

Module 7 Lab 3: VPC Peering

VPCs - Create VPC

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 i

IPv4 CIDR block* i

IPv6 CIDR block No IPv6 CIDR Block i
 Amazon provided IPv6 CIDR block

Tenancy i

* Required Cancel **Create**

Two VPC's will be created, this is the first one.

Internet gateways - Create internet gateway

Internet gateways > Create internet gateway

Create internet gateway

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.

Name tag i

* Required Cancel **Create**

An IG will allow VPCA to access the Internet and public subnets.

Internet gateways - Attach to VPC

Internet gateways > Attach to VPC

Attach to VPC

Attach an internet gateway to a VPC to enable communication with the internet. Specify the VPC you would like to attach below.

VPC* vpc-0d491f035333874ed

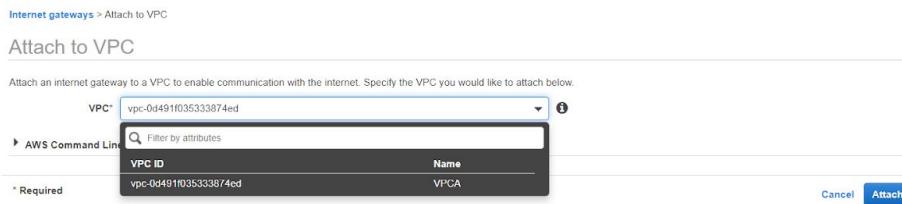
AWS Command Line

Filter by attributes

VPC ID	Name
vpc-0d491f035333874ed	VPCA

* Required

Cancel Attach



Only one IG at a time can be attached to a VPC, thus only the new VPCA is shown.

Internet Gateways Dashboard

Create internet gateway Actions ▾

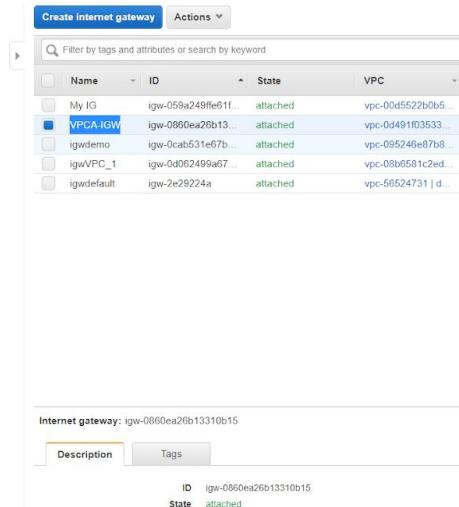
Filter by tags and attributes or search by keyword

Name	ID	State	VPC
My IG	igw-059a249ffe61f...	attached	vpc-00d5522b0b5...
VPCA-IGW	igw-0860ea26b13310b15	attached	vpc-0d491f03533...
igwdemo	igw-0cab531e7b...	attached	vpc-095246e07b8...
igwVPC_1	igw-0d062499a67...	attached	vpc-08b6581c2ed...
igwdefault	igw-2e29224a	attached	vpc-56524731 d...

Internet gateway: igw-0860ea26b13310b15

Description Tags

ID igw-0860ea26b13310b15
State attached



VPCA-IGW has been attached to VPCA.

Subnets - Create subnet

Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag	VPCA-Subnet-Public		
VPC*	vpc-0d491f035333874ed		
Availability Zone	No preference		
VPC CIDRs	CIDR	Status	Status Reason
	10.100.0.0/16	associated	
IPv4 CIDR block*	10.100.0.0/24		

* Required

Cancel Create

A public subnet for VPCA is created.

VPC - Subnets

[Create subnet](#) [Actions](#)

Filter by tags and attributes or search by keyword 1 to 11 of 11

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability Zone ID	Route table
<input checked="" type="checkbox"/> VPCA-Subnet-Public	subnet-06f0c22e6b2844e2c	available	vpc-0d491f035333874ed VPCA	10.100.0.0/24	251	-	us-west-1b	usw1-az1	rtb-0b659e61a36
Public 2	subnet-0036ca5fc8ddc34f	available	vpc-00d5522b0b5c9e656 My VPC	10.0.2.0/24	251	-	us-west-1b	usw1-az1	rtb-024d574a4ee1
Public 1	subnet-01eabb8989487eac0	available	vpc-00d5522b0b5c9e656 My VPC	10.0.1.0/24	250	-	us-west-1a	usw1-az3	rtb-024d574a4ee1
Private 2	subnet-020fce19aa5731b	available	vpc-00d5522b0b5c9e656 My VPC	10.0.4.0/24	251	-	us-west-1b	usw1-az1	rtb-0aaaf3c16e035
Private 1	subnet-0af66705498a670	available	vpc-00d5522b0b5c9e656 My VPC	10.0.3.0/24	250	-	us-west-1a	usw1-az3	rtb-0aaaf3c16e035
10.0.2.0 - us-west-1b	subnet-0f1a3c8f627a7772	available	vpc-095246e87b82cc2c9 vpcdemo	10.0.2.0/24	250	-	us-west-1b	usw1-az1	rtb-054642092b2
10.0.1.0 - us-west-1a	subnet-012a74242ca9f53d	available	vpc-095246e87b82cc2c9 vpcdemo	10.0.1.0/24	250	-	us-west-1a	usw1-az3	rtb-00376893ebd1
	subnet-077cd1a3367eb6c3c	available	vpc-08b6581c2ed32f417 VPC_1	172.30.1.0/24	251	-	us-west-1b	usw1-az1	rtb-018fdcf8e317
	subnet-02c105fc3a196d181	available	vpc-08b6581c2ed32f417 VPC_1	172.30.0.0/24	251	-	us-west-1a	usw1-az3	rtb-018fdcf8e317
	subnet-7991551f	available	vpc-56524731 default	172.31.16.0/20	4091	-	us-west-1b	usw1-az1	rtb-385adb5e
	subnet-6dafbe36	available	vpc-56524731 default	172.31.0.0/20	4091	-	us-west-1a	usw1-az3	rtb-385adb5e

Subnet: subnet-06f0c22e6b2844e2c

Description Flow Logs Route Table Network ACL Tags Sharing

Subnet ID: subnet-06f0c22e6b2844e2c
VPC: vpc-0d491f035333874ed | VPCA
Available IPv4 Addresses: 251
Availability Zone: us-west-1b (usw1-az1)
Network ACL: acd0901799130239bc7c
Auto-assign public IPv4 address: No

State: available
IPv4 CIDR: 10.100.0.0/24
IPv6 CIDR: -
Route Table: rtb-0b659e61a3678698c
Default subnet: No
Auto-assign IPv6 address: No

VPCA public subnet is created.

Route Tables - Create route table

Route Tables > Create route table

Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag: VPCA-RT-Public

VPC: vpc-0d491f035333874ed

* Required Cancel Create

A route table is created for VPCA.

Route Tables - Edit routes

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	igw-0860ea26b13310b15 VPCA-IGW		No X

Add route Cancel Save routes

At this point, only internal traffic can be routed. Editing routes can allow external traffic. In essence, all traffic not on 10.100.0.0/16 will be allowed through the IG. Non-local traffic can be sent out into the Internet.

VPC - Route table

The screenshot shows the AWS VPC Route Table list and a detailed view of a specific route table.

Route Table List:

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
rtb-0546f42092b2af8fa	-	-	-	Yes	vpc-095246e87b82cc2c9...
rtb-0aa3c16e0352a9ff	-	-	-	Yes	vpc-00d5522b0b5c9e556...
rtb-0b659e61a3678698c	-	-	-	Yes	vpc-0d491f035333874ed...
rtb-385adbf5e	-	-	-	Yes	vpc-565247311default...
rtb-018dfc8e317474d0	-	-	-	Yes	vpc-08b6581c2ed32f417...
Public Route Table	rtb-024d574a4fee9a5389	2 subnets	-	No	vpc-00d5522b0b5c9e556...
VPCA-RT-Public	rtb-03198b0b3e3c7dd85	-	-	No	vpc-0d491f035333874ed...
rttdemo	rtb-00376893ebd9e1c74	subnet-012a74242ca9f538d	-	No	vpc-095246e87b82cc2c9...

Route Table Details: Route Table: rtb-03198b0b3e3c7dd85

- Summary
- Routes**
- Subnet Associations
- Edge Associations
- Route Propagation
- Tags

Edit routes

View: All routes

Destination	Target	Status
10.100.0.0/16	local	active
0.0.0.0	igw-0860ea26b13310b15	active

The public route table has been updated.

Subnets - Edit route table association

The screenshot shows the AWS Subnets - Edit route table association page.

Subnets > Edit route table association

Edit route table association

Subnet ID: subnet-06f0c22e6b2844e2c

Route Table ID:

Route table ID	Route table name	VPC ID
rtb-0b659e61a3678698c	vpc-0d491f035333874ed	
rtb-03198b0b3e3c7dd85	VPCA-RT-Public	vpc-0d491f035333874ed
10.100.0.0/16	local	
0.0.0.0/0	igw-0860ea26b13310b15	

* Required

Cancel Save

The subnet VPCA needs to be associated with the route table just created.

VPC - Subnets

The screenshot shows the AWS VPC Subnets console. A subnet named "VPCA-Subnet/Public" is selected. The subnet details include:

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability Zone ID	Route table
VPCA-Subnet/Public	subnet-06f0c22e6b2844e2c	available	vpc-0d491f035333874ed VPCA	10.100.0.0/24	251	-	us-west-1b	usw1-az1	rtb-03198b03e3c7dd85
Public_2	subnet-0036ca5fc8330c34f	available	vpc-0d5522005c0e556 My VPC	10.0.2.0/24	251	-	us-west-1b	usw1-az1	rtb-024d574a4

The "Route Table" tab is selected, showing the association with the route table "rtb-03198b03e3c7dd85 | VPCA-RT-Public". The route table contains two entries:

Destination	Target
10.100.0.0/16	local
0.0.0.0/0	igw-0960ea26b13310b15

Correct routing table information.

Subnets - Create subnet

The screenshot shows the "Create subnet" step of the AWS Subnets wizard. The form fields are:

- Name tag: VPCA-Subnet-Private
- VPC: vpc-0d491f035333874ed
- Availability Zone: No preference
- VPC CIDRs: 10.100.0.0/16 (Status: associated)
- IPv4 CIDR block: 10.100.1.0/24

A note at the bottom left says "* Required". At the bottom right are "Cancel" and "Create" buttons.

A private subnet will be created.

VPC - Subnets

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability Zone ID	Route table
VPCA-Subnet-Public	subnet-06f022e6b2944e2c	available	vpc-0d491f03533874ed VPCA	10.100.0.0/24	251	-	us-west-1b	usw1-az1	rtb-03198b0b3
VPCA-Subnet-Private	subnet-0a919aac4e652a44a	available	vpc-0d491f03533874ed VPCA	10.100.1.0/24	251	-	us-west-1b	usw1-az1	rtb-0b659e61a
Public-Subnet	subnet-0036ca5fc0dd0dc34f	available	vpc-00d5522000c9e556 My VPC	10.0.2.0/24	251	-	us-west-1b	usw1-az1	rtb-024d574a

Subnet: subnet-0a919aac4e652a44a

Description Flow Logs Route Table Network ACL Tags Sharing

Subnet ID: subnet-0a919aac4e652a44a
VPC: vpc-0d491f03533874ed | VPCA
Available IPv4 Addresses: 251
Availability Zone: us-west-1b (usw1-az1)
Network ACL: acl-090179913d239bc7c
Auto-assign public IPv4 address: No

State: available
IPv4 CIDR: 10.100.1.0/24
IPv6 CIDR: -
Route Table: rtb-0b659e61a367869c
Default subnet: No
Auto-assign IPv6 address: No

A private subnet is created.

Route Tables - Create route table

Route Tables > Create route table

Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag: VPCA-RT-Private

VPC: vpc-0d491f03533874ed

* Required

Cancel Create

Any traffic that cannot be routed into the internal subnet will be lost.

VPC - Create route table

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
rtdemo	rtb-003769393ebd9e1c74	subnet-012a74242ca9f538d	-	No	vpc-095246e87b82cc2c9...
VPCA-RT-Public	rtb-03198b0b3e3c7dd85	subnet-06f0c22e6b2844e2c	-	No	vpc-0d491f035333874ed...
VPCA-RT-Private	rtb-0058b0169fcc18814	-	-	No	vpc-0d491f035333874ed...
Public Route Table	rtb-024d574a4ee9a96389	2 subnets	-	No	vpc-00d5522b0b5c5e9e56...
rtb-054642092b2af8fa	-	-	-	Yes	vpc-095246e87b82cc2c9...
rtb-0aa3c16e0352a98f	-	-	-	Yes	vpc-00d5522b0b5c5e9e56...
rtb-0b659e61a3678698c	-	-	-	Yes	vpc-0d491f035333874ed...
rtb-385adb5e	-	-	-	Yes	vpc-56524731 default
rtb-018fdfc8e317474d0	-	-	-	Yes	vpc-08b6581c2ed32f417...

Route Table: rtb-0058b0169fcc18814

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status
10.100.0.0/16	local	active

There is no need to allow traffic from 0.0.0.0/0 because this is a private subnet.

Subnets - Edit route table association

Subnets > Edit route table association

Edit route table association

Subnet ID: subnet-0a919aac4e652a44a

Route Table ID:

Route table ID	Route table name	VPC ID
rtb-0b659e61a3678698c		vpc-0d491f035333874ed
rtb-0058b0169fcc18814	VPCA-RT-Private	vpc-0d491f035333874ed
rtb-03198b0b3e3c7dd85	VPCA-RT-Public	vpc-0d491f035333874ed

* Required

Cancel Save

Feedback English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

12:31 PM

However, the routing tables still require to be associated with the correct private subnet.

VPC - Subnets

The screenshot shows the AWS VPC Subnets console. A table lists subnets, including one named 'VPCA-Subnet-Private' which is selected. Below the table, a 'Route Table' tab is active, showing a single entry for the subnet. The 'Destination' is '10.100.0.0/16' and the 'Target' is 'local'. The status bar at the bottom indicates '1 to 12 of 12'.

The VPCA private subnet is now associated with a route table that only allows internal traffic.

EC2 - Choose AMI

The screenshot shows the 'Choose AMI' step of the EC2 instance creation wizard. It displays a list of available AMIs, with 'Amazon Linux 2 AMI (HVM), SSD Volume Type' selected. Other options shown include Amazon Linux 18.03.0, Red Hat Enterprise Linux 8, SUSE Linux Enterprise Server 15 SP1, and Ubuntu Server 18.04 LTS. Each item has a 'Select' button to the right.

The first of two new EC2 instances will be set up. Amazon Linux 2 AMI selected.

EC2 - Instance type

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by:								
Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)								
Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support	
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes	
General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes	
General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes	
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes	
General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes	
General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes	
General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes	
General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes	
General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes	
General purpose	t3a.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes	
General purpose	t3a.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes	

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

The free tier is selected.

EC2 - Configure Instance

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

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	<input type="text" value="1"/>	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-0d491f03533874ed VPC Create new VPC	
Subnet	subnet-069c22e6b2844e2c VPC-A-Subnet-Public Create new subnet 251 IP Addresses available	
Auto-assign Public IP	<input type="checkbox"/> Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	Create new Capacity Reservation
IAM role	None Create new IAM role	
Shutdown behavior	Stop	
Stop - Hibernate behavior	<input type="checkbox"/> Enable hibernation as an additional stop behavior	
Enable termination protection	<input type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring Additional charges apply	
Tenancy	Shared - Run a shared hardware instance Create new tenancy Additional charges will apply for dedicated tenancy	
T2/T3 Unlimited	<input type="checkbox"/> Enable <small>Additional charges may apply</small>	

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

Note that an auto-assigned Public IP is enabled.

EC2- Add Storage

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-068ff9d11756564539	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Cancel Previous Review and Launch Next: Add Tags

Default storage is selected.

EC2 - Add Tags

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key	(128 characters maximum)	Value	(256 characters maximum)	Instances	Volumes
Staff		Aguirre		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

Tags were established.

EC2 - Configure Security Group

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: Create a new security group Select an existing security group

Security group name: VPCA-SG-Public

Description: VPCA-SG-Public

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

Add Rule

⚠ Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel Previous Review and Launch

Only SSH will be allowed into this EC2 instance.

EC2 - Review

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

AMI Details

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-06fccff0bc2c8943f
Free tier eligible
Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.
Root Device Type: ebs Virtualization type: hvm

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups

Security group name: VPCA-SG-Public
Description: VPCA-SG-Public

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	

Instance Details

Number of instances: 1
Network: vpc-0d491fc03333874ed
Subnet: subnet-060c22e602644e2c
EBS-optimized: No
Monitoring: No
Termination protection: No
Shutdown behavior: Stop
Stop - Hibernate behavior: Disabled

Purchasing option: On demand

Edit AMI Edit Instance type Edit security groups Edit instance details Cancel Previous Launch

The review page for the EC2 instance.

New key pair

Note that a Key pair has been saved locally.

EC2 Dashboard

The EC2 Public Server is now running.

EC2 - Configure Instance

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

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	<input type="text" value="1"/>	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-0d491f035333874ed VPCA	<input type="button" value="Create new VPC"/>
Subnet	subnet-0a919aacfe652a44a VPCA-Subnet-Private	<input type="button" value="Create new subnet"/> 251 IP Addresses available
Auto-assign Public IP	<input type="checkbox"/> Use subnet setting (Disable)	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	<input type="button" value="Create new Capacity Reservation"/>
IAM role	None <input type="button" value="Create new IAM role"/>	
Shutdown behavior	<input type="radio"/> Stop	
Stop - Hibernate behavior	<input type="checkbox"/> Enable hibernation as an additional stop behavior	
Enable termination protection	<input type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring Additional charges apply	
Tenancy	Shared - Run a shared hardware instance <input type="checkbox"/> Additional charges will apply for dedicated tenancy.	

Buttons: Cancel Previous **Review and Launch** Next: Add Storage

The second private EC2 instance is created. Note that VPCA and VPCA private are selected.
Because this is an internal non-public facing instance, auto-assign public IP is disabled.

EC2 - Configure Security Group

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group:

Create a new security group
 Select an existing security group

Security group name: VPCA-SG-Private

Description: VPCA-SG-Private

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 10.100.0.0/24	e.g. SSH for Admin Desktop

Buttons: Add Rule Cancel Previous **Review and Launch**

SSH traffic from the 10.100.0.0/24 net will be allowed.

EC2 - Review

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-06fcc1f0bc2c8943f

Free tier eligible Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.

Root Device Type: ebs Virtualization type: hvm

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Edit instance type

Security Groups

VPC-SG-Private

Description VPCA-SG-Private

Type (i)	Protocol (i)	Port Range (i)	Source (i)	Description (i)
SSH	TCP	22	10.100.0.0/24	

Edit security groups

Instance Details

Number of instances: 1

Network: vpc-0d491f035333874ed
Subnet: subnet-0a919aac4e652a44a

Purchasing option: On demand

EBS-optimized: No

Edit instance details

Cancel **Previous** **Launch**

The EC2 instance review page before launch.

EC2 - key pair

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-06fcc1f0bc2c8943f

Free tier eligible Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.

Root Device Type: ebs Virtualization type: hvm

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)
t2.micro	Variable	1	1

Edit instance type

Security Groups

VPC-SG-Private

Description VPCA-SG-Private

Type (i)	Protocol (i)
SSH	TCP

Edit security groups

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair

Select a key pair

VPCPeerDemo

I acknowledge that I have access to the selected private key file (VPCPeerDemo.pem), and that without this file, I won't be able to log into my instance.

Purchasing option: On demand

Cancel **Launch Instances**

Edit instance details

Number of instances: 1

Network: vpc-0d491f035333874ed
Subnet: subnet-0a919aac4e652a44a

EBS-optimized: No
Monitoring: No
Termination protection: No

Edit instance details

Cancel **Previous** **Launch**

The same previously downloaded key pair is provisioned.

EC2 Dashboard

The screenshot shows the AWS EC2 Dashboard. A specific instance, "Private Server - VPCA", is selected. The instance details are as follows:

- Instance ID:** i-0c36590bbccc9a414
- Instance State:** running
- Instance Type:** t2.micro
- Availability Zone:** us-west-1b
- Status Checks:** 2/2 checks ...
- Alarm Status:** None
- Public DNS:** ip-10-100-1-229.us-west-1.compute.internal
- Private IP:** 10.100.1.229
- VPC ID:** vpc-0d49f03533374ed (VPCA)
- Subnet ID:** subnet-0e919aac4e652a44a (VPCA-Subnet-Private)
- Network interfaces:** enfo
- Source/dest. check:** True
- T2/T3 Unlimited:** Disabled

Private Server is now running. Note the lack of an IPv4 Public IP.

MobaXterm

The screenshot shows the MobaXterm application interface. On the left, there is a list of sessions:

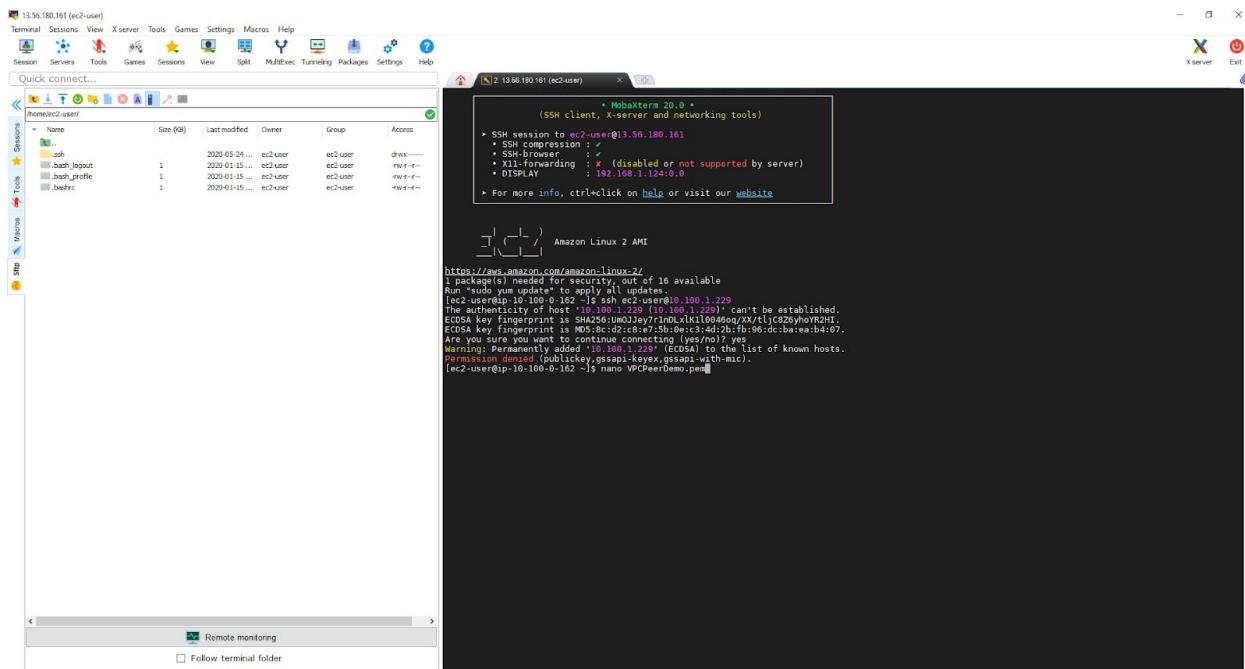
- User sessions:
 - 10.25.218.183 (ec2-user)
 - 10.25.218.180 (ec2-user)
 - 18.144.4.39 (ec2-user)
 - 18.254.201.130 (ec2-user)
 - 1.101.47.173 (ec2-user)
 - 10.18.234.133 (ec2-user)
 - 10.202.36.25 (ec2-user)
 - 32.53.193.231 (ec2-user)
 - 14.224.13.89 (agarry)
 - 14.224.13.89 (ec2-user)
 - 14.224.13.89 (ubuntu)
 - ec2-100-25-218-183.compute-1.amazonaws.com (agarry's 5728)
 - ec2-100-25-218-183.compute-1.amazonaws.com (ec2-user)
- Tools:
 - Session
 - Servers
 - Tools
 - Games
 - Sessions
 - View
 - Split
 - MultiExec
 - Tunneling
 - Packages
 - Settings
 - Help
- Macros:
 - Session
 - Servers
 - Tools
 - Games
 - Sessions
 - View
 - Split
 - MultiExec
 - Tunneling
 - Packages
 - Settings
 - Help

On the right, a "Session settings" window is open, showing the following configuration:

- SSH:** Selected
- Remote host:** 13.56.180.161
- Specify username:** ec2-user
- Port:** 22
- Advanced SSH settings:**
 - X11-Forwarding: checked
 - Compression: checked
 - Execute command: (empty)
 - SSH-browser type: SFTP protocol
- Network settings:**
 - Do not exit after command ends: unchecked
 - Follow SSH path (experimental): unchecked
- Interactive shell:** selected

MobaXterm will be used to SSH into the Public subnet.

MobaXterm



While attempting to SSH into the private instance from the public instance, a permission denial error occurs. Since the pem file is not located on the EC2 instance, a new file must be created.

Locally saved PEM file

Name	Date modified	Type	Size
▼ Today (1)			
VPCPeerDemo.pem	5/24/2020 12:41 PM	PEM File	2 KB

This is the pem file saved locally when the first EC2 instance was created.

Windows 10 - Notepad



```
VPCPeerDemo.pem - Notepad
File Edit Format View Help
-----BEGIN RSA PRIVATE KEY-----
```

Using notepad, the contents of the pem file are displayed. The complete text must be copied.

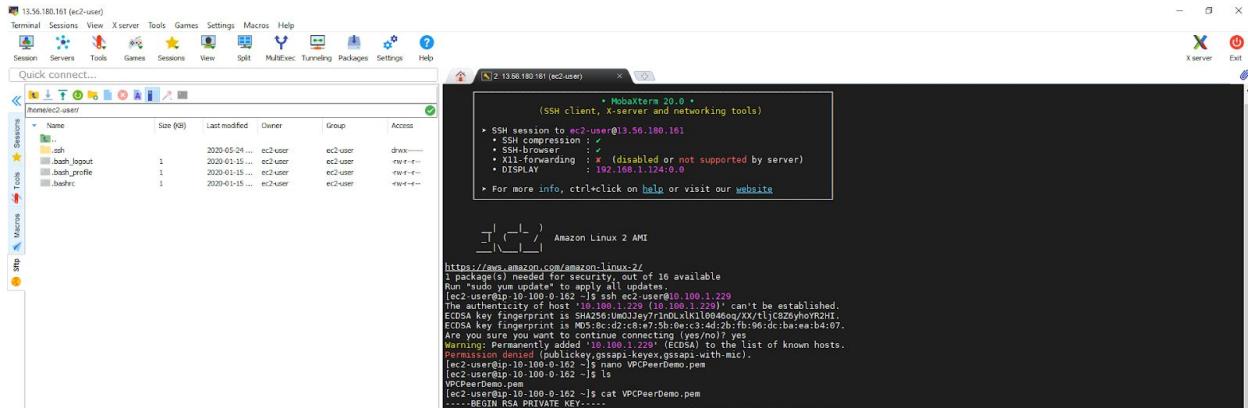
MobaXterm



```
13.56.180.161 (ec2-user)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiTerm Tunneling Packages Settings Help
Quick connect...
GNU nano 2.9.8
-----BEGIN RSA PRIVATE KEY-----
```

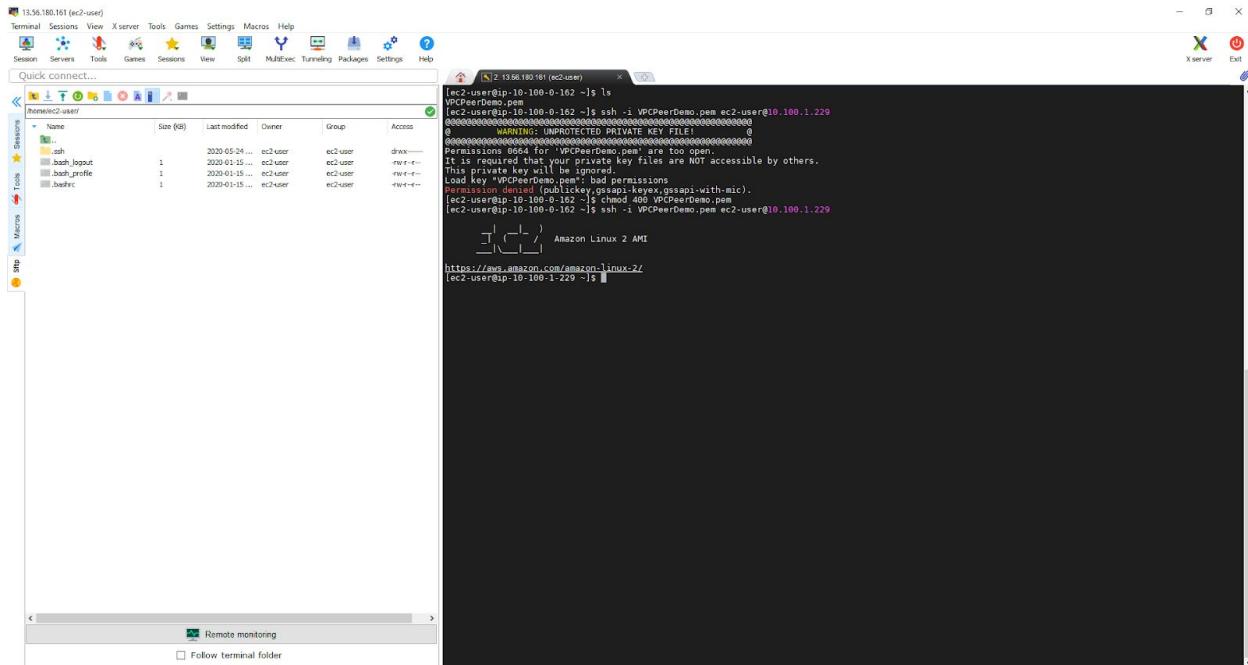
The text is pasted into the file. Note that MobaXterm confirms the correct text before pasting.

MobaXterm



Using the ls command to list files in the current working directory. The contents of the pem file are correct.

MobaXterm



A permission warning occurs. To fix this a chmod 400 command is issued. The local computer has connected to the private EC2 instance through the public EC2 instance.

AWS Console/MobaXterm

The screenshot shows the AWS CloudWatch Metrics interface with a log stream titled 'VPCPeerDemo.pem'. The log entries detail the creation of a VPC peer connection between two AWS accounts. It includes commands like 'ssh -i VPCPeerDemo.pem ec2-user@10.100.1.229' and 'chmod 400 VPCPeerDemo.pem' to manage the private key file.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status
EC2 Private Subnet	i-065b3ae3d0115132	12 micro	us-west-1b	stopped	-
EC2 Public Subnet	i-0e98bcf502eb05ea	12 micro	us-west-1a	stopped	-
Brought Server - VPCA	i-0c36590bbccc9a414	12 micro	us-west-1b	running	-

Instance: i-0c36590bbccc9a414 (Private Server - VPCA) Private IP: 10.100.1.229

Description	Status Checks	Monitoring	Tags
Instance ID	i-0c36590bbccc9a414	Public DNS (IPv4)	-
Instance state	running	IPv4 Public IP	-
Instance type	12 micro	IPv6 IPs	-
Finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more	Elastic IPs	-
Private DNS	ip-10-100-1-229.us-west-1.compute.internal	Availability zone	us-west-1b
Private IPs	10.100.1.229	Security groups	VPCA-SG-Private, view inbound rules, view outbound rules
Secondary private IPs		Scheduled events	No scheduled events
VPC ID	vpc-0d491035333874ed (VPCA)	AMI ID	amzn2-ami-hvm-2.0.20200406.0-x86_64-gp2 (ami-06fc1f0bc2c8943f)
Subnet ID	subnet-09519aac4e652a44a	Platform	-

Feedback English (US) Privacy Policy Terms of Use

A SSH session has been established to the private EC2 instance.

VPCs - Create VPC

[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 [i](#)

IPv4 CIDR block* [i](#)

IPv6 CIDR block No IPv6 CIDR Block [i](#) Amazon provided IPv6 CIDR block

Tenancy [i](#)

* Required [Cancel](#) [Create](#)

Now the VPC to peer connect to will be created. An IG is not required because there will be no internet access.

Subnets - Create subnet

Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag ⓘ

VPC* ⓘ

Availability Zone ⓘ

VPC CIDRs	CIDR	Status	Status Reason
	10.200.0.0/16	associated	

IPv4 CIDR block* ⓘ

* Required Cancel **Create**

This subnet will belong to the VPCB just created.

Route Tables - Create route table

Route Tables > Create route table

Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag ⓘ

VPC* ⓘ

* Required Cancel **Create**

Filter by attributes

vpc-00dd552b0b5c9e556	My VPC
vpc-0354483395efca4c6	VPCB
vpc-56524731	default
vpc-0d4f1f035333874ed	VPCA
vpc-09b6591c2ed32417	VPC_1

This routing table will apply to the VPCB subnet.

VPC - Route tables

The screenshot shows the AWS VPC Route Tables page. A new route table, 'VPCB-RT-Private', has been created and is selected. The table details are as follows:

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
VPCB-RT-Private	rtb-0ebd6505ccc73c2d3	-	-	No	vpc-0354483395efca4c6 VPCB
VPCA-RT-Public	rtb-03198b05e3e7d485	subnet-06f0c22e6b2844e2c	-	No	vpc-04491f035333874ed VPCA
VPCA-RT-Private	rtb-0050b0169fc18814	subnet-0a919aac4e652a44a	-	No	vpc-04491f035333874ed VPCA
Public Route Table	rtb-024d574a4ee9a6389	2 subnets	-	No	vpc-00d5522b0b5c9e656 My VPC
rtb-0aaaf3c16e0352a98f	-	-	-	Yes	vpc-00d5522b0b5c9e656 My VPC
rtb-0b659e61a3678698c	-	-	-	Yes	vpc-04491f035333874ed VPCA
rtb-0e86b16e291553864	-	-	-	Yes	vpc-0354483395efca4c6 VPCB
rtb-365adb5e	-	-	-	Yes	vpc-66524731 default
rtb-018fdfcbe317474d0	-	-	-	Yes	vpc-08b6581c2ed32f417 VPC_1

Route Table: rtb-0ebd6505ccc73c2d3

Summary **Routes** **Subnet Associations** **Edge Associations** **Route Propagation** **Tags**

Route Table ID: rtb-0ebd6505ccc73c2d3
Explicitly Associated with: -
Owner: 758287676661

Main: No
VPC: vpc-0354483395efca4c6 | VPCB

The route table is created for VPCB.

Subnets - Edit route table association

The screenshot shows the 'Edit route table association' page for a specific subnet. The subnet is associated with the 'VPCB-RT-Private' route table, which was just created.

Subnet ID: subnet-05df901393d890436

Route Table ID: rtb-0ebd6505ccc73c2d3

Route table ID **Route table name** **VPC ID**

Route table ID	Route table name	VPC ID
rtb-0ebd6505ccc73c2d3	VPCB-RT-Private	vpc-0354483395efca4c6
rtb-0e86b16e291553864		vpc-0354483395efca4c6

* Required Cancel Save

The route VPCB subnet is now associated with the VPCB route table. Traffic will route locally.

EC2 - Configure instance

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

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

Purchasing option Request Spot instances

Network vpc-0354483395efca4c6 | VPCB

Subnet subnet-05df901393d890436 | VPCB-Subnet-Private
251 IP Addresses available

Auto-assign Public IP Use subnet setting (Disable)

Placement group Add instance to placement group

Capacity Reservation Open

IAM role None

Shutdown behavior Stop

Stop - Hibernate behavior Enable hibernation as an additional stop behavior

Enable termination protection Protect against accidental termination

Monitoring Enable CloudWatch detailed monitoring
Additional charges apply

Tenancy Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.

T2/T3 Unlimited Enable
Additional charges may apply

A new EC2 instance will now be created. Note VPCB and Private subnets are provisioned and auto-assign Public IP is disabled.

EC2 - Add Tags

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key	(128 characters maximum)	Value	(256 characters maximum)	Instances	Volumes
Staff		Aguirre		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

Staff tags established instance ownership.

EC2 - Configure Security Group

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: Create a new security group Select an existing security group

Security group name: VPCB-SG-Private

Description: VPCB-SG-Private

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 10.100.1.0/24	e.g. SSH for Admin Desktop
Custom ICMP	Echo Reply	N/A	Custom 10.100.1.0/24	e.g. SSH for Admin Desktop

Add Rule

Cancel Previous Review and Launch

A security group for SSH and ICMP is created.

EC2 - Review

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-06fcc1f0bc2c8943f

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)
t2.micro	Variable	1	1

Security Groups

Security group name: VPCB-SG-Private
Description: VPCB-SG-Private

Type: SSH Protocol: TCP
Custom ICMP Rule - IPv4: Echo Reply

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair: Select a key pair: VPCPeerDemo
 I acknowledge that I have access to the selected private key file (VPCPeerDemo.pem), and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

Edit AMI Edit instance type Edit security groups Edit instance details Cancel Previous Launch

The key pair from the first EC2 instance is still in use.

EC2 Dashboard

The screenshot shows the AWS EC2 Dashboard. At the top, there are buttons for 'Launch Instance', 'Connect', and 'Actions'. A search bar is present above the instance list. The instance list table includes columns for Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, Public IP, IPv4 Public IP, IPv6 IP, Key Name, Monitoring, and Launch Time. Six instances are listed:

- Private Server - VPCB**: Instance ID i-08ffea8a728ceeb, t2.micro, us-west-1a, running, 2/2 checks, None, - (Public IP), - (IPv4 Public IP), - (IPv6 IP), VPCPeerDemo, disabled, May 24, 2020 at 1:56:45 PM.
- Private Server - VPCA**: Instance ID i-0c36590bbcc9a414, t2.micro, us-west-1b, running, 2/2 checks, None, - (Public IP), 13.56.180.161 (IPv4 Public IP), - (IPv6 IP), VPCPeerDemo, disabled, May 24, 2020 at 12:42:30 P.
- Web Server**: Instance ID i-074b2c0a919sec42, t2.micro, us-west-1a, stopped, None, - (Public IP), - (IPv4 Public IP), - (IPv6 IP), - (Key Name), disabled, May 23, 2020 at 1:41:04 PM.
- EC2 Private Subnet**: Instance ID i-06bb3ae3df0115132, t2.micro, us-west-1b, terminated, None, - (Public IP), - (IPv4 Public IP), - (IPv6 IP), - (Key Name), disabled, May 22, 2020 at 7:51:36 PM.
- EC2 Public Subnet**: Instance ID i-095bca5f02e0b5ea, t2.micro, us-west-1a, terminated, None, - (Public IP), - (IPv4 Public IP), - (IPv6 IP), - (Key Name), disabled, May 22, 2020 at 7:42:25 PM.

Below the list, it says 'Instance: i-08ffea8a728ceeb (Private Server - VPCB) Private IP: 10.200.1.34'. A detailed view of the selected instance (i-08ffea8a728ceeb) is shown with tabs for Description, Status Checks, Monitoring, and Tags. The Description tab displays various details like Instance ID, State, Type, DNS, and Network interfaces. The Status Checks tab shows 2/2 checks passing. The Monitoring tab indicates monitoring is disabled. The Tags tab lists the key pair name as VPCPeerDemo.

Private server now running.

Peering Connection - Create Peering Connection

The screenshot shows the 'Create Peering Connection' wizard. Step 1: Select a local VPC to peer with. It asks for a peering connection name tag ('VPCA to VPCB'). Below that, it says 'Select a local VPC to peer with' and shows a dropdown for 'VPC (Requester)*' containing 'vpc-0d491f03533874ed'. This dropdown has a table below it showing CIDRs, Status, and Status Reason for the selected VPC. The table shows one entry: '10.100.0.0/16' with status 'associated'.

Step 2: Select another VPC to peer with. It asks for 'Account' (My account or Another account) and 'Region' (This region (us-west-1) or Another Region). It also shows a dropdown for 'VPC (Acceptor)*' containing 'vpc-0354483395efca4c6'. This dropdown has a table below it showing CIDRs, Status, and Status Reason for the selected VPC. The table shows one entry: '10.200.0.0/16' with status 'associated'.

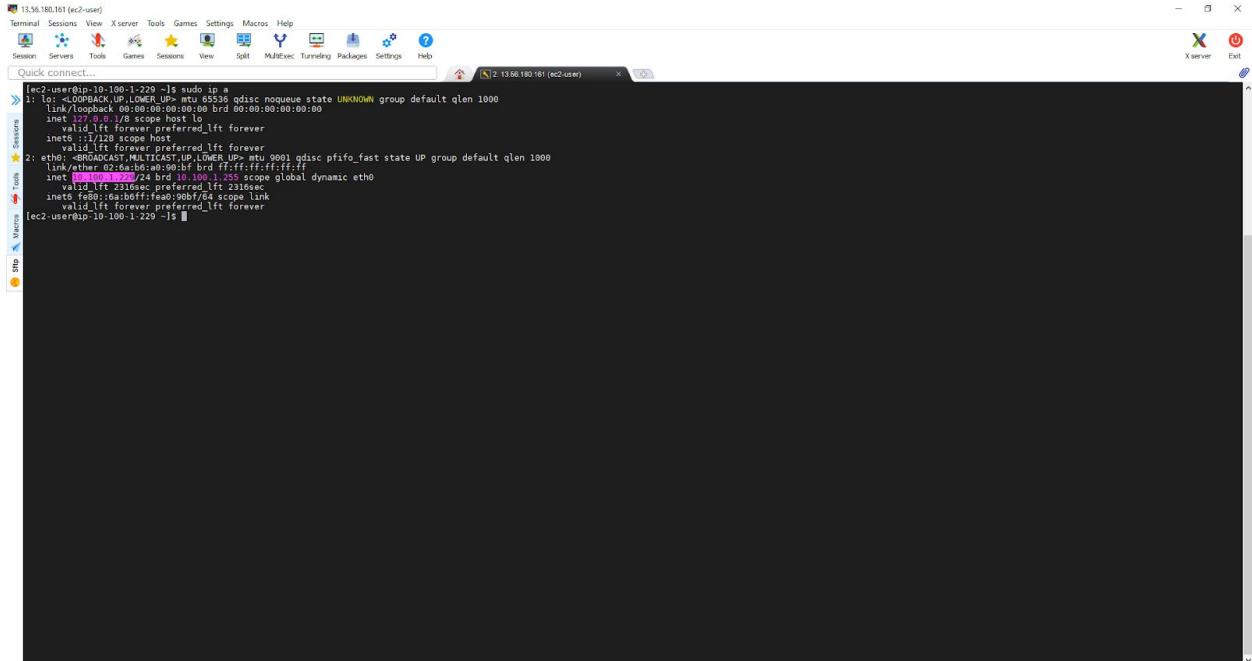
At the bottom, there are 'Cancel' and 'Create Peering Connection' buttons. A note says '* Required'.

A Peer Connection will be established between VPCA and VPCB.

Peering Connections - Request

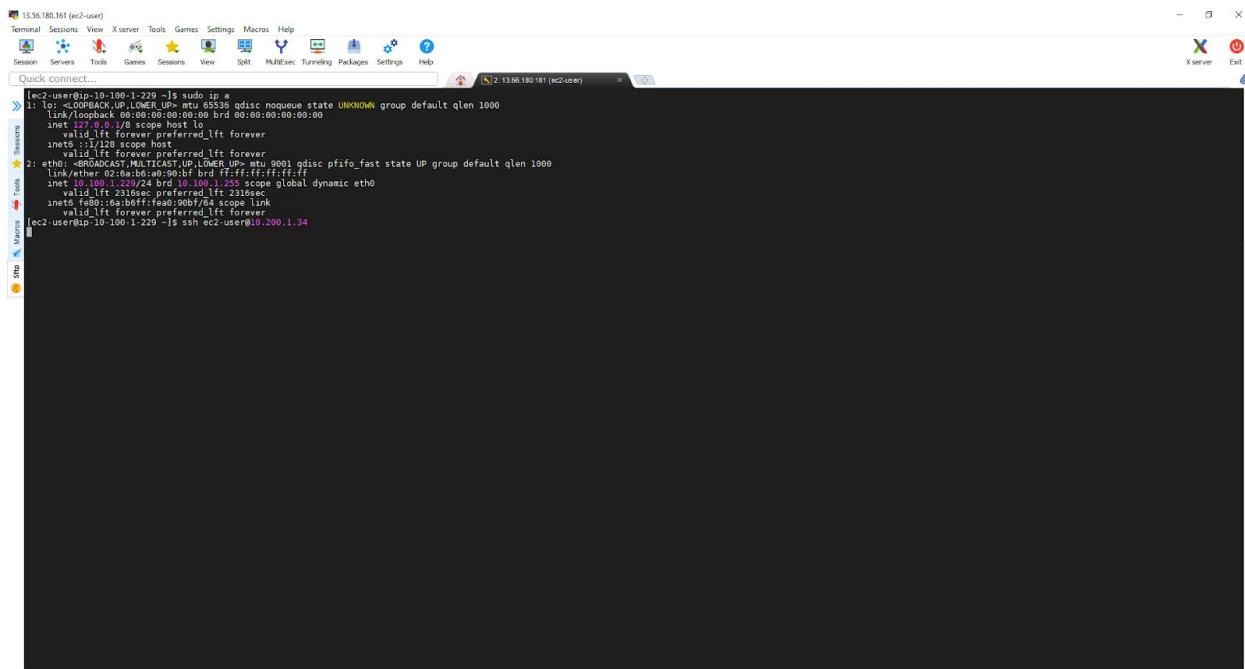


The connection must be accepted before a peer connection is made.



Next a peer connection from the private VPCA to private VPCB will be established. Using the command sudo ip a, to verify the IP corresponds to the private VPCA IP.

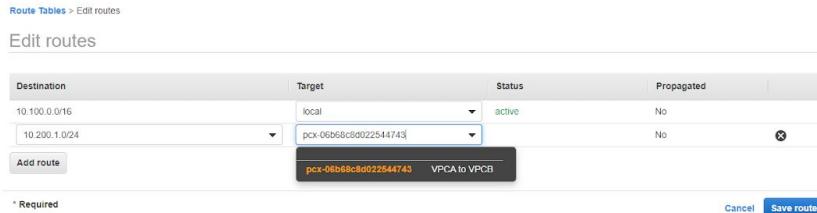
MobaXterm



```
[ec2-user@ip-10-100-1-229 ~]$ sudo ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
        valid_lft forever preferred_lft forever
        inets 1:1/2 scope host
    inets fe80::ca:beff:fea:90bf/64 scope link
        valid_lft forever preferred_lft forever
[ec2-user@ip-10-100-1-229 ~]$ ssh ec2-user@10.200.1.34
```

The connection hangs. This is because the routing tables are not properly set up between VPCA and VPCB.

Route Tables - Edit routes



Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
10.200.1.0/24	pcx-06b68c8d022544743	No	

Add route

* Required

By establishing the VPCB destination and Peer Connection target, a connection can be made between VPCA and VPCB. Note the same change must be established for VPCB private.

VPC - Route tables

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
VPCB-RT-Private	rtb-0ebd6505cc73c2d3	subnet-05df901393d690436	-	No	vpc-0354483395efca405 VPCB
VPCA-RT-Public	rtb-03198b003e3c7cd855	subnet-0670c2266b2844e2c	-	No	vpc-0d491f035333874ed VPCA
VPCA-RT-Private	rtb-0058b0169fc18814	subnet-0a919aac4e652a44a	-	No	vpc-0d491f035333874ed VPCA
Public Route Table	rtb-024d57494e0e956309	2 subnets	-	No	vpc-0dd522b00b5c9e6556 My VPC
rtb-0a3fc16e0352a98f	-	-	-	Yes	vpc-00d5522b00b5c9e6556 My VPC
rtb-0655e61a3d76698c	-	-	-	Yes	vpc-0d491f035333874ed VPCA
rtb-0e66b16e291553964	-	-	-	Yes	vpc-0554483395efca405 VPCB
rtb-385ad5e	-	-	-	Yes	vpc-56524731 default
rtb-0180dc8e317474d0	-	-	-	Yes	vpc-08b6581c2e3232417 VPC_1

Route Table: rtb-0058b0169fc18814											
Summary	Routes	Subnet Associations									
Edit routes	View All routes	Edit associations									
<table border="1"> <thead> <tr> <th>Destination</th> <th>Target</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>10.100.0.0/16</td> <td>local</td> <td>active</td> </tr> <tr> <td>10.200.1.0/24</td> <td>pcx-06b68c8d022544743</td> <td>active</td> </tr> </tbody> </table>			Destination	Target	Status	10.100.0.0/16	local	active	10.200.1.0/24	pcx-06b68c8d022544743	active
Destination	Target	Status									
10.100.0.0/16	local	active									
10.200.1.0/24	pcx-06b68c8d022544743	active									

Note 10.200.1.0/24 is listed under Routes.

Destination	Target	Status	Propagated
10.200.0.0/16	local	active	No
10.100.1.0/24	pcx-06b68c8d022544743	active	No

Add route [pcx-06b68c8d022544743](#) VPCA to VPCB

* Required [Cancel](#) [Save routes](#)

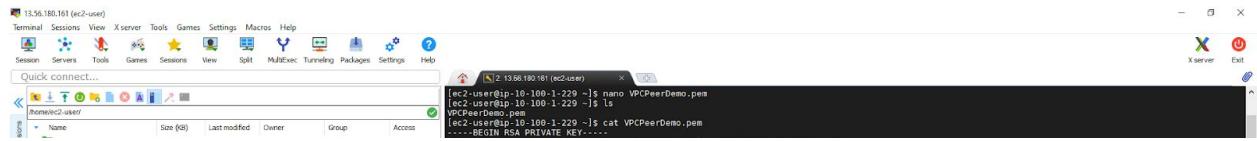
By establishing the VPCA destination and Peer Connection target, a connection can be made between VPCA and VPCB.

VPC - Route tables

The screenshot shows the AWS VPC Route Tables page. At the top, there are buttons for 'Create route table' and 'Actions'. Below is a search bar and a table with columns: Name, Route Table ID, Explicit subnet association, Edge associations, Main, and VPC ID. The table lists several route tables, including 'VPCB-RT-Private', 'VPCA-RT-Public', 'VPCA-RT-Private', 'Public Route Table', 'rtb-024574a4eeea965389', 'rtb-0aa3c3c16e035298f', 'rtb-0b659e61a3976698c', 'rtb-0e6b16e291553064', 'rtb-388abd5e', and 'rtb-018fd1c6e517474d0'. The 'Public Route Table' is highlighted.

Below the table, a specific route table ('rtb-0ebd505ccc73c2d3') is selected. A navigation bar at the top of this section includes 'Summary', 'Routes' (which is selected), 'Subnet Associations', 'Edge Associations', 'Route Propagation', and 'Tags'. Under 'Edit routes', a dropdown menu shows 'View All routes'. The 'Routes' table has columns: Destination, Target, and Status. It contains two entries: '10.200.0.0/16' with target 'local' and status 'active', and '10.100.1.0/24' with target 'pxc-05b68c8d02254743' and status 'active'.

Note 10.100.1.0/24 is listed under Routes.



The pem key must be saved to the EC2 instance. Permissions are changed to 400 with the chmod command.

MobaXterm

```
[ec2-user@ip-10-100-1-229 ~]$ nano VPCPeerDemo.pem
[ec2-user@ip-10-100-1-229 ~]$ ls
VPCPeerDemo.pem
[ec2-user@ip-10-100-1-229 ~]$ cat VPCPeerDemo.pem
-----BEGIN RSA PRIVATE KEY-----
```

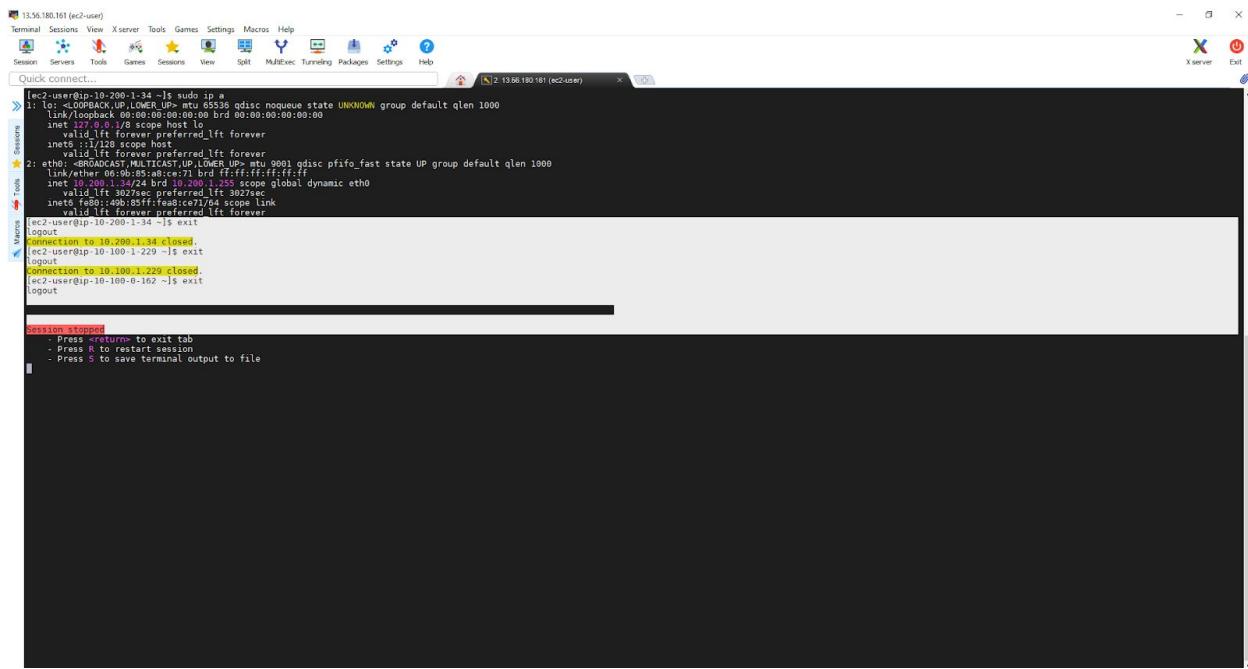
Success! A properly configured Peer Connection has been established between VPCA and VPCB.

AWS Console/MobaXterm

Handler	lambda_function.lambda_handler
Runtime	Python 3.8
Memory (MB)	128
Timeout (seconds)	3
Tracing	None

As these are private VPC's with an IP defined route table, there is no other way to have an active connection to the Private server of VPCB.

MobaXterm



Another verification method for subnet connections is when exiting MobaXterm. MobaXterm will display the IP's used in the SSH sessions. Each IP matches the EC2 instance IP.