
CLOUD
COMPUTING

Texto base

5

Virtualização de Serviços de rede (Networking)

Prof. Me. Rodolfo Riyoei Goya

Resumo

Na "Computação em Nuvem", os componentes da infraestrutura de rede de Tecnologia da Informação (T.I.) são serviços abstratos. Na prática, como são configurados e colocados em operação? Como é a comunicação com a Internet das instâncias criadas nas redes de provedores de serviços de nuvem? Abordam-se aqui, como os conceitos listados são lidados.

5.1. Introdução

Como são configuradas as redes e endereços em provedores de serviços de "Computação em Nuvem"? Como o roteamento para comunicação entre redes é configurado? Como as redes configuradas dentro de uma nuvem privada são configuradas para se comunicar com a Internet? Como configurar NAT para que uma rede de endereços privados se comunique com a Internet? Como são configurados registro e tradução de nomes em endereços em provedores de serviços de "Computação em Nuvem"?

5.1.1. Redes Virtuais Privadas

Provedores de serviços de computação em nuvem oferecem redes virtuais privadas. Na AWS, por exemplo, este serviço é chamado "Virtual Private Cloud" – VPC.

Para criar uma VPC na AWS, basta navegar pelo console até localizar o VPC Dashboard e executar o "Criar VPC", especificando nome para ela, região e o bloco de endereços IP.

Uma VPC é uma nuvem privada para o cliente isolada dos demais clientes e da Internet. Na AWS, o cliente pode criar até 5 VPCs por região (uma VPC está inteiramente dentro de uma região), usando VPCs para organizar a rede da empresa por localização geográfica, departamentos, linha de negócios, funcionalidade ou produto, por exemplo.

5.1.2. Endereçamento IP na VPC da AWS

Na AWS, cada VPC pode ocupar um bloco de endereços privados. A Tabela 1 mostra as faixas de endereços dentro das quais são permitidos escolher os blocos usados para uma VPC. Ao criar várias VPC é recomendável escolher blocos sem sobreposição de endereços (VPCs com um mesmo endereço IP interno não podem se comunicar entre si).

Tabela 1. Endereços IP reservados para redes privadas.

Faixa	Endereço Inicial	Endereço Final
10.0.0.0/8	10.0.0.0	10.255.255.255
172.16.0.0/12	172.16.0.0	172.31.255.255
192.168.0.0/16	192.168.0.0	192.168.255.255

Fonte: do autor, 2022.

Na AWS, cada VPC pode ser configurada com um bloco de endereços de tamanhos entre /28 e /16. A Tabela 2 mostra os tamanhos possíveis.

Tabela 2. Tamanhos de rede para cada máscara de rede.

Máscara	Tamanho	Endereço rede
/28	16	Múltiplo de 1.1.1.16
/27	32	Múltiplo de 1.1.1.32
/26	64	Múltiplo de 1.1.1.64
/25	128	Múltiplo de 1.1.1.128
/24	256	Múltiplo de 1.1.1.0
/23	512	Múltiplo de 1.1.2.0
/22	1.024	Múltiplo de 1.1.4.0
/21	2.048	Múltiplo de 1.1.8.0
/20	4.096	Múltiplo de 1.1.16.0
/19	8.192	Múltiplo de 1.1.32.0
/18	16.384	Múltiplo de 1.1.64.0
/17	32.768	Múltiplo de 1.1.128.0
/16	65.536	Múltiplo de 1.1.0.0

Fonte: do autor, 2022.

5.1.3. Subredes

Subredes são partições de uma VPC. A cada subrede é atribuída uma faixa de endereços. Não pode haver sobreposição de endereços de uma subrede para outra.

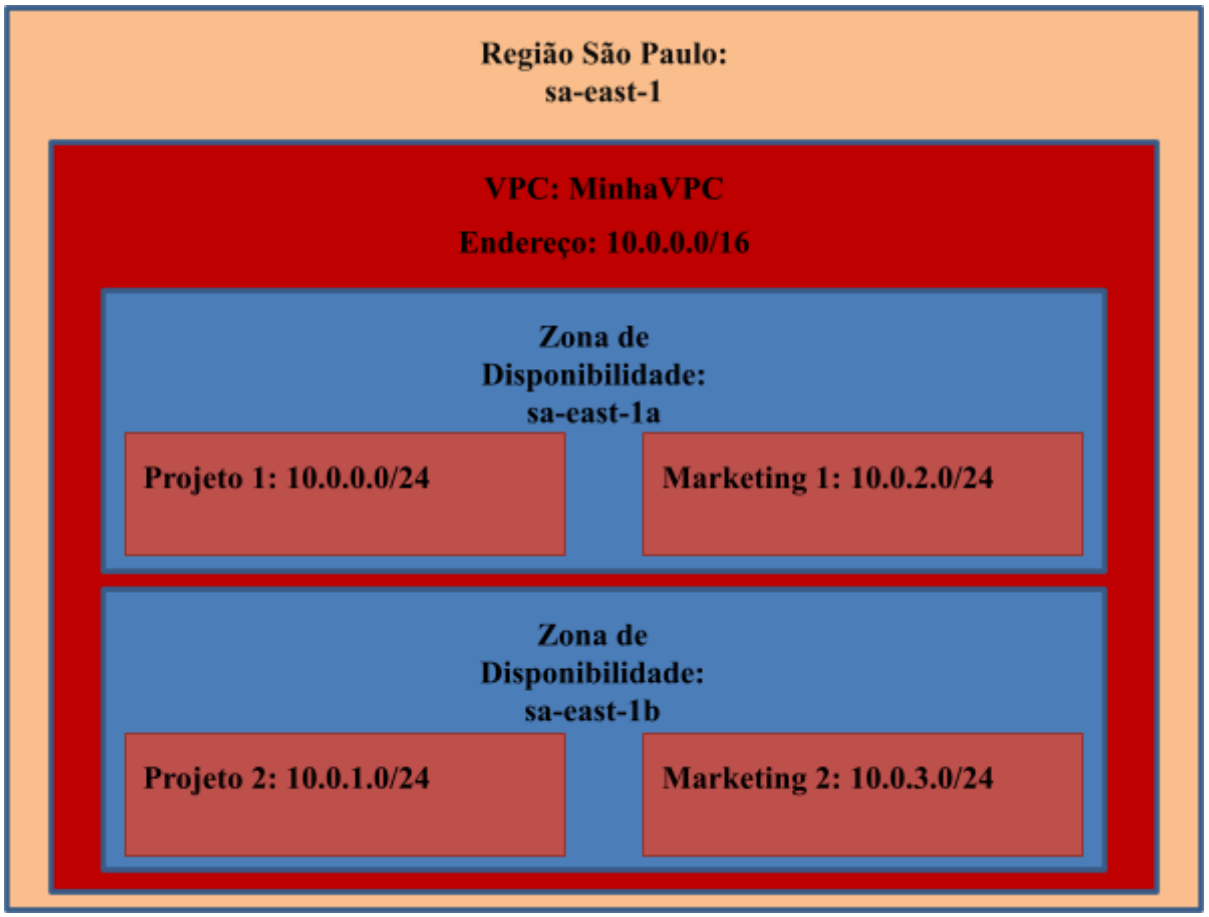
Ao se criar uma subrede, deve-se especificar um nome para ela, a qual VPC ela pertence, qual zona de disponibilidade ela pertence e qual o bloco de endereços alocado para ela.

Na AWS, o tamanho permitido de cada subrede em IPv4 é entre /28 e /16 (subredes em IPv6 são sempre /64). Consulte a Tabela 2 para os tamanhos possíveis.

A AWS reserva 5 endereços dentro de cada subrede (endereços de rede, gateway, DNS, broadcast e mais um reservado para uso futuro). Assim, uma rede /26, por exemplo, tem 59 endereços disponíveis para uso (descontando os 5 reservados dos 64 endereços).

Serviços criados dentro de uma subrede recebem automaticamente um endereço dentro da faixa selecionada para a esta rede, sem a necessidade de configurar alocação estática de endereço, cliente ou servidor DHCP.

Figura 1. Exemplo de VPC



Fonte: do autor, 2022.

A Figura 1 mostra um exemplo de como região, VPC, zonas de disponibilidade e subredes podem ser organizadas. Uma VPC (MinhaVPC) é criada dentro da região de São Paulo (sa-east-1) com o bloco de endereços 10.0.0.0/16 (endereços entre 10.0.0.0 e 10.0.255.255).

Dentro da MinhaVPC, 4 subredes foram criadas (Tabela 3). Duas subredes na Zona de Disponibilidade sa-east-1 e duas subredes na Zona de Disponibilidade sa-east-2.

As subredes de Projeto e de Marketing foram espalhadas em duas zonas de disponibilidade diferentes possibilitando uma maior proteção contra falhas.

Tabela 3. Subredes da Figura 1.

Nome	Zona	Rede	Endereço Inicial	Endereço Final
Projeto 1	as-east-1a	10.0.0.0/24	10.0.0.0	10.0.0.255
Projeto 2	as-east-1b	10.0.1.0/24	10.0.1.0	10.0.1.255
Marketing 1	as-east-1a	10.0.2.0/24	10.0.2.0	10.0.2.255
Marketing 2	as-east-1b	10.0.3.0/24	10.0.2.0	10.0.3.255

Fonte: do autor, 2022.

5.2. Roteamento

O roteamento permite comunicação entre instâncias em redes diferentes. Na AWS, isso é feito configurando tabelas de roteamento.

Para criar uma Tabela de Roteamento na AWS, basta navegar pelo console até localizar o Dashboard das Tabelas de Rotas e executar o "Criar Tabela de Rotas", especificando nome para ela, a VPC e as subredes que estão na tabela.

5.2.1. Tabelas de Roteamento

Na AWS, para configurar comunicação entre redes, se configuram tabelas de roteamento. Em uma tabela de roteamento, as redes listadas nela podem se comunicar entre si. No exemplo da Figura 2, mostra um possível cenário de configuração com duas tabelas de roteamento.

Figura 2. Tabelas de Roteamento

Rotas-Marketing

Rede	Destino
10.0.2.0/24	Local
10.0.3.0/24	Local

Rotas-Projeto

Rede	Destino
10.0.0.0/24	Local
10.0.1.0/24	Local

Fonte: do autor, 2022.

A tabela Rotas-Marketing indica que instâncias na subrede 10.0.2.0/24 (por exemplo, uma instância com endereço 10.0.2.100) e instâncias na subrede 10.0.3.0/24 (por exemplo, uma instância com endereço 10.0.3.150) podem se comunicar.

A tabela Rotas-Projeto indica que instâncias nas subredes 10.0.0.0/24 e 10.0.1.0/24 podem se comunicar.

Pela configuração feita, uma instância na subrede 10.0.0.0/24 não pode se comunicar com uma instância nas subredes 10.0.2.0/24 e 10.0.3.0/24 por não haver rotas para isso.

5.3. Internet Gateway e Network Address Translation

Para que uma instância se comunique com algum endereço IP fora da VPC na Internet, é necessária uma rota para a Internet na tabela de rotas. Na AWS isto é proporcionado pelos serviços de Internet Gateway e NAT Gateway.

Na AWS, os serviços de Internet Gateway e NAT Gateway são providos e gerenciados pela AWS em infraestrutura de alta disponibilidade (inclui redundância que protege contra falhas de suas partes) e escalabilidade (sua estrutura se ajusta com a demanda para impedir congestionamento).

5.3.1. Internet Gateway

Para criar um Internet Gateway na AWS, basta navegar pelo console até localizar o Dashboard de Gateways de Internet e executar o "Criar Gateways de Internet", especificando o nome para ele e a VPC.

Criado o Gateways de Internet, quando ele é incluído numa tabela de roteamento, as instâncias dentro das subredes que estão nesta tabela podem acessar (e serem acessados por) instâncias na Internet.

Por exemplo, um Internet Gateway foi criado com o nome igw-projeto e colocado na tabela de Rotas-Projeto (Figura-3) como rota para a rede 0.0.0.0/0 (endereços entre 0.0.0.0 e 255.255.255.255), ou seja, para todos os endereços IP da Internet vá através do igw-projeto.

Assim, as instâncias nas redes Projeto 1 e Projeto 2 podem acessar (e serem acessadas da) a Internet (as redes Marketing 1 e Marketing 2 não tem acesso a Internet).

Figura 3. Tabelas de Roteamento com Internet Gateway

Rotas-Marketing

Rede	Destino
10.0.2.0/24	Local
10.0.3.0/24	Local

Rotas-Projeto

Rede	Destino
0.0.0.0/0	igw-projeto
10.0.0.0/24	Local
10.0.1.0/24	Local

Fonte: do autor, 2022.

Para que as instâncias nas redes Projeto 1 e Projeto 2 possam acessar (e serem acessadas da) a Internet elas têm que ter um endereço IP público na hora que foram criadas. Assim, por exemplo, para dar acesso para a Internet para a instância de endereço 10.0.0.100 ela precisa de um endereço IP público também.

5.3.2. Network Address Translation

O uso do Internet Gateway pode ser inconveniente por demandar o uso de endereços IP públicos e entregar excesso de acesso - às vezes se quer apenas que se possa acessar a Internet, mas não ter instâncias que possam ser acessadas da Internet por ser inseguro.

Uma forma alternativa que não exige endereços IP públicos para instâncias e permite apenas conexões originadas das subredes para fora é o uso de Network Address Translation – NAT.

Na AWS, NAT é oferecido pelo serviço NAT Gateway. Para criar um NAT Gateway na AWS, basta navegar pelo console até localizar o Dashboard de NAT Gateway e executar o "Criar NAT Gateways", especificando nome para ele, a subrede onde estará criado e um endereço IP público.

Uma vez criado, o NAT Gateways pode ser incluído numa tabela de roteamento. Quando isso é feito, as instâncias das subredes que estão nela podem acessar a Internet através do NAT Gateway usando o endereço IP público dele.

Por exemplo, supondo que um NAT Gateway seja criado na rede projeto (porque esta rede já tem acesso a Internet) com o nome igw-marketing.

Quando uma rota é colocada na tabela de Rotas-marketing (Figura-4) para todos os endereços, vá para o igw-marketing, as instâncias nas redes Marketing 1 e Marketing 2 podem acessar a Internet (mas não serem acessadas da Internet).

Figura 4. Tabelas de Roteamento com NATGateway e Internet Gateway

Rotas-Marketing

Rede	Destino
0.0.0.0/0	nat-marketing
10.0.2.0/24	Local
10.0.3.0/24	Local

Rotas-Projeto

Rede	Destino
0.0.0.0/0	igw-projeto
10.0.0.0/24	Local
10.0.1.0/24	Local

Fonte: do autor, 2022.

5.4. Serviços de Nomes

Todos os provedores de serviços de computação em nuvem oferecem resolução de nomes. O serviço da AWS, por exemplo, usa o DNS e é chamado Route53.

5.4.1. Resolução de nomes

Os nomes processados no Route53 são do cliente e podem estar registrados no próprio Route53 ou em outro serviço de DNS na Internet. As principais características da resolução de nomes em endereços IP do Route53 são:

a. Resolve nomes para endereços IP públicos (que podem ser de dentro ou de fora da VPC da AWS) IPv4 e Ipv6
b. Pode traduzir o mesmo nome para diversos endereços IP permitindo a distribuição do tráfego para este nome entre diversos destinos para de balanço de carga
c. Política de tradução ponderada de nome para múltiplos endereços. Por exemplo, 5% para um endereço (versão nova em teste) e 95% para outro endereço
d. Política de tradução de nome, para múltiplos endereços, baseada na localização da origem da consulta. Por exemplo, se vem de um lugar que fala inglês vai para um endereço, se fala espanhol outro endereço, senão vai para um terceiro endereço
e. Testar se o equipamento no endereço traduzido está funcionando bem antes de responder a solicitações de tradução para este endereço
f. Com a tradução de um nome para diversos endereços, redirecionar o atendimento para outro endereço caso algum se torne indisponível, oferecendo contingência para falhas

5.4.2. Registro de nomes

O processo para registrar nomes no Route53 passa por uma série de etapas:

a. Escolha do nome: uma série de consultas para verificar se o nome que se deseja registrar já não pertence a outro
b. Configuração do tipo de nome: http, email, sip, IPv4/IPv6 etc. a ser registrado
c. Registro: Criação e propagação para que o registro seja globalmente estabelecido
d. Manutenção: Feito o registro ele é mantido mediante pagamento de taxa anual

5.5. Vamos praticar?

5.5.1. Quer experimentar de graça?

Há vários serviços de nuvem comerciais que permitem usar serviços gratuitamente ou por preços muito baixos por tempo limitado com propósitos de introdução e treinamento. Veja as ofertas desses serviços para alguns destes provedores nos links abaixo e experimente criar sua própria nuvem (infelizmente, registrar nomes não é serviços gratuito).

https://cloud.google.com/free

https://aws.amazon.com/pt/free

https://azure.microsoft.com/en-us/pricing/free-services/

5.5.2. Quanto custa?

Quanta custa criar uma rede privada em um provedor de serviços de nuvem? Veja os links abaixo e verifique o quando custa e como o uso é medido e cobrado.

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

https://cloud.google.com/vpc/pricing

5.6. Você quer ler?

5.6.1. VPC em provedores públicos

Quer saber mais sobre nuvens virtuais privadas de provedores públicos? Veja mais detalhes nos links:

https://azure.microsoft.com/pt-br/services/virtual-network/#overview

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

https://cloud.google.com/vpc

5.6.2. Políticas de resolução de nome

Quando um serviço de DNS está configurado com vários endereços para o mesmo nome, o critério usado para escolher qual endereço responde para uma consulta para este nome pode obedecer a diferentes políticas. Veja mais detalhes sobre políticas de resolução de nomes em endereços no link:

https://docs.aws.amazon.com/pt_br/Route53/latest/DeveloperGuide/routing-policy.html

Referências

TAURION, Cezar. **Cloud Computing:** computação em nuvem: transformando o mundo da tecnologia da informação. Rio de Janeiro: Brasport, 2009.

VELTE, Anthony T.; VELTE, Toby J.; ELSENPRETER, Robert. **Cloud Computing:** a practical approach. EUA:McGraw-Hill, 2010.

MARSHALL, Nick; BROWN, Mike; BLAIR FRITZ, G.; JOHNSON, Ryan. **Mastering VMware vSphere 6.7.** 1.ed. New Jersey: Sybex, 2019. 848p.

SANTOS, Tiago. **Fundamentos da computação em nuvem** (Série Universitária). 1ª ed., São Paulo, Editora Senac, 2018. 211p.

ANDREWS, Joshua; HALL, Jon. VMware Certified Professional **Data Center Virtualization on vSphere 6.7** Study Guide: Exam 2V0-21.19. 1.ed. New Jersey: Sybex, 2020. 640p.

Official Amazon Web Services (AWS) Documentation. **Amazon Elastic Compute Cloud:** User Guide for Linux Instances. Amazon. 2.105p. Disponível em: <https://aws.amazon.com/documentation/ec2/>. Acesso em 14 jan. 2022.