# 1. O que é computação em nuvem

Entrega sob demanda de computação, banco de dados, armazenamento, aplicativos e outros recursos de TI por meio de uma plataforma de serviços em nuvem via Internet com preços pré-pagos.

Infraestrutura do AWS – [www.infrastructure.aws](http://www.infrastructure.aws)

As três principais categorias de computação são máquinas virtuais (VMs), contêineres e computação sem servidor

## 3 tipos de computação em nuvem

* **Infraestrutura como serviço (IAAS)**
  + Você gerencia o servidor, que pode ser físico ou virtual, bem como o sistema operacional
* **Plataforma como serviço (PAAS)**
  + Outra pessoa gerencia o hardware e os sistemas subjacentes, você apenas se concentra em seus aplicativos, outra pessoa se preocupa com segurança, aplicação de patches, atualizações, manutenção e etc.
* **Software como serviço (SAAS)**
  + Pense no Outlook. Você se preocupa em como usar o software, o resto é terceirizado.

## 3 tipos de implantações de computação em nuvem

Nuvem pública (Cloud-based) - AWS, Azure, GCP

Híbrido (Hybrid) - mistura público e privado

Nuvem privada (on-premises) - você gerencia o datacenter

## 6 vantagens da computação em nuvem

1 – Mudar de despesa de capital para despesa variável. Pagar conforme o uso.

2 – Enormes economias de escala

3 – Parar de adivinhar a capacidade

4 – Aumentar velocidade e agilidade

5 – Parar de gastar dinheiro executando e mantendo datacenter

6 – Tornar-se global

# 2. Região X Zona de Disponibilidade X Edge Location

Região - é uma localização física on globo que consiste em três ou mais zonas de disponibilidade.

AZ - formação de um ou mais datacenter em que cada um tem energia redundante, rede e conectividade entre si, e pelo menos 100km de distância um do outro

Edge Locations - são endpoints para a AWS usados para cache e conteúdo. Consiste no serviço de CloudFront, que é o CDN da AWS.

# 3. Amazon Virtual Private Cloud (Amazon VPC)

Um serviço de rede que você pode usar para estabelecer limites em torno de seus recursos da AWS.

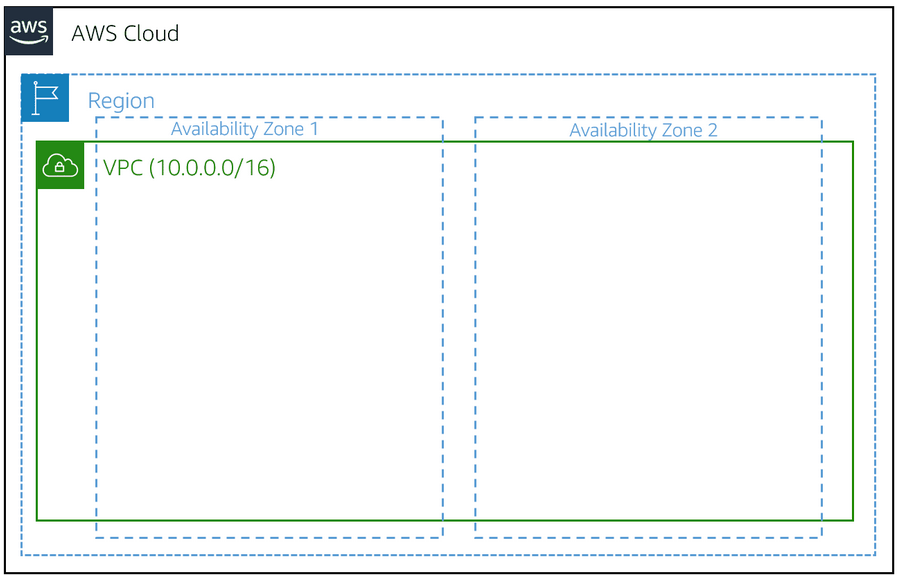
Permite que você provisione uma seção isolada da Nuvem AWS. Nesta seção isolada, você pode iniciar recursos em uma rede virtual que você define. Dentro de uma nuvem privada virtual (VPC), você pode organizar seus recursos em sub-redes. Uma sub-rede é uma seção de uma VPC que pode conter recursos como instâncias do Amazon EC2.

Ao criar uma Amazon VPC, você deve escolher três fatores principais:

Nome da VPC

Região onde a VPC ficará – Uma VPC abrange todas as Zonas de Disponibilidade dentro da Região selecionada.

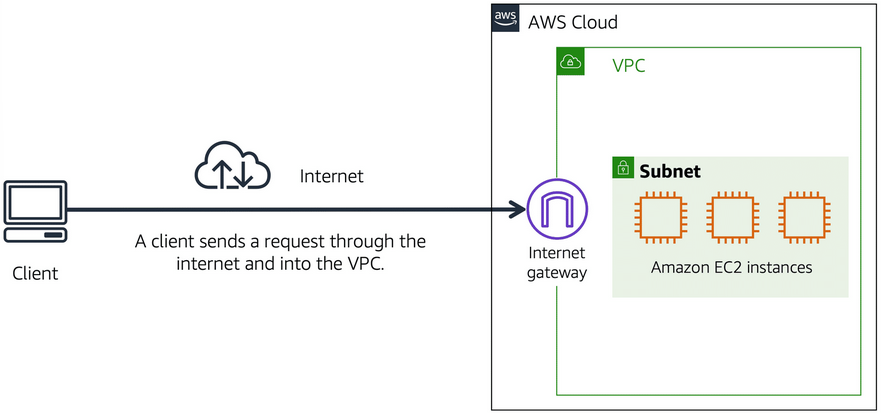
Intervalo de IP para a VPC na notação CIDR – Isso determina o tamanho da sua rede. Cada VPC pode ter até cinco CIDRs: um primário e quatro secundários para IPv4. Cada um desses intervalos pode ter entre /28 (na notação CIDR) e /16 em tamanho.



## Gateway de Internet

Para permitir que o tráfego público da internet acesse sua VPC

Um gateway de internet é uma conexão entre uma VPC e a internet. Você pode pensar em um gateway de internet como sendo semelhante a uma porta que os clientes usam para entrar na cafeteria. Sem um gateway de internet, ninguém pode acessar os recursos dentro da sua VPC.

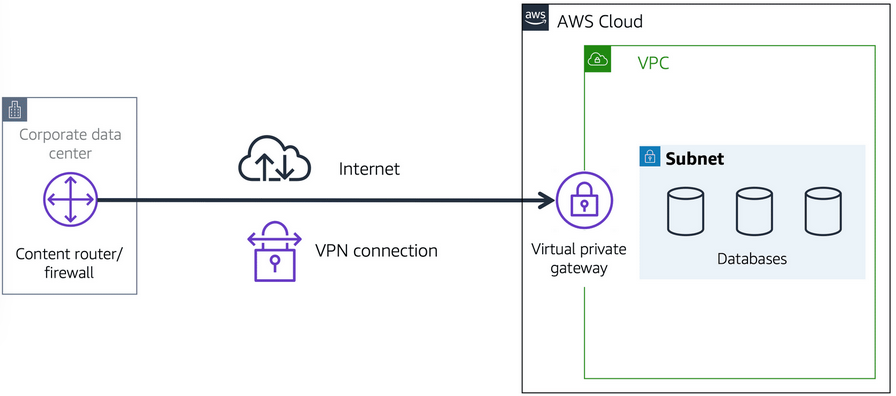


## Gateway privado virtual

Para acessar recursos privados em uma VPC, você pode usar um gateway privado virtual.

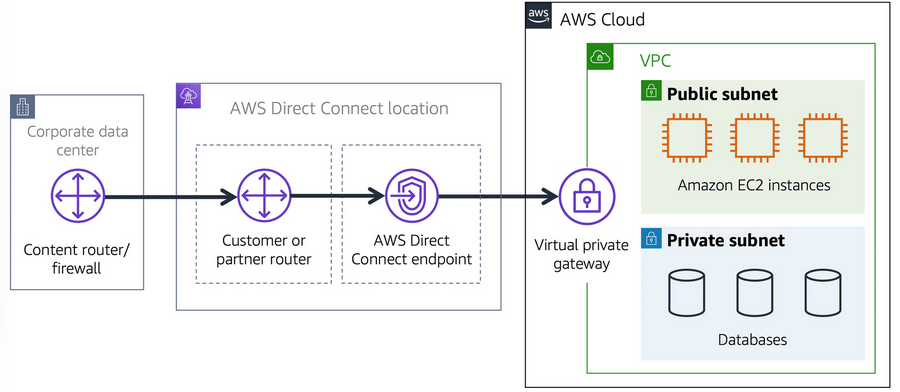
O gateway privado virtual é o componente que permite que o tráfego de internet protegido entre na VPC.

Um gateway privado virtual permite que você estabeleça uma conexão de rede privada virtual (VPN) entre sua VPC e uma rede privada, como um data center local ou rede corporativa interna. Um gateway privado virtual permite o tráfego para a VPC somente se estiver vindo de uma rede aprovada.



## AWS Direct Connect

um serviço que permite que você estabeleça uma conexão privada dedicada entre seu data center e uma VPC. A conexão privada que o AWS Direct Connect fornece ajuda a reduzir os custos de rede e aumentar a quantidade de largura de banda que pode trafegar pela sua rede.



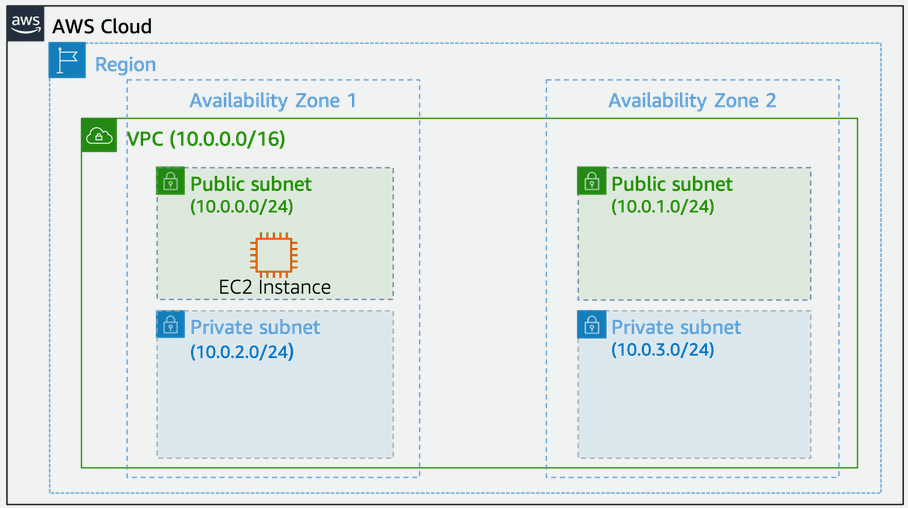
## Sub-redes

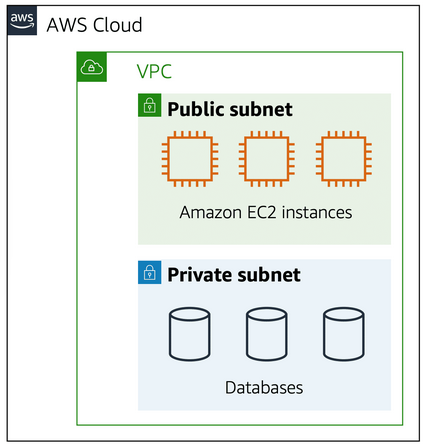
Uma sub-rede é uma seção de uma VPC na qual você pode agrupar recursos com base em necessidades de segurança ou operacionais. As sub-redes podem ser públicas ou privadas.

As sub-redes públicas contêm recursos que precisam ser acessíveis ao público, como o site de uma loja online.

As sub-redes privadas contêm recursos que devem ser acessíveis apenas através da sua rede privada, como um banco de dados que contém informações pessoais dos clientes e históricos de pedidos.

Em uma VPC, as sub-redes podem se comunicar entre si. Por exemplo, você pode ter um aplicativo que envolve instâncias do Amazon EC2 em uma sub-rede pública se comunicando com bancos de dados localizados em uma sub-rede privada.





## ACLs de Rede

Uma ACL de rede é um firewall virtual que controla o tráfego de entrada e saída no nível da sub-rede.

Cada conta AWS inclui uma ACL de rede padrão. Ao configurar sua VPC, você pode usar a ACL de rede padrão da sua conta ou criar ACLs de rede personalizadas.

**Por padrão, a ACL de rede padrão da sua 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 permitir. Além disso, todas as ACLs de rede têm uma regra de negação explícita. Esta regra garante que, se um pacote não corresponder a nenhuma das outras regras da lista, o pacote será negado.

### Filtragem de pacotes sem estado

As ACLs de rede realizam filtragem de pacotes sem estado. Eles não se lembram de nada e verificam os pacotes que atravessam a borda da sub-rede em cada sentido: de entrada e saída.

Quando uma resposta de pacote para essa solicitação retorna à sub-rede, a ACL da rede não se lembra da sua solicitação anterior. A ACL da rede verifica a resposta do pacote em relação à sua lista de regras para determinar se deve permitir ou negar.

Depois que um pacote entra em uma sub-rede, ele deve ter suas permissões avaliadas para recursos dentro da sub-rede, como instâncias do Amazon EC2.

O componente VPC que verifica as permissões de pacote para uma instância do Amazon EC2 é um grupo de segurança

## Grupos de segurança

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

**Por padrão, um grupo de segurança nega todo o tráfego de entrada e permite todo o tráfego de saída**. Você pode adicionar regras personalizadas para configurar qual tráfego deve ser permitido; qualquer outro tráfego seria negado

Se você tiver várias instâncias do Amazon EC2 dentro do mesmo VPC, poderá associá-las ao mesmo grupo de segurança ou usar grupos de segurança diferentes para cada instância.

### Filtragem de pacotes com estado

Grupos de segurança realizam filtragem de pacotes com estado. Eles se lembram de decisões anteriores tomadas para pacotes recebidos.

Considere o mesmo exemplo de envio de uma solicitação de uma instância do Amazon EC2 para a internet.

Quando uma resposta de pacote para essa solicitação retorna à instância, o grupo de segurança se lembra da sua solicitação anterior. O grupo de segurança permite que a resposta prossiga, independentemente das regras do grupo de segurança de entrada.

# 4. Route 53

## Sistema de Nomes de Domínio (DNS)

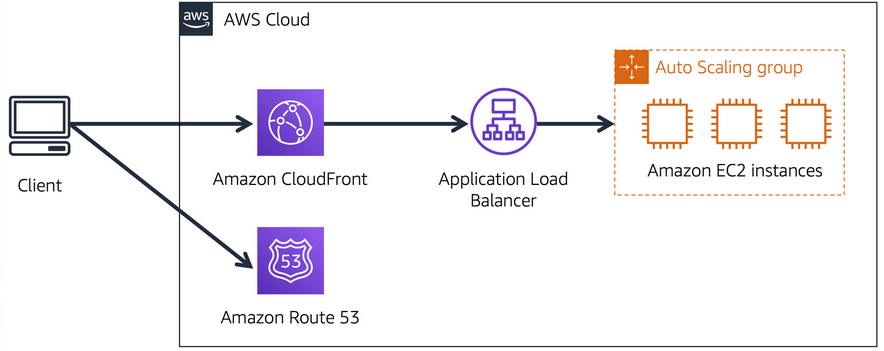
Suponha que AnyCompany tenha um site hospedado na Nuvem AWS. Os clientes inserem o endereço da web em seu navegador e podem acessar o site. Isso acontece por causa da resolução do Sistema de Nomes de Domínio (DNS). A resolução de DNS envolve um solucionador de DNS do cliente se comunicando com um servidor DNS da empresa.

Você pode pensar no DNS como sendo a lista telefônica da internet. A resolução DNS é o processo de tradução de um nome de domínio para um endereço IP.

O Amazon Route 53 conecta solicitações de usuários à infraestrutura em execução na AWS (como instâncias do Amazon EC2 e balanceadores de carga). Ele pode rotear usuários para infraestrutura fora da AWS.

Outro recurso do Route 53 é a capacidade de gerenciar os registros DNS para nomes de domínio. Você pode registrar novos nomes de domínio diretamente no Route 53. Você também pode transferir registros DNS para nomes de domínio existentes gerenciados por outros registradores de domínio. Isso permite que você gerencie todos os seus nomes de domínio em um único local.Pode demorar até 3 dias para registrar o domínio.

Cobra em dólar para o período de 1 ano de registro



# 5. Serviço de Migração de Banco de Dados AWS (AWS DMS)

O AWS Database Migration Service (AWS DMS) (abre em uma nova guia) permite migrar bancos de dados relacionais, bancos de dados não relacionais e outros tipos de armazenamentos de dados.

Com o AWS DMS, você move dados entre um banco de dados de origem e um banco de dados de destino. Os bancos de dados de origem e de destino (abre em uma nova guia) podem ser do mesmo tipo ou de tipos diferentes. Durante a migração, seu banco de dados de origem permanece operacional, reduzindo o tempo de inatividade de qualquer aplicativo que dependa do banco de dados.

Por exemplo, suponha que você tenha um banco de dados MySQL armazenado no local em uma instância do Amazon EC2 ou no Amazon RDS. Considere o banco de dados MySQL como seu banco de dados de origem. Usando o AWS DMS, você pode migrar seus dados para um banco de dados de destino, como um banco de dados Amazon Aurora.

# 6. Centro de Conformidade com o Cliente

O Centro de Conformidade do Cliente contém recursos para ajudá-lo a aprender mais sobre a conformidade com a AWS.

No Centro de Conformidade do Cliente, você pode ler histórias de conformidade do cliente para descobrir como as empresas dos setores regulamentados resolveram vários desafios de conformidade, governança e auditoria.

Você também pode acessar whitepapers de conformidade e documentação sobre tópicos como:

•     Respostas da AWS às principais questões de conformidade

•     Uma visão geral do risco e conformidade da AWS

•     Uma lista de verificação de segurança de auditoria

Além disso, o Centro de Conformidade do Cliente inclui um caminho de aprendizado do auditor. Este caminho de aprendizado foi projetado para indivíduos em funções de auditoria, conformidade e legais que desejam aprender mais sobre como sua ópera interna

As ações podem demonstrar conformidade usando a Nuvem AWS.

# 7. Escudo AWS (Shield)

O AWS Shield é um serviço que protege aplicativos contra ataques DDoS. O AWS Shield fornece dois níveis de proteção: Padrão e Avançado.

O **AWS Shield Standard** protege automaticamente todos os clientes da AWS sem custo algum. Ele protege seus recursos da AWS dos tipos mais comuns e frequentes de ataques DDoS.

Conforme o tráfego de rede entra em seus aplicativos, o AWS Shield Standard usa uma variedade de técnicas de análise para detectar tráfego malicioso 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 DDoS sofisticados.

Ele também se integra a outros serviços, como Amazon CloudFront, Amazon Route 53 e Elastic Load Balancing. Além disso, você pode integrar o AWS Shield com o AWS WAF escrevendo regras personalizadas para mitigar ataques DDoS complexos.

## Ataques de negação de serviço

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

Por exemplo, um invasor pode inundar um site ou aplicativo com tráfego de rede excessivo até que o site ou aplicativo alvo fique sobrecarregado e não seja mais capaz de responder. Se o site ou aplicativo ficar indisponível, isso nega o serviço aos usuários que estão tentando fazer solicitações legítimas.

## Ataques distribuídos de negação de serviço

Em um ataque distribuído de negação de serviço (DDoS), várias fontes são usadas para iniciar um ataque que visa tornar um site ou aplicativo indisponível. Isso pode vir de um grupo de atacantes, ou até mesmo de um único atacante. O único invasor pode usar vários computadores infectados (também conhecidos como “bots”) para enviar tráfego excessivo para um site ou aplicativo.

Para ajudar a minimizar o efeito dos ataques DoS e DDoS em seus aplicativos, você pode usar o AWS Shield (abre em uma nova guia).

# 8. O AWS Key Management Service (AWS KMS)

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

Com o AWS KMS, você pode escolher os níveis específicos de controle de acesso que precisa para suas chaves. Por exemplo, você pode especificar quais usuários e funções do IAM são capazes de gerenciar chaves. Alternativamente, você pode desativar temporariamente as chaves para que elas não sejam mais usadas por ninguém. Suas chaves nunca saem do AWS KMS, e você está sempre no controle delas.

# 9. AWS WAF

O AWS WAF é um firewall de aplicativos da web que permite monitorar e controlar as solicitações de rede que entram em seus aplicativos da web, funcionando como a primeira camada de proteção contra ataques. Ele trabalha em conjunto com o Amazon CloudFront, Application Load Balancer e API Gateway para gerenciar o acesso aos seus recursos.

O AWS WAF utiliza uma lista de controle de acesso à web (web ACL) para proteger seus recursos da AWS, permitindo configurar regras para bloquear ou permitir tráfego com base em condições específicas. Por exemplo, você pode configurar a ACL da web para bloquear solicitações de endereços IP maliciosos enquanto permite o acesso de usuários legítimos.

Quando uma solicitação chega ao AWS WAF, ela é avaliada com base nas regras configuradas na web ACL. Dependendo das condições, a solicitação pode ser:

* Permitida.
* Bloqueada.
* Contabilizada (contando o número de requisições que satisfazem as propriedades especificadas).

O AWS WAF oferece proteção adicional contra ataques da web, permitindo configurar condições como:

* Endereços IP de origem.
* Países de origem das solicitações.
* Valores nos cabeçalhos das solicitações.
* Sequências específicas ou padrões de expressão regular (REGEX) presentes nas solicitações.
* Duração das solicitações.
* Bloqueio de SQL Injection.
* Bloqueio de Cross-Site Scripting (XSS).

Além disso, você pode definir critérios como quais endereços têm permissão para acessar o conteúdo ou quais parâmetros na cadeia de consulta são necessários para que uma solicitação seja permitida. Após a análise das regras configuradas, o balanceador de carga do aplicativo, o CloudFront ou o API Gateway permite que o conteúdo seja recebido ou retorna um código de status HTTP 403.

# 10. O Amazon Inspector

ajuda a melhorar a segurança e a conformidade dos aplicativos executando avaliações de segurança automatizadas. Ele verifica os aplicativos em busca de vulnerabilidades de segurança e desvios das melhores práticas de segurança, como acesso aberto a instâncias do Amazon EC2 e instalações de versões de software vulneráveis.

Depois que o Amazon Inspector realiza uma avaliação, ele fornece uma lista de descobertas de segurança. A lista prioriza por nível de gravidade, incluindo uma descrição detalhada de cada problema de segurança e uma recomendação de como corrigi-lo. No entanto, a AWS não garante que seguir as recomendações fornecidas resolva todos os possíveis problemas de segurança. Sob o modelo de responsabilidade compartilhada, os clientes são responsáveis pela segurança de seus aplicativos, processos e ferramentas que são executados nos serviços da AWS.

## AWS Trust Advisor

Recursos on-line para ajudar a reduzir custos, aumentar o desempenho e melhorar a segurança, otimizando o ambiente AWS.

Fornece orientação em tempo real para ajudar a provisionar recursos seguindo as práticas recomendardes pelo AWS.

Aconselha sobre otimizações de custo, desempenho, segurança e tolerância a falhas.

O Trusted Advisor compara suas descobertas com as melhores práticas da AWS em cinco categorias:

otimização de custos,

desempenho,

segurança,

tolerância a falhas e

limites de serviço.

Para as verificações em cada categoria, o Trusted Advisor oferece uma lista de ações recomendadas e recursos adicionais para aprender mais sobre as melhores práticas da AWS.

A orientação fornecida pelo AWS Trusted Advisor pode beneficiar sua empresa em todos os estágios da implantação. Por exemplo, você pode usar o AWS Trusted Advisor para ajudá-lo enquanto cria novos fluxos de trabalho e desenvolve novos aplicativos. Você também pode usá-lo enquanto faz melhorias contínuas em aplicativos e recursos existentes.

# 11. Amazon Guard Duty

O Amazon GuardDuty é um serviço que fornece detecção inteligente de ameaças para sua infraestrutura e recursos da AWS. Ele identifica ameaças monitorando continuamente a atividade da rede e o comportamento da conta dentro do seu ambiente AWS.

Depois de ativar o GuardDuty para sua conta AWS, o GuardDuty começa a monitorar a atividade da sua rede e conta. Você não precisa implantar ou gerenciar nenhum software de segurança adicional. O GuardDuty então analisa continuamente dados de várias fontes da AWS, incluindo Logs de Fluxo VPC e Logs DNS.

Se o GuardDuty detectar quaisquer ameaças, você pode revisar descobertas detalhadas sobre elas no Console de Gerenciamento da AWS. As descobertas incluem etapas recomendadas para remediação. Você também pode configurar as funções do AWS Lambda para tomar medidas de remediação automaticamente em resposta às descobertas de segurança do GuardDuty.

# 12. S3

Armazenamento de objetos seguros, durável e altamente escalável

É baseado em armazenamento de objetos, permite upload de qualquer arquivo

O dado é distribuído em vários devices e vários lugares (AZ)

De 0 bytes até 5Tb por arquivo

O armazenamento é ilimitado

Os arquivos são armazenados em buckets.

É universal, não tem outro bucket com o mesmo nome



## O Arquivo é dividido:

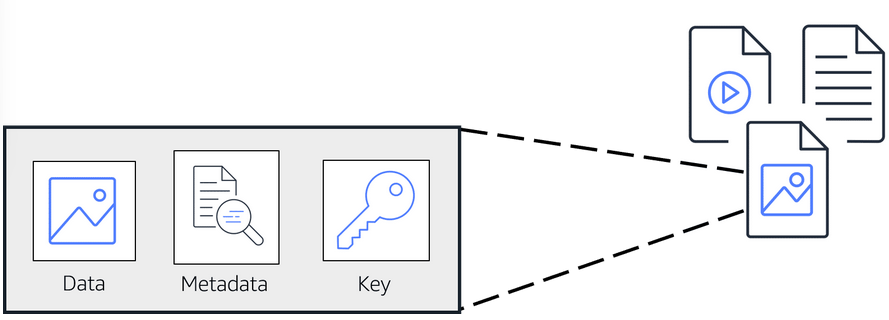
- Chave (key) - nome do arquivo

- Valor (value) - consiste no dado em si

- Id da versão (version id)

- Metadados: são os dados dos dados

- Detalhamento: Lista de controle de acessos, torrent e etc.



## Consistência de dados

- Ler depois de escrever para puts de novos objetos.

- Consistência eventual quando sobrescrever puts e deletes.

as mudanças de objetos podem levar um tempo para se propagar.

## Segurança

**Tudo no Amazon S3 é privado por padrão**. Isso significa que todos os recursos do Amazon S3, como buckets e objetos, só podem ser visualizados pelo usuário ou pela conta da AWS que criou o recurso. Os recursos do Amazon S3 são todos privados e protegidos para começar.

Se você decidir que quer que todos na internet vejam suas fotos, você pode escolher tornar seus buckets e objetos públicos. Um recurso público significa que todos na internet podem vê-lo. Na maioria das vezes, você não quer que suas permissões sejam tudo ou nada. Normalmente, você quer ser mais granular sobre a maneira como fornece acesso aos seus recursos.

O Amazon S3 reforça a criptografia em trânsito (enquanto viaja de e para o Amazon S3) e em repouso. Para proteger os dados, o Amazon S3 criptografa automaticamente todos os objetos no upload e aplica criptografia do lado do servidor com chaves gerenciadas pelo S3 como o nível base de criptografia para cada bucket no Amazon S3 sem custo adicional.

## Funcionalidades

- Armazenamento em camadas

- Gerenciamento de ciclo de vida

- Versionamento

- Encriptação

- Exclusão por mfa

- Segurança com access control lista e bucket policies

## Gerenciamento de ciclo de vida

Ao definir uma configuração de ciclo de vida para um objeto ou grupo de objetos, você pode escolher automatizar entre dois tipos de ações: transição e expiração.

Ações de transição definem quando os objetos devem fazer a transição para outra classe de armazenamento.

Ações de expiração definem quando os objetos expiram e devem ser excluídos permanentemente.

Por exemplo, você pode fazer a transição de objetos para a classe de armazenamento S3 Standard-IA 30 dias após criá-los. Ou você pode arquivar objetos na classe de armazenamento S3 Glacier Deep Archive 1 ano após criá-los.



## Classes de Armazenamento

### Standard

durabilidade, disponibilidade e redundância entre AZ

### IA

Acesso infrequente: Dados que são acessados menos frequentemente, mas requerem rápido acesso quando necessário. Tem custo inferior, mas pode ser cobrado por taxas de recuperação adicionais.

### IA One Zone

Acesso infrequente e disponível em apenas uma AZ

### Classificação Inteligente

Projetado para otimizar custos, movendo dados automaticamente para a camada de acesso mais econômica, sem impacto no desempenho ou sobrecarga operacional.

### Glacier

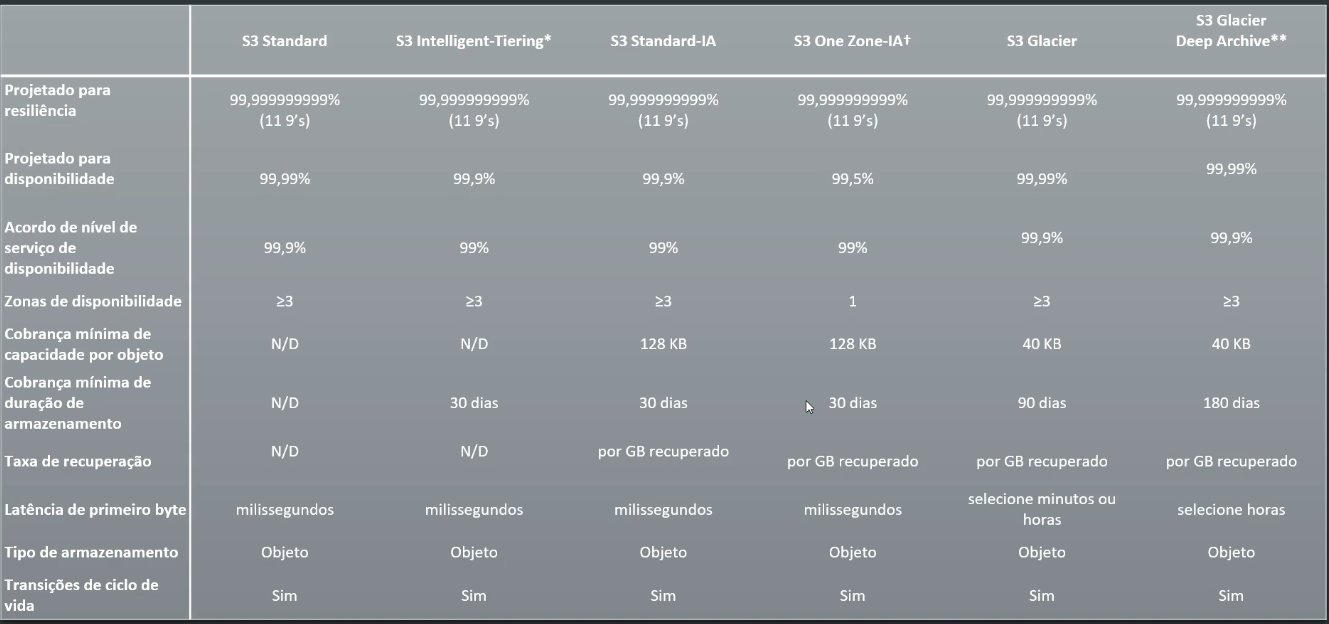
Armazenamento de baixo custo, com as mesmas características das outras, a diferença é que o tempo de recuperação do arquivo é configurável em minutos ou horas.

### Glacier deep archive

Classe de menor custo, onde é aceitável um tempo de recuperação de 12h

## S3 Outposts

Cria buckets S3 no Amazon S3 Outposts. Facilita a recuperação, o armazenamento e o acesso a dados no AWS Outposts. O Amazon S3 Outposts fornece armazenamento de objetos para seu ambiente AWS Outposts local. O Amazon S3 Outposts foi projetado para armazenar dados de forma durável e redundante em vários dispositivos e servidores em seus Outposts. Ele funciona bem para cargas de trabalho com requisitos de residência de dados locais que devem satisfazer as necessidades de desempenho exigentes, mantendo os dados próximos aos aplicativos locais.



## Aceleração de Transferência de S3

AWS S3 Transfer Acceleration permite transferências de arquivos entre usu final e um bucket. Aproveita os pontos de presença (edge locations) distribuídos pelo CloudFront. À medida que os dados chegam a um local de borda, os dados são roteados para o S3 por um caminho de rede otimizado.



## Como funciona a cobrança

Armazenamento

Requisições

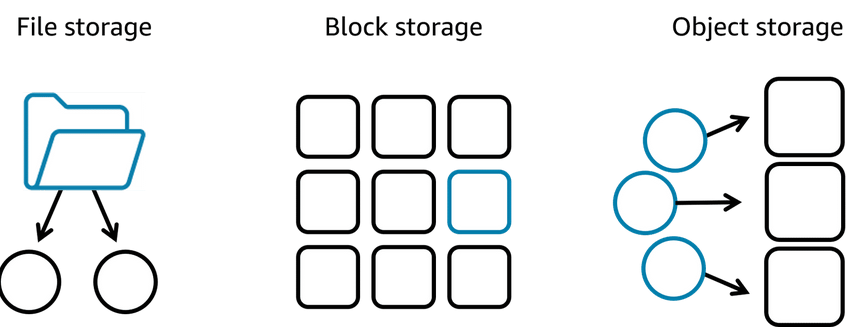
Tipos de classes

Transferência de dados para fora do AWS

Aceleração de Transferência

Replicação entre regiões

## S3 x EBS



Lembre-se de que quando você modifica um arquivo no armazenamento em bloco, apenas as peças que são alteradas são atualizadas. Quando um arquivo no armazenamento de objetos é modificado, todo o objeto é atualizado.

### Armazenamento em bloco

O armazenamento em bloco divide os arquivos em pedaços de dados de tamanho fixo chamados blocos que têm seus próprios endereços. Cada bloco é uma parte individual do armazenamento de dados. Como cada bloco é endereçável, os blocos podem ser recuperados de forma eficiente. Pense no armazenamento em bloco como uma rota mais direta para acessar os dados.

Quando os dados são solicitados, os endereços são usados ​​pelo sistema de armazenamento para organizar os blocos na ordem correta para formar um arquivo completo para apresentar de volta ao solicitante. Além do endereço, nenhum metadado adicional é associado a cada bloco.

### Armazenamento de objetos

No armazenamento de objetos, os arquivos são armazenados como objetos. Objetos, assim como arquivos, são tratados como uma única unidade distinta de dados quando armazenados. No entanto, diferentemente do armazenamento de arquivos, esses objetos são armazenados em um bucket usando uma estrutura plana, o que significa que não há pastas, diretórios ou hierarquias complexas. Cada objeto contém um identificador exclusivo. Esse identificador, junto com quaisquer metadados adicionais, é agrupado com os dados e armazenado.

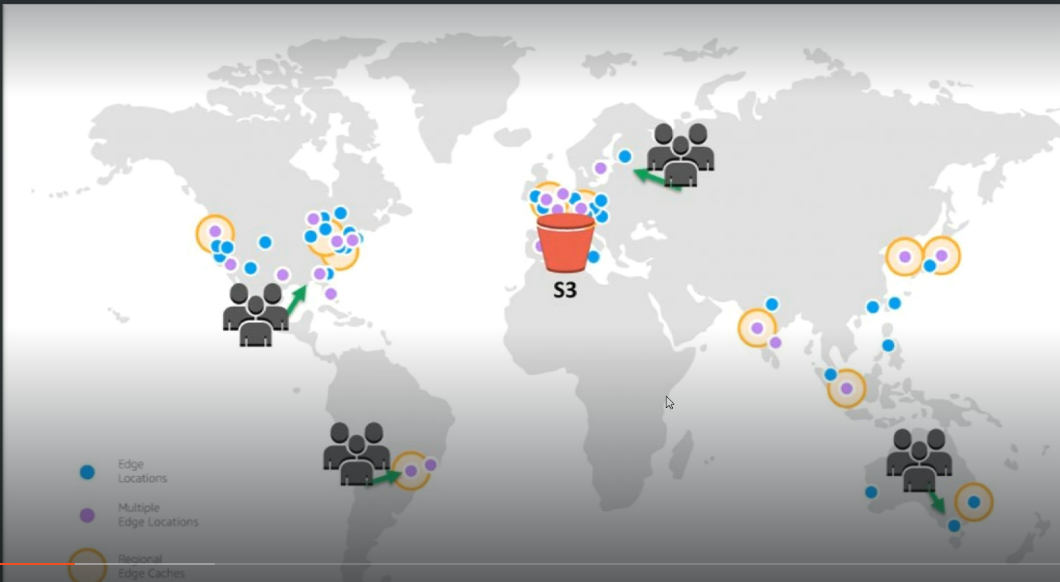
### Armazenamento de arquivos

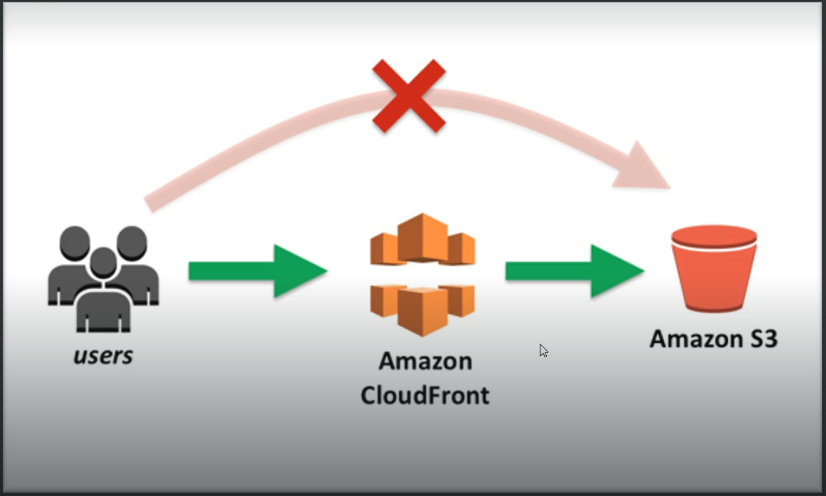
No armazenamento de arquivos, vários clientes (como usuários, aplicativos, servidores e assim por diante) podem acessar dados armazenados em pastas de arquivos compartilhados. Nesta abordagem, um servidor de armazenamento usa armazenamento em bloco com um sistema de arquivos local para organizar arquivos. Os clientes acessam dados por meio de caminhos de arquivos.

Em comparação com o armazenamento em bloco e o armazenamento de objetos, o armazenamento de arquivos é ideal para casos de uso em que um grande número de serviços e recursos precisam acessar os mesmos dados ao mesmo tempo.

O Amazon Elastic File System (Amazon EFS) é um sistema de arquivos escalável usado com serviços AWS Cloud e recursos locais. À medida que você adiciona e remove arquivos, o Amazon EFS cresce e encolhe automaticamente. Ele pode ser dimensionado sob demanda para petabytes sem interromper os aplicativos.

# 13. AWS Cloud Front

Uma rede de entrega de conteúdo (CDN) é um sistema de servidores distribuídos que entregam páginas da Web e outros conteúdos da Web a um usuário com base nas localizações geográficas do usuário, na origem da página da Web e em m servidor de entrega de conteúdo.



## O que é uma Edge Location

Local em que o conteúdo será armazenado em cache. Separado para uma região da AWS

**Origin** - é a origem de todos os arquivos que a CDN distribuirá. Pode ser um S3, uma EC2, um Elastic Load Balancer ou Route 53.

**Distribution –** Nome dado à CDN que consiste em uma coleção de edge locations

## Uso do Cloud Front

- Fornece um site inteiro, incluindo conteúdo dinâmico, estático, streaming e interativo

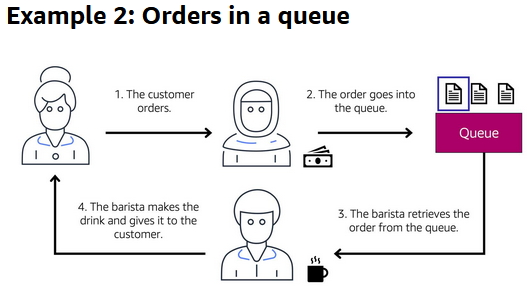
- Pode ser usado para escrita também, não é somente leitura. Pode usar com o S3 transfer acceleration por exemplo

- Objetos são armazenados por um TTL – time to live e dá p limpar o cache, mas tem custo p limpar.

# 14. Amazon Simple Queue Service (Amazon SQS)

O Amazon Simple Queue Service (Amazon SQS) é um serviço de enfileiramento de mensagens.

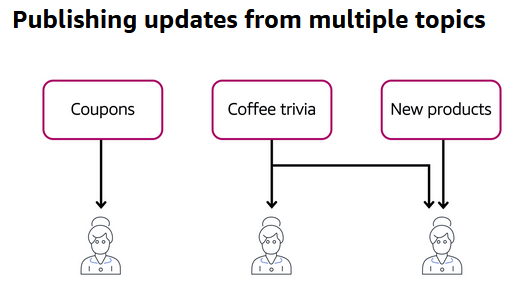
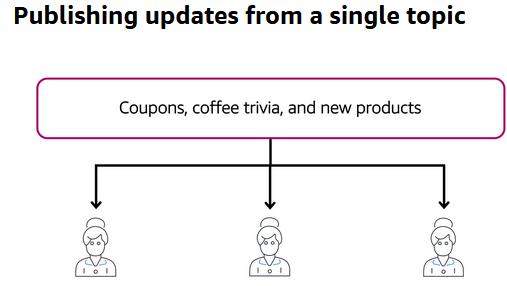
Usando o Amazon SQS, você pode enviar, armazenar e receber mensagens entre componentes de software, sem perder mensagens ou exigir que outros serviços estejam disponíveis. No Amazon SQS, um aplicativo envia mensagens para uma fila. Um usuário ou serviço recupera uma mensagem da fila, processa-a e a exclui da fila.



# 15. Amazon Simple Notification Service (Amazon SNS)

Amazon Simple Notification Service (Amazon SNS) é um serviço de publicação/assinatura. Usando tópicos do Amazon SNS, um editor publica mensagens para assinantes.

No Amazon SNS, os assinantes podem ser servidores Web, endereços de e-mail, funções do AWS Lambda ou várias outras opções.

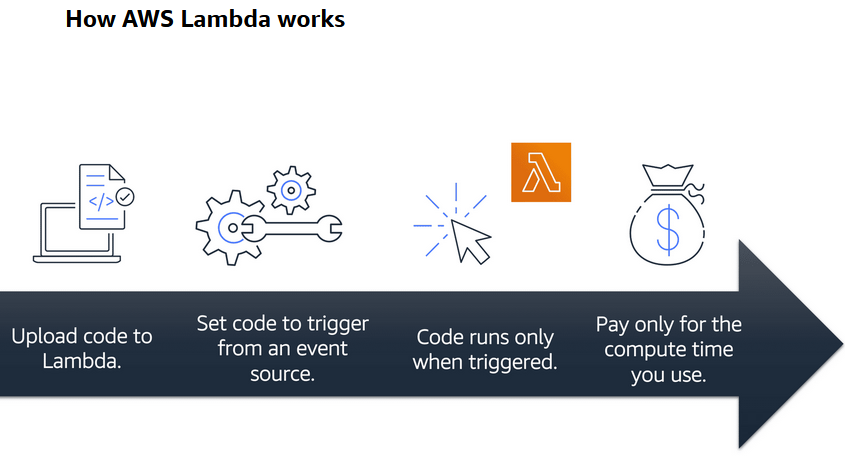


# 16. AWS Lambda

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

Ao usar o AWS Lambda, você paga apenas pelo tempo de computação que consome. As cobranças se aplicam apenas quando seu código está em execução. Você também pode executar código para praticamente qualquer tipo de aplicativo ou serviço de backend, tudo sem administração.

Por exemplo, uma função simples do Lambda pode envolver o redimensionamento automático de imagens carregadas para a Nuvem AWS. Nesse caso, a função é acionada ao carregar uma nova imagem.



Você tem a opção de configurar suas funções Lambda usando o console Lambda, a API Lambda, o AWS CloudFormation ou o AWS Serverless Application Model (AWS SAM). Você pode invocar sua função diretamente usando a API Lambda ou pode configurar um serviço ou recurso AWS para invocar sua função em resposta a um evento.

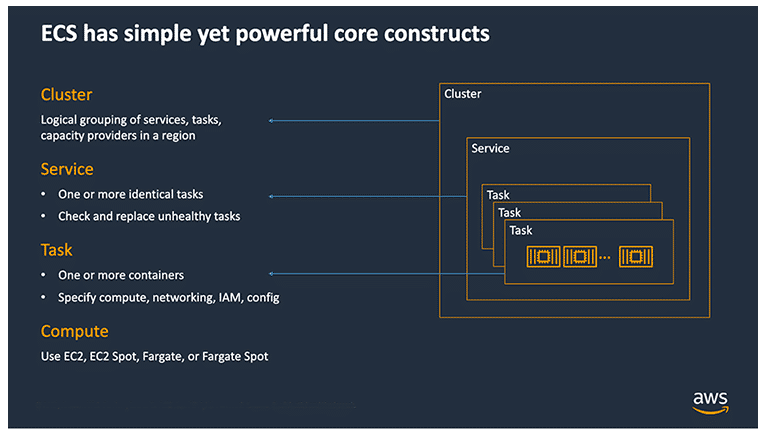
# 16. Amazon Elastic Container Service (Amazon ECS)

É um sistema de gerenciamento de contêineres altamente escalável e de alto desempenho que permite executar e dimensionar aplicativos em contêineres na AWS.

O Amazon ECS oferece suporte a contêineres do Docker. O Docker é uma plataforma de software que permite criar, testar e implantar aplicativos rapidamente. A AWS oferece suporte ao uso de código aberto

Com o Amazon ECS, seus contêineres são definidos em uma definição de tarefa que você usa para executar uma tarefa individual ou uma tarefa dentro de um serviço. Você tem a opção de executar suas tarefas e serviços em uma infraestrutura sem servidor que é gerenciada por outro serviço da AWS chamado AWS Fargate. Como alternativa, para mais controle sobre sua infraestrutura, você pode executar suas tarefas e serviços em um cluster de instâncias do EC2 que você gerencia.

Para preparar seu aplicativo para execução no Amazon ECS, você cria uma definição de tarefa. A definição de tarefa é um arquivo de texto, no formato JSON, que descreve um ou mais contêineres. Uma definição de tarefa é semelhante a um blueprint que descreve os recursos necessários para executar um contêiner, como CPU, memória, portas, imagens, armazenamento e informações de rede.



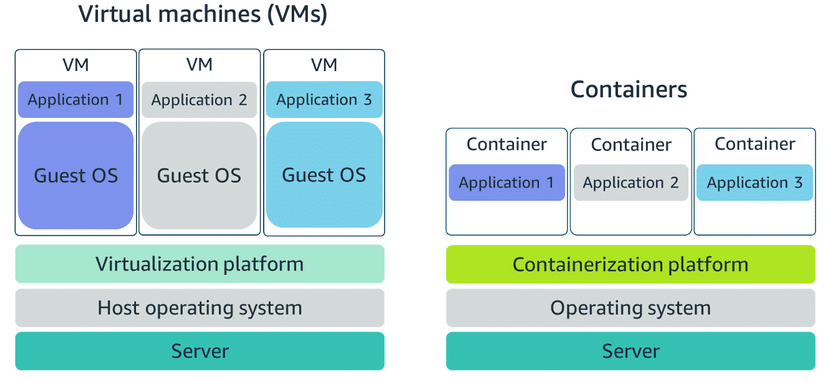
## Containers

fornecem uma maneira padrão de empacotar o código e as dependências do aplicativo em um único objeto. Você também pode usar contêineres para processos e fluxos de trabalho nos quais há requisitos essenciais de segurança, confiabilidade e escalabilidade.

Um contêiner é uma unidade padronizada que empacota seu código e suas dependências. Este pacote é projetado para rodar de forma confiável em qualquer plataforma, porque o contêiner cria seu próprio ambiente independente. Com contêineres, as cargas de trabalho podem ser transportadas de um lugar para outro, como do desenvolvimento para a produção ou de ambientes locais para a nuvem.

Um exemplo de plataforma de conteinerização é o Docker. O Docker é um runtime de contêiner popular que simplifica o gerenciamento de toda a pilha do sistema operacional necessária para o isolamento do contêiner, incluindo rede e armazenamento. O Docker ajuda os clientes a criar, empacotar, implantar e executar contêineres.

Os contêineres podem hospedar uma variedade de cargas de trabalho diferentes, incluindo aplicativos da web, migrações de elevação e mudança, aplicativos distribuídos e otimização de ambientes de desenvolvimento, teste e produção.



# 17. Serviço Amazon Elastic Kubernetes (EKS)

Um serviço totalmente gerenciado que você pode usar para executar Kubernetes na AWS. Kubernetes é um software de código aberto que permite implantar e gerenciar aplicativos em contêineres em escala. Uma grande comunidade de voluntários mantém o Kubernetes, e a AWS trabalha ativamente em conjunto com a comunidade do Kubernetes. À medida que novos recursos e funcionalidades são lançados para aplicativos Kubernetes, você pode aplicar facilmente essas atualizações em seus aplicativos gerenciados pelo Amazon EKS.

O Amazon EKS é um serviço gerenciado que você pode usar para executar o Kubernetes na AWS sem precisar instalar, operar e manter seu próprio plano de controle ou nós do Kubernetes. O Amazon EKS é conceitualmente semelhante ao Amazon ECS, mas com as seguintes diferenças:

No Amazon ECS, a máquina que executa os contêineres é uma instância do EC2 que tem um agente ECS instalado e configurado para executar e gerenciar seus contêineres. Essa instância é chamada de instância de contêiner. No Amazon EKS, a máquina que executa os contêineres é chamada de nó de trabalho ou nó do Kubernetes.

Um contêiner ECS é chamado de tarefa. Um contêiner EKS é chamado de pod.

O Amazon ECS é executado na tecnologia nativa da AWS. O Amazon EKS é executado no Kubernetes.

# 18. AWS Fargate

é um mecanismo de computação sem servidor para contêineres. Funciona com Amazon ECS e Amazon EKS.

Ao usar o AWS Fargate, você não precisa provisionar ou gerenciar servidores. O AWS Fargate gerencia sua infraestrutura de servidores para você. Você pode se concentrar mais na inovação e no desenvolvimento de seus aplicativos e pagar apenas pelos recursos que são disponibilizados.

É necessário para executar seus contêineres.



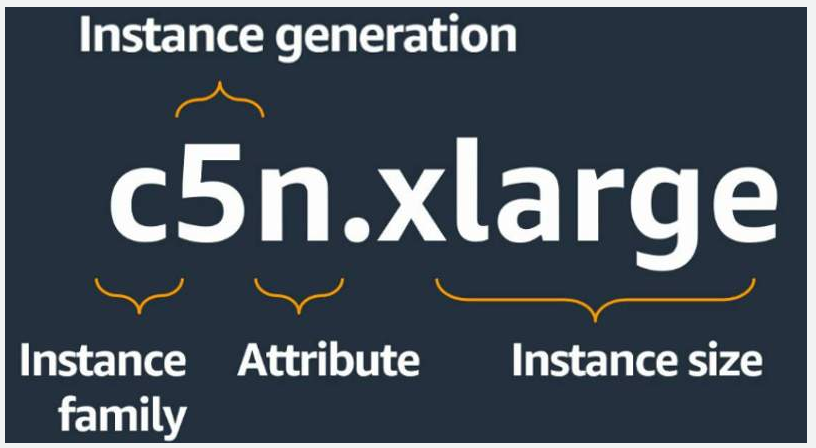
# 19. EC2 – Elastic Compute Cloud

Serviço que fornece capacidade de computação redimensionável

Reduz o tempo necessário para obter e inicializar novas instâncias de servidor.

Essa ideia de compartilhamento de hardware subjacente é chamada de multilocação. O hipervisor é responsável por coordenar essa multilocação e é gerenciado pela AWS. O hipervisor é responsável por isolar as máquinas virtuais umas das outras à medida que compartilham recursos do host. Isso significa que as instâncias do EC2 são seguras. Mesmo que eles possam estar compartilhando recursos, uma instância do EC2 não está ciente de nenhuma outra instância do EC2 também nesse host. Eles são seguros e separados uns dos outros.

## Tipos de Instâncias



Instâncias de uso geral

fornecem um equilíbrio de recursos de computação, memória e rede. Você pode usá-las para uma variedade de cargas de trabalho, como:

servidores de aplicativos

servidores de jogos

servidores de backend para aplicativos empresariais

bancos de dados pequenos e médios

Instâncias otimizadas para computação

são ideais para aplicativos vinculados à computação que se beneficiam de processadores de alto desempenho. Assim como instâncias de uso geral, você pode usar instâncias otimizadas para computação para cargas de trabalho como servidores da Web, de aplicativos e de jogos. No entanto, a diferença é que os aplicativos otimizados para computação são ideais para servidores da Web de alto desempenho, servidores de aplicativos com uso intensivo de computação e servidores de jogos dedicados. Você também pode usar instâncias otimizadas para computação para cargas de trabalho de processamento em lote que exigem o processamento de muitas transações em um único grupo.

Instâncias otimizadas de memória

são projetadas para fornecer desempenho rápido para cargas de trabalho que processam grandes conjuntos de dados na memória. Uma carga de trabalho que requer que grandes quantidades de dados sejam pré-carregadas antes de executar um aplicativo. Este cenário pode ser um banco de dados de alto desempenho ou uma carga de trabalho que envolve a execução de processamento em tempo real de uma grande quantidade de dados não estruturados. Nesses tipos de casos de uso, considere usar uma instância otimizada de memória. Instâncias otimizadas de memória permitem que você execute cargas de trabalho com altas necessidades de memória e receba ótimo desempenho.

Instâncias de computação acelerada

usam aceleradores de hardware, ou coprocessadores, para executar algumas funções de forma mais eficiente do que é possível em softwares executados em CPUs. Exemplos dessas funções incluem cálculos de números de ponto flutuante, processamento gráfico e correspondência de padrões de dados. Na computação, um acelerador de hardware é um componente que pode agilizar o processamento de dados. Instâncias de computação acelerada são ideais para cargas de trabalho como aplicativos gráficos, streaming de jogos e streaming de aplicativos.

Instâncias otimizadas para armazenamento

são projetadas para cargas de trabalho que exigem alto acesso sequencial de leitura e gravação a grandes conjuntos de dados no armazenamento local. Exemplos de cargas de trabalho adequadas para instâncias otimizadas para armazenamento incluem sistemas de arquivos distribuídos, aplicativos de data warehousing e sistemas de processamento de transações on-line de alta frequência (OLTP). Na computação, o termo operações de entrada/saída por segundo (IOPS) é uma métrica que mede o desempenho de um dispositivo de armazenamento. Ele indica quantas operações diferentes de entrada ou saída um dispositivo pode executar em um segundo. Instâncias otimizadas para armazenamento são projetadas para fornecer dezenas de milhares de IOPS aleatórios de baixa latência para aplicativos.

Você pode pensar em operações de entrada como dados inseridos em um sistema, como registros inseridos em um banco de dados. Uma operação de saída são dados gerados por um servidor. Um exemplo de saída pode ser a análise executada nos registros em um banco de dados. Se você tiver um aplicativo que tenha um alto requisito de IOPS, uma instância otimizada para armazenamento pode fornecer melhor desempenho em relação a outros tipos de instância não otimizados para esse tipo de caso de uso.

## Modelos de preços

### Sob demanda

Paga por horas utilizadas sem termo de compromisso.

Não tem pagamento adiantado

Aplicativos com cargas de trabalho de curto prazo, com picos de demanda ou imprevisíveis que não podem ser interrompidas.

### Reservado

Fornece uma reserva de capacidade e oferece um desconto significativo na tarifa horária de uma instância (saving plans).

Os termos de contrato são de 1 ou 3 anos.

Aplicativos com estado controlado ou uso previsível e que requerem capacidade reservada.

#### Tipos de reserva de preço

##### Reserva padrão

Oferecem até 75% de desconto em instâncias sob demanda. Quanto mais pagar antecipadamente e quanto maior o contrato, maior o desconto

##### Reserva Conversível

Oferecem até 54% de desconto na sob demanda para alterar os atributos desde que a troca resulte na criação de instâncias reservadas de valor igual ou superior.

##### Reserva Agendada

São lançados dentro das janelas de tempo que você reserva. Essa opção permite que combine a reserva de capacidade com uma programação recorrente previsível que requer apenas uma fração de um dia uma semana ou um mês.

### Reservada x Saving Plans

Na reservada vc especifica a máquina, sistema operacional e a qtde de horas. No Saving plans vc não precisa especificar a máquina, só a família da máquina.

### Spot

Tipo leilão, oferecer um preço que desejar pela capacidade desejada, proporcionando economia ainda maior se os aplicativos tiverem horários de início e término flexíveis.

Aplicativos que possuem horário de início e término flexíveis

Viáveis apenas a preços de computação muito baixos.

Usuário com necessidades urgentes de computação para grande quantidade de capacidade adicional

### Host Dedicados

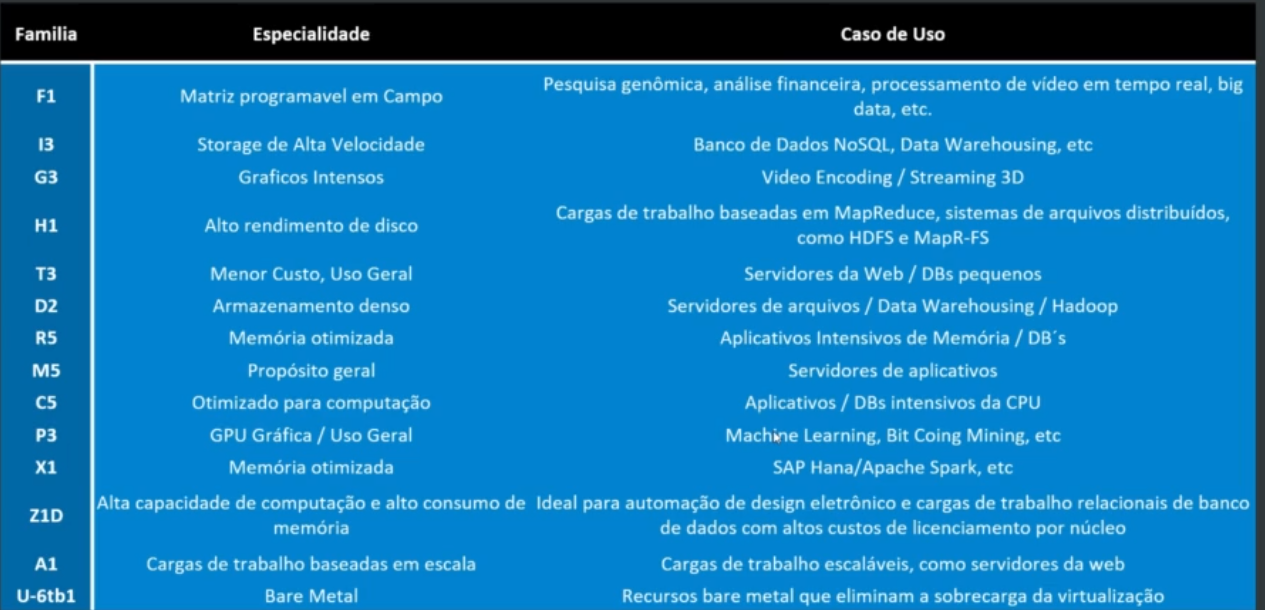
Servidores físicos EC2 dedicado para o uso. Ajuda a reduzir custo permitindo o uso de suas próprias licenças de software vinculadas ao servidor existente.

Requisitos regulamentares que podem não oferecer suporte a virtualização de hosts compartilhados.

Ótimo para licenciamento que não suporte implantações de multilocação ou nuvem.

Pode ser adquirido sob demanda ou com reserva com até 70% de desconto

## Famílias de EC2



## AWS CLI – Command Line Interface

Pode interagir com a AWS por linha de comando.

Tem que fazer as configurações das chaves pelo IAM, igual eu fiz para os IPs. É a mesma ideia, usar as keys para interagir ou por bibliotecas, ou pelo ec2 do linux por linha de comando.

## Instance stores

É um armazenamento em disco que é fisicamente conectado ao computador host para uma instância EC2 e, portanto, tem a mesma vida útil da instância. Quando a instância é encerrada, você perde todos os dados no repositório de instâncias.

## Amazon Elastic Block Store (Amazon EBS)

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

## Amazon EBS snapshots

É um backup incremental. Isso significa que o primeiro backup feito de um volume copia todos os dados. Para backups subsequentes, apenas os blocos de dados que foram alterados desde o snapshot mais recente são salvos. Os backups incrementais são diferentes dos backups completos, nos quais todos os dados em um volume de armazenamento são copiados sempre que um backup ocorre. O backup completo inclui dados que não foram alterados desde o backup mais recente.

## ROLES AWS (políticas)

Roles são mais seguras do que armazenar as chaves da IAM

São mais fáceis de gerenciar e podem ser atribuídas para instância depois de serem criadas.

São universais, podem ser usadas em qualquer região.

A ideia é criar uma Role que vai ter permissão de acessar determinadas funções do AWS e daí atribuir essa Role à EC2, daí sim, por CLI dá p fazer todas as funções que a Role permite, sem precisar de chaves. E no momento que tira a Role da EC2, ou que modifica sua função, a EC2 para de ter permissão de acessar determinadas coisas.

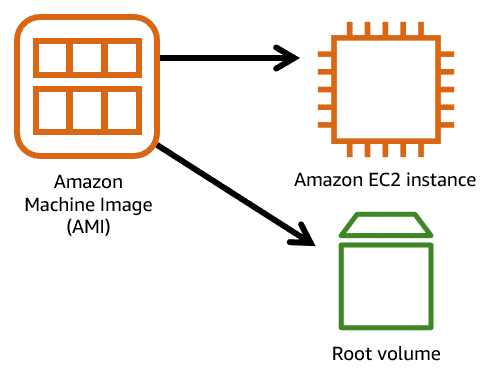
## Usando Scripts Boot Strap

Na inicialização de uma EC2 Linux é possível colocar scripts de inicialização da máquina para ela já subir com configurações pré-definidas, como no exemplo que instala o apache, inicializa ele, cria o arquivo index.html e copia o arquivo index.html para o bucket existente

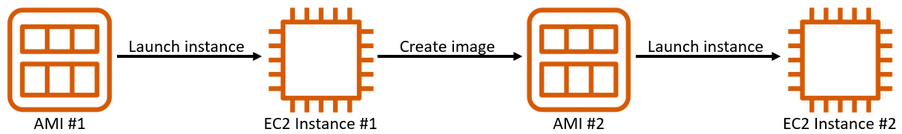


## Relação entre AMIs (Amazon Machine Image) e instâncias EC2

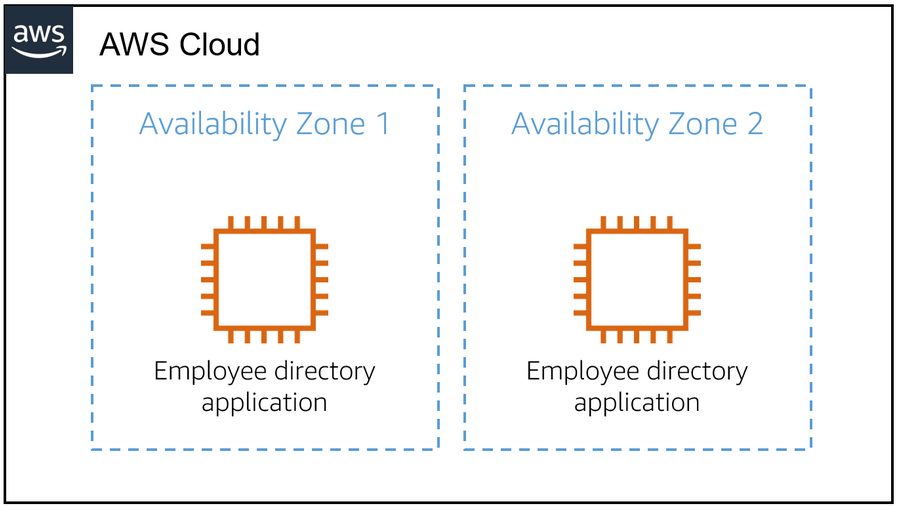
Quando você inicia uma nova instância, a AWS aloca uma máquina virtual que roda em um hypervisor. Então, a AMI que você selecionou é copiada para o volume do dispositivo raiz, que contém a imagem que é usada para inicializar o volume. No final, você obtém um servidor ao qual pode se conectar e instalar pacotes e software adicional



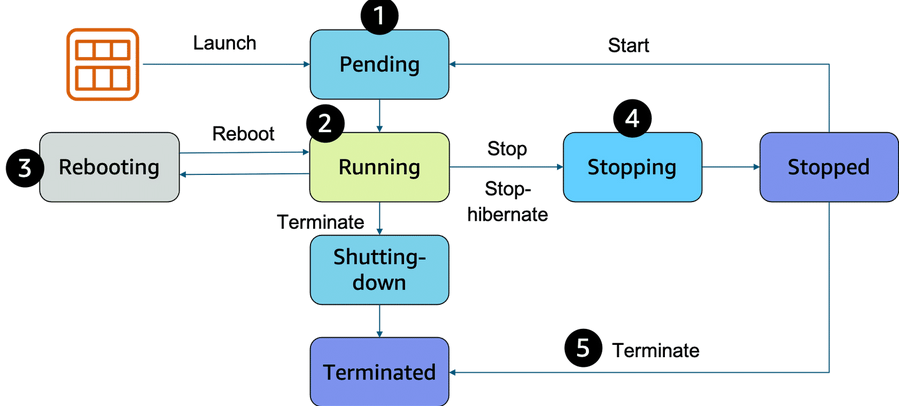
Uma vantagem de usar AMIs é que elas são reutilizáveis. Você pode escolher uma AMI baseada em Linux e configurar o servidor HTTP, pacotes de aplicativos e software adicional que você precisa para executar seu aplicativo. Se você quiser criar outra instância EC2 com as mesmas configurações, você pode criar e configurar uma nova instância EC2 para corresponder à primeira instância. Ou você pode criar uma AMI a partir da sua instância em execução e usar a AMI para iniciar uma nova instância. Dessa forma, sua nova instância teria as mesmas configurações que sua instância atual porque as configurações definidas nas AMIs são as mesmas.



Ao arquitetar qualquer aplicativo para alta disponibilidade, considere usar pelo menos duas instâncias do EC2 em duas Zonas de Disponibilidade separadas.



## Ciclo de vida da instância EC2



# 20. Load Balancer e Healt Checks

O Elastic Load Balancing é o serviço da AWS que distribui automaticamente o tráfego de entrada de aplicativos em vários recursos, como instâncias do Amazon EC2.

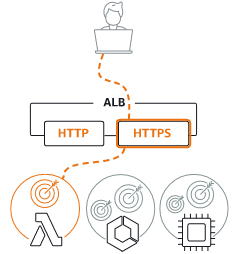
Um balanceador de carga atua como um único ponto de contato para todo o tráfego da Web de entrada para seu grupo de Auto Scaling. Isso significa que, conforme você adiciona ou remove instâncias do Amazon EC2 em resposta à quantidade de tráfego de entrada, essas solicitações são roteadas para o balanceador de carga primeiro. Em seguida, as solicitações são distribuídas em vários recursos que as manipularão. Por exemplo, se você tiver várias instâncias do Amazon EC2, o Elastic Load Balancing distribui a carga de trabalho entre as várias instâncias para que nenhuma instância tenha que carregar a maior parte dela.

## Como o Elastic Load Balancing Funciona

1. Os clientes fazem solicitações à sua aplicação.
2. Os listeners no balanceador de carga recebem solicitações correspondentes ao protocolo e à porta que você configurar.
3. O listener de recebimento avalia a solicitação de entrada em relação às regras que você especificar e, se aplicável, roteia a solicitação para o grupo de destino apropriado. Você pode usar um listener HTTPS para descarregar o trabalho de criptografia e descriptografia TLS para seu balanceador de carga.
4. Destinos íntegros em um ou mais grupos de destino recebem tráfego com base no algoritmo de balanceamento de carga e nas regras de roteamento que você especifica no listener.

## Tipo de Load Balancer

### Application Load Balancer



conjunto de recursos flexível para suas aplicações com tráfego HTTP e HTTPS. Operando no nível da solicitação, os Application Load Balancers fornecem roteamento avançado e recursos de visibilidade direcionados a arquiteturas de aplicações, incluindo microsserviços e contêineres.

### Network Load Balancer



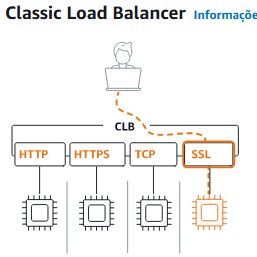
desempenho altíssimo, descarga de TLS em escala, implantação de certificados centralizada, suporte para UDP e endereços IP estáticos para sua aplicação. Operando no nível da conexão, os Network Load Balancers são capazes de atender a milhões de solicitações por segundo com segurança, enquanto mantêm latências extremamente baixas.

### Gateway Load Balancer

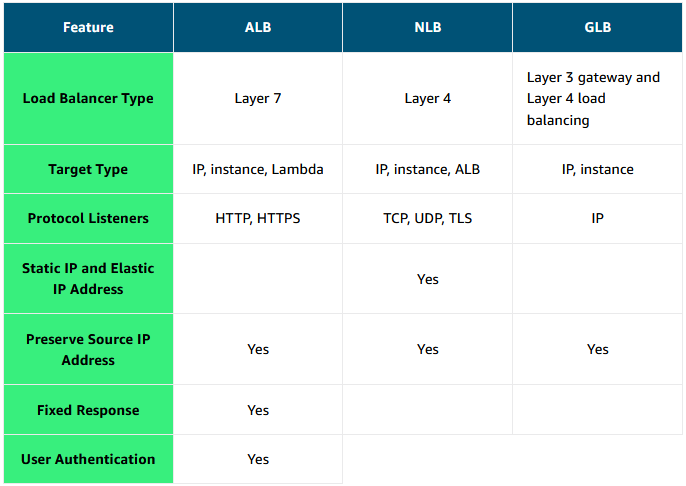


implantar e gerenciar uma frota de dispositivos virtuais de terceiros compatíveis com GENEVE. Esses dispositivos permitem que você melhore a segurança, a conformidade e os controles de políticas.

### Classic Load Balancer



quando tiver uma aplicação existente em execução na rede EC2-Classic.



## Health Check

Na configuração do Load Balancer, dá para configurar o Health Check, ele faz um ping em uma página que vc configurar e na porta que vc configurar. Daí tá para colocar intervalor desse ping, tempo de resposta esperado.

Erro 504 significa que o gateway expirou. Isso significa que o aplicativo não está respondendo dentro do período de tempo limite inativo.

Problemas com a aplicação. Veja se é o servidor Web ou o Servidor de banco de dados.

Se precisar do endereço ipv4 do seu usuário final, procure o cabeçalho X-Fowarded-For

# 21. RDS

Roda em máquinas virtuais (tipo T2, R5) mas não tem acesso a elas.

Não pode logar em sistemas operacionais RDS

Atualização e patches nos SO dos RDS e BDs, são de responsabilidades da AWS.

RDS não é Serverless.

Aurora Serverless é Serverless.

Escalonar componentes do serviço significa que você pode alterar a memória, o tamanho do processador, o armazenamento alocado ou o IOPS individualmente, sem modificar outras configurações definidas no seu banco de dados.

A parte de armazenamento de instâncias de BD para Amazon RDS usa volumes do Amazon Elastic Block Store (Amazon EBS) para armazenamento de banco de dados e log. Isso inclui MySQL, MariaDB, PostgreSQL, Oracle e SQL Server.

Ao usar o Aurora, os dados são armazenados em volumes de cluster, que são volumes virtuais únicos que usam unidades de estado sólido (SSDs). Um volume de cluster contém cópias dos seus dados em três Zonas de Disponibilidade em uma única Região da AWS. Para arquivos temporários não persistentes, o Aurora usa armazenamento local.

## Amazon RDS em uma Amazon Virtual Private Cloud

Ao criar uma instância de BD, você seleciona a Amazon Virtual Private Cloud (Amazon VPC) em que seus bancos de dados ficarão. Em seguida, você seleciona as sub-redes que serão designadas para seu BD. Isso é chamado de grupo de sub-redes de BD e tem pelo menos duas Zonas de Disponibilidade em sua Região. As sub-redes em um grupo de sub-redes de BD devem ser privadas, para que não tenham uma rota para o gateway da Internet. Isso garante que sua instância de BD e os dados dentro dela possam ser acessados ​​apenas pelo backend do aplicativo.

O acesso à instância de BD pode ser restringido ainda mais usando listas de controle de acesso à rede (ACLs de rede) e grupos de segurança. Com esses firewalls, você pode controlar, em um nível granular, o tipo de tráfego que deseja fornecer acesso ao seu banco de dados.

O uso desses controles fornece camadas de segurança para sua infraestrutura. Ele reforça que apenas as instâncias de backend têm acesso ao banco de dados.

## Banco de dados relacional

Pensar no SQL Server. Linhas, colunas e tabelas

No AWS

SQL Server

Oracle

My SQL server

PostgreSQL

Aurora

Maria DB

## Banco de dados não relacionais

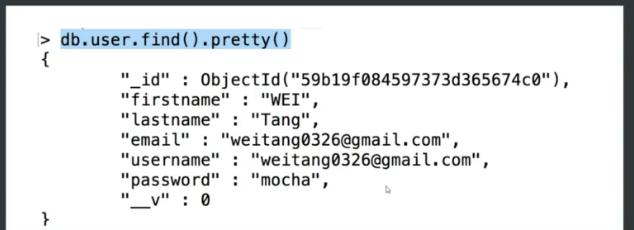
São formados por:

Collection = Table

Document = Row

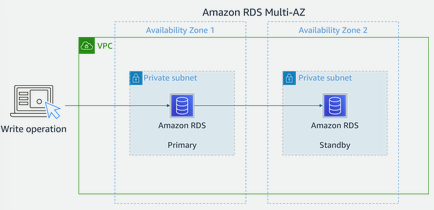
Key value Pairs = Fields

Basicamente é pensar num Json



## Multi-AZ x Read Replicas

Multi-AZ -> Para recuperação de Desastres

****

Para melhorar a disponibilidade, o Amazon RDS Multi-AZ garante que você tenha duas cópias do seu banco de dados em execução e que uma delas esteja na função primária. Se surgir um problema de disponibilidade, como o banco de dados primário perder a conectividade, o Amazon RDS iniciará um failover automático.

Quando você cria uma instância de banco de dados, um nome do Sistema de Nomes de Domínio (DNS) é fornecido. A AWS usa esse nome DNS para fazer failover para o banco de dados em espera. Em um failover automático, o banco de dados em espera é promovido para a função primária e as consultas são redirecionadas para o novo banco de dados primário.

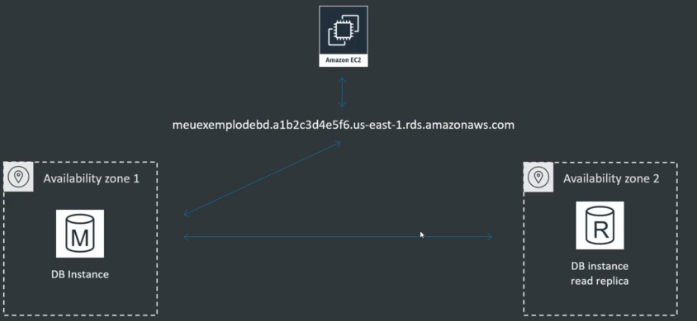
Para ajudar a garantir que você não perca a configuração Multi-AZ, há duas maneiras de criar um novo banco de dados em espera. Elas são as seguintes:

Rebaixar o primário anterior para o modo de espera se ele ainda estiver ativo e em execução.

Estabelecer uma nova instância de banco de dados em espera.

O motivo pelo qual você pode selecionar várias sub-redes para um banco de dados Amazon RDS é por causa da configuração Multi-AZ. Você vai querer garantir que tenha sub-redes em diferentes Zonas de Disponibilidade para suas cópias primária e em espera.

## Read Replicas -> Para Performance



## AWS Serviços de Banco de dados



# 22. Amazon ReadShift

Serviço de gerenciamento de banco de dados para Data Warehousing

**O que é Data WareHouse**

Usado para inteligência de negócios (BI). Ferramentas como Cognos, Jaspersoft, SQl server reporting Services, oracle Hyperion, SAP NetWeaver.

Usados para puxar dados em ambientes de dados muito grandes e complexos, geralmente usados para gerenciamento de querys de dados.

## OLTP x OLAP

Online Transaction Processin (OLTP) é diferente do Online Analytics Processing (OLAP) em termos dos tipos de queries que você executa.

OLTP – Order number 1010121 puxará dados como nome, data, endereço de entrega, status da entrega, etc.

OLAP – Lucro líquido da Petrobras no brasil e américa latina. Puxara dados em larga escala de registro de várias origens.

# 23. Elasticache

É um serviço web que torna fácil o uso para deploy, operar e escalar cache de memória na nuvem.

# 24. Auto Scaling

## Componentes do Auto scaling

### Grupos

Componente lógico, grupo de servidor web, aplicação ou grupo de banco de dados e etc.

### Templates de configuração

Grupos são usados como launch templates (templates de lançamento) ou launch configuration (configurações de lançamento) como um template para EC2. Pode especificar informações como ID da AMI, tipo de instância, Key pai, security groups.

## Opções de scaling

fornecem diversas opções para escalar os grupos de auto scaling. Por exemplo configurar um grupo para escalar baseado em uma ocorrência em específico ou com agendamentos.

### 1 - Manter as instâncias em um mesmo nível

Configurar para manter um número especificado de instâncias em execução o tempo todo.

Ele executa uma verificação de integridade periódica nas instâncias em execução em um grupo de auto scaling.

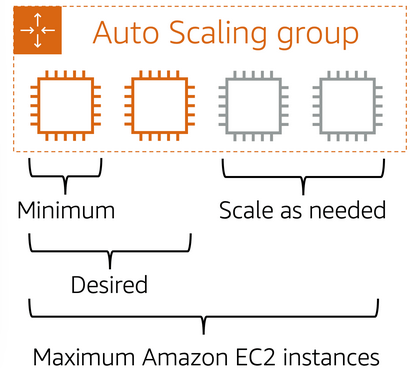
Quando encontra uma instância não íntegra, ele termina a instância e inicia uma nova.



### 2 - Escalar manualmente

Maneira mais básica de dimensionar seus recursos, onde você especifica apenas a alteração na capacidade máxima, mínima ou desejada no grupo de dimensionamento automático.

O auto scaling gerencia o processo de criação ou encerramento de instâncias para manter a capacidade atualizada.



### 3 - Escalar baseado em um agendamento

Significa que as ações de escalonamento são executadas automaticamente em função da hora e da data.

É útil quando se sabe exatamente quando aumentar ou diminuir o número de instâncias no seu grupo, simplesmente porque a necessidade surge em um cronograma previsível.

### 4 - Escalar baseado em demanda

Maneira mais avançada de dimensionar os recursos – usando políticas de dimensionamento – permite definir parâmetros que controlam o processo de dimensionamento.

Por exemplo um app web que está em duas instâncias e deseja que a utilização da cpu do grupo de auto scaling permaneça em torno de 50% quando a carga no app for alterada.

É útil para dimensionar em resposta a mudanças nas condições quando você não sabe quando essas condições mudarão. Pode-se permitir configurar a EC2 Auto scaling para responder por você.

### 5 - Escalação preditiva

Pode usar o EC2 Auto scaling com o AWS Auto Scaling para dimensionar recursos em vários serviços.

Pode ajudar a manter a disponibilidade e o desempenho ideais, combinando o dimensionamento preditivo e o dinâmico (abordagens proativas e reativas, respectivamente) para dimensionar sua capacidade do EC2 rapidamente.

# 26. ElasticBeanStalk

Implementar e gerenciar aplicativos web com rapidez sem se preocupar com infraestrutura que executa esses aplicativos.

Na prática vc escolhe o provisionamento e o server e ele monta tudo e depois vc se preocupa só com o deploy da aplicação.

É como se eu subisse o ISS com a EC2 tudo de uma vez, e daí só precisasse dar deploy do sistema sempre que fosse lançar coisa nova, mas não teria uma EC2 com ISS rodando à parte.

Você simplesmente carrega seu aplicativo e o EBS lida automaticamente com detalhes de provisionamento de capacidade, balanceamento de carga, dimensionamento e monitoramento da integridade do aplicativo.

E EBS sobe os recursos a partir de uma CloudFormation. Então quando usa um EBS ele sobe automaticamente os recursos utilizando o próprio CloudFormation.

# 27. CloudFormation

Permite criação de aplicações a partir de templates. Então se pesquisar na internet os templates para CloudFormation, tem templates que juntam funções do aws e quando lança o CloudFormation, ele se encarrega de subir todas as funções necessárias para rodar o seu template. Por exemplo, se for subir um Wordpress usando o CloudFormation, ele vai subir o RDS com mySQL, a EC2 com linux, as subnets e etc.

Na exclusão funciona da mesma forma, se excluir uma CloudFormation, ele vai excluir todos os recursos vinculados.

# 28. Arquitetando para melhores práticas de Cloud

O AWS Well-Architected Framework ajuda você a entender como projetar e operar sistemas confiáveis, seguros, eficientes e econômicos na Nuvem AWS. Ele fornece uma maneira de você medir consistentemente sua arquitetura em relação às melhores práticas e princípios de design e identificar áreas para melhoria.



## Operational excellence

a capacidade de executar e monitorar sistemas para entregar valor comercial e melhorar continuamente os processos e procedimentos de suporte.

Os princípios de design para excelência operacional na nuvem incluem executar operações como código, anotar documentação, antecipar falhas e frequentemente fazer pequenas alterações reversíveis.

## Performance efficiency

a capacidade de usar recursos de computação de forma eficiente para atender aos requisitos do sistema e manter essa eficiência conforme a demanda muda e as tecnologias evoluem.

Avaliar a eficiência de desempenho da sua arquitetura inclui experimentar com mais frequência, usar arquiteturas sem servidor e projetar sistemas para que possam se tornar globais em minutos.

## Reliability

a capacidade de um sistema de fazer o seguinte:

Recuperar-se de interrupções de infraestrutura ou serviço

Adquirir dinamicamente recursos de computação para atender à demanda

Mitigar interrupções como configurações incorretas ou problemas de rede temporários

A confiabilidade inclui testar procedimentos de recuperação, dimensionar horizontalmente para aumentar a disponibilidade agregada do sistema e recuperar-se automaticamente de falhas.

## Sustainability

a capacidade de melhorar continuamente os impactos da sustentabilidade reduzindo o consumo de energia e aumentando a eficiência em todos os componentes de uma carga de trabalho, maximizando os benefícios dos recursos provisionados e minimizando os recursos totais necessários.

Para facilitar um bom design para sustentabilidade:

Entenda seu impacto

Estabeleça metas de sustentabilidade

Maximize a utilização

Antecipe e adote novas ofertas de hardware e software mais eficientes

Use serviços gerenciados

Reduza o impacto downstream de suas cargas de trabalho na nuvem

## Computação Tradicional x Computação em Nuvem

Ativos de TI são vistos como recursos provisionados

Global, sempre disponível com capacidade escalável

Serviços gerenciados de alto nível

Segurança por padrão

Direcionado para custos

## Escalabilidade

Escalar para cima (scale up)

Escalar para os lados (scale out)

Aplicações Stateless (Sem estado)

Componente Stateless (Sem estado)

Distribuição de carga para vários nós (multiple nodes)

Implementação de afinidade de seções

## Recursos computacionais instanciados

Bootstrapping

Golden Images

Containers

Hybrid

Infraestrutura como código

CloudFormation

## Automação

Gerenciamento e Deploy Serverless - funções Lambda

Gerenciamento e deploy de infraestrutura

AWS Elastic Beanstalk

EC2 auto recovery

System Manager

Auto Scaling

Eventos e alarmes

CloudWatch alarmes

CloudWatch Eventos

Eventos agendados do aws Lambda

Automações de segurança com o AWS WAF

## Serviços desacoplados

Amazon API Gateway

Service discovery

## Foco em serviços e não servidores

Serviços gerenciados

Arquitetura Serverless

## Banco de dados

Banco de dados relacionais (Aurora)

Banco de dados não relacionais (DynamoDB)

## Data Warehouse (ReadShift)

Todos escaláveis e com alta Disponibilidade – multi – az

Graph Database – Neptune

## Mecanismos de busca

CloudSearch

Amazon ElasticSearch

## Gerenciamento de aumento de volume de dados

O Data Lake é um modelo arquitetural que permite armazenar grandes volumes de dados numa localização central que é rapidamente disponível, pode ser categorizado, processado, analisado e consumido por diversos grupos em sua organização.

Como os dados podem ser armazenados como eles são, você não precisa convertê-los em qualquer esquema pré-definido.

## Remoção de pontos únicos de falha

Pensar em redundância

Detectar falhas

Armazenamento de dados duráveis

Resiliência Multi-Data centers

Isolamento e Escalar Horizontalmente

Sharding

## Otimizar para custos

a capacidade de executar sistemas para entregar valor comercial ao menor preço.

A otimização de custos inclui adotar um modelo de consumo, analisar e atribuir despesas e usar serviços gerenciados para reduzir o custo de propriedade.

Tamanho correto

Elasticidade

Avaliar opções de compra de recursos

## Cache

Cache de aplicações

Edge Caching – Edge Locations

## Segurança

a capacidade de proteger informações, sistemas e ativos, ao mesmo tempo em que fornece valor comercial por meio de avaliações de risco e estratégias de mitigação.

Ao considerar a segurança da sua arquitetura, aplique estas práticas recomendadas:

Automatize as práticas recomendadas de segurança quando possível.

Aplique segurança em todas as camadas.

Proteja os dados em trânsito e em repouso.

Usar as funcionalidades da AWSD para defesa em camadas

Segurança compartilhada com a aws

Reduzir acesso privilegiado

Segurança como código

Auditoria em tempo real

## Serviços globais da AWS

IAM

Route 53

CloudFront

AWS S3 - Serviço global com visão regional

## Serviços usados On Premises

Serviços que rodam no seu datacenter local

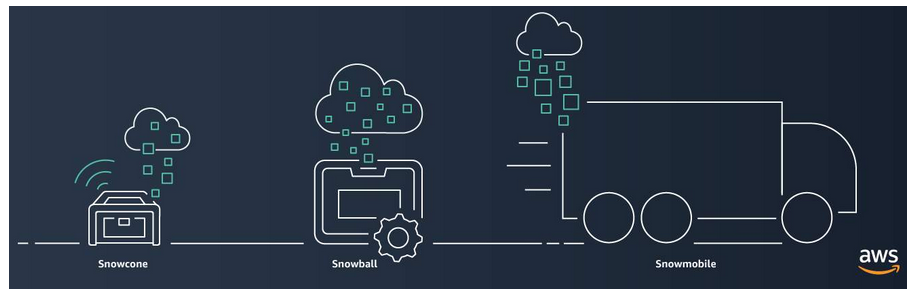
Code Deploy – Deploy de código

Ops Works – Deploy de aplicações

IotGreenGrass – Usado para conectar dispositivos IoT e enviar os dados para nuvem.

### AWS Snowcone, AWS Snowball, and AWS Snowmobile

Usados para migrar grandes dados para o AWS





**AWS Snowcone** é um dispositivo de transferência de dados e computação de ponta pequeno, robusto e seguro.

Ele possui 2 CPUs, 4 GB de memória e até 14 TB de armazenamento utilizável.

**O AWS Snowball** oferece dois tipos de dispositivos:

Os dispositivos **Snowball Edge Storage Optimized** são adequados para migrações de dados em larga escala e fluxos de trabalho de transferência recorrentes, além de computação local com necessidades de maior capacidade.

Armazenamento: 80 TB de capacidade de unidade de disco rígido (HDD) para volumes de bloco e armazenamento de objetos compatível com Amazon S3 e 1 TB de unidade de estado sólido (SSD) SATA para volumes de bloco.

Computação: 40 vCPUs e 80 GiB de memória para oferecer suporte a instâncias Amazon EC2 sbe1 (equivalente a C5).

O **Snowball Edge Compute Optimized** fornece recursos de computação poderosos para casos de uso como aprendizado de máquina, análise de vídeo em movimento completo, análises e pilhas de computação local.

Armazenamento: capacidade de HDD utilizável de 80 TB para armazenamento de objetos compatível com Amazon S3 ou volumes de bloco compatíveis com Amazon EBS e 28 TB de capacidade de SSD NVMe utilizável para volumes de bloco compatíveis com Amazon EBS.

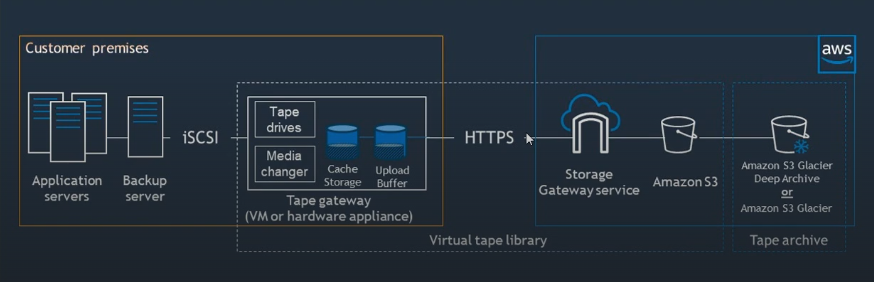
Computação: 104 vCPUs, 416 GiB de memória e uma GPU NVIDIA Tesla V100 opcional. Os dispositivos executam instâncias Amazon EC2 sbe-c e sbe-g, que são equivalentes às instâncias C5, M5a, G3 e P3.

**AWS Snowmobile** é um serviço de transferência de dados em escala de exabytes usado para mover grandes quantidades de dados para a AWS.

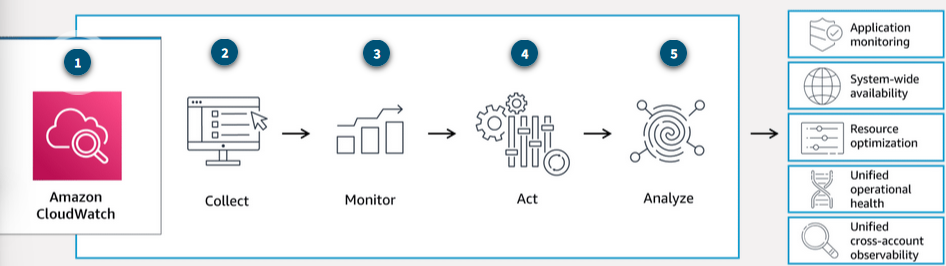
Você pode transferir até 100 petabytes de dados por Snowmobile, um contêiner de transporte reforçado de 45 pés de comprimento, puxado por um caminhão semirreboque.

### Storage Gateway

Utiliza a infra local e o cache pelo AWS



# 29. CloudWatch



É um serviço de monitoramento de recursos AWS, assim como aplicações que estejam rodando na AWS.

É possível instalar CloudWatch em computadores On Premises, que não estão no AWS. Para conseguir monitorá-los a partir da nuvem tmb.

Muitos serviços da AWS enviam métricas automaticamente para o CloudWatch gratuitamente a uma taxa de 1 ponto de dados por métrica a cada intervalo de 5 minutos. Isso é chamado de monitoramento básico e fornece visibilidade dos seus sistemas sem nenhum custo extra. Para muitos aplicativos, o monitoramento básico é adequado.

Para aplicativos em execução em instâncias EC2, você pode obter mais granularidade postando métricas a cada minuto em vez de a cada 5 minutos usando um recurso como monitoramento detalhado. O monitoramento detalhado incorre em uma taxa.

Com o CloudWatch, você pode criar alarmes que executam ações automaticamente se o valor da sua métrica ficar acima ou abaixo de um limite predefinido.

Detecte comportamento anômalo em seus ambientes.

•Defina alarmes para alertá-lo quando algo não estiver certo.

•Visualize logs e métricas com o AWS Management Console.

•Tome ações automatizadas, como dimensionamento.

•Solucione problemas.

•Descubra insights para manter seus aplicativos saudáveis.

Serve para monitorar nível de performance.

## Métricas personalizadas

Suponha que você tenha um aplicativo e queira registrar o número de visualizações de página que seu site obtém. Como você registraria essa métrica com o CloudWatch? Primeiro, é uma métrica de nível de aplicativo. Isso significa que não é algo que a instância do EC2 postaria no CloudWatch por padrão. É aqui que entram as métricas personalizadas. Com métricas personalizadas, você pode publicar suas próprias métricas no CloudWatch.

Se quiser obter visibilidade mais granular, você pode usar métricas personalizadas de alta resolução, que possibilitam coletar métricas personalizadas com resolução de até 1 segundo. Isso significa que você pode enviar 1 ponto de dados por segundo por métrica personalizada.

Alguns exemplos de métricas personalizadas incluem o seguinte:

•Tempos de carregamento de página da Web

•Taxas de erro de solicitação

•Número de processos ou threads em sua instância

•Quantidade de trabalho realizado pelo seu aplicativo

## Monitora recursos como:

Computacional

Instâncias EC2

Autoscaling groups

Elastic Load Balancers

Saúde do Route 53

Armazenamento e entrega de conteúdo

Volume EBS

Storage Gateways

CloudFront

Métricas de nível de hosts:

CPU / Rede / Disco / Status Check

# 30. CloudTrail

Funciona como uma auditoria. Aumenta a visibilidade de suas atividades de usuários e recursos, registrando ações do AWS Management console e chamadas de API.

Consegue identificar quais usuários e contas AWS chamaram, o endereço de IP de origem a partir do qual as chamadas foram feitas e quando a chamada ocorreu.

Com o CloudTrail, você pode visualizar um histórico completo das atividades do usuário e chamadas de API para seus aplicativos e recursos.

No CloudTrail, você também pode habilitar o CloudTrail Insights(abre em uma nova aba). Esse recurso opcional permite que o CloudTrail detecte automaticamente atividades incomuns de API na sua conta da AWS.

Por exemplo, o CloudTrail Insights pode detectar que um número maior de instâncias do Amazon EC2 do que o normal foram lançadas recentemente na sua conta. Você pode então revisar os detalhes completos do evento para determinar quais ações você precisa tomar em seguida.

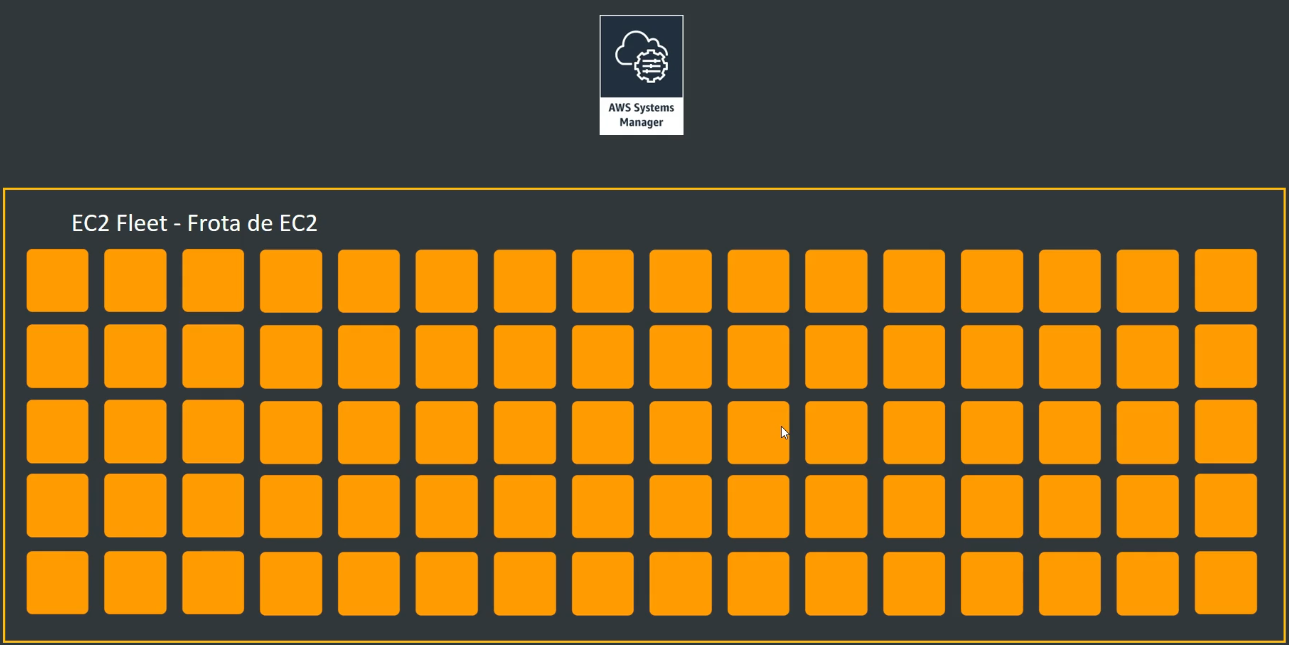
## CloudWatch x CloudTrail

CloudWatch monitora performance

CloudTrail monitora chamadas de API feitas na plataforma AWS

# 31. AWS System Manager

Permite gerenciar instâncias EC2 em escala. Que é chamado de EC2 Fleet – Frota de EC2



Por exemplo um “run Command” que roda comandos de SO em todas as máquinas ao mesmo tempo.

Um pedaço de software é instalado em cada VM

Pode ser dentro do AWS e on-premises

Integra-se ao CloudWatch para fornecer Dashboard de toda a sua infraestrutura.

# 32. Precificação no AWS

## Diferentes modelos de preço

### Capex x Opex

Capex significa Despesas de capital que você paga antecipadamente. Custo fixo irrecuperável.

Opex significa despesas operacionais que é onde você paga pelo que usa.

## Política de preço

Pague menos conforme o uso

Pague menos quando reservar

Pague ainda menos por unidade usando mais

Pague ainda memo com o crescimento do AWS

## AWS Free Tier

Três tipos de ofertas estão disponíveis:

Sempre grátis

12 meses grátis

Testes

## Fundamentos de precificação do AWS

Fatores fundamentais de custo

Computação / armazenamento/ dados de saída

## Usar o modelo certo para o trabalho

Modelos de preço

Sob demanda

Instâncias dedicadas

Instâncias apor

Reservas

## Serviços sempre gratuitos

Amazon VPC

Elástico Beanstalk

CloudFormation

Gerenciamento de acesso a identidade (IAM)

Escala automática

Opswork

Fatiamento consolidado (Consolidated Billings)

## Precificação da EC2

Horas usadas no servidor

Tipo de instância

Modelo de preço

Número de instância

Loas Balancing

Monitoramento detalhado

Auto scaling

Elastic IP adresses

Sistema operacional e pacotes

## Modelos de preço da ec2

Sob demanda – paga taxa fixa por hora

Reservado – reserva de capacidade que pode ser contratado por 1 ou 3 anos

Spot – permite oferecer qualquer preço que desejar pela capacidade desejada proporcionando economia ainda maior se os app tiverem horário de início e fim flexíveis.

Hosts Dedicados – máquina dedicadas ao seu uso exclusivo. Permite o uso de suas licenças de software vinculadas ao servidor existente.

## Tipos de reserva de preços

### Reserva padrão

Até 75% de desconto em ec2 sob demanda.

### Reserva conversível

Até 54% de desconto na ec2 sob demanda que permite alterar atributos desde que a troca resulte na criação de instâncias reservadas de valor igual ou superior.

### Reservas agendadas

Disponíveis para serem lançadas dentro de janelas de tempo que vc reserva. Permite combinar reserva de capacidade com uma programação recorrente previsível que requer apenas uma fração de um dia, uma semana ou um mês.

## Precificação do lambda

### Por requisição

Até 1M por mês de graça, depois 0,20 por 1M de requisições

### Por duração

400,000GB por segundo por mês grátis, e até 3,2M de segundo de tempo de computação. 0,00001667 por cada GB por segundo usado

## Precificação do EBS

Volume por GB

Snapshots por GB

Transferência de dados

## Precificação do S3

Armazenamento

Requisições

Tipos de classes de armazenamento

Transferência de dados

Aceleração de transferência

## Precificação do RDS

Horas ligadas do servidor

Características do banco de dados

Tipo de banco de dados

Armazenamento provisionado

Armazenamento adicional

Requisições

Transferência de dados

## Precificação do CloudFront

Distribuição do tráfego

Requests

Saída de dados

# 33. AWS Billing e Cost Management Dashboard

Use o painel AWS Billing & Cost Management (abre em uma nova aba) para pagar sua fatura da AWS, monitorar seu uso e analisar e controlar seus custos.

Compare seu saldo atual do mês até a data com o do mês anterior e obtenha uma previsão do próximo mês com base no uso atual.

Veja os gastos do mês até a data por serviço.

Veja o uso do Free Tier por serviço.

Acesse o Cost Explorer e crie orçamentos.

Compre e gerencie Savings Plans.

Publique AWS Cost and Usage Reports (abre em uma nova aba).

# 33. AWS Budget

Permite definir orçamentos personalizados que alertam quando seus custos ou uso excedem (ou se prevê que irão exceder) seu valor orçado.

Usado para orçar os custos antes de serem incorridos.

No AWS Budgets você pode criar orçamentos para planejar o uso do serviço, os custos do serviço e as reservas de instância.

As informações no AWS Budgets são atualizadas três vezes por dia. Isso ajuda você a determinar com precisão o quão próximo seu uso está dos valores orçados ou dos limites do AWS Free Tier.

No AWS Budgets, você também pode definir alertas personalizados quando seu uso exceder (ou estiver previsto para exceder) o valor orçado.

# 34. AWS cost explorer

Visualizar cobranças ao longo do tempo

Utilizado para explorar os custos após a ocorrência

AWS Cost Explorer é uma ferramenta que permite visualizar, entender e gerenciar seus custos e uso da AWS ao longo do tempo.

AWS Cost Explorer inclui um relatório padrão dos custos e uso para seus cinco principais serviços da AWS com acúmulo de custos. Você pode aplicar filtros e grupos personalizados para analisar seus dados. Por exemplo, você pode visualizar o uso de recursos no nível de hora em hora.

# 35. Tags

Etiquetas de valor-chave anexados aos recursos do AWS

Metadados (dados sobre dados)

As vezes as tags podem ser herdadas

Grupos de recursos facilitam o agrupamento de recursos usando tags atribuídas.

Podem conter informações como

Região/ nome / id do empregado/ departamento

Pode ter informações específicas

Para ec2 – endereços de ip público e privado

Para elb – configuração de porta

Para rds- mecanismo de banco de dados, etc.

# 36. AWS Organizations

Serviço de gerenciamento de contas que permite consolidar várias contas da AWS em uma organização de maneira centralizada.

Permite aplicar políticas de acesso entre contas e permite consolidar os pagamentos de uma maneira só.

O número máximo padrão de contas permitidas para uma organização é 4, mas você pode entrar em contato com o Suporte da AWS para aumentar sua cota, se necessário.

## Vantagens

Uma fatura por conta

Fácil de rastrear cobranças e alocar custo

Desconto de preços por volume

Alocação de reservas de recursos entre as contas. Saving plans entre contas

É recomendado que a conta payer(pagante) seja usada apenas pra billing e nenhum outro serviço rode nela

Usar sempre SCP (SERVICE control policies) para habilitar/desabilitar algum serviço de maneira global por OU (Organizational units)

## Service Control Policies (SCPs)

Os SCPs permitem que você imponha restrições aos serviços, recursos e ações individuais da API da AWS que usuários e funções em cada conta podem acessar.

Você pode aplicar políticas de controle de serviço (SCPs) **à raiz da organização, a uma conta de membro individual ou a uma UO**

## Organizational units

No AWS Organizations, você pode agrupar contas em unidades organizacionais (OUs) para facilitar o gerenciamento de contas com requisitos comerciais ou de segurança semelhantes. Quando você aplica uma política a uma OU, todas as contas na OU herdam automaticamente as permissões especificadas na política.

Ao organizar contas separadas em OUs, você pode isolar mais facilmente cargas de trabalho ou aplicativos que têm requisitos de segurança específicos. Por exemplo, se sua empresa tiver contas que podem acessar apenas os serviços da AWS que atendem a determinados requisitos regulatórios, você pode colocar essas contas em uma OU. Em seguida, você pode anexar uma política à OU que bloqueia o acesso a todos os outros serviços da AWS que não atendem aos requisitos regulatórios.

# 37. AWS Quick start

Maneira de implementar ambientes rapidamente, usando modelos do CloudFormation criados por arquitetos de soluções da AWS, especialistas na tecnologia específica.

Então acessando o Quick Start é possível achar uma arquitetura pronta pra rodar SAP por exemplo, ou p rodar blockchain… escolhendo o template, o AWS já provisiona os recursos que são necessários para rodar o ambiente.

# 38. AWS Landing Zone

Ajuda a configurar mais rapidamente um ambiente seguro entre contas do AWS, com base nas práticas recomendadas.

Então, tendo um cenário de várias contas, é possível utilizar o landing zone pra entender as melhores práticas de configuração entre contas da empresa.

# 39. Calculadora AWS

## Dois modelos disponíveis

### AWS Simple Monthly calculator

Usado para calcular os custos correntes mensais na AWS. Não é uma ferramenta de comparação.

### AWS total cost of ownership calculator (calculadora de custo total de propriedade da AWS)

Usado para comparar custo de rodar sua infra on-premisses x na nuvem.

Gera relatórios comparativos pra ter um plano de negócios para uma eventual mudança para nuvem.

# 40. AWS Compliance

Site do AWS que mostra quais certificado e ISO que o AWS possui e trabalha com

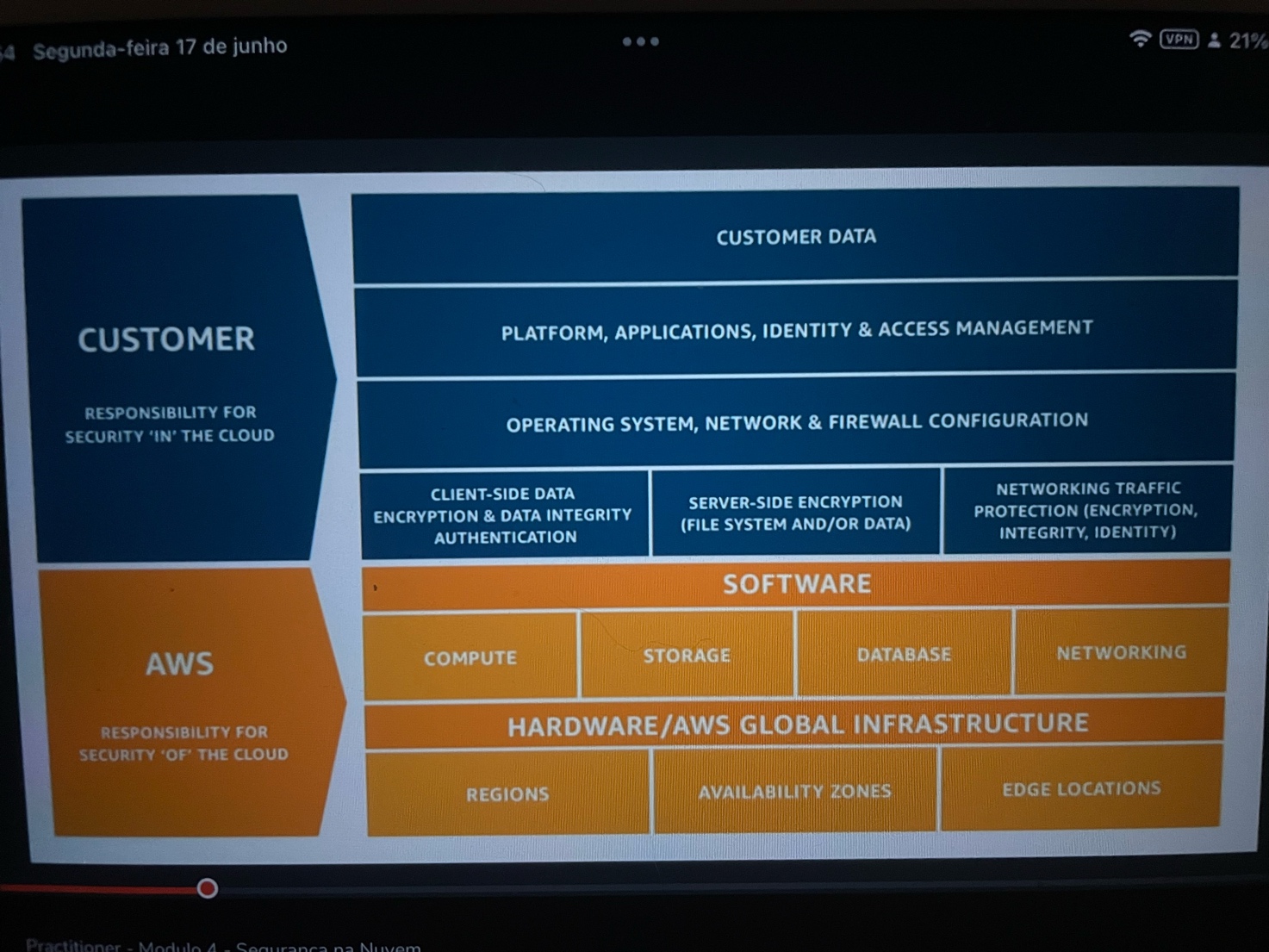
## AWS Artifact

Ferramenta do console que permite fazer download de todos os relatórios referentes aos compliances que o AWS trabalha.

Serve para apresentar em auditorias e apresentações para comprovar a segurança da infra.

## Modelo de responsabilidade compartilhada

O AWS gerencia a segurança da nuvem enquanto o cliente é responsável pela segurança na nuvem. O cliente mantém controle sobre qual segurança eles escolhem implementar para proteger seu próprio conteúdo, da mesma forma que em um datacenter local.



Dentro da página de compliance do AWS tem o modelo de responsabilidade compartilhada com a explicação detalhada.

Na prova, visualize o que a pergunta realmente indaga.

- Você pode fazer isso no console da AWS ou no EC2?

Se sim, provavelmente é responsável. Grupos de segurança, usuários do IAM, sistemas operacionais com patch EC2, banco de dados com patches em execução no Ec2 etc.

Caso contrário, a AWS provavelmente será responsável. Gerenciamento de data centers, câmeras de segurança, cabeamento, correção de sistema operacional, RDS etc.

**Criptografia é uma responsabilidade compartilhada.**

# 41. AWS Suporte

A AWS oferece quatro planos de suporte diferentes para ajudar você a solucionar problemas, reduzir custos e usar os serviços da AWS de forma eficiente.

Você pode escolher entre os seguintes planos de suporte para atender às necessidades da sua empresa:

## Básico

Gratuito para todos os clientes da AWS. Inclui acesso a whitepapers, documentação e comunidades de suporte. Com o Suporte Básico, você também pode entrar em contato com a AWS para perguntas sobre cobrança e aumentos de limite de serviço.

Com o Suporte Básico, você tem acesso a uma seleção limitada de verificações do AWS Trusted Advisor. Além disso, você pode usar o AWS Personal Health Dashboard, uma ferramenta que fornece alertas e orientação de correção quando a AWS está passando por eventos que podem afetá-lo.

## Desenvolvedor

Os clientes no plano Developer Support têm acesso a recursos como:

Orientação de melhores práticas

Ferramentas de diagnóstico do lado do cliente

Suporte à arquitetura de blocos de construção, que consiste em orientação sobre como usar ofertas, recursos e serviços da AWS juntos.

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

## Empresarial

Os clientes com um plano Business Support têm acesso a recursos adicionais, incluindo:

Orientação de caso de uso para identificar ofertas, recursos e serviços da AWS que podem dar melhor suporte 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 Business Support e queira instalar um sistema operacional comum de terceiros 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 otimização de desempenho, uso de scripts personalizados ou resolução de problemas de segurança, pode ser necessário entrar em contato diretamente com o fornecedor de software de terceiros.

## Enterprise On-Ramp

Além de todos os recursos incluídos nos planos Basic, Developer e Business Support, os clientes com um plano Enterprise On-Ramp Support têm acesso a:

Um grupo de gerentes de contas técnicas para fornecer orientação proativa e coordenar o acesso a programas e especialistas da AWS

Um workshop de otimização de custos (um por ano)

Uma equipe de suporte do Concierge para cobrança e assistência de conta

Ferramentas para monitorar custos e desempenho por meio do Trusted Advisor e Health API/Dashboard

O plano Enterprise On-Ramp Support também fornece acesso a um conjunto específico de serviços de suporte proativos, que são fornecidos por um grupo de gerentes de contas técnicas.

Revisão consultiva e orientação de arquitetura (um por ano)

Suporte ao Infrastructure Event Management (um por ano)

Fluxos de trabalho de automação de suporte

Tempo de resposta de 30 minutos ou menos para problemas críticos de negócios

## Enterprise

Clientes com Enterprise Support têm acesso a:

Um Technical Account Manager designado para fornecer orientação proativa e coordenar o acesso a programas e especialistas da AWS

Uma equipe de suporte do Concierge para cobrança e assistência de conta

Revisões de operações e ferramentas para monitorar a saúde

Treinamento e Game Days para impulsionar a inovação

Ferramentas para monitorar custos e desempenho por meio do Trusted Advisor e Health API/Dashboard

O plano Enterprise também fornece acesso total a serviços proativos, que são fornecidos por um Technical Account Manager designado:

Revisão consultiva e orientação de arquitetura

Suporte ao Infrastructure Event Management

Workshop e ferramentas de otimização de custos

Fluxos de trabalho de automação de suporte

Tempo de resposta de 15 minutos ou menos para problemas críticos de negócios

# 41. AWS MarketPlace

O AWS Marketplace é um catálogo digital que inclui milhares de listagens de software de fornecedores independentes. Você pode usar o AWS Marketplace para encontrar, testar e comprar software que roda na AWS.

Para cada listagem no AWS Marketplace, você pode acessar informações detalhadas sobre opções de preços, suporte disponível e avaliações de outros clientes da AWS.

Você também pode explorar soluções de software por setor e caso de uso. Por exemplo, suponha que sua empresa esteja no setor de saúde. No AWS Marketplace, você pode revisar casos de uso que o software ajuda a abordar, como implementar soluções para proteger registros de pacientes ou usar modelos de aprendizado de máquina para analisar o histórico médico de um paciente e prever possíveis riscos à saúde.



# 41. AWS Config

Fornece uma visão detalhada da configuração dos recursos da AWS. Isso inclui como os recursos estão relacionados entre si e como foram configurados no passado, para que você possa ver como as configurações e os relacionamentos mudam com o tempo.

# 42. AWS Identity and Access Management (IAM)

O AWS Identity and Access Management (IAM) permite que você gerencie o acesso aos serviços e recursos da AWS com segurança.

O IAM oferece a flexibilidade de configurar o acesso com base nas necessidades operacionais e de segurança específicas da sua empresa. Você faz isso usando uma combinação de recursos do IAM, que são:

Usuários, grupos e funções do IAM

Políticas do IAM

Autenticação multifator

Prática recomendada:

**Não use o usuário root para tarefas cotidianas**.

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

Em seguida, continue a criar outros usuários do IAM e acesse essas identidades para executar tarefas regulares em toda a AWS. Use o usuário root somente quando precisar executar um número limitado de tarefas que estão disponíveis apenas para o usuário root. Exemplos dessas tarefas incluem alterar seu endereço de e-mail de usuário root e alterar seu plano de suporte da AWS.

## IAM users

Um usuário do IAM é uma identidade que você cria na AWS. Ele representa a pessoa ou aplicativo que interage com serviços e recursos da AWS. Ele consiste em um nome e credenciais.

Por padrão, quando você cria um novo usuário do IAM na AWS, ele não tem 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.

## IAM policies

Uma política do IAM é um documento que permite ou nega permissões para serviços e recursos da 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 dentro da sua conta da AWS, ou apenas um bucket específico.

Siga o princípio de segurança do menor privilégio ao conceder permissões.

Ao seguir esse princípio, você ajuda a evitar que usuários ou funções tenham mais permissões do que o necessário para executar suas tarefas.

A maioria das políticas do IAM são armazenadas na AWS como documentos JSON. Elas têm vários elementos de política, incluindo uma Versão, Efeito, Ação e Recurso.

## IAM groups

Um grupo IAM é uma coleção de usuários IAM. Quando você atribui uma política IAM a um grupo, todos os usuários no grupo recebem permissões especificadas pela política.

## IAM roles

O funcionário pode alternar facilmente entre estações de trabalho, mas em qualquer momento, ele pode ter acesso a apenas uma única estação de trabalho. Esse mesmo conceito existe na AWS com funções do IAM.

Uma função do IAM é uma identidade que você pode assumir para obter acesso temporário a permissões.

Antes que um usuário, aplicativo ou serviço do IAM possa assumir uma função do IAM, ele deve receber permissões para alternar para a função. 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.

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

## Melhores práticas para usuários root da AWS

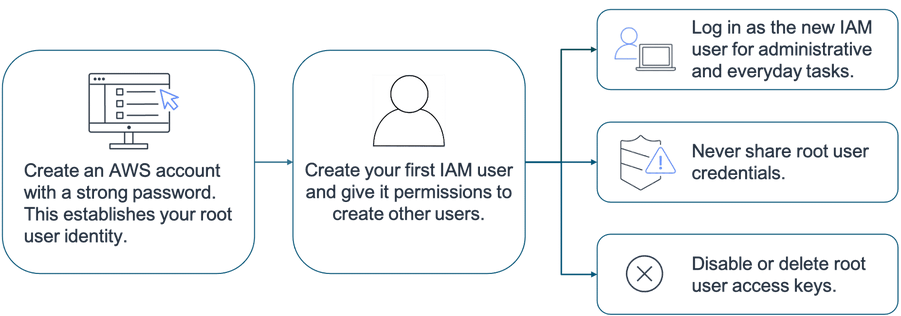
Para garantir a segurança do usuário root, siga estas práticas recomendadas:

Escolha uma senha forte para o usuário root.

Habilite a autenticação multifator (MFA) para o usuário root.

Nunca compartilhe sua senha de usuário root ou chaves de acesso com ninguém.

Desabilite ou exclua as chaves de acesso associadas ao usuário root.

Crie um usuário do Identity and Access Management (IAM) para tarefas administrativas ou tarefas cotidianas.

# 42. AWS Athena

Serviço de consulta interativo que permite analisar e consultar dados localizamos no S3 usando padrão de linguagem SQL.

- Serverless, nada a provisionar, cobrado por consulta / por TB analisado.

- Não precisa de configuração de extração de dados/ transformação/ carga (ETL)

- Funciona diretamente com dados armazenados no S3

## Para que usar?

- Pode ser usado para consultar arquivos de log armazenados no S3. Ex: Logs ELB, logs de acesso e etc.

- Gerar relatórios comerciais sobre dados armazenados no s3.

- Analisar relatórios de custos e uso da AWS.

- Executar consultas nos dados de streaming.

# 43. AWS Macie

Ligado à segurança de dados PII (personal identification information)

- Dados pessoais usados pra estabelecer a identidade de um indivíduo.

O macie é um serviço de segurança que usa machine learning e NLP (natural language Processing) para descobrir, classificar e proteger dados confidenciais armazenados no S3.

Usa AI para reconhecer os objetos no S3 e se contém dados confidenciais.

Pode-se criar Dashboards, relatórios e alertas.

Pode analisar logs do CloudTrail.

Ótimo para PCI-DDS e prevenção de roubo de identidade.

# 44. AWS Cloud Adoption Framework (AWS CAF)

Organiza a orientação em seis áreas de foco, chamadas Perspectivas. Cada Perspectiva aborda responsabilidades distintas. O processo de planejamento ajuda as pessoas certas em toda a organização a se prepararem para as mudanças futuras.

Em geral, as Perspectivas de Negócios, Pessoas e Governança focam em capacidades de negócios, enquanto as Perspectivas de Plataforma, Segurança e Operações focam em capacidades técnicas.

## Business Perspective

garante que a TI esteja alinhada com as necessidades do negócio e que os investimentos em TI estejam vinculados aos principais resultados do negócio.

Use a Perspectiva de Negócios para criar um caso de negócios forte para adoção da nuvem e priorizar iniciativas de adoção da nuvem. Garanta que suas estratégias e objetivos de negócios estejam alinhados com suas estratégias e objetivos de TI.

Funções comuns na Perspectiva de Negócios incluem:

Gerentes de negócios

Gerentes financeiros

Proprietários do orçamento

Partes interessadas da estratégia

## People Perspective

suporta o desenvolvimento de uma estratégia de gerenciamento de mudanças em toda a organização para 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, equipe e mudanças organizacionais.

Funções comuns na Perspectiva de Pessoas incluem:

Recursos humanos

Equipe

Gerentes de pessoas

## Governance Perspective

foca nas habilidades e processos para alinhar a estratégia de TI com a estratégia de negócios. Isso garante que você maximize o valor do negócio 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 avalie os investimentos em nuvem para avaliar os resultados de negócios.

Funções comuns na Perspectiva de Governança incluem:

Diretor de Informação (CIO)

Gerentes de programa

Arquitetos corporativos

Analistas de negócios

Gerentes de portfólio

## Platform Perspective

inclui princípios e padrões para implementar novas soluções na nuvem e migrar cargas de trabalho locais para a nuvem.

Use uma variedade de modelos arquitetônicos para entender e comunicar a estrutura dos sistemas de TI e seus relacionamentos. Descreva a arquitetura do ambiente de estado de destino em detalhes.

Funções comuns na Perspectiva da Plataforma incluem:

Diretor de Tecnologia (CTO)

Gerentes de TI

Arquitetos de soluções

## Security Perspective

garante que a organização atenda aos objetivos de segurança para visibilidade, auditabilidade, controle e agilidade.

Use o AWS CAF para estruturar a seleção e implementação de controles de segurança que atendam às necessidades da organização.

Funções comuns na Perspectiva de Segurança incluem:

Diretor de Segurança da Informação (CISO)

Gerentes de segurança de TI

Analistas de segurança de TI

## Operations Perspective

ajuda você a habilitar, executar, usar, operar e recuperar cargas de trabalho de TI no nível acordado com as partes interessadas do seu negócio.

Defina como os negócios do dia a dia, trimestre a trimestre e ano a ano são conduzidos. Alinhe e dê suporte às operações do negócio. O AWS CAF ajuda essas partes interessadas a definir os procedimentos operacionais atuais e identificar as mudanças de processo e o treinamento necessários para implementar a adoção bem-sucedida da nuvem.

Funções comuns na Perspectiva de Operações incluem:

Gerentes de operações de TI

Gerentes de suporte de TI

# 45. 6 estratégias para migração

Ao migrar aplicativos para a nuvem, seis das estratégias de migração mais comuns que você pode implementar são:

## Rehosting

Rehosting também conhecido como “lift-and-shift” envolve mover aplicativos sem alterações.No cenário de uma grande migração de legado, na qual a empresa está buscando implementar sua migração e escalar rapidamente para atender a um caso de negócios, a maioria dos aplicativos é rehospedada.

## Replatforming

Replatforming, também conhecido como “lift, tinker, and shift,” envolve fazer algumas otimizações de nuvem para obter um benefício tangível. A otimização é alcançada sem alterar a arquitetura central do aplicativo.

## Refactoring/re-architecting

Refatoração (também conhecida como re-arquitetura) envolve reimaginar como um aplicativo é arquitetado e desenvolvido usando recursos nativos da nuvem. A refatoração é motivada por uma forte necessidade comercial de adicionar recursos, escala ou desempenho que, de outra forma, seriam difíceis de atingir no ambiente existente do aplicativo.

## Repurchasing

A recompra envolve a mudança de uma licença tradicional para um modelo de software como serviço. Por exemplo, uma empresa pode escolher implementar a estratégia de recompra migrando de um sistema de gerenciamento de relacionamento com o cliente (CRM) para o Salesforce.com.

## Retaining

Retenção consiste em manter aplicativos que são críticos para o negócio no ambiente de origem. Isso pode incluir aplicativos que exigem grande refatoração antes de poderem ser migrados, ou trabalho que pode ser adiado para um momento posterior.

## Retiring

Aposentadoria é o processo de remoção de aplicativos que não são mais necessários.

# 46. Exame de certificação

<https://d1.awsstatic.com/training-and-certification/docs-cloud-practitioner/AWS-Certified-Cloud-Practitioner_Exam-Guide.pdf>

https://wmx-api-production.s3.amazonaws.com/courses/56802/supplementary/AWS%20Exam%20Preparation%20Official%20Practice%20Question%20Sets%20Overview%20and%20Instructions.pdf

Format: Multiple choice and multiple response questions only

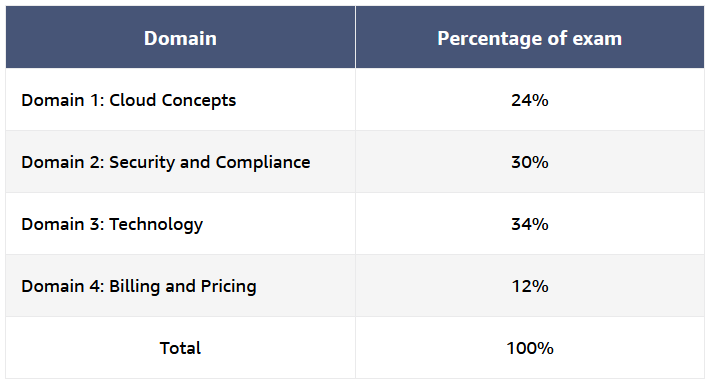
Type: Foundational

Delivery method: Pearson VUE testing center or online proctored exam

Number of questions: 65

Time: 90 minutes

Cost: 100 USD



## Official Practice Question Set

<https://awscertificationpractice.benchprep.com/app/aws-certified-cloud-practitioner-official-practice-question-set-clf-c02#exams>

# 47. Exemplo de Questões

1 - What are benefits of using the AWS cloud for companies with customers in many countries around the world? (select two)

a - companies can deploy applications in multple AWS regions to reduce latency

b - Amazon translate automatically translates third-party website interfaces into multiple languages

c - Amazon CloudFront has multiple edge locations around the world to reduce latency

d - Amazon comprehend allows users to build applications that can respond to user request in many languages

e - Elastic Load Balancing can distribute application web traffic to multiple AWS regions around the world, which reduces latency

Correct Answer: A,C

2 - A company wants to establish a consistent and private connection from the company's on-premises data center to the AWS Cloud.

Which AWS Service will meet theses requirements?

a - AWS Client VPN

b - Amazon Connect

c - AWS Direct Connect

d - AWS Site-to-Site VPN

Correct Answer: C

3 - Which AWS service should be used to implement encryption in transit?

a - AWS Certificate Manager (ACM)

b - AWS Resource Access Manager (AWS RAM)

c - AWS Shield

d - AWS Security Hub

Correct Answer: A

4 - A user needs to automatically discover, classify, and protect sensitive data stored in Amazon S3?

Which AWS service can meet theses requirements?

a - Amazon Inspector

b - Amazon Macie

c - Amazon GuardDuty

d - AWS Secrets Manager

Correct Answer: B

5 - Whats are the advantages of deploying an application with Amazon EC2 instances in multiple Availability Zones? (Select two)

a - Preventing a single point of failure

b - Reducing the operational costs of the application

c - Allowing the application to serve cross-Region users with low latency

d - Increasin the availability of the application

e - Increasing the load of the application

Correct Answer: A,D

6 - Which AWS service allows customers to purchase unused Amazon EC2 capacity at an often discounted rate?

a - Reserved Instances

b - On-Demand Instances

c - Dedicated instances

d - Sport Instances

Correct Answer: D

7 - A company requires an encrypted connection between the company's on-premises servers and AWS. The connection must use the company's existing internet connection. Which solution will meet theses requirements?

a - AWS Direct Connect

b - Amazon Connect

c - Amazon CloudFront

d - AWS Site-to-Site VPN

Correct Answer: D

8 - Which tasks are the customer's responsibility according to the AWS shared responsibility model? (select two)

a - Patch the operating system that AWS Lambda functions use.

b - Install pacthes on Amazon RDS DB instances.

c - Control physical access to the data center that contains a customer's VPC

d - Configure IAM users according to the principle of least privilege

e - Configure an Amazon S3 bucket to allow public access

Correct Answer: D,E

9 - How does AWS charge for AWS Lambda usage once the free tier has been exceeded? (select two)

a - by the time it takes for the Lambda function to run

b - by the number of versions of the specific Lambda function

c - By the number of requests made for a given Lambda function

d - By the programming language that is used for Lambda function

e - by the total number of Lambda functions in an AWS Account

Correct Answer: A,C

10 – Each department within a company has its own independent AWS account and its own payment method. The company needs to centralize departmanetal governance and consolidate payments. How can the company achieve theses objectives by using AWS services or features?

A – Use AWS cloud map on each departmental account

B – Create an organization in aws organizations with all features enabled whitin one account. Invite all accounts to join the organization.

c – use aws systema manager opscenter.

D – use the aws cost and usage reports page of the aws billing and cost management console.

Correct Answer: B

11 – a user deploys an amazon rds db instance in multiple availability zones. This strategy involves which pillar of the aws well-architected framework?

A – performance efficiency

B – realiability

C – cost optimization

D – security

Correct Answer: B

12 - a company wants to create a learning application for students. The learning application must give students the option to choose a button to have the text read out loud to them. Which aws machine learning service will meet this requirement?

A – amazon transcribe

B – amazon polly

C – amazon translate

D – amazon textract

Correct Answer: B

13 – a company has an on-premises linux-based server with an oracle database tah runs on it. The company wants to migrate the database server to run an amazon ec2 instance in aws. Which service should the company use to complete the migration?

A – aws database migration service (aws dms)

B – aws migration hub

C – aws application migration service (aws mgn)

D – aws application discovery service

Correct Answer: C

14 – a company is hosting a static website from a single s3 bucket. Which aws service will achieve lower latency and high transfer speeds?

A – aws elastic beanstalk

B – amazon dynamodb accelerator(dax)

C – amazon Route 53

D – amazon cloudfront

Correct Answer: D

15 – an application development team needs a solution that sends an alert to entire development team if a quality assurance test fails on a application. Which aws service should the application development team use to meet the requirement?

A – amazon connect

B – amazon eventbridge

C – amazon simple queue servisse (amazon sqs)

D – amazon simple Notification service (amazon sns)

Correct Answer: D

16 – which credential components are required to gain programmatic access to an aws account(select two)

A – an access key id

B – a primary key

C – a secret access key

D – a user id

E – a secondary key

Correct Answer: A,C

17 – which aws service identifies sercurity groups that allow unrestricted access to a user’s aws resource?

A – aws trusted advisor

B – aws identity and access management (IAM)

C – amazon cloudwatch

d- aws cloudtrail

Correct Answer: A

18 – a company requires a relational database on aws that records new customer orders from a website. Which aws service or feature will meet this requirement?

A – aws global accelerator

B – amazon dynamodb

C – amazon aurora

D – amazon elastic block store (amazon ebs)

Correct Answer: C

19 – which of the functionalities are characteristics of amazon s3 (select two)

A – a global file system

B – a object store

C – a local file store

D – a network file system

E – a durable storage system

Correct Answer: B,E

20 – what is the minimun aws support plan that provides technical support through phone calls?

A – enterprise

B – business

C – developer

D – basic

Correct Answer: B