o plano de suporte Business e queira instalar um sistema operacional de terceiros comum em suas instâncias do Amazon EC2. Você pode entrar em contato com o AWS Support para obter assistência com a instalação, configuração e solução de problemas do sistema operacional. Para tópicos avançados, como otimizar o desempenho, usar scripts personalizados ou resolver problemas de segurança, pode ser necessário entrar em contato diretamente com o provedor de software de terceiros.~

**Enterprise**

Além de todos os recursos incluídos nos planos de suporte Basic, Developer e Business, os clientes com um plano de suporte **Enterprise** têm acesso a recursos como:

* Orientação de arquitetura de aplicativos, que é um relacionamento consultivo para apoiar casos de uso e aplicativos específicos da sua empresa
* Gerenciamento de eventos de infraestrutura: engajamento de curto prazo com o AWS Support que ajuda sua empresa a compreender melhor seus casos de uso. Também fornece à sua empresa orientação de arquitetura e scaling.
* Um technical account manager

O[**AWS Marketplace**](https://aws.amazon.com/marketplace) é um catálogo digital com milhares de ofertas de fornecedores independentes de software. Você pode usar o AWS Marketplace para encontrar, testar e comprar software que pode ser executado na AWS.



# **MIGRAÇÃO E INOVAÇÃO**

## [**AWS Cloud Adoption Framework (AWS CAF)**](https://d1.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf)

Ajuda você a gerenciar esse processo migração para a AWS por meio de orientações para 6 áreas de foco chamadas **perspectivas**.  as perspectivas e **negócio**, **pessoas** e **governança** se concentram nas capacidades comerciais, enquanto as perspectivas de **plataforma**, **segurança** e **operações** se concentram em capacidades técnicas.

**Perspectiva de negocia**

A **perspectiva de negócio** garante que a TI esteja alinhada às necessidades de negócio e que os investimentos em TI estejam vinculados aos principais resultados dos negócios.  
  
Use a perspectiva de negócio para criar um caso de negócio sólido para adoção da nuvem e priorizar as iniciativas de adoção da nuvem. Garanta que suas estratégias e metas de negócios estejam alinhadas com suas estratégias e metas de TI.

As funções comuns a perspectiva de negócio são:

* Gerentes de negócios
* Gerentes financeiros
* Proprietários de orçamento
* Stakeholders de estratégia

**Perspectiva de pessoas**

A **perspectiva de pessoas** promove o desenvolvimento de uma estratégia de gerenciamento de alterações em toda a organização para a adoção bem-sucedida da nuvem.  
  
Use a perspectiva de pessoas para avaliar estruturas e funções organizacionais, novos requisitos de habilidades e processos e identificar lacunas. Isso ajuda a priorizar treinamento, pessoal e mudanças organizacionais.  
  
As funções comuns da perspectiva de pessoas são:

* Recursos humanos
* Equipe
* Gerentes de pessoas

**Perspectiva de governança**

A **perspectiva de governança** concentra-se nas habilidades e nos processos para alinhar as estratégias de TI e de negócios. Isso garante que você maximize o valor comercial e minimize os riscos.

Use a perspectiva de governança para entender como atualizar as habilidades e os processos da equipe necessários para garantir a governança de negócios na nuvem. Gerencie e mensure os investimentos em nuvem para avaliar os resultados de negócios.  
  
As funções comuns na perspectiva de governança são:

* Diretor de informações (CIO)
* Gerentes do programa
* Arquitetos empresariais
* Analistas de negócios
* Gerentes de portfólio

**Perspectiva de plataforma**

A **perspectiva de plataforma** inclui princípios e padrões para implementação de novas soluções na nuvem e migração de cargas de trabalho locais para a nuvem.

Use uma variedade de modelos arquitetônicos para entender e comunicar a estrutura dos sistemas de TI e suas relações. Descreva a arquitetura do ambiente de destino em detalhes.  
  
As funções comuns da perspectiva de plataforma são:

* Diretor de tecnologia (CTO)
* Gerentes de TI
* Arquitetos de soluções

**Perspectiva de segurança**

A **perspectiva de segurança** garante que a organização atenda aos objetivos de segurança de visibilidade, auditoria, controle e agilidade.

Use o AWS CAF para estruturar a seleção e a implementação de controles de segurança que atendam às necessidades da organização.  
  
As funções comuns da perspectiva de segurança são:

* Diretor de segurança da informação (CISO)
* Gerentes de segurança de TI
* Analistas de segurança de TI

**Perspectiva de operações**

A **perspectiva de operações** ajuda você a habilitar, executar, usar, operar e recuperar cargas de trabalho de TI para o nível definido com os stakeholders da empresa.

Defina como os negócios diários, trimestrais e anuais são conduzidos. Alinhe e dê suporte às operações do negócio. O AWS CAF ajuda os stakeholders a definir os procedimentos operacionais atuais e identificar mudanças de processo e treinamento necessários para implementar a nuvem com sucesso.  
  
As funções comuns da perspectiva de operações são:

* Gerentes de operações de TI
* Gerentes de suporte de TI

**Seis estratégias de migração**

* **Redefinir hospedagem**, também conhecida como “lift-and-shift”, envolve a movimentação de aplicativos sem alterações.    
  No cenário de uma grande migração legada, em que a empresa busca implementar sua migração e dimensionar rapidamente para atender a um caso de negócio, a hospedagem da maioria dos aplicativos é redefinida.
* **Realocação de plataforma**, também conhecida como “lift, tinker and shift”, envolve fazer algumas otimizações na nuvem para obter um benefício tangível. A otimização é alcançada sem alterar a arquitetura central do aplicativo.
* **Refatoração** (também conhecida como **rearquitetura**) envolve reimaginar como um aplicativo é arquitetado e desenvolvido usando recursos nativos da nuvem. A refatoração costuma ser orientada pela forte necessidade que a empresa tem de adicionar recursos, scaling ou desempenho que, de outra forma, seriam difíceis de obter no ambiente atual do palicativo.
* **Recompra** envolve a mudança de uma licença tradicional para um modelo de software como serviço.  
  Por exemplo, uma empresa pode optar por implementar a estratégia de recompra migrando de um sistema de gerenciamento de relacionamento com o cliente (CRM) para o Salesforce.com.
* **Retenção** consiste em manter os aplicativos essenciais para a empresa no ambiente de origem. Isso pode incluir aplicativos que exigem refatoração importante antes de serem migrados ou trabalhos que podem ser adiados.
* **Inativação** é o processo de remoção de aplicativos que não são mais necessários.

## [**AWS Snow Family**](https://aws.amazon.com/snow)

é uma coleção de dispositivos físicos para transporte físico de até exabytes de dados para dentro e para fora da AWS. A AWS Snow Family consiste nos serviços **AWS Snowcone**, **AWS Snowball** e **AWS Snowmobile**.

1. [**AWS Snowcone**](https://aws.amazon.com/snowcone) é um dispositivo pequeno, robusto e seguro para transferência de dados e computação de borda. Ele tem 2 CPUs, 4 GB de memória e 8 TB de armazenamento utilizável.
2. [**AWS Snowball**](https://aws.amazon.com/snowball/) oferece dois tipos de dispositivos: os dispositivos

* **Snowball Edge otimizados para armazenamento**são ideais para migrações de dados de grande escala e fluxos de trabalho de transferência recorrentes, em além da computação local com necessidades maiores de capacidade.
  + Armazenamento: 80 TB de capacidade de disco rígido (HDD) para volumes de blocos e armazenamento de objeto compatível com o Amazon S3, além de unidade de estado sólido (SSD) de 1 TB para volumes de blocos.
  + Computação: 40 vCPUs e 80 GiB de memória para dar suporte a instâncias sbe1 do Amazon EC2 (equivalente a C5).
* **O Snowball Edge otimizado para computação**fornece recursos de computação poderosos para casos de uso, como machine learning, análise de vídeo em movimento completo, análise e pilhas de computação locais.
  + Armazenamento: capacidade de HDD utilizável de 42 TB para armazenamento de objeto compatível com o Amazon S3 ou volumes de blocos compatíveis com o Amazon EBS e também 7,68 TB de capacidade de SSD NVMe utilizável para volumes de blocos compatíveis com o Amazon EBS.
  + Computação: 52 vCPUs, 208 GiB de memória e uma GPU NVIDIA Tesla V100 opcional. Os dispositivos executam as instâncias sbe-c e sbe-g do Amazon EC2, que são equivalentes às instâncias C5, M5a, G3 e P3.

1. [**O AWS Snowmobile**](https://aws.amazon.com/snowmobile) é um serviço de transferência dados na escala de exabytes usado para mover grandes quantidades de dados para a nuvem AWS.  
   Você pode transferir até 100 petabytes por Snowmobile, um contêiner de transporte reforçado com 13,71 metros de comprimento puxado por um caminhão semirreboque.

**inteligência artificial (IA)**.

* Amazon Transcribe: Converte fala em texto
* Amazon Comprehend: Descobre padrões em texto
* Amazon Fraud Detector: Identifica atividades on-line potencialmente fraudulentas.
* Amazon Lex: Cria chatbots de voz e texto

**machine learning**

* **Amazon Textract** que extrai automaticamente texto e dados de documentos digitalizados.
* **AWS DeepRacer** é um carro de corrida autônomo de escala 1/18 que você pode usar para testar modelos de aprendizado por reforço.
* **Amazon SageMaker**, que remove o trabalho difícil do processo e ajuda você a criar, treinar e implantar modelos de ML rapidamente.

[**AWS Well-Architected Framework**](https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf)   
ajuda você a entender como projetar e operar sistemas confiáveis, seguros, eficientes e econômicos na nuvem AWS. Com ele, é possível avaliar de forma consistente suas arquiteturas em relação às melhores práticas e aos princípios de projeto e a identificar áreas para melhorias.

Well-Architected Framework tem pilares. Esses pilares são: excelência operacional, segurança, confiabilidade, eficiência de performance e otimização de custos.

* **Excelência operacional** é a capacidade de executar e monitorar sistemas para entregar valor comercial e melhorar continuamente os processos e procedimentos de apoio.
* **segurança** inclui a capacidade de proteger informações, sistemas e ativos e, ao mesmo tempo, entregar valor comercial por meio de avaliações de risco e estratégias de mitigação.
* **Confiabilidade** é a capacidade de:
* Recuperar-se de interrupções na infraestrutura ou no serviço
* Adquirir dinamicamente recursos de computação para atender à demanda
* Reduzir interrupções, como configurações incorretas ou problemas de rede transitórios

A confiabilidade inclui testes de procedimentos de recuperação, scaling horizontal para aumentar a disponibilidade agregada do sistema e recuperação automática de falhas.

* **eficiência de desempenho** é a capacidade de usar recursos computacionais com eficiência para cumprir requisitos do sistema e manter essa eficiência à medida que a demanda muda e as tecnologias evoluem.  
  A avaliação da eficiência de desempenho de sua arquitetura inclui experimentar com mais frequência, usar arquiteturas sem servidor e projetar sistemas para ter alcance global em minutos.
* **Otimização de custos** é a capacidade de executar sistemas para entregar valor comercial com o menor preço.  
  A otimização de custos inclui a adoção de um modelo de consumo, análise e atribuição de despesas e uso de serviços gerenciados para reduzir o custo de propriedade.

**Recursos adicionais**

Para saber mais sobre os conceitos que foram explorados no módulo 7, revise estes recursos.

* [Gerenciamento e governança na AWS](https://aws.amazon.com/products/management-tools)
* [Monitoramento e observabilidade](https://aws.amazon.com/products/management-tools/use-cases/monitoring-and-observability/)
* [Configuração, conformidade e auditoria](https://aws.amazon.com/products/management-tools/use-cases/configuration-compliance-and-auditing/)
* [Blog de gerenciamento e governança da AWS](https://aws.amazon.com/blogs/mt/)
* [Whitepaper: AWS Governance at Scale](https://docs.aws.amazon.com/whitepapers/latest/aws-governance-at-scale/introduction.html)

**Recursos adicionais**

Para saber mais sobre os conceitos que foram explorados no módulo 8, revise estes recursos.

* [Definição de preços da AWS](https://aws.amazon.com/pricing)
* [Nível gratuito da AWS](https://aws.amazon.com/free)
* [Gerenciamento de custos da AWS](https://aws.amazon.com/aws-cost-management/)
* [Whitepaper: How AWS Pricing Works](https://d1.awsstatic.com/whitepapers/aws_pricing_overview.pdf)
* [Whitepaper: Introduction to AWS Economics](https://d1.awsstatic.com/whitepapers/introduction-to-aws-cloud-economics-final.pdf)
* [AWS Support](https://aws.amazon.com/premiumsupport)
* [Central de conhecimento da AWS](https://aws.amazon.com/premiumsupport/knowledge-center/)
* AO AWS Direct Connect é um serviço que estabelece uma conexão privada dedicada entre o seu data center e a VPC. A conexão privada que o AWS Direct Connect fornece ajuda você a reduzir os custos de rede e a aumentar a quantidade de largura de banda que pode trafegar pela sua rede.
* O Amazon CloudFront é um serviço de entrega de conteúdo. Ele usa uma rede de locais de borda para armazenar conteúdo em cache e entregar conteúdo para clientes em todo o mundo.
* Um gateway privado virtual estabelece uma conexão VPN (rede virtual privada) entre a VPC e uma rede privada, como um data center local ou uma rede corporativa interna. Um gateway privado virtual só permite o tráfego na VPC se for proveniente de uma rede aprovada.
* Um gateway da internet é uma conexão entre uma VPC e a internet. Permite que o tráfego público da internet acesse uma VPC.
* O AWS Snowball é um dispositivo para transferência de grandes quantidades de dados para dentro e para fora da AWS.