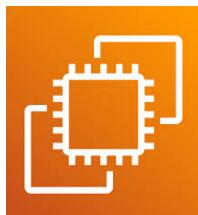


Resumo AWS Cloud Practitioner

Instâncias do Amazon EC2



(Elastic Compute Cloud, observação o 2, é por conta dos dois C's)

Compreendendo que esse serviço se consiste na alocação de uma máquina virtual, podemos segregar esse serviços em diversos tipos para determinadas funções, priorizando o uso eficiente e econômico para cada usuário, sendo que nessa separação, há outras separações, partiu ver?

[Amazon EC2 tipos de instâncias - AWS](#)

▼ Uso Geral

As **instâncias otimizadas para computação** são ideais para aplicações que precisam de muito poder de processamento. Elas são úteis para diversos tipos de trabalho, incluindo servidores web, de aplicações e de jogos, assim como as instâncias de uso geral.

A principal diferença é que as instâncias otimizadas para computação são melhores para:

- Servidores web que precisam lidar com muitas solicitações
- Aplicações que exigem cálculos complexos
- Servidores de jogos dedicados
- Processamento em lote (quando muitas tarefas são realizadas de uma vez)

Essas instâncias são especialmente boas para lidar com muitas operações ao mesmo tempo, tornando-as ideais para tarefas que exigem alta capacidade de processamento.

▼ Otimizadas para computação

As instâncias otimizadas para computação são ideais para aplicativos que requerem alto desempenho computacional. São adequadas para processamento em lote, transcodificação de mídia, servidores web de alta performance, HPC, modelagem científica, servidores de jogos, mecanismos de anúncios, inferência de machine learning e outras aplicações computacionalmente intensivas.

▼ Otimizadas para memória

As instâncias otimizadas para memória são feitas para trabalhar rápido com grandes quantidades de dados. Elas são especialmente boas para programas que precisam processar muita informação de uma vez só, guardando tudo na memória do computador para acesso rápido.

▼ Computação acelerada

Instâncias de computação acelerada usam hardware especial, chamado de aceleradores ou coprocessadores, para fazer certas tarefas mais rapidamente que os computadores normais. Essas tarefas incluem:

- Cálculos matemáticos complexos
- Processamento de imagens e vídeos
- Análise de grandes quantidades de dados

Esses aceleradores trabalham junto com o processador principal (CPU) para tornar essas operações mais rápidas e eficientes.

▼ Otimizadas para armazenamento

As instâncias otimizadas para armazenamento são feitas para lidar com grandes quantidades de dados que precisam ser lidos e gravados rapidamente. Elas são boas para:

- Trabalhar com conjuntos de dados muito grandes armazenados localmente
- Realizar muitas operações de leitura e gravação ao mesmo tempo
- Processar rapidamente milhares de pequenas tarefas de leitura e gravação por segundo

Essas instâncias são especialmente úteis para aplicações que precisam acessar e processar dados de forma rápida e eficiente.

▼ Otimizadas para HPC

As instâncias de computação de alta performance (HPC) são projetadas para oferecer a melhor relação custo-benefício para workloads de HPC em grande escala na AWS. São ideais para aplicações que exigem processadores potentes, como simulações complexas e aprendizado profundo.

Definição de preço EC2

Compreendo o que a Amazon deixa claro: "você só paga pelo o que usar", está na hora de se aprofundar sobre as definições de preço da Amazon EC2;

▼ Sob demanda

Instâncias sob demanda são ideais para cargas de trabalho curtas e irregulares que não podem ser interrompidas. Não há custos iniciais ou contratos, e você paga apenas pelo tempo usado. Elas funcionam até serem interrompidas.

São recomendadas para desenvolvimento, teste e aplicações com uso imprevisível. Para cargas que duram um ano ou mais, instâncias reservadas podem ser mais econômicas.

▼ Instâncias reservadas

Instâncias reservadas oferecem descontos no uso de instâncias sob demanda. Existem dois tipos:

1. **Standard Reserved Instances:** São indicadas se você sabe o tipo e tamanho da instância EC2 que precisa, além da região em que vai utilizá-las. Você pode definir a Zona de Disponibilidade para garantir a capacidade da instância. Disponíveis em períodos de 1 ou 3 anos, com mais economia no prazo de 3 anos.
2. **Instâncias reservadas conversíveis:** Oferecem flexibilidade para alterar Zona de Disponibilidade ou tipo de instância durante o uso, mas com um desconto menor.

Após o término do período de instância reservada, você pode continuar usando-a com preços de sob demanda até encerrar ou adquirir uma nova instância reservada com as mesmas especificações.

As Standard Reserved Instances exigem que você especifique:

- *tamanho e família de instância*
- *descrição da plataforma*
- *tenancy*
- *Região*

Sua quantidade específica de instâncias do EC2 é coberta por um período de vigência de um ou três anos.

Uma Região consiste em três ou mais Zonas de Disponibilidade.

Por exemplo, a Região América do Sul (São Paulo) é sa-east-1.

Ela tem três Zonas de Disponibilidade: sa-east-1
a, sa-east-1**b** e sa-east-1**c**.

▼ Savings Plans

A AWS oferece Savings Plans para reduzir custos no EC2. Você se compromete com um gasto fixo por hora em uma família de instâncias e região por 1 ou 3 anos, economizando até 72% comparado às taxas sob demanda. O uso dentro do compromisso tem preço reduzido, e o extra segue as taxas normais.

Savings Plans são ideais para quem precisa de flexibilidade no EC2, sem definir o tipo ou tamanho de instância. Use o **AWS Cost Explorer** para ver recomendações e calcular possíveis economias.

Os Savings Plans reduzem o custo das instâncias do EC2 em troca do compromisso de um gasto por hora com uma família e uma Região, por um ou três anos.

▼ Instâncias spot

Instâncias spot são ideais para cargas de trabalho com horários flexíveis ou que podem ser interrompidas. Elas usam a capacidade não utilizada do EC2, com descontos de até 90% em relação às instâncias sob demanda.

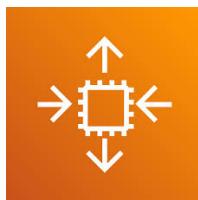
Por exemplo, se você tiver um processo em segundo plano que pode ser pausado (como uma pesquisa de cliente), as instâncias spot são adequadas. Elas só iniciam se houver capacidade disponível, e podem ser interrompidas caso essa capacidade se torne indisponível.

Se o trabalho não pode ser interrompido, como desenvolvimento e teste de aplicativos, é melhor escolher outro tipo de instância EC2.

▼ Host dedicados

Os hosts dedicados são servidores físicos do Amazon EC2 exclusivos para o uso do cliente. Eles permitem usar suas próprias licenças de software conforme necessário. Podem ser adquiridos sob demanda ou como reservas. Entre as opções do EC2, os hosts dedicados são os mais caros.

Scaling do Amazon EC2



O dimensionamento envolve começar com os recursos necessários e ajustar automaticamente conforme a demanda aumenta ou diminui, garantindo que você pague apenas pelo que usa. Isso evita falta de capacidade para atender os clientes.

Existem duas maneiras de lidar com o aumento da demanda:

aumentar verticalmente, dar mais potência a uma máquina;

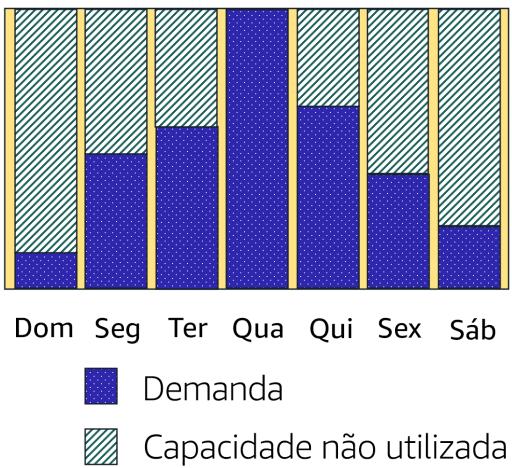
aumentar a quantidade, adicionar mais máquinas;

Embora aumentar a potência funcione às vezes, não resolve tudo.

O

Amazon EC2 Auto Scaling ajusta automaticamente o número de instâncias, adicionando mais quando necessário e desligando as que estão ociosas. Isso garante que você tenha a quantidade certa de instâncias a qualquer momento, otimizando custos e atendendo as requisições.

EC2 Auto Scaling



O Amazon EC2 Auto Scaling ajusta automaticamente a quantidade de instâncias EC2 conforme a demanda da aplicação aumenta ou diminui, garantindo maior disponibilidade. Ele funciona como uma cafeteria que adiciona mais baristas quando há mais clientes, evitando longas esperas.

Existem duas abordagens no Auto Scaling:

- **Scaling dinâmico:** responde automaticamente a mudanças na demanda.
- **Scaling preditivo:** ajusta o número de instâncias com base em previsões de demanda futura, antecipando a necessidade de mais ou menos recursos.

Para dimensionar mais rapidamente, você pode combinar o scaling dinâmico e preditivo.

Elastic Load Balancing

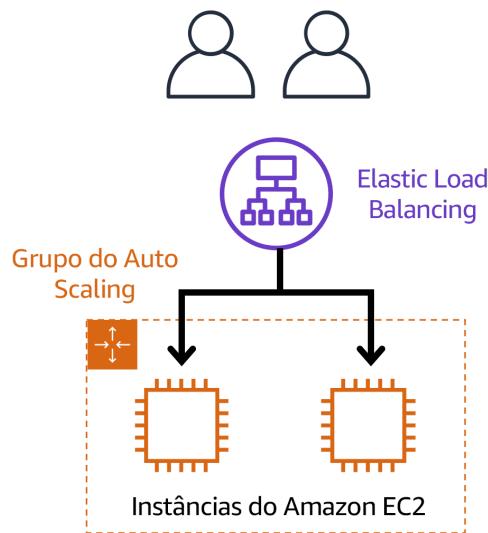


O **Elastic Load Balancing** é um serviço da AWS que distribui automaticamente o tráfego de aplicações entre várias instâncias do Amazon EC2.

Ele atua como um ponto único para todo o tráfego da web, direcionando as solicitações para o balanceador de carga, que as distribui entre as instâncias. Isso evita que uma única instância fique sobrecarregada.

Embora sejam serviços diferentes, o Elastic Load Balancing e o Amazon EC2 Auto Scaling trabalham juntos para garantir que as aplicações tenham bom desempenho e alta disponibilidade.

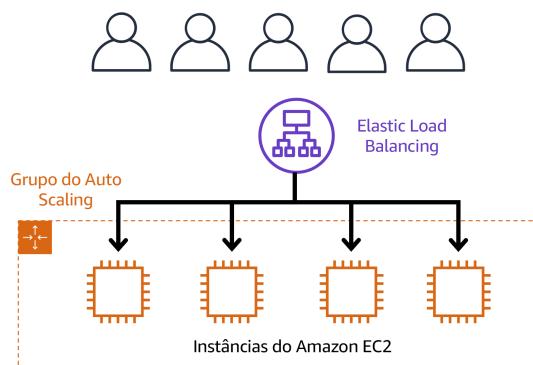
Baixa demanda



Um site pode enfrentar problemas quando recebe um aumento repentino de acessos e muitos visitantes fazem solicitações ao mesmo tempo.

Se apenas algumas instâncias do Amazon EC2 estiverem ativas, o site não consegue atender a toda a demanda, o que pode deixá-lo lento ou até travado. Para resolver isso, é necessário ter mais instâncias do EC2 disponíveis para lidar com o aumento do tráfego.

Alta demanda



à medida que o número de visitantes de um site aumenta, o site ativa mais instâncias do Amazon EC2 para atendê-los.

Além disso, um sistema de平衡amento de carga direciona as solicitações dos usuários para as instâncias disponíveis, garantindo que a carga seja distribuída uniformemente entre elas. Assim, o balanceador de carga garante que o site funcione de maneira eficiente, mesmo com o aumento de acessos.

Enfileiramento e sistema de mensagens

podemos imaginar um site recebendo muito tráfego e fazendo diversas solicitações ao mesmo tempo. Sem uma fila, cada solicitação teria que ser processada imediatamente o que causaria uma sobrecarregando o sistema, portanto o **Amazon SQS** é a solução que gera esse enfileiramento.

Onde os pedidos ficam armazenados até poderem ser processados. Assim, não sobrecarregado as instâncias e as solicitações não se perdem e são processadas quando possível. Isso é chamado de **acoplamento fraco**, evitando falhas no sistema.

Assim o **SQS** armazena as solicitações entre componentes, e o **Amazon SNS**, envia notificações para os destinatários, como notificações push, SMS ou e-mails.

- **Amazon Simple Notification Service (SNS)**: envia notificações para vários destinatários ao mesmo tempo.
- **Amazon Simple Queue Service (SQS)**: armazena e gerencia mensagens entre os componentes de forma confiável.

Amazon Simple Queue Service (Amazon SQS)



Assim como explicamos anteriormente o **SQS** é usado para armazena 'filas de requisições' e assim ele compartilha para os outros componentes do sistema, garantindo a entrega e o processamento no momento correto.

Para aplicações e microsserviços desacoplados, o **Amazon SQS** permite enviar, armazenar e recuperar mensagens entre diferentes componentes.

Isso permite que cada parte funcione de forma mais eficiente e independente, sem depender diretamente das outras.

Amazon Simple Notification Service (Amazon SNS)



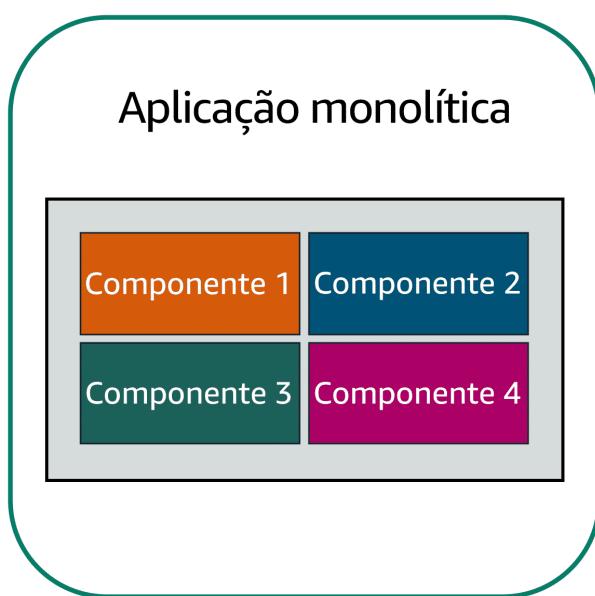
O **Amazon Simple Notification Service (SNS)** é um serviço de publicação/assinatura. Com ele, um editor envia mensagens para vários assinantes. Isso funciona de forma parecida com um newsletter: o servidor recebe as solicitações e distribui

para os assinantes, que podem ser servidores, e-mails, funções do AWS Lambda ou outros destinos.

- **Publicação de atualizações de um único tópico**
 - Pegando o exemplo de Newsletter ou jornais digitais, nessa categoria, todos os assinantes recebem todas as notícias publicadas pelo site.
- **Publicação de atualizações de vários tópicos**
 - Já nessa função, o assinante escolhe, quais notícias ele deseja receber, por exemplo; quero somente notificações sobre política ou cantores pop, assim então, só chegará pautas com esses assuntos.

Aplicações monolíticas e microsserviços

Aplicação monolítica



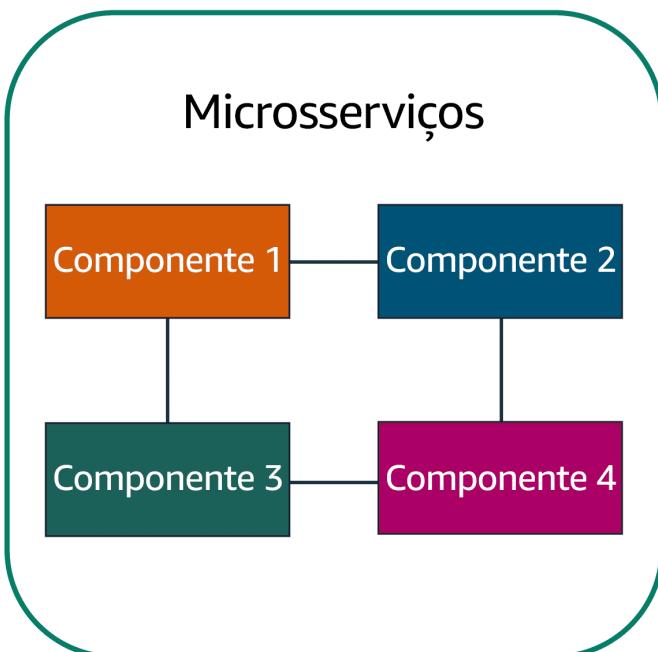
As aplicações são compostas por vários componentes que se comunicam para trocar dados, atender solicitações e manter o sistema funcionando.

Em uma arquitetura de **acoplamento forte**, esses componentes (como banco de dados, servidores, interface do usuário e lógica de negócios) estão fortemente interligados, formando uma aplicação **monolítica**.

Nesse tipo de arquitetura, se um componente falhar, isso pode causar a falha de outros e até derrubar toda a aplicação.

Para manter a disponibilidade da aplicação quando um único componente falha, você pode projetar essa aplicação com uma abordagem de microsserviços.

Microsserviços



Na abordagem de **microsserviços**, os componentes da aplicação são independentes, com **acoplamento fraco**.

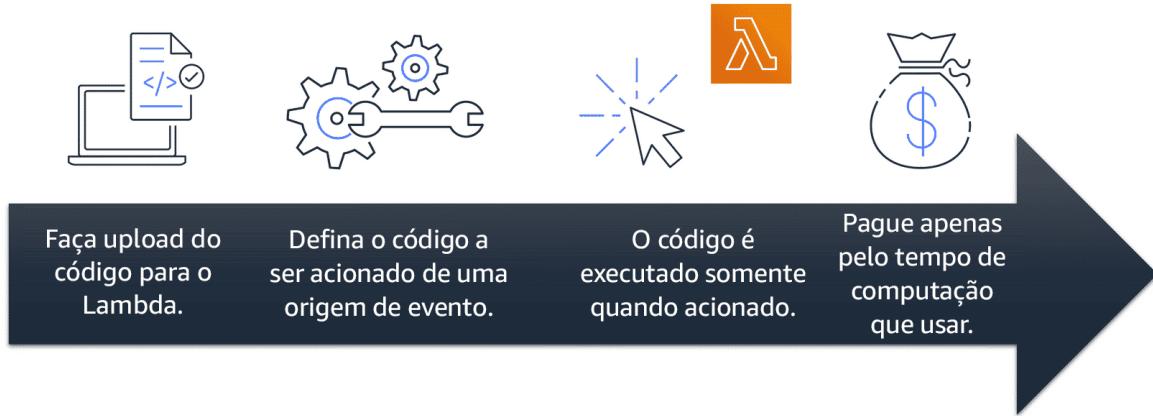
Isso significa que, se um componente falhar, os demais continuam operando normalmente, pois não dependem diretamente uns dos outros. Esse design reduz o risco de falha total da aplicação, garantindo maior resiliência e estabilidade.

AWS Lambda



Diferente do EC2 o Lambda você utiliza para 'alocar códigos/programas/executáveis', portanto, vamos supor que você precise rodar um script de rotina, através do Lambda você pode executar através de um comando.

Quanto ao custo, ele só cobrará o tempo em que o código permaneceu em execução.



1. Você faz upload do código para o Lambda.
2. Você configura o código para ser acionado pelos eventos de uma origem como serviços da AWS, aplicações móveis ou endpoints HTTP.
3. O Lambda executa o código somente quando acionado.
4. Você paga apenas pelo tempo de computação que usar.

Contêineres

Contêineres, propriamente dito, armazenam desde códigos, configurações ou informações das aplicações, também servindo para 'filtrar acesso de segurança'

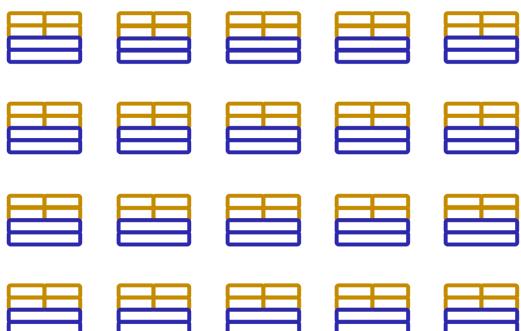
Um host com vários contêineres



Um host com vários contêineres permite que o desenvolvedor garanta que o ambiente do aplicativo seja o mesmo, independentemente de onde ele seja implantado.

Isso resolve o problema de ambientes diferentes entre o computador do desenvolvedor e os sistemas da equipe de TI. Usar contêineres mantém o ambiente consistente, reduzindo o tempo gasto com depuração e diagnóstico de problemas causados por diferenças nas configurações.

Dezenas de hosts com centenas de contêineres



Quando você executa aplicações em contêineres em grande escala, com dezenas ou centenas de hosts e centenas ou milhares de contêineres, o gerenciamento se torna mais complexo. É preciso monitorar o uso de memória, segurança, registro de logs e outros fatores.

Fazer isso manualmente levaria muito tempo e seria trabalhoso. Por isso, é importante usar ferramentas de orquestração de contêineres, como o **Amazon ECS** ou **Amazon EKS**, que automatizam e facilitam o gerenciamento e o dimensionamento dessas operações.

Os serviços de orquestração de contêineres ajudam a implantar, gerenciar e dimensionar aplicações em contêineres. Dois serviços que fazem isso são:

Amazon Elastic Container Service (Amazon ECS)



É um sistema de gerenciamento que executa e dimensiona aplicações em contêineres.

Com o **Amazon ECS**, você pode usar APIs para iniciar e parar aplicações baseadas no Docker de maneira simples.

Amazon Elastic Kubernetes Service (Amazon EKS)



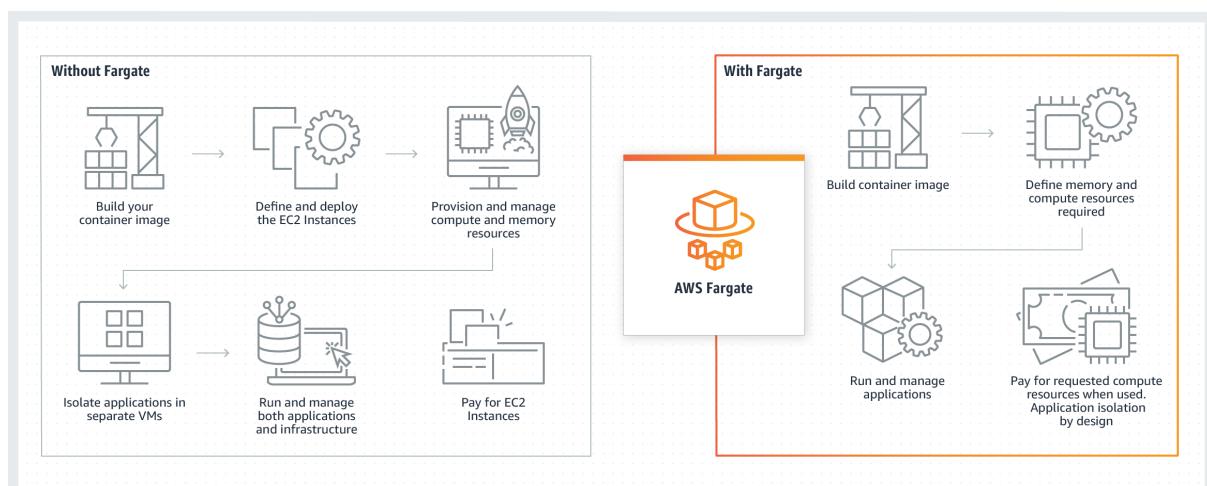
É um serviço gerenciado que permite executar **Kubernetes**.

O **Kubernetes** é usado para implantar e gerenciar aplicações em contêineres em grande escala.

AWS Fargate



É um serviço que funciona com o **Amazon ECS** e o **Amazon EKS**, permitindo executar contêineres sem precisar gerenciar servidores. Basta escolher uma imagem de contêiner e o Fargate automaticamente provisiona os recursos necessários, executa o contêiner, lida com o dimensionamento e mantém a infraestrutura, sem que você precise gerenciar servidores ou clusters.



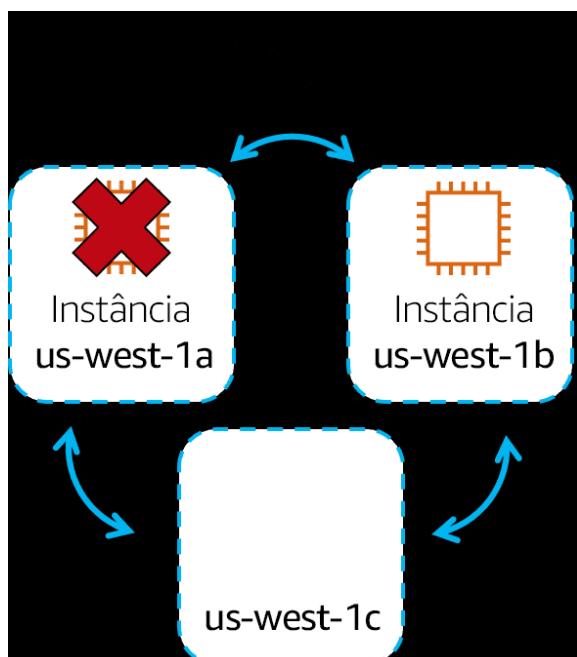
Zona de Disponibilidade

Dentro de cada região, há vários data centers separados fisicamente. Se um falhar, outro mantém seus dados seguros.

Vamos supor que por algum motivo a AWS decidiu realizar uma manutenção no servidor da região que você está alocado, isso impactaria toda sua operação, portanto, a orientação seria de distribuir suas aplicações em vários locais para garantir alta disponibilidade e resistência a falhas.

Na AWS essa distribuição é denominada de **zonas de disponibilidade (AZs)**.

- **Regiões:** São áreas geográficas distintas, cada uma com vários data centers (AZs).
- **Zonas de Disponibilidade (AZs):** São data centers independentes dentro de uma região, com infraestrutura redundante.



Se us-west-1a falhasse, sua aplicação ainda seria executada em us-west-1b

Alta disponibilidade: O recomendado é rodar ao menos duas instâncias em AZs diferentes para garantir redundância e escalabilidade.

Benefícios:

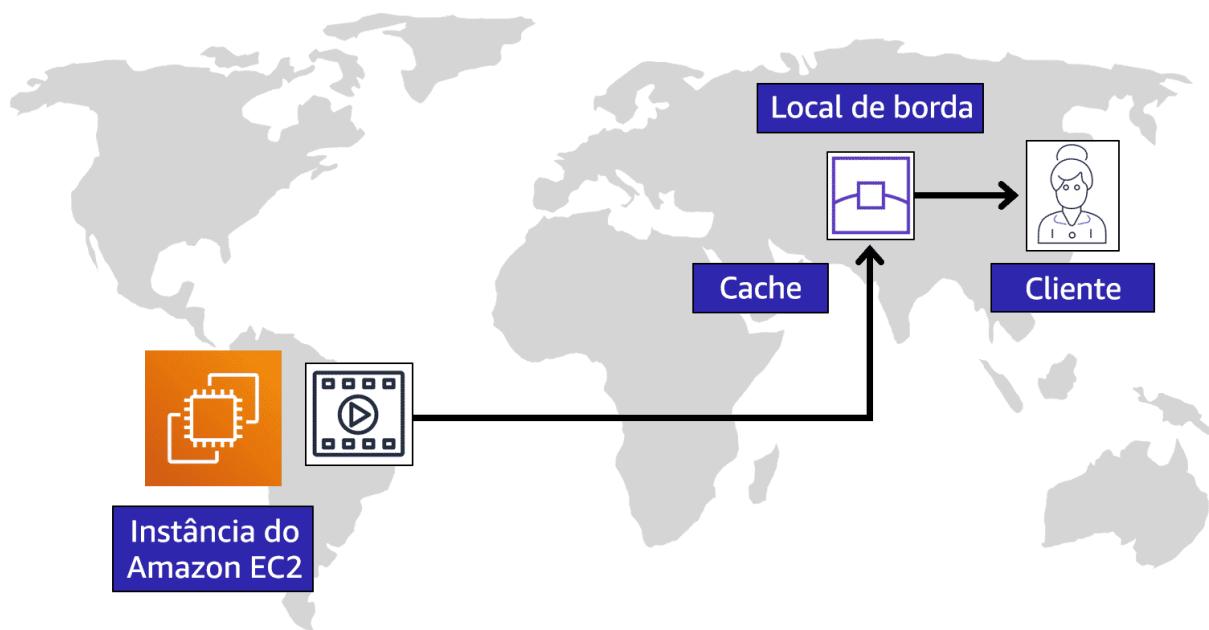
- Minimiza interrupções.
- Resiste a falhas regionais.
- Facilita o aumento de capacidade.
- Atende a requisitos de conformidade.

Planejar falhas e implantar aplicações em várias Zonas de Disponibilidade é uma parte importante da criação de uma arquitetura

resiliente e altamente disponível.

Locais de borda

Pequenas estações espalhadas pelo mundo que armazenam dados perto dos clientes, acelerando o carregamento de sites.



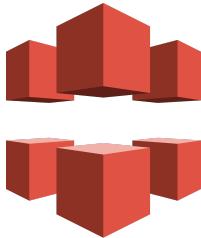
Exemplo: NETFLIX, ela carrega 'conteúdos mais acessados' em 'locais de borda' no setor Cache, para quando o cliente solicitar, já esteja 'pré-carregado' no local de borda

1. Origem: Suponha que os dados da empresa estejam no Brasil, entretanto, há cliente da China que gostariam dos arquivos, demandaria um tempo longo até transferir os arquivos solicitados.
2. Local de borda: Agora em vez de realizar toda essa trajetória, o 'local de borda' armazena uma cópia cache dos arquivos, ficando mais 'próximo para o cliente'

Isso é realizado através de solicitações feitas para o **Amazon CloudFront**, que recupera os arquivos do cache do 'local de borda'

Amazon CloudFront

Um serviço global de entrega de conteúdo.



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. Quando o conteúdo é armazenado em cache, ele é mantido localmente como uma cópia. Esse conteúdo pode ser arquivos de vídeo, fotos, páginas da web e assim por diante.

Maneiras de interagir com os serviços da AWS

A interação com os serviços da AWS são realizados pelas "APIs". Essas APIs permitem a criação, configuração e gerenciamento de recursos, como instâncias EC2 ou funções Lambda. Existem várias formas de fazer essas chamadas:

Console de Gerenciamento da AWS

Sendo uma interface web para acessar e gerenciar. Podendo procurar funções e usar assistentes para facilitar tarefas, também permite monitorar recursos, ver alarmes e acessar informações de cobrança, suportando várias identidades ao mesmo tempo.

Command Line Interface (CLI)

Permite controlar diretamente por linha de comando, economizando tempo ao fazer solicitações de API. Permite automatizar ações por meio de scripts, como iniciar instâncias do Amazon EC2 ou conectá-las a grupos de Auto Scaling.

Kits de Desenvolvimento de Software (SDKS)

Permite acessar e gerenciar usando APIs adaptadas para diversas linguagens de programação. Facilitando a integração em suas aplicações. Fornecendo documentação e exemplos de código para começar, com suporte a linguagens como C++, Java, .NET e outras.

O console é fácil para iniciantes e útil em testes, mas, em ambientes de produção, o provisionamento manual pode causar erros. Por isso, automação via CLI ou SDKs é preferível, permitindo ações programáveis e repetíveis, minimizando falhas humanas.

Além das opções manuais como o console de gerenciamento, a CLI e os SDKs. O

AWS Elastic Beanstalk é destacado como uma ferramenta que automatiza os ambientes baseados no EC2.

Basta fornecer o código da aplicação e as configurações desejadas, e ele cria o ambiente sem a necessidade de gerenciar cada elemento separadamente.

Já o **AWS CloudFormation** permite criar implantações automatizadas e repetíveis usando "infraestrutura como código". Definindo os recursos da AWS em modelos de texto (JSON ou YAML), o CloudFormation cuida do provisionamento e gerenciamento dos recursos, reduzindo o erro humano. Ambos os serviços ajudam a automatizar e simplificar a criação e o gerenciamento de recursos da AWS, enquanto o console é mais útil para aprendizado e tarefas manuais.

AWS Elastic Beanstalk



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

- Ajustar capacidade
- Balancear carga
- Auto scaling
- Monitorar o health da aplicação

AWS CloudFormation



Com o **AWS CloudFormation**, você pode considerar sua infraestrutura como código. Isso significa que você pode criar um ambiente escrevendo linhas de código em vez de usar o console de gerenciamento da AWS para provisionar recursos individualmente.

O AWS CloudFormation provisiona os recursos de maneira segura e repetível, permitindo que você crie frequentemente a infraestrutura e as aplicações sem precisar executar ações manuais. Ele determina quais são as operações mais adequadas para gerenciar sua pilha e reverte as alterações automaticamente se detecta erros.

AWS Outposts



O **AWS Outposts** oferece uma infraestrutura da AWS para seu próprio data center ou local.

Com ele, você pode rodar os mesmos serviços da AWS (como EC2 e S3) no local, mas com a mesma experiência da nuvem.

Casos de uso do **AWS Outposts**:

- **Computação de baixa latência:** Estando com a 'nuvem' no seu ambiente, diminui a latência das respostas, ideal para onde a latência precisa ser muito baixa e a nuvem pública/conectividade não atende a essa demanda.
- **Residência de dados:** Atende a requisitos regulatórios que exigem que dados permaneçam em um local específico, como em setores de finanças, processos civis e documentação.
- **Processamento local de dados:** Permite processar grandes volumes de dados localmente, como em data lakes ou treinamento de machine learning, antes de enviar para a nuvem para armazenamento.

Cada instalação do Outposts é dedicada a uma única empresa e isolada para garantir a segurança e a privacidade dos dados

Amazon Virtual Private Cloud (VPC)



A VPC é uma rede virtual que você cria dentro do ambiente. Permitindo que você isole seus recursos dos demais ambientes.

- **Sub-rede pública:** Nesta sub-rede, os recursos podem ter acesso à internet. É ideal para serviços que precisam interagir com usuários externos, como servidores web.
- **Sub-rede privada:** Os recursos nesta sub-rede não têm acesso direto à internet, sendo usados para serviços de backend, como bancos de dados e servidores de aplicação.

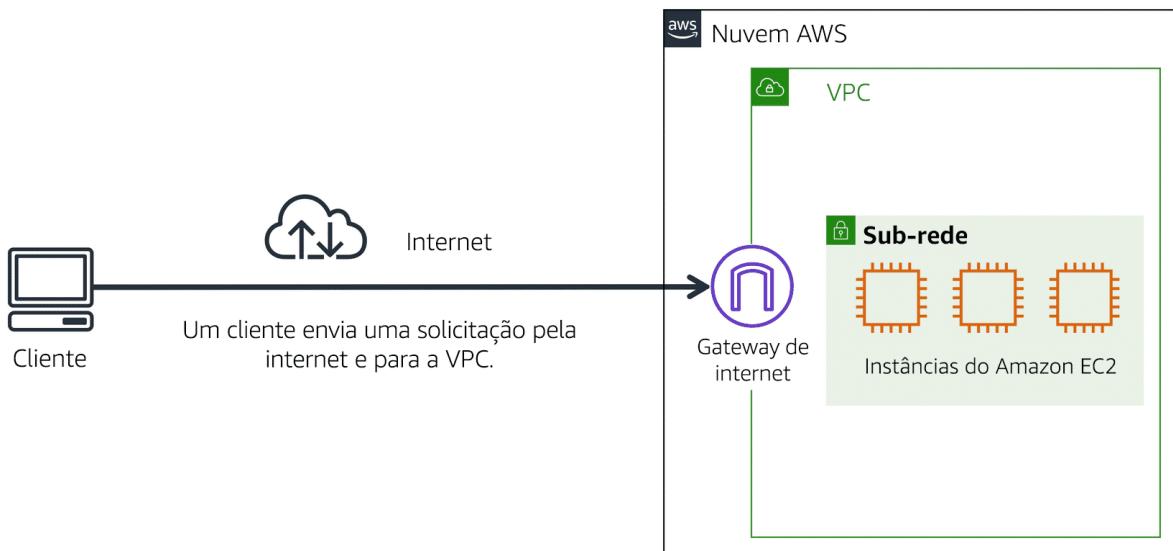
Isola bancos de dados contendo informações pessoais dos clientes.

Você pode organizar seus recursos em sub-redes, garantindo que os serviços que precisam de interação com a internet fiquem separados dos serviços internos e sensíveis.

Portanto proporciona um ambiente seguro e isolado na nuvem AWS, permitindo que você gerencie como e onde seus recursos são acessados.

Gateway de internet

Para permitir que o tráfego público da internet acesse sua VPC, é preciso anexar um **gateway de internet** à VPC.

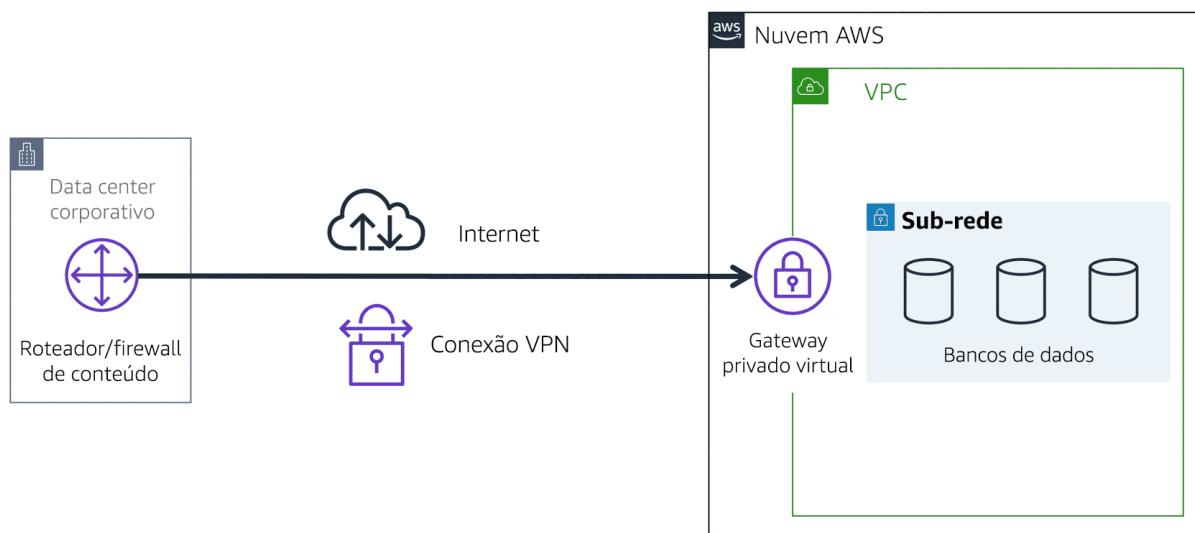


Ícone do gateway de internet anexado a uma VPC que contém três instâncias do EC2. Uma seta conecta o cliente ao gateway na internet indicando que a solicitação do cliente obteve acesso à VPC.

É compatível com o site voltado para o cliente.

Gateway privado virtual

É um componente que permite a comunicação segura entre a sua rede local e uma Virtual Private Cloud (VPC) na AWS.



Cria uma conexão VPN entre a VPC e a rede corporativa interna.

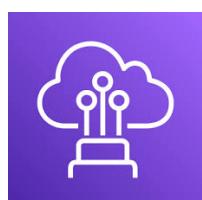
Quando você deseja acessar recursos privados em uma VPC, o gateway privado virtual cria uma conexão segura. Ele criptografa o tráfego, garantindo

que os dados transmitidos entre sua rede e a VPC estejam protegidos de acessos não autorizados.

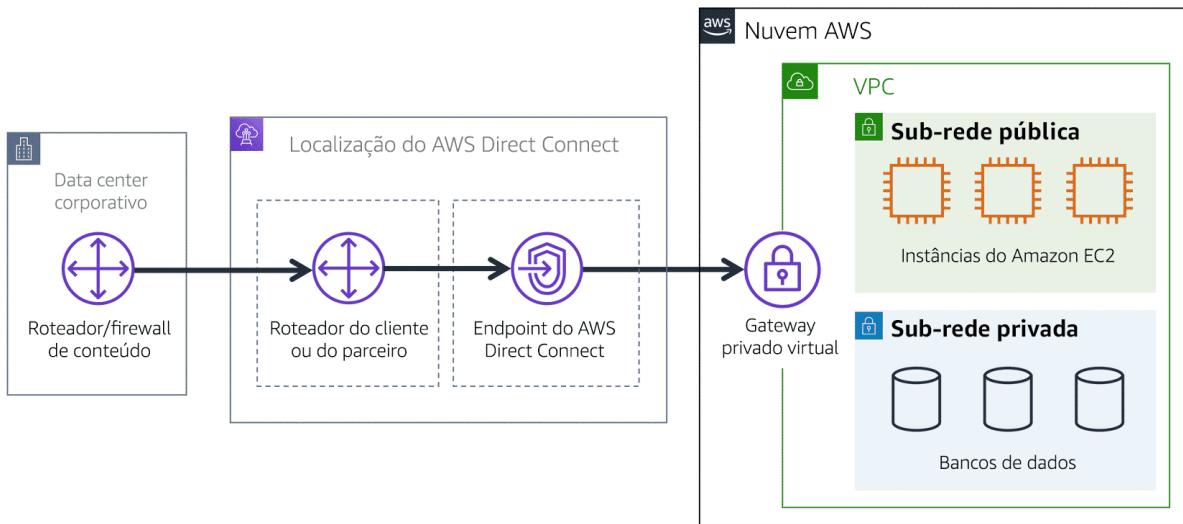
Mesmo que você esteja usando a mesma infraestrutura de rede que outros usuários, a conexão via gateway privado virtual oferece uma camada adicional de segurança, permitindo que você acesse recursos internos sem expô-los diretamente à internet.

O gateway privado virtual é fundamental para garantir que o tráfego entre sua rede e a VPC seja seguro e criptografado, permitindo um acesso controlado a recursos privados na nuvem da AWS.

AWS Direct Connect



é um serviço que permite criar uma conexão privada e dedicada entre seu data center e uma Virtual Private Cloud (VPC) na AWS.



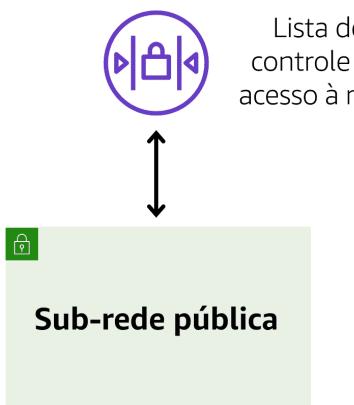
Um data center corporativo roteia tráfego de rede para uma localização do AWS Direct Connect. Em seguida, esse tráfego é roteado para uma VPC por meio de um gateway privado virtual. Todo o tráfego de rede entre o data center corporativo e a VPC passa por essa conexão privada dedicada.

Com o Direct Connect, você pode se conectar diretamente à AWS, evitando a internet pública. Isso resulta em maior segurança, menor latência e uma conexão mais estável.

O AWS Direct Connect é uma solução ideal para empresas que precisam de uma conexão confiável e segura entre suas instalações e a AWS, facilitando o acesso a recursos na nuvem de forma dedicada.

Sub-redes e listas de controle de acesso à rede

ACLs de rede



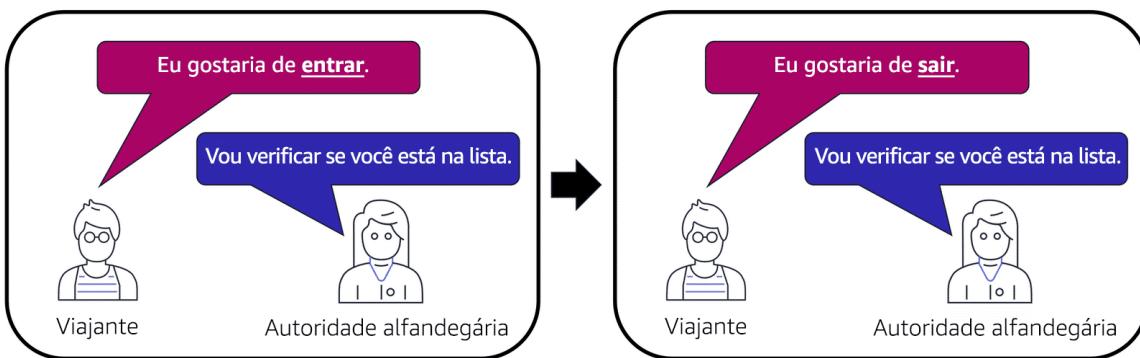
Uma ACL de rede é um firewall virtual que controla o tráfego de entrada e saída em uma sub-rede dentro de uma Virtual Private Cloud (VPC).

A ACL examina os pacotes de dados que tentam entrar ou sair da sub-rede e aplica regras específicas para permitir ou negar o tráfego.

As ACLs de rede são essenciais para gerenciar e proteger o tráfego de dados em uma VPC, permitindo um controle rigoroso sobre quais pacotes podem acessar a sub-rede.

Filtragem de pacotes STATELESS

As ACLs de rede executam 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.



Grupos de Segurança

Um grupo de segurança é um firewall virtual que controla o tráfego de entrada e saída de uma instância do Amazon EC2.

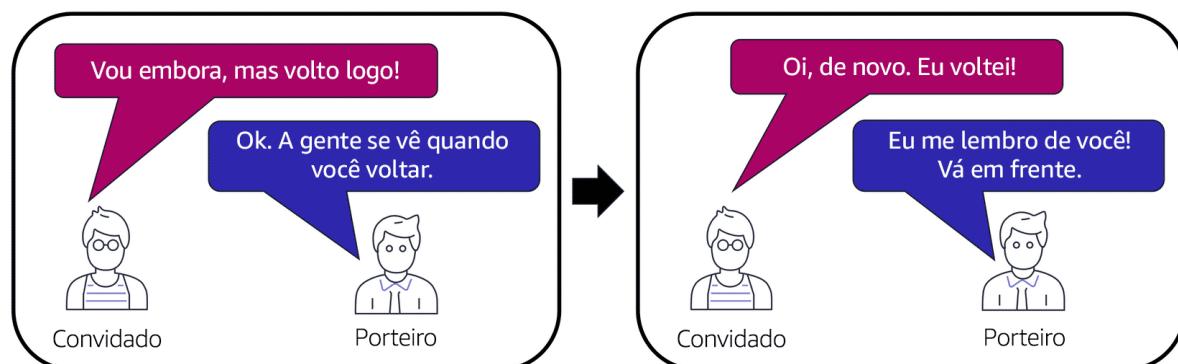
Configuração Padrão: Por padrão, um grupo de segurança nega todo o tráfego de entrada e permite todo o tráfego de saída.

Isso significa que, para permitir a comunicação, você deve adicionar regras

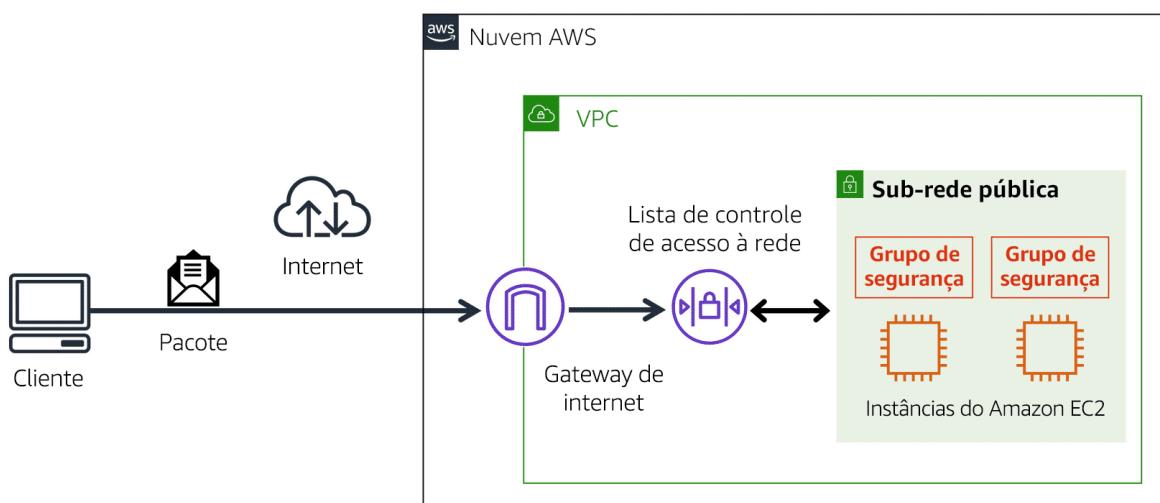
específicas. (Essas regras podem ser baseadas em endereços IP, protocolos e portas.)

Filtragem de pacotes STATEFUL

Os grupos de segurança fazem a filtragem de pacotes **stateful**. Eles se lembram de decisões anteriores tomadas para pacotes recebidos.



Com as ACLs de rede e os grupos de segurança, você pode configurar regras personalizadas para o tráfego na sua VPC. Conforme você sabe mais sobre a segurança e a rede da AWS, entenda as diferenças entre ACLs de rede e grupos de segurança.



Um pacote viaja pela internet de um cliente para o gateway de internet e para a VPC. Em seguida, o pacote passa pela lista de controle de acesso à rede e acessa a sub-rede pública, na qual estão localizadas duas instâncias do EC2.

Amazon Route 53



O Amazon Route 53 é um serviço de DNS (Sistema de Nomes de Domínio) da AWS que ajuda a rotear usuários para aplicativos da internet hospedados na AWS.

Conectando solicitações de usuários à infraestrutura da AWS, como instâncias do Amazon EC2 e平衡adores de carga, também podendo direcionar usuários para serviços fora da AWS.

permite que você registre novos domínios ou transfira registros DNS de domínios existentes de outros registradores. Isso facilita o gerenciamento de todos os seus domínios em um único local.

Integração com Amazon CloudFront

- O Amazon Route 53 pode trabalhar em conjunto com o Amazon CloudFront, um serviço de entrega de conteúdo, para fornecer conteúdo de forma eficiente aos clientes.

Exemplo:

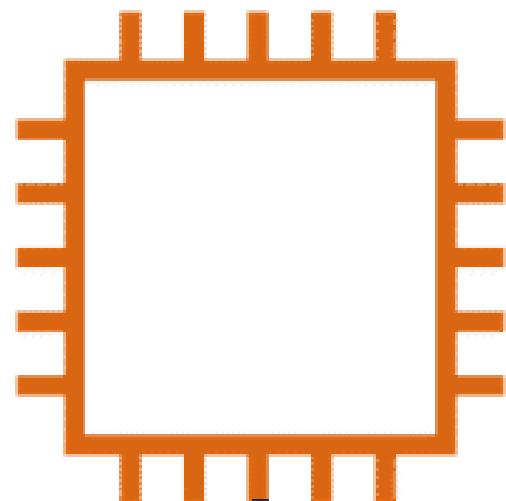
1. Um cliente solicita dados da aplicação acessando o site da AnyCompany.
2. O Amazon Route 53 usa a resolução de DNS para identificar o endereço IP correspondente da AnyCompany.com, 192.0.2.0. Essas informações são enviadas de volta para o cliente.
3. A solicitação do cliente é enviada para o local de borda mais próximo por intermédio do Amazon CloudFront.
4. O Amazon CloudFront se conecta ao Application Load Balancer, que envia o pacote de entrada para uma instância do Amazon EC2.

Armazenamentos de instância e Amazon Elastic Block Store (Amazon EBS)



O Amazon EC2 fornece CPU, memória, rede e armazenamento, sendo o armazenamento em nível fundamental para as aplicações que estão em execução, Sendo esse armazenamento denominado de “armazenamento de instância (instance store)”.

Instância do Amazon EC2



Armazenamento de instância com dados



Contudo, esses volumes são voláteis; se a instância for interrompida, todos os dados neles são perdidos, eles são adequados para dados temporários ou facilmente recriáveis, mas não para informações importantes.



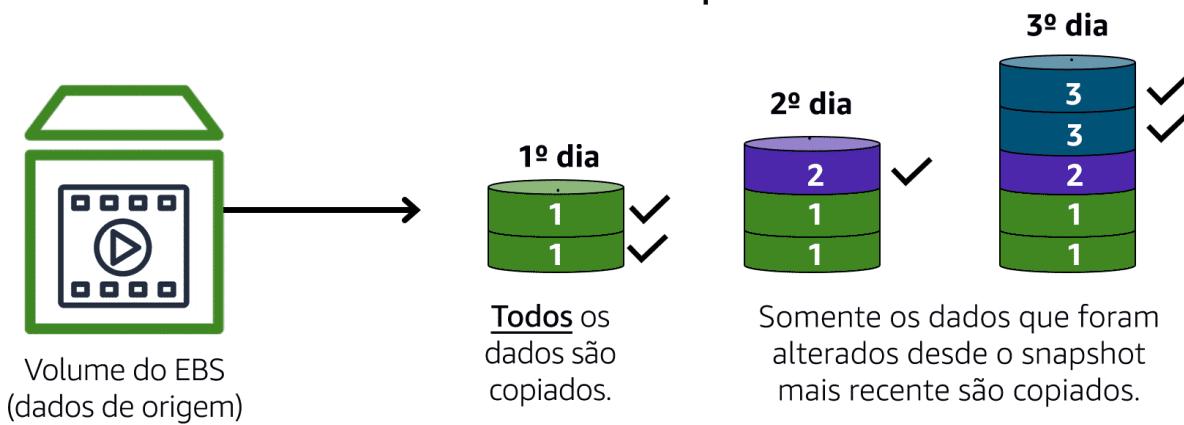
Para garantir o armazenamento dos dados que entra no **Amazon Elastic Block Store (EBS)**.

Permitindo a criação de volumes virtuais que podem ser anexados a instâncias EC2, mantendo os dados mesmo após a interrupção da instância. Os volumes do EBS podem ser configurados em diferentes tamanhos e tipos.

É crucial fazer backups regulares dos volumes do EBS através de snapshots, garantindo a recuperação de dados em caso de corrupção.

Snapshots do Amazon EBS

Snapshots do EBS

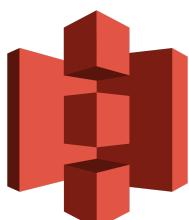


Backups incrementais de volumes do EBS criando snapshots do Amazon EBS. No dia 1, dois volumes são salvos em backup. No dia 2, um novo volume é adicionado e salvo em backup. No dia 3, são adicionados mais dois volumes para um total de cinco volumes. Somente os dois novos volume são salvos em backup.

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 EC2 quanto o volume do EBS precisam residir na mesma Zona de Disponibilidade.

Amazon Simple Storage Service (Amazon S3)



É um serviço de armazenamento que permite guardar e recuperar uma quantidade praticamente ilimitada de dados. Os dados são armazenados como objetos em **buckets**, com um tamanho máximo de 5 terabytes por objeto.

O S3 oferece recursos como gerenciamento de objetos e permissões de acesso.

Existem diferentes classes de armazenamento no S3:

1. **S3 Standard**: Alta durabilidade (99,99999999%) e ideal para dados acessados com frequência.
2. **S3 Standard-IA (Infrequent Access)**: Para dados acessados menos frequentemente, como backups e arquivos de recuperação de desastres.
3. **S3 One Zone-IA (One Zone)**: Armazena dados em uma única Zona de Disponibilidade.
4. **Intelligent-Tiering**: Se um objeto não for acessado por 30 dias consecutivos, ele é movido automaticamente para a classe de acesso pouco frequente (S3 Standard-IA). Se o objeto for acessado novamente, o S3 o moverá de volta para o nível de acesso frequente (S3 Standard).
5. **S3 Glacier Instant Retrieval**: ideal para dados arquivados que requerem acesso imediato. Esta classe permite recuperar objetos em apenas alguns milissegundos
6. **S3 Glacier Flexible Retrieval**: Para arquivamento de dados que precisam ser retidos por longos períodos, com opções de recuperação que variam de minutos a horas. Políticas de vault-lock podem ser aplicadas para conformidade.
7. **S3 Glacier Deep Archive**: é uma storage class de baixo custo, projetada para arquivamento de longo prazo e preservação digital
8. **Outposts**: é uma extensão do Amazon S3 que permite criar buckets de armazenamento de objetos diretamente no seu ambiente on-premises do AWS Outposts

O S3 também permite a configuração de políticas de ciclo de vida, que movem dados automaticamente entre classes de

armazenamento conforme critérios definidos. Outras classes incluem S3 One Zone-IA, S3 Glacier Instant Retrieval e S3 Glacier Deep Archive.

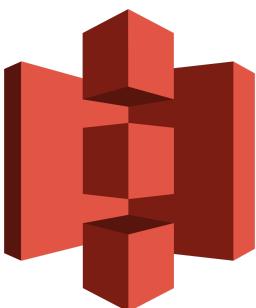
Amazon EBS vs. Amazon S3

Amazon EBS (Elastic Block Storage):



- **Armazenamento de Blocos:** Permite volumes de até 16 tebibytes.
- **Persistência:** Os dados permanecem mesmo após o encerramento das instâncias do EC2.
- **Eficiente para Edições:** Ideal para arquivos que precisam ser editados frequentemente, como vídeos. As alterações são feitas apenas nos blocos relevantes, tornando o processo mais rápido e econômico em termos de largura de banda.
- Para tarefas que exigem múltiplas microedições, o EBS é a melhor escolha.

Amazon S3 (Simple Storage Service):



- **Armazenamento de Objetos:** Suporta armazenamento ilimitado com objetos de até 5.000 gigabytes.
- **Alta Durabilidade:** Oferece 99,99999999% de durabilidade, tornando-o uma excelente opção para backup.
- **Caso de Uso Ideal:** Perfeito para armazenar e distribuir arquivos, como imagens e documentos, especialmente quando não se requer atualizações frequentes. A URL de cada objeto permite controlar o acesso e a distribuição facilmente.

- Para aplicações que envolvem upload e visualização de imagens, o S3 é a escolha mais econômica e eficiente.

Considerações Finais

- **Decisão Baseada na Carga de Trabalho:** O vencedor entre EBS e S3 depende das necessidades específicas de armazenamento. O S3 é ideal para arquivos completos e situações com acesso menos frequente, enquanto o EBS é melhor para tarefas que requerem múltiplas atualizações e edições em arquivos grandes.
- **Escolha do Serviço:** Compreender suas necessidades de armazenamento ajudará a determinar qual serviço se encaixa melhor em seu caso de uso.

Amazon Elastic File System (Amazon EFS)



O EFS é um sistema de arquivos gerenciado que permite armazenamento de arquivos compartilhados para aplicações empresariais, fazendo também backups e redundância.

Ideal para situações em que várias instâncias de servidores precisam acessar grandes quantidades de dados simultaneamente, como em análises de dados.

- O EFS escala automaticamente conforme os dados são adicionados, sem necessidade de intervenções manuais. Isso significa que ele aumenta ou diminui de tamanho conforme a demanda, funciona como um verdadeiro sistema de arquivos, permitindo operações de leitura e gravação por múltiplas instâncias ao mesmo tempo, tornando-o ideal para aplicações que exigem compartilhamento de dados.

O Amazon Elastic File System 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 on-premises podem acessar o Amazon Elastic File System usando o AWS Direct Connect.

Amazon Relational Database Service (Amazon RDS)

Sistemas de Gerenciamento de Bancos de Dados Relacionais (RDBMS)

Um RDBMS permite a relação de dados armazenados, facilitando a identificação de padrões, como oferecer descontos a clientes frequentes.

- **Armazenamento de Dados:** Os dados são organizados em **tabelas** (ex.: tabela de clientes e tabela de endereços).
- **Relacionamento de Tabelas:** As tabelas podem ser **relacionadas** por atributos comuns, permitindo consultas integradas.
- **Consultas:** A linguagem SQL é utilizada para consultar dados em RDBMS.
- **Sistemas Compatíveis:** A AWS suporta vários RDBMS populares, como MySQL, PostgreSQL, Oracle e Microsoft SQL Server.
- **Migração para a Nuvem:** A migração pode ser feita por meio de **lift and shift**, movendo bancos de dados para **Amazon EC2**, ou utilizando o **Amazon Relational Database Service (RDS)**.

Amazon RDS



O Amazon RDS é um serviço gerenciado que facilita a configuração, operação e escalabilidade de bancos de dados relacionais na nuvem. Suas principais características incluem backups automáticos, escalabilidade, alta disponibilidade em várias zonas e suporte a diversos motores de banco de dados.

- Gerenciamento automatizado de tarefas como:

- Aplicação de patches, Backups, Alta disponibilidade e failover, Recuperação de desastres
- Permite que as empresas foquem mais em seus negócios e menos na administração de bancos de dados.

Amazon Aurora



O Amazon Aurora é uma solução de **banco de dados relacional** que combina desempenho elevado, alta disponibilidade e escalabilidade flexível, utilizando uma arquitetura nativa da nuvem e tecnologias de código aberto. Ele facilita o gerenciamento de dados e reduz os custos de infraestrutura, apresentando-se como uma opção eficiente para empresas.

- **Performance:** Oferece uma versão gerenciada dos RDBMS MySQL e PostgreSQL com melhor desempenho que as versões padrão.
- **Replicação e Escalabilidade:**
 - Mantém seis cópias dos dados em diferentes zonas de disponibilidade.
 - Possibilidade de adicionar até 15 réplicas de leitura para melhorar a performance.
- **Backup e Recuperação:**
 - Backups contínuos são armazenados no **S3**.
 - Oferece **Point in Time Recovery** para restaurar o banco de dados a um estado específico.

RDS: Melhor para análises complexas e dados altamente inter-relacionados.

Amazon DynamoDB



O **Amazon DynamoDB** é um banco de dados NoSQL **sem servidor** (serverless) que elimina a necessidade de gerenciar a infraestrutura, cuidando automaticamente do armazenamento.

Os dados são organizados em **tabelas**, onde cada tabela armazena **itens** (unidades de dados) e **atributos** (propriedades dos itens). Você pode adicionar ou remover atributos a qualquer momento.

Escalabilidade e Desempenho

- **Escalabilidade:** O DynamoDB se adapta automaticamente, suportando desde um único item até milhões, com armazenamento redundante em várias zonas de disponibilidade.
- **Desempenho:** Ele oferece tempos de resposta em milissegundos, essencial para aplicações com muitos usuários.

Comparação com Bancos de Dados Relacionais

- **Relacionais (ex: MySQL):** Usam SQL, possuem esquemas rígidos e requerem relacionamentos entre tabelas, podendo enfrentar problemas de desempenho com altas cargas.
- **NoSQL (ex: DynamoDB):** Flexíveis, sem esquemas rígidos, ideais para conjuntos de dados variados e acessos massivos.

Consultas

As consultas no DynamoDB se baseiam em atributos definidos como **chaves** e são mais simples, focando em um conjunto de itens em uma única tabela.

Casos de Uso

O DynamoDB é excelente para conjuntos de dados com formatos variáveis e foi testado em situações de alta escala, como no Prime Day de 2019, onde lidou com 7,11 trilhões de chamadas de API em 48 horas.

Conclusão

O Amazon DynamoDB é um banco de dados NoSQL gerenciado e escalável, ideal para aplicações que exigem flexibilidade, desempenho rápido e capacidade de lidar com grandes volumes de dados. É perfeito para cenários em que a estrutura dos dados pode mudar e a velocidade de resposta é crucial.

DynamoDB: Melhor para dados simples e requisitos de alta escalabilidade e desempenho.

Amazon Redshift



Nos negócios, precisamos não apenas de dados em tempo real, mas também de análises históricas. Os **data warehouses** são essenciais para isso, permitindo analisar dados passados e responder perguntas importantes para **Business Intelligence (BI)**, como o desempenho de vendas em diferentes fontes, como estoque e finanças.

Os bancos de dados relacionais são ótimos para operações em tempo real, mas podem ter dificuldades com grandes volumes de dados, especialmente com a crescente quantidade de informações da IoT. Além disso, fazer consultas em múltiplos bancos de dados pode ser complicado.

Data warehouses são projetados para armazenar dados históricos e possibilitar análises profundas, como quantas vendas ocorreram em um determinado período. Isso é diferente de consultas em tempo real, como verificar o estoque disponível.

O **Amazon Redshift** é um serviço de data warehouse da AWS que facilita a análise de grandes volumes de dados:

- **Escalabilidade:** Pode lidar com petabytes de dados e consultar até exabytes diretamente de um data lake.
- **Desempenho:** Oferece até 10 vezes mais desempenho que bancos de dados tradicionais para inteligência de negócios.
- **Gerenciamento Simplificado:** Reduz a carga operacional, permitindo que os usuários se concentrem na análise de dados, em vez da manutenção.

Em resumo, quando você precisa extrair insights de grandes volumes de dados para decisões informadas, o **Amazon Redshift** é a solução ideal.

AWS Database Migration Service



O **Amazon Database Migration Service (DMS)** facilita a migração de bancos de dados para a nuvem de maneira segura e sem parar as operações. Os dados podem ser transferidos entre bancos de dados diferentes, o que torna o processo flexível.

Existem duas maneiras principais de migração com o DMS:

- **Migrações homogêneas:** entre bancos de dados do mesmo tipo, como MySQL para RDS MySQL.
- **Migrações heterogêneas:** entre bancos de dados diferentes, que exigem primeiro a conversão do esquema usando a **AWS Schema Conversion Tool**.

O DMS também é útil para criar cópias de bancos de dados de produção para desenvolvimento e teste, consolidar vários bancos em um só e replicar dados continuamente, ajudando na recuperação de desastres.

Em resumo, o **Amazon DMS** torna a migração de bancos de dados fácil e eficiente, ajudando a mover dados para a nuvem sem complicações.

Serviços de banco de dados adicionais

Escolhendo o Banco de Dados e Armazenamento Certos

Na hora de selecionar um banco de dados ou uma plataforma de armazenamento, é crucial escolher a solução que melhor atende às necessidades específicas do negócio, em vez de forçar os dados a se adequarem a um banco de dados específico. Vamos revisar algumas opções de bancos de dados que a AWS oferece, cada uma projetada para finalidades específicas:

1. Amazon DynamoDB

- **Tipo:** Banco de dados NoSQL (chave-valor)
- **Uso:** Ideal para aplicações que requerem alta performance e escalabilidade, como armazenamento de dados em tempo real.

2. Amazon DocumentDB

- **Tipo:** Banco de dados de documentos
- **Uso:** Melhor para gerenciamento de conteúdo, catálogos e perfis de usuários, permitindo armazenar e consultar dados com estruturas mais complexas que simples pares de chave-valor.

3. Amazon Neptune

- **Tipo:** Banco de dados de grafos
- **Uso:** Projetado para redes sociais, mecanismos de recomendação e detecção de fraudes, permitindo monitorar relações complexas entre dados.

4. Amazon Managed Blockchain

- **Tipo:** Plataforma de blockchain
- **Uso:** Adequado para rastreamento de cadeias de suprimentos e para situações que exigem descentralização, embora não seja a solução ideal para todos os cenários.

5. Amazon QLDB (Quantum Ledger Database)

- **Tipo:** Banco de dados de ledger imutável
- **Uso:** Proporciona um registro auditável que não pode ser alterado, ideal para aplicações que requerem integridade e imutabilidade nos dados, como registros financeiros.

6. Amazon ElastiCache

- **Tipo:** Serviço de cache
- **Uso:** Adiciona uma camada de cache aos bancos de dados, reduzindo os tempos de leitura para microsegundos, melhorando drasticamente a performance geral.

7. DynamoDB Accelerator (DAX)

- **Tipo:** Cache para DynamoDB
- **Uso:** Específico para melhorar a performance de leituras em aplicações que utilizam o DynamoDB, permitindo um acesso ainda mais rápido aos dados não relacionais.

Considerações Finais

A AWS oferece uma ampla gama de serviços de banco de dados para atender a diferentes necessidades de armazenamento e consulta de dados. Cada serviço é projetado para resolver um tipo específico de problema, permitindo que as empresas escolham a solução mais adequada para suas necessidades. A chave é entender as características de cada serviço e como eles podem ser utilizados de forma otimizada para alcançar os objetivos de negócios.

Modelo de responsabilidade compartilhada da AWS

Quando falamos sobre segurança na AWS, tanto a AWS quanto o cliente têm papéis importantes:

Entidade responsável	Parte do ambiente da AWS
Cliente	Dados do cliente
	Plataforma, aplicações, Identity and Access Management (IAM)
	Configuração de sistemas operacionais, rede e firewall
	Criptografia de dados no lado do cliente, criptografia de dados no lado do servidor e proteção de tráfego de rede
Amazon Web Services (AWS)	Software: computação, armazenamento, banco de dados, rede
	Hardware: Regiões, Zonas de Disponibilidade, locais de borda

Responsabilidade do Cliente:

O cliente é responsável pela segurança na nuvem, que envolve gerenciar e configurar seus recursos. Isso inclui escolher e manter o sistema operacional das instâncias, aplicar atualizações e patches de segurança, além de controlar o acesso e a proteção de seus dados. O cliente também deve configurar os controles de acesso e as permissões de maneira adequada.

| Segurança na nuvem

Responsabilidade da AWS:

A AWS é responsável pela segurança da nuvem, que inclui a proteção da infraestrutura física (datacenters, redes, etc.) e a segurança do hypervisor. Eles garantem a segurança da camada física e oferecem documentação e auditorias para ajudar na conformidade.

Segurança da nuvem

Resumo

A AWS cuida da segurança da infraestrutura, enquanto o cliente é responsável pela configuração e proteção de seus dados e recursos. Essa compreensão é crucial para manter um ambiente seguro.

Permissões de usuário e acesso

AWS Identity and Access Management (IAM)



Serviço de configuração de permissão de acessos aos serviços e recursos.

Principais Componentes do IAM:

- **Usuários, Grupos e Perfis:** Controla quem pode acessar o quê, atribuindo permissões a indivíduos (usuários), grupos de usuários ou funções (roles) temporárias.
- **Políticas do IAM:** Define permissões usando documentos que especificam as ações que usuários ou grupos podem realizar.
- **Autenticação Multifator (MFA):** Adiciona uma camada extra de segurança, exigindo mais de uma forma de autenticação além de senha.

Práticas Recomendadas:

- Implementar o princípio do privilégio mínimo, dando a cada usuário apenas as permissões necessárias.
- Utilizar o MFA para fortalecer a segurança da conta.

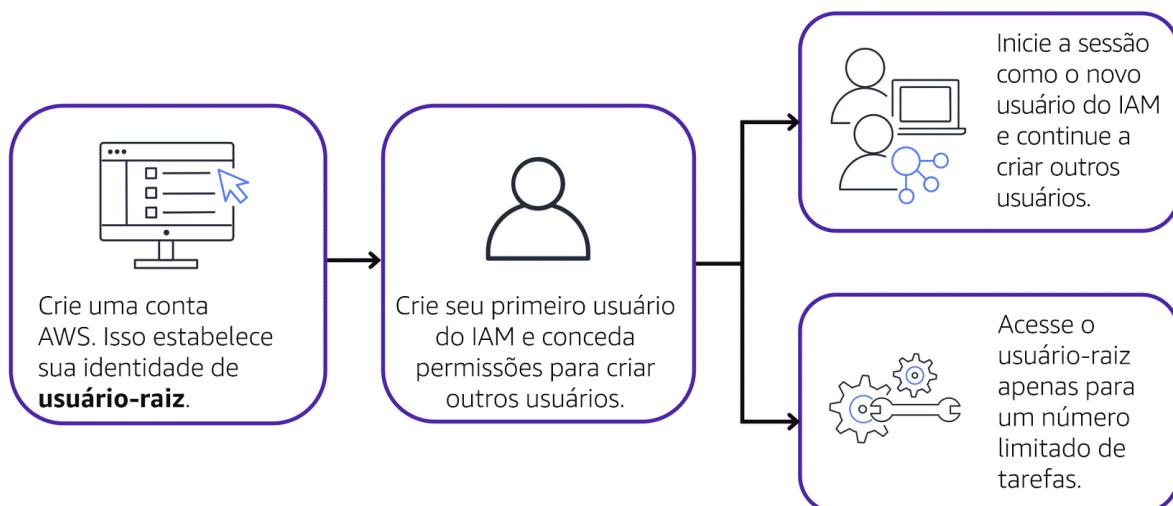
- Gerenciar o acesso por meio de grupos e políticas, facilitando a administração e aumentando a segurança.

Esses recursos e boas práticas permitem que você controle o acesso à sua infraestrutura de forma eficiente e segura.

Usuário-raiz da conta AWS

Ao criar uma conta AWS pela primeira vez, você começa com uma identidade conhecida como usuário-raiz.

O usuário-raiz é acessado ao entrar com o endereço de e-mail e a senha usados para criar a conta AWS, tendo acesso completo a todos os serviços e recursos AWS na conta.



Prática recomendada: **não** use o usuário-raiz para tarefas cotidianas.

Em vez disso, use o usuário-raiz para criar seu primeiro usuário do IAM e atribua a ele permissões para criar outros usuários.

Usuários do IAM

Identidade que você cria na AWS.

Representando uma pessoa ou o aplicativo que interage com os serviços e recursos AWS.

Consiste em um nome e credenciais.

Por padrão, ao criar um novo usuário do IAM na AWS, não há permissões associadas a ele.

Para permitir que o usuário do IAM execute ações específicas na AWS, como iniciar uma instância do Amazon EC2 ou criar um bucket do Amazon S3, você deve conceder ao usuário do IAM as permissões necessárias.

Prática recomendada: recomendamos que crie usuários individuais do IAM para cada pessoa que precisa acessar a AWS.

Políticas do IAM

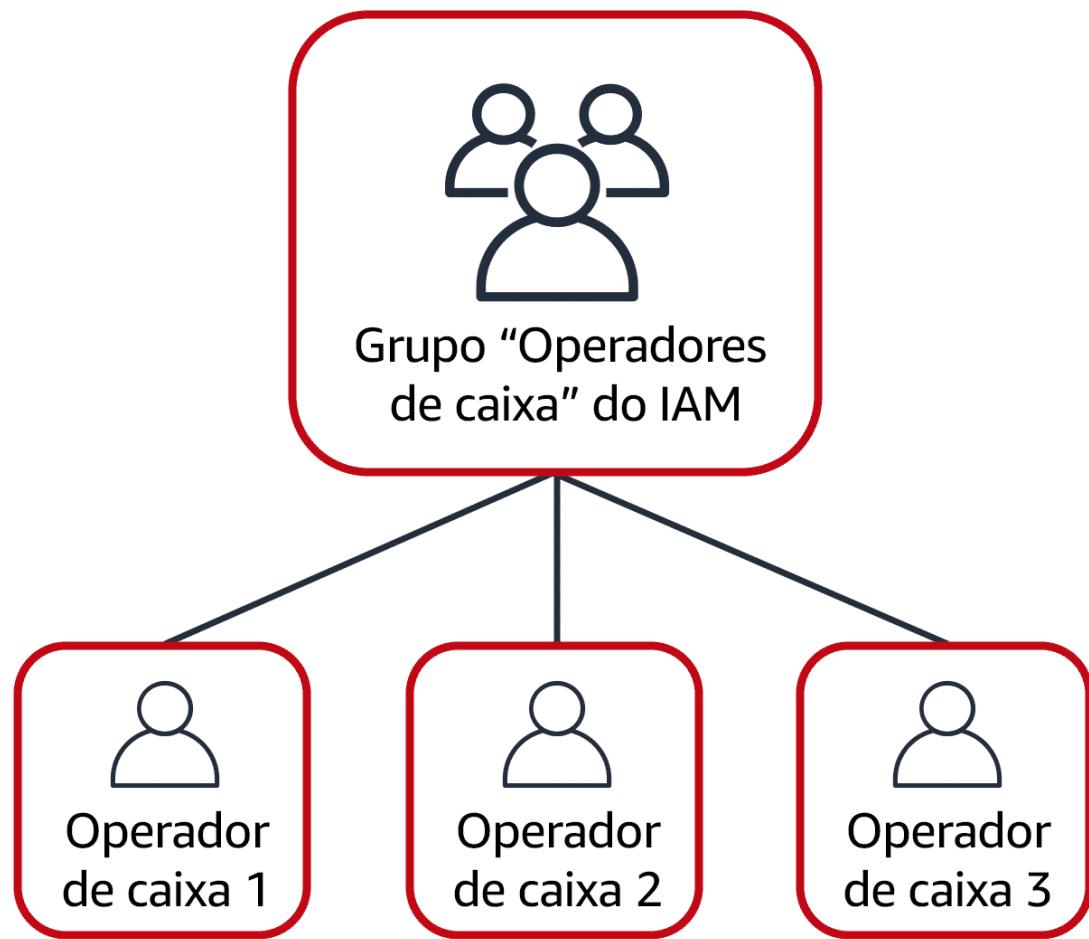
é um documento que concede ou nega permissões para serviços e recursos AWS.

As políticas do IAM permitem que você personalize os níveis de acesso dos usuários aos recursos. Por exemplo, você pode permitir que os usuários acessem todos os buckets do Amazon S3 em sua conta AWS ou apenas um bucket específico.

Prática recomendada: siga o princípio de segurança de **menor privilégio** ao conceder permissões. Seguindo esse princípio, você ajuda a impedir que usuários ou perfis tenham mais permissões do que o necessário para executar as tarefas.

Grupos do IAM

Semelhante a administração de usuários do active directory, é possível criar um grupo de usuários, aonde ao aplicar permissão nele, essa mesma permissão recai aos usuários dentro do grupo.



Perfis do IAM

Antes que um usuário, aplicação ou serviço do IAM possa assumir um perfil do IAM, ele precisa receber permissões para alternar para o perfil. Quando alguém assume uma função do IAM, ele abandona todas as permissões anteriores que tinha em uma função anterior e assume as permissões da nova função.

AWS Organizations



Conforme o número de usuários IAM aumenta, é essencial separar responsabilidades e recursos entre equipes. Para gerenciar várias contas AWS, o **AWS Organizations** oferece:

- **Gerenciamento Centralizado:** Administra múltiplas contas e permissões de forma organizada.

- **Cobrança Consolidada:** Centraliza os custos em uma conta principal, proporcionando uma visão unificada e aproveitando descontos.
- **Estrutura Hierárquica:** Agrupa contas em **Unidades Organizacionais (OUs)**, facilitando a gestão por segurança, conformidade ou orçamento.
- **Service Control Policies (SCPs):** Define permissões máximas para limitar serviços e ações nas contas.

Esses recursos garantem uma administração mais segura e eficiente de várias contas, ajustando o acesso para cada equipe.

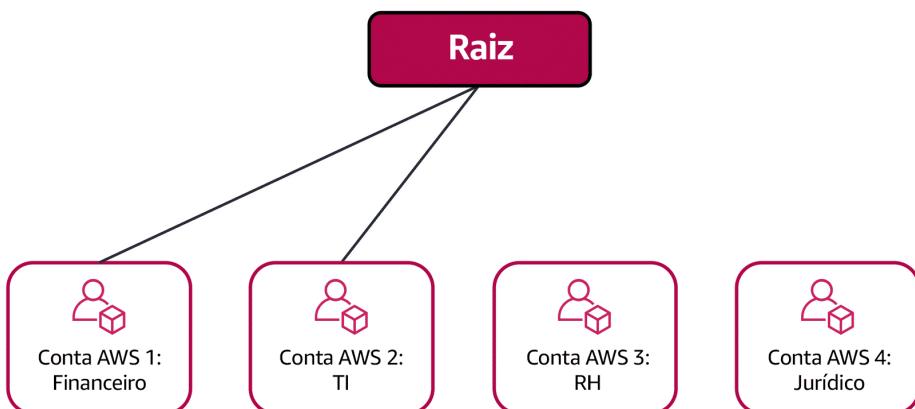
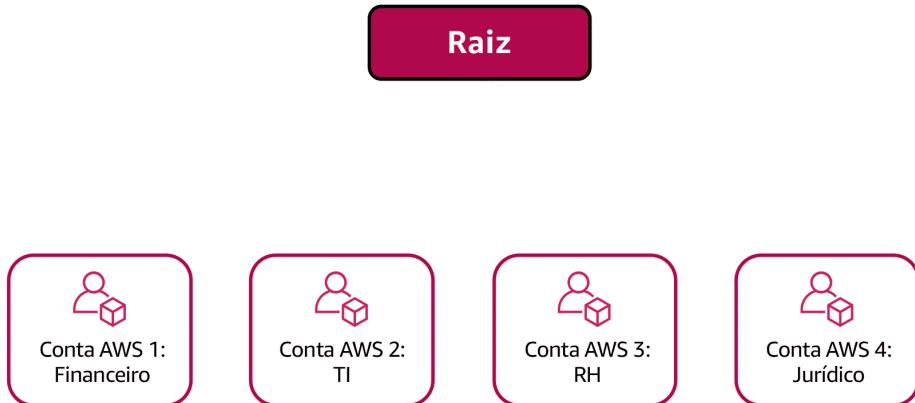
Unidades organizacionais

No **AWS Organizations**, é possível agrupar contas em **Unidades Organizacionais (UOs)** para facilitar o gerenciamento de contas com requisitos semelhantes de negócios ou segurança. Por exemplo, ao consolidar contas para os departamentos **Financeiro, TI, Recursos Humanos (RH) e Jurídico**, você pode criar UOs específicas para cada um:

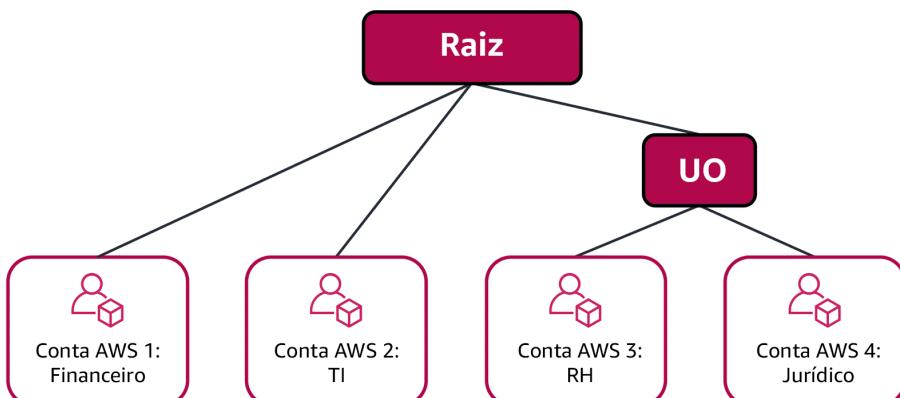
- **Financeiro:** UO com políticas que restringem o acesso a serviços para atender às exigências de conformidade.
- **TI:** UO com permissões amplas para gerenciar redes e infraestrutura.
- **RH:** UO dedicada para acessar serviços seguros de armazenamento de dados confidenciais.
- **Jurídico:** UO com acesso restrito a serviços que atendem a requisitos legais.

Essa organização garante que cada departamento tenha o acesso adequado, com segurança e controle necessários.

Exemplo:



Os departamentos financeiros e de TI têm requisitos que não se sobrepõem aos de nenhum outro departamento. Você pode trazer essas contas para sua organização para aproveitar benefícios como cobrança consolidada, mas não as colocar em nenhuma UO.



Os departamentos jurídicos e de RH precisam acessar os mesmos serviços e recursos AWS, por isso, é preciso colocá-los em uma UO juntos. Colocá-los em uma UO permite que você anexe políticas que se aplicam às contas AWS dos departamentos jurídicos e de RH.

Conclusão

Mesmo que tenha colocado essas contas em UOs, você pode continuar concedendo acesso a usuários, grupos e perfis por meio do IAM.

Ao agrupar suas contas em UOs, você pode conceder acesso facilmente aos serviços e recursos de que eles precisam. Você também impede o acesso a qualquer serviço ou recurso desnecessário.

AWS Artifact



O **AWS Artifact** é um serviço que fornece acesso a relatórios de segurança e conformidade, além de contratos online. Ele ajuda empresas a garantir que estão em conformidade com padrões regulatórios e normativos. O AWS Artifact é dividido em duas seções principais:

1. **AWS Artifact Agreements:** Permite que sua empresa revise e aceite acordos legais específicos, como emendas de processamento de dados ou outros contratos de conformidade. Isso garante que suas operações estejam alinhadas com os requisitos legais e regulatórios aplicáveis.
2. **AWS Artifact Reports:** Oferece acesso a relatórios detalhados de conformidade e auditoria, como ISO, SOC e PCI. Esses documentos são usados para comprovar que os serviços da AWS atendem aos padrões de segurança e conformidade exigidos pelo seu setor.

Essas ferramentas ajudam sua empresa a manter conformidade e facilitar auditorias.

AWS Artifact Agreements

No **AWS Artifact Agreements**, sua empresa pode visualizar, aceitar e gerenciar contratos diretamente com a AWS, relacionados ao uso de informações sensíveis em seus serviços. Isso inclui a possibilidade de assinar acordos para uma conta individual ou para todas as contas dentro do **AWS Organizations**.

Diferentes tipos de contratos estão disponíveis para atender requisitos regulatórios específicos, como a **Lei HIPAA** dos EUA, garantindo que o uso dos serviços da AWS esteja em conformidade com essas normas. Dessa forma, sua

empresa pode gerenciar de forma centralizada os acordos de conformidade necessários.

AWS Artifact Reports

O **AWS Artifact Reports** oferece à sua equipe de desenvolvimento acesso a relatórios de conformidade de auditores terceirizados, que verificaram se a AWS está em conformidade com normas e regulamentações globais, regionais e setoriais de segurança. Esses relatórios são atualizados regularmente, garantindo que as informações estejam sempre recentes.

Se um membro da equipe precisar de mais detalhes sobre as responsabilidades regulatórias de uma aplicação, o **AWS Artifact Reports** pode ser utilizado para fornecer evidências aos auditores e reguladores, demonstrando os controles de segurança adotados pela AWS.



O AWS Artifact concede acesso a documentos de segurança e conformidade da AWS, como relatórios de certificações ISO da AWS, relatórios do Payment Card Industry (PCI) e Service Organization Control (SOC).

Centro de conformidade para o cliente

O **Centro de Conformidade para o Cliente** oferece recursos para entender a conformidade da AWS. Lá, você pode ler histórias de empresas de setores regulamentados que superaram desafios de conformidade, governança e auditoria.

Você também encontra whitepapers e documentos sobre:

- Respostas da AWS a questões de conformidade

- Visão geral dos riscos e conformidade da AWS
 - Lista de verificação de segurança para auditorias
-

Ataques de negação de serviço

Um ataque de negação de serviço distribuída (DDoS) visa sobrecarregar uma aplicação para torná-la indisponível, inundando-a com tráfego excessivo e forçando a interrupção dos serviços. Um DDoS utiliza uma rede de máquinas comprometidas (botnets) que enviam múltiplas requisições à aplicação simultaneamente.

A AWS oferece diversas camadas de proteção contra esses ataques. Grupos de segurança filtram tráfego indesejado no nível de rede, bloqueando solicitações ilegítimas antes que elas alcancem suas instâncias. Elastic Load Balancer (ELB) ajuda a gerenciar tráfego HTTP, distribuindo a carga de forma eficaz para evitar sobrecarga.

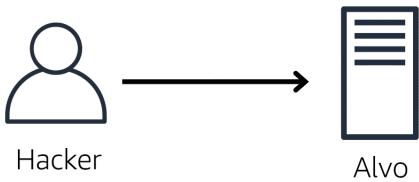
Além disso, ferramentas especializadas como o **AWS Shield** e o **AWS WAF** oferecem proteção avançada. O AWS Shield, especialmente na versão Advanced, protege contra ataques DDoS em larga escala, enquanto o AWS WAF (Web Application Firewall) filtra tráfego malicioso com base em regras configuradas e capacidades de machine learning, defendendo pró-ativamente contra novas ameaças.

Em resumo, uma arquitetura bem planejada na AWS já mitiga a maioria dos ataques DDoS, com suporte adicional de ferramentas especializadas para ataques mais sofisticados.

Ataques de negação de serviço

Um **ataque de negação de serviço (DoS)** é uma tentativa deliberada de tornar um site ou aplicação indisponível para os usuários.

Ataque de negação de serviço

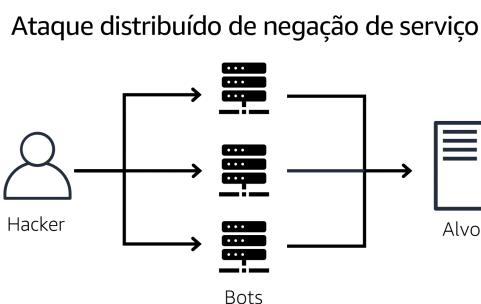


O ataque se origina de uma fonte **única**.

Por exemplo, um invasor pode inundar um site ou aplicação com tráfego excessivo de rede até que o site ou a aplicação de destino se sobrecarregue e não seja mais capaz de responder. Se o site ou aplicativo ficar indisponível, o serviço será negado aos usuários tentando fazer solicitações legítimas.

Ataques distribuídos de negação de serviço

Imagine que alguém e seus amigos repetidamente acessam um site para fazer solicitações, mesmo sem intenção de usá-lo. Essas solicitações vêm de diferentes endereços IP, tornando impossível bloquear todos. Além disso, o volume de tráfego faz com que os usuários legítimos tenham dificuldade em acessar o site. Esse cenário se assemelha a um ataque distribuído de negação de serviço (DDoS).



O ataque tem origem em **várias** fontes.

Em um ataque distribuído de negação de serviço (DDoS), várias origens são usadas para iniciar um ataque que visa tornar um site ou aplicação indisponível. O ataque pode ser feito por um grupo de invasores, ou até mesmo um único invasor. O único invasor pode usar vários computadores infectados (também conhecidos como "bots") para enviar tráfego excessivo a um site ou aplicação.

Para ajudar a minimizar o efeito de ataques DoS e DDoS em suas

aplicações, você pode usar o [AWS Shield](#)

AWS Shield



O AWS Shield é um serviço que protege aplicações contra ataques DDoS. O AWS Shield oferece dois níveis de proteção:

Standard

O **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 nas suas aplicações, o AWS Shield Standard usa diversas técnicas de análise para detectar tráfego mal-intencionado em tempo real e mitigá-lo automaticamente.

Advanced

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.

Serviços de segurança adicionais

Para proteger seu site e suas informações, é essencial garantir a segurança dos dados. Isso envolve proteger os dados tanto em repouso quanto em trânsito.

- **Criptografia em Repouso:** Isso significa proteger dados armazenados, como os do banco de dados. A criptografia é gerenciada pelo **AWS Key**

Management Service (KMS), que cuida das chaves usadas para acessar os dados.

- **Criptografia em Trânsito**: Isso se refere aos dados que estão sendo transferidos, como entre um serviço da AWS e um usuário do site. Por exemplo, o **Amazon Redshift** usa SSL (Secure Sockets Layer) para proteger os dados durante a transferência.

Serviços de Segurança:

1. **Amazon Inspector**: Realiza avaliações de segurança automatizadas. Ele verifica se há problemas, como instâncias EC2 com portas abertas. Ao habilitar o Inspector, você recebe relatórios sobre possíveis vulnerabilidades e soluções sugeridas.
2. **Amazon GuardDuty**: Monitora continuamente sua conta em busca de ameaças, analisando logs e usando machine learning. Ele identifica ameaças sem afetar o desempenho da sua infraestrutura.

Além desses, existem outros serviços de segurança na AWS, como **Shield Advanced** e **Security Hub**. Consulte a seção de Recursos para mais informações.

AWS Key Management Service (AWS KMS)



O **AWS Key Management Service (AWS KMS)** permite que você realize operações de criptografia com chaves de criptografia que são sequências aleatórias.

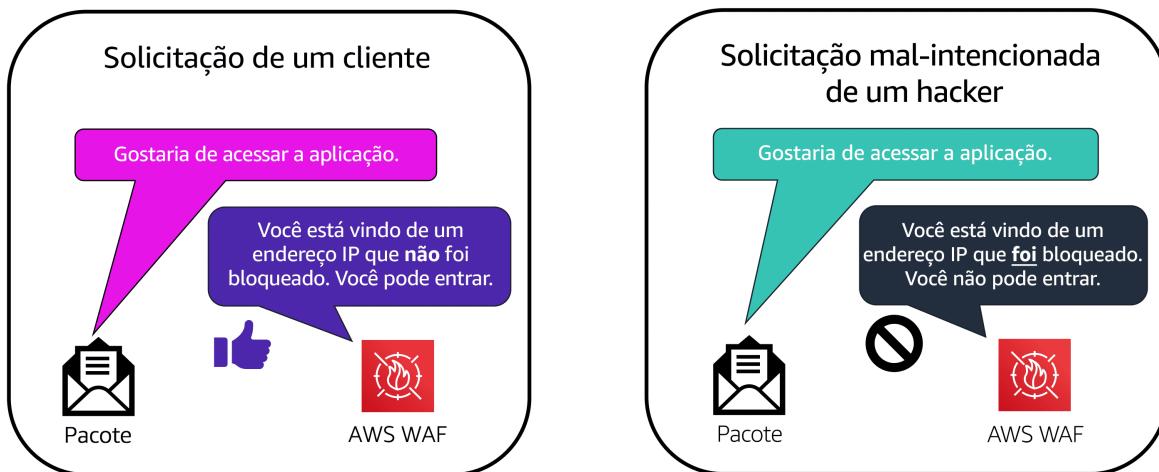
AWS WAF



O **AWS WAF** é um firewall de aplicação web que monitora as solicitações de rede que chegam às suas aplicações web.

Ele funciona em conjunto com o **Amazon CloudFront** e um **Application Load Balancer**. Semelhante às listas de controle de acesso de rede, o AWS WAF permite ou bloqueia o tráfego usando uma lista de controle de acesso (ACL) da web, protegendo seus recursos na AWS.

Você pode usar o AWS WAF para definir quais solicitações específicas devem ser permitidas ou bloqueadas, garantindo a segurança das suas aplicações.



Amazon Inspector



O **Amazon Inspector** melhora a segurança e a conformidade das aplicações ao realizar avaliações de segurança automatizadas. Ele verifica os aplicativos em busca de vulnerabilidades e desvios das práticas recomendadas, como acesso aberto a instâncias do Amazon EC2 e uso de versões de software vulneráveis.

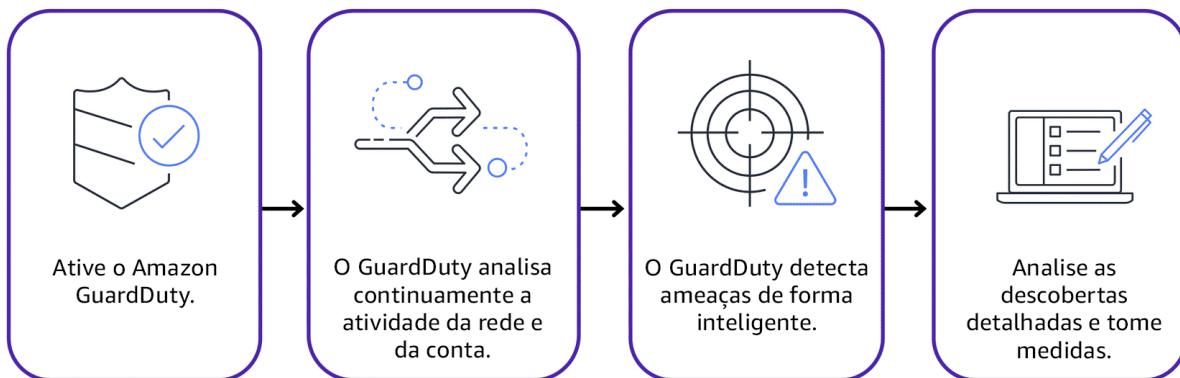
Após cada avaliação, o Amazon Inspector fornece uma lista de descobertas, priorizadas por nível de gravidade. Cada problema de segurança vem com uma descrição detalhada e recomendações para correção.

É importante lembrar que a AWS não garante que seguir essas recomendações resolverá todos os problemas de segurança. De acordo com o modelo de responsabilidade compartilhada, os clientes são responsáveis pela segurança de suas ferramentas, aplicativos e processos executados nos serviços da AWS.

Amazon GuardDuty



Serviço que detecta ameaças de forma inteligente, pois o mesmo monitora a rede e o comportamento das atividades.



O GuardDuty realiza uma análise em dados de várias fontes, incluindo logs de fluxo de VPC e logs de DNS

Se o GuardDuty detectar ameaças, você poderá analisar as descobertas detalhadas no console de gerenciamento da AWS. 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.

Amazon CloudWatch



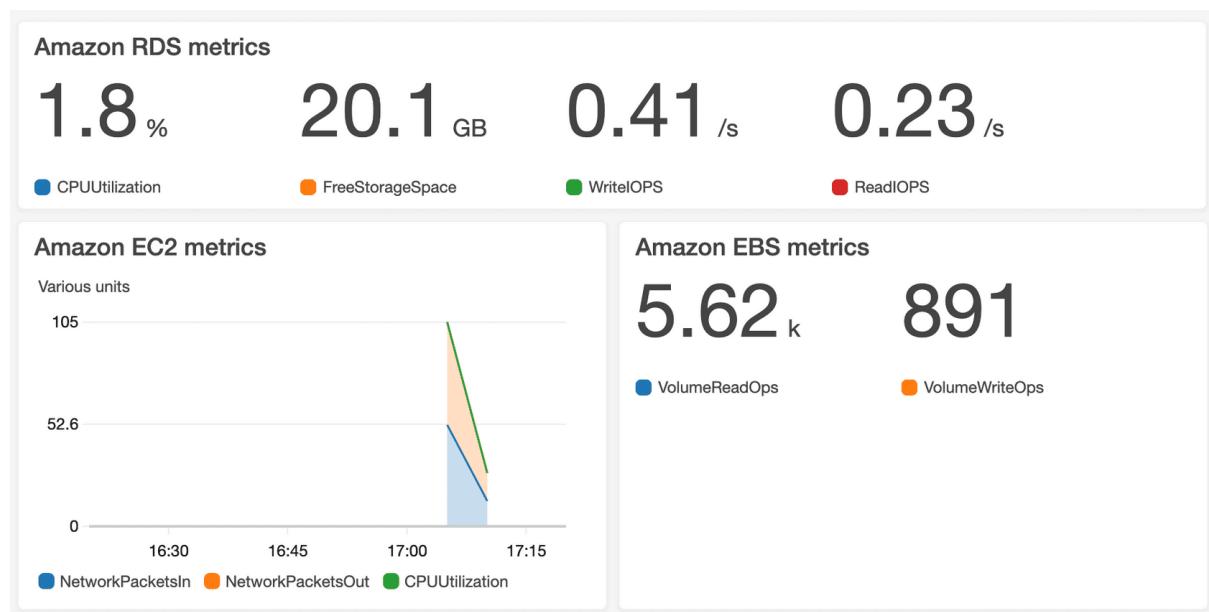
Para saber do funcionamento ao longo do dia, não podemos ficar olhando o tempo todo. portanto é importante receber alertas automáticos em caso de problemas e ter registro do que ocorreu em seu ambiente, portanto, essa prática de acompanhar sistemas pode ser realizado pelo **CloudWatch**

Na nuvem, é importante configurar o monitoramento, pois os serviços da AWS mudam automaticamente. Por exemplo, se uma instância do EC2 estiver sobrecarregada, você pode iniciar outra instância automaticamente. Se uma aplicação

começar a gerar muitos erros, o monitoramento pode alertar você.

O **Amazon CloudWatch** permite monitorar e gerenciar métricas e configurar alarmes, essas métricas mencionadas se convertem em gráficos que mostram as mudanças.

Painel do CloudWatch



Por exemplo, você pode usar um painel do CloudWatch para monitorar a utilização da CPU de uma instância do Amazon EC2, o número total de solicitações feitas para um bucket do Amazon S3 e muito mais. Você pode até personalizar painéis separados para diferentes fins comerciais, aplicativos ou recursos.

AWS CloudTrail



O AWS CloudTrail é um serviço essencial para auditoria de **chamadas de API**.

Ele registra todas as solicitações feitas ao seu ambiente, como iniciar uma instância EC2 ou alterar permissões de usuário. Isso inclui informações detalhadas, como:

O que aconteceu?	Um novo usuário do IAM (Mary) foi criado.
Quem fez a solicitação?	Usuário do IAM John
Quando isso ocorreu?	1º de janeiro de 2020, às 9:00
Como a solicitação foi feita?	Por meio do console de gerenciamento da AWS

- Qual operação foi realizada
- Quem fez a solicitação
- De onde veio (endereço IP)
- Quando a chamada de API foi enviada
- Qual foi a resposta da solicitação

Esse registro é crucial para garantir a conformidade e segurança das operações em sua infraestrutura.

CloudTrail Insights

Esse recurso opcional permite que o CloudTrail detecte automaticamente atividades de API incomuns em sua conta AWS

AWS Trusted Advisor



O **AWS Trusted Advisor** é um consultor automatizado que ajuda a otimizar sua conta AWS com base em cinco pilares:
Otimização de custos, Desempenho, Segurança, Tolerância a falhas e Cotas de serviço.
Ele avalia seus recursos em tempo real, pontuando melhorias nas práticas recomendadas da AWS.

Otimização de custos



0 ✓ 9 ▲ 0 !
USD 7.516,85

Possíveis economias mensais

Desempenho



3 ✓ 7 ▲ 0 !

Segurança



2 ✓ 4 ▲ 11 !

Tolerância a falhas



0 ✓ 15 ▲ 5 !

Limites de serviço



37 ✓ 0 ▲ 1 !

Para cada categoria:

- A marca de verificação verde indica o número de itens para os quais **nenhum problema foi detectado**.

- O triângulo laranja representa o número de **investigações** recomendadas.
 - O círculo vermelho representa o número de **ações** recomendadas.
-

Nível gratuito da AWS

Com o nível gratuito da AWS, você começa a usar determinados serviços sem ter que se preocupar com o custo durante o período especificado.

Três tipos de ofertas estão disponíveis:

- Sempre gratuito
- 12 meses gratuitos
- Versões de teste

Definição de preço da AWS

- Pague somente pelo que usar
 - Pague menos ao fazer reserva
 - Pague menos com descontos baseados em volume, usar mais
-

AWS Budgets



O **AWS Budgets** é uma ferramenta essencial para quem quer manter o controle dos custos e uso dos serviços da AWS. Com ele, você pode criar orçamentos personalizados para acompanhar seu consumo e evitar surpresas com faturas elevadas. Além disso, as informações são atualizadas três vezes ao dia, o que permite um monitoramento mais próximo da realidade.

AWS Budgets							
Filter by budget name						Download CSV	Create budget
All budgets (7)	Cost budgets (5)	Usage budgets (2)	Reservation budgets (0)				
Budget name	Budget type	Current	Budgeted	Forecasted	Current vs. budgeted	Forecasted vs. budgeted	
Project Nemo Cost Budget	Cost	\$43.90	\$45.00	\$56.33	<div style="width: 97.55%; background-color: #0072bc;"></div> 97.55%	<div style="width: 125.17%; background-color: #e74c3c;"></div> 125.17%	...
Eastern US Regional Budget	Cost	\$85.21	\$100.00	\$125.28	<div style="width: 85.21%; background-color: #0072bc;"></div> 85.21%	<div style="width: 125.28%; background-color: #e74c3c;"></div> 125.28%	...
Total Monthly Cost Budget	Cost	\$141.50	\$175.00	\$187.00	<div style="width: 80.86%; background-color: #0072bc;"></div> 80.86%	<div style="width: 106.86%; background-color: #e74c3c;"></div> 106.86%	...
Total EC2 Cost Budget	Cost	\$136.90	\$200.00	\$195.21	<div style="width: 68.45%; background-color: #0072bc;"></div> 68.45%	<div style="width: 97.61%; background-color: #0072bc;"></div> 97.61%	...
S3 Usage Budget	Usage	3,601 Requests	5,500 Requests	4,675.75 Requests	<div style="width: 65.47%; background-color: #0072bc;"></div> 65.47%	<div style="width: 85.01%; background-color: #0072bc;"></div> 85.01%	...

Recursos do AWS Budgets:

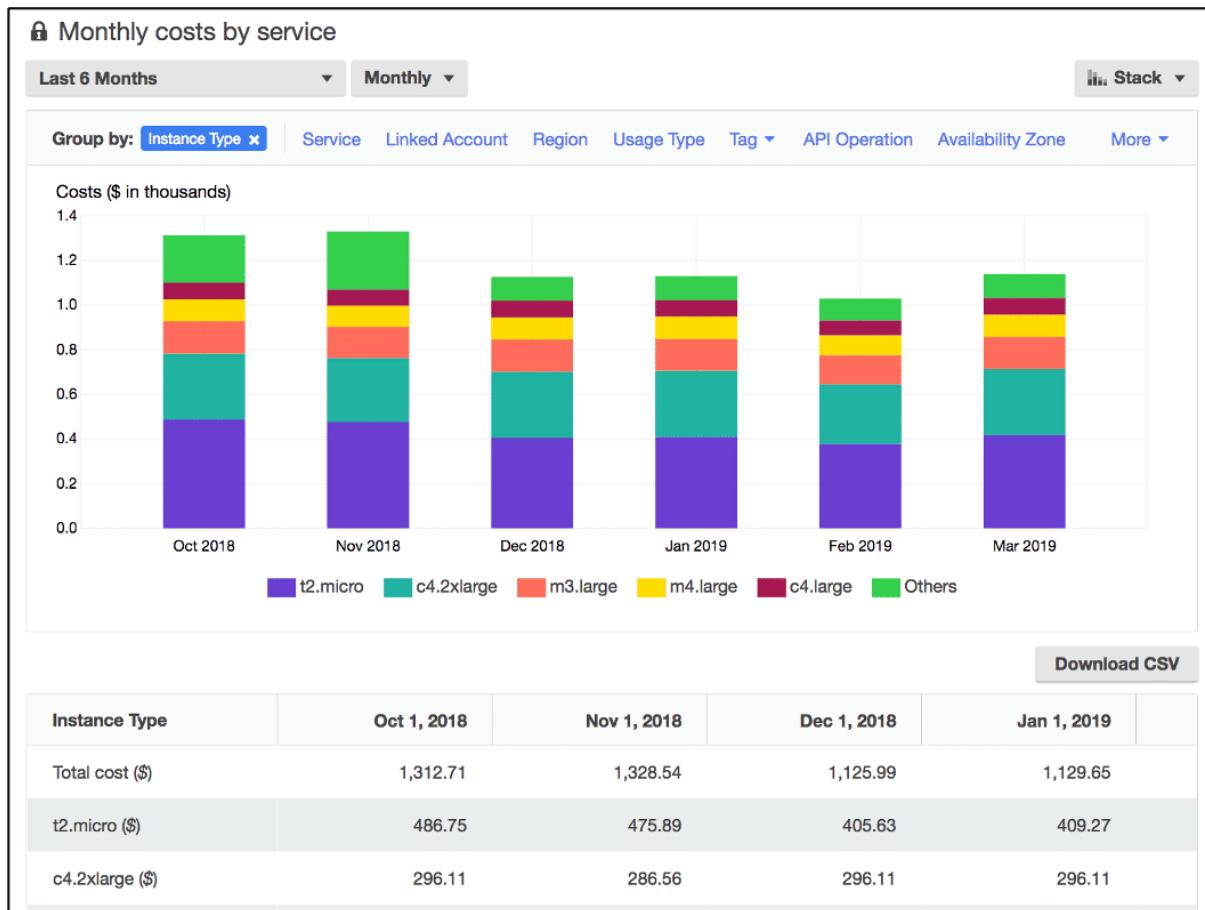
- Planejamento de custos e uso:** Permite que você crie orçamentos para serviços específicos, grupos de serviços ou toda a sua conta, baseado no uso ou no custo.
- Acompanhamento de reservas de instâncias:** Você pode monitorar suas reservas, como instâncias EC2 reservadas, ajudando a garantir que você esteja utilizando suas reservas de forma eficiente.
- Alertas personalizados:** É possível definir notificações para avisar quando você está prestes a ultrapassar seu orçamento ou os limites do nível gratuito da AWS.
- Três atualizações diárias:** Isso garante que você tenha informações quase em tempo real para ajustar suas estratégias de uso e orçamento, otimizando os recursos.

Essa ferramenta é crucial para evitar gastos inesperados, principalmente se sua conta está com muitos serviços em uso ou sob crescimento. Você também pode integrar o AWS Budgets a outros serviços, como o **AWS Cost Explorer**, para uma análise mais detalhada dos custos.

AWS Cost Explorer



O **AWS Cost Explorer** é uma ferramenta poderosa para monitorar, interpretar e otimizar seus custos e uso na AWS ao longo do tempo. Com ele, você pode gerar relatórios detalhados e personalizar as visualizações para entender melhor como os recursos da AWS estão sendo consumidos e onde os custos estão se acumulando.



Resumo dos Recursos do AWS Cost Explorer

- Visualização de Custos e Uso:** Permite acompanhar gastos e uso de recursos da AWS ao longo do tempo, ajudando a identificar padrões e tendências.
- Relatório Padrão:** Inclui um relatório pré-configurado que mostra os custos acumulados dos cinco principais serviços da AWS, facilitando a identificação dos serviços que mais consomem recursos.

3. **Filtros e Grupos Personalizados:** Oferece opções para aplicar filtros e agrupar dados conforme suas necessidades, como por serviço, conta ou região, permitindo uma análise mais detalhada.
 4. **Exibição de Uso por Hora:** Permite visualizar o uso de recursos em nível horário, útil para identificar padrões específicos, como picos de demanda ou subutilização.
-

Planos do AWS Support

Independentemente do tamanho da sua empresa, a AWS oferece opções de suporte para atender às suas necessidades específicas. Vamos explorar os principais planos disponíveis:

- **AWS Basic Support:** Inclui acesso 24/7 ao atendimento ao cliente, documentação, fóruns de suporte, Trusted Advisor e AWS Personal Health Dashboard, tudo sem custo adicional.

▼ Support do Desenvolvedor

Os clientes com um plano **Desenvolvedor do Support** têm acesso a recursos como:

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

▼ Support Empresarial

Os clientes com um plano **Empresarial do Support** têm acesso a recursos adicionais, incluindo:

- Orientação de caso de uso para identificar ofertas, recursos e serviços da 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 aplicações

▼ Support Empresarial Rápido

Além de todos os recursos incluídos nos planos Basic, Desenvolvedor e Empresarial do Support, os clientes com um plano Empresarial Rápido do Support têm acesso a:

- Um grupo de Technical Account Managers para orientar proativamente e coordenar o acesso a programas e especialistas da AWS
- A Oficina de otimização de custos (uma por ano)
- Uma equipe de suporte do Concierge para cobrança e assistência à conta
- Ferramentas para monitorar custos e desempenho por meio do Trusted Advisor e do painel/API Health

▼ Support Empresarial de Grande porte

Além de todos os recursos incluídos nos planos de suporte Basic, Desenvolvedor, Empresarial e Empresarial Rápido, os clientes com Support Empresarial de Grande Porte têm acesso a:

- Um Technical Account Manager designado para realizar orientação proativa e coordenar o acesso a programas e especialistas da AWS
- Uma equipe de suporte Concierge para cobrança e assistência à conta
- Análises de operações e ferramentas para monitorar o health
- Dias de treinamento e jogos para impulsionar a inovação
- Ferramentas para monitorar custos e desempenho por meio do Trusted Advisor e do painel/API Health

Somente os planos Empresarial, Empresarial Rápido e Empresarial de Grande Porte do Support têm todas as verificações do AWS Trusted Advisor. Desses três planos do Support, o plano Empresarial tem um custo mais baixo.

Technical Account Manager (TAM)

Os planos Empresarial Rápido e Empresarial de Grande Porte do Support inclui acesso a um

Technical Account Manager (TAM).

O TAM será seu principal ponto de contato com a AWS. Se sua empresa assina o Support Empresarial de Grande Porte ou Empresarial Rápido, o TAM educa, capacita e desenvolve sua jornada para a nuvem em toda a gama de serviços da AWS

AWS Marketplace



É um catálogo digital com milhares de ofertas de software de provedores independentes de software. Você pode usar o AWS Marketplace para encontrar, testar e comprar software que pode ser executado na AWS.



Dentro de cada categoria, você pode restringir sua pesquisa navegando pelas listas de produtos em subcategorias. Por exemplo, as subcategorias na categoria DevOps incluem áreas como Desenvolvimento de aplicações, Monitoramento e Teste.

AWS Cloud Adoption Framework (AWS CAF)

Migrar para a nuvem é um processo complexo que requer esforço.

O

AWS Cloud Adoption Framework foi criado pela equipe de **Professional Services da AWS** para orientar empresas em suas migrações, oferecendo orientações detalhadas.

O Framework abrange seis áreas principais, divididas em dois grupos:

1. **Corporativas**: Negócios, Pessoas e Governança.
2. **Técnicas**: Plataforma, Segurança e Operações.

Cada perspectiva é importante para envolver diferentes equipes, como desenvolvedores, arquitetos de nuvem, analistas comerciais e RH. Ao identificar lacunas de habilidades e processos, a empresa pode criar um plano de ação para garantir uma migração tranquila para a nuvem.

▼ Corporativas

▼ Perspectiva de negócio

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.

Os perfis comuns na 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 perfis organizacionais, novos requisitos de habilidades e processos e identificar lacunas. Isso ajuda a priorizar treinamento, pessoal e mudanças organizacionais.

Os perfis comuns da perspectiva de pessoas são:

- Recursos humanos
- Equipe
- Gerentes de pessoas

▼ Perspectiva de governança

A **perspectiva de governança** se concentra nas habilidades e processos para alinhar a estratégia de TI à estratégia 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.

Os perfis comuns na perspectiva de governança são:

- Chief Information Officer (CIO)
- Gerentes do programa
- Enterprise architect
- Analistas de negócios
- Gerentes de portfólio

▼ Técnicas

▼ Perspectiva de operações

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

Defina como os negócios diárias, 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.

Os perfis comuns da perspectiva de operações são:

- Gerentes de operações de TI
- Gerentes de suporte de TI

▼ 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.

Os perfis comuns da perspectiva de segurança são:

- Chief information security officer (CISO)
- Gerentes de segurança de TI
- Analistas de segurança de TI

▼ Perspectiva de plataforma

A **perspectiva de plataforma** inclui princípios e padrões para implementação de novas soluções na nuvem e migração de cargas de trabalho on-premises 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.

Os perfis comuns da perspectiva de plataforma são:

- Chief Technology Officer (CTO)
 - Gerentes de TI
 - Arquitetos de soluções
-

Seis estratégias de migração

Na migração para a AWS, existem seis opções conhecidas como os "Seis Rs" que ajudam a escolher a melhor estratégia para mover aplicações e sistemas do ambiente on-premises para a nuvem. Essas opções são baseadas em fatores como tempo, custo e criticidade:

1. **Redefinir a hospedagem (Lift & Shift):** Move as aplicações sem alterações, trazendo benefícios imediatos, como até 30% de economia, e facilita a otimização futura.
2. **Redefinir plataforma (Lift-tinker-and-shift):** Pequenas otimizações são feitas sem alterar o código, como mover um banco de dados para o Amazon RDS.
3. **Retirar:** Identificar e remover aplicações obsoletas, economizando recursos.
4. **Reter:** Manter temporariamente algumas aplicações que estão em vias de serem desativadas, evitando migração desnecessária.
5. **Recomprar:** Substituir soluções legadas por novas, como mudar de CRM ou banco de dados, com potencial para grandes benefícios.
6. **Refatorar:** Reescrever o código para aproveitar ao máximo os recursos da nuvem, o que demanda mais planejamento, mas pode trazer grandes

vantagens de desempenho e recursos.

Escolher a estratégia certa para cada aplicação é essencial para garantir uma migração bem-sucedida.

AWS Snow Family

A **AWS Snow Family** oferece soluções para transferir grandes volumes de dados para a AWS de forma eficiente, quando a internet ou o Direct Connect são insuficientes.

A família inclui três dispositivos principais:



1. **AWS Snowcone**: Pequeno, portátil e com até 8 TB de armazenamento. Além de transferência de dados, suporta computação de borda com Amazon EC2 e AWS IoT Greengrass.
2. **AWS Snowball Edge**: Oferece duas versões - "Compute Optimized" e "Storage Optimized". Pode armazenar mais dados (até dezenas de terabytes) e realizar processamento local com suporte para AWS Lambda e Amazon EC2.
3. **AWS Snowmobile**: Um enorme contêiner de 13,7 metros com capacidade para 100 petabytes de dados. Ideal para migrações massivas, como desligamentos de datacenters.

Todos os dispositivos garantem segurança com criptografia de 256 bits e opções de gerenciamento de chaves através do AWS Key Management Service. Eles são projetados para lidar com grandes volumes de dados em locais remotos e difíceis, garantindo integridade e segurança durante o transporte.



AWS SnowBall

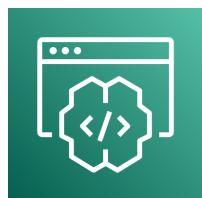


AWS SnowBall Edge



AWS Snowmobile

Amazon CodeWhisperer



O **Amazon CodeWhisperer** é uma ferramenta de codificação assistida por inteligência artificial que ajuda desenvolvedores a criar código mais rápido e com mais segurança. Ele funciona dentro do ambiente de desenvolvimento integrado (IDE), oferecendo sugestões automáticas de código com base em comentários e no código que o desenvolvedor está escrevendo.

Principais benefícios:

- **Sugestões inteligentes:** Gera automaticamente funções e blocos de código com base em descrições de comentários em inglês, economizando tempo e esforço.
- **Adaptação ao estilo de codificação:** Alinha-se ao estilo e convenções de nomeação do desenvolvedor.
- **Segurança incorporada:** Verifica vulnerabilidades com base em padrões como OWASP e recomendações da AWS.

- **Automatização de tarefas repetitivas:** Simplifica o desenvolvimento e permite que os desenvolvedores se concentrem em partes críticas dos projetos.
- **Proteção de código aberto:** Identifica referências a códigos de software de código aberto, ajudando a garantir o uso legal e seguro de bibliotecas.

Isso acelera o desenvolvimento de aplicações, melhora a segurança e a qualidade do código, e reduz o tempo dedicado a aprender novas linguagens ou funções.

Amazon SageMaker



Com o Amazon SageMaker, é rápido e fácil começar a trabalhar em projetos de machine learning. Você não precisa seguir o processo tradicional de reunir manualmente ferramentas e fluxos de trabalho separados.

Principais benefícios:

- **Ajuste Automático:** O SageMaker ajusta automaticamente as configurações para que seus modelos façam previsões mais precisas.
- **Use Qualquer Ferramenta:** Você pode usar diferentes ferramentas de aprendizado de máquina, incluindo as populares como TensorFlow e Apache MXNet, e até trazer suas próprias.
- **Funciona com Seu Trabalho:** O SageMaker se encaixa no que você já faz, ajudando na criação, treinamento e hospedagem de modelos.
- **Algoritmos Rápidos:** Oferece algoritmos que trabalham mais rápido com grandes quantidades de dados, até dez vezes mais rápido que outros serviços.

- **Exemplos Prontos:** Disponibiliza exemplos prontos de código em cadernos, para que você comece seus projetos de forma rápida.
 - **Treinamento Barato e Rápido:** O treinamento é feito rapidamente usando vários recursos ao mesmo tempo, e você só paga pelo que usar.
 - **Fácil de Usar:** Você pode colocar seus modelos em funcionamento sem precisar mudar o código da sua aplicação e ainda faz testes automáticos para garantir que tudo funcione bem.
-

Well-Architected Framework



O **Well-Architected Framework** foi criado para ajudar arquitetos, desenvolvedores e usuários da AWS a construir infraestruturas seguras, de alto desempenho, resilientes e eficientes. Ele é baseado em seis pilares que orientam a revisão e a criação de arquiteturas:

1. **Excelência Operacional:** Foca em monitorar e gerenciar sistemas para entregar valor e melhorar continuamente processos. Por exemplo, automatizar implementações com pipelines.
2. **Segurança:** Prioridade da AWS, este pilar inclui práticas para garantir a integridade dos dados e o uso de criptografia.
3. **Confiabilidade:** Trata de planos de recuperação, como restaurar uma instância EC2 que falhou, garantindo que a aplicação atenda às necessidades de negócios.
4. **Eficiência de Performance:** Envolve a utilização inteligente de recursos, como escolher a instância EC2 correta para a carga de trabalho e tomar decisões baseadas em dados.
5. **Otimização de Custos:** Busca evitar gastos desnecessários, como monitorar instâncias EC2 para não usar recursos excessivos sem

necessidade.

6. **Sustentabilidade:** Minimiza o impacto ambiental dos workloads na nuvem, focando na redução do consumo de energia e na criação de arquiteturas mais eficientes.

No passado, a avaliação da infraestrutura na AWS exigia a ajuda de um arquiteto de soluções. Agora, com a **Well-Architected Tool**, você pode fazer isso de forma autônoma. A ferramenta está disponível na console da AWS e permite que você crie uma carga de trabalho, execute uma revisão e receba um relatório com áreas a serem melhoradas.

O relatório é visualizado como um semáforo:

- **Verde** indica que tudo está bem.
- **Amarelo** sinaliza áreas que precisam de melhorias.
- **Vermelho** destaca riscos potenciais.

A ferramenta é personalizável e permite que você ignore perguntas que não se aplicam ao seu cenário. Ao utilizar a ferramenta, você poderá responder a perguntas específicas de cada pilar, receber recomendações e acessar vídeos explicativos.

