Cabeça nas nuvens CLF-C01-RT23 AWS

Tópicos de estudo

- Introdução
    - alguns passos antes de entrar na nuvem
    - O que é AWS?
    - Infraestrutura AWS
    - Regiões
    - Zonas de disponibilidade
    - pontos de presença
    - Escopo de serviço
    - Entendendo alguns serviços

- Segurança na AWS
    - Responsabilidade compartilhada
    - IAM - Gerenciamento de Identificação e Acesso
- Networking na AWS (Redes)
    - VPC - nuvem privada virtual
    - sub-rede
    - Portal da Internet
    - Portal Privado Virtual
    - Tabela de rotas
    - Grupos de segurança e Network ACLs

Introdução

O que é um modelo cliente-servidor?

Na computação, um **cliente** pode ser um navegador da web ou um aplicativo de desktop com o qual uma pessoa interage para fazer a inclusão a servidores de computador. Um **servidor** pode ser um serviço como o Amazon Elastic Cloud Compute (Amazon EC2), um tipo de servidor virtual.

O que é computar em nuvem?

A computação na nuvem é a entrega de recursos de TI sob demanda pela internetr com uma definição de preço de pagamento conforme você utiliza. Em vez de comprar, ter e manter datacenters e servidores físicos, você pode acessar serviços de tecnologia, como capacidade computacional, armazenamento e banco de dados, conforme a necessidade, usando um provedor de nuvem como por exemplo a AWS (Amazon Web Services) .

A AWS oferece três modelos de implantação da computação em nuvem:

- **Implantação baseada na nuvem** , nesse modelo você pode migrar aplicativos existentes para a nuvem ou projetar e criar novos aplicativos na nuvem. Você pode criar esses aplicativos em uma infraestrutura de baixo nível que precisa do gerenciamento de sua equipe de TI. Como alternativa, você pode criá-los usando serviços de nível superior que cumprem os requisitos de gerenciamento, arquitetura e dimensionamento da infraestrutura principal. Tópicos importantes sobre o modelo de implantação baseado na nuvem:
    - Execute todas as partes do aplicativo na nuvem
    - Migrar aplicativos existentes para a nuvem
    - Projete e crie novos aplicativos na nuvem
- Implantação no local,

A computação na nuvem tem diversos benefícios como:

- Troque despesas iniciais por despesas variáveis
- Pare de gastar dinheiro para executar e manter data centers
- Para tentar adivinhar capacidade
- Beneficie-se de enormes economias de escala
- Aumente a velocidade e a agilidade
- Ter alcance global em minutos

Além dos benefícios seguidos, você também pode escolher qual tipo de computação na nuvem mais se adequa às suas necessidades.

Os três principais tipos de computação em nuvem são: **(IaaS)** , **(PaaS)** e **(SaaS)**

- **Infraestrutura como serviço (IaaS)** , contém componentes básicos de TI na nuvem. Normalmente, o IaaS oferece acesso a recursos de rede, computadores (virtuais ou em hardware dedicado) e espaço de armazenamento de dados. O IaaS oferece o mais alto nível de flexibilidade e

controle de gerenciamento sobre os recursos de TI. Ele é o tipo de computação mais semelhante aos recursos existentes de TI, já conhecidos por vários departamentos e desenvolvedores de TI.

- **Plataforma como Serviço (PaaS)** , com o PaaS você não precisa mais gerenciar a infraestrutura subjacente (geralmente, hardware e sistemas operacionais) e pode manter o foco na implantação e no gerenciamento de aplicativos. Dessa forma, você fica mais eficiente, pois não precisa se preocupar com aquisição de recursos, planejamento de capacidade, manutenção de software, correções ou qualquer outro tipo de trabalho repetitivo genérico necessário para a execução dos aplicativos.
- **Software como Serviço (SaaS)** , oferece um produto completo, executado e gerenciado pelo provedor de serviços. Na maioria dos casos, quando as pessoas mencionam SaaS, estão falando de aplicativos de usuários finais (como e-mail baseado na web). Com uma oferta de SaaS, você não precisa pensar sobre a manutenção do serviço ou o gerenciamento da infraestrutura subjacente. Você só precisa se preocupar sobre como usará esse software específico.

O que é AWS?

Amazon Web Services ou simplesmente AWS é uma plataforma de nuvem, que possui mais de 200 serviços completos de datacenters transmitidos pelo mundo. Clique aqui para saber mais: https://aws.amazon.com/pt/what-is-aws/

Infraestrutura AWS

- 31 regiões espalhadas pelo globo
- 99 zonas de disponibilidade
- 410 pontos de presença
- 245 paises e territórios atendidos

Clique aqui par conferir a infraestrutura da AWS: https://aws.amazon.com/pt/about-aws/global-infrastructure/

Regiões (Regiões)

Zonas de disponibilidade (Availability Zones)

Uma AZ é um conjunto altamente redundante de datacenters, onde são projetados para operar de forma compreensiva das demais AZs.

As zonas de disponibilidade ficam geograficamente, ou seja fisicamente, separado uma das outras para que em caso de algum evento numa AZ (ex: desastres naturais ou eventos causados pelo homem) outra AZ não seja impactada.

As AZs são divididas das seguintes formas:

AZ - A

AZ-B

AZ-C

AZ - D

AZ-E

AZ-F

Temos um total de no máximo (até agora) de 6 AZs por região.

Pontos importantes:

- A AWS faz um balanceamento de carga totalmente transparente para os usuários. Esse balanceamento é feito para que as zonas de disponibilidade não funcionem sobrecarregadas, pois por exemplo: Se todos mundo escolhesse as AZs A, B e C, elas ficariam sobrecarregadas. Com o balanceamento feito pela AWS a AZ - A para mim pode não ser a mesma AZ - A para outro usuário, pode estar em locais diferentes e com isso a AWS evita sobrecarga em suas AZs.
- Uma AZ não é necessariamente um datacenter (é um local onde estão concentrados os sistemas computacionais de uma empresa ou organização, como um sistema de telecomunicações ou um sistema de armazenamento de dados). Uma AZ pode ser um conjunto de datacenters por exemplo.

Pontos de presença (Edge Locations)

São **datacenters provedores de serviços considerados "globais"** . Os pontos de presença são endpoints da AWS usados para cache de conteúdo. ao realizar o cache dos conteúdos a latência é diminuída (tem como fazer cache temporário, você poderá definir isso).

Principais serviços hospedados em um ponto de presença:

- Caches do CloudFront
- Serviços de CDN
- Rota 53 (Serviço de DNS)
- Aceleração de transferência do Amazon S3

Escopo de serviço

É definido se o serviço será executado dentro de uma zona de disponibilidade, dentro de todas as AZs ou se o serviço será executado globalmente, isto é, dentro de todas as regiões da AWS.

Temos 3 níveis de escopo de serviço:

- Escopo de zona de disponibilidade
- Escopo da região
- Escopo global

Escopo de zona de disponibilidade, serviços englobados:

- EC2
- RDS
- EBS
- IP Privado

Escopo de região, serviços englobados:

- ELB
- Escalonamento automático

- IAM
- S3
- Grupo de segurança

Escopo global, serviços englobados:

- EU SOU
- rota 53
- Frente Nuvem

Entendendo alguns serviços

Amazon CloudFront

É uma rede de entrega de conteúdo (CDN) rápida, altamente programável e segura.

O Amazon CloudFront é um serviço rápido de rede de entrega de conteúdo (CDN) que entrega dados, vídeos, aplicativos e APIs a clientes em todo o mundo com segurança, baixa latência e altas velocidades de download em um ambiente de uso facilitado para desenvolvedores. O CloudFront é integrado com a AWS; ambos são locais físicos conectados diretamente à infraestrutura global da AWS, bem como a outros serviços da AWS. O CloudFront funciona de forma transparente com serviços como AWS Shield para mitigação de ataques DDoS; Amazon S3, Elastic Load Balancing ou Amazon EC2 como origens para os aplicativos; e Lambda@Edge para executar código personalizado mais perto dos usuários dos clientes e personalizar a experiência dos usuários. Por fim, se você usar origens na AWS, como Amazon S3, Amazon EC2 ou Elastic Load Balancing,https://aws.amazon.com/pt/cloudfront/

O CloudFront obtém seus conteúdos de um bucket (contêineres para objetos) do Amazon S3, uma instância do Amazon EC2, um load balancer do Amazon Elastic Load Balancing ou seu próprio servidor web, quando não está em um ponto de presença. Uma coisa legal do ClouFront é que ele pode ser usado para fornecer um site ou aplicativo inteirinho incluindo conteúdo dinâmico, estático, interativo e de streaming.

rota 53

O Amazon 53 é um serviço web de DNS (Domain Name System) altamente disponível e dimensionável.

O que é um DNS?

O DNS é um sistema de nomes de domínio. são os responsáveis por localizar e traduzir para números IP os endereços dos sites que digitamos nos navegadores.

Mais sobre DNS: https://canaltech.com.br/internet/o-que-e-dns/

Amazon S3

O Amazon Simple Storage Service (Serviço de Armazenamento Simples) é armazenamento para a Internet. Ele foi projetado para facilitar a compatibilidade de escala na web para os devs.

Vantagens de usar esse serviço:

- Criação de baldes
- armazenamento de dados
- Download de dados
- Gerenciamento de permissões
- Uso de interfaces padrão como por exemplo REST e SOAP

OBS: é recomendável utilizar o padrão API REST

Resumo sobre Amazon S3:

Podemos pensar no Amazon S3 como um mapa de dados básicos constituídos por: **balde + chave + ID de versão + o objeto em si**

Principais conceitos do Amazon S3

- baldes
- Objetos
- Chaves
- Regiões

Buckets: é um contêiner para armazenamento de objetos.

Objetos: são as entidades armazenadas dentro dos baldes esses objetos consistem em metadados e dados de objeto. **Os metadados são um conjunto de pares de nome e valor que descrevem o objeto** (pense em JSON, por exemplo). Um objeto pode ser identificado dentro de um balde por meio de uma **chave e um ID de versão** .

Chaves: são as chaves de identificação de falar acima, a chave é um identificador exclusivo de um objeto em um balde. **Cada objeto em um balde tem exatamente uma chave** .

Regiões: são as regiões da AWS. Você pode escolher em qual região quer criar o seu bucket e pode levar em conta alguns critérios já mencionados como custo, menor latência na entrega do conteúdo e etc. Um ponto importante é que os dados armazenados em um bucket em determinada região, não são transferidos para outra região a menos que o usuário o transfira para outra região.

Antes de começar a usar o Amazon S3 confira os endpoints que estão disponíveis na região
escolhida: https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region

Como configurar um bucket S3 e distribuir o conteúdo usando um navegador web: https://aws.amazon.com/pt/getting-started/hands-on/deliver-content-faster/

Documentação para começar a usar o
CloudFront: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/GettingStarted.html

OBS: É possível utilizar o Amazon S3 gratuitamente pelo período de 12 meses

Documentação sobre o Amazon
S3: https://docs.aws.amazon.com/pt_br/AmazonS3/latest/dev/Welcome.html

Segurança na AWS

responsabilidade compartilhada

Ao utilizar os serviços da AWS nós possuímos uma responsabilidade compartilhada com a empresa.

Responsabilidade da AWS: a AWS é responsável por proteger a infraestrutura que executa todos os serviços oferecidos na sua nuvem. Essa infraestrutura é composta por hardware, software, redes e instalações que executam os serviços.

Responsabilidade do usuário: a responsabilidade do usuário será determinada pelos serviços de nuvem selecionados por ele hehehe, então cabe ao cliente ler quais "suas atribuições" para cada serviço que for utilizar.

Modelo de responsabilidade compartilhada: https://aws.amazon.com/pt/compliance/shared-responsibility-model/

IAM - Gerenciamento de Identificação e Acesso

IAM é um serviço da web que ajuda você a controlar o acesso aos recursos da AWS de forma segura

Com o IAM você controla quem é autenticado e autorizado, então é possível criar e gerenciar usuários e grupos dentro da AWS e conceder ou negar permissões por meio de policias.

Identidades:

- Usuários: representa uma pessoa ou serviço para interagir com recursos na AWS (quando você cria uma conta na AWS você já é um usuário).
- Grupos: conjunto de usuários com atribuições atribuídas.

- Funções/Papéis: permite que delegue acesso a usuários e serviços que normalmente não tem acesso aos serviços da AWS. **Permite criar um conjunto de permissões temporárias para usuários ou instâncias** .

Políticas: permissões e regras de acesso a recursos da AWS, as políticas são atreladas a usuários, grupos e funções/papéis

Boas práticas para a criação de usuários ou grupos: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#create-iam-users

Networking na AWS (Redes)

VPC - nuvem privada virtual

Uma Amazon Virtual Private Cloud (Amazon VPC) permite executar os recursos da AWS em uma rede virtual definida por você. Essa rede virtual se assemelha a uma rede tradicional que você operaria em seu datacenter, com os benefícios de usar a infraestrutura dimensionável da AWS. https://docs.aws.amazon.com/pt_br/vpc/latest/userguide/what-is-amazon-vpc.html

Resumidamente VPC é um serviço que permite o usuário criar e gerenciar uma rede privada dentro da nuvem AWS. Amazon VPC é a camada de rede para as instâncias criadas no EC2.

Principais conceitos de uma VPC:

- VPC — uma rede virtual dedicada à sua conta da AWS.
- Sub-rede — uma gama de endereços IP na VPC.
- Tabela de rotas — um conjunto de regras, chamadas de rotas, que são usadas para determinar para onde o tráfego de rede será direcionado.
- Gateway da Internet — um gateway que você conecta à VPC para permitir a comunicação entre recursos na VPC e na Internet.
- VPC endpoint — permite conectar de forma privada a VPC aos serviços compatíveis da AWS e aos serviços do VPC endpoint apresentados pelo PrivateLink sem exigir um gateway da Internet, um dispositivo NAT, uma conexão VPN ou uma conexão do AWS Direct Connect. **As instâncias na**

sua VPC não permitiram que endereços IP públicos se comuniquem com recursos no serviço. O tráfego entre a sua VPC e os outros serviços não deixa a rede da Amazon.

Principais componentes de uma VPC:

- Networking access control list (ACLs): lista de controle de acessos, é uma camada de segurança opcional para sua VPC, **funciona como um firewall que controla o tráfego de entrada e saída de uma ou mais sub redes** .
- Grupo de segurança: grupo que fornece controle de entrada e saída.
- Tabela de rotas: tabela de rotas que contém um conjunto de regras usadas para determinar para onde o tráfego de rde ou sub rede será direcionado.
- Nat Gateway: fornece acesso a internet para instâncias EC2.
- Gateway de Internet: onde é liberado e fornecido acesso à internet.

OBS: VPC tem o escopo de região, então quando você criar uma VPC ela existirá em todas as AZs dessa região.

Informações sobre preço do serviço de VPC: https://aws.amazon.com/pt/vpc/pricing/

Cotas da Amazon VPC: https://docs.aws.amazon.com/pt_br/vpc/latest/userguide/amazon-vpc-limits.html

O que é o AWS Direct Connect? https://docs.aws.amazon.com/pt_br/directconnect/latest/UserGuide/Welcome.html

sub-rede

Uma sub-rede faz a segmentação de endereçamentos de uma rede dentro de uma VPC na AWS.

As sub-redes são onde vamos disponibilizar os nossos recursos, como por exemplo uma instância EC2

- Faixa maior: /16
- Alcance menor: /28

Existem dois tipos de sub-rede:

- Subnet pública: possui acesso à internet, é necessário fazer uma configuração de entrada na tabela de rotas para um gateway de internet.
- Subnet privada: não possui acesso a internet.

Documentação: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html

gateway de internet

Um Internet Gateway é um componente da VPC horizontalmente dimensionado, redundante e altamente disponível que permite a comunicação entre a VPC e a Internet.

Um gateway da internet tem duas finalidades:

- Fornecer um destino nas tabelas de rotas da VPC para o tráfego roteável na Internet.
- Executar um NAT - Network address translation (tradução de endereços de rede) para instâncias designadas com endereços IPv4 públicos.

Mais informações sobre NAT: https://www.youtube.com/watch?v=BSe7EgvDB6Q

https://www.cisco.com/c/pt_br/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html

Um gateway da internet oferece suporte para tráfego IPv4 e IPv6. Não causa riscos de disponibilidade ou restrições de largura de banda no tráfego de rede. **Não há custo adicional por ter um gateway da Internet na sua conta.**

Documentação: https://docs.aws.amazon.com/pt_br/vpc/latest/userguide/VPC_Internet_Gateway.html

Resumidamente o Internet Gateway é um recurso que possibilita a comunicação das instâncias com a internet.

- Por padrão o internet gateway vem associado a VPC padrão que é gerado quando criamos nossa conta na AWS
- Cada VPC só poderá ter um Internet Gateway associado

Portal Privado Virtual

É um recuso que possibilita a conexão do ambiente no local com sua VPC na AWS.

Existem duas formas de configurar um Virtual Private Gateway

- Blade site a site: https://docs.aws.amazon.com/vpn/latest/s2svpn/VPNRoutingTypes.html
- Conexão direta do blade: https://docs.aws.amazon.com/pt_br/directconnect/latest/UserGuide/Welcome.html

Blade: espaço dentro da AW onde configuramos os recursos.

Tabela de rotas

É uma tabela lógica que possui um conjunto de regras, chamadas de rotas, que são utilizadas para direcionar onde seu tráfego de rede, de subnet, ou gateway deve chegar.

Pontos importantes:

- Uma tabela de rotas pode estar associada a várias sub-redes, já uma sub-rede só poderá estar associada a uma tabela de rotas.
- Uma VPC pode ter várias tabelas de rotas.

Normalmente as tabelas de rotas são utilizadas para configurar rotas, como por exemplo:

- Portal da Internet
- Gateway privado virtual
- Gateway NAT
- Emparelhamento de VPC

Os principais conceitos das tabelas de rotas são os seguintes:

Tabela de rotas principais — uma tabela de rotas que vem automaticamente com um VPC. Ela controla o roteamento de todas as sub-redes que não estejam oficialmente associadas com outra tabela de rotas.

Tabela de rotas personalizadas — uma tabela de rotas que você cria para o VPC.

Associação de borda — uma tabela de rotas que é usada para encaminhar o tráfego de entrada da VPC para um equipamento. Associe uma tabela de rotas ao gateway da Internet ou ao gateway privado virtual e especifique uma interface de rede do seu equipamento como destino do tráfego da VPC.

Associação de tabela de rotas — a associação entre uma tabela de rotas e uma sub-rede, gateway da Internet ou gateway privado virtual.

Tabela de rotas de sub-rede — uma tabela de rotas associadas a uma sub-rede.

Tabela de rotas de gateway — uma tabela de rotas associada a um gateway da Internet ou gateway privado virtual.

Tabela de rotas de gateway local — uma tabela de rotas associada a um gateway local do Outposts. Para obter informações sobre gateways locais, consulte Gateways locais no Guia do usuário do AWS Outposts.

Destination (Destino) – o intervalo de endereços IP para onde você deseja que o tráfego vá (CIDR de destino). Por exemplo, uma rede corporativa externa com um CIDR 172.16.0.0/12 .

Propagação — a controlada das rotas permite que um gateway privado virtual propague automaticamente as rotas para as tabelas de rotas. Isso significa que você não precisa inserir as rotas VPN manualmente para suas tabelas de rotas. Para obter mais informações sobre as opções de roteamento da VPN, consulte Opções de roteamento do Site-to-Site VPN no Guia do usuário do Site-to-Site VPN.

Target (Destino) – o gateway, uma interface de rede ou uma conexão por meio da qual enviar o tráfego de destino; por exemplo, um gateway da Internet.

Rota local — uma rota padrão para comunicação dentro da VPC.

Documentação: https://docs.aws.amazon.com/pt_br/vpc/latest/userguide/VPC_Route_Tables.html#RouteTables

Grupos de segurança e Network ACLs

São recursos que liberam tráfego de entrada e saída.

Diferenças entre security groups e Network ACLs:

Security Groups (atualmente como um firewall para instâncias EC2):

- Escopo de instâncias
- Política padrão é permitir
- Regras são stateful (qualquer alteração aplicada a uma regra de entreda será aplicada automaticamente para as regras de saída)
- Aplica-se a uma instância somente se alguém especificar o security group ao executar uma instância ou associar posteriormente o security group com a instância
- Avaliamos todas as regras antes de decidir se permitimos ou não o tráfego

Documentação: https://docs.aws.amazon.com/pt_br/vpc/latest/userguide/VPC_SecurityGroups.html

Network ACLs (atuaam como firewall das subnets):

- Escopo de sub-rede
- Suporta permissão e negação (podemos negar que endereços de IP estabeleção conexão com a minha instância)
- As regras são sem estado (qualquer alteração aplicada na regra de entrada não será aplicada automaticamente para a regra de saída, é necessário que você faça manualmente a regra desejada para saída)
- Aplica-se automaticamente a todas as instâncias nas sub-redes com as quais está associada (portanto, fornece uma camada adicional de defesa, caso as regras do grupo de segurança sejam permissivas demais)
- Processamos regras em ordem, começando com a regra de número menor, ao decidir se devemos permitir o tráfego

Documentação: https://docs.aws.amazon.com/pt_br/vpc/latest/userguide/vpc-network-acls.html

Leia mais sobre privacidade do tráfego entre redes na VPC: https://docs.aws.amazon.com/pt_br/vpc/latest/userguide/VPC_Security.html#VPC_Security_Comparison