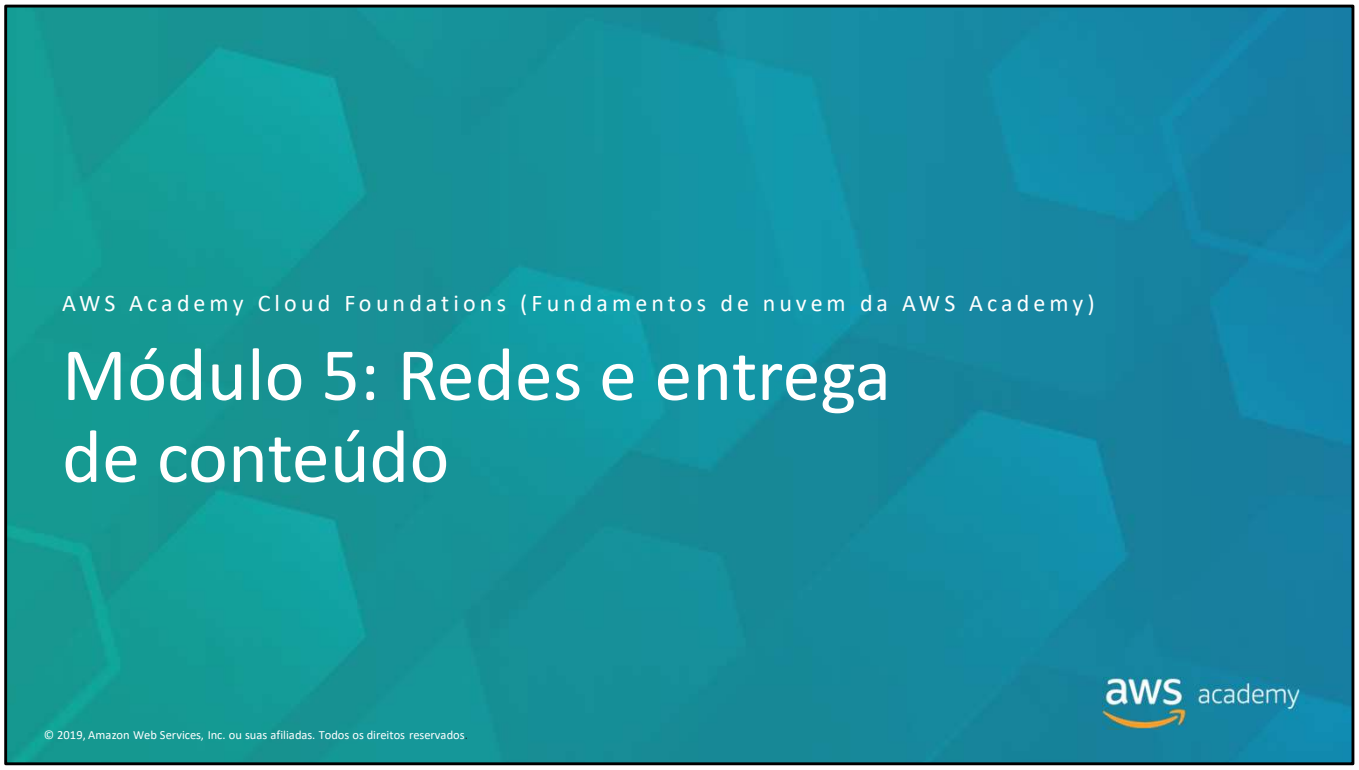


Bem-vindo ao Módulo 5: Redes e entrega de conteúdo

Este módulo abrange três Amazon Web Services (AWS) fundamentais para entrega de conteúdo e redes: Amazon Virtual Private Cloud (Amazon VPC), Amazon Route 53 e Amazon CloudFront.

Visão geral do módulo

aws academy

Tópicos

- Noções básicas de redes
- Amazon VPC
- Redes da VPC
- Segurança da VPC
- Amazon Route 53
- Amazon CloudFront

Atividades

- Rotular um diagrama de rede
- Projetar uma arquitetura básica de VPC

Demonstração

- Demonstração da VPC

Laboratório

- Crie uma VPC e inicie um servidor Web

Teste de conhecimento

Este módulo aborda os seguintes tópicos:

- Noções básicas de redes
- Amazon Virtual Private Cloud (Amazon VPC)
- Redes da VPC
- Segurança da VPC
- Amazon Route 53
- Amazon CloudFront

Este módulo inclui algumas atividades que desafiam você a rotular um diagrama de rede e projetar uma arquitetura básica de VPC.

Você assistirá a uma demonstração gravada para saber como usar o assistente de VPC para criar uma VPC com sub-redes públicas e privadas.

Em seguida, você terá a chance de aplicar o que aprendeu em um laboratório prático em que usa o assistente de VPC para criar uma VPC e iniciar um servidor web.

Por fim, você deverá concluir um teste de conhecimento que será usado para avaliar sua compreensão dos principais conceitos abordados neste módulo.

Objetivos do módulo

Depois de concluir este módulo, você deverá ser capaz de:

- Reconhecer os conceitos básicos de redes
- Descrever as redes virtuais na nuvem com a Amazon VPC
- Rotular um diagrama de rede
- Projetar uma arquitetura básica de VPC
- Indicar as etapas para criar uma VPC
- Identificar grupos de segurança
- Criar sua própria VPC e incluir outros componentes nela para produzir uma rede personalizada
- Identificar os fundamentos do Amazon Route 53
- Reconhecer os benefícios do Amazon CloudFront

Depois de concluir este módulo, você deverá ser capaz de:

- Reconhecer os conceitos básicos de redes
- Descrever as redes virtuais na nuvem com a Amazon VPC
- Rotular um diagrama de rede
- Projetar uma arquitetura básica de VPC
- Indicar as etapas para criar uma VPC
- Identificar grupos de segurança
- Criar sua própria VPC e incluir outros componentes nela para produzir uma rede personalizada
- Identificar os fundamentos do Amazon Route 53
- Reconhecer os benefícios do Amazon CloudFront

Módulo 5: Redes e entrega de conteúdo

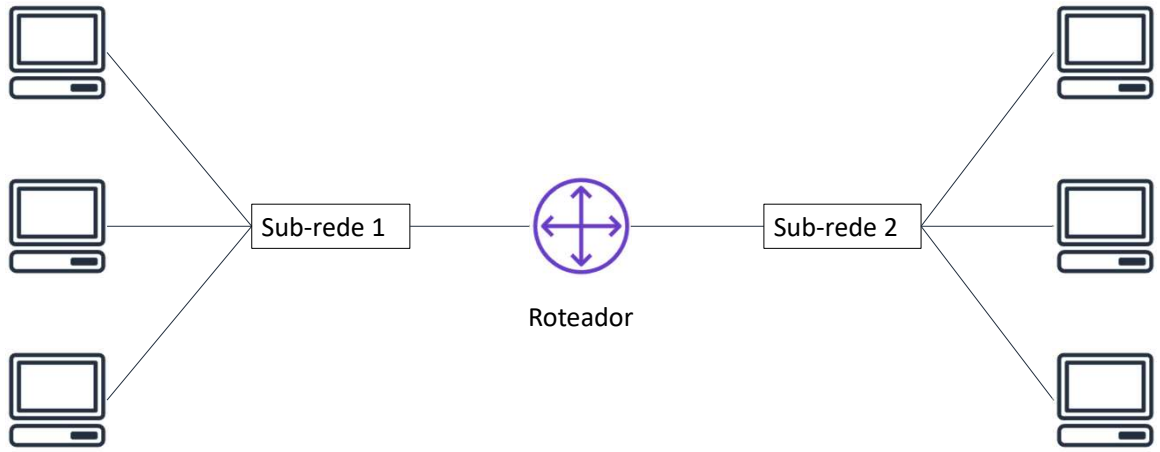
Seção 1: Noções básicas de redes

aws academy

Seção 1: Noções básicas de redes

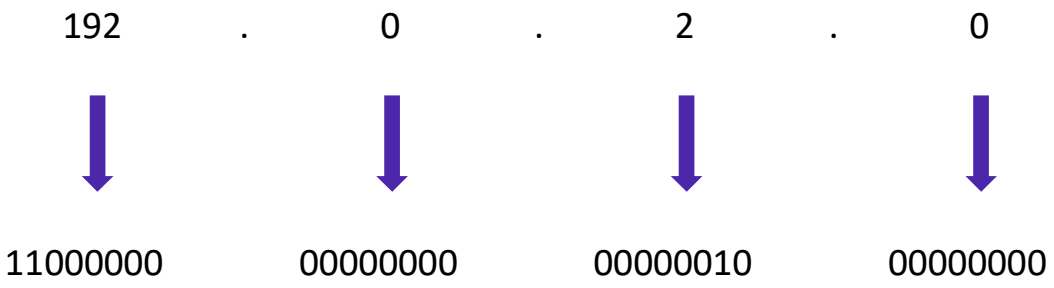
Nesta seção, você analisará alguns conceitos básicos de redes que fornecem a base necessária para a compreensão do serviço de rede da AWS, Amazon Virtual Private Cloud (Amazon VPC).

Redes



Uma *rede de* computadores são duas ou mais máquinas cliente conectadas para compartilhar recursos. Uma rede pode ser particionada logicamente em *sub-redes*. A rede requer um dispositivo de rede (como um roteador ou switch) para conectar todos os clientes e permitir a comunicação entre eles.

Endereços IP



Cada máquina cliente em uma rede tem um endereço IP (Internet Protocol) exclusivo que o identifica. Um endereço IP é um rótulo numérico em formato decimal. As máquinas convertem esse número decimal em um formato binário.

Neste exemplo, o endereço IP é 192.0.2.0. Cada um dos quatro números separados por pontos (.) do endereço IP representa 8 bits no formato de número octal. Isso significa que cada um dos quatro números pode ser de 0 a 255. O total combinado dos quatro números para um endereço IP é 32 bits no formato binário.

Endereços IPv4 e IPv6

Endereço IPv4 (32 bits): 192.0.2.0

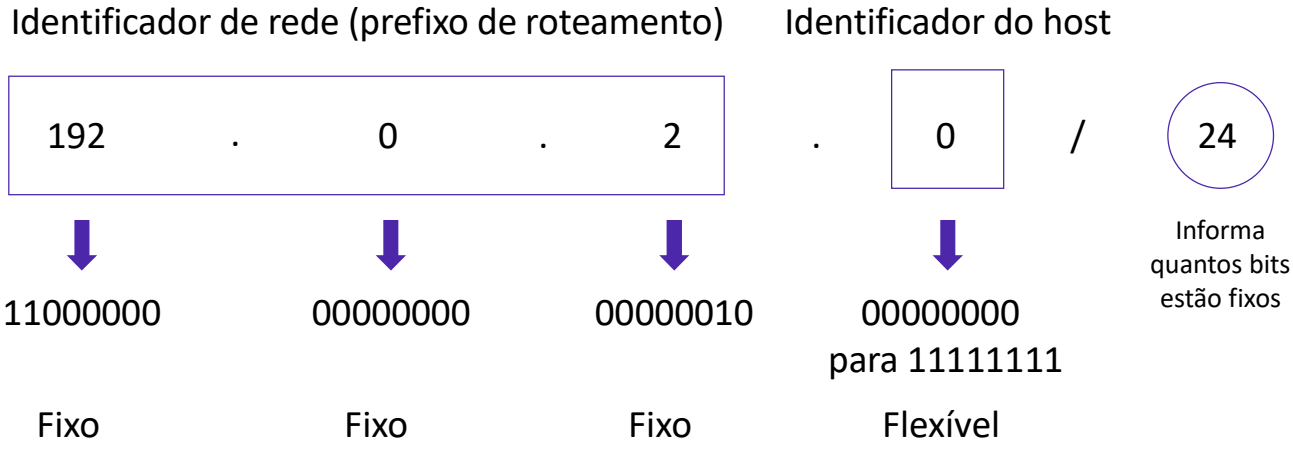
Endereço IPv6 (128 bits): 2600:1f18:22ba:8c00:ba86:a05e:a5ba:00FF

Um endereço IP de 32 bits é chamado de endereço IPv4.

Endereços IPv6, com 128 bits, também estão disponíveis. Endereços IPv6 podem acomodar mais dispositivos do usuário.

Um endereço IPv6 é composto de oito grupos de quatro letras e números separados por dois pontos (:). Neste exemplo, o endereço IPv6 é 2600:1f18:22ba:8c00:ba86:a05e:a5ba:00FF. Cada um dos oito grupos separados por dois pontos do endereço IPv6 representa 16 bits no formato de número hexadecimal. Isso significa que cada um dos oito grupos pode ser qualquer coisa de 0 a FFFF. O total combinado dos oito grupos para um endereço IPv6 é 128 bits no formato binário.

Roteamento sem classe entre domínios (CIDR)



Um método comum para descrever redes é o Classless Inter-Domain Routing (CIDR - Roteamento sem classe entre domínios). O endereço CIDR é expresso da seguinte forma:

- Um endereço IP (que é o primeiro endereço da rede)
- Em seguida, um caractere de barra (/)
- Finalmente, um número que informa quantos bits do prefixo de roteamento devem ser corrigidos ou alocados para o identificador de rede

Os bits que não são fixos podem ser alterados. CIDR é uma maneira de expressar um grupo de endereços IP consecutivos entre si.

Neste exemplo, o endereço CIDR é 192.0.2.0/24. O último número (24) mostra que os primeiros 24 bits devem ser corrigidos. Os últimos 8 bits são flexíveis, o que significa que 2^8 (ou 256) endereços IP estão disponíveis para a rede, que variam de 192.0.2.0 a 192.0.2.255. O quarto dígito decimal tem permissão para mudar de 0 para 255.

Se o CIDR foi 192.0.2.0/16, o último número (16) informa que os primeiros 16 bits devem ser corrigidos. Os últimos 16 bits são flexíveis, o que significa que 2^{16} (ou 65.536) endereços IP estão disponíveis para a rede, variando de 192.0.0.0 a 192.0.255.255. O terceiro e quarto dígitos decimais podem mudar de 0 para 255.

Há dois casos especiais:

- Endereços IP fixos, em que cada bit é fixo, representam um único endereço IP (por exemplo, *192.0.2.0/32*). Esse tipo de endereço é útil quando você deseja configurar uma regra de firewall e conceder acesso a um host específico.
- A Internet, em que cada bit é flexível, é representada como 0.0.0.0/0

Modelo Open Systems Interconnection (OSI - Interconexão de sistemas abertos)

Camada	Número	Função	Protocolo/endereço
Aplicativo	7	Meios para um aplicativo acessar uma rede de computadores	HTTP(S), FTP, DHCP, LDAP
Apresentação	6	• Garante que a camada do aplicativo possa ler os dados • Criptografia	ASCI, ICA
Sessão	5	Permite a troca ordenada de dados	NetBIOS, RPC
rede/	4	Fornece protocolos para oferecer suporte à comunicação host a host	TCP, UDP
Rede	3	Roteamento e encaminhamento de pacotes (roteadores)	IP
Link de dados	2	Transferir dados na mesma rede LAN (hubs e switches)	MAC
Físico	1	Transmissão e recepção de fluxo de bits brutos em um meio físico	Sinais (1s e 0s)

O modelo Open Systems Interconnection (OSI - Interconexão de sistemas abertos) é um modelo conceitual usado para explicar como os dados viajam por uma rede. Consiste em sete camadas e mostra os protocolos e endereços comuns que são usados para enviar dados em cada camada. Por exemplo, hubs e switches funcionam na camada 2 (a camada de link de dados). Os roteadores funcionam na camada 3 (a camada de rede). O modelo OSI também pode ser usado para entender como a comunicação ocorre em uma nuvem privada virtual (VPC), que você aprenderá na próxima seção.

Módulo 5: Redes e entrega de conteúdo

Seção 2: Amazon VPC

aws academy

Seção 2: Amazon VPC

Muitos dos conceitos de uma rede local se aplicam a uma rede baseada na nuvem, mas boa parte da complexidade da configuração de uma rede foi abstraída sem sacrificar o controle, a segurança e a usabilidade. Nesta seção, você aprenderá sobre a Amazon VPC e os componentes fundamentais de uma VPC.

Amazon VPC

Amazon VPC

- Permite provisionar uma seção **isolada logicamente** da Nuvem AWS onde você pode executar recursos da AWS em uma rede virtual que você mesmo define
- Fornece **controle sobre seus recursos de rede virtual**, incluindo:
  - Seleção do intervalo de endereços IP
  - Criação de sub-redes
  - Configuração de tabelas de rotas e gateways de rede
- Permite **personalizar a configuração de rede** para sua VPC
- Permite usar **várias camadas de segurança**

O Amazon Virtual Private Cloud (Amazon VPC) é um serviço que permite provisionar uma seção logicamente isolada da Nuvem AWS (chamada de nuvem privada virtual ou VPC) onde você pode executar seus recursos da AWS.

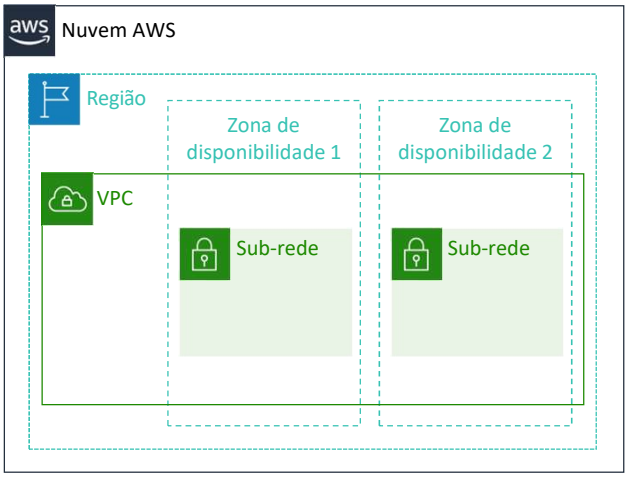
A Amazon VPC oferece controle sobre seus recursos de rede virtual, incluindo a seleção do seu próprio intervalo de endereços IP, a criação de sub-redes e a configuração de tabelas de rotas e gateways de rede. Você pode usar IPv4 e IPv6 na VPC para acesso seguro a recursos e aplicativos.

Você também pode personalizar a configuração de rede para sua VPC. Por exemplo, você pode criar uma sub-rede pública para seus servidores web que podem acessar a Internet pública. Você pode colocar seus sistemas de back-end (como bancos de dados ou servidores de aplicativos) em uma sub-rede privada sem acesso público à Internet.

Por fim, você pode usar várias camadas de segurança, incluindo grupos de segurança e listas de controle de acesso à rede (ACLs de rede), para ajudar a controlar o acesso às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em cada sub-rede.

VPCs e sub-redes

- VPCs:
  - **Logicamente isoladas** de outras VPCs
  - **Dedicadas** à sua conta da AWS
  - Pertencem a uma única **região da AWS** e podem abranger várias zonas de disponibilidade
- Sub-redes:
  - **Intervalo de endereços IP** que dividem uma VPC
  - Pertencem a uma única **zona de disponibilidade**
  - Classificadas como **públicas** ou **privadas**

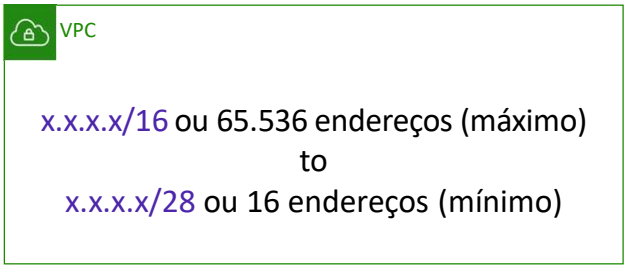


A Amazon VPC permite provisionar nuvens privadas virtuais (VPCs). Uma *VPC* é uma rede virtual isolada logicamente de outras redes virtuais na Nuvem AWS. Uma VPC é dedicada à sua conta. As VPCs pertencem a uma única região da AWS e podem abranger várias zonas de disponibilidade.

Depois de criar uma VPC, você pode dividi-la em uma ou mais sub-redes. Uma *sub-rede* é um intervalo de endereços IP em uma VPC. As sub-redes pertencem a uma única zona de disponibilidade. Você pode criar sub-redes em diferentes zonas de disponibilidade para alta disponibilidade. As sub-redes geralmente são classificadas como públicas ou privadas. *As sub-redes públicas* têm acesso direto à Internet, mas as *sub-redes privadas* não têm.

Endereçamento IP

- Ao criar uma VPC, você a atribui a um **bloco CIDR** IPv4 (intervalo de endereços IPv4 **privados**).
- Você **não pode alterar o intervalo de endereços** depois de criar a VPC.
- O **maior** tamanho de bloco CIDR IPv4 é **/16**.
- O **menor** tamanho do bloco CIDR IPv4 é **/28**.
- O IPv6 também é compatível (com um limite de tamanho de bloco diferente).
- Os blocos CIDR de sub-redes **não podem se sobrepor**.



Os endereços IP permitem que os recursos em sua VPC se comuniquem entre si e com recursos pela Internet. Ao criar uma VPC, você atribui um bloco CIDR IPv4 (um intervalo de endereços IPv4 *privados*) a ela. Depois de criar uma VPC, você não poderá alterar o intervalo de endereços, portanto, é importante escolhê-lo com cuidado. O bloco CIDR IPv4 pode ser tão grande quanto/16 (que é 2^{16}, ou 65.536 endereços) ou tão pequeno quanto/28 (que é 2^4, ou 16 endereços).

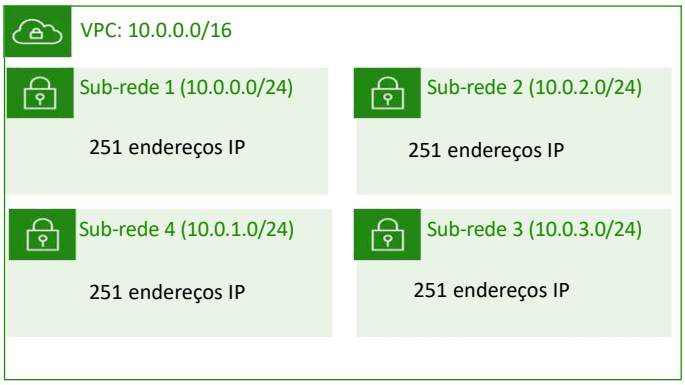
Como opção, você pode associar um bloco CIDR IPv6 a sua VPC e sub-redes e atribuir endereços IPv6 desse bloco a recursos em sua VPC. Os blocos CIDR IPv6 têm um limite de tamanho de bloco diferente.

O bloco CIDR de uma sub-rede pode ser o mesmo que o bloco CIDR de uma VPC. Nesse caso, a VPC e a sub-rede têm o mesmo tamanho (uma única sub-rede na VPC). Além disso, o bloco CIDR de uma sub-rede pode ser um subconjunto do bloco CIDR da VPC. Essa estrutura permite a definição de várias sub-redes. Se você criar mais de uma sub-rede em uma VPC, os blocos CIDR das sub-redes não podem se sobrepor. Você não pode ter endereços IP duplicados na mesma VPC.

Para saber mais sobre o endereçamento IP em uma VPC, consulte a Documentação da AWS.

Endereços IP reservados

Exemplo: uma VPC com um bloco CIDR IPv4 de 10.0.0.0/16 tem 65.536 endereços IP no total. A VPC tem quatro sub-redes de tamanho igual. Somente 251 endereços IP estão disponíveis para uso por cada sub-rede.



Endereços IP para o bloco CIDR 10.0.0.0/24	Reservado para
10.0.0.0	Endereço de rede
10.0.0.1	Comunicação interna
10.0.0.2	Resolução do Domain Name System (DNS)
10.0.0.3	Uso futuro
10.0.0.255	Endereço de transmissão de rede

Quando você cria uma sub-rede, ela requer seu próprio bloco CIDR. Para cada bloco CIDR que você especificar, a AWS reserva cinco endereços IP dentro desse bloco, e esses endereços não estão disponíveis para uso. A AWS reserva esses endereços IP para:

- Endereço de rede
- Roteador local da VPC (comunicações internas)
- Resolução do Domain Name System (DNS)
- Uso futuro
- Endereço de transmissão de rede

Por exemplo, suponha que você crie uma sub-rede com um bloco CIDR IPv4 de 10.0.0.0/24 (que tem um total de 256 endereços IP). A sub-rede tem 256 endereços IP, mas apenas 251 estão disponíveis porque cinco são reservados.

Tipos de endereços IP públicos

aws academy

Endereço IPv4 público

- Atribuído manualmente por meio de um endereço IP elástico
- Atribuído automaticamente por meio das configurações de endereço IP público de atribuição automática no nível da sub-rede

Endereço IP elástico

- Associado a uma conta da AWS
- Pode ser alocado e remapeado a qualquer momento
- Custos adicionais podem ser aplicados

Quando você cria uma VPC, cada instância nessa VPC obtém um endereço IP privado automaticamente. Você também pode solicitar que um endereço IP público seja atribuído ao criar a instância modificando as propriedades do endereço IP público de atribuição automática da sub-rede.

Um *endereço IP elástico* é um endereço IPv4 estático e público projetado para computação em nuvem dinâmica. Você pode associar um endereço IP elástico a qualquer instância ou interface de rede para qualquer VPC em sua conta. Com um endereço IP elástico, você pode mascarar a falha de uma instância remapeando rapidamente o endereço para outra instância na VPC. Associar o endereço IP elástico à interface de rede tem uma vantagem sobre associá-lo diretamente à instância. Você pode mover todos os atributos da interface de rede de uma instância para outra em uma única etapa.

Custos adicionais podem ser aplicados quando você usa endereços IP elásticos, portanto, é importante liberá-los quando você não precisar mais deles.

Para saber mais sobre endereços IP elásticos, consulte Endereços IP elásticos na documentação da AWS.

Interface de rede elástica

- Uma interface de rede elástica é uma **interface de rede virtual** que você pode:
  - Anexar a uma instância.
  - Separar da instância e anexar a outra instância para redirecionar o tráfego de rede.
- Seus **atributos a seguem** quando são reanexadas a uma nova instância.
- Cada instância em sua VPC tem uma **interface de rede padrão** que recebe um endereço IPv4 privado do intervalo de endereços IPv4 de sua VPC.

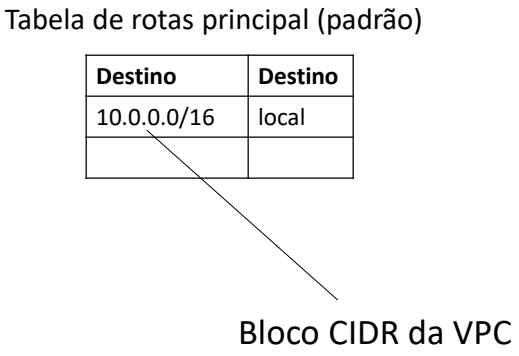
Uma *interface de rede elástica* é uma interface de rede virtual que você pode anexar ou desanexar de uma instância em uma VPC. Os atributos de uma interface de rede a seguem quando ela é reanexada a outra instância. Quando você move uma interface de rede de uma instância para outra, o tráfego de rede é redirecionado para a nova instância.

Cada instância na VPC possui uma interface de rede padrão (a interface de rede primária) à qual está atribuído um endereço IPv4 privado do intervalo de endereços IPv4 da VPC. Não é possível separar uma interface de rede primária de uma instância. Você pode criar e anexar uma interface de rede adicional a qualquer instância da VPC. O número de interfaces de rede que você pode anexar varia de acordo com o tipo de instância.

Para obter mais informações sobre interfaces de rede elástica, consulte a Documentação da AWS.

Tabelas de rotas e rotas

- Uma **tabela de rotas** contém um conjunto de regras (ou rotas) que **você pode configurar** para direcionar o tráfego de rede da sub-rede.
- Cada **rota** especifica um destino e um destino.
- Por padrão, toda tabela de rotas contém uma **rota local** para comunicação dentro da VPC.
- Cada **sub-rede deve estar associada a uma tabela de rotas** (no máximo uma).



Uma *tabela de rotas* contém um conjunto de regras (chamadas *rotas*) que direciona o tráfego de rede da sua sub-rede. Cada rota especifica um *destino* e um *destino*. O *destino* é o bloco CIDR de destino para onde você deseja que o tráfego da sua sub-rede vá. O *destino* é o destino pelo qual o tráfego de destino é enviado. Por padrão, cada tabela de rotas que você cria contém uma *rota local* para comunicação na VPC. Você pode personalizar tabelas de rotas adicionando rotas. Você não pode excluir a entrada de rota local usada para comunicações internas.

Toda sub-rede em sua VPC deve ser associada a uma tabela de rotas. A *tabela de rotas principal* é a tabela de rotas atribuída automaticamente à sua VPC. Ela controla o roteamento de todas as sub-redes que não estejam explicitamente associadas a outra tabela de rotas. Uma sub-rede só pode ser associada a uma única tabela de rotas por vez, mas é possível associar várias sub-redes a uma mesma tabela de rotas.

Para saber mais sobre tabelas de rotas, consulte a Documentação da AWS.

Principais lições da Seção 2

- Uma VPC é uma seção isolada logicamente da Nuvem AWS.
- Uma VPC pertence a uma região e requer um bloco CIDR.
- Uma VPC é subdividida em sub-redes.
- Uma sub-rede pertence a uma zona de disponibilidade e requer um bloco CIDR.
- As tabelas de rotas controlam o tráfego de uma sub-rede.
- As tabelas de rotas têm uma rota local integrada.
- Você adiciona outras rotas à tabela.
- Não é possível excluir a rota local.

Algumas das principais lições desta seção do módulo são:

- Uma VPC é uma seção isolada logicamente da Nuvem AWS.
- Uma VPC pertence a uma região e requer um bloco CIDR.
- Uma VPC é subdividida em sub-redes.
- Uma sub-rede pertence a uma zona de disponibilidade e requer um bloco CIDR.
- As tabelas de rotas controlam o tráfego de uma sub-rede.
- As tabelas de rotas têm uma rota local integrada.
- Você adiciona outras rotas à tabela.
- Não é possível excluir a rota local.

Módulo 5: Redes e entrega de conteúdo

Seção 3: Redes VPC

aws academy

Seção 3: Redes VPC

Agora que você aprendeu sobre os componentes básicos de uma VPC, pode começar a rotear o tráfego de maneiras interessantes. Nesta seção, você aprenderá sobre as diferentes opções de rede.

Gateway da Internet

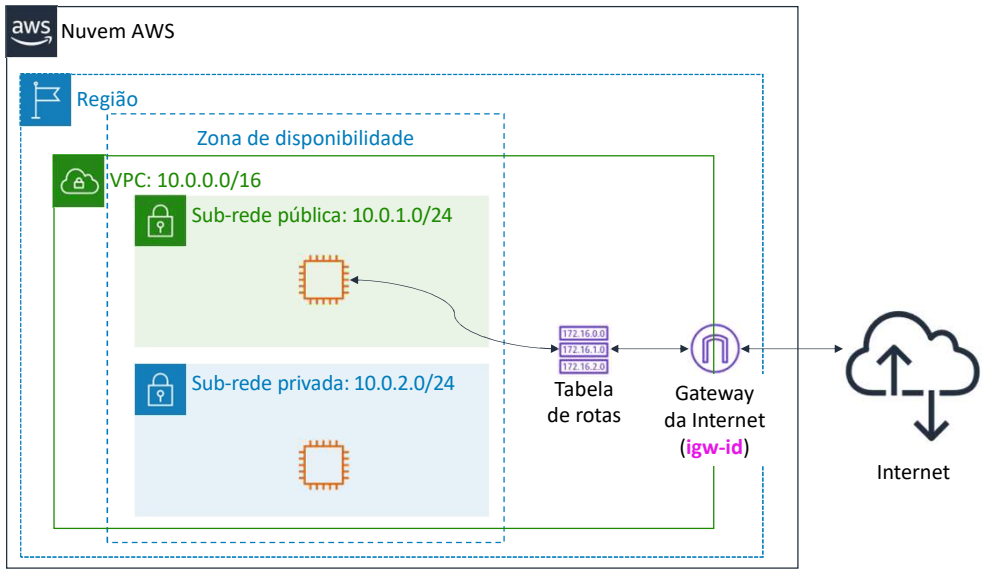


Tabela de rotas da sub-rede pública

Destino	Destino
10.0.0.0/16	local
0.0.0.0/0	igw-id

Um *gateway da Internet* é um componente da VPC escalável, redundante e altamente disponível que permite a comunicação entre instâncias na VPC e a Internet. Um gateway da Internet tem duas finalidades: fornecer um destino nas tabelas de rotas da VPC para tráfego roteável pela Internet e executar a conversão de endereços de rede para instâncias que receberam endereços IPv4 públicos.

Para tornar uma sub-rede *pública*, anexe um *gateway da Internet* à VPC e adicione uma rota à tabela de rotas para enviar tráfego não local por meio do gateway da Internet para a Internet (0.0.0.0/0).

Para obter mais informações sobre gateways da Internet, consulte Gateways da Internet na documentação da AWS.

Gateway de tradução de endereços de rede (NAT)

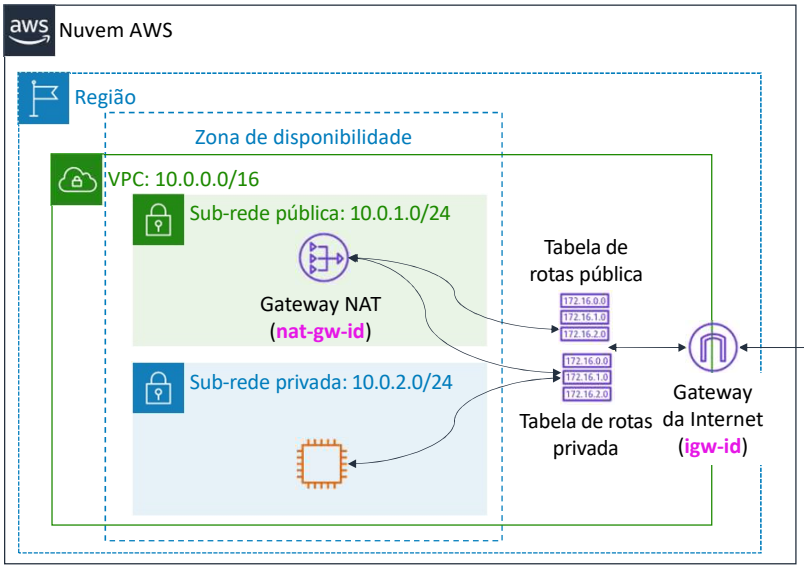


Tabela de rotas da sub-rede pública

Destino	Destino
10.0.0.0/16	local
0.0.0.0/0	igw-id

Tabela de rotas da sub-rede privada

Destino	Destino
10.0.0.0/16	local
0.0.0.0/0	nat-gw-id

Um *gateway de conversão de endereços de rede (NAT)* permite que instâncias em uma sub-rede privada se conectem à Internet ou a outros serviços da AWS, mas impede que a Internet inicie uma conexão com essas instâncias.

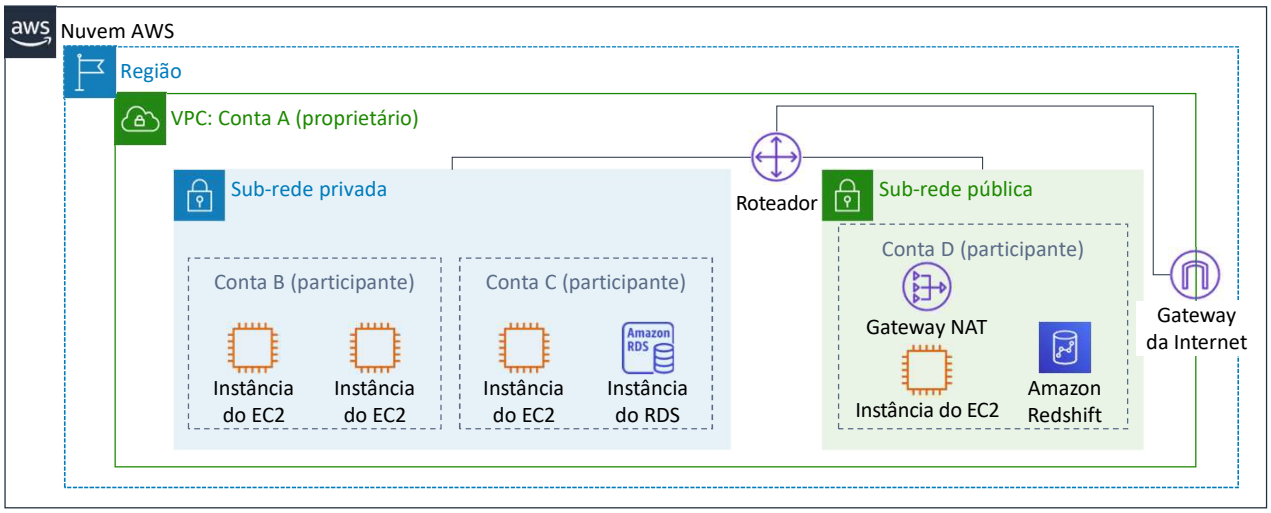
Para criar um gateway NAT, você deve especificar uma sub-rede pública na qual o gateway NAT residirá. É também necessário especificar um endereço IP elástico para associá-lo ao gateway NAT ao criá-lo. Depois de criar um gateway NAT, você deverá atualizar a tabela de rotas associada a uma ou mais de suas sub-redes privadas para apontar o tráfego vinculado à Internet para o gateway NAT. Assim, as instâncias em suas sub-redes privadas podem se comunicar com a Internet.

Você também pode usar uma instância NAT em uma sub-rede pública em sua VPC, em vez de um gateway NAT. No entanto, um gateway NAT é um serviço NAT gerenciado que fornece melhor disponibilidade, maior largura de banda e menos esforço administrativo. Para casos de uso comuns, a AWS recomenda que você use um gateway NAT em vez de uma instância NAT.

Consulte a documentação da AWS para obter mais informações sobre

- Gateways NAT
- Instâncias NAT
- Diferenças entre gateways NAT e instâncias NAT

Compartilhamento da VPC



O compartilhamento de VPC permite que os clientes compartilhem sub-redes com outras contas da AWS na mesma organização no AWS Organizations. O compartilhamento de VPC permite que várias contas da AWS criem recursos de aplicativos, como instâncias do Amazon EC2, bancos de dados do Amazon Relational Database Service (Amazon RDS), clusters do Amazon Redshift e funções do AWS Lambda, em VPCs compartilhadas e gerenciadas de maneira centralizada. Nesse modelo, a conta proprietária da VPC (proprietário) compartilha uma ou mais sub-redes com outras contas (participantes) que pertencem à mesma organização no AWS Organizations. Depois que uma sub-rede é compartilhada, os participantes podem visualizar, criar, modificar e excluir seus recursos de aplicativo nas sub-redes compartilhadas com eles. Os participantes não poderão visualizar, modificar ou excluir recursos pertencentes a outros participantes ou proprietários da VPC.

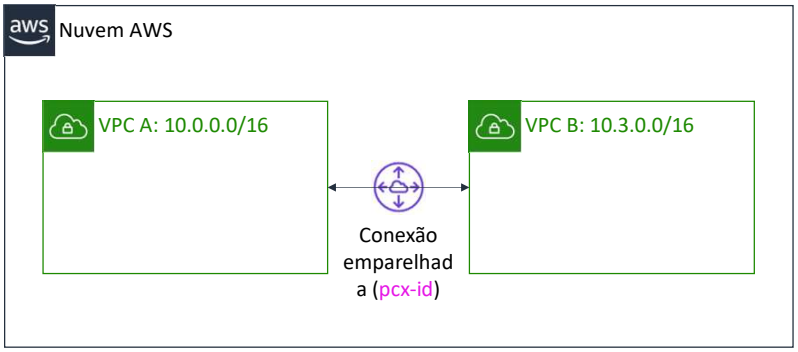
O compartilhamento de VPC oferece vários benefícios:

- Separação de responsabilidades - Estrutura de VPC controlada centralmente, roteamento, alocação de endereços IP
- Propriedade - os proprietários de aplicativos continuam a ter recursos, contas e grupos de segurança
- Grupos de segurança - os participantes do compartilhamento de VPC podem fazer referência aos IDs de grupos de segurança uns dos outros
- Eficiências - densidade mais alta em sub-redes, uso eficiente de VPNs e AWS Direct Connect

- Sem limites rígidos - é possível evitar limites rígidos - por exemplo, 50 interfaces virtuais por conexão do AWS Direct Connect por meio de arquitetura de rede simplificada
- Custos otimizados - os custos podem ser otimizados por meio da reutilização de gateways NAT, endpoints de interface VPC e tráfego dentro da zona de disponibilidade

O compartilhamento de VPC permite dissociar contas e redes. Você tem menos VPCs maiores e gerenciadas centralmente. Aplicativos altamente interconectados se beneficiam automaticamente com essa abordagem.

Emparelhamento de VPC



Você pode conectar VPCs em sua própria conta da AWS, entre contas da AWS ou entre regiões da AWS.

Restrições:
- Espaços IP não podem se sobrepor.
- O emparelhamento transitivo não é compatível.
- Você pode ter apenas um recurso de emparelhamento entre as mesmas duas VPCs.

Tabela de rotas para VPC A

Destino	Destino
10.0.0.0/16	local
10.3.0.0/16	pcx-id

Tabela de rotas para VPC B

Destino	Destino
10.3.0.0/16	local
10.0.0.0/16	pcx-id

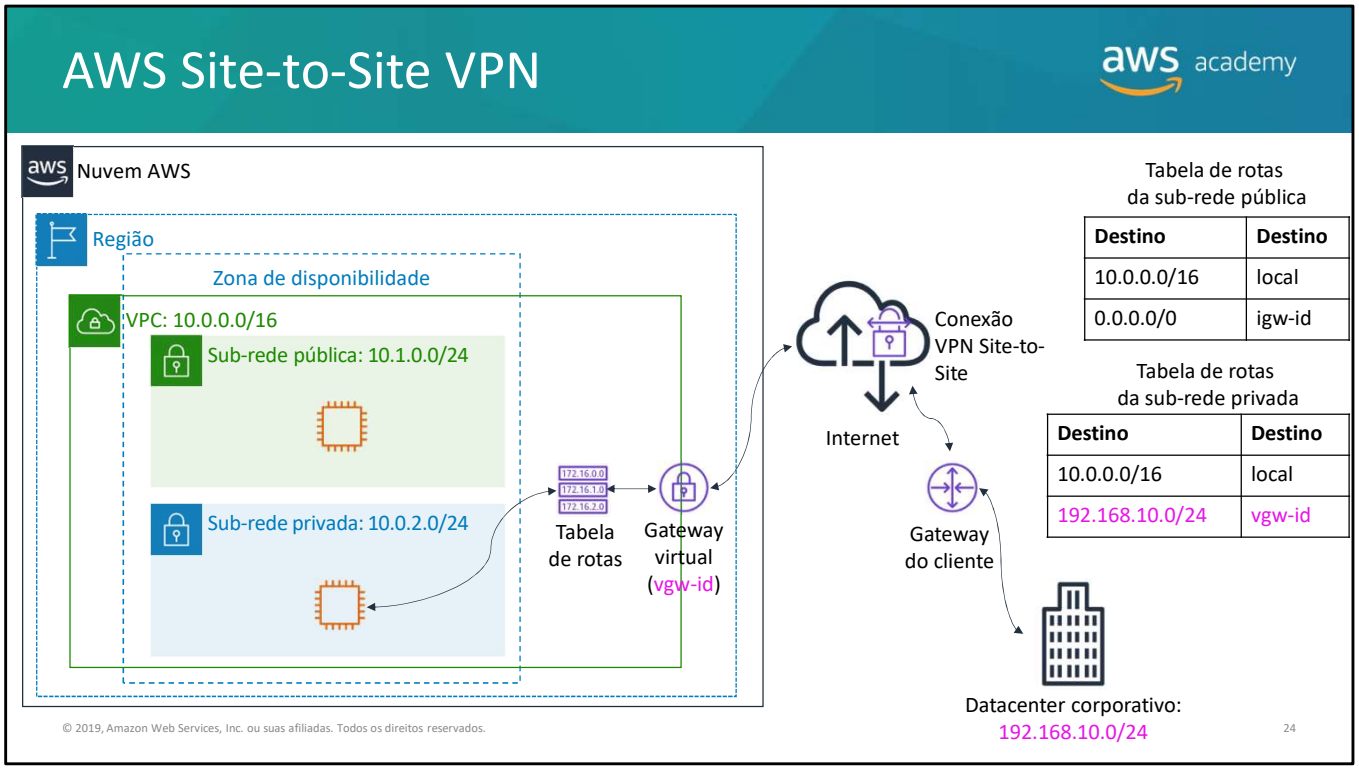
Uma *conexão de emparelhamento de VPC* é uma conexão de rede entre duas VPCs que permite rotear o tráfego entre elas de forma privada. Instâncias em qualquer VPC podem se comunicar umas com as outras como se estivessem na mesma rede. Você pode criar uma conexão de emparelhamento da VPC entre suas próprias VPCs, com uma VPC de outra conta da AWS ou com uma VPC em uma região diferente da AWS.

Ao configurar a conexão de emparelhamento, você cria regras na tabela de rotas para permitir que as VPCs se comuniquem entre si por meio do recurso de emparelhamento. Por exemplo, suponha que você tenha duas VPCs. Na tabela de rotas da VPC A, você define o destino como o endereço IP da VPC B e o destino como o ID do recurso de emparelhamento. Na tabela de rotas da VPC B, você define o destino como o endereço IP da VPC A e o destino como o ID do recurso de emparelhamento.

O emparelhamento de VPC tem algumas restrições:
- Os intervalos de endereços IP não podem se sobrepor.
- O emparelhamento transitivo não é compatível. Por exemplo, suponha que você tenha três VPCs: A, B e C. A VPC A está conectada à VPC B e a VPC A está conectada à VPC C. No entanto, a VPC B *não* está conectada à VPC C implicitamente. Para conectar a VPC B à VPC C, você deve estabelecer explicitamente essa conectividade.

- Você pode ter apenas um recurso de emparelhamento entre as mesmas duas VPCs.

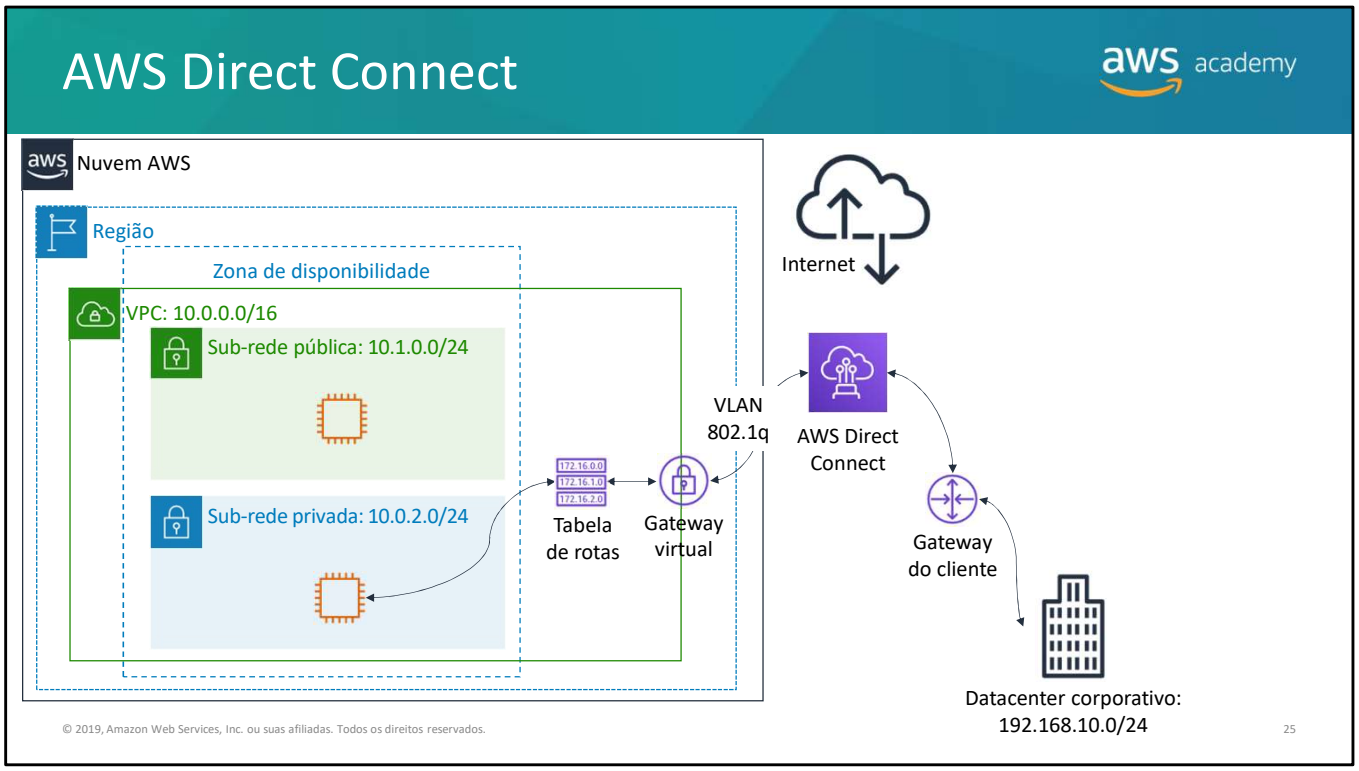
Para obter mais informações sobre o emparelhamento de VPCs, consulte Emparelhamento de VPCs na documentação da AWS.



Por padrão, as instâncias executadas em uma VPC não podem se comunicar com uma rede remota. Para conectar a VPC à rede remota (ou seja, crie uma rede privada virtual ou uma conexão VPN), você:

1. Crie um novo dispositivo de gateway virtual (chamado de *gateway de rede privada virtual (VPN)*) e anexe-o à sua VPC.
2. Defina a configuração do dispositivo VPN ou do *gateway do cliente*. O gateway do cliente não é um dispositivo, mas um recurso da AWS que fornece informações à AWS sobre seu dispositivo VPN.
3. Crie uma tabela de rotas personalizada para apontar o tráfego vinculado ao datacenter corporativo para o gateway VPN. Você também deve atualizar as regras do grupo de segurança. (Você aprenderá sobre grupos de segurança na próxima seção.)
4. Estabeleça uma *conexão Site-to-Site VPN (Site-to-Site VPN) da AWS* para vincular os dois sistemas.
5. Configure o roteamento para passar o tráfego pela conexão.

Para obter mais informações sobre o AWS Site-to-Site VPN e outras opções de conectividade VPN, consulte Conexões VPN na documentação da AWS.



Um dos desafios da comunicação de rede é o desempenho da rede. O desempenho poderá ser afetado negativamente se o datacenter estiver localizado longe da região da AWS. Para essas situações, a AWS oferece o AWS Direct Connect ou o DX. *O AWS Direct Connect* permite estabelecer uma conexão de rede dedicada e privada entre a rede e um dos locais do DX. Essa conexão privada pode reduzir os custos de rede, aumentar a taxa de transferência de largura de banda e fornecer uma experiência de rede mais consistente do que as conexões baseadas na Internet. O DX usa Virtual Local Area Networks (VLANs - Redes locais locais virtuais) 802.1q de padrão aberto.

Para obter mais informações sobre o DX, consulte a página de produto do AWS Direct Connect.

VPC Endpoints

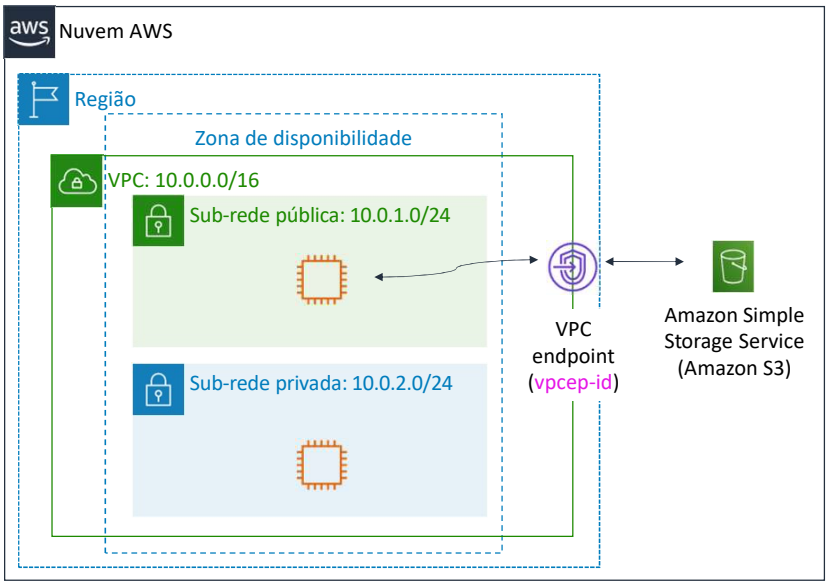


Tabela de rotas da sub-rede pública

Destino	Destino
10.0.0.0/16	local
ID do Amazon S3	vpcep-id

Dois tipos de endpoints:

- Endpoints da **interface** (desenvolvidos pelo AWS PrivateLink)
- Endpoints do **gateway** (Amazon S3 e Amazon DynamoDB)

Um *VPC endpoint* é um dispositivo virtual que permite que você conecte de forma privada sua VPC aos serviços da AWS compatíveis e aos serviços de VPC endpoint desenvolvidos pelo AWS PrivateLink. A conexão com esses serviços não exige um gateway de Internet, um dispositivo NAT, uma conexão VPN ou uma conexão do AWS Direct Connect. As instâncias na sua VPC não exigem 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.

Há dois tipos de VPC endpoints:

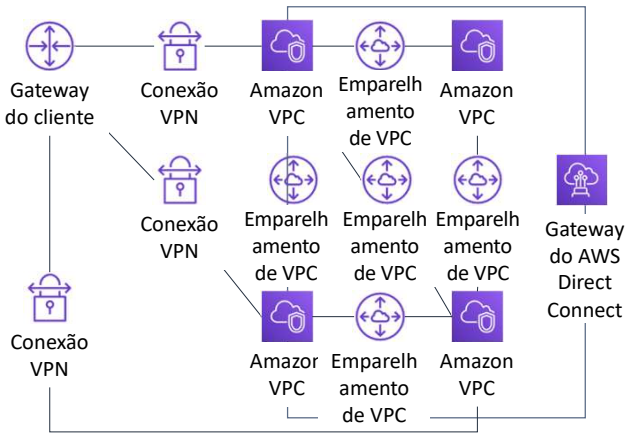
- Um *VPC endpoint* de interface (endpoint de interface) permite que você se conecte a serviços desenvolvidos pelo AWS PrivateLink. Esses serviços incluem alguns serviços da AWS, serviços hospedados por outros clientes da AWS e parceiros da rede de parceiros da AWS (APN) em suas próprias VPCs (chamados de serviços de *endpoint) e serviços* compatíveis de parceiros do APN do AWS Marketplace. O proprietário do serviço é o *provedor de serviços*, e você, como o principal que cria o endpoint da interface, é o *consumidor do serviço*. Você é cobrado pela criação e pelo uso de um endpoint de interface a um serviço. Aplicam-se taxas de uso por hora e de processamento de dados. Consulte a documentação da AWS para obter uma lista de endpoints de interface compatíveis.

- Endpoints de gateway: o uso de endpoints de gateway não incorre em custo adicional. Aplicam-se as cobranças padrão pela transferência de dados e pelo uso de recursos.

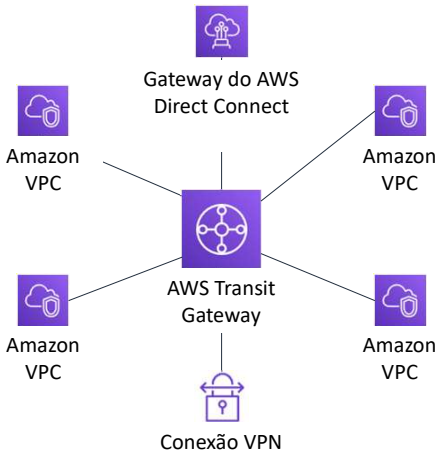
Para obter mais informações sobre VPC endpoints, consulte VPC endpoints na documentação da AWS.

AWS Transit Gateway

Disto...



Para isto...

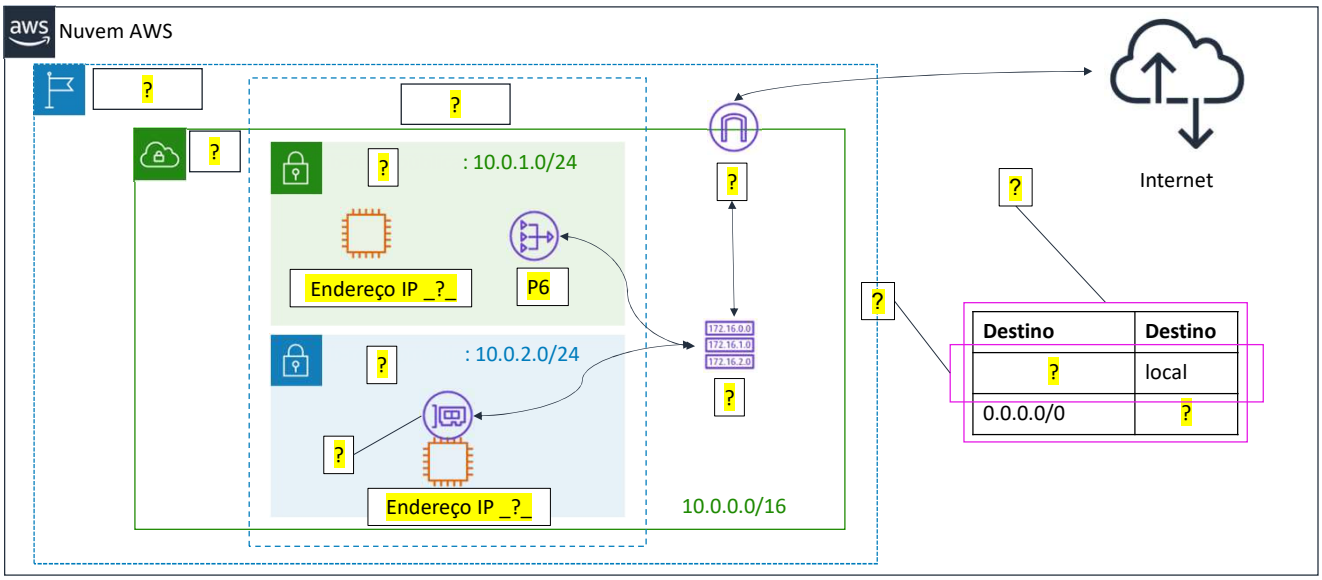


Você pode configurar suas VPCs de várias maneiras e aproveitar várias opções de conectividade e gateways. Essas opções e gateways incluem AWS Direct Connect (via gateways DX), gateways NAT, gateways de Internet, emparelhamento de VPC etc. Não é incomum encontrar clientes da AWS com centenas de VPCs distribuídas entre contas e regiões da AWS para atender a várias linhas de negócios, equipes, projetos e assim por diante. As coisas ficam mais complexas quando os clientes começam a configurar a conectividade entre suas VPCs. Todas as opções de conectividade são estritamente ponto a ponto, portanto, o número de conexões de VPC para VPC pode crescer rapidamente. À medida que aumenta o número de cargas de trabalho executadas na AWS, você deve ser capaz de escalar suas redes em várias contas e VPCs para acompanhar o crescimento.

Embora você possa usar o emparelhamento de VPCs para conectar pares de VPCs, gerenciar a conectividade ponto a ponto em várias VPCs sem a capacidade de gerenciar centralmente as políticas de conectividade pode ser caro e difícil em termos operacionais. Para conectividade local, você deve anexar sua VPN a cada VPC individual. Essa solução pode ser demorada para criar e difícil de gerenciar quando o número de VPCs aumenta para centenas.

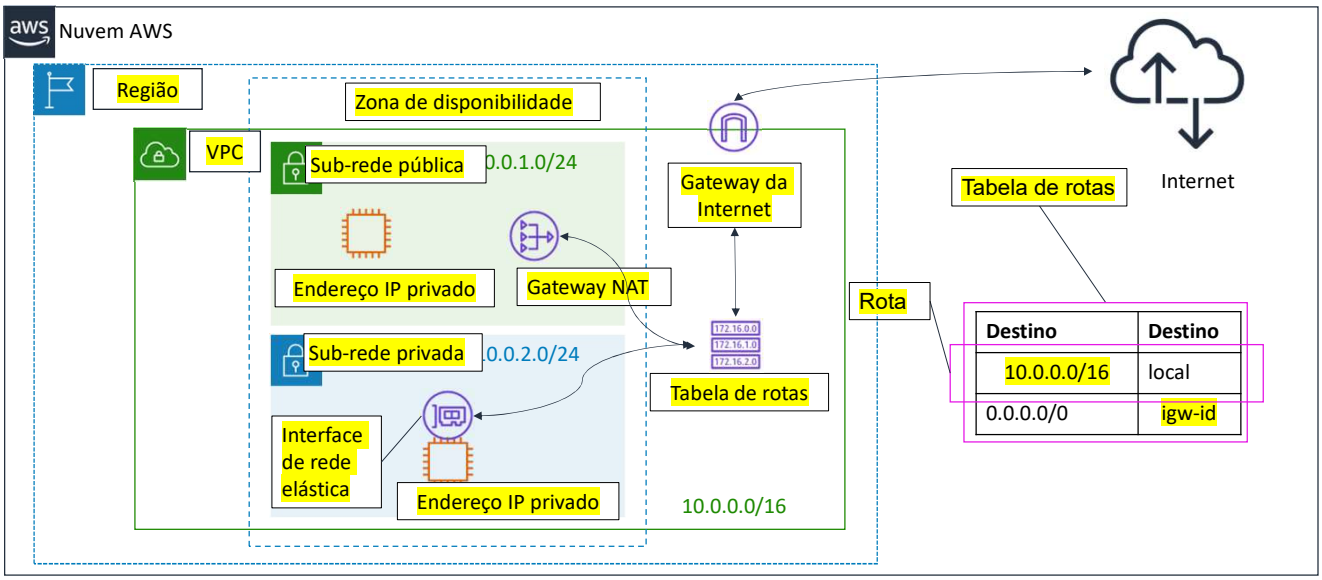
Para resolver esse problema, você pode usar o AWS Transit Gateway para simplificar o modelo de rede. Com o AWS Transit Gateway, você só precisa criar e gerenciar uma única conexão do gateway central para cada VPC, datacenter local ou escritório remoto em toda a rede. O Transit Gateway atua como um hub que controla como o tráfego é roteado entre todas as redes conectadas, que agem como spokes. Este modelo de hub e spoke simplifica significativamente o gerenciamento e reduz os custos operacionais porque cada rede só precisa se conectar ao Transit Gateway e não a todas as outras redes. Qualquer nova VPC é conectada de forma simples ao Transit Gateway e é disponibilizada automaticamente para todas as outras redes conectadas ao Transit Gateway. Essa facilidade de conectividade facilita a escalabilidade da rede para acompanhar sua expansão.

Atividade: rotular este diagrama de rede

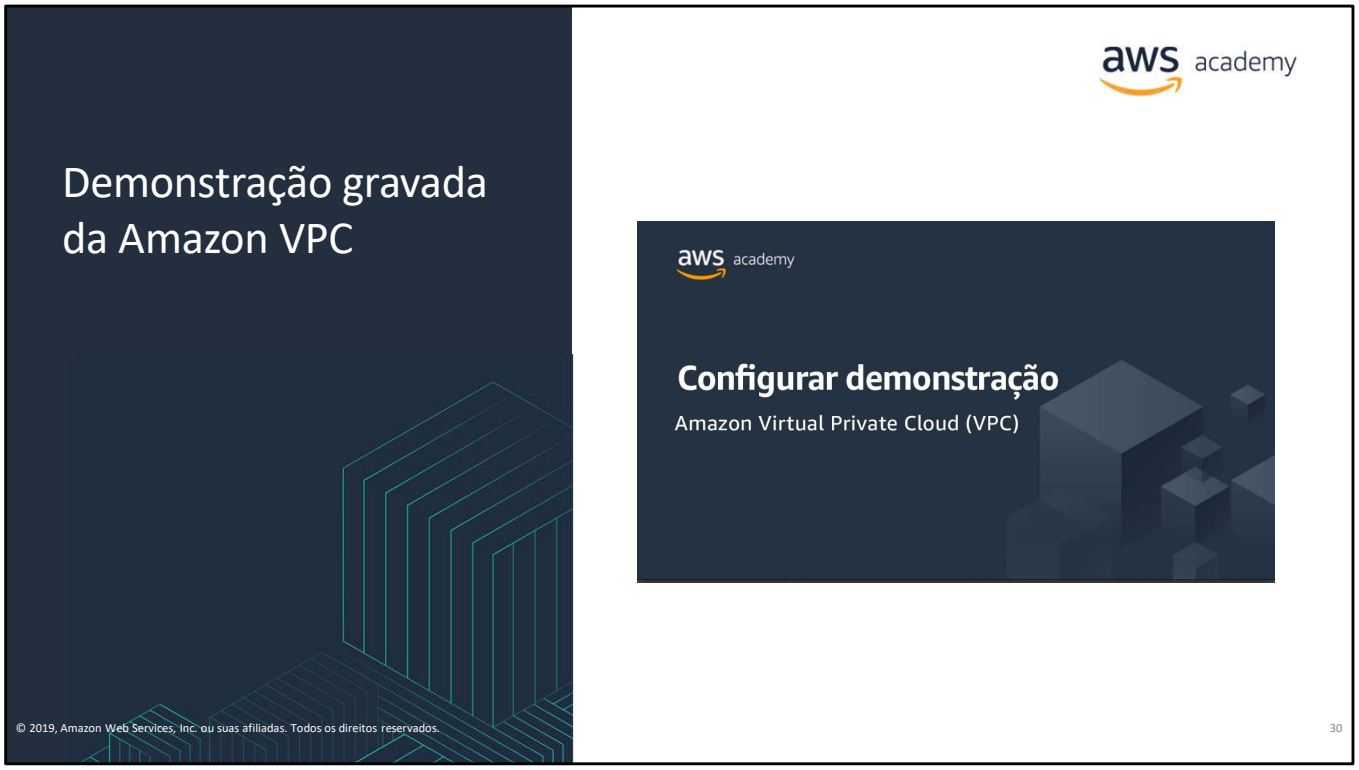


Veja se você consegue reconhecer os diferentes componentes de rede da VPC que você aprendeu ao rotular esse diagrama de rede.

Atividade: Solução



Agora veja como você se saiu bem.



Agora que você sabe como projetar uma VPC, assista a esta demonstração para saber como usar o assistente de VPC para configurar uma VPC com sub-redes públicas e privadas.

Principais lições da Seção 3

- Existem várias opções de rede da VPC, que incluem:
  - Gateway da Internet
  - Gateway NAT
  - VPC endpoint
  - Emparelhamento de VPC
  - Compartilhamento da VPC
  - AWS Site-to-Site VPN
  - AWS Direct Connect
  - AWS Transit Gateway
- Você pode usar o assistente da VPC para implementar seu projeto.

Algumas das principais lições desta seção do módulo são:

- Existem várias opções de rede da VPC, que incluem:
  - Gateway da Internet: conecta sua VPC à Internet
  - Gateway NAT: permite que instâncias em uma sub-rede privada se conectem à Internet
  - VPC endpoint: conecta sua VPC aos serviços da AWS compatíveis
  - Emparelhamento de VPC: conecta sua VPC a outras VPCs
  - Compartilhamento de VPC: permite que várias contas da AWS criem seus recursos de aplicativos em Amazon VPCs compartilhadas e gerenciadas centralmente
  - AWS Site-to-Site VPN: conecta sua VPC a redes remotas
  - AWS Direct Connect: conecta a VPC a uma rede remota usando uma conexão de rede dedicada
  - AWS Transit Gateway: uma alternativa de conexão hub-and-spoke ao emparelhamento de VPC
- Você pode usar o assistente da VPC para implementar seu projeto.

Módulo 5: Redes e entrega de conteúdo

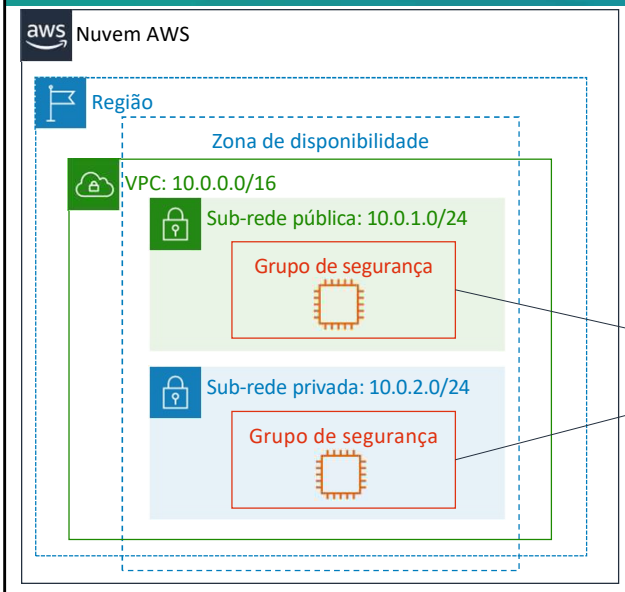
Seção 4: Segurança da VPC

aws academy

Seção 4: Segurança da VPC

Você pode incorporar segurança em sua arquitetura de VPC de várias maneiras para ter controle total sobre o tráfego de entrada e de saída. Nesta seção, você aprenderá sobre duas opções de firewall da Amazon VPC que podem ser usadas para proteger sua VPC: grupos de segurança e listas de controle de acesso à rede (ACLs de rede).

Grupos de segurança



Os grupos de segurança atuam no **nível da instância**.

Um *grupo de segurança* atua como um firewall virtual da instância e controla o tráfego de entrada e saída. Os grupos de segurança atuam no nível da instância, não no nível da sub-rede. Portanto, cada instância em uma sub-rede na VPC pode ser atribuída a um conjunto diferente de grupos de segurança.

No nível mais básico, um grupo de segurança é uma maneira de filtrar o tráfego direcionado a suas instâncias.

Grupos de segurança

Entrada				
Tipo	Protocolo	Intervalo de portas	Origem	Descrição
Todo tráfego	Todos	Todos	sg-xxxxxxxx	
Saída				
Tipo	Protocolo	Intervalo de portas	Origem	Descrição
Todo tráfego	Todos	Todos	sg-xxxxxxxx	

- Os grupos de segurança têm **regras** que controlam o tráfego de instâncias de entrada e saída.
- Os grupos de segurança padrão **negam todo o tráfego de entrada** e **permitem todo o tráfego de saída**.
- Os grupos de segurança são **stateful**.

Os grupos de segurança têm *regras* que controlam o tráfego de entrada e saída. Quando você cria um grupo de segurança, ele não tem regras de entrada. Portanto, *nenhum tráfego de entrada originado de outro host para sua instância será permitido* até que você adicione regras de entrada ao grupo de segurança. Por padrão, um grupo de segurança inclui uma regra de saída que *permite todo o tráfego de saída*. Você pode remover a regra e adicionar regras de saída que permitem somente tráfego de saída específico. Se o grupo de segurança não tiver nenhuma regra de saída, nenhum tráfego de saída originário da instância será permitido.

Osgrupos de segurança são *stateful*, o que significa que as informações de estado são mantidas mesmo depois que uma solicitação é processada. Portanto, se você enviar uma solicitação de sua instância, o tráfego da resposta dessa solicitação terá permissão para fluir, independentemente das regras de entrada do grupo de segurança. As respostas ao tráfego de entrada permitido podem sair, independentemente das regras de saída.

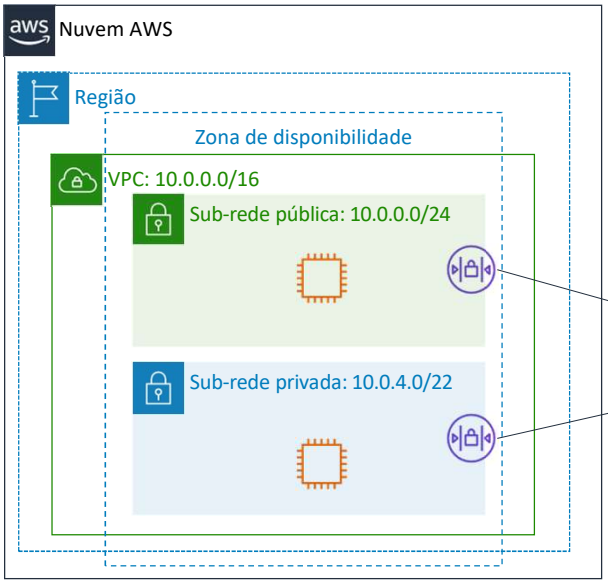
Grupos de segurança personalizados

Entrada				
Tipo	Protocolo	Intervalo de portas	Origem	Descrição
HTTP	TCP	80	0.0.0.0/0	Todo o tráfego da web
HTTPS	TCP	443	0.0.0.0/0	Todo o tráfego da web
SSH	TCP	22	54.24.12.19/32	Endereço comercial
Saída				
Tipo	Protocolo	Intervalo de portas	Origem	Descrição
Todo tráfego	Todos	Todos	0.0.0.0/0	
Todo tráfego	Todos	Todos	::/0	

- Você pode **especificar regras de permissão,** mas não de negação.
- **Todas as regras são avaliadas** antes da decisão de permitir o tráfego.

Ao criar um grupo de segurança personalizado, você pode especificar regras de permissão, mas não de negação. Todas as regras são avaliadas antes da decisão de permitir o tráfego.

Listas de controle de acesso à rede (ACLs de rede)



As ACLs de rede atuam no **nível da sub-rede**.

Uma *lista de controle de acesso à rede (ACL de rede)* é uma camada opcional de segurança para a Amazon VPC. Ela atua como um firewall para controlar o tráfego de entrada e saída de uma ou mais sub-redes. Para adicionar outra camada de segurança à sua VPC, você pode configurar ACLs de rede com regras semelhantes às dos seus grupos de segurança.

Toda sub-rede em sua VPC deve ser associada com uma ACL de rede. Se você não associar explicitamente uma sub-rede a uma ACL de rede, as sub-redes serão associadas automaticamente com a ACL de rede padrão. Você pode associar uma ACL de rede a várias sub-redes; porém, uma sub-rede pode ser associada a apenas uma ACL de rede por vez. Quando uma ACL de rede é associada a uma sub-rede, a associação anterior é removida.

ACLs de rede

Entrada					
Nº da regra	Tipo	Protocolo	Intervalo de portas	Origem	Permitir/Negar
100	Todo tráfego IPv4	Todos	Todos	0.0.0.0/0	PERMITIR
*	Todo tráfego IPv4	Todos	Todos	0.0.0.0/0	NEGAR
Saída					
Nº da regra	Tipo	Protocolo	Intervalo de portas	Origem	Permitir/Negar
100	Todo tráfego IPv4	Todos	Todos	0.0.0.0/0	PERMITIR
*	Todo tráfego IPv4	Todos	Todos	0.0.0.0/0	NEGAR

- Uma ACL de rede tem **regras de entrada e saída separadas**, e cada regra pode **permitir ou rejeitar tráfego**.
- As ACLs de rede **padrão permitem** todo o tráfego IPv4 de entrada e saída.
- As ACLs de rede são **stateless**.

Uma ACL de rede tem regras de entrada e saída separadas, e cada regra pode permitir ou rejeitar tráfego. Sua VPC já vem com uma ACL de rede padrão modificável. Por padrão, ela permite todos os tráfegos de IPv4 de entrada e saída e, se aplicável, o tráfego IPv6. A tabela mostra uma ACL de rede padrão.

AsACLs de rede são *stateless*, o que significa que nenhuma informação sobre uma solicitação é mantida depois que ela é processada.

ACLs de rede personalizadas

Entrada					
Nº da regra	Tipo	Protocolo	Intervalo de portas	Origem	Permitir/Negar
103	SSH	TCP	22	0.0.0.0/0	PERMITIR
100	HTTPS	TCP	443	0.0.0.0/0	PERMITIR
*	Todo tráfego IPv4	Todos	Todos	0.0.0.0/0	NEGAR
Saída					
Nº da regra	Tipo	Protocolo	Intervalo de portas	Origem	Permitir/Negar
103	SSH	TCP	22	0.0.0.0/0	PERMITIR
100	HTTPS	TCP	443	0.0.0.0/0	PERMITIR
*	Todo tráfego IPv4	Todos	Todos	0.0.0.0/0	NEGAR

- As ACLs de rede **personalizadas negam** todo o tráfego de entrada e saída até que você adicione regras.
- Você pode especificar regras **de permissão e negação** .
- As regras são avaliadas em ordem numérica, começando com o **menor número**.

Você pode criar uma ACL de rede personalizada e associá-la a uma sub-rede. Por padrão, enquanto você não adicionar regras, toda ACL de rede personalizada negará todo e qualquer tráfego de entrada e saída.

Uma ACL de rede contém uma lista numerada de regras que são avaliadas em ordem, começando com a regra de menor número. O objetivo é determinar se o tráfego é permitido para dentro ou para fora de qualquer sub-rede associada à ACL de rede. O número mais alto que é possível usar para uma regra é 32.766. A AWS recomenda que você crie regras em incrementos (por exemplo, incrementos de 10 ou 100) para que você possa inserir novas regras onde precisar delas posteriormente.

Para obter mais informações sobre ACLs de rede, consulte Network ACLs na documentação da AWS.

Comparação entre grupos de segurança e ACLs de rede

Atributo	Grupos de segurança	ACLs de rede
Escopo	Nível da instância	Nível de sub-rede
Regras compatíveis	Permitir somente regras	Regras de permissão e negação
Estado	Stateful (o tráfego de retorno é permitido automaticamente, independentemente das regras)	Stateless (o tráfego de retorno deve ser explicitamente permitido pelas regras)
Ordem das regras	Todas as regras são avaliadas antes da decisão de permitir o tráfego	As regras são avaliadas em ordem numérica antes da decisão de permitir tráfego

Este é um resumo das diferenças entre grupos de segurança e ACLs de rede:

- Os grupos de segurança atuam no nível da instância, mas as ACLs de rede atuam no nível da sub-rede.
- Os grupos de segurança oferecem suporte apenas a regras de permissão, mas as ACLs de rede oferecem suporte a regras de permissão e de negação.
- Os grupos de segurança são stateful, mas as ACLs de rede são stateless.
- Para grupos de segurança, todas as regras são avaliadas antes de ser tomada a decisão de permitir o tráfego ou não. Para ACLs de rede, as regras são avaliadas em ordem numérica antes de ser tomada a decisão de permitir o tráfego ou não.

Atividade: projetar uma VPC

Cenário: você tem uma pequena empresa com um site hospedado em uma instância do Amazon Elastic Compute Cloud (Amazon EC2). Você tem dados do cliente armazenados em um banco de dados de back-end que deseja manter privados. Você deseja usar a Amazon VPC para configurar uma VPC que atenda aos seguintes requisitos:

- O servidor web e o servidor de banco de dados devem estar em sub-redes separadas.
- O primeiro endereço da rede deve ser 10.0.0.0. Cada sub-rede deve ter um total de 256 endereços IPv4.
- Seus clientes devem sempre ser capazes de acessar seu servidor Web.
- Seu servidor de banco de dados deve ser capaz de acessar a Internet para fazer atualizações de patches.
- Sua arquitetura deve ser altamente disponível e usar pelo menos uma camada de firewall personalizada.

Agora, é a sua vez! Nesse cenário, você é proprietário de uma pequena empresa com um site hospedado em uma instância do Amazon Elastic Compute Cloud (Amazon EC2). Você tem dados do cliente armazenados em um banco de dados de back-end que deseja manter privados.

Veja se você pode projetar uma VPC que atenda aos seguintes requisitos:

- O servidor web e o servidor de banco de dados devem estar em sub-redes separadas.
- O primeiro endereço da rede deve ser 10.0.0.0. Cada sub-rede deve ter 256 endereços IPv4.
- Seus clientes devem sempre ser capazes de acessar seu servidor Web.
- Seu servidor de banco de dados deve ser capaz de acessar a Internet para fazer atualizações de patches.
- Sua arquitetura deve ser altamente disponível e usar pelo menos uma camada de firewall personalizada.

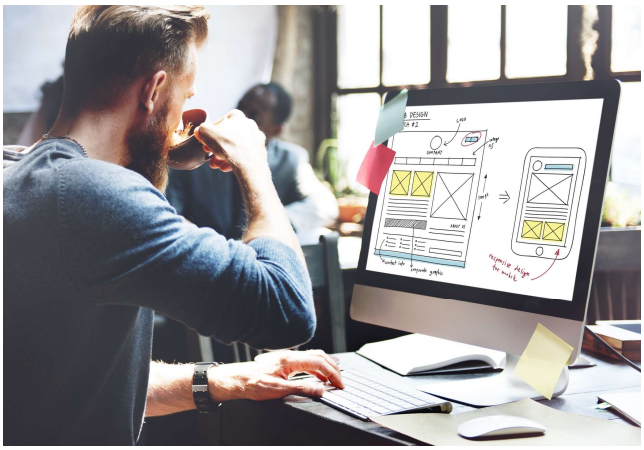
Principais lições da Seção 4

- Criar segurança em sua arquitetura de VPC:
  - Isolar sub-redes, se possível.
  - Escolher o dispositivo de gateway ou conexão VPN apropriado para suas necessidades.
  - Usar firewalls.
- Grupos de segurança e ACLs de rede são opções de firewall que você pode usar para proteger sua VPC.

As principais lições desta seção do módulo são:

- Criar segurança em sua arquitetura de VPC.
- Grupos de segurança e ACLs de rede são opções de firewall que você pode usar para proteger sua VPC.

Laboratório 2: Crie uma VPC e inicie um servidor Web



Agora, você trabalhará no Laboratório 2: criar sua VPC e executar um servidor web.

Laboratório 2: Cenário

Neste laboratório, você usa a Amazon VPC para criar sua própria VPC e adicionar alguns componentes para produzir uma rede personalizada. Você cria um grupo de segurança para sua VPC. Você também cria uma instância do EC2 e a configura para executar um servidor web e usar o grupo de segurança. Em seguida, execute a instância do EC2 na VPC.

Amazon VPC

Amazon EC2

Neste laboratório, você usa a Amazon VPC para criar sua própria VPC e adicionar alguns componentes para produzir uma rede personalizada. Você também cria um grupo de segurança para sua VPC e, em seguida, cria uma instância do EC2 e a configura para executar um servidor web e usar o grupo de segurança. Em seguida, execute a instância do EC2 na VPC.

Laboratório 2: Tarefas

- Criar uma VPC

- Criar sub-redes adicionais.

- Criar um grupo de segurança da VPC.

- Iniciar uma instância de servidor Web.

Neste laboratório, você conclui estas tarefas:

- Criar uma VPC.
- Criar sub-redes adicionais.
- Criar um grupo de segurança da VPC.
- Iniciar uma instância de servidor Web.

Laboratório 2: Produto final

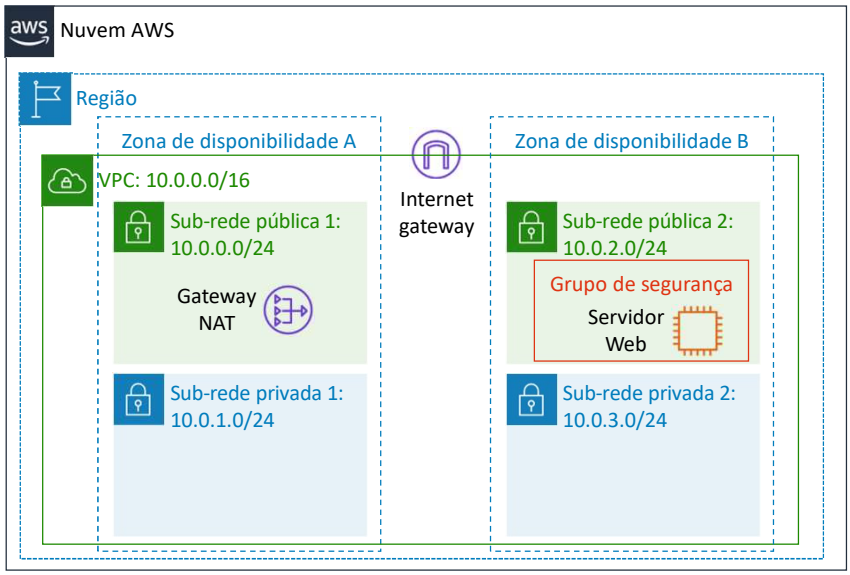


Tabela de rotas pública

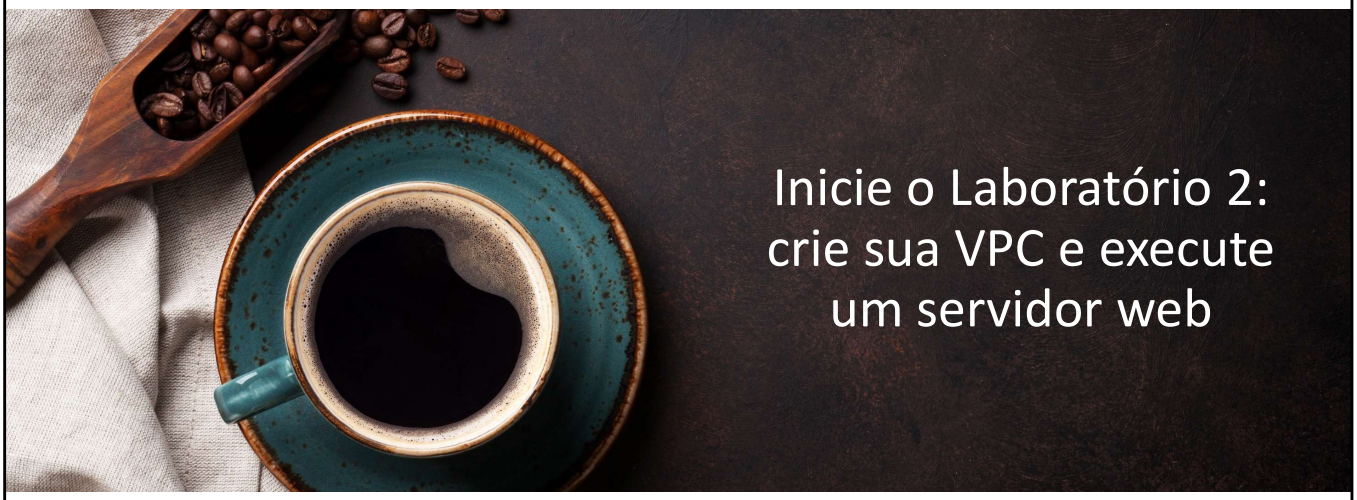
Destino	Destino
10.0.0.0/16	Local
0.0.0.0/0	Gateway da Internet

Tabela de rotas privada

Destino	Destino
10.0.0.0/16	Local
0.0.0.0/0	Gateway NAT

Este diagrama de arquitetura descreve o que você cria no laboratório.

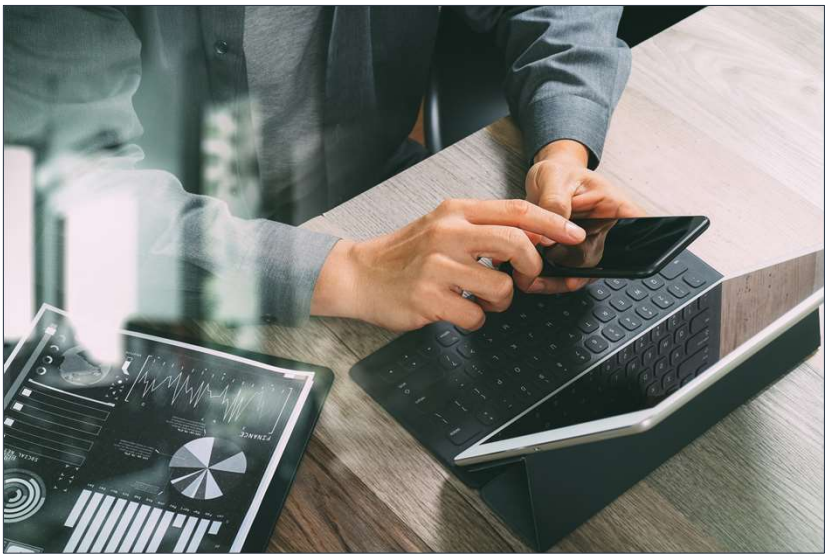
Aproximadamente 30 minutos



Inicie o Laboratório 2: crie sua VPC e execute um servidor web

Agora é hora de iniciar o laboratório. Você deve levar aproximadamente 30 minutos para concluí-lo.

Resumo do laboratório: principais lições



Neste laboratório, você:

- Criou uma Amazon VPC.
- Criou sub-redes adicionais.
- Criou um grupo de segurança da Amazon VPC.
- Executou uma instância de servidor web no Amazon EC2.

Módulo 5: Redes e entrega de conteúdo

Seção 5: Amazon Route 53

aws academy

Seção 5: Amazon Route 53

Amazon Route 53

Amazon Route 53

- É um servidor Web do Domain Name System (DNS) altamente disponível e escalável
- É usado para rotear usuários finais para aplicativos da Internet ao traduzir nomes (como *www.exemplo.com*) em endereços IP numéricos (como *192.0.2.1*) que os computadores usam para se conectarem uns aos outros
- É totalmente compatível com IPv4 e IPv6
- Conecta solicitações de usuários à infraestrutura executada na AWS e também fora da AWS
- É usado para verificar a integridade de seus recursos
- Recursos de fluxo de tráfego
- Permite registrar nomes de domínio

O Amazon Route 53 é um serviço web de Domain Name System (DNS) na nuvem altamente disponível e escalável. Ele foi projetado para oferecer a desenvolvedores e empresas uma maneira confiável e econômica de direcionar os usuários para aplicativos de Internet ao converter nomes (como *www.example.com*) em endereços IP numéricos (como *192.0.2.1*) que os computadores usam para se conectar uns aos outros. Além disso, o Amazon Route 53 é totalmente compatível com IPv6.

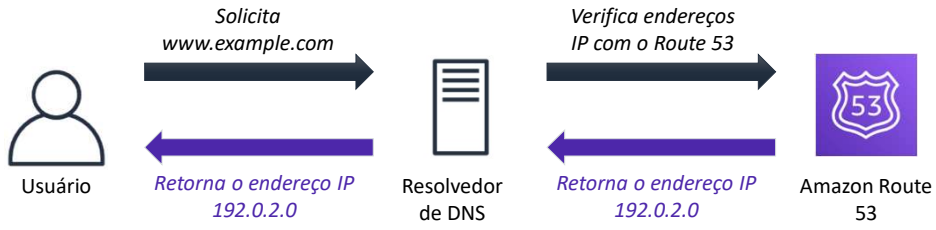
O Amazon Route 53 conecta com eficiência as solicitações de usuários com a infraestrutura executada na AWS, como instâncias do Amazon EC2, load balancers do Elastic Load Balancing e buckets do Amazon S3, e também pode ser usado para rotear usuários para infraestruturas fora da AWS.

Você pode usar o Amazon Route 53 para configurar verificações de integridade do DNS para que você possa rotear o tráfego para endpoints íntegros ou monitorar de forma independente a integridade do seu aplicativo e de seus endpoints.

O fluxo de tráfego do Amazon Route 53 ajuda você a gerenciar o tráfego globalmente por meio de vários tipos de roteamento, que podem ser combinados com failover de DNS para habilitar diversas arquiteturas de baixa latência e tolerantes a falhas. Você pode usar o editor visual simples do fluxo de tráfego do Amazon Route 53 para gerenciar como os usuários são roteados para os endpoints do aplicativo, estejam em uma única região da AWS ou distribuídos em todo o mundo.

O Amazon Route 53 também oferece registro de nome de domínio. Você pode comprar e gerenciar nomes de domínio (como *example.com*), e o Amazon Route 53 definirá automaticamente as configurações de DNS para seus domínios.

Resolução de DNS do Amazon Route 53



Este é o padrão básico que o Amazon Route 53 segue quando um usuário inicia uma solicitação de DNS. O resolvedor de DNS verifica com seu domínio no Route 53, obtém o endereço IP e o retorna para o usuário.

Roteamento compatível com o Amazon Route 53

- **Roteamento simples** - use em ambientes de servidor único
- **Roteamento ponderado Round Robin** - atribua pesos a conjuntos de registros de recursos para especificar a frequência
- **Roteamento de latência** -ajude a melhorar seus aplicativos globais
- **Roteamento de localização geográfica** - roteie o tráfego com base na localização de seus usuários
- **Roteamento de geoproximidade** - roteie o tráfego com base na localização de seus recursos
- **Roteamento de failover** - faça failover para um site de backup se o site principal se tornar inacessível
- **Roteamento de resposta com valores múltiplos** - responda a consultas DNS com até oito registros íntegros selecionados aleatoriamente

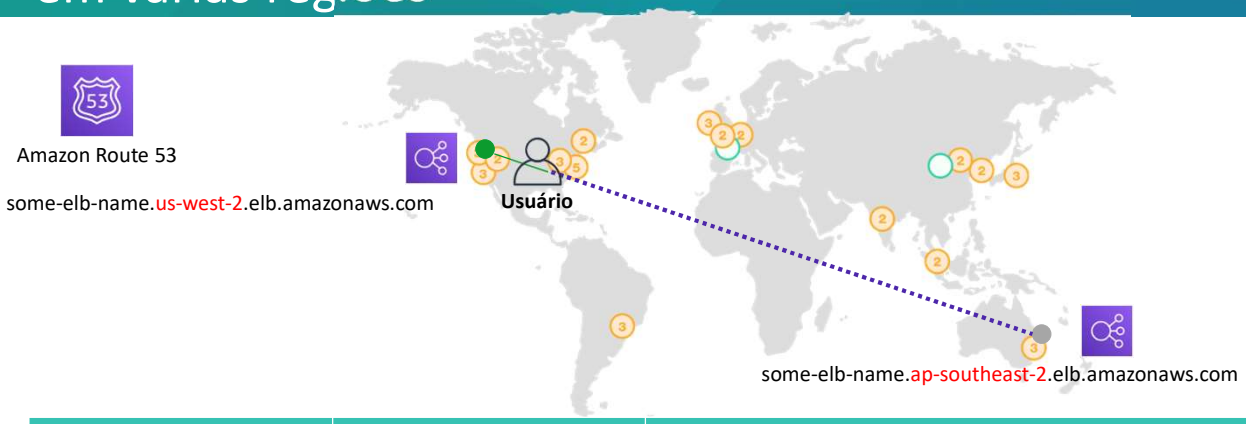
O Amazon Route 53 oferece suporte a vários tipos de políticas de roteamento, que determinam como o Amazon Route 53 responde às consultas:

- *Roteamento simples (Round Robin)* - use para um único recurso que executa uma determinada função para seu domínio (como um servidor web que fornece conteúdo para o site example.com).
- *Roteamento ponderado Round Robin* - use para rotear o tráfego para vários recursos nas proporções que você especificar. Permite atribuir pesos a conjuntos de registros de recursos para especificar a frequência com que diferentes respostas são atendidas. Permite atribuir pesos a conjuntos de registros de recursos para especificar a frequência com que diferentes respostas são atendidas. Por exemplo, suponha que você tem dois conjuntos de registros associados a um nome de DNS: um com peso 3 e um com peso 1. Nesse caso, durante 75% do tempo, o Amazon Route 53 retornará o conjunto de registros com peso 3, e durante 25% do tempo, o Amazon Route 53 retornará o conjunto de registros com peso 1. Os pesos podem ser qualquer número entre 0 e 255.
- *Roteamento de latência (LBR)* - use quando você tiver recursos em várias regiões da AWS e quiser rotear o tráfego para a região que fornece a melhor latência. O roteamento de latência funciona roteando seus clientes para o endpoint da AWS (por exemplo, instâncias do Amazon EC2, endereços IP elásticos ou load balancers) que oferece a experiência mais rápida com base nas medidas de desempenho reais das diferentes regiões da AWS onde seu aplicativo é executado.
- *Roteamento de localização geográfica* - use quando quiser rotear o tráfego com base

na localização de seus usuários. Quando você usa o roteamento por geolocalização, pode traduzir o conteúdo e apresentar todo o seu site ou parte dele no idioma de seus usuários. Você também pode usar o roteamento de localização geográfica para restringir a distribuição de conteúdo apenas para os locais onde você tem direitos de distribuição. Outro uso possível é o balanceamento da carga entre endpoints de uma forma previsível e fácil de gerenciar, para que cada local de usuário seja roteado de forma consistente para o mesmo endpoint.

- Roteamento de *geoproximidade* -use quando quiser rotear o tráfego com base na localização de seus recursos e, opcionalmente, mudar o tráfego de recursos em um local para recursos em outro.
- *Roteamento de failover (failover de DNS)* - use quando quiser configurar o failover ativo-passivo. O Amazon Route 53 pode ajudar a detectar uma interrupção do site e redirecionar os usuários para locais alternativos onde o aplicativo está funcionando corretamente. Quando você habilita esse recurso, os agentes de verificação de integridade do Amazon Route 53 monitoram cada local ou endpoint do seu aplicativo para determinar sua disponibilidade. Você pode aproveitar esse recurso para aumentar a disponibilidade do aplicativo voltado ao cliente.
- *Roteamento de resposta com valores múltiplos* - use quando quiser que o Route 53 responda a consultas DNS com até oito registros íntegros selecionados aleatoriamente. Você pode configurar o Amazon Route 53 para retornar vários valores, como endereços IP para seus servidores web, em resposta a consultas DNS. Você pode especificar vários valores para praticamente qualquer registro, mas o roteamento de resposta com valores múltiplos também permite que você verifique a integridade de cada recurso para que o Route 53 retorne somente valores de recursos íntegros. Não é um substituto para um load balancer, contudo a capacidade de retornar vários endereços IP verificáveis pela integridade é uma maneira de usar o DNS para melhorar a disponibilidade e o balanceamento de carga.

Caso de uso: implantação em várias regiões



Nome	Tipo	Valor
example.com	ALIAS	some-elb-name.us-west-2.elb.amazonaws.com
example.com	ALIAS	some-elb-name.ap-southeast-2.elb.amazonaws.com

A implantação em várias regiões é um exemplo de caso de uso para o Amazon Route 53. Com o Amazon Route 53, o usuário é direcionado automaticamente para o load balancer do Elastic Load Balancing mais próximo do usuário.

Os benefícios da implantação em várias regiões do Route 53 incluem:

- Roteamento com base na latência para a região
- Roteamento de balanceamento de carga para a zona de disponibilidade

Failover de DNS do Amazon Route 53

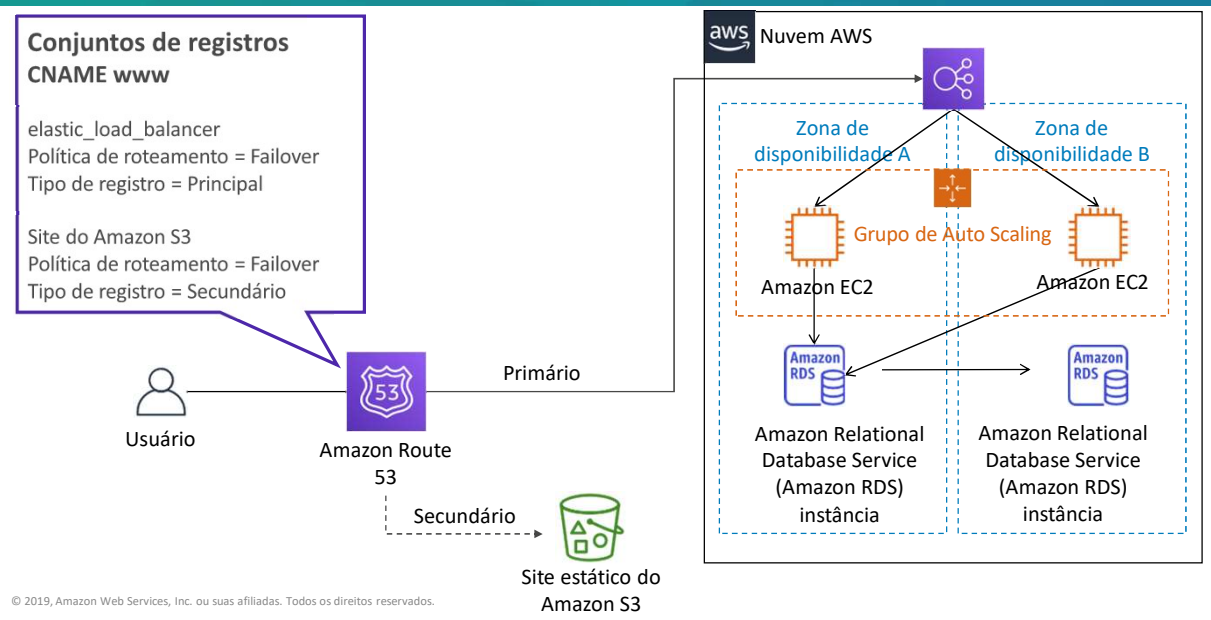
Melhore a disponibilidade dos aplicativos executados na AWS:

- Configurando cenários de backup e failover para seus próprios aplicativos
- Habilitando arquiteturas multirregião altamente disponíveis na AWS
- Criação de verificações de integridade

O Amazon Route 53 permite que você melhore a disponibilidade dos aplicativos executados na AWS:

- Configurando cenários de backup e failover para seus próprios aplicativos.
- Habilitando arquiteturas multirregião altamente disponíveis na AWS.
- Criando verificações de integridade para monitorar a integridade e o desempenho de seus aplicativos web, servidores web e outros recursos. Cada verificação de integridade criada por você pode monitorar um dos seguintes: a integridade de um recurso especificado, como um servidor web, o status de outras verificações de integridade e o status de um alarme do Amazon CloudWatch.

Failover de DNS para um aplicativo web multicamadas



Aqui, você verá como o failover de DNS funciona em uma arquitetura típica para um aplicativo web multicamadas. O Route 53 passa o tráfego para um load balancer, que distribui o tráfego para uma frota de instâncias do EC2.

É possível realizar as seguintes tarefas com o Route 53 para garantir alta disponibilidade:

1. Crie dois registros DNS para o Registro de nome canônico (CNAME) *www* com uma política de roteamento de *roteamento de failover*. O primeiro registro é a principal política de rotas, que aponta para o load balancer do seu aplicativo web. O segundo registro é a política de rotas secundária, que aponta para o site estático do Amazon S3.
2. Use as verificações de integridade do Route 53 para garantir que a primária esteja em execução. Se estiver, todo o tráfego assumirá como padrão a pilha de aplicativos web. O failover para o site de backup estático seria acionado se o servidor web for desativado (ou travar) ou se a instância do banco de dados for desativada.

Principais lições da seção 5

- O Amazon Route 53 é um serviço web de DNS na nuvem altamente disponível e escalável que converte nomes de domínio em endereços IP numéricos.
- O Amazon Route 53 oferece suporte a vários tipos de políticas de roteamento.
- A implantação em várias regiões melhora o desempenho do aplicativo para um público global.
- Você pode usar o failover do Amazon Route 53 para melhorar a disponibilidade dos seus aplicativos.

Algumas das principais lições desta seção do módulo são:

- O Amazon Route 53 é um serviço web de DNS na nuvem altamente disponível e escalável que converte nomes de domínio em endereços IP numéricos.
- O Amazon Route 53 oferece suporte a vários tipos de políticas de roteamento.
- A implantação em várias regiões melhora o desempenho do aplicativo para um público global.
- Você pode usar o failover do Amazon Route 53 para melhorar a disponibilidade dos seus aplicativos.

Módulo 5: Redes e entrega de conteúdo

Seção 6: Amazon CloudFront

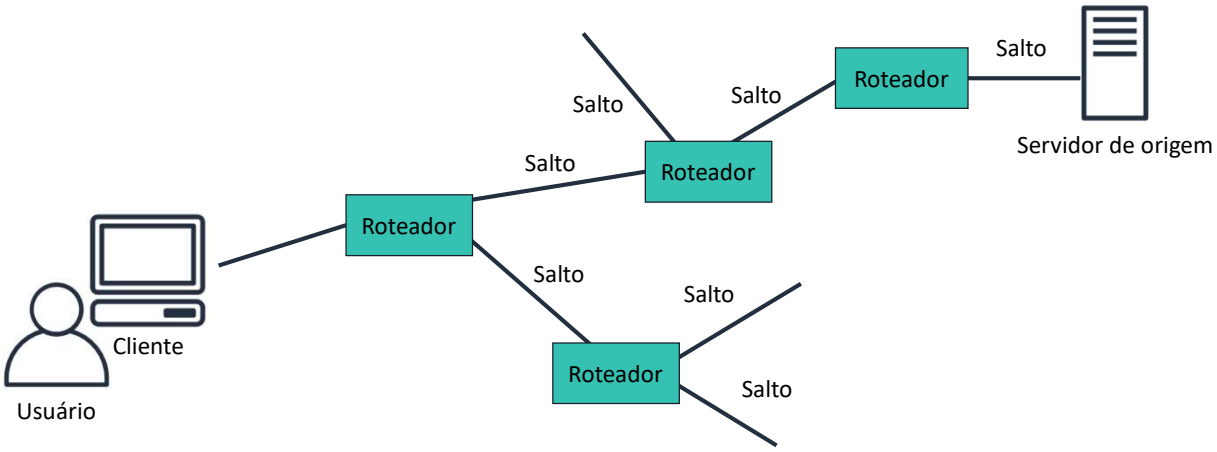
aws academy

Seção 6: Amazon CloudFront

O objetivo das redes é compartilhar informações entre recursos conectados. Até agora, neste módulo, você aprendeu sobre as redes de VPC com a Amazon VPC. Você aprendeu sobre as diferentes opções para conectar sua VPC à Internet, a redes remotas, a outras VPCs e a serviços da AWS.

A entrega de conteúdo também ocorre em redes, por exemplo, quando você faz streaming de um filme do seu serviço de streaming favorito. Nesta seção final, você aprenderá sobre o Amazon CloudFront, que é um serviço de rede de entrega de conteúdo (CDN).

Entrega de conteúdo e latência de rede



Como explicado anteriormente neste módulo, quando você estava aprendendo sobre o AWS Direct Connect,um dos desafios da comunicação de rede é o desempenho da rede. Quando você navega em um site ou faz streaming de vídeo, sua solicitação é roteada por várias redes diferentes para acessar um servidor de origem. O servidor de origem (ou origem) armazena as versões originais e definitivas dos objetos (páginas da web, imagens e arquivos de mídia). O número de saltos de rede e a distância que a solicitação deve percorrer afetam significativamente o desempenho e a capacidade de resposta do site. Além disso, a latência de rede é diferente em várias localizações geográficas. Por esses motivos, uma rede de entrega de conteúdo pode ser a solução.

Rede de entrega de conteúdo (CDN)

- É um sistema distribuído globalmente de servidores de armazenamento em cache
- Armazena cópias de arquivos comumente solicitados (conteúdo estático) em cache
- Fornece uma cópia local do conteúdo solicitado de um ponto de presença ou ponto de presença de cache próximo
- Acelera a entrega de conteúdo dinâmico
- Melhora o desempenho e a escalabilidade do aplicativo

Uma rede de entrega de conteúdo (CDN) é um sistema distribuído globalmente de servidores de armazenamento em cache. Uma CDN armazena em cache cópias de arquivos normalmente solicitados (conteúdo estático, como Hypertext Markup Language ou HTML; folhas de estilo em cascata ou CSS; JavaScript e arquivos de imagem) que são hospedados no servidor de origem do aplicativo. A CDN entrega uma cópia local do conteúdo solicitado de uma borda de cache ou ponto de presença que fornece a entrega mais rápida para o solicitante.

As CDNs também fornecem conteúdo dinâmico exclusivo do solicitante e não armazenável em cache. A entrega de conteúdo dinâmico de uma CDN melhora o desempenho e a escalabilidade dos aplicativos. A CDN estabelece e mantém conexões seguras mais próximas do solicitante. Se a CDN estiver na mesma rede que a origem, o roteamento de volta para a origem para recuperar conteúdo dinâmico será acelerado. Além disso, conteúdo como dados de formulário, imagens e texto podem ser ingeridos e enviados de volta para a origem, aproveitando as conexões de baixa latência e o comportamento de proxy do PoP.

Amazon CloudFront

Amazon CloudFront

- Serviço de CDN rápido, global e seguro
- Rede global de pontos de presença e pontos de presença de caches regionais
- Modelo de autoatendimento
- Definição de preço com pagamento conforme o uso

O Amazon CloudFront é um serviço de CDN rápido que entrega dados, vídeos, aplicativos e interfaces de programação de aplicativos (APIs) aos clientes globalmente com baixa latência e altas velocidades de transferência. Ele também oferece um ambiente amigável para desenvolvedores. O Amazon CloudFront entrega arquivos aos usuários por meio de uma rede global de pontos de presença e pontos de presença de caches regionais. O Amazon CloudFront é diferente das soluções tradicionais de entrega de conteúdo, pois permite que você obtenha rapidamente os benefícios da entrega de conteúdo de alta performance sem contratos negociados, preços altos ou taxas mínimas. Como outros serviços da AWS, o Amazon CloudFront é uma oferta de autoatendimento com definição de preço de pagamento conforme o uso.

Infraestrutura Amazon CloudFront

- **Pontos de presença -** rede de datacenters que o CloudFront usa para fornecer conteúdo popular rapidamente aos clientes.
- **Cache de ponto regional -** Localização do CloudFront que armazena em cache conteúdo que não é popular o suficiente para permanecer em um ponto de presença. Ele está localizado entre o servidor de origem e o ponto de presença global.

O Amazon CloudFront entrega conteúdo por meio de uma rede mundial de datacenters denominados *pontos de presença*. Quando um usuário solicita conteúdo fornecido por você com o CloudFront, ele é roteado para o ponto de presença com a menor latência (ou tempo de atraso) para que o conteúdo seja entregue com a melhor performance possível. Os pontos de presença do CloudFront são projetados para fornecer conteúdo popular rapidamente aos visualizadores.

À medida que os objetos são menos acessados, pontos de presença individuais poderão removê-los para liberar espaço para conteúdo mais solicitado. Para conteúdo menos popular, o CloudFront tem caches de presença *regionais.* Os caches de presença regionais são os locais do CloudFront que estão implantados globalmente e próximos dos visualizadores. Eles estão localizados entre o servidor de origem e os pontos de presença globais que fornecem conteúdo diretamente aos visualizadores. Um cache de presença regional tem um cache maior do que um ponto de presença individual, portanto, os objetos permanecem no cache de ponto regional por mais tempo. Mais conteúdo permanece mais próximo dos visualizadores, o que reduz a necessidade de o CloudFront voltar para o servidor de origem e melhora o desempenho geral para os visualizadores.

Para obter mais informações sobre como o Amazon CloudFront funciona, consulte Como o CloudFront entrega conteúdo na documentação da AWS.

Benefícios do Amazon CloudFront

- Rápido e global
- Segurança na borda
- Altamente programável
- Profundamente integrado à AWS
- Econômico

O Amazon CloudFront oferece os seguintes benefícios:

- *Rápido e global* - o Amazon CloudFront tem escalabilidade massiva e é distribuído globalmente. Para entregar conteúdo aos usuários finais com baixa latência, o Amazon CloudFront usa uma rede global que consiste em pontos de presença e caches regionais.

- *Segurança na borda* - o Amazon CloudFront oferece proteção no nível da rede e no nível do aplicativo. Seu tráfego e seus aplicativos se beneficiam com várias proteções integradas, como o AWS Shield Standard, sem custo adicional. Você também pode usar recursos configuráveis, como o AWS Certificate Manager (ACM), para criar e gerenciar certificados Secure Sockets Layer (SSL) personalizados sem custo adicional.

- *Altamente programável* - os recursos do Amazon CloudFront podem ser personalizados para requisitos específicos de aplicativos. Ele se integra ao Lambda@Edge para que você possa executar código personalizado em locais da AWS em todo o mundo, o que permite mover lógica complexa de aplicativos para mais perto dos usuários para melhorar a capacidade de resposta. A CDN também oferece suporte a integrações com outras ferramentas e interfaces de automação para DevOps. Ele oferece ambientes de integração e entrega contínuas (CI/CD).

- *Profundamente integrado à AWS* - o Amazon CloudFront é integrado à AWS, com

localizações físicas diretamente conectadas à infraestrutura global da AWS e a outros serviços da AWS. Você pode usar APIs ou o Console de Gerenciamento da AWS para configurar programaticamente todos os recursos na CDN.

- *Econômico* - o Amazon CloudFront é econômico porque não tem compromissos mínimos e cobra apenas pelo que você usa. Em comparação com a hospedagem própria, o Amazon CloudFront evita as despesas e a complexidade de operar uma rede de servidores de cache em vários sites na Internet. Ele elimina a necessidade de provisionar capacidade em excesso para atender a picos potenciais no tráfego. O Amazon CloudFront também usa técnicas como recolher solicitações simultâneas do visualizador em um ponto de presença do mesmo arquivo em uma única solicitação para o seu servidor de origem. O resultado é a redução da carga nos servidores de origem e a redução da necessidade de escalar a infraestrutura de origem, o que pode resultar em uma maior economia de custos. Se você usar origens da AWS, como o Amazon Simple Storage Service (Amazon S3) ou o Elastic Load Balancing, pagará apenas pelos custos de armazenamento, e não pelos dados transferidos entre esses serviços e o CloudFront.

"Definição de preços do Amazon CloudFront"

Transferência de dados para fora

- Cobrado pelo volume de dados transferidos do ponto de presença do Amazon CloudFront para a Internet ou para sua origem.

Solicitações HTTP (S)

- Cobrado pelo número de solicitações HTTP (S).

Solicitações de invalidação

- Não há cobrança adicional para os primeiros 1.000 caminhos solicitados para invalidação a cada mês. Depois disso, 0,005 USD por caminho solicitado para invalidação.

IP dedicado SSL personalizado

- 600 USD por mês para cada certificado SSL personalizado associado com uma ou mais distribuições do CloudFront usando a versão com IP dedicado do suporte de certificado SSL personalizado.

As cobranças do Amazon CloudFront se baseiam no uso real do serviço em quatro áreas:

- *Transferência de dados para fora* - você será cobrado pelo volume de dados transferidos de pontos de presença do Amazon CloudFront, medidos em GB, para a Internet ou para sua origem (origens da AWS e outros servidores de origem). O uso de transferência de dados é totalizado separadamente por regiões geográficas específicas. O custo é calculado de acordo com os níveis de definição de preço em cada área. Se você usar outros serviços da AWS como origem de arquivos, será cobrado separadamente pelo uso desses serviços, inclusive armazenamento e horas de computação.

- *Solicitações HTTP(S)* - você é cobrado pelo número de solicitações HTTP(S) feitas ao Amazon CloudFront para seu conteúdo.

- *Solicitações de invalidação* - você é cobrado por caminho na solicitação de invalidação. Um caminho listado na solicitação de invalidação representa o URL (ou vários URLs, se o caminho contém um caractere curinga) do objeto que você deseja invalidar no cache do CloudFront. Você pode solicitar até 1.000 caminhos por mês do Amazon CloudFront sem nenhum custo adicional. Após os primeiros 1.000 caminhos, você será cobrado por caminho listado nas solicitações de invalidação.

- *IP dedicado personalizado Secure Sockets Layer (SSL)* - você paga 600 USD por mês

para cada certificado SSL personalizado associado a uma ou mais distribuições do CloudFront que usam a versão de IP dedicado do suporte a certificados SSL personalizados. Essa tarifa mensal é rateada por hora. Por exemplo, se você tiver um certificado SSL personalizado associado a pelo menos uma distribuição do CloudFront por apenas 24 horas (ou seja, um dia) no mês de junho, seu custo total pelo uso do recurso de certificado SSL personalizado será (1 dia/30 dias) x 600 USD = 20 USD.

Para obter as informações de definição de preço mais recentes, consulte a página de definição de preço do Amazon CloudFront.

Principais lições da Seção 6

- Uma CDN é um sistema distribuído globalmente de servidores de armazenamento em cache que acelera a entrega de conteúdo.
- O Amazon CloudFront é um serviço de CDN rápido que entrega dados, vídeos, aplicativos e APIs com segurança em uma infraestrutura global com baixa latência e altas velocidades de transferência.
- O Amazon CloudFront oferece muitos benefícios.

Algumas das principais lições desta seção do módulo são:

- Uma CDN é um sistema distribuído globalmente de servidores de armazenamento em cache que acelera a entrega de conteúdo.
- O Amazon CloudFront é um serviço de CDN rápido que entrega dados, vídeos, aplicativos e APIs com segurança em uma infraestrutura global com baixa latência e altas velocidades de transferência.
- O Amazon CloudFront oferece muitos benefícios, incluindo:
    - Rápido e global
    - Segurança na borda
    - Altamente programável
    - Profundamente integrado à AWS
    - Econômico

Módulo 5: Redes e entrega de conteúdo

Conclusão do módulo

Agora é hora de revisar o módulo e encerrar com um teste de conhecimento e discussão sobre uma pergunta simulada do teste de certificação.

Resumo do módulo

Resumindo, neste módulo você aprendeu a:

- Reconhecer os conceitos básicos de redes
- Descrever as redes virtuais na nuvem com a Amazon VPC
- Rotular um diagrama de rede
- Projetar uma arquitetura básica de VPC
- Indicar as etapas para criar uma VPC
- Identificar grupos de segurança
- Crie sua própria VPC e adicione componentes adicionais a ela para produzir uma rede personalizada
- Identificar os fundamentos do Amazon Route 53
- Reconhecer os benefícios do Amazon CloudFront

Resumindo, neste módulo você aprendeu a:

- Reconhecer os conceitos básicos de redes
- Descrever as redes virtuais na nuvem com a Amazon VPC
- Rotular um diagrama de rede
- Projetar uma arquitetura básica de VPC
- Indicar as etapas para criar uma VPC
- Identificar grupos de segurança
- Crie sua própria VPC e adicione componentes adicionais a ela para produzir uma rede personalizada
- Identificar os fundamentos do Amazon Route 53
- Reconhecer os benefícios do Amazon CloudFront

Conclua o teste de conhecimento

Agora, conclua o teste de conhecimento.

Exemplo de pergunta do exame

Qual serviço de rede da AWS permite que uma empresa crie uma rede virtual dentro da AWS?

A. AWS Config
B. Amazon Route 53
C. AWS Direct Connect
D. Amazon VPC

Examine as opções de resposta e as exclua com base nas palavras-chave destacadas anteriormente.

Recursos adicionais

- Página de visão geral da Amazon VPC
- Artigo técnico Amazon Virtual Private Cloud Connectivity Options
- Publicação no blog de arquitetura da AWS One to Many: Evolving VPC Design
- Guia do usuário da Amazon VPC
- Página de visão geral do Amazon CloudFront

Se quiser saber mais sobre os tópicos abordados neste módulo, estes recursos adicionais podem ser úteis:

- Página de visão geral da Amazon VPC
- Artigo técnico Amazon Virtual Private Cloud Connectivity Options
- Publicação no blog de arquitetura da AWS One to Many: Evolving VPC Design
- Guia do usuário da Amazon VPC
- Página de visão geral do Amazon CloudFront

Obrigado

Agradecemos a sua participação!