GUILHERME TELES

E-BOOK

CERTIFICADO DE EXAME AWS

Cloud Practitioner

POR GUILHERME TELES

ÍNDICE

INTRODUÇÃO

Estamos em uma era de rápida inovação tecnológica e troca de informações. Novas tecnologias são produzidas todos os dias por diferentes indústrias, governos e pesquisadores para tornar a vida mais agradável. Portanto, as pessoas também estão começando a mudar suas infraestruturas para a nuvem, especialmente para os Amazon Web Services (AWS). A nuvem é a plataforma perfeita para inovação. Ele permite que você obtenha capacidade de computação e armazenamento simplesmente com o clique de um botão. Não há mais necessidade de alocar meticulosamente capital para infraestrutura física e configurá-la você mesmo.

Por vários anos, a AWS foi reconhecida como o provedor de nuvem líder no mercado. Eles vêm atualizando continuamente seus serviços para proporcionar a satisfação do cliente e impulsionar o sucesso do cliente. Todos os anos, você pode esperar que a AWS entregue algo novo para a mesa. E como a nuvem AWS já é tão vasta, os setores precisarão de pessoas treinadas que entendam como a nuvem AWS opera e como maximizar as soluções que produzirão os melhores resultados. A AWS formaliza este processo de treinamento e reconhecimento por meio de seus valiosos **Certificações AWS**.

O caminho para a nuvem de aprendizagem é como uma jornada longa e emocionante. Tornar-se um AWS Cloud Practitioner é uma ótima maneira de começar. Isso abre muitas oportunidades de carreira para você, e você pode escolher o caminho que deseja seguir. Você pode se tornar um arquiteto de soluções de nuvem, um desenvolvedor de nuvem, um administrador de operações de nuvem ou até mesmo algo totalmente diferente (especializações).

AWS Cloud Practitioner é a primeira etapa para ajudá-lo a entender o valor de mudar para a nuvem, bem como os serviços básicos da AWS que são fundamentais e cruciais para construir o sucesso na AWS.

Observação: Tomamos cuidado redobrado para criar esses guias de estudo e folhas de referências; no entanto, eles são apenas um recurso complementar na preparação para o exame. É altamente recomendável trabalhar em mãos em sessões e exames práticos para expandir ainda mais seus conhecimentos e melhorar suas habilidades de fazer o teste.

https://aws.amazon.com/blogs/aws/aws-named-as-a-leader-in-gartners-infrastructure-as-a-service-iaas-magic-quadrant-for-the-9th-consecutiveyear/

VISÃO GERAL DO EXAME PROFISSIONAL DE NUVEM CERTIFICADO AWS

Em 2013, a Amazon Web Services (AWS) iniciou o Programa de Certificação Global com o objetivo principal de validar as habilidades técnicas e o conhecimento para construir aplicativos baseados em nuvem seguros e confiáveis usando a plataforma AWS. Ao passar no exame da AWS, os indivíduos podem provar sua experiência para seus empregadores atuais e futuros. O exame AWS Certified Cloud Practitioner é atualmente o certificado mais básico que você pode obter e também é conhecido por ser o mais fácil entre todos os exames de certificação.

Fato engraçado: O AWS Certified Cloud Practitioner foi o primeiro exame de certificação permitido pela AWS que pode ser feito em sua casa ou escritório.

Detalhes do exame

O exame AWS Certified Cloud Practitioner (CLF-C01) é destinado a indivíduos que têm o conhecimento e as habilidades necessárias para demonstrar efetivamente um entendimento geral da AWS Cloud, independente de funções técnicas específicas abordadas por outras certificações AWS (por exemplo, Arquiteto de Soluções

- Associate, Developer - Associate ou SysOps Administrator - Associate). É composto de perguntas de identificação e enumeração formatadas como múltipla escolha ou múltipla resposta.

Para tipos de perguntas de múltipla escolha, você terá que escolher uma resposta correta entre quatro opções. Para tipos de perguntas de múltiplas respostas, você terá que escolher duas ou mais respostas corretas de cinco ou mais opções. Você pode fazer o exame por meio de supervisão online ou em um centro de testes próximo a você.

Exame Código: CLF-C01

Pré-requisitos: Nenhum

Nº de perguntas: 65

Faixa de pontuação: 100-1000

Custo: 100 USD (exame simulado: 20 USD)

Pontuação de aprovação: 700

Tempo Limite: 90 minutos

Domínios de exame

O exame AWS Certified Cloud Practitioner tem quatro domínios diferentes, cada um com um peso e cobertura de tópico correspondentes. Os domínios são: Conceitos de Nuvem (28%), Segurança (24%), Tecnologia (36%), Faturamento e Preços (12%).

Domínio 1: Conceitos de nuvem

1.1 Defina a nuvem AWS e sua proposta de valor

1.2 Identifique os aspectos da economia da nuvem AWS

1.3 Liste os diferentes princípios de design de arquitetura de nuvem Domínio 2: Segurança

2.1 Defina o modelo de responsabilidade compartilhada da AWS

2.2 Definir os conceitos de segurança e conformidade da nuvem AWS

2.3 Identifique os recursos de gerenciamento de acesso da AWS

2.4 Identificar recursos para suporte de segurança Domínio 3: Tecnologia

3.1 Definir métodos de implantação e operação na nuvem AWS

3.2 Defina a infraestrutura global da AWS

3.3 Identifique os principais serviços da AWS

3.4 Identificar recursos para suporte de tecnologia Domínio 4: Faturamento e preços

4.1 Compare e contraste os vários modelos de preços para AWS

4.2 Reconhecer as várias estruturas de conta em relação ao faturamento e preços da AWS

4.3 Identifique os recursos disponíveis para suporte de faturamento

Sistema de pontuação do exame

Você pode obter uma pontuação de 100 a 1.000 com uma pontuação mínima para aprovação de **700** quando você faz o exame AWS Certified Cloud Practitioner. A AWS usa um modelo de pontuação em escala para associar pontuações em vários tipos de exames que podem ter diferentes níveis de dificuldade. Seu relatório de pontuação completo será enviado a você por e-mail de 1 a 5 dias úteis após o exame. No entanto, assim que terminar o exame, você verá imediatamente uma notificação de aprovação ou reprovação na tela de teste.

Para indivíduos que infelizmente não foram aprovados nos exames, você deve esperar 14 dias antes de poder refazer o exame. Não há limite rígido para o número de tentativas de refazer um exame. Depois de passar, você receberá vários benefícios, como um cupom de desconto que pode ser usado em seu próximo exame da AWS.

Depois de receber seu relatório de pontuação por e-mail, o resultado também deve ser salvo em sua conta de Certificação AWS. O relatório de pontuação contém uma tabela de seu desempenho em cada domínio e indica se você atingiu o nível de competência exigido para esses domínios. Observe que você não precisa obter competência em todos os domínios para ser aprovado no exame. No final do relatório, haverá uma tabela de pontuação de desempenho que destaca seus pontos fortes e fracos, o que o ajudará a determinar as áreas que você precisa melhorar.

	Score Performance		
Section	% of Scored Items	Needs Improvement	Meets Competencies
Billing and Pricing	12%		
Cloud Concepts	28%		
Security	24%		
Technology	36%		

Benefícios do exame

- Se você for aprovado em qualquer exame da AWS, terá direito aos seguintes benefícios:

- **Desconto de exame** - Você receberá um voucher de 50% de desconto que poderá aplicar para sua recertificação ou qualquer outro exame que pretenda fazer. Para acessar o código do voucher de desconto, vá para a seção “Benefícios” da sua conta de certificação da AWS e aplique o voucher ao se registrar para o próximo exame.
- **Exame simulado grátis** - Para ajudá-lo a se preparar para seu próximo exame, a AWS fornece outro voucher que você pode usar para fazer qualquer exame prático oficial da AWS gratuitamente. Você pode acessar o código do voucher na seção “Benefícios” da sua conta de certificação da AWS.

- **Loja Certificada da AWS** - Todos os profissionais certificados pela AWS terão acesso a mercadorias certificadas pela AWS exclusivas. Você pode obter acesso à sua loja na seção “Benefícios” da sua conta de certificação da AWS.

- **Crachás Digitais de Certificação** - Você pode mostrar suas realizações para seus colegas e empregadores com emblemas digitais em suas assinaturas de e-mail, perfil do Linkedin ou em suas contas de mídia social. Você também pode mostrar seu selo digital para obter acesso exclusivo às salas de certificação na AWS re: Invent, recepções de agradecimento regionais e eventos selecionados do AWS Summit. Para visualizar seus crachás, simplesmente vá para a seção “Crachás digitais” de sua conta de certificação da AWS.

Você pode visitar a página oficial AWS Certification FAQ para ver as perguntas mais frequentes sobre como obter a AWS Certification e outras informações sobre a AWS Certification: https://aws.amazon.com/certification/faqs/**.**

GUIA DE ESTUDO DE EXAME DE EXAME DE NUVEM CERTIFICADO AWS

O exame de certificação AWS Cloud Practitioner ou AWS CCP é o mais fácil de conseguir entre todos os exames de certificação da AWS. Esta certificação cobre a maioria, senão todos, os conhecimentos fundamentais que se deve saber ao se aventurar na nuvem. Embora o curso CCP seja o básico da AWS, ainda é crucial que você aprenda e entenda adequadamente esses conceitos e a razão pela qual a AWS oferece uma certificação para ele.

O curso AWS CCP tem como objetivo fornecer aos profissionais uma compreensão fundamental da nuvem AWS sem ter que mergulhar profundamente nos aspectos técnicos. Isso inclui a infraestrutura global da AWS, práticas recomendadas no uso da nuvem da AWS, modelos de preços, opções de suporte técnico e muito mais. É por isso que a AWS recomenda fazer o exame AWS CCP primeiro, antes de tentar as outras certificações mais difíceis. Você pode ver os detalhes completos e as diretrizes para o exame de certificação aqui.

O que revisar:

Há uma série de coisas que devemos estudar principalmente para passar no exame. Listando-os, eles são:

1. Os serviços em nuvem da AWS

Atualmente, a AWS oferece mais de 160 + serviços e produtos para seus clientes. E a cada ano, a lista fica maior e mais complexa. Você não precisa memorizar cada serviço e função para passar no exame (embora isso seria incrível se você fizesse!). O que é importante é que você se familiarize com os serviços mais comumente usados, como os de computação, armazenamento, bancos de dados, segurança, rede e entrega de conteúdo, gerenciamento e governança e alguns outros. Para visualizar rapidamente as diferentes categorias.

Para ajudá-lo a familiarizar-se com esses serviços, a AWS oferece um papel branco que contém uma visão geral dos diferentes serviços da AWS, juntamente com suas definições e casos de uso. Também é importante saber o que a computação em nuvem introduz no setor e como a infraestrutura global da AWS é configurada para ajudá-lo a maximizar os recursos da computação em nuvem. Além de perguntas sobre os diferentes serviços, perguntas sobre regiões e zonas de disponibilidade geralmente aparecem no exame também.

Por último, tente se familiarizar com o AWS Management Console. Você pode facilmente criar uma conta na AWS ou usar o Qwiklabs para essa finalidade. O console de gerenciamento contém alguns serviços que não são enumerados em nenhuma categoria (como painéis de saúde, diferentes regiões da AWS, grupos de recursos) e, às vezes, também podem aparecer no exame.

1. Práticas recomendadas ao arquitetar para a nuvem

Esta seção é o que considero ser o mais importante para estudar e, na maioria dos casos, também compreende a maior parte do exame CCP. Como um profissional de nuvem, espera-se de você saber quais são as melhores práticas para usar a AWS. A nuvem é diferente de um ambiente local de várias maneiras. Alguns princípios tradicionais de sistemas de arquitetura podem ser aplicados na nuvem, enquanto alguns não são adequados. Saber quais se adaptam melhor aos seus requisitos de negócios é fundamental para criar uma infraestrutura bem arquitetada.

Nesta seção, você deve se concentrar na leitura do conteúdo deste papel branco. As práticas recomendadas são essencialmente as maneiras pelas quais você pode aproveitar as vantagens da nuvem da AWS. Pontos como desacoplar seu aplicativo para controlar pontos de falha e saber quando aplicar escalabilidade e elasticidade sobre o gerenciamento de custos e vice-versa são os cenários típicos que normalmente encontramos ao arquitetar na nuvem. Saber como construir corretamente seus sistemas na AWS também significa estar ciente dos serviços e recursos que a AWS oferece a você.

Outra boa leitura opcional é o Artigo da AWS Well-Architected Framework. Este artigo complementa bem esta seção, uma vez que discorre sobre os diferentes pilares que constituem um sistema bem arquitetado. Ler os princípios de design e os principais serviços de cada pilar o ajudará a conectar os pontos entre as práticas recomendadas e os serviços da AWS. Por fim, você pode visitar este local para reunir mais informações e visualizar conteúdo adicional para sua revisão desta seção.

2. Segurança na nuvem

A segurança na nuvem AWS é outra parte importante do seu exame CCP. Como você iniciará seus aplicativos e armazenará seus dados em um serviço externo, protegê-los deve ser sua prioridade. Felizmente, a AWS já definiu qual aspecto de segurança será de responsabilidade deles e qual será seu, por meio do Compartilhado

O principal recurso que você deve estudar para esta seção é este papel branco. O whitepaper de práticas recomendadas de segurança da AWS discute as várias maneiras de proteger seus aplicativos e serviços. Eu sugiro que você reveja cuidadosamente o seguinte:

1) Criptografia de dados em repouso e em trânsito (EBS, S3, EC2, RDS, etc)

2) Gerenciamento de identidade e acesso (IAM)

3) Segurança de rede de aplicativos e VPC (grupos de segurança, ACLs, etc)

4) Monitoramento e registro de sua infraestrutura (Cloudwatch, cloudtrail etc.)

5) Programas de conformidade da AWS

3. Modelo de preços AWS

Uma das vantagens de usar a nuvem é o provisionamento de capacidade sob demanda. Portanto, também é fundamental que você entenda o modelo de precificação do provedor. A AWS cobra de você de várias maneiras. Não existe um modelo exato que se aplique a todos, uma vez que diferentes serviços da AWS têm seus próprios planos de custo. No entanto, a AWS tem três motivadores fundamentais de custo que geralmente se aplicam a qualquer tipo de serviço. Eles são:

I- Custo de computação
II- Custo de armazenamento
III- Custo de transferência de dados de saída

Informações detalhadas sobre cada um desses custos podem ser vistas neste papel branco, que também serve como seu principal material de estudo para esta seção.

Além do provisionamento de capacidade sob demanda, a AWS também oferece a opção de reservar capacidade. Com capacidade reservada, você paga o custo total do serviço dependendo do plano que você solicitou. Se você selecionar o plano de reserva de um (1) ano, promete pagar à AWS o custo do serviço, como se estivesse em execução por um ano inteiro.

O mesmo conceito se aplica ao prazo de três (3) anos. A capacidade reservada é mais barata do que a capacidade sob demanda se você espera que seus aplicativos sejam executados continuamente por um longo período. O desconto aplicado também aumenta, dependendo do seu pagamento inicial. Dessa forma, você pode economizar até 75% sobre a capacidade equivalente adquirida em um modelo sob demanda. Você pode aprender mais sobre a capacidade reservada no papel branco.

O objetivo de estudar os modelos de custos e preços é ajudá-lo a otimizar seus custos na AWS. Eles fornecem uma ótima ferramenta que você pode usar para calcular os custos mensais esperados, conhecido como **Calculadora de preços AWS**. Outra ótima ferramenta que a AWS oferece é o Calculadora de custo total de propriedade da AWS, que ajuda a comparar o custo de seus aplicativos em um ambiente de hospedagem local com a AWS. Isso é acompanhado por um papel branco que você também deve ler. Observe que o exame CCP frequentemente pergunta cenários em que você teria que otimizar seus custos.

4. Planos de suporte da AWS

A AWS oferece quatro tipos de planos de suporte: Basic, Developer, Business e Enterprise. É importante saber como cada plano de suporte difere um do outro. Com isso dito, esta página da Internet servirá como seu principal material de estudo. Você pode perder os detalhes sutis se não ler cada plano de suporte adequadamente, portanto, certifique-se de anotar esses detalhes.

Em conjunto com o aprendizado dos planos de suporte da AWS, está estudando o AWS Trusted Advisor. AWS Trusted Advisor é uma ferramenta que oferece verificações de práticas recomendadas e recomendações em cinco categorias: otimização de custos, segurança, tolerância a falhas, desempenho e limites de serviço. Você não precisa memorizar cada verificação no AWS Trusted Advisor, embora navegar por eles seja uma vantagem.

Como revisar

Como em qualquer exame, a primeira etapa é sempre a mesma - SABER O QUE ESTUDAR. Embora já os tenhamos enumerado na seção anterior deste artigo, eu sugiro que você examine o AWS CCP Guia de exame novamente e veja o conteúdo do exame.

AWS já tem um grande número de (grátis!) recursos disponível para você se preparar para o exame. Como seu objetivo é o AWS CCP, presumo que você tenha pouco ou nenhum conhecimento sobre AWS. Portanto, eu sugiro que você primeiro:

Leia o Resumo do white paper Amazon Web Services e obter uma boa compreensão dos diferentes conceitos e serviços da AWS. Este é o mais longo dos 5 white papers, portanto, não se apresse em lê-lo. Compreender este white paper tornará mais fácil para você entender as próximas partes desta revisão. Para cada conceito que você encontrar, quase sempre haverá uma documentação correspondente da AWS disponível que vai em mais detalhes sobre esse conceito. E, como um lembrete, você não precisa memorizar todos os serviços e funções da AWS que estão por aí. Em vez disso, concentre-se nos serviços mais comumente usados pelo setor. Você pode conferir o incrível Folhas de dicas do Guilherme Teles para complementar sua revisão para esta seção.

Depois de estudar a visão geral, o white paper O custo total de (não) propriedade de aplicativos da Web em a nuvem é um bom acompanhamento. Aqui você pode ler tudo rapidamente, já que este artigo não é muito conceitual. Ele também lista muitos cenários que comparam a AWS de configurações tradicionais. Você deve ler e compreender esses cenários, pois há uma grande chance de encontrar um tipo de pergunta semelhante no exame.

Neste ponto, estamos basicamente terminando todos os resumos white papers que discutem os serviços e recursos da AWS. Portanto, eu recomendo a leitura do papel branco Como funcionam os preços em seguida, antes de prosseguir para as coisas pesadas, como as melhores práticas. O exame AWS CCP frequentemente lança questões complicadas sobre preços, TCO e otimização de custos. Saiba, em geral, como os preços dos serviços da AWS se comparam entre si, ou seja, o EFS é mais caro do que o EBS, o EBS é mais caro do que o S3. Mas seja extremamente cuidadoso ao responder às perguntas que pedem a solução mais econômica. Sempre priorize a utilidade em relação ao preço, uma vez que pode haver uma escolha na questão em que é a solução mais barata, mas não é apropriada para as necessidades do cenário. Quando não tiver certeza de qual é mais barato, use as calculadoras de custo fornecidas a você pela AWS ou pesquise os preços nas Perguntas frequentes dos serviços ou neste local na rede Internet.

AWS também oferece um curso virtual online gratuito chamado AWS Cloud Practitioner Essentials que você pode fazer para se preparar melhor para o exame AWS CCP. Este curso contém um conjunto de aulas em vídeo que cobrem todos os white papers que você leu até agora em sua revisão e é uma boa transição para o próximo white paper sobre segurança da AWS. Você não é obrigado a assistir a essas aulas em vídeo, pois elas contêm o mesmo conteúdo dos white papers. Embora isso ajude a compactar todas as informações que você estudou até agora, e ao mesmo tempo, você pode verificar se esqueceu algo importante em suas anotações.

Supondo que você tenha feito o curso de vídeo acima, agora você deve ter uma ideia da Segurança da AWS e como implementá-la. Se você não assistiu ao vídeo do curso, tudo bem também, pois o AWS Security Best Artigo de prática discute a mesma coisa. Para AWS Security, familiarize-se com o **Compartilhado Modelo de Responsabilidade**. Isso frequentemente surge no exame AWS CCP. Em seguida, é estudar como você pode proteger seus dados dentro e fora da AWS. Diferentes serviços têm diferentes métodos e protocolos de criptografia. Terceiro, familiarize-se com a segurança em nível de rede e segurança em nível de sub-rede. Há muitas maneiras de proteger seu VPC e os serviços dentro dele. Conheça as diferenças entre nACLs e grupos de segurança. Quarto, sinta-se confortável com o IAM. É um serviço muito importante na segurança da AWS e certamente aparecerá no seu exame.

Concentre-se nos conceitos de usuários, grupos, políticas e funções do IAM. Por último, esteja ciente dos recursos de monitoramento e registro da AWS, como CloudTrail e CloudWatch Logs. Entenda como os dois serviços diferem e durante quais situações em que são usados.

O último white paper que você precisa revisar é o AWS Best Practices papel branco. O material envolve muito bem todos os serviços, produtos, recursos e preços da AWS que você aprendeu. É muito importante entender quais são as melhores práticas, uma vez que as questões do cenário no exame sempre giram em torno desses tópicos. Também será muito útil se você tiver um console de gerenciamento pronto para ajudá-lo a visualizar o que está sendo discutido neste documento ao longo de sua revisão. Tente lembrar de cor todos os princípios de design e imagine situações em que você possa aplicá-los.

Depois de ler todos os white papers, a última seção de sua análise são os planos de suporte da AWS. Esta é uma navegação rápida em uma página da web e não deve demorar muito para estudar. Observe quais planos de suporte estão disponíveis e como eles diferem entre si. Pode haver perguntas no exame que indiquem qual plano de suporte oferece algum serviço específico.

Exemplos de perguntas do teste prático:

Questão 1

Qual das afirmações a seguir é verdadeira sobre como a AWS diminui o tempo para provisionar seus recursos de TI?

Ele fornece uma plataforma de tíquetes de TI com tecnologia de IA para atender às solicitações de recursos.

1. Ele fornece várias maneiras de programar provisionar recursos de TI.

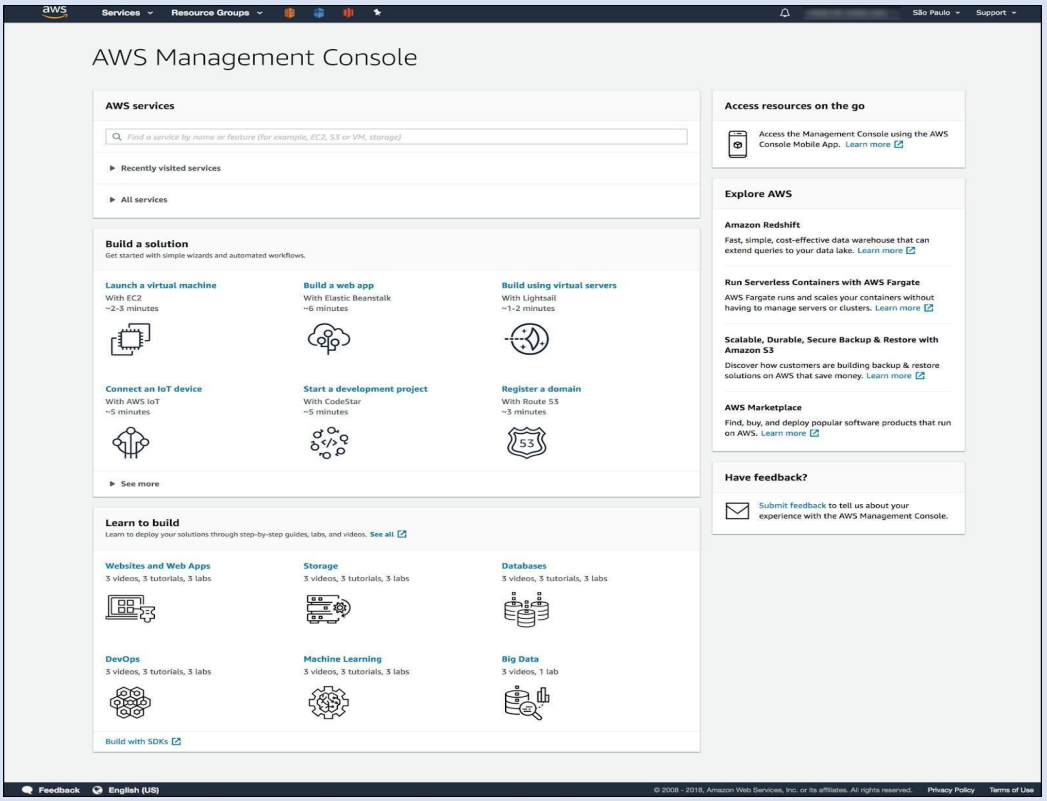
2. Ele fornece um sistema automatizado de solicitação e preenchimento de recursos de TI de fornecedores terceirizados.

3. Ele fornece serviço expresso para entregar seus servidores aos seus data centers com rapidez.

Resposta correta: 2

A computação em nuvem é a entrega sob demanda de poder de computação, banco de dados, armazenamento, aplicativos e outros recursos de TI por meio da Internet com preços pré-pagos.

Esteja você usando para executar aplicativos que compartilham fotos com milhões de usuários móveis ou para dar suporte a operações críticas de negócios, uma plataforma de serviços em nuvem fornece acesso rápido a recursos de TI flexíveis e de baixo custo. Com a computação em nuvem, você não precisa fazer grandes investimentos iniciais em hardware e gastar muito tempo no trabalho pesado de gerenciamento desse hardware. Em vez disso, você pode provisionar exatamente o tipo e o tamanho certo de recursos de computação de que precisa para impulsionar sua ideia mais recente ou operar seu departamento de TI. Você pode acessar quantos recursos precisar, quase instantaneamente, e pagar apenas pelo que usar.



Com Cloud Computing, você pode parar de gastar dinheiro executando e mantendo data centers. Você pode então se concentrar em projetos que diferenciam sua empresa, não na infraestrutura. A computação em nuvem permite que você se concentre em seus próprios clientes, em vez de no trabalho pesado de empilhar, empilhar e alimentar servidores.

Com a nuvem, as empresas não precisam mais planejar e adquirir servidores e outras infraestruturas de TI com semanas ou meses de antecedência. Em vez disso, eles podem girar instantaneamente centenas ou milhares de servidores em minutos e entregar resultados mais rapidamente. A AWS oferece várias maneiras e ferramentas para provisionar recursos de TI de maneira programática, como AWS CLI, AWS API e o AWS Management Console baseado na web.

Portanto, a resposta correta é: Ele fornece várias maneiras de provisionar recursos de TI de maneira programática.

A opção que diz: Fornece uma plataforma de tíquetes de TI com tecnologia de IA para atender às solicitações de recursos está incorreta porque a AWS não tem esse tipo de plataforma de

tíquetes. O que a AWS realmente faz é permitir que você provisione recursos de TI programaticamente usando AWS CLI, AWS API e o AWS Management Console baseado na web.

A opção que diz: Fornece um sistema automatizado de solicitação e preenchimento de recursos de TI de terceiros ***vendedores*** está incorreto porque a AWS é principalmente o fornecedor da nuvem e não depende de fornecedores terceirizados para provisionar seus recursos.

A opção que diz: Fornece serviço expresso para entregar seus servidores aos seus data centers com rapidez está incorreta porque a AWS realmente lida com os servidores subjacentes necessários para executar os recursos de nuvem solicitados.

Lembre-se de que Cloud Computing é a entrega sob demanda de poder de computação, banco de dados, armazenamento, aplicativos e outros recursos de TI por meio da Internet e não de seus data centers locais. Referências:

https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html

https://d1.awsstatic.com/whitepapers/aws-overview.pdf

Questão 2

Qual das opções abaixo você pode usar para lançar um novo cluster de banco de dados Amazon RDS para o seu VPC? (Selecione DOIS)

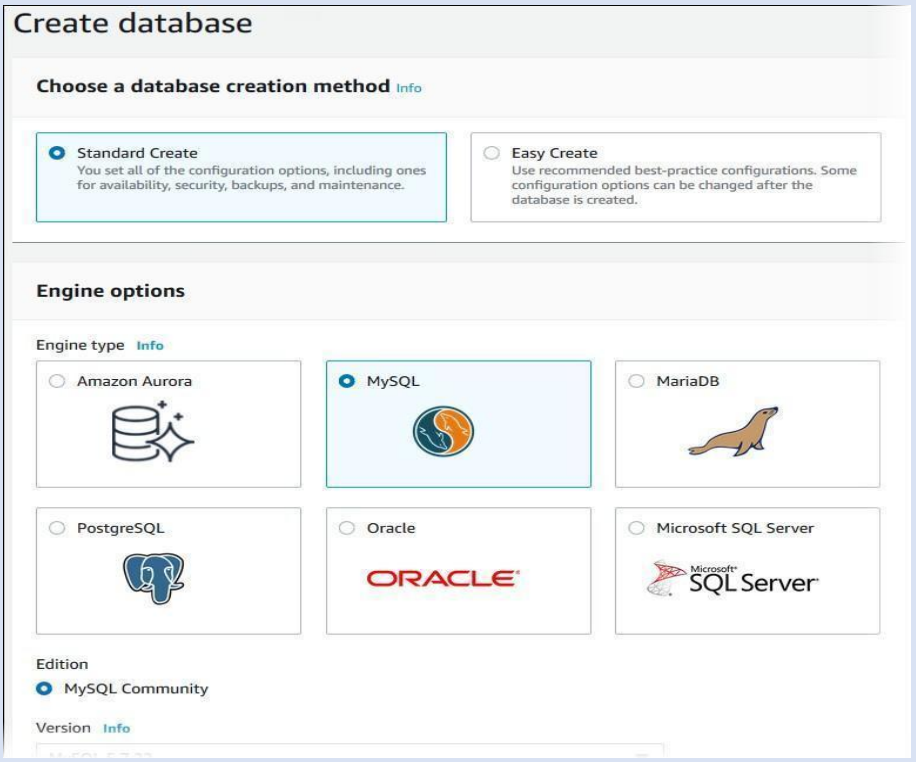
1. AWS Management Console
2. AWS Concierge
3. AWS CodePipeline
4. AWS Cloud Formation
5. Gerente de Sistemas AWS

Respostas corretas: 1,4

O Amazon Relational Database Service (Amazon RDS) facilita a configuração, operação e escalonamento de um banco de dados relacional na nuvem. Ele oferece capacidade econômica e redimensionável ao mesmo tempo em que automatiza tarefas de administração demoradas, como provisionamento de hardware, configuração de banco de dados, patching e backups. Ele libera você para se concentrar em seus aplicativos para que possa oferecer a eles o desempenho rápido, a alta disponibilidade, a segurança e a compatibilidade de que precisam.

Você pode iniciar um novo cluster de banco de dados RDS usando o AWS Management Console, AWS CLI e AWS CloudFormation. O AWS Management Console fornece uma maneira baseada na web para administrar os serviços da AWS. Você pode entrar no console e criar, listar e

executar outras tarefas com os serviços da AWS para sua conta. Essas tarefas podem incluir iniciar e interromper instâncias do Amazon EC2 e bancos de dados Amazon RDS, criando tabelas do Amazon DynamoDB, criação de usuários IAM e assim por diante. A AWS Command Line Interface (CLI), por outro lado, é uma ferramenta unificada para gerenciar seus serviços AWS.



O AWS CloudFormation fornece uma linguagem comum para você descrever e provisionar todos os recursos de infraestrutura em seu ambiente de nuvem. O CloudFormation permite que você use linguagens de programação ou um arquivo de texto simples para modelar e provisionar, de maneira automatizada e segura, todos os recursos necessários para seus aplicativos em todas as regiões e contas.

Portanto, as respostas corretas são: AWS Management Console e AWS CloudFormation.

AWS Concierge está incorreto porque este é, na verdade, um agente sênior de atendimento ao cliente atribuído à sua conta quando você se inscreve em um plano de Suporte ao Revendedor Enterprise ou qualificado. Este agente de atendimento ao cliente não está autorizado a iniciar um cluster RDS em seu nome.

AWS CodePipeline está incorreto porque este é apenas um serviço de entrega contínua totalmente gerenciado que ajuda a automatizar seus pipelines de lançamento para aplicativos rápidos e confiáveis e atualizações de infraestrutura.

Gerente de Sistemas AWS está incorreto porque esta é apenas uma interface de usuário unificada para que você possa visualizar dados operacionais de vários serviços da AWS e permite automatizar tarefas operacionais em seus recursos da AWS.

Referências: https://docs.aws.amazon.com/IAM/latest/UserGuide/console.html

https://aws.amazon.com/cli/

https://aws.amazon.com/cloudformation/

O que esperar do exame

Existem dois tipos de perguntas no exame:

- Múltipla escolha: tem uma resposta correta e três respostas incorretas (distratores).
- Resposta múltipla: tem duas ou mais respostas corretas de cinco ou mais opções.

Distratores, ou respostas incorretas, são opções de resposta que um examinando com conhecimento ou habilidade incompleta provavelmente escolheria. No entanto, geralmente são respostas plausíveis que se enquadram na área de conteúdo definida pelo objetivo do teste.

As perguntas não respondidas são pontuadas como incorretas; não há penalidade para adivinhação.

A maioria das perguntas é geralmente baseada em cenários. Alguns pedirão que você identifique um serviço ou conceito específico. Enquanto outros pedirão que você selecione várias respostas que atendam aos requisitos fornecidos. Não importa o estilo da pergunta, contanto que você entenda o que está sendo perguntado, você se sairá bem.

Seu exame pode incluir itens sem pontuação que são colocados no teste pela AWS para coletar informações estatísticas. Esses itens não são identificados no formulário e não afetam sua pontuação.

O exame AWS Certified Cloud Practitioner (CLF-C01) é um exame de aprovação ou reprovação. Seus resultados para o exame são relatados como uma pontuação em escala de 100 a 1000, com uma pontuação mínima de aprovação de 700. Logo após o exame, você saberá imediatamente se foi aprovado ou reprovado. E nos dias úteis seguintes, você deve receber seus resultados completos com a análise da pontuação (e, com sorte, o certificado também).

Mais algumas dicas:

1. Certifique-se de dormir bem na noite anterior e não seja preguiçoso ao se preparar para o exame. Se achar que não está pronto o suficiente, você pode simplesmente reagendar seu exame.

2. Chegue cedo ao local do exame para ter tempo de lidar com contratempos, se houver algum.

3. Leia as perguntas do exame corretamente, mas não gaste muito tempo com uma pergunta para a qual você não sabe a resposta. Você sempre pode voltar a ele depois de responder ao resto.

4. Mantenha seu revisor se você planeja obter outras certificações da AWS no futuro. Será útil, com certeza.

FOLHAS DE CHEAT AWS - VISÃO GERAL DA AWS

Infraestrutura global da AWS

- A infraestrutura global da AWS é construída em torno de regiões e zonas de disponibilidade (AZs).
- **Regiões** fornecem zonas de disponibilidade múltiplas, fisicamente separadas e isoladas, conectadas com baixa latência, alto rendimento e rede altamente redundante.
- **Zonas de disponibilidade** oferecem alta disponibilidade, tolerância a falhas e escalabilidade.
    - Consistem em um ou mais data centers distintos, cada um com energia, rede e conectividade redundantes, alojados em instalações separadas.
    - Uma zona de disponibilidade é representada por um código de região seguido por um identificador de letra; por exemplo, us-east-1a.
- Uma região local da AWS é um único datacenter projetado para complementar uma região da AWS existente. Uma zona local da AWS coloca computação, armazenamento, banco de dados e outros serviços selecionados da AWS mais perto de uma grande população, indústria e centros de TI onde nenhuma região da AWS existe hoje.
- Para fornecer conteúdo de baixa latência para usuários em todo o mundo, a AWS colocou pontos de presença, que são pontos de presença ou caches de presença. Esses pontos são usados pelos serviços Cloudfront e Lambda @edge.
- **Locais de ponta** são locais onde os usuários finais acessam serviços localizados na AWS. Veja

  o mapa interativo da infraestrutura global da AWS aqui.

Fontes:

https://aws.amazon.com/about-aws/global-infrastructure/

https://docs.aws.amazon.com/aws-technical-content/latest/aws-overview/global-infrastructure.html https://www.infrastructure.aws/

Precificação na AWS

- Existem três motivadores fundamentais de custo com AWS:
    - Calcular
    - Armazenar
    - Transferência de dados de saída.
- A AWS oferece preços pré-pagos.

- Para determinados serviços como Amazon EC2, Amazon EMR e Amazon RDS, você pode investir na capacidade reservada. Com as instâncias reservadas, você pode economizar até 75% sobre a capacidade sob demanda equivalente. Quando você compra instâncias reservadas, quanto maior for o pagamento inicial, maior será o desconto.
    - Com a opção All Upfront, você paga por todo o período da Instância reservada com um pagamento adiantado. Esta opção oferece o maior desconto em comparação com o preço da instância On-Demand.
    - Com a opção Partial Upfront, você faz um pagamento inicial baixo e, em seguida, é cobrado uma taxa horária com desconto para a instância durante o período da instância reservada.
    - A opção No Upfront não exige nenhum pagamento adiantado e oferece uma taxa horária com desconto durante o período.
- Também há descontos com base no volume para serviços como o Amazon S3.
    - Para novas contas, o nível gratuito da AWS está disponível.
    - O nível gratuito oferece uso limitado de produtos da AWS sem custo por 12 meses desde a criação da conta. Mais detalhes em https://aws.amazon.com/free/.
- Você pode estimar sua fatura mensal da AWS usando **AWS Pricing Calculator**.
- **O** Calculadora AWS TCO
    - dá a você a opção de avaliar a economia com o uso da AWS
    - compara custos e economias em relação aos ambientes locais e de co-localização
    - combina sua infraestrutura atual com a oferta AWS mais econômica

Fontes:

https://d1.awsstatic.com/whitepapers/aws_pricing_overview.pdf

https://aws.amazon.com/pricing/

https://aws.amazon.com/ec2/pricing/reserved-instances/pricing/

Estrutura bem arquitetada da AWS - cinco pilares

Ter sistemas bem arquitetados aumenta muito a plausibilidade do sucesso dos negócios, razão pela qual a AWS criou o AWS Well-Architected Framework para ajudar as organizações. O AWS Well-Architected Framework é composto de cinco pilares que ajudam você a entender os prós e os contras das decisões que você toma ao construir arquiteturas e sistemas em nuvem na plataforma AWS. Você aprenderá as práticas recomendadas de arquitetura para projetar e operar sistemas confiáveis, eficientes, econômicos e seguros na nuvem usando a estrutura. Ele também fornece uma

maneira de medir consistentemente suas arquiteturas em relação às melhores práticas e identificar áreas de melhoria.

1. **Excelência operacional**
   - A capacidade de executar e monitorar sistemas para agregar valor ao negócio e melhorar continuamente os processos e procedimentos de suporte.
   - Existem três áreas de práticas recomendadas e ferramentas para excelência operacional na nuvem:
     - Prepare - AWS Configuração
     - Operar - Amazon CloudWatch
     - Evolve - Amazon Elasticsearch Serviço
   - Serviço chave da AWS
     - AWS CloudFormation para a criação de modelos. (Consulte a folha de referências das ferramentas de gerenciamento da AWS)
2. **Segurança**
   - A capacidade de proteger informações, sistemas e ativos ao mesmo tempo em que agrega valor aos negócios por meio de avaliações de risco e estratégias de mitigação.
   - Existem cinco áreas de práticas recomendadas e ferramentas para segurança na nuvem:
     - Gerenciamento de identidade e acesso - IAM, autenticação multifator, organizações AWS
     - Controles de detetive - AWS CloudTrail, AWS Config, Amazon GuardDuty
     - Proteção de infraestrutura - Amazon VPC, Amazon CloudFront com AWS Shield, AWS WAF
     - Proteção de dados - criptografia ELB, Amazon Elastic Block Store (Amazon EBS), Amazon S3 e Amazon Relational Database Service (Amazon RDS), Amazon Macie, AWS Key Management Service (AWS KMS)
     - Resposta a incidentes - IAM, eventos Amazon CloudWatch
   - Serviço chave da AWS:
     - AWS Identity and Access Management (IAM)
3. **Confiabilidade**
   - A capacidade de um sistema de se recuperar de interrupções de infraestrutura ou serviço, adquirir dinamicamente recursos de computação para atender à demanda e mitigar interrupções, como erros de configuração ou problemas transitórios de rede.

- Existem três áreas de práticas recomendadas e ferramentas para confiabilidade na nuvem:
  - Fundações - IAM, Amazon VPC, AWS Trusted Advisor, AWS Shield
  - Gerenciamento de mudanças - AWS CloudTrail, AWS Con fi g, Auto Scaling, Amazon CloudWatch
  - Gerenciamento de falhas - AWS CloudFormation, Amazon S3, AWS KMS, Amazon Glacier
- Serviço chave da AWS:
  - Amazon CloudWatch

4. Eficiência de desempenho

- A capacidade de usar recursos de computação com eficiência para atender aos requisitos do sistema e manter essa eficiência conforme a demanda muda e as tecnologias evoluem.
- Existem quatro áreas de práticas recomendadas para eficiência de desempenho na nuvem:
  - Seleção - Auto Scaling for Compute, Amazon EBS e S3 for Storage, Amazon RDS e DynamoDB for Database, Route53, VPC e AWS Direct Connect for Network
  - Revisão - AWS Blog e seção Novidades do site
  - Monitoramento - Amazon CloudWatch
  - Trocas - Amazon Elasticache, Amazon CloudFront, AWS Snowball, réplicas de leitura do Amazon RDS.
- Serviço chave da AWS
  - Amazon CloudWatch

5. Otimização de custos

- A capacidade de evitar ou eliminar custos desnecessários ou recursos abaixo do ideal.
- Existem quatro áreas de melhores práticas e ferramentas para otimização de custos na nuvem:
  - Recursos de baixo custo - Explorador de custos, Amazon CloudWatch e Consultor confiável, Amazon Aurora para RDS, AWS Direct Connect com Amazon CloudFront
  - Fornecimento e demanda correspondentes - Auto Scaling
  - Conscientização de despesas - AWS Cost Explorer, AWS Budgets
  - Otimizando ao longo do tempo - AWS News Blog e a seção Novidades no

site da AWS, AWS Trusted Advisor

- Serviço chave da AWS:
  - Explorador de custos

Fonte:https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf

Estrutura bem arquitetada da AWS - Princípios de design

- **Escalabilidade**
  - **Dimensionando horizontalmente** - um aumento no número de recursos
  - **Dimensionando verticalmente** - um aumento nas especificações de um recurso individual

1. Recursos descartáveis em vez de servidores fixos

- **Instanciar recursos de computação** - automatizar a configuração de novos recursos junto com sua configuração e código
- **Infraestrutura como código** - Os ativos da AWS são programáveis. Você pode aplicar técnicas, práticas e ferramentas de desenvolvimento de software para tornar toda a sua infraestrutura reutilizável, sustentável, extensível e testável.

2. Automação

- **Gerenciamento e implantação sem servidor** - estar sem servidor muda seu foco para a automação de sua implantação de código. A AWS cuida das tarefas de gerenciamento para você.
- **Gerenciamento e implantação de infraestrutura** - A AWS lida automaticamente com detalhes, como provisionamento de recursos, balanceamento de carga, dimensionamento automático e monitoramento, para que você possa se concentrar na implantação de recursos.
- **Alarmes e Eventos** - Os serviços da AWS monitorarão continuamente seus recursos e iniciarão eventos quando determinadas métricas ou condições forem atendidas.

3. Acoplamento solto

- **Interfaces bem definidas** - reduza as interdependências em um sistema, permitindo que vários componentes interajam uns com os outros apenas por meio de interfaces específicas e agnósticas de tecnologia, como APIs RESTful.
- **Descoberta de serviço** - os aplicativos implantados como um conjunto de serviços menores devem ser consumidos sem o conhecimento prévio dos detalhes da topologia de rede. Além

de ocultar a complexidade, isso também permite que os detalhes da infraestrutura mudem a qualquer momento.

- **Integração Assíncrona** - componentes interagentes que não precisam de resposta imediata e onde bastará o reconhecimento de que uma solicitação foi registrada, devem ser integrados por meio de uma camada de armazenamento durável intermediária.
- **Melhores Práticas de Sistemas Distribuídos** - construir aplicativos que lidam com falhas de componentes de uma maneira elegante.

4. Serviços, não servidores

- **Serviços gerenciados** - fornece blocos de construção que os desenvolvedores podem consumir para potencializar seus aplicativos, como bancos de dados, aprendizado de máquina, análises, enfileiramento, pesquisa, e-mail, notificações e muito mais.
- **Arquiteturas sem servidor** - permitem que você crie serviços orientados a eventos e síncronos sem gerenciar a infraestrutura do servidor, o que pode reduzir a complexidade operacional dos aplicativos em execução.

5. Bancos de dados

- Escolha a tecnologia de banco de dados certa para cada carga de trabalho
- **Bancos de dados relacionais** fornecem uma linguagem de consulta poderosa, recursos de indexação flexíveis, controles de integridade fortes e a capacidade de combinar dados de várias tabelas de maneira rápida e eficiente.
- **Bancos de dados NoSQL** troque alguns dos recursos de consulta e transação de bancos de dados relacionais por um modelo de dados mais flexível que escala horizontalmente de maneira contínua. Ele usa uma variedade de modelos de dados, incluindo gráficos, pares de valores-chave e documentos JSON, e são amplamente reconhecidos pela facilidade de desenvolvimento, desempenho escalonável, alta disponibilidade e resiliência.
- **Armazéns de dados** são um tipo especializado de banco de dados relacional, que é otimizado para análise e relatório de grandes quantidades de dados.
- **Bancos de dados gráficos** usa estruturas de gráfico para consultas.
    - Funcionalidades de pesquisa
        - A pesquisa costuma ser confundida com consulta. Uma consulta é uma consulta formal ao banco de dados, que é endereçada em

termos formais a um conjunto de dados específico. A pesquisa permite que sejam consultados conjuntos de dados que não são estruturados com precisão.

- Um serviço de pesquisa pode ser usado para indexar e pesquisar em formato de texto estruturado e livre e pode oferecer suporte a funcionalidades que não estão disponíveis em outros bancos de dados, como classificação de resultados personalizável, facetação para filtragem, sinônimos e lematização.

6. Gerenciando volumes crescentes de dados

- **Data Lake** - uma abordagem arquitetônica que permite armazenar grandes quantidades de dados em um local central para que estejam prontamente disponíveis para serem categorizados, processados, analisados e consumidos por diversos grupos dentro de sua organização.

7. Removendo Pontos Únicos de Falha

- **Apresentando a Redundância**
  - **Redundância em espera** - quando um recurso falha, a funcionalidade é recuperada em um recurso secundário com o processo de failover. O failover normalmente requer algum tempo antes de ser concluído e, durante esse período, o recurso permanece indisponível. Isso geralmente é usado para componentes com estado, como bancos de dados relacionais.
  - Redundância ativa-as solicitações são distribuídas para vários recursos de computação redundantes. Quando um deles falha, o resto pode simplesmente absorver uma parte maior da carga de trabalho.
- **Detectar falha** - usar verificações de saúde e coletar registros
- Armazenamento de dados durável
  - **Replicação síncrona** - apenas reconhece uma transação após ela ter sido armazenada de forma durável no armazenamento primário e em suas réplicas. É ideal para proteger a integridade dos dados em caso de falha do nó primário.
  - **Replicação assíncrona** - desacopla o nó primário de suas réplicas às custas da introdução do atraso de replicação. Isso significa que as mudanças no nó primário não são refletidas imediatamente em suas réplicas.

- **Replicação baseada em quorum** - combina síncrono e replicação assíncrona, definindo um número mínimo de nós que devem participar de uma operação de gravação bem-sucedida.
    - **Multi-Dados Automatizados Resiliência Central** - utilizar regiões e zonas de disponibilidade da AWS (princípio Multi-AZ). (Consulte a seção Recuperação de desastres)
    - **Isolamento de falha e dimensionamento horizontal tradicional** - Fragmentação Shuffl

8. Otimize para o custo

- **Tamanho certo** - A AWS oferece uma ampla variedade de tipos de recursos e configurações para muitos casos de uso.
- **Elasticidade** - economize dinheiro com a AWS tomando vantagem da elasticidade da plataforma.
- **Aproveite a variedade de opções de compra** - Instâncias reservadas vs instâncias spot (consulte os preços da AWS)

9. Cache

- **Cache de dados de aplicativos** - armazene e recupere informações de caches na memória rápidos e gerenciados.
- **Edge Caching** - fornece conteúdo por uma infraestrutura mais próxima dos visualizadores, o que reduz a latência e oferece taxas de transferência de dados altas e sustentadas, necessárias para entregar grandes objetos populares aos usuários finais em escala.

10. Segurança

- **Use recursos da AWS para defesa em profundidade** - proteja vários níveis de sua infraestrutura, desde a rede até o aplicativo e o banco de dados.
- **Compartilhe a responsabilidade pela segurança com a AWS** - A AWS lida com a segurança da nuvem enquanto os clientes lidam com a segurança na nuvem.
- **Reduza o acesso privilegiado** - implementar controles do Princípio de Menor Privilégio.
- **Segurança como código** - regras de firewall, controles de acesso à rede, sub-redes internas / externas e proteção do sistema operacional podem ser capturados em um modelo que define um Golden Environment.

- **Auditoria em tempo real** - implementar monitoramento contínuo e automação de controles na AWS para minimizar a exposição aos riscos de segurança.

11. Práticas recomendadas de arquitetura em nuvem

Existem várias práticas recomendadas que você pode seguir e que podem ajudá-lo a criar um aplicativo na nuvem AWS. Os mais notáveis são:

1. **Desacople seus componentes** - o conceito principal é construir componentes que não tenham dependências rígidas entre si, de forma que, se um componente falhar por algum motivo, os outros componentes do sistema continuarão a funcionar. Isso também é conhecido como acoplamento solto. Isso reforça o princípio de design da Arquitetura Orientada a Serviços (SOA) de que quanto mais fracamente acoplados forem os componentes do sistema, melhor e mais estável ele será escalonado.

2. **Pense em paralelo** - Isso internaliza o conceito de paralelização ao projetar arquiteturas na nuvem. Ele o incentiva a implementar a paralelização sempre que possível e a automatizar os processos de sua arquitetura de nuvem.

3. **Implementar elasticidade** - Este princípio é implementado automatizando seu processo de implantação e agilizando a configuração e o processo de construção de sua arquitetura. Isso garante que o sistema possa ser ampliado e ampliado para atender à demanda sem qualquer intervenção humana.

4. **Projetar para o fracasso** - Este conceito incentiva você a ser pessimista ao projetar arquiteturas na nuvem e supor que os componentes de sua arquitetura falharão. Isso reforça você a sempre projetar sua arquitetura de nuvem para ser altamente disponível e tolerante a falhas.

Fontes: https://d0.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf

https://www.slideshare.net/AmazonWebServices/best-practices-for-architecting-in-the-cloud-jeff-barr

AWS Well-Architected Framework - Disaster Recovery

RTO é o tempo que leva após uma interrupção para restaurar um processo de negócios ao seu nível de serviço.

RPO é a quantidade aceitável de perda de dados medida em tempo antes da ocorrência do desastre.

Recuperação de desastres com AWS

Backup e restauração - armazenar dados de backup no S3 e recuperar dados de forma rápida e confiável.

Luz piloto para recuperação rápida na AWS - tempo de recuperação mais rápido

do que backup e restauração porque as partes principais do sistema já estão em execução e são continuamente atualizadas.

Espera Quente Solução - uma versão reduzida de um ambiente totalmente funcional é sempre correndo na nuvem

Multi-Site Solução - execute sua infraestrutura em outro site, em uma configuração ativo-ativo. Produção da AWS para uma solução AWS DR usando várias regiões da AWS - aproveite as vantagens das várias zonas de disponibilidade da AWS

Serviços

S3 como um destino para dados de backup que podem ser necessários rapidamente para executar uma restauração.

Importar / Exportar para transferir conjuntos de dados muito grandes, enviando dispositivos de armazenamento diretamente para a AWS.

- **Serviço de migração de servidor** para realizar migrações de servidor sem agente de local para AWS.
- **Serviço de migração de banco de dados e ferramenta de conversão de esquema** para mover bancos de dados de
    - no local para AWS e convertendo automaticamente o esquema SQL de um mecanismo para outro.
- **Geleira** para armazenamento de dados de longo prazo, onde tempos de recuperação de várias horas são adequados.
- **Gateway de armazenamento** cópia instantâneos de seus volumes de dados locais para o S3 para backup. Você pode criar volumes locais ou volumes EBS a partir desses instantâneos.
- Servidores pré-configurados agrupados como Amazon Machine Images (AMIs).
- **Elastic Load Balancing (ELB)** para distribuir o tráfego para várias instâncias.
- **Rota 53** para rotear o tráfego de produção para locais diferentes que oferecem o mesmo aplicativo ou serviço.
- **Endereço Elastic IP** para endereços IP estáticos.
- **Nuvem privada virtual (VPC)** para provisionar uma seção privada e isolada da nuvem AWS.
- **Conexão direta** para uma conexão de rede dedicada de suas instalações para a AWS.
- **Serviço de banco de dados relacional (RDS)** para escala de um banco de dados relacional na nuvem.
- **DynamoDB** para um serviço de banco de dados NoSQL totalmente gerenciado para armazenar e recuperar qualquer quantidade de dados e atender a qualquer nível de tráfego de solicitação.

- **Redshift** para um serviço de data warehouse em escala de petabyte que analisa todos os seus dados usando as ferramentas de business intelligence existentes.
- **CloudFormation** para criar uma coleção de recursos da AWS relacionados e provisioná-los de maneira ordenada e previsível.
- **Elastic Beanstalk** é um serviço de implantação e dimensionamento de aplicativos e serviços da web desenvolvidos.
- **Ops Works** é um serviço de gerenciamento de aplicativos para implantação e operação de aplicativos de todos os tipos e tamanhos.

Fonte: https://www.slideshare.net/AmazonWebServices/disaster-recovery-options-with-aws

Planos de suporte da AWS

Com centenas de serviços e recursos, a AWS oferece uma combinação de várias ferramentas, tecnologias, programas e recursos humanos para ajudar proativamente seus clientes. A AWS oferece vários planos de suporte que os clientes podem escolher com base em suas necessidades.

AWS tem 4 planos de suporte diferentes:

1. Básico
2. Desenvolvedor
3. O negócio
4. Empreendimento

O plano de suporte básico já está disponível para todos os clientes da AWS por padrão e é gratuito. Ele também oferece suporte para questões de conta e faturamento, incluindo solicitações de aumento de limite de serviço. Este tipo de suporte da AWS inclui o seguinte:

- **Atendimento ao cliente e comunidades** - Você tem acesso 24 horas por dia, 7 dias por semana ao atendimento ao cliente, documentação da AWS, white papers e fóruns de suporte.
- **Consultor confiável da AWS** - Fornece orientação sobre como provisionar adequadamente seus recursos da AWS com base nas melhores práticas para aumentar ainda mais o desempenho e melhorar a segurança geral de sua arquitetura de nuvem. Você só tem acesso às 7 verificações principais do Trusted Advisor.
- **AWS Personal Health Dashboard** - Esta é uma visão personalizada do status de saúde de cada serviço da AWS que você possui atualmente. Ele também fornece um alerta quando seus recursos são afetados por uma atividade iniciada pela AWS.

Um gerente técnico de contas (TAM) é um ponto de contato técnico que fornece defesa e orientação para ajudá-lo no planejamento e construção de soluções na AWS usando as práticas recomendadas do setor. Essa pessoa coordena e interliga de forma proativa suas preocupações com especialistas no assunto e equipes de produto para garantir que seu ambiente AWS opere de maneira ideal.

Observe que um TAM designado só estará disponível se você optar pelo plano AWS Enterprise Support.

Comparação de planos de suporte da AWS

Os clientes com um plano de suporte Enterprise são elegíveis para serviços adicionais que não estão disponíveis nos planos Developer ou Business. Além de ter um gerente técnico de conta designado, você também terá os seguintes benefícios se optar por um suporte de nível empresarial na AWS:

- Gerenciamento de eventos de infraestrutura
- Suporte de Arquitetura
- Roteamento de estojo de luvas brancas
- Avaliações de negócios de gerenciamento
- Equipe de Suporte de Concierge

Tempos de resposta do suporte técnico

Você também pode escolher um tipo de plano de suporte da AWS com base em sua carga de trabalho de produção. Se você estiver apenas experimentando, testando ou fazendo uma Prova de Conceito (POC) na AWS, é recomendável que você escolha o plano de Desenvolvedor. Se você tiver cargas de trabalho de produção em execução na AWS, é adequado optar pelo plano de negócios. Por último, se você tiver cargas de trabalho de missão crítica, é melhor ficar com um plano empresarial porque ele fornece os tempos de resposta mais eficientes para dar suporte aos seus sistemas.

Com seu suporte técnico aprimorado, o plano de suporte empresarial fornece acesso 24 horas por dia, 7 dias por semana aos engenheiros de suporte da nuvem da AWS por telefone, chat e e-mail. Você também pode ter um número ilimitado de contatos que podem abrir uma quantidade ilimitada de casos. A AWS também oferece um tempo de resposta de menos de 15 minutos no caso de seus sistemas essenciais para os negócios ficarem inativos.

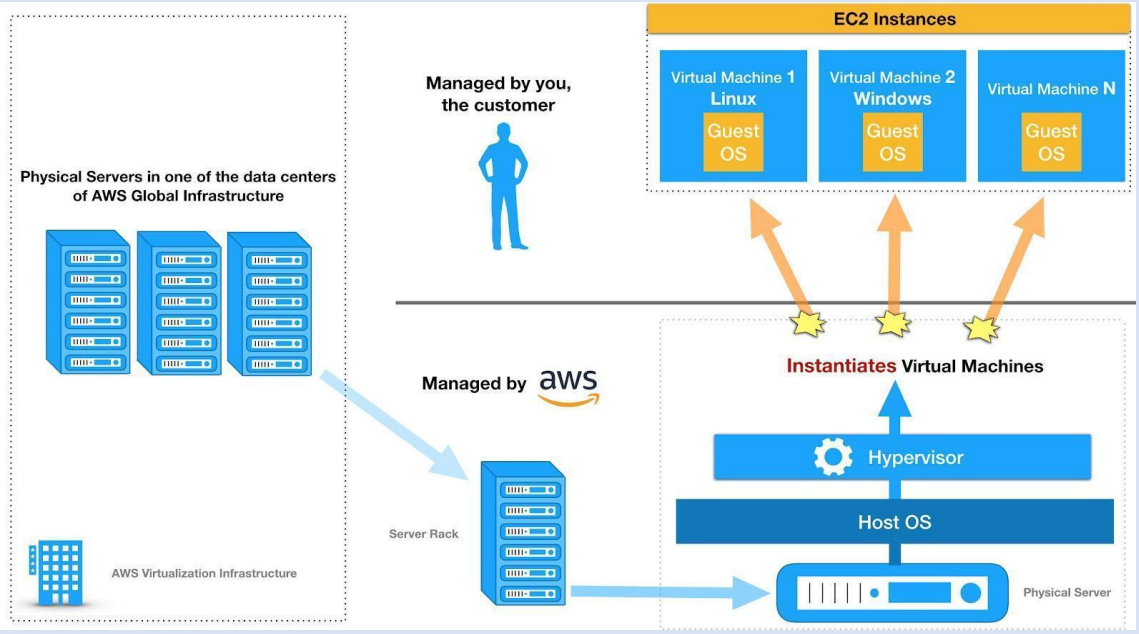
Precificação

A AWS fornece uma variedade de serviços de computação flexíveis e econômicos para atender às necessidades de sua organização, como Amazon Elastic Compute Cloud (EC2), Amazon Elastic

Container Service (ECS), Amazon Elastic Container Service para Kubernetes (EKS), Amazon Lightsail, AWS Batch e AWS Lambda, para citar alguns. Para alguns serviços como Amazon EC2, você tem amplo controle dos recursos subjacentes, enquanto para outros, a AWS tem controle total.

Com esses serviços de computação na AWS, você pode provisionar dinamicamente uma série de recursos e pagar apenas os recursos de computação que realmente consumir. Isso reduz significativamente o investimento inicial de capital necessário e o substitui por custos variáveis mais baixos. Em vez dos contratos tradicionais de longo prazo ou compromissos iniciais, você pode optar por pagar seus recursos de computação na AWS usando uma opção de preço On-Demand ou Spot para descontinuar facilmente seus recursos de nuvem se você não precisar deles, reduzindo efetivamente suas despesas operacionais. Amazon EC2 é um serviço AWS comumente usados que pode ser integrado a vários recursos e serviços, como Amazon Machine Image, Instance Store, Elastic Block Store, Elastic Network Interface, Elastic IP, Auto Scaling, Elastic Load Balancer, grupos de canais, Enhanced Networking, Segurança Grupos e muito mais.

Você já ouviu as pessoas dizerem “Instância Amazon Linux EC2” em vez de “Servidor Amazon Linux EC2” quando lançam um recurso de computação na AWS? É porque a AWS está criando programaticamente uma instância de máquina virtual (VM), em vez de fornecer a você um servidor físico real, quando você inicia uma instância EC2. A AWS tem uma infraestrutura de virtualização poderosa composta de servidores físicos gerenciados por eles. Cada servidor físico tem um sistema operacional host que executa um monitor de máquina virtual (VMM), também conhecido como hipervisor, que instancia várias “instâncias” de VM que você pode usar. Essas instâncias usam sistemas operacionais convidados que você pode gerenciar.



A AWS gerencia, opera e controla os componentes do sistema operacional host e da camada de virtualização até a segurança física das instalações nas quais o serviço opera. Por outro lado, o cliente é responsável pelo gerenciamento do sistema operacional convidado, como a instalação de patches e a configuração de segurança necessária.

Você também pode usar esses serviços de computação na AWS para executar seus aplicativos de computação de alto desempenho (HPC). Basicamente, o HPC requer uma maior E / S de armazenamento e grandes quantidades de memória para realizar uma tarefa complexa. Mover suas cargas de trabalho HPC para a AWS elimina os tempos de espera desnecessários e longas filas de trabalho que estão associadas a recursos HPC locais limitados. Como não há despesas de capital iniciais ou longos ciclos de aquisição, você pode obter economias de custo significativas sempre que processar cargas de trabalho sem estado e flexíveis.

Amazon EC2

- Um servidor virtual baseado em Linux / Windows que você pode provisionar.
- Você está limitado a executar um total de 20 instâncias On-Demand em toda a família de instâncias, adquirindo 20 instâncias reservadas e solicitando Instâncias Spot por seu limite Spot dinâmico por região.

Características

- Ambientes de servidor chamados de instâncias.
- Empacote o SO e instalações adicionais em um modelo reutilizável chamado Amazon Machine Images.
- Várias configurações de CPU, memória, armazenamento e capacidade de rede para suas instâncias, conhecidas como **tipos de instância.**
- Informações de login seguras para suas instâncias usando pares de chaves
- Volumes de armazenamento para dados temporários que são excluídos quando você PARA ou TERMINA sua instância, conhecidos como volumes de armazenamento de instância. Observe que você pode interromper uma instância apoiada por EBS, mas não uma instância apoiada por Armazenamento de Instância. Você só pode iniciar ou encerrar uma instância apoiada pelo armazenamento de instância.
    - Volumes de armazenamento persistente para seus dados usando volumes do Elastic Block Store (consulte serviços de armazenamento aws).
    - Vários locais físicos para implantar seus recursos, como instâncias e volumes EBS, conhecidos como
- **regiões** e zonas de disponibilidade (consulte a visão geral da AWS).
    - Um firewall que permite que você especifique os protocolos, portas e intervalos de IP de origem que podem alcançar suas instâncias usando grupos de segurança (consulte rede aws e entrega de conteúdo).
    - Endereços IPv4 estáticos para computação em nuvem dinâmica, conhecidos como endereços Elastic IP (consulte rede aws e entrega de conteúdo).
    - Metadados, conhecidos como tags, que você pode criar e atribuir aos seus

recursos EC2

- Você pode criar redes virtuais que são logicamente isoladas do resto da nuvem AWS e que você pode opcionalmente se conectar à sua própria rede, conhecidas como nuvens privadas virtuais ou VPCs (consulte rede aws e entrega de conteúdo).
- Adicione um script que será executado na inicialização da instância chamado dados do usuário.

Estados de instância

- **Começar** - execute sua instância normalmente. Você é cobrado continuamente enquanto sua instância está em execução.
- **Pare** - é apenas um desligamento normal da instância. Você pode reiniciá-lo a qualquer momento. Todos os volumes EBS permanecem conectados, mas os dados nos volumes de armazenamento de instância são excluídos. Você não será cobrado pelo uso enquanto a instância estiver parada. Você pode anexar ou desanexar volumes EBS. Você também pode criar um AMI a partir da instância e alterar o kernel, disco RAM e tipo de instância enquanto estiver neste estado.
- **Terminar** - a instância executa um desligamento normal e é excluída. Você não poderá reiniciar uma instância depois de encerrá-la. O volume do dispositivo raiz é excluído por padrão, mas todos os volumes EBS anexados são preservados por padrão. Os dados nos volumes de armazenamento da instância são excluídos.
- Para evitar encerramento acidental, ative a proteção contra encerramento.

Volumes do dispositivo raiz

- O volume do dispositivo raiz contém a imagem usada para inicializar a instância.
- Instâncias com suporte de armazenamento de instância
  - Todos os dados nos volumes de armazenamento da instância são excluídos quando a instância é encerrada (instâncias apoiadas pelo armazenamento da instância não suportam a ação parar) ou se falhar (como se uma unidade subjacente tiver problemas).

Instâncias apoiadas por Amazon EBS

- Uma instância apoiada pelo Amazon EBS pode ser interrompida e

reiniciada posteriormente sem afetar os dados armazenados nos volumes anexados.

- Quando em um estado interrompido, você pode modificar as propriedades da instância, alterar seu tamanho ou atualizar o kernel que está usando, ou você pode anexar seu volume raiz a uma instância diferente em execução para depuração ou qualquer outro propósito.
- Por padrão, o volume do dispositivo raiz para um AMI apoiado pelo Amazon EBS é excluído quando a instância é encerrada.

AMI

- Inclui o seguinte:
  - Um modelo para o volume raiz da instância (sistema operacional, servidor de aplicativos e aplicativos)
  - Permissões de inicialização que controlam quais contas AWS podem usar a AMI para iniciar instâncias
  - Um mapeamento de dispositivo de bloco que especifica os volumes a serem anexados à instância quando ela é iniciada
- Apoiado pelo Amazon EBS - o dispositivo raiz para uma instância iniciada a partir do AMI é um volume do Amazon EBS. AMI apoiados por instantâneos do Amazon EBS podem usar criptografia EBS.
  - Apoiado pelo armazenamento de instância. O dispositivo raiz para uma instância iniciada a partir do AMI é um volume de armazenamento de instância criado a partir de um modelo armazenado no S3.

Characteristic	Amazon EBS-Backed AMI	Amazon Instance Store-Backed AMI
Boot time for an instance	Usually less than 1 minute	Usually less than 5 minutes
Size limit for a root device	16 TiB	10 GiB
Root device volume	Amazon EBS volume	Instance store volume
Data persistence	By default, the root volume is deleted when the instance terminates.* Data on any other Amazon EBS volumes persists after instance termination by default.	Data on any instance store volumes persists only during the life of the instance.
Modifications	The instance type, kernel, RAM disk, and user data can be changed while the instance is stopped.	Instance attributes are fixed for the life of an instance.
Charges	You're charged for instance usage, Amazon EBS volume usage, and storing your AMI as an Amazon EBS snapshot.	You're charged for instance usage and storing your AMI in Amazon S3.
AMI creation/bundling	Uses a single command/call	Requires installation and use of AMI tools
Stopped state	Can be placed in stopped state where instance is not running, but the root volume is persisted in Amazon EBS	Cannot be in stopped state; instances are running or terminated

- Você pode copiar AMIs para regiões diferentes.

Preços

- On-Demand - pague pelas instâncias que você usa por segundo, sem compromissos de longo prazo ou pagamentos adiantados.
- Reservado - faça um pagamento baixo, único e adiantado para uma instância, reserve por um ou três anos prazo e pague uma taxa horária significativamente mais baixa para essas instâncias. Tem duas classes de oferta: Standard e Conversível.
  - A classe Standard oferece o desconto mais significativo, mas você só pode modificar alguns de seus atributos durante o semestre. Também pode ser vendido no mercado de instâncias reservadas.
  - A classe Conversível oferece um desconto menor do que as Instâncias Reservadas Padrão, mas pode ser trocada por outra Instância Reservada Conversível com atributos de instância diferentes. No entanto, este não pode ser vendido no mercado de instâncias reservadas.
- Spot - solicitar EC2 não utilizado instâncias, o que pode reduzir seus custos significativamente. As Instâncias Spot estão disponíveis com até 90% de desconto em comparação com os preços On-Demand.

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

- Hosts dedicados - pague por um host físico totalmente dedicado à execução de suas instâncias e traga suas licenças de software existentes por soquete, por núcleo ou por VM para reduzir custos.
- Instâncias dedicadas - pague, por hora, por instâncias executadas em hardware de locatário único.
- Há uma taxa de transferência de dados ao copiar AMI de uma região para outra

- O preço do EBS é diferente do preço da instância. (consulte os serviços de armazenamento da AWS)
- A AWS impõe uma pequena cobrança por hora se um endereço Elastic IP não estiver associado a uma instância em execução ou se estiver associado a uma instância interrompida ou a uma interface de rede não conectada.
- Você é cobrado por quaisquer endereços Elastic IP adicionais associados a uma instância.
- Se os dados são transferidos entre essas duas instâncias, eles são cobrados em "Transferência de dados de EC2 para outra região da AWS" para a primeira instância e em "Transferência de dados de outra região da AWS" para a segunda instância.

Segurança

- Use o IAM para controlar o acesso às suas instâncias (consulte AWS Security and Identity Service).
  - Políticas IAM
  - Papéis IAM
- Restrinja o acesso permitindo que apenas hosts ou redes confiáveis acessem portas em sua instância.
- Um grupo de segurança atua como um firewall virtual que controla o tráfego para uma ou mais instâncias.
  - Crie diferentes grupos de segurança para lidar com instâncias que tenham diferentes requisitos de segurança.
- Você pode adicionar regras a cada grupo de segurança que permite o tráfego de ou para suas instâncias associadas.
  - Você pode modificar as regras de um grupo de segurança a qualquer momento.
  - Novas regras são aplicadas automaticamente a todas as instâncias associadas ao grupo de segurança.
  - Avalia todas as regras de todos os grupos de segurança associados a uma instância para decidir se permite o tráfego ou não.
  - Por padrão, os grupos de segurança permitem todo o tráfego de saída.
  - As regras do grupo de segurança são sempre permissivas; você não pode criar regras que negam acesso.
  - Os grupos de segurança têm estado
- Se você não especificar um grupo de segurança ao iniciar uma instância, a instância será automaticamente associada ao grupo de segurança padrão para o VPC, que tem as seguintes regras:

- Permite todo o tráfego de entrada de outras instâncias associadas ao grupo de segurança padrão
- Permite todo o tráfego de saída da instância.

Networking

- Um endereço Elastic IP é um endereço IPv4 estático projetado para computação em nuvem dinâmica. Com ele, você pode mascarar a falha de uma instância ou software remapeando rapidamente o endereço para outra instância em sua conta.
- Você precisa associar um endereço Elastic IP à sua instância para permitir a comunicação com a Internet.
- Um endereço Elastic IP deve ser usado apenas em uma região específica.
- Por padrão, todas as contas da AWS são limitadas a cinco (5) endereços Elastic IP por região, porque os endereços de Internet públicos (IPv4) são um recurso público escasso.
- Por padrão, as instâncias EC2 vêm com um IP privado.
- Uma interface de rede elástica é um componente de rede lógico em um VPC que representa uma placa de rede virtual, que direciona o tráfego para sua instância.
- Faça escalonamento com EC2 Scaling Groups e distribua o tráfego entre as instâncias usando o Elastic Load Balancer.

Monitoramento

- Itens EC2 para monitorar
  - Utilização da CPU, utilização da rede, desempenho do disco, leituras / gravações de disco usando métricas EC2
  - Utilização de memória, utilização de swap de disco, utilização de espaço em disco, utilização de arquivo de página, coleta de log usando um agente de monitoramento / Logs CloudWatch
- As ferramentas de monitoramento automatizadas incluem:
  - Verificações de status do sistema - monitore os sistemas AWS necessários para usar sua instância para garantir que estejam funcionando corretamente. Essas verificações detectam problemas com sua instância que requerem o envolvimento da AWS para serem reparados.
  - Verificações de status da instância - monitorar o software e a configuração da rede de sua instância individual. Essas verificações detectam problemas que requerem o seu envolvimento para serem reparados.

- Alarmes do Amazon CloudWatch - observe uma única métrica em um período que você especificar e execute uma ou mais ações com base no valor da métrica em relação a um determinado limite ao longo de vários períodos.
- Amazon CloudWatch Eventos - automatize seus serviços AWS e responda automaticamente aos eventos do sistema.
- Amazon CloudWatch Logs - monitore, armazene e acesse seus arquivos de log de instâncias do Amazon EC2, AWS CloudTrail ou outras fontes.

o Monitore suas instâncias EC2 com CloudWatch. Por padrão, o EC2 envia dados de métrica para o CloudWatch em períodos de 5 minutos.

Metadados da instância e dados do usuário

o **Metadados de instância** são dados sobre sua instância que você pode usar para configurar ou gerenciar a instância em execução.

o Visualize todas as categorias de metadados de instância de dentro de uma instância em execução em

- **http://169.254.169.254/latest/meta-data/**
  - Você pode passar dois tipos de dados do usuário para EC2: scripts de shell e diretivas de inicialização em nuvem.

Armazenar

o **EBS** (consulte AWS Storage Services)

- Fornece armazenamento durável em nível de bloco volumes que você pode anexar a uma instância em execução.
- Use como um dispositivo de armazenamento primário para dados que requerem atualizações frequentes e granulares.
- Para manter uma cópia de backup de seus dados, crie um instantâneo de um volume EBS, que é armazenado no S3. Você pode criar um volume EBS a partir de um instantâneo e anexá-lo a outra instância.

o Armazenamento de instância

- Fornece armazenamento temporário em nível de bloco para instâncias.
- Os dados em um volume de armazenamento de instância persistem apenas durante a vida da instância associada; se você parar ou encerrar uma instância, todos os dados nos volumes de armazenamento da instância serão perdidos.

o **Elastic File System (EFS)** (consulte AWS Storage Services)

- Fornece armazenamento de arquivo escalonável para uso com Amazon EC2. Você pode criar um sistema de arquivo EFS e configurar suas instâncias para montar o sistema de arquivo.
- Você pode usar um sistema de arquivos EFS como uma fonte de dados comum para cargas de trabalho e aplicativos executados em várias instâncias.

o **S3** (consulte AWS Storage Services)

- Fornece acesso a uma infraestrutura de armazenamento de dados confiável e econômica.
- Armazenamento para snapshots EBS e AMIs com suporte de armazenamento de instância.

o Recursos e marcação

- Os recursos do EC2 incluem imagens, instâncias, volumes e instantâneos. Quando você cria um recurso, a AWS atribui ao recurso um ID de recurso exclusivo.
- Alguns recursos podem ser usados em todas as regiões (global) e alguns recursos são específicos para a região ou Zona de disponibilidade em que residem.

Recurso	**Modelo**	**Descrição**
Conta AWS	Global	Você pode usar a mesma conta AWS em todas as regiões.
Pares de chaves	Global ou Regional	Os pares de chaves que você cria usando EC2 estão vinculados à região onde você os criou. Você pode criar seu próprio par de chaves RSA e carregá-lo na região em que deseja usá-lo; portanto, você pode disponibilizar seu par de chaves globalmente, enviando-o para cada região.
Identificadores de recursos do Amazon EC2	Regional	Cada identificador de recurso, como um ID de AMI, ID de instância, ID de volume EBS ou ID de instantâneo EBS, está vinculado à sua região e pode ser usado apenas na região onde você criou o recurso.

Recurso fornecido pelo usuário nomes	Regional	Cada nome de recurso, como um nome de grupo de segurança ou nome de par de chaves, está vinculado à sua região e pode ser usado apenas na região onde você criou o recurso. Embora você possa criar recursos com o mesmo nome em várias regiões, eles não estão relacionados entre si.
AMIs	Regional	Um AMI está vinculado à região onde seus arquivos estão localizados no S3. Você pode copiar um AMI de uma região para outra.
Endereços Elastic IP	Regional	Um endereço Elastic IP está vinculado a uma região e pode ser associado apenas a uma instância na mesma região.
Segurança grupos	Regional	Um grupo de segurança está vinculado a uma região e pode ser atribuído apenas a instâncias na mesma região. Você não pode habilitar uma instância para se comunicar com uma instância fora de sua região usando regras de grupo de segurança.
Snapshots EBS	Regional	Um snapshot do EBS está vinculado à sua região e só pode ser usado para criar volumes na mesma região. Você pode copiar um instantâneo de uma região para outra.
Volumes EBS	Disponibilidade Zona	Um volume EBS está vinculado à sua Zona de disponibilidade e pode ser anexado apenas a instâncias na mesma Zona de disponibilidade.
Instâncias	Disponibilidade Zona	Uma instância está vinculada às Zonas de disponibilidade nas quais você a iniciou. No entanto, seu ID de instância está vinculado à região.

Você pode opcionalmente atribuir seus próprios metadados a cada recurso com tags, que consiste em

uma chave e um valor opcional que ambos definem.

Fontes: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/

https://aws.amazon.com/ec2/features/ https://aws.amazon.com/ec2/pricing/

https://aws.amazon.com/ec2/faqs/

AWS Elastic Beanstalk

- Permite que você implante e gerencie aplicativos rapidamente na nuvem AWS sem se preocupar com a infraestrutura que executa esses aplicativos.
- Elastic Beanstalk automaticamente lida com os detalhes de provisionamento de capacidade, balanceamento de carga, dimensionamento e monitoramento de integridade de aplicativos para seus aplicativos.
- É uma plataforma como serviço
- Elastic Beanstalk suporta os seguintes idiomas:
  - Go
  - Java
  - INTERNET
  - Node.js
  - PHP
  - Python
  - Rubi
- Elastic Beanstalk suporta os seguintes contêineres da web:
  - Tomcat
  - Puma
- Elástico O Beanstalk oferece suporte a contêineres Docker.
- O nome de domínio do seu aplicativo está no formato:

  subdomain.region.elasticbeanstalk.com

Monitoramento

- Console do Elastic Beanstalk Monitoring exibe o status do seu ambiente e a integridade do aplicativo em um relance.

- O Elastic Beanstalk relata a integridade de um ambiente de servidor da web dependendo de como o aplicativo em execução responde à verificação de integridade.
- Você pode criar alarmes para métricas para ajudá-lo a monitorar as alterações em seu ambiente para que possa identificar e mitigar facilmente os problemas antes que eles ocorram.
- Instâncias EC2 em seu ambiente Elastic Beanstalk geram logs que você pode visualizar para solucionar problemas com seu aplicativo ou arquivos de configuração.

Segurança

o Quando você cria um ambiente, o Elastic Beanstalk solicita que você forneça duas funções do AWS IAM: a

- **função de serviço** e um perfil de instância.

▪ Funções de serviço - assumidas pelo Elastic Beanstalk para usar outros serviços da AWS em seu nome.

▪ Perfis de instância - aplicado às instâncias em seu ambiente e permite que elas recuperem versões de aplicativos do S3, carreguem logs para S3 e executem outras tarefas que variam dependendo do tipo de ambiente e plataforma.

o Políticas do usuário - permitem que os usuários criem e gerenciem aplicativos e ambientes do Elastic Beanstalk.

Preços

- Não há custo adicional para o Elastic Beanstalk. Você paga apenas pelos recursos subjacentes da AWS que seu aplicativo consome.

Fontes: https://docs.aws.amazon.com/elasticbeanstalk/latest/dg

https://aws.amazon.com/elasticbeanstalk/details/

https://aws.amazon.com/elasticbeanstalk/pricing/

https://aws.amazon.com/elasticbeanstalk/faqs/

AWS Lambda

- o Um serviço de computação sem servidor.
- o Lambda executa seu código apenas quando necessário e dimensiona

automaticamente.

- As funções Lambda não têm estado - não há afinidade com a infraestrutura subjacente.
- Você escolhe a quantidade de memória que deseja alocar para suas funções e o AWS Lambda aloca potência de CPU proporcional, largura de banda de rede e E / S de disco.
- Suporta nativamente os seguintes idiomas:
  - Node.js
  - Java
  - C #
  - Go
  - Python
  - Rubi
- Você também pode fornecer seu próprio tempo de execução personalizado.

Componentes de um aplicativo Lambda

- **Função** - um script ou programa executado em Lambda. Lambda passa eventos de invocação para sua função. A função processa um evento e retorna uma resposta.
- **Tempos de execução** - Os tempos de execução do Lambda permitem que funções em diferentes linguagens sejam executadas no mesmo ambiente de execução básico. O tempo de execução fica entre o serviço Lambda e seu código de função, retransmitindo eventos de invocação, informações de contexto e respostas entre os dois.
- **Fonte do evento** - um serviço AWS ou um serviço personalizado que aciona sua função e executa sua lógica.
- **Fluxos de registro** - Enquanto Lambda monitora automaticamente suas invocações de função e relata métricas para CloudWatch, você pode anotar seu código de função com instruções de registro personalizadas que permitem que você analise o fluxo de execução e desempenho de sua função Lambda

Lambda @Edge

- Permite executar funções do Lambda para personalizar o conteúdo que o CloudFront oferece, executando as funções em locais da AWS mais próximos do visualizador. As funções são executadas em resposta a eventos do CloudFront, sem provisionar ou gerenciar servidores.

Preços

- Você é cobrado com base no número total de solicitações de suas funções e na duração, o tempo que leva para o código ser executado.

Fontes: https://docs.aws.amazon.com/lambda/latest/dg

https://aws.amazon.com/lambda/features/

https://aws.amazon.com/lambda/pricing/

https://aws.amazon.com/lambda/faqs/

Amazon Elastic Container Service (ECS)

- Um serviço de gerenciamento de contêiner para executar, parar e gerenciar contêineres Docker em um cluster.
- O ECS pode ser usado para criar uma implementação consistente e experiência de construção, gerenciar e dimensionar cargas de trabalho de lote e Extract-Transform-Load (ETL) e construir arquiteturas de aplicativos sofisticadas em um modelo de micros serviços.
- Amazon ECS é um serviço regional.

Características

- Você pode criar clusters ECS em um VPC novo ou existente.
- Depois que um cluster está instalado e funcionando, você pode definir definições de tarefas e serviços que especificam quais imagens de contêiner do Docker serão executadas em seus clusters.
- O AWS Compute SLA garante uma porcentagem de tempo de atividade mensal de pelo menos 99,99% para o Amazon ECS.

Componentes

- Recipientes e imagens

- Os componentes do seu aplicativo devem ser arquitetados para serem executados em contêineres contendo tudo que seu aplicativo de software precisa para ser executado: código, tempo de execução, ferramentas do sistema, bibliotecas do sistema, etc...
    - Os contêineres são criados a partir de um modelo somente leitura denominado imagem.
    - As imagens são normalmente criadas a partir de um arquivo Docker, um arquivo de texto simples que especifica todos os componentes incluídos no

contêiner. Essas imagens são então armazenadas em um registro do qual podem ser baixadas e executadas em seu cluster.

- Ao iniciar uma instância de contêiner, você tem a opção de passar os dados do usuário para a instância. Os dados podem ser usados para realizar tarefas comuns de configuração automatizada e até mesmo executar scripts quando a instância é inicializada.
- Os volumes do Docker podem ser um volume de armazenamento de instância local, volume EBS ou volume EFS. Conecte seus contêineres do Docker a esses volumes usando os drivers e plug-ins do Docker.

AWS Fargate

- Você pode usar Fargate com ECS para executar contêineres sem ter que gerenciar servidores ou clusters de instâncias EC2.
- Você não precisa mais provisionar, configurar ou dimensionar clusters de máquinas virtuais para executar contêineres.
- Fargate só oferece suporte a imagens de contêiner hospedadas no Elastic Container Registry (ECR) ou Docker Hub.

Monitoramento

- Você pode configurar suas instâncias de contêiner para enviar informações de log para CloudWatch Logs. Isso permite que você visualize diferentes registros de suas instâncias de contêiner em um local conveniente.
- Com o CloudWatch Alarms, observe uma única métrica durante um período de tempo que você especificar e execute uma ou mais ações com base no valor da métrica em relação a um determinado limite ao longo de vários períodos de tempo.
- Compartilhe arquivos de log entre contas, monitore os arquivos de log do CloudTrail em tempo real, enviando-os para CloudWatch Logs.

Etiquetagem

- Os recursos do ECS, incluindo definições de tarefas, clusters, tarefas, serviços e instâncias de contêiner, são atribuídos a um Amazon Resource Name (ARN) e um identificador de recurso exclusivo (ID). Esses recursos podem ser marcados com valores que você define, para ajudá-lo a organizá-los e identificá-los.

Preços

- Com o Fargate, você paga pela quantidade de recursos de vCPU e memória que seu aplicativo em contêiner solicita. Os recursos de vCPU e memória são calculados a partir do momento em que suas imagens de contêiner são extraídas até o encerramento da Tarefa do Amazon ECS.
- Não há cobrança adicional para o tipo de inicialização EC2. Você paga pelos recursos da AWS (por exemplo, instâncias EC2 ou volumes EBS) que cria para armazenar e executar seu aplicativo.

Fontes: https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html
https://aws.amazon.com/ecs/features/

https://aws.amazon.com/ecs/pricing/

https://aws.amazon.com/ecs/faqs/

AWS Batch

- Permite que você execute cargas de trabalho de computação em lote na nuvem AWS.
- É um serviço regional que simplifica a execução de trabalhos em lote em várias AZs dentro de uma região.

Características

  - O Batch gerencia ambientes de computação e filas de trabalho, permitindo que você execute facilmente milhares de trabalhos de qualquer escala usando EC2 e EC2 Spot.
  - O lote escolhe onde executar os trabalhos, iniciando capacidade adicional da AWS, se necessário.
  - O Lote monitora cuidadosamente o progresso de seus trabalhos. Quando a capacidade não for mais necessária, ela será removida.
  - O Lote oferece a capacidade de enviar trabalhos que fazem parte de um pipeline ou fluxo de trabalho, permitindo que você expresse quaisquer interdependências que existam entre eles ao enviar trabalhos.

Segurança

- Aproveite as vantagens das políticas, funções e permissões do IAM.

Monitoramento

- Você pode usar o fluxo de eventos do AWS Batch para eventos do CloudWatch para receber notificações quase em tempo real sobre o estado atual dos trabalhos que foram enviados às suas filas de trabalhos.
- Os eventos do fluxo de eventos do AWS Batch são garantidos para serem entregues pelo menos uma vez.
- O CloudTrail captura todas as chamadas de API para AWS Batch como eventos.

Preços

- Não há cobrança adicional para o AWS Batch. Você paga pelos recursos que cria para armazenar e executar seu aplicativo.

Fontes: https://docs.aws.amazon.com/batch/latest/userguide/

https://aws.amazon.com/batch/features/

https://aws.amazon.com/batch/pricing/

https://aws.amazon.com/batch/faqs/

Amazon Elastic Container Registry (ECR)

- Um serviço de registro AWS Docker gerenciado.
- Amazon ECR é um serviço regional.

Características

- ECR suporta Docker Registry HTTP API V2, permitindo que você use comandos Docker CLI ou suas ferramentas Docker preferidas para manter seu fluxo de trabalho de desenvolvimento existente.
- O ECR armazena os contêineres que você cria e qualquer software de contêiner que você compra por meio do AWS Marketplace.
- ECR armazena suas imagens de contêiner no Amazon S3.
- ECR suporta a capacidade de definir e organizar repositórios em seu registro usando name spaces.

- Você pode transferir suas imagens de contêiner de e para Amazon ECR via HTTPS.

Preços

- Você paga apenas pela quantidade de dados que armazena em seus repositórios e os dados transferidos para a Internet.

Fontes: https://docs.aws.amazon.com/AmazonECR/latest/userguide/

https://aws.amazon.com/ecr/features/

https://aws.amazon.com/ecr/pricing/

https://aws.amazon.com/ecr/faqs/

Plano de economia da AWS

- O Plano de Economia é um modelo de preço flexível que ajuda a economizar custos no uso do Amazon EC2, AWS Fargate e AWS Lambda.
- Você pode adquirir Planos de Poupança de qualquer conta, pagador ou vinculado.
- Por padrão, o benefício fornecido pelos Planos de Poupança é aplicável ao uso em todas as contas dentro de uma Organização AWS / família de faturamento consolidado. Você também pode optar por restringir o benefício dos Planos de Poupança apenas à conta que os comprou.
- Semelhante às instâncias reservadas, você tem todas as opções de pagamento adiantado, parcial antecipado ou sem opções de pagamento adiantado.

Tipos de planos

  - **Planos de economia de computação** - fornece a maior flexibilidade e preços que são até 66 por cento fora de
  - Taxas sob demanda. Esses planos se aplicam automaticamente ao uso da instância EC2, independentemente da família da instância (exemplo, M5, C5, etc.), tamanhos das instâncias (exemplo, c5.large, c5.xlarge, etc.), Região (por exemplo, us-east -1, us-east-2, etc.), sistema operacional (por exemplo, Windows, Linux, etc.) ou locação (dedicado, padrão, host dedicado). Eles também se aplicam ao uso de Fargate e Lambda.
    - Você pode mover uma carga de trabalho entre famílias de instâncias diferentes, mudar seu uso entre regiões diferentes ou migrar seu aplicativo do Amazon EC2 para o Amazon ECS usando Fargate a qualquer momento

e continuar a receber a taxa de desconto fornecida por seu Plano de Economia.

- **Planos de economia de instância EC2** - fornece economia de até 72 por cento sob demanda, em troca de um compromisso com uma família de instância específica em uma região AWS escolhida (por exemplo, M5 em N. Virginia US-East-1). Esses planos se aplicam automaticamente ao uso, independentemente do tamanho da instância, sistema operacional e locação dentro da família especificada em uma região.
  - Você pode alterar o tamanho da instância dentro da família da instância (por exemplo, de c5.xlarge para

- c5.2xlarge) ou o sistema operacional (por exemplo, de Windows para Linux), ou mude de Locação dedicada para Padrão e continue a receber a taxa com desconto fornecida por seu Plano de Poupança.

Plano de Poupança vs RIs

	Compute Savings Planos	Planos de economia de instância EC2	RIs conversíveis	RIs padrão
Economia sob demanda	Até 66 por cento	Até 72 por cento	Até 66 por cento	Até 72 por cento
Aplica preços automaticamente a qualquer família de instâncias	✓	-	-	-
Aplica automaticamente o preço a qualquer tamanho de instância	✓	✓	Apenas regional	Apenas regional
Aplica automaticamente o preço a qualquer locação ou sistema operacional	✓	✓	-	-
Aplica-se automaticamente a	✓	-	-	-

Amazon ECS usando Fargate e Lambda				
Aplica-se automaticamente preços nas regiões da AWS	✓	-	-	-
Opções de duração do mandato de 1 ou 3 anos	✓	✓	✓	✓

Monitoramento

- A página Inventário de Planos de Poupança mostra uma visão geral detalhada dos Planos de Poupança que você possui.
- Se você for um usuário em uma conta vinculada do AWS Organizations, poderá visualizar os Planos de Poupança pertencentes à sua conta vinculada específica.
- Se você for um usuário na conta do pagador no AWS Organizations, você pode visualizar os Planos de Poupança pertencentes apenas à conta do pagador ou pode visualizar os Planos de Poupança pertencentes a todas as contas no AWS Organizations.
- Você pode usar o AWS Budgets para definir orçamentos para a utilização, cobertura e custos do seu Plano de Economia.

Fontes: https://aws.amazon.com/savingsplans/

https://docs.aws.amazon.com/savingsplans/latest/userguide/what-is-savings-plans.htmeu

https://aws.amazon.com/savingsplans/faq/

ARMAZENAR

Amazon S3

- S3 armazena dados como objetos dentro de depósitos.
- Um objeto consiste em um arquivo e, opcionalmente, em qualquer metadado que descreva esse arquivo.
- Uma chave é o identificador exclusivo de um objeto dentro de um intervalo.
- A capacidade de armazenamento é virtualmente ilimitada.

Buckets

- Para cada intervalo, você pode:

- Controlar o acesso a ele (criar, excluir e listar objetos no intervalo)
- Ver os registros de acesso para ele e seus objetos
- Escolha a região geográfica onde armazenar o bucket e seu conteúdo.

o **Nome do intervalo** deve ser um nome compatível com DNS exclusivo.

- O nome deve ser exclusivo em todos os nomes de intervalo existentes no Amazon S3.
- Depois de criar o intervalo, você não pode alterar o nome.
- O nome do intervalo é visível na URL que aponta para os objetos que você colocará em seu intervalo.

o Por padrão, você pode criar até 100 buckets em cada uma de suas contas AWS.

o Você não pode alterar sua região após a criação.

o Você pode hospedar sites estáticos configurando seu intervalo para hospedagem de sites.

o Você não pode excluir um bucket S3 usando o console do Amazon S3 se o bucket contém 100.000 ou mais objetos. Você não pode excluir um bucket S3 usando o AWS CLI se o controle de versão estiver habilitado.

Classes de Armazenamento

o Classes de armazenamento para objetos acessados com frequência

- S3 STANDARD para armazenamento de uso geral de dados acessados com frequência.

o Classes de armazenamento para objetos acessados com pouca frequência

- S3 STANDARD_IA para dados de longa duração, mas acessados com menos frequência. Ele armazena os dados do objeto de maneira redundante em várias AZs separadas geograficamente.
- S3 ONEZONE_IA armazena os dados do objeto em apenas um AZ. Menos caro do que STANDARD_IA, mas os dados não são resilientes à perda física do AZ.
- Essas duas classes de armazenamento são adequadas para objetos com mais de 128 KB que você planeja armazenar por pelo menos 30 dias. Se um objeto tiver menos de 128 KB, o Amazon S3 cobrará 128 KB de você. Se você excluir um objeto antes do mínimo de 30 dias, será cobrado por 30 dias.

o Amazon S3 Intelligent Tiering

- S3 Intelligent-Tiering é uma classe de armazenamento projetada

para clientes que desejam otimizar os custos de armazenamento automaticamente quando os padrões de acesso aos dados mudam, sem impacto no desempenho ou sobrecarga operacional.

- S3 Intelligent-Tiering é a primeira classe de armazenamento de objeto em nuvem que oferece economia automática de custos movendo dados entre duas camadas de acesso - acesso frequente e acesso não frequente - quando os padrões de acesso mudam e é ideal para dados com padrões de acesso desconhecidos ou em mudança.
- Não há recuperação taxas no S3 Intelligent-Tiering.

o GLACIER

- Para arquivo de longo prazo
- Objetos arquivados não estão disponíveis para acesso em tempo real. Você deve primeiro restaurar os objetos antes de acessá-los.
- Os objetos glaciares são visíveis apenas através do S3.
- Opções de recuperação
  - **Expedido** - permite que você acesse rapidamente seus dados quando pedidos urgentes ocasionais para um subconjunto de arquivos são necessários. Para todos, exceto os maiores objetos arquivados, os dados acessados são normalmente disponibilizados em 1–5 minutos.
  - **Padrão** - permite que você acesse qualquer um dos seus objetos arquivados em várias horas. As recuperações padrão normalmente são concluídas em 3–5 horas. Esta é a opção padrão para pedidos de recuperação que não especificam a opção de recuperação.
  - **Volume** - A opção de recuperação de menor custo do Glacier, permitindo que você recupere grandes quantidades, mesmo petabytes, de dados de forma econômica em um dia. As recuperações em massa geralmente são concluídas em 5 a 12 horas.
- Para S3 Standard, S3 Standard-IA e Glacier classes de armazenamento, seus objetos são armazenados automaticamente em vários dispositivos abrangendo um mínimo de três zonas de disponibilidade.

Configurações de Bucket

Sub recurso	Descrição
localização	Especifique a região AWS onde deseja que S3 crie o bucket.
política e ACL (lista de controle de acesso)	Todos os seus recursos são privados por padrão. Use a política de intervalo e opções de ACL para conceder e gerenciar permissões no nível do intervalo.
local na rede Internet	Você pode configurar seu intervalo para hospedagem estática de sites.
exploração madeireira	O registro permite que você rastreie as solicitações de acesso ao seu intervalo. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso, como o solicitante, nome do intervalo, hora da solicitação, ação da solicitação, status de resposta e código de erro, se houver.
etiquetagem	O S3 fornece o sub-recurso de marcação para armazenar e gerenciar tags em um bucket. A AWS gera um relatório de alocação de custos com uso e custos agregados por suas tags.

Objetos

- Cada objeto S3 possui dados, uma chave e metadados.
- Etiquetagem
  - Você pode associar até 10 tags a um objeto. As tags associadas a um objeto devem ter chaves de tag exclusivas.

Preços

- O S3 cobra apenas pelo que você realmente usa, sem taxas ocultas e sem taxas de sub recurso
- Não há custo para criar um bucket, mas apenas para armazenar objetos no bucket e para transferir objetos para dentro e para fora do bucket.

Cobrar	Comentários
Armazenar	Você paga para armazenar objetos em seus depósitos S3. A taxa cobrada depende do tamanho dos seus objetos, por quanto tempo você os armazenou durante o mês e da classe de armazenamento.
Solicitações	Você paga por solicitações, por exemplo, solicitações GET, feitas em seus depósitos e objetos S3. Isso inclui solicitações de ciclo de vida. As taxas de solicitações dependem do tipo de solicitação que você está fazendo.
Recuperações	Você paga para recuperar objetos que estão armazenados no armazenamento STANDARD_IA, ONEZONE_IA e GLACIER.
Exclusões Antecipadas	Se você excluir um objeto armazenado no armazenamento STANDARD_IA, ONEZONE_IA ou GLACIER antes que o compromisso mínimo de armazenamento tenha passado, você paga uma taxa de exclusão antecipada para esse objeto.
Gerenciamento de armazenamento	Você paga pelos recursos de gerenciamento de armazenamento que estão ativados nos intervalos da sua conta.
Largura de banda	Você paga por toda a largura de banda de entrada e saída do S3, exceto pelo seguinte: ● Dados transferidos da Internet ● Dados transferidos para uma instância do Amazon EC2, quando a instância está na mesma região AWS que o bucket S3 ● Dados transferidos para o Amazon CloudFront Você também paga uma taxa por quaisquer dados transferidos usando o Amazon S3 Transfer Acceleration.

Segurança

- As políticas contêm o seguinte:
- **Recursos** - buckets e objetos
  - **Ações** - conjunto de operações
  - **Efeito** - pode ser permitir ou negar. Precisa conceder permissão explicitamente a um recurso.
  - **Diretor** - a conta, serviço ou usuário que tem permissão para acessar as ações e recursos do extrato.
- Políticas Baseadas em Recursos
  - Políticas de Bucket

- Fornece controle de acesso centralizado a buckets e objetos com base em uma variedade de condições, incluindo operações S3, solicitantes, recursos e aspectos da solicitação (por exemplo, endereço IP).
- Pode adicionar ou negar permissões em todos (ou um subconjunto) de objetos em um intervalo.
- Os usuários IAM precisam de permissões adicionais da conta raiz para realizar operações de intervalo.
- As políticas de intervalo são limitadas a 20 KB de tamanho.

▪ Listas de controle de acesso

- Uma lista de concessões identificando o beneficiário e a permissão concedida.
- ACLs usam um esquema XML específico do S3.
- Você pode conceder permissões apenas a outras contas da AWS, não a usuários em sua conta.
- Você não pode conceder permissões condicionais, nem negar explicitamente as permissões.
- As ACLs de objeto são limitadas a 100 permissões concedidas por ACL.
- O único caso de uso recomendado para o bucket ACL é conceder permissões de gravação para o

- Grupo de entrega de log S3.

o Políticas do usuário

▪ AWS IAM (consulte AWS Security and Identity Services)

- Chaves de acesso de usuário IAM
- Credenciais de segurança temporárias

o Controle de versão

▪ Use o controle de versão para manter várias versões de um objeto em um intervalo.

▪ O controle de versão protege você das consequências de sobregravações e exclusões não intencionais.

▪ Você também pode usar o controle de versão para arquivar objetos para ter acesso às versões anteriores.

▪ Você pode excluir permanentemente um objeto especificando a versão que deseja excluir. Apenas o proprietário de um bucket do Amazon S3 pode excluir permanentemente uma versão.

- Encriptação
  - Criptografia do lado do servidor usando
    - Chaves gerenciadas pelo Amazon S3 (SSE-S3)
    - **Chaves gerenciadas por AWS KMS (SSE-KMS)**
    - Chaves fornecidas pelo cliente (SSE-C)
  - Criptografia do lado do cliente usando
    - Chave mestra do cliente gerenciada por AWS KMS
    - chave mestra do lado do cliente
- Excluir MFA
  - A exclusão de MFA concede autenticação adicional para qualquer uma das seguintes operações:
    - Altere o estado de controle de versão do seu intervalo
    - Exclua permanentemente uma versão de objeto
  - A exclusão de MFA requer duas formas de autenticação juntas:
    - Suas credenciais de segurança
    - A concatenação de um número de série válido, um espaço e o código de seis dígitos exibido em um dispositivo de autenticação aprovado
- Acesso entre contas
  - Você pode fornecer a outra conta da AWS acesso a um objeto armazenado em um bucket do Amazon Simple Storage Service (Amazon S3). Estes são os métodos de como conceder acesso entre contas a objetos armazenados em seu próprio bucket do Amazon S3:
    - Políticas baseadas em recursos e políticas AWS Identity and Access Management (IAM) para acesso somente programático a objetos de bucket S3
    - Lista de controle de acesso baseada em recursos (ACL) e políticas de IAM para acesso somente programático a objetos de intervalo S3
    - Funções de IAM entre contas para acesso programático e de console a objetos de intervalo S3
- O solicitante paga parcelas
  - Os proprietários de intervalos pagam por todos os custos de armazenamento e transferência de dados do Amazon S3 associados a seus intervalos. Para economizar custos, você pode habilitar o recurso Requester Pays para que o

solicitante pague o custo da solicitação e o download dos dados do depósito em vez do proprietário do depósito. Observe que o proprietário do intervalo sempre paga o custo de armazenamento de dados.

- Monitoramento
  - Ferramentas de monitoramento automatizadas para assistir S3:
    - Alarmes do Amazon CloudWatch - observe uma única métrica durante um período de tempo que você especificar e execute uma ou mais ações com base no valor da métrica em relação a um determinado limite durante vários períodos de tempo.
    - AWS CloudTrail Log Monitoring - compartilhe arquivos de log entre contas, monitore arquivos de log do CloudTrail em tempo real enviando-os para CloudWatch Logs, escreva aplicativos de processamento de log em Java e valide que seus arquivos de log não mudaram após a entrega pelo CloudTrail.
  - Monitorando com CloudWatch
    - Métricas de armazenamento diário para buckets - você pode monitorar o armazenamento de buckets usando CloudWatch, que coleta e processa dados de armazenamento do S3 em métricas diárias legíveis.
    - Solicitar métricas - você pode escolher monitorar solicitações S3 para identificar e agir rapidamente questões operacionais. As métricas estão disponíveis em intervalos de 1 minuto após alguma latência para processar.

Fontes: https://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html

https://aws.amazon.com/s3/faqs/

Amazon S3 Glacier

- **Arquivo de longa duração** solução otimizada para dados usados com pouca frequência ou "dados frios".
- Você pode armazenar um número ilimitado de arquivos e uma quantidade ilimitada de dados.
- Você não pode especificar Glacier como a classe de armazenamento no momento de criar um objeto.
- Ele é projetado para fornecer uma durabilidade média anual de 99,999999999% para um

arquivo. O Glacier armazena de forma síncrona seus dados em vários AZs antes de confirmar um upload bem-sucedido.

- Para evitar a corrupção de pacotes de dados durante a transmissão, o Glacier carrega a soma de verificação dos dados durante o upload de dados. Ele compara a soma de verificação recebida com a soma de verificação dos dados recebidos e valida a autenticidade dos dados com as somas de verificação durante a recuperação de dados.
- O Glacier trabalha junto com as regras de ciclo de vida do Amazon S3 para ajudá-lo a automatizar o arquivamento de dados S3 e reduzir seus custos gerais de armazenamento. Os dados de arquivo solicitados são copiados para S3 One Zone-IA

Modelo de dados

- **Cofre**
  - Um contêiner para armazenamento de arquivos.
  - Cada recurso do cofre tem um endereço único com o formato: https: // endpoint específico da região / id da conta / vaults / nome do cofre
  - Você pode armazenar um número ilimitado de arquivos em um cofre.
  - As operações do Vault são específicas da região.
- Arquivo
  - Pode ser qualquer dado como foto, vídeo ou documento e é uma unidade básica de armazenamento no Glacier.
  - Cada arquivo possui um endereço único com o formulário:

- https: // endpoint-speci fi c-região / id-conta / vaults / nome-vault / archives / id-arquivo

Segurança

- O Glacier criptografa seus dados em repouso por padrão e oferece suporte ao trânsito de dados seguro com SSL.
- Os dados armazenados no Amazon Glacier são imutáveis, o que significa que depois que um arquivo é criado, ele não pode ser atualizado.
- O acesso ao Glacier requer credenciais que a AWS pode usar para autenticar suas solicitações. Essas credenciais devem ter permissões para acessar os cofres Glacier ou buckets S3.
- Você pode anexar políticas baseadas em identidade às identidades IAM.

- Um cofre Glacier é o principal recurso e as políticas baseadas em recursos são chamadas de políticas de cofre.
- Quando a atividade ocorre no Glacier, essa atividade é registrada em um evento CloudTrail junto com outros eventos de serviço AWS no histórico de eventos.

Preços

- Você é cobrado por GB por mês de armazenamento
- Você é cobrado por operações de recuperação, como solicitações de recuperação e quantidade de dados recuperados, dependendo do nível de acesso a dados - Acelerado, Padrão ou Em Massa
- As solicitações de upload são cobradas.
- Você é cobrado pelos dados transferidos para fora do Glacier.
- Os preços do Glacier Select são baseados na quantidade total de dados verificados, na quantidade de dados retornados e no número de solicitações iniciadas.
- Haverá uma cobrança se você excluir dados em 90 dias.

Fontes: https://docs.aws.amazon.com/amazonglacier/latest/dev/

https://aws.amazon.com/glacier/features/?nc=sn&loc=2

https://aws.amazon.com/glacier/pricing/?nc=sn&loc=3

https://aws.amazon.com/glacier/faqs/?nc=sn&loc=6

Amazon EBS

- **Armazenamento em nível de bloco** volumes para uso com instâncias EC2.
- Adequado para uso como armazenamento primário para sistemas de arquivo, bancos de dados ou qualquer aplicativo que requeira atualizações granulares finas e acesso a armazenamento bruto e não formatado em nível de bloco.
- Adequado para aplicativos de estilo de banco de dados (leituras e gravações aleatórias) e para uso intensivo de taxa de transferência aplicativos (leituras e gravações longas e contínuas).
- Novos volumes EBS recebem seu desempenho máximo no momento em que estão disponíveis e não requerem inicialização (anteriormente conhecido como pré-aquecimento). No entanto, os blocos de armazenamento em volumes que foram restaurados de snapshots devem ser inicializados (retirados do Amazon S3 e gravados no volume) antes que você possa acessar o bloco.

Características

- Diferentes tipos de opções de armazenamento: SSD de uso geral (gp2), SSD IOPS provisionado (io1), HDD otimizado de rendimento (st1) e volumes de HDD frio (sc1) de até 16 TiB de tamanho.
- Você pode montar vários volumes na mesma instância e pode montar um volume em várias instâncias ao mesmo tempo usando o Amazon EBS Multi-Attach.
- Habilite Multi-Attach em volumes IOPS io1 provisionados EBS para permitir que um único volume seja conectado simultaneamente a até dezesseis instâncias do Amazon EC2 baseadas no sistema AWS Nitro dentro do mesmo AZ.
- Você pode criar um sistema de arquivos sobre esses volumes ou usá-los de qualquer outra forma que usaria em um dispositivo de bloco (como um disco rígido).
- Você pode usar volumes EBS criptografados para atender aos requisitos de criptografia de dados em repouso para regulamentados / auditados dados e aplicativos.
- Você pode criar instantâneos point-in-time de volumes EBS, que são persistidos no Amazon S3. Igual aAMIs. Os instantâneos podem ser copiados nas regiões da AWS.
- Os volumes são criados em uma AZ específica e podem ser anexados a qualquer instância dessa mesma AZ. Para disponibilizar um volume fora do AZ, você pode criar um instantâneo e restaurá-lo em um novo volume em qualquer lugar da região.
- Você pode copiar instantâneos para outras regiões e restaurá-los em novos volumes, facilitando o aproveitamento de várias regiões da AWS para expansão geográfica, migração de data center e recuperação de desastres.
- Métricas de desempenho, como largura de banda, taxa de transferência, latência e comprimento médio da fila, fornecidas pelo Amazon CloudWatch, permitem que você monitore o desempenho de seus volumes para certificar-se de que está fornecendo desempenho suficiente para seus aplicativos sem pagar por recursos que não necessidade. Tipos de volumes EBS.

	Unidades de estado sólido (SSD)		Unidades de disco rígido (HDD)	
Tipo de Volume	Propósito geral SSD (gp2)	IOPS provisionado SSD (IO1)	Taxa de transferência otimizada HDD (st1)	Cold HDD (sc1)
Casos de Uso	-Recomendado para a maioria cargas de trabalho - Inicialização do sistema volumes - Desktops virtuais -Baixa latência interativo apps -Desenvolvimento e ambientes de teste	-Critical business aplicações que requer sustentado Desempenho de IOPS, ou mais que 16.000 IOPS ou 250 MiB / s de Taxa de transferência por volume. Quando anexado ao Nitro sistema EC2 instâncias, pico desempenho pode vá até 64.000 IOPS e 1.000 MB / s de Taxa de transferência por	-Transmissão cargas de trabalho exigindo consistente, rápido rendimento em um preço baixo -Grandes dados -Armazém de dados - Processamento de registro **-Não pode ser uma bota volume**	-Throughput-orien armazenamento ted para grandes volumes de dados que são raramente acessado - Cenários onde o menor armazenamento custo é importante **-Não pode ser uma bota volume**

		volume. -Grande banco de dados cargas de trabalho.		
Atributo de desempenho dominante	IOPS	IOPS	MiB / s	MiB / s

Encriptação

- Os dados armazenados em repouso em um volume criptografado, E / S de disco e instantâneos criados a partir dele são todos criptografados.
- Também fornece criptografia para dados em trânsito do EC2 para o EBS, pois a criptografia ocorre nos servidores que hospedam as instâncias do EC2.
- Os seguintes tipos de dados são criptografados:
  - Dados em repouso dentro do volume
  - Todos os dados se movendo entre o volume e a instância
  - Todos os instantâneos criados a partir do volume
  - Todos os volumes criados a partir desses instantâneos
- Usa chaves mestras do AWS Key Management Service (AWS KMS) ao criar volumes criptografados e qualquer instantâneo criado a partir de seus volumes criptografados.
- Os volumes restaurados de instantâneos criptografados são criptografados automaticamente.
- A criptografia EBS está disponível apenas em certos tipos de instância.
- Não há uma maneira direta de criptografar um volume não criptografado existente ou de remover a criptografia de um volume criptografado. No entanto, você pode migrar dados entre volumes criptografados e não criptografados.
- Agora você pode habilitar a criptografia do Amazon Elastic Block Store (EBS) por padrão, garantindo que todos os novos volumes EBS criados em sua conta sejam criptografados.

Monitoramento

- Monitoramento Cloudwatch de dois tipos: monitoramento básico e detalhado

- As verificações de status de volume fornecem as informações de que você precisa para determinar se seus volumes EBS estão danificados e ajudam a controlar como um volume potencialmente inconsistente é tratado. A lista de status inclui:
  - Ok - normal volume
  - Aviso - volume degradado
  - Prejudicado - volume estagnado
  - Dados insuficientes - dados insuficientes

Modificando o tamanho, IOPS ou tipo de um volume EBS no Linux

- Se o seu volume EBS da geração atual estiver conectado a um tipo de instância EC2 da geração atual, você pode aumentar seu tamanho, alterar seu tipo de volume ou (para um volume IO1) ajustar seu desempenho de IOPS, tudo sem desconectá-lo.
- O EBS atualmente oferece suporte a um tamanho de volume máximo de 16 TiB.
- A redução do tamanho de um volume EBS não é suportada.

EBS Snapshots

- Faça backup dos dados em seus volumes EBS para S3 tirando instantâneos pontuais.
- Os instantâneos são backups incrementais, o que significa que apenas os blocos no dispositivo que foram alterados após o instantâneo mais recente são salvos. Isso minimiza o tempo necessário para criar o instantâneo e economiza custos de armazenamento por não duplicar os dados.
- Quando você exclui um instantâneo, apenas os dados exclusivos desse instantâneo são removidos.
- Um instantâneo é restrito à região onde foi criado.
- Os snapshots do EBS suportam amplamente a criptografia EBS.
- Você não pode excluir um instantâneo do dispositivo raiz de um volume EBS usado por um AMI registrado. Você deve primeiro cancelar o registro da AMI antes de excluir o instantâneo.
- As tags definidas pelo usuário não são copiadas do instantâneo de origem para o novo instantâneo.
- Os instantâneos são restritos à região em que foram criados. Para compartilhar um instantâneo com outra Região, copie o instantâneo para essa região.

Amazon EBS - Instâncias otimizadas

- Oferece o melhor desempenho para seus volumes de EBS, minimizando a contenção entre E / S de EBS e outro tráfego de sua instância.
- Por exemplo, tipos que são otimizados para EBS por padrão, não há necessidade de habilitar a otimização EBS e nenhum efeito se você desabilitar a otimização EBS.

Preços

- Você é cobrado pelo valor provisionado em GB por mês até liberar o armazenamento.
- Armazenamento provisionado para volumes gp2, armazenamento provisionado e IOPS provisionado para volumes io1, armazenamento provisionado para volumes st1 e sc1 será cobrado em incrementos por segundo, com um mínimo de 60 segundos.
- Com os volumes Provisioned IOPS SSD (io1), você também é cobrado pelo valor provisionado em IOPS por mês.
- Depois de desconectar um volume, você ainda será cobrado pelo armazenamento do volume, desde que a quantidade de armazenamento exceda o limite do nível gratuito da AWS. Você deve excluir um volume para evitar incorrer em cobranças adicionais.
- O armazenamento de instantâneos é baseado na quantidade de espaço que seus dados consomem no Amazon S3.
- Copiar um instantâneo para uma nova região incorre em novos custos de armazenamento.
- Ao habilitar a otimização do EBS para uma instância que não é otimizada para EBS por padrão, você paga uma taxa adicional baixa por hora pela capacidade dedicada.

Fontes: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html

https://aws.amazon.com/ebs/faqs/

Amazon EFS

Um serviço de armazenamento de arquivos totalmente gerenciado que facilita a configuração e o dimensionamento do armazenamento de arquivos na Amazon Cloud.

Características

- O serviço gerencia toda a infraestrutura de armazenamento de arquivos para você, evitando a complexidade de implantação, aplicação de patches e manutenção de configurações complexas do sistema de arquivos.
- O EFS oferece suporte ao protocolo Network File System versão 4.
- Várias instâncias do Amazon EC2 podem acessar um sistema de arquivos EFS ao mesmo tempo, fornecendo uma fonte de dados comum para cargas de trabalho e aplicativos executados em mais de uma instância ou servidor.
- Os sistemas de arquivo EFS armazenam dados e metadados em várias zonas de disponibilidade em uma região AWS.
- Os sistemas de arquivos EFS podem crescer até atingir uma escala de petabytes, gerar altos níveis de rendimento e permitir acesso massivamente paralelo de instâncias EC2 aos seus dados.
- O EFS fornece semântica de acesso ao sistema de arquivo, como consistência forte de dados e bloqueio de arquivo.
- O EFS permite que você controle o acesso aos seus sistemas de arquivo por meio de permissões da Interface do Sistema Operacional Portátil (POSIX).
- O Amazon EFS Infrequent Access (EFS IA) é uma nova classe de armazenamento para o Amazon EFS com custo otimizado para arquivos acessados com menos frequência.

Sistemas de monitoramento de arquivos

- Alarmes Amazon CloudWatch
- Amazon CloudWatch Logs
- Eventos Amazon CloudWatch
- AWS CloudTrail Log Monitoring
- Arquivos de log em seu sistema de arquivos

Segurança

- Você deve ter credenciais válidas para fazer solicitações de API EFS, como criar um sistema

de arquivos.

- Você também deve ter permissões para criar ou acessar recursos.
- Especifique grupos de segurança EC2 para suas instâncias EC2 e grupos de segurança para os destinos de montagem EFS associados ao sistema de arquivos.

Preços

- Você paga apenas pelo armazenamento usado pelo seu sistema de arquivos.
- Os custos relacionados à taxa de transferência provisionada são determinados pelos valores de taxa de transferência que você especifica.

EFS vs EBS vs S3

Comparação de Desempenho

	Amazon EFS	**IOPS provisionado Amazon EBS**
Latência por operação	Latência baixa e consistente.	Mais baixo, consistente latência.
Escala de rendimento	Vários GBs por segundo	GB único por segundo
	Amazon EFS	**Amazon S3**
Latência por operação	Latência baixa e consistente.	Baixo, para tipos de solicitação mistos e integração com o CloudFront.
Escala de rendimento	Vários GBs por segundo	Vários GBs por segundo

- **Comparação de Armazenamento**

	Amazon EFS	**IOPS provisionado Amazon EBS**
Disponibilidade e durabilidade	Os dados são armazenados de forma redundante em vários AZs.	Os dados são armazenados redundantemente em um único AZ.
Acesso	Até milhares de instâncias EC2 de vários AZs podem se conectar simultaneamente a um sistema de arquivos.	Uma única instância EC2 em um único AZ pode se conectar a um sistema de arquivos.
Casos de uso	Big data e análises, fluxos de trabalho de processamento de mídia, gerenciamento de conteúdo, serviço da Web e diretórios pessoais.	Volumes de inicialização, transacionais e Bancos de dados NoSQL, armazenamento de dados e ETL.
	Amazon EFS	**Amazon S3**
Disponibilidade e durabilidade	Os dados são armazenados de forma redundante em vários AZs.	Armazenado de forma redundante em vários AZs.
Acesso	Até milhares de instâncias EC2 de vários AZs podem se conectar simultaneamente a um sistema de arquivos.	Um a milhões de conexões na web.
Casos de uso	Big data e análises, fluxos de trabalho de processamento de mídia, gerenciamento de conteúdo, serviço da Web e diretórios pessoais.	Serviço da Web e gerenciamento de conteúdo, mídia e entretenimento, backups, análise de big data, data lake.

Temos mais comparações para EFS, S3 e EBS em nossa seção Comparação de serviços da AWS.

Fontes: https://docs.aws.amazon.com/efs/latest/ug/

https://aws.amazon.com/efs/pricing/

https://aws.amazon.com/efs/faq/

https://aws.amazon.com/efs/features/

https://aws.amazon.com/efs/when-to-choose-efs/

AWS Storage Gateway

- O serviço permite o armazenamento híbrido entre ambientes locais e a nuvem AWS.
- Ele integra aplicativos corporativos locais e fluxos de trabalho com a nuvem de blocos e objetos da Amazon serviços de armazenamento por meio de protocolos de armazenamento padrão da indústria.
- O serviço armazena arquivos como objetos S3 nativos, arquiva fitas virtuais no Amazon Glacier e armazena EBS Snapshots gerados pelo Volume Gateway com Amazon EBS.
- Soluções de Armazenamento
    - **Gateway de arquivo** - suporta uma interface de arquivo no S3 e combina um serviço e um dispositivo de software virtual.
        - O dispositivo de software, ou gateway, é implementado em seu ambiente local como uma máquina virtual em execução no VMware ESXi ou no hypervisor Microsoft Hyper-V.
        - Suporte para gateway de arquivos
            - S3 Standard
            - Padrão S3 - Infrequente Acesso
            - S3 One Zone - IA
        - Com um gateway de arquivo, você pode fazer o seguinte:
            - Você pode armazenar e recuperar arquivos diretamente usando o protocolo NFS versão 3 ou 4.1.
            - Você pode armazenar e recuperar arquivos diretamente usando a versão do sistema de arquivos SMB, protocolo 2 e 3.
            - Você pode acessar seus dados diretamente no S3 de qualquer aplicativo ou serviço da nuvem AWS.
    - **Gateway de Volume** - fornece suporte de nuvem volumes de armazenamento que você pode montar como dispositivos iSCSI de seus servidores de aplicativos locais.
        - **Volumes em cache** - você armazena seus dados no S3 e mantém uma cópia de subconjuntos de dados acessados com frequência localmente.
        - **Volumes armazenados** - se você precisar de acesso de baixa latência

a todo o seu conjunto de dados, primeiro configure seu gateway local para armazenar todos os seus dados localmente. Em seguida, faça backup de instantâneos point-in-time desses dados de forma assíncrona para o S3.

- **Gateway de fita** - arquivar dados de backup no Amazon Glacier.
    - Possui uma interface de biblioteca de fita virtual (VTL) para armazenar dados em cartuchos de fita virtuais que você cria.
    - Implante seu gateway em uma instância EC2 para provisionar volumes de armazenamento iSCSI na AWS.
    - O serviço AWS Storage Gateway integra Tape Gateway com a classe de armazenamento Amazon S3 Glacier Deep Archive, permitindo que você armazene fitas virtuais na classe de armazenamento Amazon S3 de menor custo.
        - O Tape Gateway também tem a capacidade de mover suas fitas virtuais arquivadas no Amazon S3 Glacier para a classe de armazenamento Amazon S3 Glacier Deep Archive, permitindo que você reduza ainda mais o custo mensal para armazenar dados de longo prazo na nuvem em até 75%.

Segurança

- Depois que seu gateway de arquivo estiver ativado e em execução, você pode adicionar compartilhamentos de arquivo adicionais e conceder acesso a buckets S3.
- Você pode usar o AWS KMS para criptografar dados gravados em uma fita virtual.
- Autenticação e controle de acesso com IAM.

- **Preços**
    - Você é cobrado com base no tipo e na quantidade de armazenamento que usa, nas solicitações feitas e na quantidade de dados transferidos para fora da AWS.
    - Você é cobrado apenas pela quantidade de dados gravados na fita do Tape Gateway, não pela capacidade da fita.

Fontes: https://docs.aws.amazon.com/storagegateway/latest/userguide/

https://aws.amazon.com/storagegateway/features/

https://aws.amazon.com/storagegateway/pricing/

https://aws.amazon.com/storagegateway/faqs/

BASE DE DADOS

A AWS oferece bancos de dados desenvolvidos especificamente para todas as necessidades de seu aplicativo. Se você precisa de um Relacional, Valor-chave, na memória, ou em qualquer outro tipo de armazenamento de dados, a AWS provavelmente teria um serviço de banco de dados que você pode usar.

Os bancos de dados relacionais armazenam dados com esquemas predefinidos e "relacionamentos" entre as tabelas, daí o nome "Relacional". Ele é projetado para oferecer suporte a transações ACID (Atomicidade, Consistência, Isolamento, Durabilidade) com forte consistência de dados para manter a integridade referencial. Os bancos de dados de valor-chave são adequados para armazenar e recuperar grandes volumes de dados. Ele oferece tempos de resposta rápidos, mesmo em grandes volumes de solicitações simultâneas.

Os bancos de dados na memória são usados principalmente para aplicativos que requerem acesso em tempo real aos dados. É capaz de entregar dados a aplicativos em microssegundos e não apenas em milissegundos, uma vez que os dados são armazenados diretamente na memória e não no disco. Além disso, a AWS também oferece Documentos, Séries Temporais, Razões e muitos outros tipos de banco de dados.

Amazon Aurora

- Um mecanismo de banco de dados relacional totalmente gerenciado compatível com MySQL e PostgreSQL.
- Aurora inclui um subsistema de armazenamento de alto desempenho. O armazenamento subjacente cresce automaticamente conforme necessário, até 64 tera bytes.
- Aurora manterá seu banco de dados atualizado com os patches mais recentes.
- Aurora é tolerante a falhas e auto curativa.
- Armazenamento e Confiabilidade
    - Os dados do Aurora são armazenados no volume do cluster, que é projetado para confiabilidade. Um volume de cluster consiste em cópias dos dados em várias zonas de disponibilidade em uma única região da AWS.
    - O Aurora detecta automaticamente falhas nos volumes de disco que compõem o volume do cluster. Quando um segmento de um volume de

disco falha, o Aurora repara imediatamente o segmento. Quando o Aurora repara o segmento de disco, ele usa os dados nos outros volumes que constituem o volume do cluster para garantir que os dados no segmento reparado sejam atuais.

- O Aurora foi projetado para se recuperar de um travamento quase que instantaneamente e continuar a servir os dados do seu aplicativo sem o log binário. O Aurora executa a recuperação de falhas de maneira assíncrona em threads paralelos, para que seu banco de dados esteja aberto e disponível imediatamente após uma falha.

- Alta disponibilidade e tolerância a falhas
  - Quando você cria réplicas Aurora em Zonas de disponibilidade, RDS provisiona e mantém automaticamente de forma síncrona.
  - Um cluster Aurora DB é tolerante a falhas por design. Se a instância primária em um cluster de banco de dados falhar, o Aurora fará o failover automaticamente para uma nova instância primária de uma das duas maneiras:
    - Ao promover uma réplica Aurora existente para a nova instância primária
    - Criando uma nova instância primária
  - O armazenamento Aurora também é autocura. Blocos de dados e discos são verificados continuamente em busca de erros e reparados automaticamente.
  - O Aurora faz backup do volume do cluster automaticamente e retém os dados de restauração durante o período de retenção do backup, de 1 a 35 dias.
  - Aurora mantém automaticamente 6 cópias de seus dados em 3 zonas de disponibilidade e tentará automaticamente recuperar seu banco de dados em uma AZ saudável sem perda de dados.
  - Aurora tem um recurso Backtrack que retrocede ou restaura o cluster de banco de dados para o tempo que você especificar. No entanto, observe que o recurso Amazon Aurora Backtrack não é uma substituição total para o backup completo de seu cluster de banco de dados, uma vez que o limite para uma janela de backtrack é de apenas 72 horas.

- Tag
  - Você pode usar tags Amazon RDS para adicionar metadados aos seus recursos RDS.
  - As tags podem ser usadas com políticas IAM para gerenciar o acesso e controlar quais ações podem ser aplicadas aos recursos RDS.

- As tags podem ser usadas para rastrear custos agrupando despesas para recursos com tags semelhantes.

Monitoramento

- Inscreva-se em eventos do Amazon RDS para ser notificado quando ocorrerem alterações em uma instância de banco de dados, cluster de banco de dados, instantâneo de cluster de banco de dados, grupo de parâmetros de banco de dados ou grupo de segurança de banco de dados.
- Arquivos de log de banco de dados
- Use métricas, alarmes e registros do CloudWatch

Segurança

- Use IAM para controlar o acesso.
- Para controlar quais dispositivos e instâncias EC2 podem abrir conexões com o endpoint e a porta da instância de banco de dados para clusters de banco de dados Aurora em um VPC, você usa um grupo de segurança VPC.
- Você pode fazer conexões de ponto de extremidade e porta usando Transport Layer Security (TLS) / Secure Sockets Layer (SSL). Além disso, as regras de firewall podem controlar se os dispositivos em execução em sua empresa podem abrir conexões com uma instância de banco de dados.
- Use a criptografia RDS para proteger suas instâncias RDS e instantâneos em repouso.

Preços

- Você é cobrado por horas de instância de banco de dados, solicitações de E / S, armazenamento de backup e transferência de dados.
- Você pode comprar instâncias de banco de dados sob demanda e pagar por hora pelas horas de instância de banco de dados que você usa, ou instâncias reservadas para reservar uma instância de banco de dados por um período de um ou três anos e receber um desconto significativo em comparação com as instâncias de banco de dados sob demanda Preço da instância de banco de dados.

Fontes: https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/

https://aws.amazon.com/rds/aurora/serverless/

https://aws.amazon.com/rds/aurora/pricing/

https://aws.amazon.com/rds/aurora/faqs/

Amazon Relational Database Service (RDS)

- Banco de dados relacional padrão da indústria
- O RDS gerencia backups, patches de software, detecção automática de falhas e recuperação.
- Você pode realizar backups automatizados quando precisar deles ou criar manualmente seu próprio instantâneo de backup. Você pode usar esses backups para restaurar um banco de dados.
- **Apoia** Aurora, MySQL, MariaDB, PostgreSQL, Oracle, Microsoft SQL Server.
- O bloco de construção básico do RDS é a instância de banco de dados, que é um ambiente de banco de dados isolado na nuvem.
- Você pode ter até 40 instâncias de banco de dados Amazon RDS.
- Cada instância de banco de dados executa um mecanismo de banco de dados.
- Você pode executar sua instância de banco de dados em vários AZs, uma opção chamada implantação Multi-AZ. A Amazon provisiona e mantém automaticamente uma instância de banco de dados de reserva secundária em um AZ diferente. Sua instância de banco de dados primária é replicada de forma síncrona em AZs para a instância secundária para fornecer redundância de dados, suporte a failover, eliminar congelamentos de E / S e minimizar picos de latência durante backups do sistema.
- Instância de banco de dados:

- Ponto final: rds. <region>.amazonaws.com
- Armazenar
  - Amazon RDS para MySQL, MariaDB, PostgreSQL, Oracle e Microsoft SQL Server usam volumes Amazon EBS para armazenamento de banco de dados e log.
  - Tipos de armazenamento:
- SSD de uso geral (gp2)

- Instâncias de banco de dados MySQL, MariaDB, Oracle e PostgreSQL: tamanho de armazenamento de 20 GiB – 64 TiB
- SQL Server para edições Enterprise, Standard, Web e Express: tamanho de armazenamento de 20 GiB – 16 TiB

- SSD IOPS provisionado (IO1)

Mecanismo de Banco de Dados	Faixa de IOPS provisionadas	Faixa de Armazenamento
MariaDB	1.000-80.000	100 GiB – 64 TiB
SQL Server, Enterprise e Standard edições	1000-32.000 ou 64.000 para Tipos de instância m5 baseados em nitro	20 GiB – 16 TiB
Servidor SQL, Edições Web e Express	1000-32.000 ou 64.000 para Tipos de instância m5 baseados em nitro	100 GiB – 16 TiB
MySQL	1.000-80.000	100 GiB – 64 TiB
Oráculo	1.000-80.000	100 GiB – 64 TiB
PostgreSQL	1.000-80.000	100 GiB – 64 TiB

- Para casos de uso de OLTP de produção, use implantações Multi-AZ para maior tolerância a falhas com armazenamento IOPS provisionado para desempenho rápido e previsível.
- Magnético
  - Não permite que você dimensione o armazenamento ao usar o mecanismo de banco de dados do SQL Server.
  - Não suporta volumes elásticos.
  - Limitado a um tamanho máximo de 3 TiB.
  - Limitado a um máximo de 1.000 IOPS.

- Segurança

  - Segurança Grupos

- **Grupos de segurança de banco de dados** - controla o acesso a uma instância de banco de dados que não está em um VPC. Por padrão, o acesso à rede é desativado para uma instância de banco de dados. Este SG é para a plataforma EC2-Classic.
- **Grupos de segurança VPC** - controla o acesso a uma instância de banco de dados dentro de um VPC. Este SG é para a plataforma EC2-VPC.
- **Grupos de Segurança EC2** - controla o acesso a uma instância EC2 e pode ser usado com uma instância de banco de dados.

o Práticas

- Atribua uma conta IAM individual a cada pessoa que gerencia os recursos RDS. Não use credenciais de raiz da AWS para gerenciar recursos RDS.
- Conceda a cada usuário o conjunto mínimo de permissões necessárias para executar suas funções.
- Use grupos IAM para gerenciar com eficácia as permissões para vários usuários.
- Gire seu Credenciais IAM regularmente.
- Use grupos de segurança para controlar quais endereços IP ou instâncias do Amazon EC2 podem se conectar aos seus bancos de dados em uma instância de banco de dados.
- Execute sua instância de banco de dados em uma Amazon Virtual Private Cloud (VPC) para obter o maior controle de acesso à rede possível.
- Use conexões Secure Socket Layer (SSL) com instâncias de banco de dados executando os mecanismos de banco de dados MySQL, MariaDB, PostgreSQL, Oracle ou Microsoft SQL Server.
- Use a criptografia RDS para proteger suas instâncias RDS e instantâneos em repouso.
- Use os recursos de segurança de seu mecanismo de banco de dados para controlar quem pode efetuar login nos bancos de dados em uma instância de banco de dados.

o Encriptação

- Em repouso e em trânsito.
- Gerencie as chaves usadas para instâncias de banco de dados criptografadas usando o AWS KMS. As chaves de criptografia KMS são específicas da região em que foram criadas.
- A criptografia RDS está disponível atualmente para todos os mecanismos de banco de dados e tipos de armazenamento. A criptografia RDS está

disponível para a maioria das classes de instância de banco de dados.

- Você não pode restaurar um backup não criptografado ou instantâneo para uma instância de banco de dados criptografada.
- Você pode usar SSL de seu aplicativo para criptografar uma conexão com uma instância de banco de dados executando MySQL, MariaDB, SQL Server, Oracle ou PostgreSQL.

o O Amazon RDS oferece suporte aos seguintes cenários para acessar uma instância de banco de dados em um VPC:

Instância de banco de dados	**Acessado por**
Em um VPC	Uma instância EC2 no mesmo VPC
	Uma instância EC2 em um VPC diferente
	Uma instância EC2 não está em um VPC
	Um aplicativo de cliente pela Internet
Não está em um VPC	Uma instância EC2 em um VPC
	Uma instância EC2 não está em um VPC
	Um aplicativo de cliente pela Internet

Etiquetagem - TAG

o Uma etiqueta RDS é um par nome-valor que você define e associa a um recurso RDS. O nome é conhecido como chave. Fornecer um valor para a chave é opcional.

o Todos os recursos do Amazon RDS podem ser marcados.

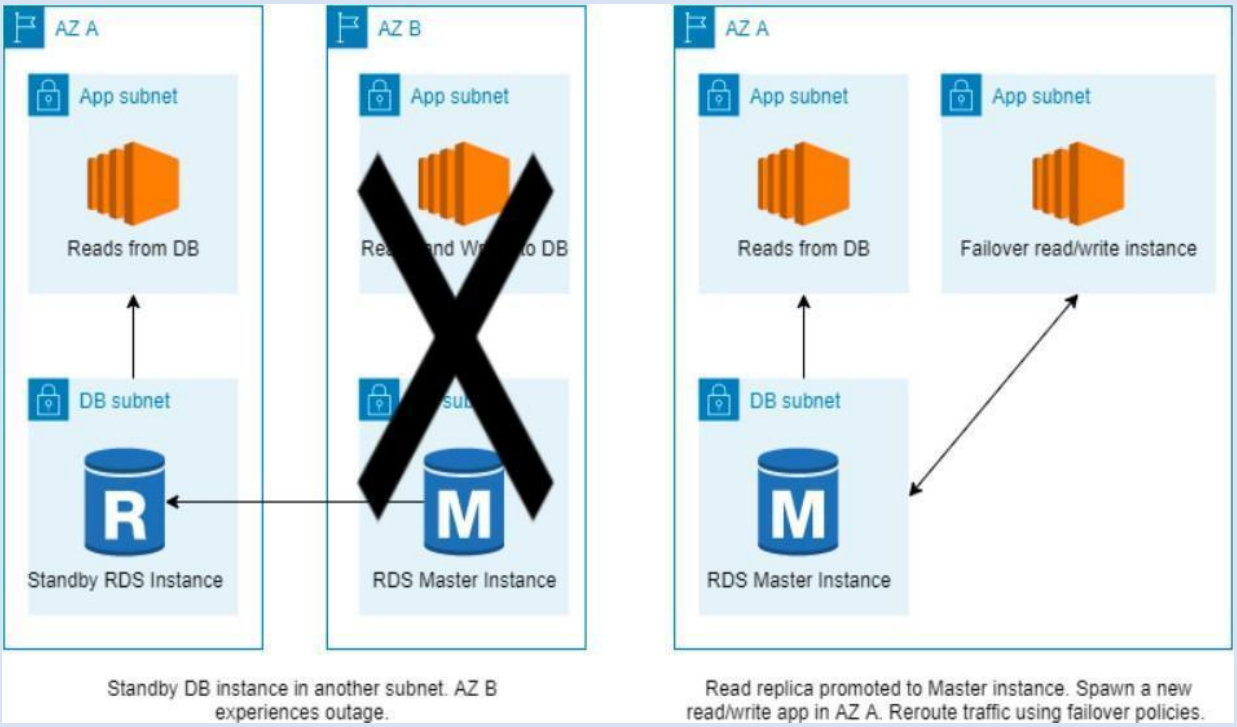
o Use tags para organizar sua fatura da AWS para refletir sua própria estrutura de custos.

o Um conjunto de tags pode conter até 10 tags ou pode estar vazio.

o Alta disponibilidade usando Multi-AZ

o As implantações Multi-AZ para instâncias Oracle, PostgreSQL, MySQL e MariaDB DB usam a tecnologia de failover da Amazon. As instâncias de banco de dados do SQL Server usam o espelhamento do SQL Server.

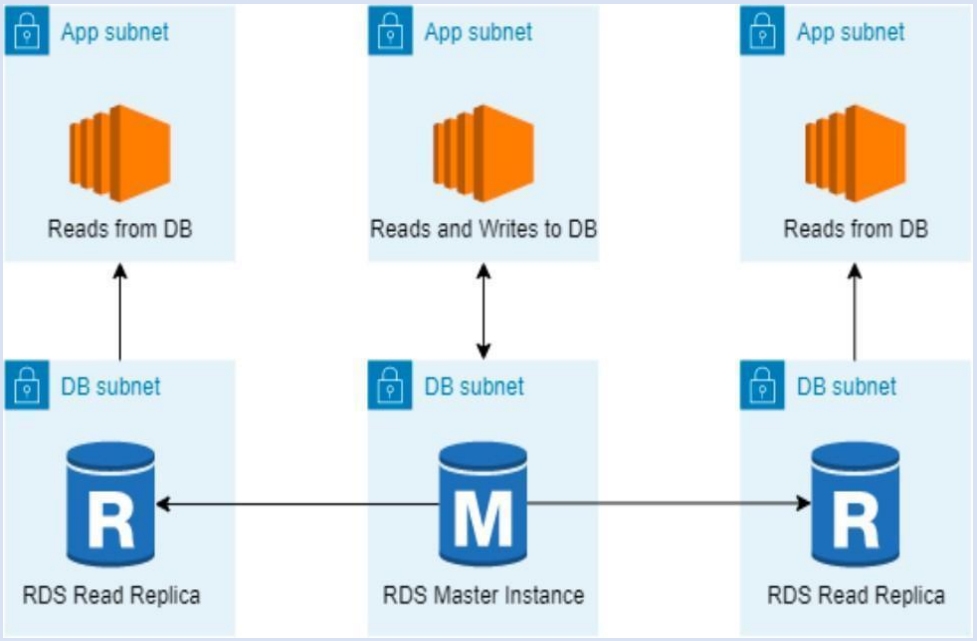
- **Amazon RDS para SQL Server** oferece grupos de disponibilidade Always On para a configuração Multi-AZ em todas as regiões da AWS
- Você pode modificar uma instância de banco de dados em uma implantação Single-AZ para uma implantação Multi-AZ.
- A instância de banco de dados primária muda automaticamente para a réplica em espera se ocorrer alguma das seguintes condições:
  - Uma interrupção da zona de disponibilidade
  - A instância de banco de dados primária falha
  - O tipo de servidor da instância de banco de dados foi alterado
  - O sistema operacional da instância de banco de dados está passando por patch de software
  - Um failover manual da instância de banco de dados foi iniciado usando reinicializar com failover



Réplicas de leitura

- As atualizações feitas na instância do banco de dados de origem são copiadas de forma assíncrona para a réplica de leitura.

- Você pode reduzir a carga em sua instância de banco de dados de origem roteando consultas de leitura de seus aplicativos para a réplica de leitura.



Implantações Multi-AZ versus réplicas de leitura

Backups e restaurações

- Sua instância de banco de dados deve estar no estado ATIVO para que os backups automatizados ocorram.
- O primeiro instantâneo de uma instância de banco de dados contém os dados de toda a instância de banco de dados. Os instantâneos subsequentes da mesma instância de banco de dados são incrementais.

Monitoramento

- Amazon CloudWatch
- Eventos RDS
  - Um evento Amazon RDS é criado quando a reinicialização é concluída.
  - Seja notificado quando ocorrerem alterações em uma instância de banco de dados, instantâneo de banco de dados, grupo de parâmetros de banco de dados ou grupo de segurança de banco de dados.
  - Usa o Amazon Simple Noti fi cation Service (SNS) para fornecer notificação quando ocorre um evento Amazon RDS.
- Arquivos de log de banco de dados
- O CloudWatch reúne métricas sobre a utilização da CPU do hipervisor para uma instância de banco de dados e o Enhanced Monitoring reúne suas métricas de um agente na instância.
- Status da instância - indica a integridade da instância.
- O CloudTrail captura todas as chamadas de API para RDS como eventos.

Preços

- Com o Amazon RDS, você paga apenas pelas instâncias RDS que estão ativas.
- Os dados transferidos para replicação entre regiões incorrem em taxas de transferência de dados RDS.
- As instâncias são cobradas por horas de instância de banco de dados (por segundo), armazenamento (por GiB por mês), solicitações de I / O (por 1 milhão de solicitações por mês), IOPS provisionado (por IOPS por mês), armazenamento de backup (por GiB por mês) e Transferência de dados (por GB).
    - O Amazon RDS é cobrado em incrementos de um segundo para instâncias de banco de dados e armazenamento anexado. O preço ainda é listado por hora, mas as contas agora são calculadas em segundos e mostram o uso na forma decimal. Há uma cobrança mínima de 10 minutos quando uma instância é criada, restaurada ou iniciada.
- Opções de compra RDS:
    - **Instâncias sob demanda** - Pague por hora pelas horas de instância de banco de dados que você usa.
    - **Instâncias reservadas** - Reserve uma instância de banco de dados por um período de um ou três anos e receba um desconto significativo em comparação com o preço da instância de banco de dados sob demanda.
- O Amazon RDS agora é cobrado em incrementos de um segundo para instâncias de banco de dados e armazenamento anexado. O preço ainda é listado por hora, mas as contas agora são calculadas em segundos e mostram o uso na forma decimal. Há uma cobrança mínima de 10 minutos quando uma instância é criada, restaurada ou iniciada.

Fontes: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/

https://aws.amazon.com/rds/features/

https://aws.amazon.com/rds/pricing/

https://aws.amazon.com/rds/faqs/

Amazon DynamoDB

- Serviço de banco de dados NoSQL que fornece desempenho rápido e previsível com escalabilidade contínua.
- Oferece criptografia em repouso.
- Você pode criar tabelas de banco de dados que podem armazenar e recuperar qualquer quantidade de dados e atender a qualquer nível de tráfego de solicitação.
- Você pode aumentar ou diminuir a capacidade de rendimento de suas tabelas sem tempo de inatividade ou degradação do desempenho e usar o AWS Management Console para monitorar a utilização de recursos e as métricas de desempenho.
- Fornece capacidade de backup sob demanda, bem como permite recuperação pontual para seu DynamoDB tabelas.
- Todos os seus dados são armazenados em partições, apoiados por discos de estado sólido (SSDs) e replicados automaticamente em vários AZs em uma região AWS, fornecendo alta disponibilidade integrada e durabilidade de dados.
- As transações fornecem atomicidade, consistência, isolamento e durabilidade (ACID) no DynamoDB, ajudando você para manter a correção dos dados em seus aplicativos.

Etiquetagem - TAG

- As tags podem ajudá-lo a:
  - Identifique rapidamente um recurso com base nas tags que você atribuiu a ele.
  - Veja as contas da AWS divididas por tags.
- Número máximo de tags por recurso: 50

Backup e restauração sob demanda

- Você pode usar o IAM para restringir as ações de backup e restauração do DynamoDB para alguns recursos.
- Todas as ações de backup e restauração são capturadas e registradas no AWS CloudTrail.
- Backups
  - Cada vez que você cria um backup sob demanda, é feito o backup de todos os dados da tabela.
  - Todos os backups e restaurações no DynamoDB trabalhe sem consumir nenhuma taxa de transferência provisionada na mesa.

- Os backups do DynamoDB não garantir consistência causal entre os itens; no entanto, a diferença entre as atualizações em um backup é geralmente muito menor do que um segundo.
- Você pode restaurar backups como novas tabelas do DynamoDB em outras regiões.

o Restaurar

- Você não pode substituir uma tabela existente durante uma operação de restauração.
- Você restaura os backups para uma nova tabela.
- Para tabelas com distribuição uniforme de dados em suas chaves primárias, o tempo de restauração é proporcional à maior partição única por contagem de itens e não ao tamanho geral da tabela.
- Se sua tabela de origem contém dados com inclinação significativa, o tempo para restaurar pode aumentar.

Segurança

o Encriptação

- Criptografa seus dados em repouso usando uma chave de criptografia gerenciada AWS Key Management Service (AWS KMS) para DynamoDB.
- A criptografia em repouso pode ser ativada apenas quando você está criando uma nova tabela do DynamoDB.
- Depois que a criptografia em repouso for ativada, ela não poderá ser desativada.
- Usa criptografia AES-256.
- Autenticação e controle de acesso
  - O acesso ao DynamoDB requer credenciais.
  - Além de credenciais válidas, você também precisa ter permissões para criar ou acessar recursos do DynamoDB.
  - Tipos de Identidades

- Usuário raiz da conta AWS
- **Usuário IAM**
- Papel IAM

Monitoramento

- Ferramentas automatizadas:
  - **Alarmes Amazon CloudWatch** - Observe uma única métrica ao longo de um período de tempo que você especificar e execute uma ou mais ações com base no valor da métrica em relação a um determinado limite ao longo de vários períodos de tempo.
  - **Amazon CloudWatch Logs** - Monitore, armazene e acesse seus arquivos de registro do AWS CloudTrail ou outras fontes.
  - **Eventos Amazon CloudWatch** - Combine eventos e encaminhe-os para uma ou mais funções ou fluxos de destino para fazer alterações, capturar informações de estado e tomar medidas corretivas.
  - **AWS CloudTrail Log Monitoring** - Compartilhe arquivos de log entre contas, monitore os arquivos de log do CloudTrail em tempo real enviando-os para CloudWatch Logs, escreva aplicativos de processamento de log em Java e valide que seus arquivos de log não mudaram após a entrega pelo CloudTrail.
- Usando as informações coletadas pelo CloudTrail, você pode determinar a solicitação que foi feita ao DynamoDB, o endereço IP a partir do qual a solicitação foi feita, quem fez a solicitação, quando foi feita e detalhes adicionais.

Melhores Práticas

Conheça as diferenças entre o design de dados relacionais e o NoSQL.

Sistemas de banco de dados relacional (RDBMS)	**Banco de dados NoSQL**
No RDBMS, os dados podem ser consultados de maneira flexível, mas as consultas são relativamente caras e não escalam bem em situações de alto tráfego.	Em um banco de dados NoSQL como o DynamoDB, os dados podem ser consultados de maneira eficiente em um número limitado de maneiras, fora das quais as consultas podem ser caras e lentas.
No RDBMS, você projeta para flexibilidade sem se preocupar com detalhes de implementação ou desempenho. A otimização de consulta geralmente não afeta o design do esquema, mas a normalização é muito importante.	No DynamoDB, você projeta seu esquema especificamente para tornar as consultas mais comuns e importantes o mais rápido e barato possível. Suas estruturas de dados são adaptadas aos requisitos específicos de seus casos de uso de negócios.

Para um RDBMS, você pode ir em frente e criar um modelo de dados normalizado sem pensar sobre os padrões de acesso. Você pode estendê-lo mais tarde, quando surgirem novas questões e requisitos de consulta. Você pode organizar cada tipo de dados em sua própria tabela.	Para o DynamoDB, por outro lado, você não deve começar a projetar seu esquema antes de saber as perguntas que ele precisará responder. Compreender os problemas de negócios e os casos de uso do aplicativo com antecedência é essencial. Você deve manter o mínimo de tabelas possível em um aplicativo DynamoDB. A maioria dos aplicativos bem projetados requer apenas uma mesa.
	É importante compreender três propriedades fundamentais dos padrões de acesso do seu aplicativo: 1. Tamanho dos dados: saber quantos dados serão armazenados e solicitados de uma vez ajudará a determinar a maneira mais eficaz de particionar os dados. 2. Formato dos dados: em vez de remodelar os dados quando uma consulta é processada, um banco de dados NoSQL organiza os dados para que sua forma no banco de dados corresponda ao que será consultado. 3. Velocidade de dados: O DynamoDB pode ser escalado aumentando o número de partições físicas disponíveis para processar consultas e distribuindo dados de maneira eficiente por essas partições. Saber com antecedência quais podem ser as cargas de consulta de pico ajuda a determinar como particionar os dados para melhor usar a capacidade de E / S.

Preços

- O DynamoDB cobra por GB de espaço em disco que sua mesa consome. Os primeiros 25 GB consumidos por mês são gratuitos.
- O DynamoDB cobra pela taxa de transferência provisionada WCU e RCU, capacidade reservada e transferência de dados fora.
- Você deve arredondar para o KB mais próximo ao estimar quantas unidades de capacidade provisionar.
- Existem encargos adicionais para DAX, tabelas globais, backups sob demanda (por GB), backups contínuos e recuperação pontual (por GB), restaurações de tabelas (por GB) e fluxos (unidades de solicitação de leitura).

Fontes:https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html?shortFooter=true

https://aws.amazon.com/dynamodb/faqs/

Amazon Elasticache

- ElastiCache é um ambiente de cache em memória distribuído na nuvem AWS.
- O ElastiCache funciona com os mecanismos Redis e Memcached.
- Elasticache pode ser usado para armazenar o estado da sessão.
- Redis VS Memcached
    - O Memcached foi projetado para simplificar, enquanto o Redis oferece um rico conjunto de recursos que o tornam eficaz para uma ampla variedade de casos de uso.

Preços

- Sob demanda, você paga apenas pelos recursos que consome por hora, sem nenhum compromisso de longo prazo.
- Com os nós reservados, você pode fazer um pagamento inicial baixo e único para cada nó que desejar para reservar por um período de 1 ou 3 anos. Em troca, você recebe um desconto significativo sobre a taxa de uso por hora em andamento para os nós que reservar.
- O ElastiCache fornece espaço de armazenamento para um instantâneo gratuitamente para cada cluster ElastiCache para Redis ativo. O armazenamento de backup adicional é cobrado.
- Os encargos de transferência regional de dados do EC2 se aplicam ao transferir dados entre uma instância do EC2 e um nó ElastiCache em diferentes zonas de disponibilidade da mesma região.

Fontes: https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/

https://aws.amazon.com/elasticache/redis-details/

https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/

https://aws.amazon.com/elasticache/redis-vs-memcached/

https://aws.amazon.com/elasticache/features/

https://aws.amazon.com/elasticache/pricing/

Amazon Redshift

- Um serviço de data warehouse totalmente gerenciado e em escala de petabytes.
- O Redshift estende as consultas do data warehouse ao seu data lake. Você pode executar consultas analíticas em petabytes de dados armazenados localmente no Redshift e diretamente em exabytes de dados armazenados no S3.
- RedShift é um tipo de banco de dados OLAP.
- Atualmente, o Redshift só oferece suporte a implantações Single-AZ.
- Características
    - Redshift usa armazenamento colunar, compressão de dados e mapas de zona para reduzir a quantidade de E / S necessária para realizar consultas.
    - Ele usa uma arquitetura de data warehouse de processamento massivamente paralelo para paralelizar e distribuir operações SQL.
    - O Redshift usa aprendizado de máquina para fornecer alto rendimento com base em suas cargas de trabalho.
    - O Redshift usa o cache de resultados para fornecer tempos de resposta abaixo de um segundo para consultas repetidas.
    - Redshift automaticamente e faz o backup contínuo de seus dados no S3. Ele pode replicar de forma assíncrona seus instantâneos para S3 em outra região para recuperação de desastres.
- Segurança
    - Por padrão, um cluster do Amazon Redshift é acessível apenas para a conta da AWS que cria o cluster.
    - Use o IAM para criar contas de usuário e gerenciar permissões para essas contas para controlar as operações de cluster.
    - Se você estiver usando a plataforma EC2-Classic para seu cluster Redshift, você deve usar grupos de segurança Redshift.
    - Se você estiver usando a plataforma EC2-VPC para o cluster Redshift, deverá usar grupos de segurança VPC.
    - Ao provisionar o cluster, você pode optar por criptografar o cluster para segurança adicional. A criptografia é uma propriedade imutável do cluster.
    - Os instantâneos criados a partir do cluster criptografado também são criptografados.
- Preços
    - Você paga uma taxa de faturamento por segundo com base no tipo e número de nós em seu cluster.

- Você paga pelo número de bytes verificados pelo RedShift Spectrum
- Você pode reservar instâncias comprometendo-se a usar o Redshift por um período de 1 ou 3 anos e economizar custos.

Fontes: https://docs.aws.amazon.com/redshift/latest/mgmt/

https://aws.amazon.com/redshift/features/

https://aws.amazon.com/redshift/pricing/

https://aws.amazon.com/redshift/faqs/

REDE E ENTREGA DE CONTEÚDO

Amazon API Gateway

- Permite que os desenvolvedores criem, publiquem, mantenham, monitorem e protejam APIs em qualquer escala.
- Permite criar, implantar e gerenciar uma API RESTful para expor endpoints HTTP de back-end, funções Lambda ou outros serviços AWS.
- Junto com a Lambda, o API Gateway forma a parte voltada para o aplicativo da infraestrutura sem servidor da AWS.
- Características
  - O API Gateway pode executar código Lambda em sua conta, iniciar máquinas de estado de Step Functions ou fazer chamadas para Elastic Beanstalk, EC2 ou serviços da web fora da AWS com endpoints HTTP publicamente acessíveis.
  - O API Gateway ajuda a gerenciar o tráfego para seus sistemas de back-end, permitindo que você defina regras de limitação com base no número de solicitações por segundo para cada método HTTP em suas APIs.
  - Você pode configurar um cache com chaves personalizáveis e tempo de vida em segundos para seus dados de API para evitar atingir seus serviços de back-end para cada solicitação.
  - Depois de construir, testar e implantar suas APIs, você pode empacotá-las em um plano de uso do API Gateway e vender o plano como um produto Software as a Service (SaaS) por meio do AWS Marketplace.
  - O API Gateway oferece a capacidade de criar, atualizar e excluir a documentação associada a cada parte de sua API, como métodos e recursos.
  - O Amazon API Gateway oferece disponibilidade geral de APIs HTTP, o que dá a você a capacidade de rotear solicitações para ELBs privados e serviços baseados em IP

registrados no AWS CloudMap, como tarefas ECS. Anteriormente, as APIs HTTP permitiam que os clientes criassem APIs apenas para seus aplicativos sem servidor ou para solicitações de proxy para terminais HTTP.

- Todas as APIs criadas expõem apenas terminais HTTPS. O API Gateway não oferece suporte a pontos de extremidade não criptografados (HTTP).
- Monitoramento
    - O console do API Gateway é integrado ao CloudWatch, para que você obtenha métricas de desempenho de back-end, como chamadas de API, latência e taxas de erro.
    - Você pode configurar alarmes personalizados em APIs de gateway de API.
    - O API Gateway também pode registrar erros de execução de API em CloudWatch Logs.
- Preços
    - Você paga apenas pelas chamadas de API que recebe e pela quantidade de dados transferidos para fora.
    - O API Gateway também fornece armazenamento em cache de dados opcional cobrado por hora que varia de acordo com o tamanho do cache selecionado.

Fontes: https://docs.aws.amazon.com/apigateway/latest/developerguide/

https://aws.amazon.com/api-gateway/features/

https://aws.amazon.com/api-gateway/pricing/

https://aws.amazon.com/api-gateway/faqs/

Amazon CloudFront

- Um serviço da web que acelera a distribuição de seu conteúdo estático e dinâmico da web para seus usuários. Um serviço Content Delivery Network (CDN).
- Ele entrega seu conteúdo por meio de uma rede mundial de data centers chamados pontos de presença. Quando um usuário solicita conteúdo que você está servindo com o CloudFront, o usuário é roteado para o ponto de presença que fornece a menor latência, para que o conteúdo seja entregue com o melhor desempenho possível.
    - Se o conteúdo já está no ponto de presença com a latência mais baixa, o CloudFront o entrega imediatamente.
    - Se o conteúdo não estiver nesse ponto de presença, o CloudFront o recupera de uma origem que você definiu

- O CloudFront também tem caches de presença regionais que trazem mais de seu conteúdo para mais perto de seus visualizadores, mesmo quando o conteúdo não é popular o suficiente para ficar em um ponto de presença do CloudFront, para ajudar a melhorar o desempenho desse conteúdo.
- Fontes diferentes do CloudFront
    - **Usando buckets S3 para sua origem** - você coloca quaisquer objetos que deseja que o CloudFront para entregar em um bucket S3.
    - *Usar buckets S3 configurados como endpoints de site para sua origem*
    - **Usando um contêiner de armazenamento de mídia ou um canal de pacote de mídia para sua origem** - você pode configurar um bucket S3 que é configurado como um contêiner MediaStore, ou criar um canal e endpoints com MediaPackage. Em seguida, você cria e configura uma distribuição no CloudFront para transmitir o vídeo.
    - **Usando EC2 ou outras Fontes personalizadas** - Uma origem personalizada é um servidor HTTP, por exemplo, um servidor da web.
    - **Usando grupos de origem do CloudFront para failover de origem** - use o failover de origem para designar uma origem primária para o CloudFront, além de uma segunda origem para a qual o CloudFront muda automaticamente quando a origem primária retorna respostas de falha de código de status HTTP específicas.

Distribuições do CloudFront

- Você cria uma distribuição do CloudFront para informar ao CloudFront de onde você deseja que o conteúdo seja entregue e os detalhes sobre como rastrear e gerenciar a entrega de conteúdo.
- Você cria uma distribuição e escolhe as configurações de configuração que deseja:
    - A origem do seu conteúdo, ou seja, o bucket do Amazon S3, o canal Media Package ou o servidor HTTP a partir do qual o CloudFront obtém os arquivos para distribuir. Você pode especificar qualquer combinação de até 25 buckets S3, canais e / ou servidores HTTP como suas Fontes.
    - Acesso - se você deseja que os arquivos estejam disponíveis para todos ou restrinja o acesso a alguns usuários.
    - Segurança - se você deseja que o CloudFront exija que os usuários usem HTTPS para acessar seu conteúdo.

- **Classe de preço**

o Escolha a classe de preço que corresponde ao preço máximo que você deseja pagar pelo serviço do CloudFront. Por padrão, o CloudFront atende seus objetos de pontos de presença em todas as regiões do CloudFront.

Monitoramento

- O CloudFront se integra às métricas do Amazon CloudWatch para que você possa monitorar seu site ou aplicativo.
- Capture solicitações de API com AWS CloudTrail. CloudFront é um serviço global. Para visualizar as solicitações do CloudFront em logs do CloudTrail, você deve atualizar uma trilha existente para incluir serviços globais.

Preços

o Cobrar pelo armazenamento em um bucket S3.

o Cobrar por servir objetos de locais de borda.

o Cobrança pelo envio de dados para sua origem.

- Transferência de dados para fora
- Solicitações HTTP / HTTPS
- Invalidação Solicitações de,
- Certificados SSL personalizados de IP dedicado associados a uma distribuição do CloudFront.

o Você também incorre em uma sobretaxa para solicitações HTTPS e uma sobretaxa adicional para solicitações que também têm criptografia em nível de campo habilitada.

Fontes: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide

https://aws.amazon.com/cloudfront/features/

https://aws.amazon.com/cloudfront/pricing/

https://aws.amazon.com/cloudfront/faqs/

AWS Elastic Load Balancing

- Distribui o aplicativo de entrada ou tráfego de rede em vários destinos, como instâncias EC2, contêineres (ECS), funções Lambda e endereços IP, em várias Zonas de disponibilidade.
- Ao criar um balanceador de carga, você deve especificar uma sub-rede pública de pelo menos duas zonas de disponibilidade. Você pode especificar apenas uma sub-rede pública por Zona de disponibilidade.

Características gerais

- Aceita tráfego de entrada de clientes e roteia solicitações para seus destinos registrados.
- Monitora a integridade de seus alvos registrados e roteia o tráfego apenas para alvos saudáveis.
- Ative a proteção contra exclusão para evitar que seu balanceador de carga seja excluído acidentalmente. Desativado por padrão.
- A exclusão do ELB não excluirá as instâncias registradas nele.
- **Balanceamento de carga entre zonas** - quando habilitado, cada nó do balanceador de carga distribui o tráfego entre os destinos registrados em todas as AZs habilitadas.
- Suporta SSL O ffloading, que é um recurso que permite ao ELB contornar a terminação SSL removendo a criptografia baseada em SSL do tráfego de entrada.

Três tipos de balanceadores de carga

- **Balanceador de carga de aplicativo**
    - Funções na camada de aplicativo, a sétima camada do modelo Open Systems Inter connection (OSI).
    - Permite HTTP e HTTPS.
    - Pelo menos 2 sub-redes devem ser especificadas ao criar este tipo de balanceador de carga.
    - Monitoramento:
        - Métricas do CloudWatch - recupere estatísticas sobre pontos de dados para seus balanceadores de carga e destinos como um conjunto ordenado de dados de séries temporal, conhecido como métricas.
        - Logs de acesso - capture informações detalhadas sobre as solicitações feitas ao balanceador de carga e armazene-as

como arquivos de log no S3.

- Logs do CloudTrail - capture informações detalhadas sobre as chamadas feitas à API Elastic Load Balancing API e armazene-as como arquivos de log no S3.

Balanceador de carga de rede

- Funções na quarta camada do modelo Open Systems Interconnection (OSI). Usa conexões TCP e UDP.
- Ao menos 1 sub-rede deve ser especificada ao criar este tipo de balanceador de carga, mas o número recomendado é 2.
- Monitoramento:
  - Métricas do CloudWatch - recupere estatísticas sobre pontos de dados para seus balanceadores de carga e destinos como um conjunto ordenado de dados de séries temporal, conhecido como métricas.
  - Logs de fluxo de VPC - capture informações detalhadas sobre o tráfego que vai de e para o balanceador de carga de rede.
  - Logs do CloudTrail - capture informações detalhadas sobre as chamadas feitas para a API Elastic Load Balancing API e armazene-as como arquivos de log no Amazon S3.

Balanceador de carga clássico

- Distribui o tráfego de entrada de aplicativos em várias instâncias do EC2 em disponibilidade múltipla Zonas.
- Para uso apenas com EC2 classic. Registre instâncias com o balanceador de carga. A AWS recomenda usar balanceadores de carga de aplicativo ou rede.
- Um balanceador de carga voltado para a Internet tem um nome DNS resolvível publicamente, para que possa rotear solicitações de clientes pela Internet para as instâncias EC2 registradas com o balanceador de carga. Os balanceadores de carga clássicos estão sempre voltados para a Internet.
- Monitoramento:
  - Métricas do CloudWatch - recupera estatísticas sobre pontos de dados publicados por ELB como um ordenado conjunto de dados de série temporal, conhecido como

métricas.

- Logs de acesso - capture informações detalhadas para solicitações feitas ao seu balanceador de carga e os armazene como arquivos de log no bucket S3 que você especificar.
- Logs do CloudTrail - acompanhe as chamadas feitas para a API Elastic Load Balancing por ou em nome de sua conta AWS

Segurança, autenticação e controle de acesso

- Use as políticas do IAM para conceder permissões
- Permissões de nível de recurso
- Grupos de segurança que controlam o tráfego permitido de e para seu balanceador de carga. Regras recomendadas para balanceador de carga voltado para a Internet:

De entrada	
Fonte	**Faixa Portuária**
0.0.0.0/0	*ouvinte*
Saída	
Destino	***Faixa Portuária***
grupo de segurança da instância	*ouvinte de instância*
grupo de segurança da instância	*exame de saúde*

Para balanceador de carga interno:

De entrada	
Fonte	**Faixa Portuária**
VPC CIDR	*ouvinte*
Saída	
Destino	**Faixa Portuária**
grupo de segurança da instância	*ouvinte de instância*
grupo de segurança da instância	*exame de saúde*

Resumo dos recursos

Preços

- Você é cobrado por cada hora ou hora parcial em que um Balanceador de Carga do Aplicativo está em execução e o número de Unidades de Capacidade do Balanceador de Carga (LCU) usado por hora.
- Você é cobrado por cada hora ou hora parcial em que um balanceador de carga de rede está em execução e pelo número de unidades de capacidade do balanceador de carga (LCU) usadas pelo balanceador de carga de rede por hora.
- Você é cobrado por cada hora ou hora parcial em que um Classic Load Balancer está em execução e por cada GB de dados transferidos por meio de seu balanceador de carga.

Fontes: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.htm

https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html
https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/introduction.html
https://aws.amazon.com/elasticloadbalancing/features/

https://aws.amazon.com/elasticloadbalancing/pricing/?nc=sn&loc=3

Amazon Route 53

- Um serviço da Web de Sistema de Nome de Domínio (DNS) altamente disponível e escalonável usado para registro de domínio, roteamento de DNS e verificação de integridade.

Características principais

- Resolver
- Fluxo de tráfego
- Roteamento baseado em latência
- Geo DNS
- DNS privado para Amazon VPC
- Failover de DNS
- Verificações e monitoramento de saúde
- Registro do Domínio
- Suporte para Apex do CloudFront e S3 Zone
- Integração Amazon ELB

o Registro do Domínio

- Escolha um nome de domínio e confirme que está disponível, então registre o nome de domínio com o Route 53. O serviço torna-se automaticamente o serviço DNS para o domínio ao fazer o seguinte:
    - o Cria uma zona hospedada com o mesmo nome de seu domínio.
    - o Atribui um conjunto de quatro servidores de nomes à zona hospedada. Quando alguém usa um navegador para acessar seu site, comowww.example.com, esses servidores de nome informam ao navegador onde encontrar seus recursos, como um servidor web ou um bucket S3.
    - o Obtém os servidores de nomes da zona hospedada e os adiciona ao domínio.
        - Se você já registrou um nome de domínio com outro registrador, pode optar por transferir o registro de domínio para o Route 53.

o Encaminhando o tráfego da Internet para o seu site ou aplicativo da web

- Use o console do Route 53 para registrar um nome de domínio e configurar o Route 53 para rotear o tráfego da Internet para seu site ou aplicativo da web.
- Depois de registrar seu nome de domínio, o Route 53 cria automaticamente uma zona

hospedada pública com o mesmo nome do domínio.

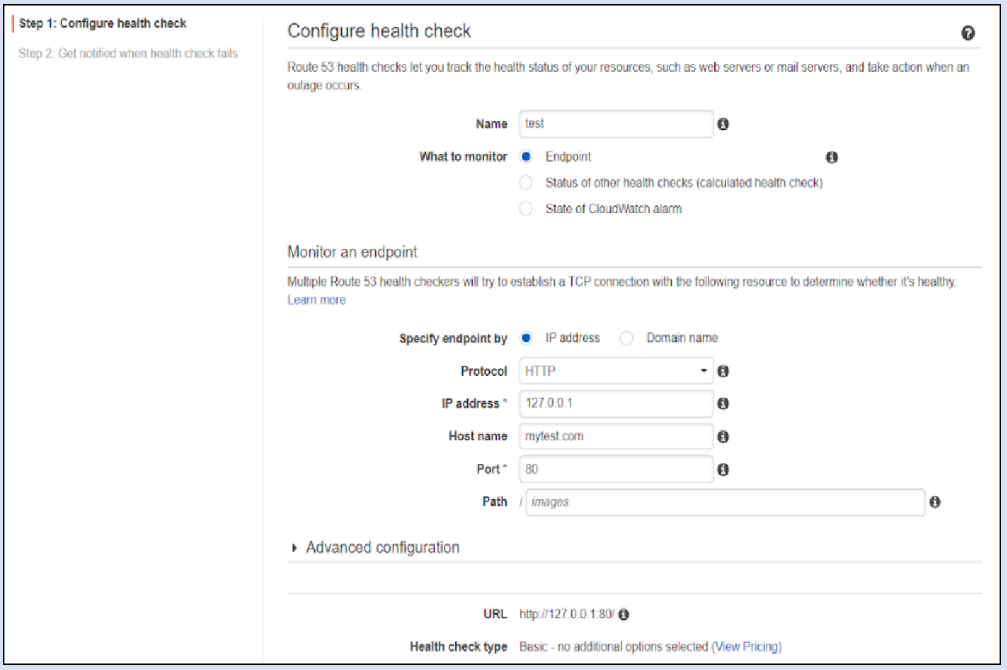
- Para encaminhar o tráfego para seus recursos, você cria registros, também conhecidos como conjuntos de registros de recursos, em sua zona hospedada.
- Você pode criar registros especiais do Route 53, chamados de registros de aliás, que direcionam o tráfego para buckets S3, distribuições do CloudFront e outros recursos da AWS.
- Cada registro inclui informações sobre como você deseja rotear o tráfego para seu domínio, como:
    - Nome - o nome do registro corresponde ao nome de domínio ou nome de subdomínio para o qual você deseja que o Route 53 faça o roteamento do tráfego.
    - Tipo - determina o tipo de recurso para o qual você deseja que o tráfego seja roteado.
- Valor
- **Conheça os seguintes conceitos**
- Conceitos de registro de domínio - nome de domínio, registrador de domínio, registro de domínio, revendedor de domínio, domínio de nível superior
- Conceitos de DNS
    - **Registro de aliás** - um tipo de registro que você pode criar para rotear o tráfego para recursos da AWS.
    - Consulta DNS
    - Resolvedor DNS
    - Sistema de Nome de Domínio (DNS)
    - DNS privado
    - **Zona hospedada** - um contêiner para registros, que inclui informações sobre como rotear o tráfego para um domínio e todos os seus subdomínios.
    - **Servidores de nome** - servidores no DNS que ajudam a traduzir nomes de domínio em endereços IP que os computadores usam para se comunicarem entre si.
    - **Registro** (Registro DNS) - um objeto em uma zona hospedada que você usa para definir como deseja rotear o tráfego para o domínio ou subdomínio.
    - *Política de Roteamento*
    - **Subdomínio**
    - Tempo de vida (TTL)

Registros

- Registros de aliás
    - Os registros de alias do Route 53 fornecem uma extensão específica do Route 53 para a funcionalidade DNS. Os registros de alias permitem que você roteie o tráfego para recursos selecionados da AWS. Eles também permitem rotear o tráfego de um registro em uma zona hospedada para outro registro.
    - Você pode criar um registro de alias no nó superior de um name space DNS, também conhecido como ápice da zona.
- Registro CNAME
    - Você não pode criar um registro de alias no nó superior de um name space DNS usando um registro CNAME.
- Registros de aliás x registros CNAME

Registros CNAME	**Registros de alias**
Você não pode criar um registro CNAME no ápice da zona.	Você pode criar um registro de alias no ápice da zona. Os registros de alias devem ter o mesmo tipo do registro para o qual você está roteando o tráfego.
O Route 53 cobra para consultas CNAME.	O Route 53 não cobra por consultas de alias aos recursos da AWS.
Um registro CNAME redireciona as consultas para um nome de domínio, independentemente do tipo de registro.	O Route 53 responde a uma consulta DNS apenas quando o nome e tipo do registro de alias correspondem ao nome e tipo na consulta.
Um registro CNAME pode apontar para qualquer registro DNS hospedado em qualquer lugar.	Um registro de alias só pode apontar para recursos selecionados da AWS ou para outro registro na zona hospedada em que você está criando o registro de alias.
Um registro CNAME aparece como um registro CNAME em resposta às consultas de pesquisa dig ou Name Server (NS).	Um registro de alias aparece como o tipo de registro que você especificou ao criar o registro, como A ou AAAA.

Verificações de integridade do Route 53 e failover de DNS



- Cada verificação de integridade que você cria pode monitorar um dos seguintes:
    - A saúde de um recurso específico, como um servidor web
    - O status de outras verificações de saúde
    - O status de um alarme Amazon CloudWatch
- Dois tipos de configurações de failover
    - **Failover ativo-ativo** - todos os registros que têm o mesmo nome, o mesmo tipo e a mesma política de roteamento estão ativos, a menos que o Route 53 os considere não íntegros. Use esta configuração de failover quando quiser que todos os seus recursos estejam disponíveis na maior parte do tempo.
    - **Failover Ativo-Passivo** - use esta configuração de failover quando desejar que um recurso primário ou grupo de recursos esteja disponível a maior parte do tempo e deseja que um recurso secundário ou grupo de recursos fique em espera no caso de todos os recursos primários ficarem indisponíveis. Ao responder a consultas, o Route 53 inclui apenas os recursos primários saudáveis.

o Monitoramento

- O painel do Route 53 fornece informações detalhadas sobre o status de seus registros de domínio, incluindo:
    - Status de novos registros de domínio
    - Status de transferências de domínio para Route 53

- Lista de domínios que estão se aproximando da data de expiração

- Você pode usar as métricas do Amazon CloudWatch para ver o número de consultas DNS servidas para cada uma de suas zonas hospedadas públicas do Route 53. Com essas métricas, você pode ver rapidamente o nível de atividade de cada zona hospedada para monitorar as mudanças no tráfego.
- Você pode monitorar seus recursos criando verificações de saúde do Route 53, que usam o CloudWatch para coletar e processar dados brutos em métricas legíveis, quase em tempo real.
- Registrar chamadas de API com CloudTrail

Preços

- Uma zona hospedada é cobrada no momento em que é criada e no primeiro dia de cada mês subsequente. Para permitir o teste, uma zona hospedada que é excluída dentro de 12 horas de criação não é cobrada; no entanto, quaisquer consultas nessa zona hospedada ainda incorrerão em cobranças.
- Bilhões de consultas / mês
- As consultas aos registros de alias são fornecidas sem custo adicional para os clientes atuais do Route 53 quando os registros são mapeados para os seguintes tipos de recursos da AWS:
  - Elastic Load Balancers
  - Amazon CloudFront distribuições
  - Ambientes AWS Elastic Beanstalk
  - Buckets do Amazon S3 que são con fi gurados como endpoints de sites
- Registro de política de fluxo de tráfego / mês
- Os preços para nomes de domínio variam de acordo com o domínio de nível superior (TLD)

Fontes: *https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.htmeu*

https://aws.amazon.com/route53/features/

https://aws.amazon.com/route53/pricing/

Amazon VPC

- Crie uma rede virtual na nuvem dedicada à sua conta AWS, onde você pode iniciar recursos AWS
- Amazon VPC é a camada de rede do Amazon EC2
- Um VPC abrange todas as zonas de disponibilidade da região. Depois de criar um VPC, você pode adicionar uma ou mais sub-redes em cada zona de disponibilidade.

Conceitos chave

- Uma nuvem privada virtual (VPC) permite que você especifique um intervalo de endereços IP para o VPC, adicione sub-redes, associe grupos de segurança e configure tabelas de rotas.
- Uma sub-rede é um intervalo de endereços IP em seu VPC. Você pode lançar recursos da AWS em uma sub-rede específica. Use uma sub-rede pública para recursos que devem ser conectados à Internet e uma sub-rede privada para recursos que não serão conectados à Internet.
- Para proteger os recursos da AWS em cada sub-rede, use grupos de segurança e listas de controle de acesso à rede (ACL).
- Expanda seu VPC adicionando intervalos de IP secundários.

VPC padrão vs não padrão

Acessando uma rede corporativa ou doméstica

- Opcionalmente, você pode conectar seu VPC ao seu próprio data center corporativo usando uma conexão VPN gerenciada IPsec AWS, tornando a nuvem AWS uma extensão do seu data center.
- Uma conexão VPN consiste em:
    - um gateway privado virtual (que é o concentrador de VPN no lado da Amazon da conexão VPN) conectado ao seu VPC.
    - um gateway de cliente (que é um dispositivo físico ou dispositivo de software do seu lado da conexão VPN) localizado no data center.
    - Um diagrama da conexão

Cenários de caso de uso de VPC

- VPC com uma única sub-rede pública
- VPC com sub-redes públicas e privadas (NAT)
- VPC com sub-redes públicas e privadas e acesso VPN gerenciado AWS
- VPC com apenas uma sub-rede privada e acesso VPN gerenciado AWS

Sub-redes

- Ao criar um VPC, você deve especificar um intervalo de endereços IPv4 para o VPC na forma de um bloco Class less Inter-Domain Routing (CIDR) (exemplo: 10.0.0.0/16). Este é o bloco CIDR primário para seu VPC.
- Você pode adicionar uma ou mais sub-redes em cada zona de disponibilidade da região do seu VPC.
- Você especifica o bloco CIDR para uma sub-rede, que é um subconjunto do bloco CIDR VPC.
- Um bloco CIDR não deve se sobrepor a nenhum bloco CIDR existente associado ao VPC.
- Tipos de sub-redes
    - Sub-rede pública - tem um gateway de internet
    - Sub-rede privada - não tem um gateway de internet
    - Sub-rede apenas VPN - tem, em vez disso, um gateway privado virtual
- Você não pode aumentar ou diminuir o tamanho de um bloco CIDR existente.
- Quando você associa um bloco CIDR ao seu VPC, uma rota é adicionada automaticamente às suas tabelas de rota VPC para habilitar o roteamento dentro do VPC (o destino é o bloco CIDR e o destino é local).
- Você tem um limite para o número de blocos CIDR que pode associar a um VPC e o número de rotas que pode adicionar a uma tabela de rotas.

Roteamento de sub-rede

- Cada sub-rede deve ser associada a uma tabela de rotas, que especifica as rotas permitidas para o tráfego de saída que sai da sub-rede.
- Cada sub-rede que você cria é automaticamente associada à tabela de rota principal para o VPC.
- Você pode alterar a associação e o conteúdo da tabela de rota principal.

- Você pode permitir que uma instância em seu VPC inicie conexões de saída para a Internet por IPv4, mas evitar conexões de entrada não solicitadas da Internet usando um gateway NAT ou instância NAT.
- Para iniciar a comunicação apenas de saída com a Internet por IPv6, você pode usar uma Internet apenas de saída Porta de entrada.

Segurança de sub-rede

- Grupos de segurança - controle o tráfego de entrada e saída para suas instâncias
    - Você pode associar um ou mais (até cinco) grupos de segurança a uma instância em seu VPC.
    - Se você não especificar um grupo de segurança, a instância pertence automaticamente ao grupo de segurança padrão.
    - Quando você cria um grupo de segurança, ele não tem regras de entrada. Por padrão, inclui uma regra de saída que permite todo o tráfego de saída.
    - Os grupos de segurança são associados a interfaces de rede.
- Listas de controle de acesso à rede - controle o tráfego de entrada e saída para suas sub-redes
    - Cada sub-rede em seu VPC deve ser associada a uma rede ACL. Se nenhum estiver associado, automaticamente associado à ACL de rede padrão.
    - Você pode associar uma ACL de rede a várias sub-redes; entretanto, uma sub-rede pode ser associada a apenas uma ACL de rede por vez.
    - Uma rede ACL contém uma lista numerada de regras que é avaliada em ordem, começando com a regra de menor número, para determinar se o tráfego é permitido dentro ou fora de qualquer sub-rede associada à rede ACL.
    - A rede ACL padrão é configurada para permitir que todo o tráfego entre e saia das sub-redes às quais está associada.
- Logs de fluxo - capture informações sobre o tráfego de IP indo e vindo das interfaces de rede em seu VPC que são publicadas nos Logs do CloudWatch.
- Diagrama de grupos de segurança e NACLs em um VPC

Componentes de rede VPC

- Interfaces de rede

- uma interface de rede virtual que pode incluir:
  - um endereço IPv4 privado primário
  - um ou mais endereços IPv4 privados secundários
  - um endereço Elastic IP por endereço IPv4 privado
  - um endereço IPv4 público, que pode ser atribuído automaticamente à interface de rede para eth0 quando você inicia uma instância
  - um ou mais endereços IPv6
  - um ou mais grupos de segurança
  - um endereço MAC
  - uma bandeira de verificação de origem / destino
  - Uma descrição
- As interfaces de rede podem ser conectadas e desconectadas das instâncias, no entanto, você não pode desconectar uma interface de rede primária.

Tabelas de rota

- contém um conjunto de regras, chamadas rotas, que são usadas para determinar para onde o tráfego da rede é direcionado.
- Uma sub-rede só pode ser associada a uma tabela de rota por vez, mas você pode associar várias sub-redes à mesma tabela de rota.
- Você não pode excluir a tabela de rota principal, mas pode substituir a tabela de rota principal por uma tabela personalizada que você criou.
- Você deve atualizar a tabela de rotas para qualquer sub-rede que use gateways ou conexões.

Gateways de Internet

- Permite a comunicação entre instâncias em seu VPC e a Internet.
- Não impõe riscos de disponibilidade ou restrições de largura de banda em seu tráfego de rede.

NAT

- Habilite instâncias em uma sub-rede privada para se conectar à Internet ou

outros serviços da AWS, mas evite que a Internet inicie conexões com as instâncias.

Instância NAT vs Gateways NAT

DNS

- A AWS fornece instâncias iniciadas em um VPC padrão com nomes de host DNS públicos e privados que correspondem aos endereços IPv4 públicos e IPv4 privados para a instância.

Elastic IP Addresses

- ***UM endereço*** *IPv4 público estático.*
- Você pode associar um endereço Elastic IP a qualquer instância ou interface de rede para qualquer VPC em sua conta.
- Você pode mascarar a falha de uma instância remapeando rapidamente o endereço para outra instância em seu VPC.
- Seus endereços Elastic IP permanecem associados à sua conta AWS até que você os libere explicitamente.
- A AWS impõe uma pequena cobrança por hora quando os EIPs não estão associados a uma instância em execução ou quando estão associados a uma instância interrompida ou a uma interface de rede não conectada.
- Você está limitado a cinco endereços Elastic IP.

Preços

- Cobrado por hora de conexão VPN
- Cobrado por cada "hora de gateway de NAT" que seu gateway de NAT está provisionado e disponível.
- As taxas de processamento de dados se aplicam a cada Gigabyte processado por meio do gateway NAT, independentemente da origem ou destino do tráfego.
- Você também incorre em encargos de transferência de dados padrão da AWS para todos os dados transferidos por meio do gateway NAT.
- Cobranças por Elastic IPs não utilizados ou inativos.

Fontes:

https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

https://aws.amazon.com/vpc/details/

https://aws.amazon.com/vpc/pricing/ https://aws.amazon.com/vpc/faqs/

SEGURANÇA E IDENTIDADE

AWS Identity and Access Management (IAM)

- Controle quem está autenticado (conectado) e autorizado (tem permissões) para usar os recursos.
- O usuário raiz da conta da AWS é uma identidade de login único que tem acesso completo a todos os serviços e recursos da AWS na conta.

- ***Características***
  - Você pode conceder permissão a outras pessoas para administrar e usar recursos em sua conta da AWS sem precisar compartilhar sua senha ou chave de acesso.
  - Você pode conceder permissões diferentes a pessoas diferentes para recursos diferentes.
  - Você pode adicionar autenticação de dois fatores à sua conta e a usuários individuais para segurança extra.
  - Você recebe registros de log do AWS CloudTrail que incluem informações sobre as identidades do IAM que fizeram solicitações de recursos em sua conta.
  - Você usa uma chave de acesso (uma ID de chave de acesso e uma chave de acesso secreta) para fazer solicitações programáticas à AWS. Um ID de chave de acesso e uma chave de acesso secreta podem ser gerados exclusivamente uma vez e devem ser regenerados se perdidos.
  - URL exclusivo da página de login da sua conta:
    - https://My_AWS_Account_ID.signin.aws.amazon.com/console/
  - Você pode usar tags IAM para adicionar atributos personalizados a um usuário ou função IAM usando um par de valores-chave de tag.

Elementos de infraestrutura

- **Diretor**
  - Uma entidade que pode fazer uma solicitação para uma ação ou operação em um recurso da AWS. Usuários, funções, usuários federados e aplicativos são todos os principais da AWS.
  - O usuário root da sua conta AWS é seu primeiro diretor.
- *Solicitação*
  - Quando um principal tenta usar o AWS Management Console, a AWS API ou o AWS CLI, esse principal envia uma solicitação para a AWS.

- As solicitações incluem as seguintes informações:
    - **Ações ou operações** - as ações ou operações que o diretor deseja realizar.
    - **Recursos** - o objeto de recurso da AWS sobre o qual as ações ou operações são realizadas.
    - **Diretor** - o usuário, função, usuário federado ou aplicativo que enviou a solicitação. As informações sobre o principal incluem as políticas associadas a esses principal.
    - **Dados ambientais** - informações sobre o endereço IP, agente do usuário, status de SSL habilitado ou a hora do dia.
    - **Dados de recursos** - dados relacionados ao recurso que está sendo solicitado.

Autenticação

- Para se autenticar no console como um usuário, você deve entrar com seu nome de usuário e senha.
- Para autenticar a partir da API ou AWS CLI, você deve fornecer sua chave de acesso e chave secreta.

o Autorização

- Para fornecer a seus usuários permissões para acessar os recursos da AWS em suas próprias contas, você precisa de políticas baseadas em identidade.
- **Políticas baseadas em recursos** destinam-se a conceder acesso entre contas.
- Regras lógicas de avaliação para políticas:
    - Por padrão, todas as solicitações são negadas.
    - Uma permissão explícita em uma política de permissões substitui esse padrão.
    - Um limite de permissões substitui a permissão. Se houver um limite de permissõesque se aplica, esse limite deve permitir a solicitação. Caso contrário, é negado implicitamente.
    - Uma negação explícita em qualquer política substitui qualquer permissão.

o Ações ou operações

        - As operações são definidas por um serviço e incluem coisas que você pode fazer em um recurso, como visualizar, criar, editar e excluir esse recurso.

    - *Recurso*

        - Um objeto que existe dentro de um serviço. O serviço define um conjunto de ações que podem ser executadas em cada recurso.

- *Comercial*

    - **Usuários IAM**

        - Em vez de compartilhar suas credenciais de usuário root com outras pessoas, você pode criar usuários IAM individuais em sua conta que correspondam aos usuários em sua organização. Os usuários do IAM não são contas separadas; eles são usuários de sua conta.
        - Cada usuário pode ter sua própria senha para acessar o AWS Management Console. Você também pode criar uma chave de acesso individual para cada usuário, de modo que o usuário possa fazer solicitações programáticas para trabalhar com recursos em sua conta.
        - Por padrão, um novo usuário IAM NÃO tem permissão para fazer nada.
        - Os usuários são entidades globais.

    - *Usuários Federados*

        - Se os usuários em sua organização já têm uma maneira de serem autenticados, você pode federar essas identidades de usuário na AWS.

    - *Grupos IAM*

        - Um grupo IAM é uma coleção de usuários IAM.
        - Você pode organizar os usuários IAM em grupos IAM e anexar políticas de controle de acesso a um grupo.
        - Um usuário pode pertencer a vários grupos.
        - Os grupos não podem pertencer a outros grupos.
        - Os grupos não têm credenciais de segurança e não podem acessar os serviços da web diretamente.

    - *Papel IAM*

        - Uma função não possui credenciais associadas a ela.
        - Um usuário IAM pode assumir uma função para assumir temporariamente diferentes permissões para uma tarefa específica. Uma função pode ser atribuída a um usuário federado que entra usando um provedor de identidade externo em vez de IAM.

        - **Função de serviço AWS** é uma função que um serviço assume para realizar ações em sua conta em seu nome. Esta função de serviço deve incluir todas as permissões necessárias para que o serviço acesse os recursos da AWS de que precisa.
    - Os usuários ou grupos podem ter várias políticas anexadas a eles que concedem permissões diferentes.

- *Políticas*
    - A maioria das políticas de permissão são documentos de política JSON.
    - Para atribuir permissões a usuários federados, você pode criar uma entidade referida como função e definir permissões para a função.
    - *Políticas baseadas em identidade*
        - Políticas de permissões que você anexa a um principal ou identidade.
        - **Políticas gerenciadas** são políticas autônomas que você pode anexar a vários usuários, grupos e funções em sua conta da AWS.
        - **Políticas inline** são políticas que você cria e gerencia e que são incorporadas diretamente a um único usuário, grupo ou função.
    - *Políticas baseadas em recursos*
        - Políticas de permissões que você anexa a um recurso como um bucket do Amazon S3.
        - As políticas baseadas em recursos são apenas políticas embutidas.
        - **Políticas de confiança** - políticas baseadas em recursos que são anexadas a uma função e definem quais diretores podem assumir a função.
- *Serviço de token de segurança AWS (STS)*
    - Crie e forneça a usuários confiáveis credenciais de segurança temporárias que podem controlar o acesso aos seus recursos da AWS.
    - Credenciais de segurança temporárias são de curto prazo e não são armazenados com o usuário, mas são gerados dinamicamente e fornecidos ao usuário quando solicitados.
    - Por padrão, AWS STS é um serviço global com um único endpoint em https://sts.amazonaws.com.
- Assumir opções de função
    - AssumeRole - Retorna um conjunto de credenciais de segurança temporárias que

você pode usar para acessar recursos da AWS aos quais você normalmente não teria acesso. Essas credenciais temporárias consistem em um ID de chave de acesso, uma chave de acesso secreta e um token de segurança. Normalmente, você usa AssumeRole em sua conta ou para acesso entre contas.

- Você pode incluir informações de autenticação multifator (MFA) ao chamar AssumeRole. Isso é útil para cenários de contas cruzadas para garantir que o usuário que assume a função foi autenticado com um dispositivo AWS MFA.

- AssumeRoleWithSAML - Retorna um conjunto de credenciais de segurança temporárias para usuários que foram autenticados por meio de uma resposta de autenticação SAML. Isso permite que você vincule seu armazenamento de identidade corporativa ou diretório ao acesso AWS baseado em função sem credenciais ou configurações específicas do usuário.

- AssumeRoleWithWebIdentity - Retorna um conjunto de credenciais de segurança temporárias para usuários que foram autenticados em um aplicativo móvel ou web com um provedor de identidade web. Provedores de exemplo incluem Amazon Cognito, Login com Amazon, Facebook, Google ou qualquer provedor de identidade compatível com OpenID Connect.

- STS Obter Tokens

  - GetFederationToken - Retorna um conjunto de credenciais de segurança temporárias (consistindo em um ID de chave de acesso, uma chave de acesso secreta e um token de segurança) para um usuário federado. Você deve chamar a operação GetFederationToken usando as credenciais de segurança de longo prazo de um usuário IAM. Um uso típico é em um aplicativo proxy que obtém credenciais de segurança temporárias em nome de aplicativos distribuídos dentro de uma rede corporativa.

  - GetSessionToken - Retorna um conjunto de credenciais temporárias para uma conta AWS ou usuário IAM. As credenciais consistem em um ID de chave de acesso, uma chave de acesso secreta e um token de segurança. Você deve chamar a operação GetSessionToken usando as credenciais de segurança de longo prazo de um usuário IAM. Normalmente, você usa GetSessionToken se deseja usar MFA para proteger chamadas programáticas para operações específicas da API da AWS.

Melhores Práticas

- Bloqueie suas chaves de acesso de usuário raiz da conta da AWS
- Criar usuários IAM individuais
- Use grupos para atribuir permissões a usuários IAM
- Use políticas definidas pela AWS para atribuir permissões sempre que possível

- Conceder privilégio mínimo
- Use níveis de acesso para revisar as permissões do IAM
- Configure uma política de senha forte para seus usuários
- Habilitar MFA para usuários privilegiados
- Use funções para aplicativos executados em instâncias do Amazon EC2
- Use funções para delegar permissões
- Não compartilhe chaves de acesso
- Girar Credenciais regularmente
- Remover Credenciais desnecessárias
- Condições da política de uso para segurança extra
- Monitore a atividade em sua conta AWS

Fontes: https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

https://aws.amazon.com/iam/faqs/

AWS WAF

- Um firewall de aplicativo da web que ajuda a proteger os aplicativos da web de ataques, permitindo que você configure regras que permitem, bloqueiam ou monitoram (contam) solicitações da web com base nas condições que você definir.

Características

- WAF permite criar regras para filtrar o tráfego da web com base em condições que incluem endereços IP, cabeçalhos e corpo HTTP ou URIs personalizados.
- Você também pode criar regras que bloqueiam exploits comuns da web, como injeção de SQL e script entre sites.
- Para ataques à camada de aplicativo, você pode usar WAF para responder a incidentes.

Preços

- WAF cobra com base no número de listas de controle de acesso à web (ACLs da web) que você cria, o número de regras que você adiciona por ACL da web e o número de solicitações da web que você recebe.

Fontes: https://docs.aws.amazon.com/waf/latest/developerguide

https://aws.amazon.com/waf/features/

https://aws.amazon.com/waf/pricing/

https://aws.amazon.com/waf/faqs/

Amazon Macie

- Um serviço de segurança que usa aprendizado de máquina para descobrir, classificar e proteger automaticamente dados confidenciais na AWS. Macie reconhece dados confidenciais, como informações de identificação pessoal (PII) ou propriedade intelectual.
- O Amazon Macie permite que você alcance o seguinte:
    - Identifique e proteja vários tipos de dados, incluindo PII, PHI, documentos regulamentares, chaves de API e chaves secretas
    - Verifique a conformidade com registros automatizados que permitem auditoria instantânea
    - Identificar mudanças nas políticas e listas de controle de acesso
    - Observe as mudanças no comportamento do usuário e receba alertas acionáveis
    - Receba notificações quando os dados e as credenciais da conta deixarem as zonas protegidas
    - Detectar quando grandes quantidades de documentos essenciais aos negócios são compartilhadas interna e externamente

Fontes:

https://aws.amazon.com/macie/

https://docs.aws.amazon.com/macie/latest/userguide/what-is-macie.htmeu

https://aws.amazon.com/macie/faq/

https://www.youtube.com/watch?v=LCjX2rsQ2wA

Shield AWS

- Um serviço gerenciado de proteção de negação de serviço distribuída (DDoS) que protege os aplicativos em execução na AWS.

- *Escudo de níveis e recursos padrão*
    - Todos os clientes da AWS se beneficiam das proteções automáticas do Shield Standard.
- *Avançado*
    - O Shield Advanced oferece detecção aprimorada, inspecionando fl uxos de rede e também monitorando o tráfego da camada de aplicativo para seu endereço Elastic IP, Elastic Load Balancing, CloudFront ou recursos do Route 53.
    - Ele lida com a maioria das responsabilidades de proteção e mitigação de DDoS para a camada 3, camada 4 e
- **camada 7** ataques.
    - Você tem acesso 24 horas por dia, 7 dias por semana à equipe de resposta DDoS da AWS. Para entrar em contato com a equipe de resposta DDoS, os clientes precisarão dos níveis de suporte corporativo ou comercial do AWS Premium Support.

Preços

- **Escudo Padrão** fornece proteção sem custo adicional.
- **Escudo Avançado**, no entanto, é um serviço pago. Ele exige um compromisso de assinatura de 1 ano e cobra uma taxa mensal, além de uma taxa de uso com base na transferência de dados do CloudFront, ELB, EC2 e AWS Global Accelerator.

Fontes: https://aws.amazon.com/shield/features/

https://aws.amazon.com/shield/pricing/

https://aws.amazon.com/shield/faqs/

Amazon Inspector

- Um serviço de avaliação de segurança automatizado que ajuda a testar a acessibilidade de rede de suas instâncias EC2 e o estado de segurança de seus aplicativos em execução nas instâncias.
- O Inspector usa funções vinculadas a serviços do IAM.

Características

- Inspetor fornece um mecanismo que analisa a configuração do sistema e dos recursos e monitora a atividade para determinar a aparência de um alvo de avaliação, como ele se

comporta e seus componentes dependentes. A combinação dessa telemetria fornece uma imagem completa do alvo da avaliação e seus possíveis problemas de segurança ou conformidade.

- Inspetor incorpora uma biblioteca interna de regras e relatórios. Isso inclui verificações de práticas recomendadas, padrões de conformidade comuns e vulnerabilidades.
- Automatize as avaliações de vulnerabilidade de segurança em todo seu pipeline de desenvolvimento e implantação ou contra sistemas de produção estáticos.
- Inspector é um serviço orientado por API que usa um agente opcional, tornando-o fácil de implantar, gerenciar e automatizar.

Fontes: https://docs.aws.amazon.com/inspector/latest/userguide

https://aws.amazon.com/inspector/pricing/

https://aws.amazon.com/inspector/faqs/

Organizações AWS

- Ele oferece gerenciamento baseado em políticas para várias contas da AWS.

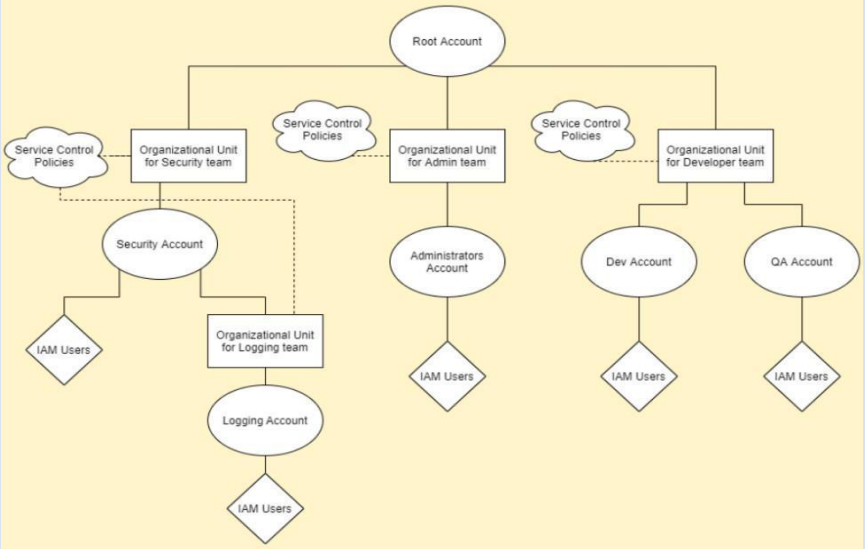
Características

- Com Organizações, você pode criar grupos de contas e aplicar políticas a esses grupos.
- Organizações fornece a você uma estrutura de política para várias contas da AWS. Você pode aplicar políticas a um grupo de contas ou a todas as contas da sua organização.
- O AWS Organizations permite que você configure um único método de pagamento para todas as contas da AWS em sua organização por meio do faturamento consolidado. Com o faturamento consolidado, você pode ter uma visão combinada das despesas incorridas por todas as suas contas, bem como aproveitar os benefícios de preços do uso agregado, como descontos por volume para EC2 e S3.
- AWS Organizations, como muitos outros serviços da AWS, é eventualmente consistente. Ele atinge alta disponibilidade ao replicar dados em vários servidores em datacenters da AWS em sua região.

Ações Administrativas em Organizações

- Crie uma conta AWS e adicione-a à sua organização ou adicione uma conta AWS existente à sua organização.
- Organize suas contas da AWS em grupos chamados unidades organizacionais (OUs).

- Organize suas UOs em uma hierarquia que reflita estrutura da sua empresa.
- Gerencie centralmente e anexe políticas a toda a organização, UOs ou contas individuais da AWS.



Conceitos

- Uma organização é uma coleção de contas da AWS que você pode organizar em uma hierarquia e gerenciar centralmente.
- Uma conta mestre é a conta da AWS que você usa para criar sua organização. Você não pode alterar qual conta em sua organização é a conta mestre.
    - A partir da conta mestre, você pode criar outras contas em sua organização, convidar e gerenciar convites para outras contas ingressarem em sua organização e remover contas de sua organização.
    - Você também pode anexar políticas a entidades como raízes administrativas, unidades organizacionais (UOs) ou contas dentro de sua organização.
    - A conta mestre tem a função de conta pagadora e é responsável por pagar todos os encargos acumulados pelas contas em sua organização.
- Uma conta de membro é uma conta da AWS, diferente da conta mestre, que faz parte de uma organização. Uma conta de membro pode pertencer a apenas uma organização por vez. A conta mestre tem responsabilidades de uma conta do pagador e é responsável por pagar todas as despesas que são acumuladas pelas contas do membro.
- Uma raiz administrativa é o ponto de partida para organizar suas contas AWS. A raiz administrativa é o contêiner superior na hierarquia de sua organização. Sob essa raiz, você pode criar UOs para agrupar logicamente suas contas e organizar essas UOs em uma

hierarquia que melhor corresponda às suas necessidades de negócios.

- Uma unidade organizacional (OU) é um grupo de contas da AWS dentro de uma organização. Uma UO também pode conter outras UOs, permitindo que você crie uma hierarquia.
- Uma política é um "documento" com uma ou mais declarações que definem os controles que você deseja aplicar a um grupo de contas da AWS.
    - **Política de controle de serviço** (SCP) é uma política que especifica os serviços e ações que os usuários e funções podem usar nas contas afetadas pelo SCP. SCPs são semelhantes às políticas de permissão do IAM, exceto que eles não concedem nenhuma permissão. Em vez disso, os SCPs são filtros que permitem que apenas os serviços e ações especificados sejam usados nas contas afetadas.
- O AWS Organizations tem dois conjuntos de recursos disponíveis:
    - Todas as organizações oferecem suporte ao faturamento consolidado, que fornece ferramentas básicas de gerenciamento que você pode usar para gerenciar de forma centralizada as contas em sua organização.
    - Se você habilitar todos os recursos, continuará a obter todos os recursos de faturamento consolidado, além de um conjunto de recursos avançados, como políticas de controle de serviço.
- Você pode remover uma conta da AWS de uma organização e torná-la uma conta independente.
- Hierarquia da Organização
    - Incluindo contas raiz e AWS criadas nas UOs mais baixas, sua hierarquia pode ter cinco níveis de profundidade.
    - Políticas herdadas por meio de conexões em uma organização.
    - As políticas podem ser atribuídas em diferentes pontos da hierarquia.

Preços

- Este serviço é gratuito.

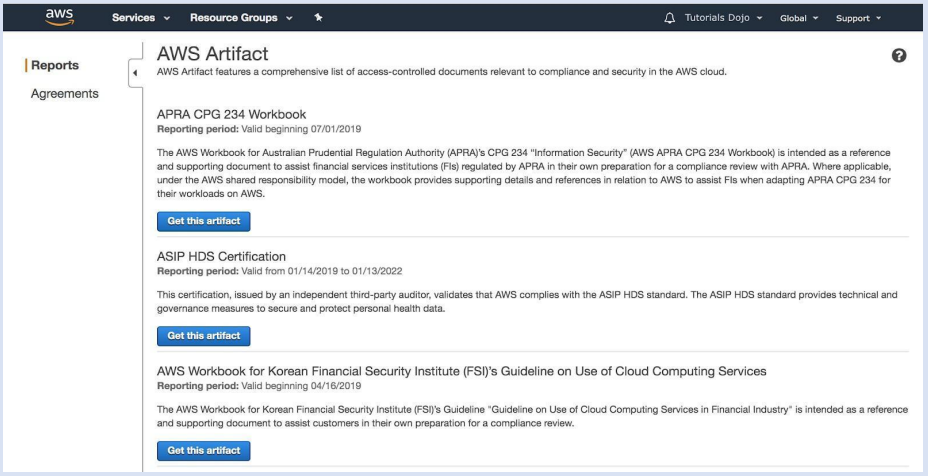
Fontes: https://docs.aws.amazon.com/organizations/latest/userguide/

https://aws.amazon.com/organizations/features/

https://aws.amazon.com/organizations/faqs/

Artefato AWS

- Um repositório central de autoatendimento de relatórios de segurança e conformidade da AWS e contratos selecionados online.
- Um artefato de auditoria é uma evidência que demonstra que uma organização está seguindo um processo documentado ou atendendo a um requisito específico (conformidade de negócios).
- **Relatórios de artefato AWS** inclui o seguinte:
    - ISO,
    - Relatórios de controle da organização de serviços (SOC),
    - Relatórios da indústria de cartões de pagamento (PCI),
    - e certificações que validam a implementação e eficácia operacional dos controles de segurança da AWS.



- **Acordos de artefatos da AWS** incluir
    - o Acordo de Confidencialidade (NDA)
    - o Business Associate Addendum (BAA), que normalmente é exigido para empresas que estão sujeitas à Lei HIPAA para garantir que as informações de saúde protegidas (PHI) sejam devidamente protegidas.
- **Todas as contas da AWS com permissões do AWS Artifact IAM têm acesso ao AWS Artifact**. Usuários root e usuários IAM com permissões de administrador podem baixar todos os artefatos de auditoria disponíveis para suas contas concordando com os termos e condições associados. Você precisará conceder aos usuários do IAM com permissões de não administrador acesso ao artefato AWS.
- Para usar acordos de organização no AWS Artifact, sua organização deve estar habilitada para

todos os recursos.

- Acordos de artefato AWS
    - Os contratos de conta de artefato da AWS se aplicam apenas à conta individual que você usou para fazer login na AWS.
    - Os AWS Artifact Organization Agreements se aplicam a todas as contas em uma organização criada por meio do AWS Organizations, incluindo a conta mestre da organização e todas as contas-membro. Apenas a conta principal em uma organização pode aceitar contratos em AWS Artifact Organization Agreements.
    - Contas mestras e contas-membro de uma organização podem ter acordos de conta de artefato AWS e acordos de organização de artefato AWS do mesmo tipo em vigor ao mesmo tempo.
    - Se você tiver contas em organizações diferentes que deseja que sejam cobertas por um contrato, deverá fazer login na conta principal de cada organização e aceitar os contratos relevantes por meio dos Contratos de organização de artefato da AWS.
    - Rescindir o acordo da organização não termina o acordo da conta.
    - Quando uma conta de membro é removida de uma organização (por exemplo, deixando a organização ou sendo removida da organização pela conta mestre), quaisquer acordos de organização aceitos em seu nome não serão mais aplicados a essa conta de membro.
- Adendo de associado comercial (BAA)
    - Você pode aceitar o AWS BAA para sua conta individual ou, se for uma conta principal em uma organização, pode aceitar o AWS BAA em nome de todas as contas de sua organização.
    - Ao aceitar o AWS BAA nos contratos de artefato da AWS, você designará instantaneamente sua (s) conta (s) da AWS para uso em conexão com informações de saúde protegidas (PHI) e HIPAA.
    - Se você rescindir um BAA online na guia Contratos de conta no AWS Artifact, a conta que você usou para entrar no AWS deixará de ser uma conta HIPAA imediatamente, a menos que também seja coberta por um BAA da organização.
    - Se você for um usuário de uma conta mestre e encerrar um BAA online no artefato AWS, todas as contas em sua organização serão imediatamente removidas como contas HIPAA, a menos que sejam cobertas por BAAs de conta individual.
    - Se você tiver um BAA de conta e um BAA de organização em vigor ao mesmo tempo, os termos do BAA de organização serão aplicados em vez dos termos do BAA de conta.

- Adendo de violação de dados notificáveis da AWS da Austrália (Adendo ANDB)
    - Usando a conta mestre de sua organização, você pode usar a guia de acordos de organização em AWS Artifact Agreements para aceitar um Adendo ANDB em nome de todas as contas de membros existentes e futuras em sua organização.
    - Quando o Adendo ANDB da conta e o Adendo ANDB das organizações forem aceitos, o Adendo ANDB das organizações será aplicado em vez do Adendo ANDB da conta.
    - Se você encerrar uma conta ANDB Addendum na guia Account agreement no AWS Artifact, a conta AWS que você usou para fazer login no AWS Artifact não será coberta por um ANDB Addendum com AWS, a menos que também seja coberta por uma organização ANDB Addendum.
    - Se você for um usuário de uma conta mestre e rescindir um adendo ANDB da organização na guia de acordos da organização no artefato AWS, as contas da AWS nessa organização AWS
- não serão cobertos por um Adendo ANDB com AWS, a menos que sejam cobertos por um Adendo ANDB de conta
    - A maioria dos erros que você recebe do AWS Artifact pode ser resolvida adicionando as permissões de IAM necessárias.

Fontes: https://aws.amazon.com/artifact/

https://docs.aws.amazon.com/artifact/latest/ug/what-is-aws-artifact.html

https://aws.amazon.com/artifact/faq/

MIGRAÇÃO

AWS Snowball Edge

- Um tipo de dispositivo Snowball com armazenamento on-board e poder de computação para recursos selecionados da AWS. Ele pode realizar processamento local e cargas de trabalho de computação de ponta, além de transferir dados entre seu ambiente local e a nuvem AWS.
- Possui armazenamento compatível com S3 integrado e computação para suportar a execução de funções Lambda e EC2 instâncias.

Fontes: https://aws.amazon.com/snowball-edge/features/

https://aws.amazon.com/snowball-edge/pricing/

https://aws.amazon.com/snowball-edge/faqs/

AWS Snowmobile

- Um serviço de transferência de dados em escala de exabyte usado para mover quantidades extremamente grandes de dados para a AWS. Você pode transferir até 100 PB por Snowmobile.
- O Snowmobile será devolvido à sua região AWS designada, onde seus dados serão carregados nos serviços de armazenamento da AWS que você selecionou, como S3 ou Glacier.
- Snowmobile usa várias camadas de segurança para ajudar a proteger seus dados, incluindo pessoal de segurança dedicado:
    - Rastreamento GPS, monitoramento de alarme
    - Vigilância por vídeo 24 horas por dia, 7 dias por semana
    - um veículo opcional de escolta de segurança durante o trânsito
    - Todos os dados são criptografados com chaves de criptografia de 256 bits que você gerencia por meio do AWS Key Management Service e projetado para segurança e cadeia de custódia completa de seus dados.
- O preço do snowmobile é baseado na quantidade de dados armazenados no caminhão por mês.

Fontes: https://aws.amazon.com/snowmobile/faqs/

https://aws.amazon.com/snowmobile/pricing/

GESTÃO

AWS Auto Scaling

- Configure o escalonamento automático para os recursos da AWS rapidamente por meio de um plano de escalonamento que usa escalonamento dinâmico e escalonamento preditivo.
- Otimize para disponibilidade, custo ou equilíbrio de ambos.
- Aumentar significa diminuir o tamanho de um grupo, enquanto expandir significa aumentar o tamanho de um grupo.

- Útil para
    - Tráfego cíclico, como alto uso de recursos durante o horário comercial regular e baixo uso de recursos durante a noite
    - Padrões dentro e fora do tráfego, como processamento em lote, teste ou análise periódica
    - Padrões de tráfego variáveis, como software para campanhas de marketing com períodos de crescimento acentuado
- Características
    - Inicie ou encerre instâncias EC2 em um grupo Auto Scaling.
    - Inicie ou encerre instâncias de uma solicitação EC2 Spot Fleet ou substitua automaticamente as instâncias que são interrompidas por motivos de preço ou capacidade.
    - Ajuste a contagem desejada do serviço ECS para cima ou para baixo em resposta às variações de carga.
    - Habilite uma tabela do DynamoDB ou um índice secundário global para aumentar ou diminuir sua capacidade de leitura e gravação provisionada para lidar com aumentos no tráfego sem limitação.
    - Ajuste dinamicamente o número de réplicas de leitura do Aurora provisionadas para um cluster do Aurora DB para lidar com as alterações nas conexões ativas ou na carga de trabalho.
- Amazon EC2 Auto Scaling
    - Garantir que você tenha o número correto de instâncias EC2 disponíveis para lidar com a carga de seu aplicativo usando grupos de Auto Scaling.
    - Um grupo de Auto Scaling contém uma coleção de instâncias EC2 que compartilham características semelhantes e são tratadas como um agrupamento lógico para fins de escalonamento e gerenciamento de instâncias.
    - Você especifica o número mínimo, máximo e desejado de instâncias em cada grupo do Auto Scaling.
    - Componentes chave

Grupos	Suas instâncias EC2 são organizadas em grupos para que sejam tratadas como uma unidade lógica para dimensionamento e gerenciamento. Ao criar um grupo, você pode especificar seu número mínimo, máximo e desejado de instâncias EC2.

Configurações de lançamento	Seu grupo usa uma configuração de inicialização como modelo para suas instâncias EC2. Ao criar uma configuração de inicialização, você pode especificar informações como AMI ID, tipo de instância, par de chaves, grupos de segurança e mapeamento de dispositivo de bloqueio para suas instâncias.
Opções de escala	Como dimensionar seus grupos de Auto Scaling.

- Você pode adicionar um gancho de ciclo de vida ao seu grupo do Auto Scaling para realizar ações personalizadas quando as instâncias são iniciadas ou encerradas.
- Opções de escala
  - Escale para manter os níveis de instância atuais em todos os momentos
  - Escalonamento Manual
  - Escala com base em uma programação
  - Escala com base em uma demanda
- Dimensionamento Tipos de política
  - **Escala de rastreamento de destino**—Aumente ou diminua a capacidade atual do grupo com base em um valor alvo para uma métrica específica.
  - **Escala de degraus**—Aumente ou diminua a capacidade atual do grupo com base em um conjunto de ajustes de escala, conhecidos como ajustes de etapa, que variam com base no tamanho da violação do alarme.
  - **Escala simples**—Aumente ou diminua a capacidade atual do grupo com base em um único ajuste de escala.
- O Amazon EC2 Auto Scaling marca uma instância como não íntegra se a instância estiver em um estado diferente de execução, o status do sistema for prejudicado ou o Elastic Load Balancing relatar que a instância falhou nas verificações de saúde.
- Rescisão de Instâncias
  - Ao configurar a escala automática, você deve decidir quais instâncias devem ser encerradas primeiro e definir uma política de encerramento. Você também pode usar a proteção de instância para evitar que instâncias específicas sejam encerradas durante o dimensionamento automático.
  - Rescisão Padrão Política
  - Políticas de rescisão personalizadas

- *Instância mais antiga* - Encerre a instância mais antiga do grupo.

- *Newest Instance* - Encerre a instância mais recente do grupo.
- *Oldest Launch Configuration* - Encerrar instâncias que têm o lançamento mais antiga configuração.
- *Closest To Next Instance Hour* - Encerrar instâncias que estão mais próximas da próxima hora de faturamento.
- Uma configuração de inicialização é um modelo de configuração de instância que um grupo do Auto Scaling usa para iniciar instâncias EC2 e você especifica informações para as instâncias.
    - Você pode especificar sua configuração de inicialização com vários grupos de Auto Scaling.
    - Você só pode especificar uma configuração de inicialização para um grupo do Auto Scaling por vez e não pode modificar uma configuração de inicialização depois de criá-la.
- Você pode anexar um ou mais ELBs clássicos aos seus grupos de Auto Scaling existentes. Os ELBs devem estar na mesma região.
- O Auto Scaling reequilibra iniciando novas instâncias EC2 nas AZs que têm menos instâncias primeiro, só então ele começará a encerrar instâncias nas AZs que tinham mais instâncias
- Monitoramento
    - **Verificações de saúde** - identifica todas as instâncias que não são saudáveis
        - Verificações de status do Amazon EC2 (padrão)
        - Verificações de integridade do Elastic Load Balancing
        - Verificações de saúde personalizadas.

Fontes:*https://docs.aws.amazon.com/autoscaling/plans/userguide/what-is-aws-auto-scaling.html*

https://aws.amazon.com/autoscaling/features/

https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html

https://aws.amazon.com/autoscaling/pricing/

https://aws.amazon.com/autoscaling/faqs/

AWS CloudFormation

- Um serviço que oferece aos desenvolvedores e empresas uma maneira fácil de criar uma coleção de recursos relacionados da AWS e fornecê-los de maneira ordenada e previsível.

Características

- O CloudFormation permite que você modele toda a sua infraestrutura em um arquivo de texto denominado modelo. Você pode usar JSON ou YAML para descrever quais recursos da AWS deseja criar e configurar.
- CloudFormation automatiza o provisionamento e atualização de sua infraestrutura de maneira segura e controlada.

CloudFormation vs Elastic Beanstalk

- O Elastic Beanstalk fornece um ambiente para implementar e executar facilmente aplicativos na nuvem.
- CloudFormation é um mecanismo de provisionamento conveniente para uma ampla gama de recursos da AWS.

Conceitos

- **Modelos**
    - Um arquivo de texto formatado em JSON ou YAML.
    - CloudFormation usa esses modelos como projetos para construir seus recursos AWS.
- *Pilhas*
    - Gerenciar recursos relacionados como uma única unidade.
    - Todos os recursos em uma pilha são definidos pelo modelo CloudFormation da pilha.

Preços

- Sem custo adicional para CloudFormation. Você paga pelos recursos da AWS criados usando o CloudFormation da mesma maneira que se os tivesse criado manualmente.

Fontes:https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/

https://aws.amazon.com/cloudformation/features/

https://aws.amazon.com/cloudformation/pricing/

https://aws.amazon.com/cloudformation/faqs/

AWS CloudTrail

- As ações realizadas por um usuário, função ou serviço da AWS no AWS Management Console, AWS Command Line Interface e AWS SDKs e APIs são registradas como eventos.
- O CloudTrail é habilitado em sua conta AWS quando você o cria.
- O CloudTrail se concentra na auditoria da atividade da API.
- Visualize eventos no Histórico de eventos, onde você pode visualizar, pesquisar e baixar os últimos 90 dias de atividade em sua conta da AWS.
- *Trilhas*
    - Crie uma trilha do CloudTrail para arquivar, analisar e responder às mudanças em seus recursos da AWS.
    - Tipos
        - Uma trilha que se aplica a todas as regiões - o CloudTrail registra eventos em cada região e entrega os arquivos de log de eventos do CloudTrail para um bucket S3 que você especificar. Esta é a opção padrão ao criar uma trilha no console do CloudTrail.
        - Uma trilha que se aplica a uma região - o CloudTrail registra os eventos apenas na região que você especificar. Esta é a opção padrão quando você cria uma trilha usando o AWS CLI ou a API CloudTrail.
    - O CloudTrail publica arquivos de log a cada cinco minutos.
- *Eventos*
    - O registro de uma atividade em uma conta AWS. Esta atividade pode ser uma ação realizada por um usuário, função ou serviço monitorável pelo CloudTrail.
    - Tipos
        - Eventos de gestão
            - Registrado por padrão
            - Os eventos de gerenciamento fornecem informações sobre as operações de gerenciamento realizadas nos recursos da sua conta da AWS, também conhecidas como operações de plano de controle.
        - Eventos de dados
            - Não registrado por padrão

- Os eventos de dados fornecem informações sobre as operações de recursos realizadas em ou em um recurso, também conhecidas como operações de plano de dados.
- Os eventos de dados costumam ser atividades de alto volume.

- *Preço*
  - A primeira cópia dos eventos de gerenciamento dentro de cada região é entregue gratuitamente. Cópias adicionais de eventos de gerenciamento são cobradas.
  - Os eventos de dados são registrados e cobrados apenas para as funções Lambda e buckets S3 que você especificar.
  - Uma vez que uma trilha do CloudTrail é configurada, as cobranças do S3 são aplicadas com base no seu uso, já que o CloudTrail entrega logs para um bucket do S3.

Fontes: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/

https://aws.amazon.com/cloudtrail/features/

https://aws.amazon.com/cloudtrail/pricing/

https://aws.amazon.com/cloudtrail/faqs/

Amazon CloudWatch

- Ferramenta de monitoramento para seus recursos e aplicativos da AWS.
- Exiba métricas e crie alarmes que observam as métricas e enviam notificações ou fazem alterações automaticamente nos recursos que você está monitorando quando um limite é violado.
- CloudWatch é basicamente um repositório de métricas. Um serviço AWS, como Amazon EC2, coloca métricas no repositório e você recupera estatísticas com base nessas métricas. Se você colocar suas próprias métricas customizadas no repositório, também poderá recuperar estatísticas sobre essas métricas.
- O CloudWatch não agrega dados entre regiões. Portanto, as métricas são completamente separadas entre as regiões.
- *Conceitos CloudWatch*
  - **Name spaces** - um contêiner para métricas CloudWatch.
    - Não há name space padrão.

        - Os name spaces da AWS usam a seguinte convenção de nomenclatura: AWS / serviço.
    - **Métricas** - representa um conjunto ordenado por tempo de pontos de dados que são publicados no CloudWatch.
        - Existe apenas na região em que são criados.
        - Não podem ser excluídos, mas expiram automaticamente após 15 meses se nenhum dado novo for publicado neles.
        - À medida que novos pontos de dados chegam, os dados anteriores a 15 meses são descartados.
        - Cada ponto de dados métricos deve ser marcado com um carimbo de data / hora. O carimbo de data / hora pode ter até duas semanas no passado e até duas horas no futuro. Se você não fornece um carimbo de data / hora, o CloudWatch cria um carimbo de data / hora para você com base na hora em que o ponto de dados foi recebido.
        - Por padrão, vários serviços fornecem métricas gratuitas para recursos. Você também pode habilitar
- **monitoramento detalhado** ou publique suas próprias métricas de aplicativo.
    - **Dimensões** - um par nome / valor que identifica exclusivamente uma métrica.
        - Você pode atribuir até 10 dimensões a uma métrica.
    - **Estatísticas** - agregações de dados métricos ao longo de períodos de tempo específicos.
        - Cada estatística possui uma unidade de medida. Os pontos de dados métricos que especificam uma unidade de medida são agregados separadamente.

Estatística	Descrição
Mínimo	O menor valor observado durante o período especificado. Você pode usar esse valor para determinar baixos volumes de atividade para seu aplicativo.
Máximo	O maior valor observado durante o período especificado. Você pode usar esse valor para determinar altos volumes de atividade para seu aplicativo.
Soma	Todos os valores enviados para a métrica correspondente somados. Útil para determinar o volume total de uma métrica.
Média	O valor de Sum / SampleCount durante o período especificado. Ao comparar essa estatística com o Mínimo e o Máximo, você pode determinar o escopo total de uma métrica e quão próximo o uso médio está do Mínimo e Máximo. Essa comparação ajuda você a saber quando aumentar ou diminuir seus recursos conforme necessário.

SampleCount	A contagem (número) de pontos de dados usados para o cálculo estatístico.
pNN.NN	O valor do percentil especificado. Você pode especificar qualquer percentil, usando até duas casas decimais (por exemplo, p95.45). As estatísticas de percentil não estão disponíveis para métricas que incluem quaisquer valores negativos.

- **Percentis** - indica a posição relativa de um valor em um conjunto de dados. Os percentis ajudam você a entender melhor a distribuição de seus dados métricos.
- **Alarmes** - observa uma única métrica ao longo de um período de tempo especificado e executa uma ou mais ações especificadas, com base no valor da métrica em relação a um limite ao longo do tempo
    - Quando um alarme está no painel, ele fica vermelho quando está no estado ALARME.
    - Estados de Alarme
        - **OK—**A métrica ou expressão está dentro do limite definido.
        - **ALARME—**A métrica ou expressão está fora do limite definido.
        - **DADOS INSUFICIENTES—**O alarme acabou de iniciar, a métrica não está disponível ou não há dados suficientes disponíveis para a métrica determinar o estado do alarme.
    - Você também pode monitorar suas cobranças estimadas da AWS usando o Amazon CloudWatch Alarms. No entanto, observe que você só pode rastrear as cobranças estimadas da AWS no CloudWatch e não a utilização real de seus recursos. Lembre-se de que você só pode definir metas de cobertura para suas instâncias EC2 reservadas no AWS Budgets ou no Cost Explorer, mas não no CloudWatch.

CloudWatch Dashboard

- Páginas iniciais personalizáveis no console do CloudWatch que você pode usar para monitorar seus recursos em uma única visualização, mesmo aqueles espalhados por diferentes regiões.

- *Eventos CloudWatch*
    - Entregue fluxo quase em tempo real de eventos do sistema que descrevem as mudanças nos recursos da AWS.
    - Os eventos respondem a essas mudanças operacionais e tomam as ações corretivas necessárias, enviando mensagens para responder ao ambiente, ativando funções,

fazendo mudanças e capturando informações de estado.

- Conceitos
  - **Eventos** - indica uma mudança em seu ambiente AWS.
  - **Alvos** - processos eventos.
  - **Regras** - combina eventos de entrada e os encaminha para destinos para processamento.

- *Cloud Watch Logs*
  - Características
    - Monitore registros de instâncias EC2 em tempo real
    - Monitore eventos registrados do CloudTrail
    - Por padrão, os registros são mantidos indefinidamente e nunca expiram
    - Dados de registro de arquivo
    - Log de consultas DNS da rota 53
- *Agente Cloud Watch*
  - Colete mais registros e métricas de nível de sistema de instâncias EC2 e seus servidores locais.
  - Precisa ser instalado.
- *Preços*
  - Você é cobrado pelo número de métricas que possui por mês
  - Você é cobrado por 1000 métricas solicitadas usando chamadas da API CloudWatch
  - Você é cobrado por painel por mês
  - Você é cobrado por métrica de alarme (resolução padrão e alta resolução)
  - Você é cobrado por GB de dados de registro coletados, arquivados e analisados
  - Não há cobrança de Data Transfer IN, apenas Data Transfer out.
  - Você é cobrado por milhão eventos personalizados e por milhão de eventos de contas cruzadas

Fontes: https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring

https://aws.amazon.com/cloudwatch/features/

https://aws.amazon.com/cloudwatch/pricing/

https://aws.amazon.com/cloudwatch/faqs/

AWS OpsWorks

- Um serviço de gerenciamento de configuração que ajuda a configurar e operar aplicativos em uma empresa na nuvem usando Puppet ou Chef.
- O AWS OpsWorks Stacks e o AWS OpsWorks for Chef Automate (1 e 2) permitem que você use livros de receitas e soluções do Chef para gerenciamento de configuração, enquanto o OpsWorks for Puppet Enterprise permite que você configure um servidor mestre Puppet Enterprise no AWS.
- Com o AWS OpsWorks, você pode automatizar como os nós são configurados, implantados e gerenciados, sejam eles instâncias do Amazon EC2 ou dispositivos locais:

OpsWorks para Puppet Enterprise

- Fornece um sistema totalmente gerenciado Puppet master, um conjunto de ferramentas de automação que permite inspecionar, entregar, operar e preparar seus aplicativos para o futuro, além de acessar uma interface de usuário que permite visualizar informações sobre seus nós e atividades do Puppet.
- Não suporta todas as regiões.
- Usa software fantoche-agente.
- *Preços*
    - Você é cobrado com base no número de nós (servidores executando o agente Puppet) conectados ao seu mestre Puppet e no tempo em que esses nós estão sendo executados por hora, e você também paga pela instância EC2 subjacente que executa seu mestre Puppet.
    - ***OpsWorks for Chef Automate***
- Permite criar servidores Chef gerenciados pela AWS que incluem recursos premium do Chef Automate e usar o Chef DK e outras ferramentas do Chef para gerenciá-los.
- O AWS OpsWorks para Chef Automate oferece suporte ao Chef Automate 2.
- Usa chef-cliente.
    - ***Preços***
    - Você é cobrado com base no número de nós conectados ao seu servidor Chef e no tempo em que esses nós estão em execução, e você também paga pela instância EC2 subjacente que executa seu servidor Chef.

Fontes: https://aws.amazon.com/opsworks/chefautomate/features

https://aws.amazon.com/opsworks/chefautomate/pricing

https://aws.amazon.com/opsworks/chefautomate/faqs

https://aws.amazon.com/opsworks/puppetenterprise/feature

https://aws.amazon.com/opsworks/puppetenterprise/pricing

https://aws.amazon.com/opsworks/puppetenterprise/faqs

https://aws.amazon.com/opsworks/stacks/features

https://aws.amazon.com/opsworks/stacks/pricing

https://aws.amazon.com/opsworks/stacks/faqs

AWS Management Console

- *Grupos de Recursos*
    - Uma coleção de recursos da AWS que estão todos na mesma região da AWS e que correspondem aos critérios fornecidos em uma consulta.
    - Os grupos de recursos tornam mais fácil gerenciar e automatizar tarefas em um grande número de recursos de uma só vez.
    - Dois tipos de consultas nas quais você pode criar um grupo:
        - Baseado em tag
        - AWS CloudFormation baseado em pilha
- *Editor de Tag*
    - Tags são palavras ou frases que agem como metadados para identificar e organizar seus recursos da AWS. O limite de tag varia com o recurso, mas a maioria pode ter até 50 tags.
    - Você pode classificar e filtrar os resultados de sua pesquisa de tag para encontrar as tags e os recursos com os quais você precisa trabalhar.

Fontes: https://docs.aws.amazon.com/awsconsolehelpdocs/latest/gsg

https://docs.aws.amazon.com/ARG/latest/userguide/

Consultor confiável da AWS

- O Trusted Advisor analisa seu ambiente AWS e fornece recomendações de melhores práticas em cinco categorias:
    - Otimização de custos
    - Desempenho
    - Segurança
    - Tolerância ao erro
    - Limites de serviço
- O acesso às sete principais verificações do Trusted Advisor está disponível para todos os usuários da AWS.
- O acesso ao conjunto completo de verificações do Trusted Advisor está disponível para planos de suporte empresarial e empresarial.

Fontes: https://aws.amazon.com/premiumsupport/trustedadvisor/

https://aws.amazon.com/premiumsupport/ta-faqs/

https://www.amazonaws.cn/en/support/trustedadvisor/best-practices/

ANALÍTICS

Amazon Kinesis

- Facilita a coleta, processamento e análise de dados de streaming em tempo real.
- O Kinesis pode ingerir dados em tempo real, como vídeo, áudio, logs de aplicativos, fluxos de cliques de sites e dados de telemetria Iot para aprendizado de máquina, análises e outros aplicativos.

Streams de vídeo Kinesis

- Um serviço AWS totalmente gerenciado que você pode usar para transmitir vídeo ao vivo de dispositivos para a nuvem AWS ou criar aplicativos para processamento de vídeo em tempo real ou análise de vídeo orientada em lote.

Benefício

- Você pode se conectar e transmitir de milhões de dispositivos.
- Você pode configurar seu stream de vídeo Kinesis para armazenar dados de mídia de forma durável por períodos de retenção personalizados. O Kinesis Video Streams também gera um índice sobre os dados armazenados com base em carimbos de data / hora gerados pelo produtor ou do lado do serviço.
- O Kinesis Video Streams não tem servidor, portanto, não há infraestrutura para configurar ou gerenciar.
- Você pode construir aplicativos em tempo real e em lote em fluxos de dados.
- O Kinesis Video Streams impõe criptografia baseada em Transport Layer Security (TLS) nos dados streaming de dispositivos e criptografa todos os dados em repouso usando AWS KMS.

Preços

  - Você paga apenas pelo volume de dados que ingere, armazena e consome por meio do serviço.

Fluxo de dados Kinesis

- Um serviço de processamento e ingestão de dados altamente escalável e altamente durável, otimizado para streaming de dados. Você pode configurar centenas de milhares de produtores de dados para colocar dados continuamente em um fluxo de dados Kinesis.

Segurança

- O Kinesis Data Streams pode criptografar dados confidenciais automaticamente conforme um produtor os insere em um stream. O Kinesis Data Streams usa chaves mestras AWS KMS para criptografia.
- Use o IAM para gerenciar os controles de acesso.
- Você pode usar um ponto de extremidade VPC de interface para impedir que o tráfego entre o Amazon VPC e o Kinesis Data Streams saia da rede Amazon.**Preços**
- Cada fragmento é cobrado por hora.
- A unidade de carga útil PUT é cobrada com uma taxa de unidades de carga útil PUT por milhão.
- Quando os consumidores usam fan-out aprimorado, eles incorrem em cobranças horárias por hora de fragmento do consumidor e por GB de dados recuperados.

Você é cobrado por uma taxa adicional em cada hora de fragmento incorrida por seu fluxo de dados, uma vez que você ativa a retenção de dados estendida.

Kinesis Data Firehose

- A maneira mais fácil de carregar dados de streaming em armazenamentos de dados e ferramentas de análise.
- É um serviço totalmente gerenciado que escala automaticamente para corresponder à taxa de transferência de seus dados.
- Ele também pode agrupar, compactar e criptografar os dados antes de carregá-los.
- *Características*
    - Ele pode capturar, transformar e carregar dados de streaming no S3, Redshift, Elasticsearch Service e Splunk, permitindo análises quase em tempo real com as ferramentas de business intelligence existentes e painéis usados atualmente.
    - Você pode especificar um tamanho de lote ou intervalo de lote para controlar a rapidez com que os dados são carregados para os destinos. Além disso, você pode especificar se os dados devem ser compactados.
    - Depois de lançado, seus fluxos de entrega aumentam e diminuem automaticamente para lidar com gigabytes por segundo ou mais de taxa de dados de entrada e mantém a latência de dados nos níveis que você especifica para o fluxo.
    - O Kinesis Data Firehose pode converter o formato dos dados recebidos de JSON para formatos Parquet ou ORC antes de armazenar os dados no S3.

- Você pode configurar o Kinesis Data Firehose para preparar seus dados de streaming antes de carregá-los nos armazenamentos de dados. Kinesis Data Firehose fornece blueprints Lambda pré-construídos para converter fontes de dados comuns, como logs do Apache e logs do sistema para os formatos JSON e CSV. Você pode usar esses projetos pré-construídos sem qualquer alteração, ou personalizá-los ainda mais, ou escrever suas próprias funções personalizadas.

- *Segurança*
  - O Kinesis Data Firehose oferece a opção de criptografar seus dados automaticamente após o upload para o destino.
  - Gerenciar o acesso a recursos com IAM.
- *Preços*
  - Você paga apenas pelo volume de dados que transmitir por meio do serviço. Você é cobrado pelo volume de dados ingeridos no Kinesis Data Firehose e, se aplicável, pela conversão do formato de dados para Apache Parquet ou ORC.
- *Análise de dados Kinesis*
- Analise os dados de streaming, obtenha percepções acionáveis e responda às necessidades do seu negócio e do cliente em tempo real. Você pode construir rapidamente consultas SQL e aplicativos Java usando modelos e operadores integrados para funções de processamento comuns para organizar, transformar, agregar e analisar dados em qualquer escala.
- *Características gerais*
  - O Kinesis Data Analytics não tem servidor e cuida de tudo que é necessário para executar continuamente seu aplicativo.
  - O Kinesis Data Analytics dimensiona elasticamente os aplicativos para acompanhar qualquer volume de dados no fluxo de entrada de dados.
  - Kinesis Data Analytics oferece latências de processamento de subsegundos para que você possa gerar alertas, painéis e insights acionáveis.
- *Preços*
  - Você é cobrado por hora com base no número médio de unidades de processamento Kinesis (ou KPUs) usadas para executar seu aplicativo de processamento de fluxo.

Fontes: https://aws.amazon.com/kinesis/

DESENVOLVEDOR

AWS CodeDeploy

- Um serviço de implantação totalmente gerenciado que automatiza implantações de software para uma variedade de serviços de computação, como Amazon EC2, AWS Fargate, AWS Lambda e seus servidores locais.
    - Vantagens de usar implantações azuis / verdes versus implantações in-loco
        - Um aplicativo pode ser instalado e testado no novo ambiente de substituição e implantado na produção simplesmente redirecionando o tráfego.
        - Se você estiver usando a plataforma de computação EC2 / On-Premises, voltar para a versão mais recente de um aplicativo é mais rápido e confiável. O tráfego pode apenas ser roteado de volta para as instâncias originais, desde que não tenham sido encerradas. Com uma implantação local, as versões devem ser revertidas por meio da reimplantação da versão anterior do aplicativo.
        - Se você estiver usando o EC2 / On-Premises plataforma de computação, novas instâncias são provisionadas e contêm as configurações de servidor mais atualizadas.
        - Se estiver usando a plataforma de computação AWS Lambda, você controla como o tráfego é alterado da versão original da função AWS Lambda para a nova versão da função AWS Lambda.
- Com o AWS CodeDeploy, você também pode implantar seus aplicativos em seus data centers locais.
- Preços
    - Não há cobrança adicional para implantações de código para Amazon EC2 ou AWS Lambda.
    - Você é cobrado por local atualização da instância usando AWS CodeDeploy.

Fontes: https://aws.amazon.com/codedeploy/features/?nc=sn&loc=2

https://docs.aws.amazon.com/codedeploy/latest/userguide/welcome.html

https://aws.amazon.com/codedeploy/faqs/?nc=sn&loc=6

AWS CodePipeline

- Um serviço de entrega contínua totalmente gerenciado que ajuda a automatizar seus pipelines

de liberação para atualizações de aplicativos e infraestrutura.

- Você pode integrar facilmente AWS CodePipeline com serviços de terceiros, como GitHub ou com o seu próprio plugin personalizado.
- Conceitos
    - Um pipeline define o fl uxo de trabalho do processo de lançamento e descreve como uma nova mudança de código progride no processo de lançamento.
    - Um pipeline compreende uma série de estágios (por exemplo, construir, testar e implantar), que atuam como divisões lógicas em seu fl uxo de trabalho. Cada estágio é composto de uma sequência de ações, que são tarefas como a construção de código ou implantação em ambientes de teste.
- Características
    - O AWS CodePipeline pode extrair o código-fonte do seu pipeline diretamente do AWS CodeCommit, GitHub, Amazon ECR ou Amazon S3.
    - Ele pode executar compilações e testes de unidade no AWS CodeBuild.
    - Ele pode implantar suas mudanças usando AWS CodeDeploy, AWS Elastic Beanstalk, Amazon ECS, AWS Fargate, Amazon S3, AWS Service Catalog, AWS CloudFormation e / ou AWS OpsWorks Stacks.
- Limites
    - O número máximo de pipelines por região em uma conta AWS é 300
    - O número de estágios em um pipeline é mínimo de 2, máximo de 10
- Preços
    - Você é cobrado por pipeline ativo a cada mês. Os pipelines recém-criados são gratuitos para uso durante os primeiros 30 dias após a criação.

Fontes: https://aws.amazon.com/codepipeline/features/?nc=sn&loc=2

https://aws.amazon.com/codepipeline/pricing/?nc=sn&loc=3

https://docs.aws.amazon.com/codepipeline/latest/userguide/welcome.htmeu

https://aws.amazon.com/codepipeline/faqs/?nc=sn&loc=5

AWS CodeBuild

- Um serviço de integração contínua totalmente gerenciado que compila o código-fonte, executa testes e produz pacotes de software prontos para implantação.
- Características

- O AWS CodeBuild executa suas compilações em ambientes de compilação pré-configurados que contêm o sistema operacional, o tempo de execução da linguagem de programação e as ferramentas de compilação (como Apache Maven, Gradle, npm) necessários para concluir a tarefa. Você apenas especifica a localização do seu código-fonte e seleciona as configurações para sua construção, como o ambiente de construção a ser usado e os comandos de construção a serem executados durante uma construção.
- O AWS CodeBuild constrói seu código e armazena os artefatos em um bucket do Amazon S3, ou você pode usar um comando build para carregá-los em um repositório de artefatos.
- AWS CodeBuild fornece ambientes de construção para
    - Java
    - Python
    - Node.js
    - Rubi
    - Go
    - Android
    - .NET Core para Linux
    - Docker
- Você pode definir os comandos específicos que deseja que o AWS CodeBuild execute, como instalar pacotes de ferramentas de construção, executar testes de unidade e empacotar seu código.
- Você pode integrar CodeBuild em fluxos de trabalho CI / CD existentes usando suas integrações de origem, comandos de construção ou integração Jenkins.
- CodeBuild pode se conectar a AWS CodeCommit, S3, GitHub e GitHub Enterprise e Bitbucket para extrair o código-fonte para compilações.
    - CodeBuild permite que você use imagens Docker armazenadas em outra conta da AWS como seu ambiente de construção, concedendo permissões de nível de recurso.
    - Agora, ele permite que você acesse imagens Docker de qualquer registro privado como o ambiente de construção. Anteriormente, você só podia usar imagens Docker de DockerHub público ou Amazon ECR no CodeBuild.

- Preços
    - Você é cobrado pelos recursos de computação com base na duração da execução da sua compilação. A taxa por minuto depende do tipo de

computação que você usa.

Fontes: https://aws.amazon.com/codebuild/features/?nc=sn&loc=2

https://aws.amazon.com/codebuild/pricing/?nc=sn&loc=3

https://aws.amazon.com/codebuild/faqs/?nc=sn&loc=5

https://docs.aws.amazon.com/codebuild/latest/userguide/getting-started.htmeu

AWS Code Commit

- Um serviço de controle de origem totalmente gerenciado que hospeda repositórios baseados em Git seguros, semelhantes ao Github.
- Você pode criar seu próprio repositório de código e usar comandos Git para interagir com seu próprio repositório e outros repositórios.
- Você pode armazenar e criar versão de qualquer tipo de arquivo, incluindo ativos de aplicativo, como imagens e bibliotecas, junto com seu código.
- O AWS CodeCommit Console permite que você visualize seu código, solicitações de pull, commits, branches, tags e outras configurações.
- Alta disponibilidade
    - CodeCommit armazena seus repositórios no Amazon S3 e Amazon DynamoDB.

- Monitoramento
    - CodeCommit usa AWS IAM para controlar e monitorar quem pode acessar seus dados, bem como, quando e onde podem acessá-los.
    - CodeCommit ajuda a monitorar seus repositórios por meio do AWS CloudTrail e AWS CloudWatch.
    - Você pode usar o Amazon SNS para receber notificações de eventos que afetam seus repositórios. Cada notificação incluirá uma mensagem de status, bem como um link para os recursos cujo evento gerou essa notificação.
- Preços
    - Os primeiros 5 usuários ativos por mês são gratuitos. Você também pode ter repositórios ilimitados, com valor total de armazenamento de 50 GB por mês e 10.000 solicitações Git / mês sem custo.

- Você é cobrado por cada usuário ativo além dos primeiros 5 por mês. Você também obtém um adicional de 10 GB por mês de armazenamento por usuário ativo e 2.000 solicitações Git adicionais por usuário ativo.

Fontes: https://aws.amazon.com/codecommit/

https://docs.aws.amazon.com/codecommit/latest/userguide/welcome.html

https://aws.amazon.com/codecommit/faqs/

AWS X-Ray

- O AWS X-Ray analisa e depura a produção, aplicativos distribuídos, como aqueles criados com uma arquitetura de micros serviços. Com o X-Ray, você pode identificar gargalos de desempenho, erros de casos extremos e outros problemas difíceis de detectar.
- O AWS X-Ray fornece uma visão de ponta a ponta, serviço cruzado e centrada no aplicativo das solicitações que fluem através seu aplicativo agregando os dados coletados de serviços individuais em seu aplicativo em uma única unidade chamada rastreamento.
- Você paga com base no número de rastreamentos registrados, recuperados e digitalizados. Um rastreamento representa uma solicitação para seu aplicativo e pode incluir vários pontos de dados, como para chamadas para outros serviços e acesso ao banco de dados.

Fontes: https://aws.amazon.com/xray/features/

https://aws.amazon.com/xray/pricing/

https://docs.aws.amazon.com/xray/latest/devguide/aws-xray.html

https://aws.amazon.com/xray/faqs/

AWS BILLING AND COST MANAGEMENT

- **Explorador de custos** rastreia e analisa seu uso de AWS. É gratuito para todas as contas.
- Use orçamentos para gerenciar orçamentos para sua conta.
- Use Bills para ver detalhes sobre suas cobranças atuais.
- Use o Histórico de pagamentos para ver suas transações de pagamento anteriores.

- O AWS Billing and Cost Management fecha o período de faturamento à meia-noite do último dia de cada mês e, em seguida, calcula sua fatura.
- No final de um ciclo de faturamento ou no momento em que você decidir incorrer em uma taxa única, a AWS cobra o cartão de crédito que você tem no arquivo e emite sua fatura como um arquivo PDF para download.
- Com o CloudWatch, você pode criar alertas de cobrança que o notificam quando o uso de seus serviços excede os limites que você define.
- Use tags de alocação de custos para rastrear seus custos da AWS em um nível detalhado. A AWS fornece dois tipos de tags de alocação de custos, tags geradas pela AWS e tags definidas pelo usuário.

AWS Free Tier

- Ao criar uma conta da AWS, você se inscreve automaticamente para o nível gratuito por 12 meses.
- Você pode usar vários serviços da AWS gratuitamente, contanto que não tenha ultrapassado o limite de uso alocado.
- Para ajudá-lo a permanecer dentro dos limites, você pode rastrear seu uso de nível gratuito e definir um alarme de cobrança com AWS Budgets para notificá-lo se você começar a incorrer em cobranças.

o Relatórios de custo e uso da AWS

- O relatório de custo e uso da AWS fornece informações sobre o uso de recursos da AWS e os custos estimados para esse uso.
- O relatório de custo e uso da AWS é um arquivo .csv ou uma coleção de arquivos .csv que é armazenado em um bucket do S3. Qualquer pessoa que tenha permissão para acessar o bucket S3 especificado pode ver seus arquivos de relatório de cobrança.
- Você pode usar o relatório de custo e uso para rastrear a utilização da instância reservada, encargos e alocações.
- O relatório pode ser carregado automaticamente no AWS Redshift e / ou AWS QuickSight para análise.

AWS Cost Explorer

- O Cost Explorer inclui um relatório padrão que ajuda a visualizar os custos e o uso associados aos seus serviços AWS de acúmulo de custos TOP FIVE e fornece uma análise detalhada de

todos os serviços na exibição de tabela.

- Você pode visualizar os dados dos últimos 13 meses, prever quanto provavelmente gastará nos próximos três meses e obter recomendações de quais Instâncias reservadas comprar.
- O Cost Explorer deve ser habilitado antes de ser usado. Você só pode habilitá-lo se for o proprietário da conta da AWS e se conectar à conta com suas credenciais de root.
- Se você for o proprietário de uma conta mestre em uma organização, habilitar o Cost Explorer habilita o Cost Explorer para todas as contas da organização. Você não pode conceder ou negar acesso individualmente.
- Você pode criar previsões que prevejam o uso da AWS e definir um intervalo de tempo para a previsão.
- Outros relatórios padrão disponíveis são:
    - O relatório mensal de custo e uso do EC2 permite que você visualize todos os seus custos da AWS nos últimos dois meses, bem como seus custos atuais do mês até a data atual.
    - O relatório Custos mensais por conta vinculada permite que você visualize a distribuição dos custos em sua organização.
    - O relatório Mensal de custos de funcionamento oferece uma visão geral de todos os seus custos de funcionamento nos últimos três meses e fornece números previstos para o mês seguinte com um intervalo de confiança correspondente.

Orçamentos AWS

- Defina orçamentos personalizados que alertam quando seus custos ou uso excedem ou estão previstos para exceder o valor orçado.
- Com orçamentos, você pode ver as seguintes informações:
    - Quão próximo o seu plano está do valor orçado ou dos limites do nível gratuito
    - Seu uso até o momento, incluindo o quanto você usou de suas instâncias reservadas
    - Suas cobranças estimadas atuais da AWS e quanto seu uso previsto incorrerá em cobranças até o final do mês
    - Quanto do seu orçamento foi usado
- As informações de orçamento são atualizadas até três vezes por dia.
- Tipos de orçamentos:
    - **Orçamentos de custo** - Planeje quanto você deseja gastar em um serviço.

- **Orçamentos de uso** - Planeje quanto você deseja usar um ou mais serviços.
- **Orçamentos de utilização de RI** - Defina um limite de utilização e receba alertas quando o uso de RI cair abaixo desse limite.
- **Orçamentos de cobertura de RI** - Defina um limite de cobertura e receba alertas quando o número de horas da sua instância coberta por RIs cair abaixo desse limite.

- Os orçamentos podem ser rastreados em nível mensal, trimestral ou anual, e você pode personalizar as datas de início e término.
- Alertas de orçamento podem ser enviados por e-mail e / ou tópico do Amazon SNS.
- Os dois primeiros orçamentos criados são gratuitos.

Fontes:

https://aws.amazon.com/aws-cost-management/aws-budgets/

https://aws.amazon.com/aws-cost-management/aws-cost-explorer/

https://aws.amazon.com/aws-cost-management/aws-cost-and-usage-reporting/

https://aws.amazon.com/aws-cost-management/faqs/

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2

APLICATIVO

Amazon SQS

- Uma fila hospedada que permite integrar e desacoplar sistemas e componentes de software distribuídos.
- SQS suporta filas padrão e FIFO.
- SQS usa baseado em pull (polling), não baseado em push
- *Benefícios*
  - Você controla quem pode enviar e receber mensagens de uma fila SQS.
  - Suporta criptografia do lado do servidor.
  - O SQS armazena mensagens em vários servidores para durabilidade.
  - SQS usa infraestrutura redundante para fornecer acesso altamente simultâneo a mensagens e alta disponibilidade para produzir e consumir mensagens.
  - O SQS pode ser dimensionado para processar cada solicitação em buffer e lidar com

qualquer aumento ou aumento de carga de forma independente.

- O SQS bloqueia suas mensagens durante o processamento, para que vários produtores possam enviar e vários consumidores possam receber mensagens ao mesmo tempo.

- *Tipos de filas*
- **Monitoramento, registro e automação**
  - Monitore filas SQS usando CloudWatch
  - Registrar chamadas de API SQS usando AWS CloudTrail
  - Automatize notificações de serviços AWS para SQS usando eventos CloudWatch
- *Segurança*
  - Use IAM para autenticação do usuário.
  - O SQS tem seu próprio sistema de permissões baseado em recursos que usa políticas escritas na mesma linguagem usada para políticas IAM.
  - Proteja os dados usando criptografia do lado do servidor e AWS KMS.
- *Preços*
  - Você é cobrado por 1 milhão de solicitações SQS. O preço depende do tipo de fila que está sendo usada. Os pedidos incluem:
    - Ações API
    - Pedidos FIFO
    - Uma única solicitação de 1 a 10 mensagens, até uma carga útil total máxima de 256 KB
    - Cada pedaço de 64 KB de uma carga útil é cobrado como 1 solicitação
    - Interação com Amazon S3
    - Interação com AWS KMS
  - Transferência de dados de SQS por TB / mês após consumir 1 GB naquele mês

Fontes: https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide

https://aws.amazon.com/sqs/features/

https://aws.amazon.com/sqs/pricing/

https://aws.amazon.com/sqs/faqs/

Amazon SNS

- Um serviço da web que facilita a configuração, operação e envio de notificações da nuvem. O SNS segue o paradigma de mensagens "publicar-assinar" (pub-sub), com as notificações sendo entregues aos clientes usando um mecanismo "push" em vez de verificar ou "pesquisar" periodicamente por novas informações e atualizações.

    - ***Características***

- SNS é um hub de computação orientado a eventos que possui integração nativa com uma ampla variedade de fontes de eventos AWS (incluindo EC2, S3 e RDS) e destinos de eventos AWS (incluindo SQS e Lambda).

    - **Computação orientada a eventos** é um modelo no qual os serviços do assinante executam trabalho automaticamente em resposta a eventos acionados pelos serviços do editor. Ele pode automatizar os fl uxos de trabalho enquanto desassocia os serviços que trabalham coletiva e independentemente para cumprir esses fl uxos de trabalho.

- **Filtro de mensagens** permite que um assinante crie uma política de filtro, de modo que ele só receba as notificações nas quais está interessado.

- **Fanout de mensagens** ocorre quando uma mensagem é enviada a um tópico e, em seguida, replicada e enviada para vários terminais. Fanout fornece notificações de eventos assíncronos, que por sua vez permitem o processamento paralelo.

- **Noti fi cações móveis SNS** permite que você distribua notificações push móveis para dispositivos baseados em iOS, Android, Fire OS, Windows e Baidu. Você também pode usar o SNS para distribuir mensagens de texto (SMS) para mais de 200 países e distribuir mensagens de e-mail (SMTP).

- **Alertas de aplicativo e sistema** são notificações, disparadas por limites pré-definidos, enviadas para usuários específicos por SMS e / ou e-mail.

- **Push email** e mensagens de texto são duas maneiras de transmitir mensagens a indivíduos ou grupos via e-mail e / ou SMS.

- O SNS fornece armazenamento durável de todas as mensagens que recebe. Quando o SNS recebe sua solicitação de Publicação, ele armazena várias cópias de sua mensagem no disco. Antes de o SNS confirmar que recebeu sua solicitação, ele armazena a mensagem em várias zonas de disponibilidade dentro da região escolhida da AWS.

- SNS permite definir um valor TTL (Time to Live) para cada mensagem. Quando o TTL expira para uma determinada mensagem que não foi entregue e lida por um usuário final, a mensagem é excluída.

- SNS fornece APIs simples e fácil integração com aplicativos.

Editores e assinantes

- Os editores se comunicam de forma assíncrona com os assinantes, produzindo e enviando uma mensagem a um tópico, que é um ponto de acesso lógico e canal de comunicação.
- Os assinantes consomem ou recebem a mensagem ou notificação por meio de um dos protocolos suportados quando assinam o tópico.
- Os editores criam tópicos para enviar mensagens, enquanto os assinantes se inscrevem em tópicos para receber mensagens.

Tópicos SNS

- Em vez de incluir um endereço de destino específico em cada mensagem, um editor envia uma mensagem para um tópico. SNS corresponde o tópico a uma lista de assinantes que se inscreveram nesse tópico e entrega a mensagem a cada um desses assinantes.
- Cada tópico tem um nome exclusivo que identifica o ponto de extremidade SNS para os editores postarem mensagens e assinantes para se registrar para receber notificações.
- Um tópico pode oferecer suporte a assinaturas e entregas de notificação em vários transportes.
    - O serviço SNS tentará entregar mensagens do editor na ordem em que foram publicadas no tópico, portanto, não há garantia.

o Monitoramento

- Monitorando tópicos de SNS usando CloudWatch
- Registro de chamadas SNS API usando CloudTrail

Segurança

- SNS fornece tópicos criptografados para proteger suas mensagens de acesso não autorizado e anônimo. A criptografia ocorre no lado do servidor.
- Usando políticas de controle de acesso, você tem controle detalhado sobre quais terminais um tópico permite, quem pode publicar em um tópico e sob quais condições.

Preços

- Você paga com base no número de notificações que publica, no número de notificações que entrega e em quaisquer chamadas de API adicionais para gerenciamento de tópicos e assinaturas. O preço de entrega varia de acordo com o tipo de terminal.

Fontes: https://docs.aws.amazon.com/sns/latest/dg

https://aws.amazon.com/sns/features/

https://aws.amazon.com/sns/pricing/

https://aws.amazon.com/sns/faqs/

Funções de etapa da AWS

- O AWS Step Functions é um serviço da web que fornece orquestração sem servidor para aplicativos modernos. Ele permite que você coordene os componentes de aplicativos e micros serviços distribuídos usando fluxos de trabalho visuais.

  Características

  - Usando Step Functions, você define seus fluxos de trabalho como máquinas de estado, que transformam códigos complexos em instruções e diagramas fáceis de entender.
  - Step Functions fornece etapas prontas para seu fluxo de trabalho, chamadas de estados, que implementam primitivas de serviço básicas para você, o que significa que você pode remover essa lógica de seu aplicativo. Os estados são capazes de:
    - passar dados para outros estados e micros serviços,
    - lidar com exceções,
    - adicionar tempos limite,
    - tomar decisões,
    - execute vários caminhos em paralelo,
    - e mais.
  - Usando as tarefas de serviço do Step Functions, você pode configurar seu fl uxo de trabalho do Step Functions para chamar outros serviços da AWS.
  - O Step Functions pode coordenar qualquer aplicativo que possa fazer uma conexão HTTPS, independentemente de onde esteja hospedado - instâncias do Amazon EC2, dispositivos móveis ou servidores locais.
  - O AWS Step Functions coordena suas funções e microsserviços Lambda existentes e permite que você os modifique em novas composições. As tarefas em seu fl uxo de trabalho podem ser executadas em qualquer lugar, incluindo em instâncias, contêineres, funções e dispositivos móveis.
  - Aninhar seus fluxos de trabalho de funções de etapa permite que você crie fluxos de trabalho maiores e mais complexos a partir de fluxos de trabalho menores e mais simples.
  - Step Functions mantém a lógica de seu aplicativo estritamente separada da implementação de seu aplicativo. Você pode adicionar, mover, trocar e reordenar etapas sem ter que fazer alterações em sua lógica de negócios.

- Step Functions mantém o estado de seu aplicativo durante a execução, incluindo rastrear em qual etapa da execução ele está e armazenar dados que estão se movendo entre as etapas de seu fluxo de trabalho. Você não terá que gerenciar o estado por conta própria com armazenamentos de dados ou criando um gerenciamento de estado complexo em todas as suas tarefas.
- O Step Functions lida automaticamente com erros e exceções com tentativa / captura e nova tentativa incorporadas, independentemente de a tarefa levar segundos ou meses para ser concluída. Você pode repetir automaticamente tarefas com falha ou tempo limite esgotado, responder de forma diferente a diferentes tipos de erros e se recuperar normalmente voltando ao código de limpeza e recuperação designado.
- O Step Functions tem tolerância a falhas incorporada e mantém a capacidade de serviço em várias Zonas de disponibilidade em cada região, garantindo alta disponibilidade para o serviço em si e para o fluxo de trabalho do aplicativo que opera.
- O Step Functions dimensiona automaticamente as operações e a computação subjacente para executar as etapas do seu aplicativo para você em resposta às mudanças nas cargas de trabalho.
- O AWS Step Functions tem um SLA de 99,9%.
- Ele também oferece suporte a padrões de retorno de chamada. Os padrões de retorno de chamada automatizam os fluxos de trabalho para aplicativos com atividades humanas e integrações personalizadas com serviços de terceiros.
- O AWS Step Functions oferece suporte a eventos de execução de fluxo de trabalho, o que torna mais rápido e fácil construir e monitorar fluxos de trabalho orientados a eventos e sem servidor.

- Preços
  - Step Functions conta uma transição de estado cada vez que uma etapa do seu fl uxo de trabalho é executada. Você é cobrado pelo número total de transições de estado em todas as suas máquinas de estado, incluindo novas tentativas.
- Casos de uso comuns
  - Step Functions pode ajudar a garantir que vários trabalhos ETL de longa duração sejam executados em ordem e concluídos com êxito, em vez de orquestrar manualmente esses trabalhos ou manter um aplicativo separado.
  - Usando Step Functions para lidar com algumas tarefas em sua base de código, você pode abordar a transformação de aplicativos monolíticos em micros serviços como uma série de pequenas etapas.
  - Você pode usar Step Functions para automatizar facilmente tarefas recorrentes,

como gerenciamento de patch, seleção de infraestrutura e sincronização de dados, e Step Functions será dimensionado automaticamente, responderá a tempos limite e repetirá tarefas com falha.

- Use Step Functions para combinar várias funções do AWS Lambda em aplicativos e micros serviços responsivos sem servidor, sem ter que escrever código para lógica de fluxo de trabalho, processos paralelos, tratamento de erros, tempos limite ou novas tentativas.
- Você também pode orquestrar dados e serviços executados em instâncias, contêineres ou servidores locais do Amazon EC2.

Fontes: https://aws.amazon.com/step-functions/features/

https://aws.amazon.com/step-functions/pricing/

https://docs.aws.amazon.com/step-functions/latest/dg/welcome.html

https://aws.amazon.com/step-functions/faqs/

COMPARAÇÃO DE SERVIÇOS AWS

Amazon S3 vs Glacier

- O Amazon S3 é um serviço de armazenamento durável, seguro, simples e rápido, enquanto o Amazon S3 Glacier é usado para soluções de arquivamento.
- Use o S3 se precisar de baixa latência ou acesso frequente aos seus dados. Use o S3 Glacier para baixo custo de armazenamento e você não precisa de milissegundos de acesso aos seus dados.
- Você tem três opções de recuperação quando se trata de Glacier, cada uma variando no custo e na velocidade de recuperação de um objeto para você. Você recupera dados em milissegundos do S3.
- Tanto o S3 quanto o Glacier foram projetados para durabilidade de 99,999999999% dos objetos em várias zonas de disponibilidade.
- O S3 foi projetado para disponibilidade de 99,99%, enquanto o Glacier não tem porcentagem fornecida pela AWS.
- O S3 pode ser usado para hospedar conteúdo estático da web, enquanto o Glacier não.
- No S3, os usuários criam depósitos. No Glacier, os usuários criam arquivos e cofres.
- Você pode armazenar uma quantidade virtualmente ilimitada de dados no S3 e no Glacier.
- Um único arquivo Glacier pode conter 40 TB de dados.
- S3 suporta controle de versão.
- Você pode executar análises e consultas no S3.
- Você pode configurar uma política de ciclo de vida para seus objetos S3 para transferi-los automaticamente para o Glacier. Você também pode fazer upload de objetos diretamente para S3 ou Glacier.
- S3 Standard-IA e One Zone-IA têm um mínimo carga de capacidade por objeto de 128 KB. O mínimo da geleira é 40 KB.
- Os objetos armazenados no S3 têm uma duração mínima de armazenamento de 30 dias (exceto para o S3 Standard). Os objetos arquivados no Glacier têm um mínimo de 90 dias de armazenamento. Objetos que são excluídos, substituídos ou transferidos para uma classe de armazenamento diferente antes da duração mínima incorrerão na cobrança de uso normal mais uma cobrança de solicitação proporcional para o restante da duração mínima de armazenamento.
- O Glacier tem uma taxa de recuperação por GB.
- Você pode fazer a transição de objetos de algumas classes de armazenamento S3 para outra. Os objetos Glacier não podem ser transferidos para nenhuma classe de armazenamento S3.

- S3 (padrão, padrão-IA, e uma zona-IA) é apoiada por um SLA.
    - *Notas Adicionais:*
- Os dados armazenados na classe de armazenamento S3 One Zone-IA serão perdidos no caso de destruição de AZ.
- O S3 Standard-IA custa menos do que o S3 Standard em termos de preço de armazenamento, embora ainda forneça a mesma alta durabilidade, taxa de transferência e baixa latência do S3 Standard.
- S3 One Zone-IA tem 20% a menos custo do que o Standard-IA.
- S3 Reduced Redundancy Storage (RRS) será descontinuado em breve.
- Recomenda-se usar o upload de várias partes para objetos maiores que 100 MB.

RDS vs DynamoDB

Notas Adicionais:

- O DynamoDB possui suporte integrado para transações ACID.
- O DynamoDB usa expressões de filtro porque não oferece suporte a consultas complexas.
- As implantações Multi-AZ para os mecanismos MySQL, MariaDB, Oracle e PostgreSQL utilizam síncronos replicação física. As implantações Multi-AZ para o mecanismo do SQL Server usam replicação lógica síncrona.
- Um banco de dados Oracle é limitado a um banco de dados por instância. Um SQL Server é limitado a 30 bancos de dados por instância. Outros motores RDS não têm limites.

CloudTrail vs CloudWatch

- CloudWatch é um serviço de monitoramento para recursos e aplicativos da AWS. CloudTrail é um serviço da web que registra a atividade da API em sua conta AWS. Ambos são ferramentas de monitoramento úteis na AWS.
- Por padrão, o CloudWatch oferece monitoramento básico gratuito para seus recursos, como instâncias EC2, volumes EBS e instâncias RDS DB. O CloudTrail também é habilitado por padrão quando você cria sua conta AWS.
- Com o CloudWatch, você pode coletar e rastrear métricas, coletar e monitorar arquivos de registro e definir alarmes. O CloudTrail, por outro lado, registra informações sobre quem fez uma solicitação, os serviços usados, as ações realizadas, os parâmetros das ações e os elementos de resposta retornados pelo serviço AWS. CloudTrail Logs são então armazenados em um bucket S3 ou um grupo de log CloudWatch Logs que você especificar.

- Você pode habilitar o monitoramento detalhado de seus recursos da AWS para enviar dados de métrica para o CloudWatch com mais frequência, com um custo adicional.
- O CloudTrail oferece uma cópia gratuita dos logs de eventos de gerenciamento para cada região da AWS. Os eventos de gerenciamento incluem operações de gerenciamento realizadas em recursos em sua conta da AWS, como quando um usuário efetua login em sua conta. Os eventos de dados de registro são cobrados. Os eventos de dados incluem operações de recursos realizadas no ou dentro do próprio recurso, como atividade de API de nível de objeto S3 ou atividade de execução de função Lambda.
- CloudTrail ajuda você a garantir conformidade e padrões regulatórios.
- O CloudWatch Logs relata os logs do aplicativo, enquanto o CloudTrail Logs fornece informações específicas sobre o que ocorreu em sua conta AWS.
- O CloudWatch Events é um fluxo quase em tempo real de eventos do sistema que descreve mudanças em seus recursos da AWS. O CloudTrail se concentra mais nas chamadas de API da AWS feitas em sua conta da AWS.
- Normalmente, o CloudTrail entrega um evento em até 15 minutos após a chamada da API. O CloudWatch fornece dados métricos em períodos de 5 minutos para monitoramento básico e períodos de 1 minuto para monitoramento detalhado. O CloudWatch Logs Agent enviará dados de log a cada cinco segundos por padrão.

Grupo de Segurança vs NACL

Seu VPC tem um grupo de segurança padrão com as seguintes regras:

1. Permite o tráfego de entrada de instâncias atribuídas ao mesmo grupo de segurança.
2. Permitir todo o tráfego de saída IPv4 e IPv6 se você tiver alocado um bloco CIDR IPv6.

Seu VPC tem uma ACL de rede padrão com as seguintes regras:

1. Permite todo o tráfego IPv4 de entrada e saída e, se aplicável, tráfego IPv6.
2. Cada rede ACL também inclui uma regra não modificável e não removível cujo número de regra é um asterisco. Essa regra garante que, se um pacote não corresponder a nenhuma das outras regras numeradas, ele será negado

EBS-SSD vs HDD

Em uma determinada configuração de volume, certas características de E / S conduzem o comportamento de desempenho de seus volumes EBS. Volumes com suporte de SSD, como General

Purpose SSD (gp2) e Provisioned IOPS SSD (io1), oferecem desempenho consistente, seja uma operação de E / S aleatória ou sequencial. Os volumes apoiados por HDD, como HDD otimizado de rendimento (st1) e HDD frio (sc1), oferecem desempenho ideal apenas quando as operações de E / S são grandes e sequenciais.

No exame, sempre considere a diferença entre SSD e HDD conforme mostrado na tabela abaixo. Isso permitirá que você elimine facilmente tipos específicos de EBS nas opções que não são SSD ou não HDD, dependendo se a pergunta pede um tipo de armazenamento que tenha pequenas operações de E / S aleatórias ou grandes operações de E / S sequenciais.

Os volumes IOPS SSD (io1) provisionados são projetados para atender às necessidades de cargas de trabalho com E / S intensa, especialmente cargas de trabalho de banco de dados, que são sensíveis ao desempenho e consistência do armazenamento. Ao contrário do gp2, que usa um modelo de intervalo e crédito para calcular o desempenho, um volume IO1 permite que você especifique uma taxa de IOPS consistente ao criar o volume, e o Amazon EBS fornece até 10 por cento do desempenho de IOPS provisionado

99,9 por cento do tempo em um determinado ano.

	Solid-State Drives (SSD)		Hard Disk Drives (HDD)	
Volume Type	General Purpose SSD (gp2)*	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads	Low-cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads
Use Cases	• Recommended for most workloads • System boot volumes • Virtual desktops • Low-latency interactive apps • Development and test environments	• Critical business applications that require sustained IOPS performance, or more than 16,000 IOPS or 250 MiB/s of throughput per volume • Large database workloads, such as: ◦ MongoDB ◦ Cassandra ◦ Microsoft SQL Server ◦ MySQL ◦ PostgreSQL ◦ Oracle	• Streaming workloads requiring consistent, fast throughput at a low price • Big data • Data warehouses • Log processing • Cannot be a boot volume	• Throughput-oriented storage for large volumes of data that is infrequently accessed • Scenarios where the lowest storage cost is important • Cannot be a boot volume
API Name	gp2	io1	st1	sc1
Volume Size	1 GiB - 16 TiB	4 GiB - 16 TiB	500 GiB - 16 TiB	500 GiB - 16 TiB
Max. IOPS/Volume**	16,000***	64,000****	500	250
Max. Throughput/Volume	250 MiB/s***	1,000 MiB/s†	500 MiB/s	250 MiB/s
Max. IOPS/Instance††	80,000	80,000	80,000	80,000
Max. Throughput/Instance††	1,750 MiB/s	1,750 MiB/s	1,750 MiB/s	1,750 MiB/s
Dominant Performance Attribute	IOPS	IOPS	MiB/s	MiB/s

Balanceador de carga de aplicativo vs balanceador de carga de rede vs balanceador de carga clássico

CARACTERÍSTICAS ÚNICAS

Balanceador de carga de aplicativo

- Você pode definir as funções do Lambda como alvos de balanceamento de carga
- Apenas ALB oferece suporte ao seguinte método de roteamento baseado em conteúdo:
    - Roteamento baseado em caminho
    - Roteamento baseado em host

  - Roteamento baseado em cabeçalho HTTP
  - Roteamento baseado em método HTTP
  - Roteamento baseado em parâmetro de string de consulta
  - Roteamento baseado em CIDR do endereço IP de origem
- Suporta nativamente HTTP / 2 IPv6
- Suporte para vários certificados SSL no ALB usando
- Indicação do nome do servidor (SNI)
- Permite políticas de permissão IAM baseadas em tag
- Pode ser configurado para início lento (aumentar linearmente o número de solicitações enviadas para o destino)
- Suporta balanceamento de carga round-robin
- Você pode desligar a funcionalidade de autenticação de seus aplicativos para ALB
- Pode redirecionar uma solicitação de entrada de um URL para outro, INCLUINDO HTTP para HTTPS
- Você pode definir respostas HTTP ou personalizadas para solicitações de entrada para o ALB, desativando esta tarefa de seu aplicativo
- *Balanceador de carga de rede*
- ELB de alta capacidade / baixa latência
- Pode ser atribuído a um endereço IP estático
- Pode ser atribuído um endereço IP elástico
- Preserva o endereço IP de origem de aplicativos não HTTP em instâncias EC2
- Oferece ouvintes multiprotocolo, permitindo que você execute aplicativos como DNS que dependem dos protocolos TCP e UDP na mesma porta atrás de um balanceador de carga de rede.
- Rescisão TLS
- *Balanceador de carga clássico*
- Você pode criar políticas de segurança personalizadas detalhando quais cifras e protocolos são suportados pelo ELB
- Suporta IPv4 e IPv6 para rede EC2-classic Recursos comuns entre os três balanceadores de carga
- Possui recursos de verificação de integridade da instância
- Possui monitoramento CloudWatch integrado

- Recursos de registro
- Suporte a failover zonal
- Suporte à conexão drenando quando cancelar o registro de alvos / instâncias
- Suporta balanceamento de carga de zona cruzada (distribui uniformemente o tráfego entre as instâncias registradas em habilitado AZs)
- Suporta o ffl oading / rescisão SSL
- Criptografia do servidor de back-end
- Políticas de permissão IAM baseadas em recursos

CONSIDERAÇÕES FINAIS

Quer você seja um estudante querendo aprender mais sobre a nuvem, ou um recém-formado tentando entrar na indústria, ou até mesmo um profissional experiente explorando um novo campo, a nuvem é absolutamente um espaço divertido e empolgante para se estar. Há tantas coisas que você pode fazer hoje que não eram viáveis antes com uma configuração de infraestrutura local.

Tudo que você precisa é de um navegador e conectividade com a Internet e você terá todo o ambiente ao seu alcance. E com o passar dos dias, mais e mais pessoas desejam ser certificadas pela AWS. Mais e mais pessoas querem aprender a computação em nuvem e levar suas carreiras a novos patamares. E com essas certificações, eles são como investimentos em você e em suas habilidades.

E se você tiver qualquer problema, preocupação ou feedback construtivo sobre nosso e-book, sinta-se à vontade para nos contatar em www.guilhermeteles.com.br.