



Redes e Conectividade na AWS

- A infraestrutura de redes é um dos pilares fundamentais dentro da AWS. Compreender como funcionam as redes na AWS permite projetar arquiteturas seguras, escaláveis e altamente disponíveis. Nesta aula, abordaremos os principais conceitos sobre redes e conectividade na AWS, desde a configuração de uma VPC até a implementação de soluções práticas no dia a dia.

Conceitos Fundamentais :

O que é uma VPC?

- **A Virtual Private Cloud (VPC)** é uma rede virtual privada dentro da AWS. Ela permite que você defina sua topologia de rede, incluindo sub-redes, tabelas de rotas, gateways e outras configurações essenciais.
- **CIDR (Classless Inter-Domain Routing)**: Define o intervalo de endereços IP da VPC.
- **Sub-redes**: Segmentam a rede e podem ser públicas ou privadas.
- **Tabelas de Rotas**: Controlam a direção do tráfego dentro e fora da VPC.
- **Internet Gateway (IGW)**: Permite conexões entre a VPC e a Internet.



STUDY LIBRARY

- NAT Gateway: Permite que instâncias em sub-redes privadas acessem a Internet sem ficarem expostas.

Sub-redes (Subnets):

- A VPC pode ser dividida em sub-redes públicas e privadas:
- **Sub-rede pública:** Contém instâncias com IP público acessíveis pela Internet.
- **Sub-rede privada:** Contém recursos sem acesso direto à Internet, protegendo serviços internos.

Tabelas de Rotas:

As tabelas de rotas são usadas para definir o tráfego dentro da VPC. Alguns exemplos de regras comuns:

- Destino 0.0.0.0/0 via **Internet Gateway**: Permite acesso público.
- Destino 0.0.0.0/0 via **NAT Gateway**: Permite acesso à Internet sem exposição pública.
- Destino 10.0.0.0/16 **dentro da própria VPC**: Mantém a comunicação interna.

Security Groups vs Network ACLs:

- Security Groups: Controle de tráfego a nível de instância. Funciona como um firewall stateful.
- Network ACLs: Controle de tráfego a nível de sub-rede. Atua como um firewall stateless.



STUDY LIBRARY

- NAT Gateway: Permite que instâncias em sub-redes privadas acessem a Internet sem ficarem expostas.

Sub-redes (Subnets):

- A VPC pode ser dividida em sub-redes públicas e privadas:
- **Sub-rede pública:** Contém instâncias com IP público acessíveis pela Internet.
- **Sub-rede privada:** Contém recursos sem acesso direto à Internet, protegendo serviços internos.

Tabelas de Rotas:

As tabelas de rotas são usadas para definir o tráfego dentro da VPC. Alguns exemplos de regras comuns:

- Destino 0.0.0.0/0 via **Internet Gateway**: Permite acesso público.
- Destino 0.0.0.0/0 via **NAT Gateway**: Permite acesso à Internet sem exposição pública.
- Destino 10.0.0.0/16 **dentro da própria VPC**: Mantém a comunicação interna.

Security Groups vs Network ACLs:

- Security Groups: Controle de tráfego a nível de instância. Funciona como um firewall stateful.
- Network ACLs: Controle de tráfego a nível de sub-rede. Atua como um firewall stateless.



STUDY LIBRARY

Resumo: (Cloud Practitioner)

1. VPC (Virtual Private Cloud)

- **Definição:** A **VPC** é uma rede virtual que permite provisionar um ambiente isolado dentro da nuvem da AWS. É onde você pode executar seus recursos da AWS, como instâncias EC2, bancos de dados RDS e outros serviços.
- **Características:**
 - **Sub-redes:** Você pode dividir sua VPC em sub-redes públicas e privadas. Sub-redes públicas têm acesso à Internet, enquanto sub-redes privadas são isoladas.
 - **CIDR Block:** Ao criar uma VPC, você especifica um bloco CIDR (Classless Inter-Domain Routing) que define o intervalo de endereços IP que a VPC usará.
 - **Isolamento:** Recursos dentro da VPC são isolados de outros ambientes na AWS, proporcionando segurança e controle.
 -

2. Sub-redes

- **Definição:** As sub-redes são divisões lógicas da VPC que permitem organizar recursos em diferentes segmentos de rede.
- **Tipos:**
 - **Públicas:** Permitem que recursos como instâncias EC2 se conectem à Internet. Para isso, geralmente têm um endereço IP público.
 - **Privadas:** Recursos aqui não têm acesso direto à Internet, ideal para bancos de dados e aplicações que não precisam ser expostas publicamente.
 -



STUDY LIBRARY

Resumo: (Cloud Practitioner)

3. Internet Gateway

- **Definição:** Um **Internet Gateway** é um componente que permite que a VPC se conecte à Internet. Ele fornece a capacidade de comunicação entre instâncias na VPC e a Internet.
- **Funções:**
 - Permitir o tráfego de entrada e saída entre a VPC e a Internet.
 - Associar-se a sub-redes públicas para que os recursos nelas possam acessar a Internet.
 -

4. Security Groups

- **Definição:** Os **Security Groups** atuam como um firewall virtual que controla o tráfego de entrada e saída de recursos específicos dentro da VPC.
- **Características:**
 - **Baseado em Estado:** As regras de segurança são aplicadas com base no estado da conexão, ou seja, se uma conexão de saída é permitida, as respostas dessa conexão também são permitidas automaticamente.
 - **Regras de Entrada e Saída:** Você pode definir regras que permitem ou negam tráfego com base em protocolos, portas e endereços IP.
 - **Associável a Recursos:** Os Security Groups são associados a instâncias EC2 e outros serviços, controlando o acesso a esses recursos.



Resumo: (Cloud Practitioner)

5. NACL (Network Access Control List)

- **Definição:** As **NACLS** são listas de controle de acesso que oferecem uma camada adicional de segurança em nível de sub-rede.
- **Características:**
 - **Estateless:** Ao contrário dos Security Groups, as NACLS são "stateless", o que significa que se uma regra de entrada permite tráfego, você também precisa ter uma regra de saída correspondente.
 - **Regras de Entrada e Saída:** As NACLS têm regras separadas para tráfego de entrada e saída e são aplicáveis a toda a sub-rede.
 - **Permitir ou Negar:** Você pode definir regras que permitem ou negam tráfego, e as regras são avaliadas em ordem numérica.

6. VPN (Virtual Private Network)

- **Definição:** Uma **VPN** permite conectar sua VPC a uma rede local (on-premises) através de uma conexão segura e criptografada.
- **Utilização:** Ideal para organizações que desejam integrar seus ambientes de TI na nuvem com seus data centers.
-



Resumo: (Cloud Practitioner)

7. VPC Peering

- **Definição:** O **VPC Peering** permite que duas VPCs se comuniquem entre si, mesmo que estejam em regiões diferentes ou em contas diferentes.
- **Características:**
 - Não há limite de largura de banda e é uma comunicação privada.
 - As VPCs devem ter CIDR blocks não sobrepostos.

8. Elastic IP

- **Definição:** Um **Elastic IP** é um endereço IP estático que você pode associar a instâncias EC2. Ele é útil para garantir que a aplicação tenha um endereço IP fixo, mesmo se a instância for reiniciada ou substituída.

Fluxo de Rede em uma VPC

- **Configuração Básica:**
 - **Criar uma VPC** com um bloco CIDR (por exemplo, 10.0.0.0/16).
 - **Dividir em Sub-redes:** Criar uma sub-rede pública (por exemplo, 10.0.1.0/24) e uma sub-rede privada (10.0.2.0/24).
 - **Adicionar um Internet Gateway** à VPC e associá-lo à sub-rede pública.
 - **Definir Security Groups** para instâncias EC2 que controlam o acesso.
 - **Criar NACLs** para a sub-rede, se necessário, para uma camada adicional de segurança.



STUDY LIBRARY

Conclusão

A configuração da rede na AWS é um aspecto crítico para garantir que os recursos estejam seguros, escaláveis e otimizados. A combinação de VPCs, sub-redes, gateways, Security Groups e NACLs oferece uma estrutura robusta para gerenciar a conectividade e a segurança em um ambiente de nuvem. Compreender como cada um desses componentes interage é fundamental para projetar e implementar uma arquitetura de rede eficaz na AWS.

