

Laboratório: – Arquitetura de múltiplas VPCs

1. Navegue até o serviço VPC

The screenshot shows the AWS Services search interface. At the top, it says "AWS services". Below that is a "Find Services" input field containing "VPC", with a magnifying glass icon to its left and an "X" icon to its right. A tooltip above the input field says "You can enter names, keywords or acronyms.". Below the input field, the word "VPC" is displayed in large blue letters, followed by the subtitle "Isolated Cloud Resources".

Em todas as regiões, um VPC padrão já foi criado para você. Então, mesmo que você ainda não tenha criado nada em nossa conta, você verá alguns recursos de VPC lá.

2. Crie VPCs com sub-redes e instâncias EC2

Neste laboratório, vamos criar três VPC com sub-redes privadas. Cada VPC terá sub-redes em duas Zonas de Disponibilidade dentro da Região. Implantaremos uma instância EC2 por VPC e demonstraremos que, por padrão, os VPCs fornecem isolamento de rede.

Tabela 1. Alocações de CIDR IPv4 para VPCs e AZs.

Nome VPC	Bloco DE CIDR VPC	Zona de disponibilidade	Bloco CIDR da Zona de Disponibilidade
VPC A	10.0.0.0/16	us-east-1a	10.0.0.0/24
		us-east-1b	10.0.1.0/24
VPC B	10.1.0.0/16	us-east-1a	10.1.0.0/24
		us-east-1b	10.1.1.0/24
VPC C	10.2.0.0/16	us-east-1a	10.2.0.0/24
		us-east-1b	10.2.1.0/24

2.1 Criar VPCs

Nosso primeiro passo é criar VPCs com blocos de CIDR não sobrepostos.

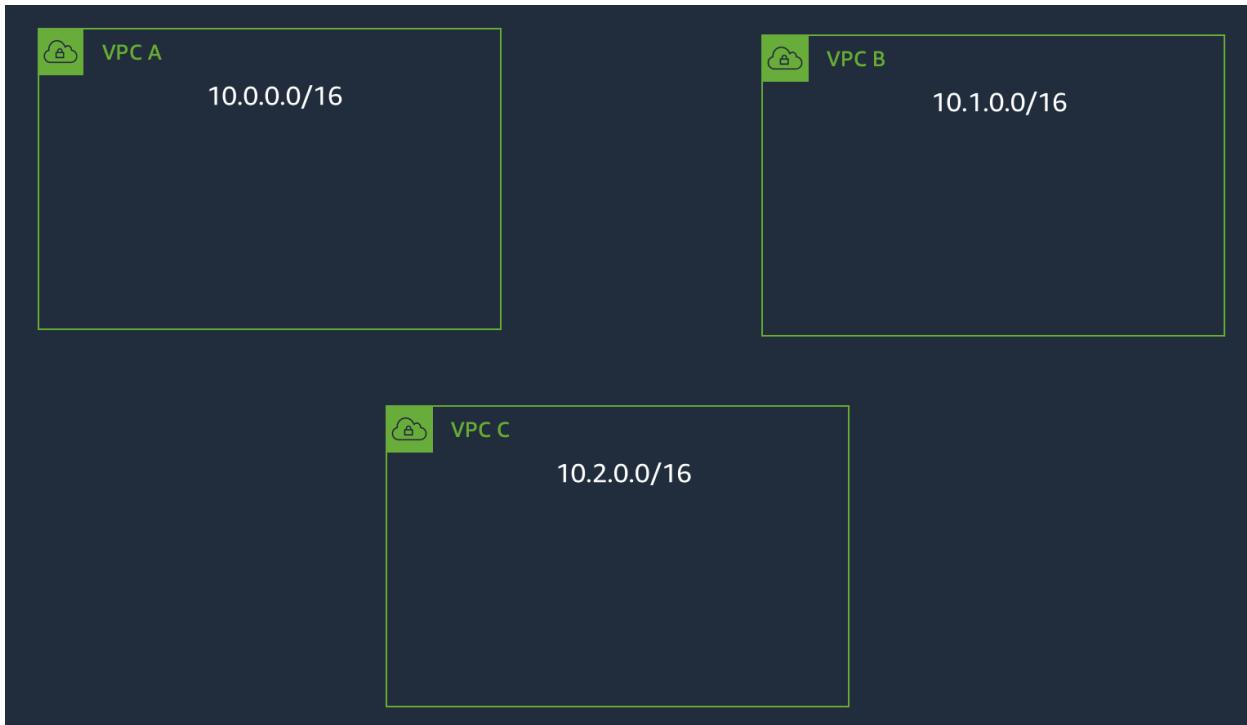
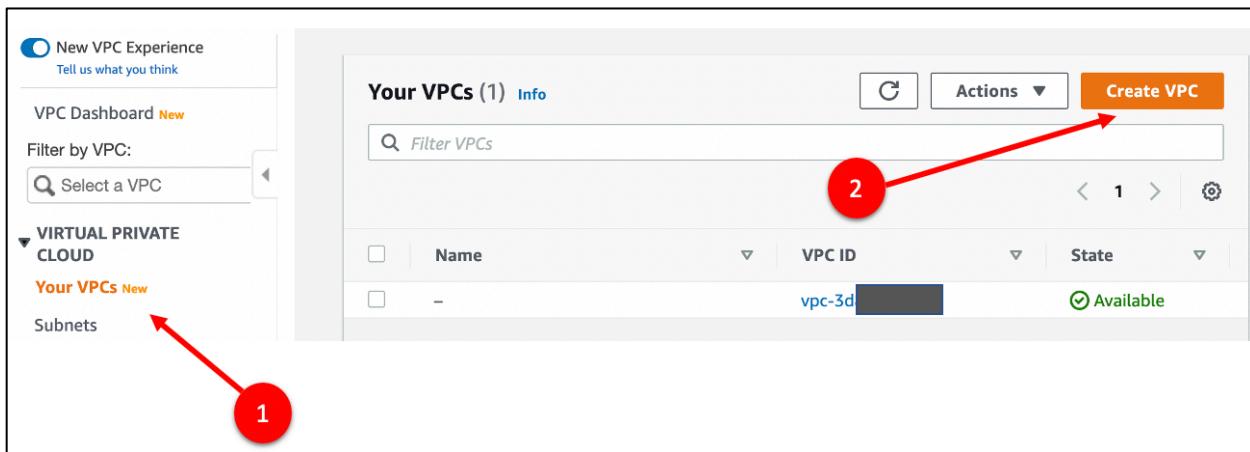


Figura 1. Três VPCs com faixas de CIDR únicas.

Navegue até a guia "Seus VPCs" e clique no botão "Criar VPCs".



- Create "VPC A", especificando 10.0.0.0/16 como bloco CIDR IPv4.
- Não habilite IPv6.
- Selecione "Default" Tenancy.

- Aceite as tags propostas:

VPCs > Create VPC

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an IPv6 CIDR block with the VPC.

Name tag	VPC A	i
IPv4 CIDR block*	10.0.0.0/16	i
IPv6 CIDR block	<input checked="" type="radio"/> No IPv6 CIDR Block <input type="radio"/> Amazon provided IPv6 CIDR block <input type="radio"/> IPV6 CIDR owned by me	i
Tenancy	Default	i

- Siga os mesmos passos para criar "VPC B" e "VPC C" (consulte **tabela 1** acima para os detalhes).

Depois de completar essas etapas, você deve ter três novos VPCs em "Seus VPCs":

	Name	VPC ID	State	IPv4 CIDR
<input type="checkbox"/>	-	vpc-3d	✓ Available	172.31.0.0/16
<input type="checkbox"/>	VPC A	vpc-0a	✓ Available	10.0.0.0/16
<input type="checkbox"/>	VPC B	vpc-06	✓ Available	10.1.0.0/16
<input type="checkbox"/>	VPC C	vpc-02	✓ Available	10.2.0.0/16

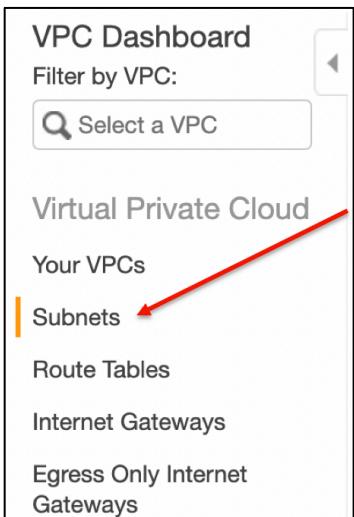
2.2 Criar sub-redes

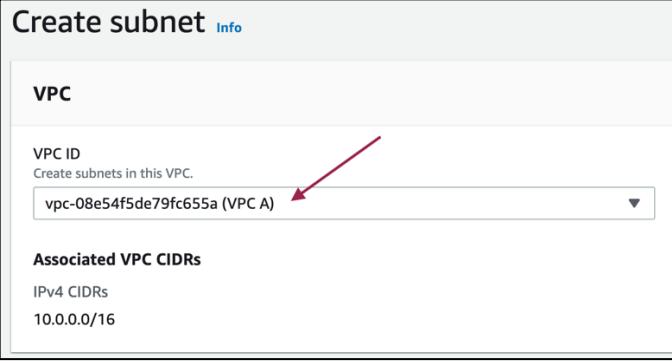
Para cada VPC, criaremos duas sub-redes - uma por zona de disponibilidade (o nome AZs pode diferir - dependendo da sua região escolhida, na imagem abaixo é "us-east-1").



Figura 2. Alocando sub-redes para AZs.

Navegue até o painel Subnets



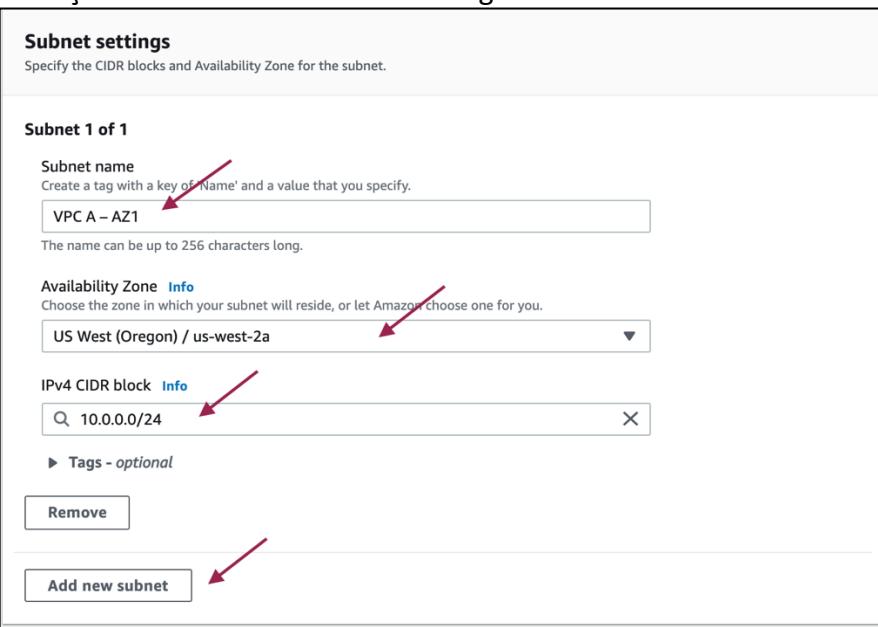
- **Create subnet** Info


VPC

VPC ID
Create subnets in this VPC.

vpc-08e54f5de79fc655a (VPC A)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16
- Crie sub-redes com nomes que refletem os VPC e AZs, como VPC A - AZ1, selecione AZ e forneça CIDR sub-rede. Use Azs da região us-east-1:


Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

VPC A - AZ1

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US West (Oregon) / us-west-2a

IPv4 CIDR block Info

10.0.0.0/24

► Tags - optional

Remove

Add new subnet

- Clique em **Adicionar nova sub-rede** para adicionar mais um subnet no AZ2 com nome como VPC A - AZ2:

Subnet 2 of 2

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

VPC A - AZ2

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US West (Oregon) / us-west-2b

IPv4 CIDR block [Info](#)

10.0.1.0/24

Tags - optional

Key	Value - optional
Name	VPC A - AZ2

Add new tag

You can add 49 more tags.

Remove

Add new subnet

Cancel **Create subnet**

Repita as etapas acima para criar sub-redes para **VPC B** e **VPC C**; consulte a Tabela1 para alocações de CIDR.

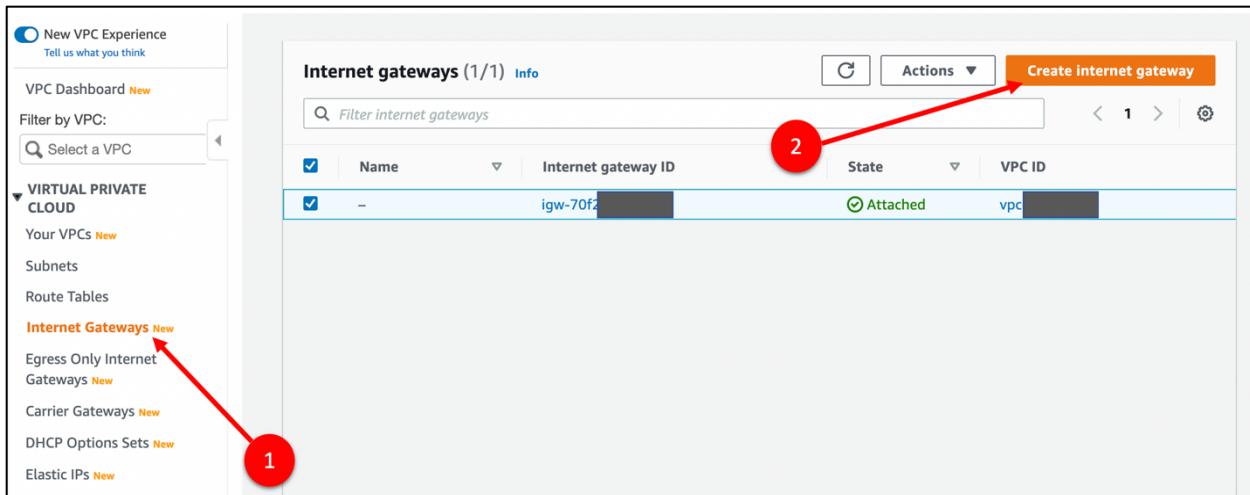
Depois de terminar a tarefa, seis novas sub-redes devem estar disponíveis:

<input type="checkbox"/>	VPC A - AZ1	subnet-019f13	available	vpc-0a529	VPC A	10.0.0.0/24	251
<input type="checkbox"/>	VPC A - AZ2	subnet-0c6770	available	vpc-0a529	VPC A	10.0.1.0/24	251
<input type="checkbox"/>	VPC B - AZ1	subnet-06c2b3	available	vpc-06576	VPC B	10.1.0.0/24	251
<input type="checkbox"/>	VPC B - AZ2	subnet-041bf3	available	vpc-06576	VPC B	10.1.1.0/24	251
<input type="checkbox"/>	VPC C - AZ1	subnet-0b3403	available	vpc-02fb16	VPC C	10.2.0.0/24	251
<input type="checkbox"/>	VPC C - AZ2	subnet-07f31f	available	vpc-02fb16	VPC C	10.2.1.0/24	251

2.3 Implantar gateways de Internet

Nesta seção, implantaremos um Gateway de Internet (IGW) por VPC. Precisamos de um Gateway de Internet para estabelecer conectividade externa às instâncias EC2 em VPCs.

Navegue até gateways da Internet e clique em "Criar gateway de internet"



Selecione o Gateway de Internet para "VPC A", como VPC A - IGW. Clique em "Criar gateway de internet"

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.

VPC A – IGW

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="VPC A – IGW"/> X Remove

Add new tag

You can add 49 more tags.

Cancel Create internet gateway

Selecione o IGW recém-criado e clique em "Anexar ao VPC":

Internet gateways (1/2) Info			
<input type="checkbox"/>	Name	Internet gateway ID	State
<input checked="" type="checkbox"/>	VPC A - IGW	igw-0b204ea7	Attached
<input type="checkbox"/>	-	igw-70f2d16	Not attached

Actions ▾ [Create internet gateway](#)

- [View details](#)
- [Attach to VPC](#)
- [Detach from VPC](#)
- [Manage tags](#)
- [Delete internet gateway](#)

47

Conecte este IGW a "VPC A":

VPC > Internet gateways > Attach to VPC (igw-0b204ea7)

Attach to VPC (igw-0b204ea7)

VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs
Attach the internet gateway to this VPC.

Select a VPC

vpc-06576b1 - VPC B
vpc-0a529e5 - VPC A
vpc-02fb165 - VPC C

Cancel [Attach internet gateway](#)

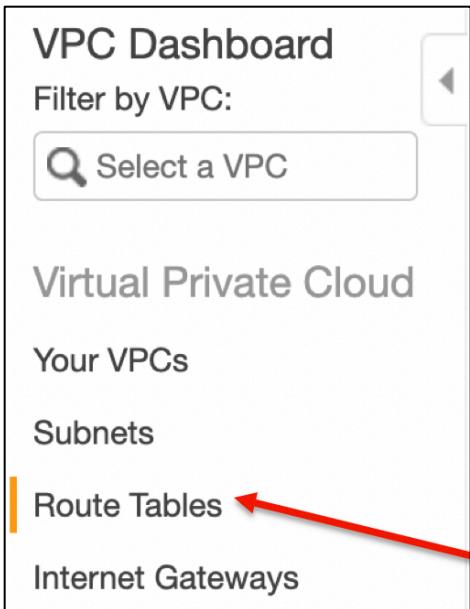
Repita estas etapas para criar e anexar IGWs em "VPC B" e "VPC C". Agora você deve ter um IGW para o VPC padrão e três IGWs recém-criados disponíveis:

<input type="checkbox"/>	Name	Internet gateway ID	State	VPC ID
<input type="checkbox"/>	-	igw-70f2d16	Attached	vpc-3d8bd16
<input type="checkbox"/>	VPC A - IGW	igw-0b204ea7	Attached	vpc-0a529e5
<input type="checkbox"/>	VPC B - IGW	igw-0987654	Attached	vpc-06576b1
<input type="checkbox"/>	VPC C - IGW	igw-0987654	Attached	vpc-02fb165

2.4 Atualização das Tabelas de roteamento

Para utilizar gateways de Internet recém-criados, você precisa atualizar as tabelas de routing do VPC para apontar as rotas padrão para esses IGWs.

No painel VPC, navegue até tabelas de rotas



Atribua nomes às tabelas de rotas identificando a tabela de rotas a que é atribuída:

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
VPC A Route Table	rtb-040166928c10	-	-	Yes	vpc-0a52 VPC A
17/255	rtb-0c3e30fb5c5f16	-	-	Yes	vpc-065
VPC C Rou...	rtb-8c	-	-	Yes	vpc-02f
		-	-	Yes	vpc-3d8

Route Table: rtb-040166928c10

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Route Table ID: rtb-040166928c10 Main: Yes
Explicitly Associated with: Owner VPC: vpc-0a52 | VPC A

Navegue até a tabela de rotas "VPC A" e clique na guia "Rotas". Clique em "Editar rotas":

VPC A Route Table	rtb-0fa	Yes
VPC B Route Table	rtb-03a	Yes
VPC C Route Table	rtb-09f	Yes

Route Table: rtb-0fa

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit routes

Modifique a tabela de rotas para adicionar a rota padrão 0.0.0.0/0 apontando para o Gateway da Internet.

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-		No

Add route igw-02649b77591127597 VPC A - IGW

Repita estes passos para tabelas de rotas "VPC B" e "VPC C".

2.5 Implantar instâncias EC2 em VPC's.

Navegue até os serviços de painel EC2.

AWS services

Find Services

You can enter names, keywords or acronyms.

EC2

Virtual Servers in the Cloud

2.5.1 Iniciar instâncias EC2

- Clique em "Lançamento de Instâncias".
- Escolha o Amazon Linux 2 AMI (HVM), SSD Volume Tipo 64 bits (x86) e clique em "Selecionar"
- Usaremos o tipo de instância "t2.micro" elegível para o nível gratuito.
- Clique em "Next: Configure detalhes da instância"
- Implante a primeira instância para AZ1 de "VPC A" escolhendo-os da rede e dos dropdowns da sub-rede.
- Escolha "Auto-atribuir IP público": Habilitar.

Vamos atribuir IP público a este caso. Sem esta etapa, não seremos capazes de nos conectar à instância remotamente.

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	1	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-0a5 VPC A	<input type="button" value="Create new VPC"/>
Subnet	subnet-019f VPC A - AZ1 us-east-1	<input type="button" value="Create new subnet"/> 251 IP Addresses available
Auto-assign Public IP	<input checked="" type="checkbox"/> Enable	

Auto-assign Public IP	<input checked="" type="checkbox"/> Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	<input type="checkbox"/> Open	
Domain join directory	No directory	<input type="button" value="Create new directory"/>
IAM role	LabInstanceProfile	<input type="button" value="Create new IAM role"/>
Shutdown behavior	Stop	

- Em IAM role, selecione "LabInstanceProfile"
- Clique em "Review and Launch". Clique em "Lançar".
- Na última etapa, escolha **Prosseguir sem par de chaves**. – Não precisaremos da chave para conectar nas instâncias.

Enquanto a instância está sendo lançada, atribua-lhe um nome que reflete as colocações VPC e AZ, como EC2 VPC A - AZ1

Inicie mais duas instâncias EC2 e atribua-lhes nomes de acordo:

- um na "VPC B" AZ1
- outra na "VPC C" AZ1.

Depois de alguns minutos, você deve ter 3 instâncias EC2 no estado "em execução".

Instances (3) Info					
<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check
<input type="checkbox"/>	EC2 VPC A - AZ1	i-0b90	<input checked="" type="checkbox"/> Running	t2.micro	<input checked="" type="checkbox"/> 2/2 checks ...
<input type="checkbox"/>	EC2 VPC B - AZ1	i-0691	<input checked="" type="checkbox"/> Running	t2.micro	<input checked="" type="checkbox"/> 2/2 checks ...
<input type="checkbox"/>	EC2 VPC C - AZ1	i-04f25	<input checked="" type="checkbox"/> Running	t2.micro	<input checked="" type="checkbox"/> 2/2 checks ...

Para cada instância do EC2, atualize as regras do Grupo de Segurança sob a guia Segurança para permitir que o tráfego de ICMP (SSH na porta 22 já estará aberto):

Instances (1/3) Info

Instance: i-0b90... (EC2 VPC A - AZ1)

Security

Security details

IAM Role: -

Owner ID: [REDACTED]

Launch time: Tue Oct 20 2020 08:33:31 GMT-0400 (Eastern Daylight Time)

Security groups:

- sg-05ac... (launch-wizard-1) 1
- sg-05ad... (launch-wizard-1)
- sg-05ae... (launch-wizard-1)
- sg-05af... (launch-wizard-1)
- sg-05ag... (launch-wizard-1)
- sg-05ah... (launch-wizard-1)
- sg-05ai... (launch-wizard-1)
- sg-05aj... (launch-wizard-1)
- sg-05ak... (launch-wizard-1)
- sg-05al... (launch-wizard-1)
- sg-05am... (launch-wizard-1)
- sg-05an... (launch-wizard-1)
- sg-05ao... (launch-wizard-1)
- sg-05ap... (launch-wizard-1)
- sg-05aq... (launch-wizard-1)
- sg-05ar... (launch-wizard-1)
- sg-05as... (launch-wizard-1)
- sg-05at... (launch-wizard-1)
- sg-05au... (launch-wizard-1)
- sg-05av... (launch-wizard-1)
- sg-05aw... (launch-wizard-1)
- sg-05ax... (launch-wizard-1)
- sg-05ay... (launch-wizard-1)
- sg-05az... (launch-wizard-1)

Modifique as Regras de Entrada no Grupo de Segurança para permitir o tráfego SSH e ICMP a partir de qualquer endereço:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
All ICMP - IPv4	ICMP	All	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Repita estes passos para as instâncias EC2 em "VPC B – AZ 1" e "VPC C – AZ1".

Anote os endereços IPv4 privados atribuídos às instâncias EC2 clicando em uma instância e navegando na guia Networking:

Instances (1/3) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm Status
EC2 VPC A - AZ1	i-0b90...	Running	t2.micro	2/2 checks ...	No alarms + us-east-1c
EC2 VPC B - AZ1	i-069...	Running	t2.micro	2/2 checks ...	No alarms + us-east-1c
EC2 VPC C - AZ1	i-04f...	Running	t2.micro	2/2 checks ...	No alarms + us-east-1c

Instance: i-0b90... (EC2 VPC A - AZ1)

Details **Security** **Networking** **Storage** **Status Checks** **Monitoring** **Tags**

Instance summary **Info**

Instance ID i-0b90... (EC2 VPC A - AZ1)	Public IPv4 address 34.206.178.120 open address ↗	Private IPv4 addresses 10.0.0.40 ↗ 1
Instance state Running	Public IPv4 DNS -	Private IPv4 DNS ip-10-0-0-40.ec2.internal

Preencha a tabela a seguir com informações ip.

Tabela 2. EC2 instâncias endereços IP privados:

VPC	Endereço IP privado de instância EC2
VPC A	10.0.0.[.....]
VPC B	10.1.0.[.....]
VPC C	10.2.0.[.....]

2.6 Teste de comunicação inter-VPC

Selecione "EC2 VPC A - AZ1" e clique em "Conectar".

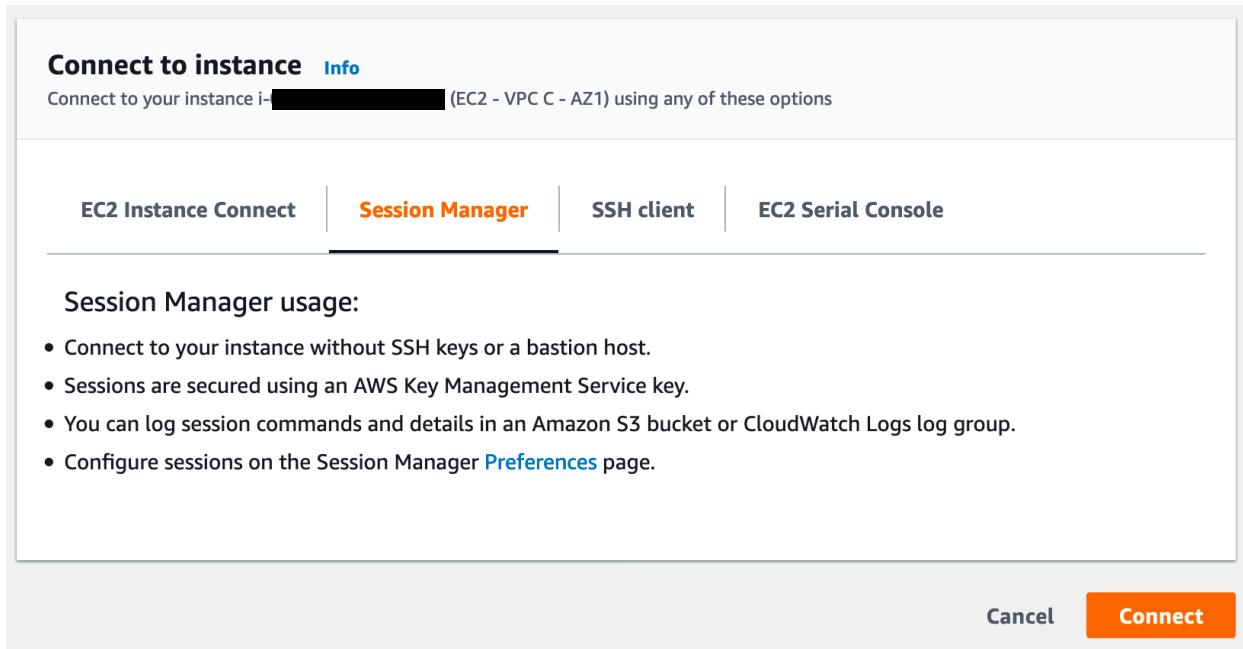
Instances (1/3) Info

Name	Instance ID	Instance state	Instance type	Status check
EC2 VPC A - AZ1	i-0b90...	Running	t2.micro	2/2 checks ...
EC2 VPC B - AZ1	i-069...	Running	t2.micro	2/2 checks ...
EC2 VPC C - AZ1	i-04f...	Running	t2.micro	2/2 checks ...

Actions ▾

- View details
- Connect** ↗ 1
- Get Windows password
- Create template from instance
- Launch more like this
- Manage tags
- Instance state

Clique em "Conectar" para conectar usando Session Manager:



A sessão do terminal deve ser aberta em uma guia nova do navegador. A partir da instância EC2 em "VPC A" tente pingar os endereços IP privados de instâncias EC2 em "VPC B" e "VPC C". Esses endereços respondem?