



**Certified Tech
Developer**

The Ultimate Degree

Infraestrutura I

Objetivos

Vamos criar uma VPC (Virtual Private Cloud). O que nos ajudará a completar dois objetivos:

Primeiro, vamos nos familiarizar com o portal da AWS. Um site com muitas opções, mas se entendermos o que está em cada lugar, com certeza podemos navegar com muita facilidade.

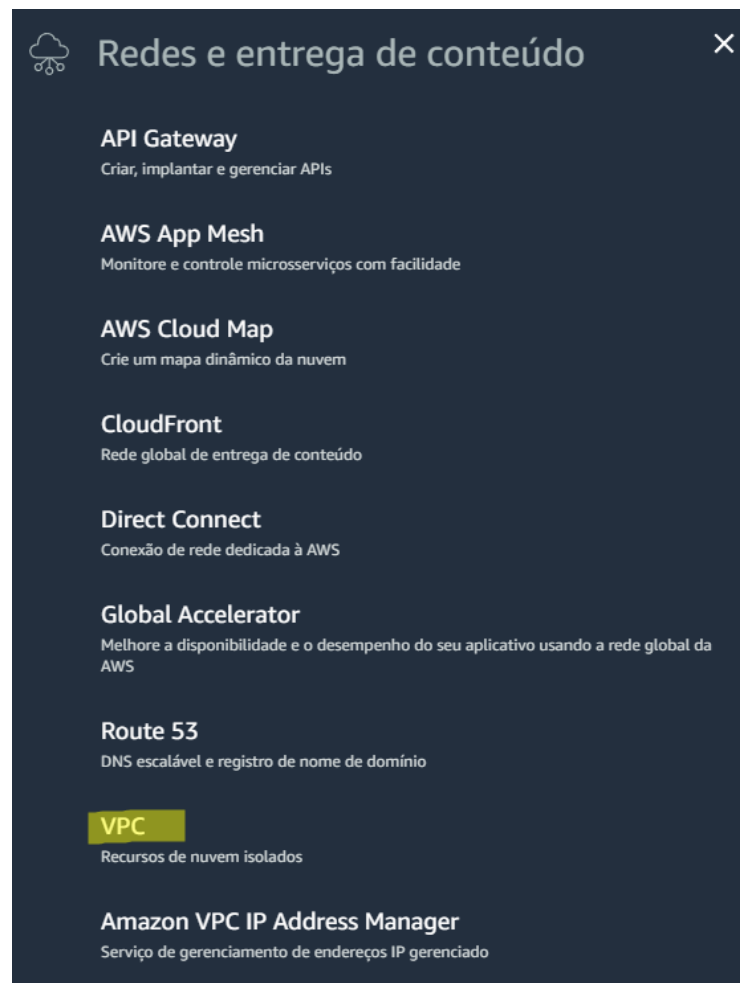
E em um segundo momento, adquirir o conceito de VPC, um conceito simples, mas muito importante para poder construir máquinas virtuais. E, finalmente, colocarmos em prática criando uma VPC.

Instruções

- 1) A primeira coisa que precisamos fazer é entrar no portal da AWS.
- 2) Uma vez no portal, vamos para a seção superior esquerda e selecionamos 'Serviços'.



- 3) Vamos procurar a seção 'Networking & Content Delivery' e abaixo dela, selecionamos 'VPC' (Redes e entrega de conteúdo):



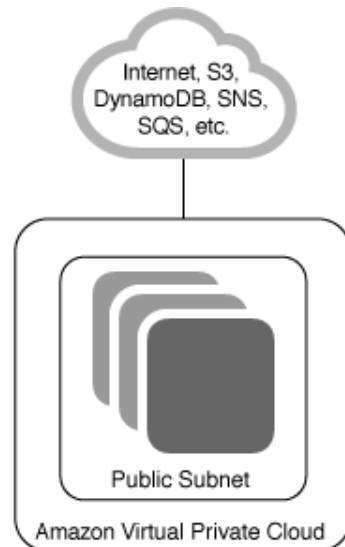
Mas antes de continuar, **o que é uma VPC ou Virtual Private Cloud?** Uma VPC é uma maneira de reservar uma pequena parte do centro de computação da AWS para executar nossas instâncias de IaaS. Isso, claro, virtualmente. Uma boa maneira de pensar em VPCs é como uma rede, à qual nossas instâncias estarão conectadas. Existem diferentes tipos:

- VPC com uma única sub-rede pública (vamos usar este tipo!)
- VPC com uma sub-rede pública e uma sub-rede privada
- VPC com sub-rede pública e privada, e acesso via VPN via hardware
- VPC com sub-rede privada e acesso por VPN via hardware



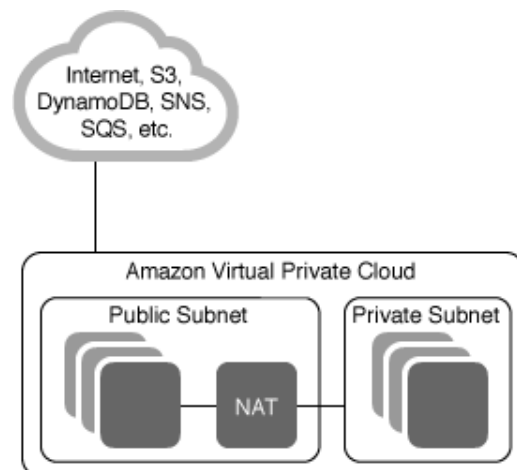
VPC com uma única sub-rede pública

Nossas instâncias serão executadas em uma seção privada e isolada da nuvem AWS, com acesso direto à Internet. Com ferramentas como listas de controle de acesso à rede e grupos de segurança, o tráfego de acesso dentro e fora das instâncias pode ser estritamente controlado.



VPC com uma sub-rede pública e uma sub-rede privada

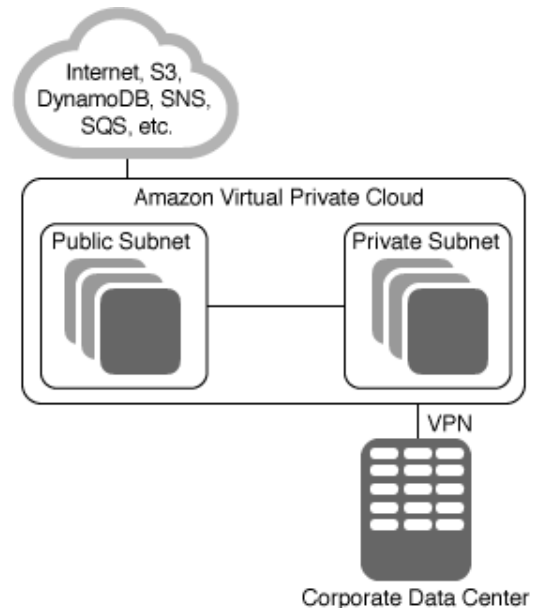
É muito semelhante ao tipo de VPC anterior, mas neste caso, é adicionada uma sub-rede do tipo privada. As instâncias conectadas a essa segunda sub-rede não podem ser acessadas pela Internet. Mas estes podem acessar a internet usando um protocolo chamado NAT (Network Address Translation).





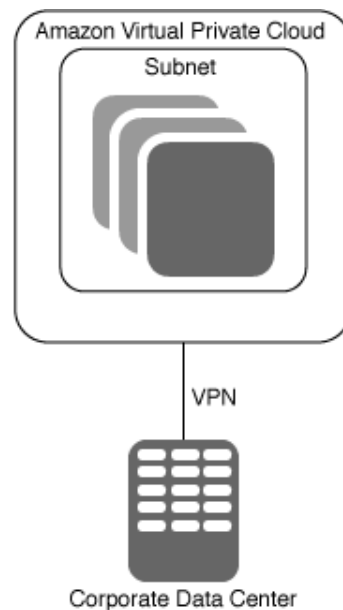
VPC com sub-redes públicas e privadas, e acesso VPN via hardware

Essa configuração adiciona uma conexão VPN (Virtual Private Network) entre a VPC e um data center em potencial. Dessa forma, as bases são configuradas para estender o centro de computação para a nuvem, proporcionando acesso direto à Internet para as instâncias conectadas à sub-rede pública.



VPC com sub-redes privadas e acesso VPN via hardware

Neste modelo de VPC, as instâncias são executadas em um espaço privado, em uma seção isolada da nuvem AWS com uma sub-rede privada, o que tornará as instâncias conectadas a ela inacessíveis pela internet. Você pode conectar esse tipo de VPC a uma rede corporativa por meio de uma VPN (Virtual Private Network) e tornar os serviços hospedados na VPC acessíveis por meio dela.



O que é uma sub-rede? E o que significa ser público ou privado?

Dentro dessa grande rede, temos que encontrar uma maneira de definir segmentos, idealmente com diferentes finalidades, por exemplo, hospedagem de servidores front-end. Cada um desses segmentos ou divisões da rede que a VPC representa é chamado de sub-rede.

Existem dois tipos, público e privado. No caso dos Privados, as instâncias que ali conectarmos poderão conversar entre si e se comunicar com a internet através de um protocolo chamado NAT. Basicamente, o que isso significa é que qualquer comunicação com recursos que residam fora da sub-rede privada deve ser iniciada a partir de um recurso conectado a essa sub-rede.

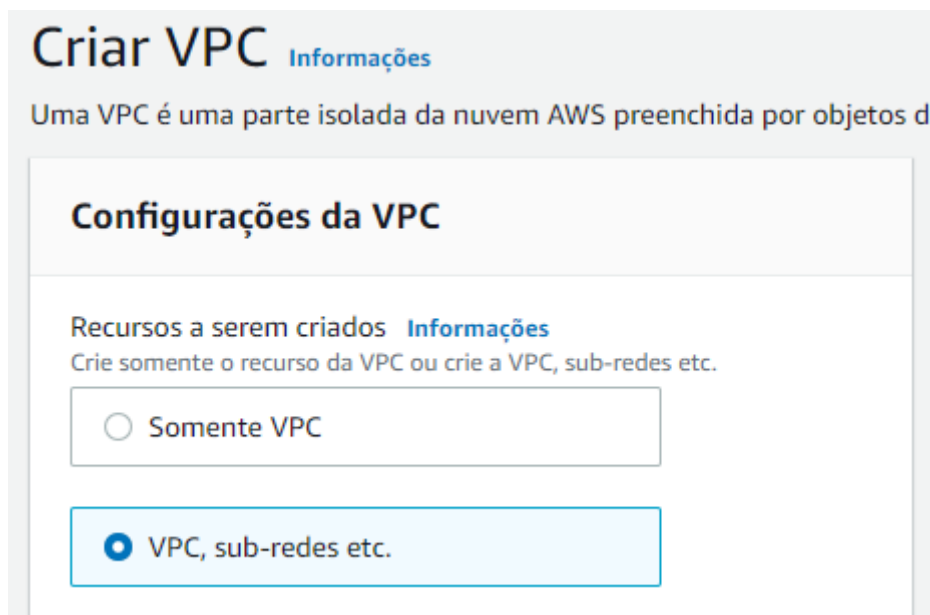
E as sub-redes públicas podem hospedar recursos que são roteáveis (se atribuirmos a eles um endereço IP público que permita) da Internet.

Bem, continuamos...

- 4) Na parte superior da página, encontraremos um botão chamado 'Launch VPC Wizard' (Iniciar assistente da VPC).

Iniciar assistente da VPC

- 5) Na primeira etapa do assistente, devemos escolher o tipo de VPC a ser criada. No nosso caso, selecionamos "VPC, sub-redes etc". Clicamos em 'Selecionar'.



Criar VPC [Informações](#)

Uma VPC é uma parte isolada da nuvem AWS preenchida por objetos d...

Configurações da VPC

Recursos a serem criados [Informações](#)
Crie somente o recurso da VPC ou crie a VPC, sub-redes etc.

☐ Somente VPC

☒ VPC, sub-redes etc.



6) Na próxima etapa, vamos configurar alguns aspectos da VPC:

Configurações da VPC

Recursos a serem criados [Informações](#)
Crie somente o recurso da VPC ou crie a VPC, sub-redes etc.

☐ Somente VPC

☒ VPC, sub-redes etc.

Geração automática da etiqueta de nome [Informações](#)
Insira um valor para a etiqueta de nome. Esse valor será usado para gerar automaticamente etiquetas de nome para todos os recursos na VPC.

☒ Gerar automaticamente

Bloco CIDR IPv4 [Informações](#)
Determine o IP inicial e o tamanho da VPC usando notação CIDR.

172.16.0.0/16 65.536 IPs

Bloco CIDR IPv6 [Informações](#)

☒ Nenhum bloco CIDR IPv6

☐ Bloco CIDR IPv6 fornecido pela Amazon

Localização [Informações](#)

Padrão ▼



Zonas de disponibilidade (AZs) [Informações](#)

Escolha o número de AZs em que as sub-redes deverão ser provisionadas. Para alta disponibilidade, recomendamos pelo menos duas AZs.

1	2	3
---	---	---

► Personalizar AZs

Número de sub-redes públicas [Informações](#)

O número de sub-redes públicas a serem adicionadas à sua VPC. Use sub-redes públicas para aplicações Web que precisam estar publicamente acessíveis pela Internet.

0	1
---	---

► Personalizar blocos CIDR de sub-redes públicas

Número de sub-redes privadas [Informações](#)

O número de sub-redes privadas a serem adicionadas à sua VPC. Use sub-redes privadas para proteger recursos de backend que não precisam de acesso público.

0	1	2
---	---	---

Gateways NAT (USD) [Informações](#)

Escolha o número de zonas de disponibilidade (AZs) em que os gateways NAT serão criados.

Nenhuma	Em 1 AZ	1 por AZ
---------	---------	----------

Endpoints da VPC [Informações](#)

Os endpoints podem ajudar a reduzir as cobranças do gateway NAT e melhorar a segurança acessando o S3 diretamente da VPC. Por padrão, a política de acesso integral será usada. Você pode personalizar essa política a qualquer momento.

Nenhuma	Gateway do S3
---------	---------------

Vamos selecionar 1 AZ, uma sub-rede pública, nenhuma privada e nenhuma Gateway NAT e Endpoint.

Nosso projeto ficará assim:





Nas configurações, encontraremos:

















Configuração	Descrição	Valores para usar
IPv4 Bloco CIDR	O bloco de endereços IP que a VPC vai usar. Isso pode ser consumido por uma única sub-rede ou dividido em várias sub-redes.	Vamos configurá-lo como: 172.16.0.0/16
Bloco CIDR IPv6	Caso queira definir um conjunto de endereços IPv6 para nossa VPC, podemos usar esta configuração.	Para simplificar, vamos definir esta configuração como: 'No IPv6 CIDR Block'
VPC	O nome da VPC, para que possamos encontrá-la no futuro quando quisermos realizar tarefas de administração ou conectar dispositivos a ela.	Cada equipe define seu próprio nome para a VPC. Dica: evite espaços e caracteres especiais.
CIDR IPv4 da sub-rede pública	O bloco de endereços IP que vamos consumir para nossa sub-rede a partir do espaço IP definido para toda a VPC.	Para o exercício em questão, vamos definir este valor como 172.16.0.0/20.
Zona de disponibilidade A	AWS nos permite definir uma preferência de como nossa VPC deve se comportar em caso de interrupção do serviço no data center da AWS onde ela está hospedada.	Para simplificar o exercício, vamos definir esta configuração como: 'Sem preferência'.

Endpoints de serviço	Esse recurso permite estabelecer conectividade via VPC com serviços do tipo PaaS.	Para nosso exercício, não vamos configurar nenhum ponto de extremidade de serviço.
Habilitar nomes de host DNS	Permite atribuir nomes DNS públicos às instâncias que possuem um IP público configurado e estão conectadas a esta sub-rede.	Esta opção deve ser definida como 'Sim'.

- 7) Após o preenchimento do formulário, clicamos em 'Criar VPC'.
- 8) Assim que o processo de criação da VPC estiver concluído, devemos ver uma mensagem como a seguinte:

 **Êxito**

 **Detalhes**

-  Criar VPC: [vpc-0142fb63fb3c03760](#) 
-  Disable DNS hostnames
-  Enable DNS resolution
-  Verifying VPC creation: [vpc-0142fb63fb3c03760](#) 
-  Create subnet: [subnet-0c46973bf5777b3d2](#) 
-  Create internet gateway: [igw-0b78381b00fcf0442](#) 
-  Attach internet gateway to the VPC
-  Create route table: [rtb-0ca3110b7d422a29b](#) 
-  Create route
-  Associate route table
-  Verifying route table creation

- 9) Ao final da configuração retornaremos à tela onde estão listadas todas as VPCs criadas para nossa conta AWS. Neste ponto, podemos considerar o exercício de criação da VPC concluído com sucesso, porém agora devemos criar uma instância para que possamos testar a nossa VPC e seu funcionamento.

Podemos criar uma Instância Linux e nele Instalar o Docker, após podemos fazer alguns testes.