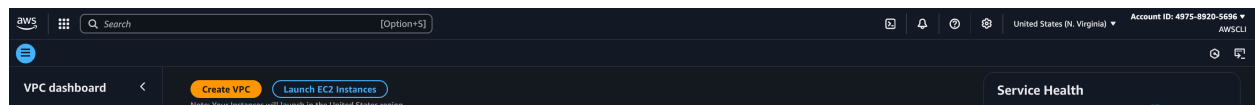


create your own Network architecture with at least 3 public Subnets and 6 private subnets.
class review: Week 4 - Class 7 ZION: Yacht Party OCT 04

Dennis' Network architecture

region = virginia (us-east-1)		
		10.71.0.0/16
public	10.71.1.0/24	a
public	10.71.2.0/24	b
public	10.71.3.0/24	c
public	10.71.4.0/24	d
private	10.71.11.0/24	a
private	10.71.12.0/24	b
private	10.71.13.0/24	c
private	10.71.14.0/24	d
private	10.71.21.0/24	a
private	10.71.22.0/24	b
private	10.71.23.0/24	c
private	10.71.24..0/24	d

Go to AWS and create a VPC



name it
fill in IPv4 CIDR block
number of availability zones - 3
number of public subnets - 3
number of private subnets - 6
Customized subnets CIDR blocks - fill out using my architecture
NAT gateways - In 1 AZ
VPC endpoints - None

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.

☐ VPC only ☒ VPC and more

Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☒ Auto-generate
dennis-network-lab-wk4

IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.

10.71.0.0/16 65,536 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info
☒ No IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block

Tenancy Info
Default

Number of Availability Zones (AZs) Info
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1 | 2 | **3**

► Customize AZs

Number of public subnets Info
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the Internet.

0 | **3**

Number of private subnets Info
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0 | 3 | **6**

► Customize subnets CIDR blocks

NAT gateways (\$) Info
Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway.

None | **In 1 AZ** | 1 per AZ

VPC endpoints Info
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None | S3 Gateway

DNS options Info
☒ Enable DNS hostnames
☒ Enable DNS resolution

► Additional tags

Preview

Subnets (9)

Subnets within this VPC

- us-east-1a
 - dennis-network-lab-wk4-subnet-
 - dennis-network-lab-wk4-subnet-
 - dennis-network-lab-wk4-subnet-
- us-east-1b
 - dennis-network-lab-wk4-subnet-
 - dennis-network-lab-wk4-subnet-
 - dennis-network-lab-wk4-subnet-
- us-east-1c
 - dennis-network-lab-wk4-subnet-
 - dennis-network-lab-wk4-subnet-
 - dennis-network-lab-wk4-subnet-

Route tables (7)

Route network traffic to resources

- dennis-network-lab-wk4-rtb-public
- dennis-network-lab-wk4-rtb-private1-
- dennis-network-lab-wk4-rtb-private2-
- dennis-network-lab-wk4-rtb-private3-
- dennis-network-lab-wk4-rtb-private4-
- dennis-network-lab-wk4-rtb-private5-
- dennis-network-lab-wk4-rtb-private6-

Network connections (2)

Connections to other networks

- dennis-network-lab-wk4-igw
- dennis-network-lab-wk4-nat-public1

[Cancel](#) [Preview code](#) [Create VPC](#)

Create VPC

Create VPC workflow

Success

Details

- Create VPC: vpc-08f5452bdde6ac295
- Enable DNS hostnames
- Enable DNS resolution
- Verifying VPC creation: vpc-08f5452bdde6ac295
- Create subnet: subnet-06fa59f97d0a6ae0e
- Create subnet: subnet-0ffbbae0d70267554
- Create subnet: subnet-0011a6029d6343f58
- Create subnet: subnet-0e096a0212e1bcd28
- Create subnet: subnet-082f2a2d10fc66f8e
- Create subnet: subnet-0054791c7ec1adb0
- Create subnet: subnet-07286747a83a1b411
- Create subnet: subnet-0401aadf496cbe3dd
- Create subnet: subnet-082e4416ce2ca2959
- Create internet gateway: igw-0165f1d962abe7b09
- Attach internet gateway to the VPC
- Create route table: rtb-0ae14dd8c35aa667a
- Create route
- Associate route table
- Associate route table
- Associate route table
- Allocate elastic IP: eipalloc-0d0e86da9f3661146
- Create NAT gateway: nat-0c354add33ba45ca1
- Wait for NAT Gateways to activate
- Create route table: rtb-0507274f20ace8f0c
- Create route
- Associate route table
- Create route table: rtb-06261557155fc5d24
- Create route
- Associate route table
- Create route table: rtb-02a9c01c899f7c6bf
- Create route
- Associate route table
- Create route table: rtb-0231d497b555121e8
- Create route
- Associate route table
- Create route table: rtb-0027d50a3db08339c
- Create route
- Associate route table
- Create route table: rtb-09d12a55da4f9e509
- Create route
- Associate route table
- Verifying route table creation

View VPC

vpc-08f5452bdde6ac295 / dennis-network-lab-wk4-vpc

Actions

Details

Info

VPC ID
vpc-08f5452bdde6ac295

DNS resolution
Enabled

Main network ACL
acl-0b69ed1d5a78f5e78

IPv6 CIDR (Network border group)
-

State

Available

Tenancy
default

Default VPC
No

Network Address Usage metrics
Disabled

Block Public Access

Off

DHCP option set
dopt-0f21e38a07d7727ba

IPv4 CIDR
10.71.0.0/16

Route 53 Resolver DNS Firewall rule groups
-

DNS hostnames

Enabled

Main route table
rtb-0fd1fbf0180ff77cf

IPv6 pool
-

Owner ID
497589205696

Resource map

Info

VPC

Your AWS virtual network

dennis-network-lab-wk4-vpc

10.71.0.0/16

No IPv6

Subnets (9)

Subnets within this VPC

us-east-1a

dennis-network-lab-wk4-subnet-pu...

10.71.1.0/24

No IPv6

dennis-network-lab-wk4-subnet-pr...

10.71.21.0/24

No IPv6

dennis-network-lab-wk4-subnet-pr...

10.71.11.0/24

No IPv6

us-east-1b

dennis-network-lab-wk4-subnet-pu...

10.71.2.0/24

No IPv6

dennis-network-lab-wk4-subnet-pr...

10.71.12.0/24

No IPv6

dennis-network-lab-wk4-subnet-pr...

10.71.22.0/24

No IPv6

us-east-1c

dennis-network-lab-wk4-subnet-pu...

10.71.3.0/24

No IPv6

dennis-network-lab-wk4-subnet-pr...

10.71.23.0/24

No IPv6

dennis-network-lab-wk4-subnet-pr...

10.71.13.0/24

No IPv6

Route tables (8)

Route network traffic to resources

rtb-0fd1fbf0180ff77cf

No subnet associations

1 route including local

dennis-network-lab-wk4-rtb-private6...

1 subnet association

2 routes including local

dennis-network-lab-wk4-rtb-private2...

1 subnet association

2 routes including local

dennis-network-lab-wk4-rtb-private4...

1 subnet association

2 routes including local

dennis-network-lab-wk4-rtb-private1...

1 subnet association

2 routes including local

dennis-network-lab-wk4-rtb-public

3 subnet associations

2 routes including local

dennis-network-lab-wk4-rtb-private5...

1 subnet association

2 routes including local

dennis-network-lab-wk4-rtb-private3...

1 subnet association

2 routes including local

Network Connections (2)

Connections to other networks

dennis-network-lab-wk4-igw

Internet routes to 3 public subnets

6 private subnets route to the Internet

dennis-network-lab-wk4-nat-public1-...

Public NAT gateway

1 ENI with 1 EIP

Show all details

View VPC
 Make an EC2 instance
 first create public security group
 name it and *put public in the title
 add a description
 choose VPC created
 Inbound rules: HTTP, SSH, and All ICMP - IPv4 *so we can ping the device later

Create security group [info](#)
 A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [info](#)
 dennis-network-lab-wk4-public
 Name cannot be edited after creation.

Description [info](#)
 dennis-network-lab-wk4-public

VPC [info](#)
 vpc-08f5452bdde6ac295 (dennis-network-lab-wk4-vpc)

Inbound rules [info](#)

Type	Protocol	Port range	Source	Description - optional	
HTTP	TCP	80	Anywhere...	unsecured internet	Delete
All ICMP - IPv4	ICMP	All	Anywhere...	enables ping the device	Delete
SSH	TCP	22	Anywhere...	remote login	Delete

[Add rule](#)

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

Outbound rules [info](#)

Type	Protocol	Port range	Destination	Description - optional	
All traffic	All	All	Custom		Delete

[Add rule](#)

Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.

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.
 No tags associated with the resource.
[Add new tag](#)
 You can add up to 50 more tags

[Cancel](#) [Create security group](#)

sg-0e30dc95b1b107b03 - dennis-network-lab-wk4-public [Actions](#)

Details

Security group name dennis-network-lab-wk4-public	Security group ID sg-0e30dc95b1b107b03	Description dennis-network-lab-wk4-public	VPC ID vpc-08f5452bdde6ac295
Owner 497589205696	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

[Inbound rules](#) [Outbound rules](#) [Sharing - new](#) [VPC associations - new](#) [Tags](#)

Inbound rules (3) [Manage tags](#) [Edit inbound rules](#)

	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sg-0ab687db773655100	IPv4	SSH	TCP	22	0.0.0.0/0	remote login
<input type="checkbox"/>	-	sg-02b352cb3567acddf	IPv4	HTTP	TCP	80	0.0.0.0/0	unsecured internet
<input type="checkbox"/>	-	sg-0304eaa0b315ccf05	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0	enables ping the device

Outbound rules : DON'T TOUCH

create private security group

Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name

dennis-network-lab-wk4-private

Name cannot be edited after creation.

Description

dennis-network-lab-wk4-private

VPC

vpc-08f5452bdde6ac295 (dennis-network-lab-wk4-vpc)

Inbound rules

Type

HTTP

Protocol

TCP

Port range

80

Source

Anywhe...

Description - optional

Delete

Type

All ICMP - IPv4

Protocol

ICMP

Port range

All

Source

Anywhe...

Description - optional

Delete

Add rule

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

Outbound rules

Type

All traffic

Protocol

All

Port range

All

Destination

Custom

Description - optional

Delete

Add rule

Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.

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.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Create security group

sg-0eebe8e28b12d0f79 - dennis-network-lab-wk4-private

Actions

Details

Security group name

dennis-network-lab-wk4-private

Security group ID

sg-0eebe8e28b12d0f79

Description

dennis-network-lab-wk4-private

VPC ID

vpc-08f5452bdde6ac295

Owner

497589205696

Inbound rules count

2 Permission entries

Outbound rules count

1 Permission entry

Inbound rules

Outbound rules

Sharing - new

VPC associations - new

Tags

Inbound rules (2)

Search

Manage tags

Edit inbound rules

Name

Security group rule ID

IP version

Type

Protocol

Port range

Source

Description

-

sgr-0bbfca3609d74d75c

IPv4

All ICMP - IPv4

ICMP

All

0.0.0.0/0

-

-

sgr-02b8fe5e8f2e45644

IPv4

HTTP

TCP

80

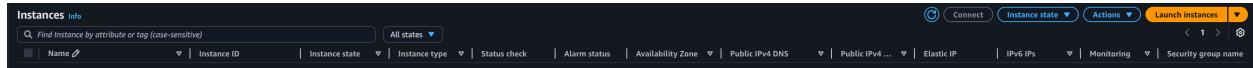
0.0.0.0/0

-

Add inbound rules: HTTP and All ICMP - IPv4

Page 5

create instance
go to EC2 - instance
launch instance



name - put public in the name of
Key pair - use the default (Proceed without a key pair...)
Network settings - Edit
VPC - choose the one created
Auto-assign public IP - enable
Firewall - select existing security group
common security groups - select the public one created
Advance details - scroll to the bottom and add script in the user data

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

dennis-network-lab-wk4-public

Add additional tags

Application and OS Images (Amazon Machine Image) Info

Instance type Info | Get advice

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Proceed without a key pair (Not recommended)

Default value

Create new key pair

Network settings Info

VPC - *required* Info

vpc-08f5452bdd6e6ac295 (dennis-network-lab-wk4-vpc)

Subnet Info

subnet-0011a6029d6343f58 dennis-network-lab-wk4-subnet-public3-us-east-1c

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

Common security groups Info

Select security groups

dennis-network-lab-wk4-public sg-0e30dc95b1b107b03

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

Advanced network configuration

Configure storage Info Advanced

1x 8 GIB gp3 Root volume, 3000 IOPS, Not encrypted

Add new volume

Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

Edit

Advanced details Info

Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.9.2...read more

ami-0341d95f75f311023

Virtual server type (instance type)

t3.micro

Firewall (security group)

dennis-network-lab-wk4-public

Storage (volumes)

1 volume(s) - 8 GIB

Cancel

Launch instance

Preview code

Page 6

Launch Instance

✓ **Success**
Successfully initiated launch of instance (i-03bd54fa757d13a37)

launch a private instance
name - private in the name
Network settings/subnet choose private subnet
auto-assign public IP - disable
common security groups - choose the created private group

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

dennis-network-lab-wk4-private [Add additional tags](#)

Application and OS Images (Amazon Machine Image) Info

Instance type Info | Get advice

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

☐ Proceed without a key pair (Not recommended) ☐ Default value [Create new key pair](#)

Network settings Info

VPC - *required* Info

vpc-08f5452bdde6ac295 (dennis-network-lab-wk4-vpc) [Refresh](#)

Subnet Info

subnet-0e096a0212e1bcd28 dennis-network-lab-wk4-subnet-private1-us-east-1a [Create new subnet](#)

VPC: vpc-08f5452bdde6ac295 Owner: 497589205696 Availability Zone: us-east-1a (use 1-a24)
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.71.11.0/24

Auto-assign public IP Info

☐ Enable ☒ Disable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group ☒ Select existing security group

Common security groups Info

Select security groups

dennis-network-lab-wk4-private sp-0eebe8e28b12d0f79 [Compare security group rules](#)

VPC: vpc-08f5452bdde6ac295

Security groups that you add or remove here will be added to or removed from all your network interfaces.

[Advanced network configuration](#)

Configure storage Info Advanced

1x GiB Root volume, 3000 IOPS, Not encrypted

[Add new volume](#)

[Click refresh to view backup information](#) [Refresh](#)

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems [Edit](#)

Advanced details Info

Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.9.2...[read more](#)
ami-0341d95f75f311023

Virtual server type (instance type)

t3.micro

Firewall (security group)

dennis-network-lab-wk4-private

Storage (volumes)

1 volume(s) ~ 8 GiB

[Cancel](#) [Launch Instance](#) [Preview code](#)

launch instance



Instances (2)

Info

Last updated less than a minute ago

Connect

Instance state

Actions

Launch instances

Find Instance by attribute or tag (case-sensitive)

All states


< 1 >

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
<input type="checkbox"/>	dennis-network-lab-wk4-public	i-03bd54fa757d13a37	Running	t3.micro	3/3 checks passed	View alarms	us-east-1c	ec2-3-238-27-1
<input type="checkbox"/>	dennis-network-lab-wk4-private	i-05d29d338b1d62396	Running	t3.micro	Initializing	View alarms	us-east-1a	-

go to public instance, copy public DNC and past with http://

AWS Instance Details

Samurai Katana



insert an image or GIF

Instance Name: ip-10-71-3-27.ec2.internal

Instance Private Ip Address: 10.71.3.27

Availability Zone: us-east-1c

Virtual Private Cloud (VPC): vpc-08f5452bdde6ac295

to check the private instance go to private instance and copy the private IPv4 address

Instance ID	Public IPv4 address	Private IPv4 addresses
<input type="checkbox"/> i-05d29d338b1d62396	-	<input type="checkbox"/> 10.71.11.221

go back to instance choose public instance and connect

Instances (1/2) Info

Last updated 13 minutes ago

Connect

Instance state

Actions

Launch instances

Find Instance by attribute or tag (case-sensitive)

All states

< 1 >

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
<input checked="" type="checkbox"/>	dennis-network-lab-wk4-public	i-03bd54fa757d13a37	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1c	ec2-3-238-27-1
<input type="checkbox"/>	dennis-network-lab-wk4-private	i-05d29d338b1d62396	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1a	-

taken to the connect page, leave all the defaults and hit connect

Connect

info

Connect to an instance using the browser-based client.


EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID


 i-03bd54fa757d13a37 (dennis-network-lab-wk4-public)

Connection type

☒ Connect using a Public IP
Connect using a public IPv4 or IPv6 address

☐ Connect using a Private IP
Connect using a private IP address and a VPC endpoint

☒ Public IPv4 address

 3.238.27.119


☐ IPv6 address
-

Username

Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ec2-user.

Q ec2-user

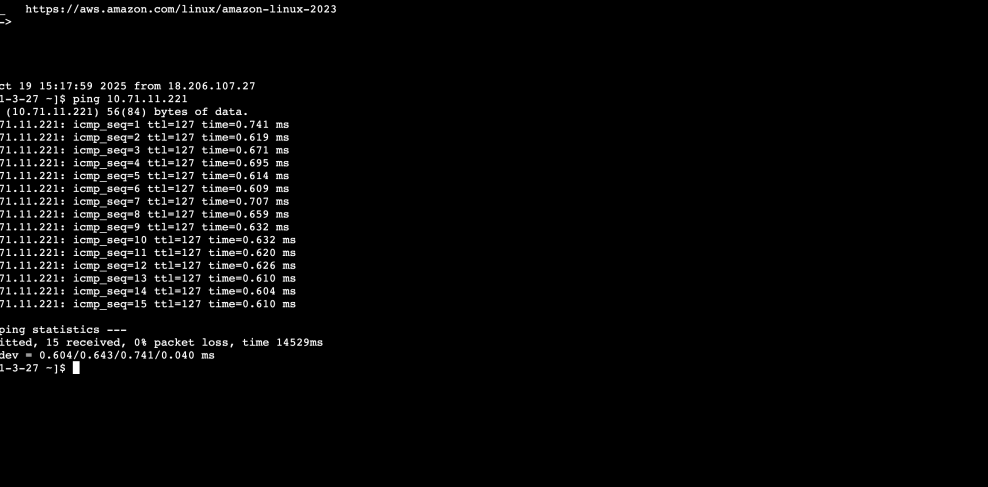
X

 Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

Cancel

Connect

type my private IPv4 address that I copied and type it with ping in the front (ping 10.71.11.221)
*if you don't want your pings to be infinite you can click "control+c" to stop or choose how the amount of pings ie. "ping -c 10 10.71.11.221" I've chosen 10 pings



The screenshot shows a terminal window with a network diagram at the top. The diagram includes a host labeled 'Amazon Linux 2023' with IP '10.71.11.221' and a URL 'https://aws.amazon.com/linux/amazon-linux-2023'. Below the diagram, a terminal session is shown:

```

Last login: Sun Oct 19 15:17:59 2025 from 18.206.107.27
[ec2-user@ip-10-71-3-27 ~]$ ping 10.71.11.221
PING 10.71.11.221 (10.71.11.221) 56(84) bytes of data.
64 bytes from 10.71.11.221: icmp_seq=1 ttl=127 time=0.741 ms
64 bytes from 10.71.11.221: icmp_seq=2 ttl=127 time=0.619 ms
64 bytes from 10.71.11.221: icmp_seq=3 ttl=127 time=0.671 ms
64 bytes from 10.71.11.221: icmp_seq=4 ttl=127 time=0.695 ms
64 bytes from 10.71.11.221: icmp_seq=5 ttl=127 time=0.614 ms
64 bytes from 10.71.11.221: icmp_seq=6 ttl=127 time=0.609 ms
64 bytes from 10.71.11.221: icmp_seq=7 ttl=127 time=0.707 ms
64 bytes from 10.71.11.221: icmp_seq=8 ttl=127 time=0.659 ms
64 bytes from 10.71.11.221: icmp_seq=9 ttl=127 time=0.632 ms
64 bytes from 10.71.11.221: icmp_seq=10 ttl=127 time=0.632 ms
64 bytes from 10.71.11.221: icmp_seq=11 ttl=127 time=0.620 ms
64 bytes from 10.71.11.221: icmp_seq=12 ttl=127 time=0.626 ms
64 bytes from 10.71.11.221: icmp_seq=13 ttl=127 time=0.610 ms
64 bytes from 10.71.11.221: icmp_seq=14 ttl=127 time=0.604 ms
64 bytes from 10.71.11.221: icmp_seq=15 ttl=127 time=0.610 ms
^C
-- 10.71.11.221 ping statistics --
15 packets transmitted, 15 received, 0% packet loss, time 14529ms
rtt min/avg/max/mdev = 0.604/0.643/0.741/0.040 ms
[ec2-user@ip-10-71-3-27 ~]$

```

At the bottom of the terminal window, there is a status bar with the text: 'i-03bd54fa757d13a37 (dennis-network-lab-wk4-public)'.

Everything looks good!

Now tear down *in reverse to how it was created

Terminate EC2 Instances

Go to EC2 Dashboard → Instances.
Select and terminate all instances in your VPC.
Delete NAT Gateway

Go to VPC Dashboard → NAT Gateways.
Delete the NAT Gateway.
Release the associated Elastic IP (in EC2 Dashboard → Elastic IPs).
Delete Subnets

Go to VPC Dashboard → Subnets.
Delete all subnets in your VPC (public and private).
Detach and Delete Internet Gateway

Go to VPC Dashboard → Internet Gateways.
Detach the Internet Gateway from your VPC.
Delete the Internet Gateway.
Delete Route Tables

Go to VPC Dashboard → Route Tables.
Delete any custom route tables (not the main route table).
Delete Security Groups

Go to VPC Dashboard → Security Groups.
Delete any custom security groups (default cannot be deleted until VPC is deleted).
Delete the VPC

Go to VPC Dashboard → Your VPCs.
Delete the VPC.