Cloud Network Deployment with AWS: Configuring VPCs and EC2 Instances

By Michael Emil Santos

Introduction

This project demonstrates configuring both default and custom Virtual Private Cloud (VPC) networks and deploying Elastic Compute Cloud (EC2) instances using AWS. By setting up these environments, I gained experience in cloud networking essentials, such as IP addressing, subnets, internet gateways, and routing.

Project Objectives and Steps

1. Configuring the Default VPC

- Objective: Understand and utilize AWS's default VPC setup.
- Steps: Reviewed the CIDR range, configured default subnets, and verified the internet gateway and route table settings to enable external connectivity for the instances.

2. Creating a Custom VPC

- Objective: Set up a unique VPC with customized IP addressing and network configurations.
- Steps: Designed a custom VPC, created subnets, and configured an internet gateway and routing table for controlled internet access.

3. Deploying EC2 Instances

- Objective: Launch EC2 instances in both the default and custom VPCs to test network connectivity.
- Steps: Deployed instances in each VPC, tested connectivity by pinging the public IPs, and accessed hosted web pages to verify network configurations.

Key Findings

1. Network Segmentation and Security

- Setting up both default and custom VPCs demonstrated the flexibility of AWS networking, allowing for segmentation and controlled internet access based on configuration needs.

2. Connectivity Testing

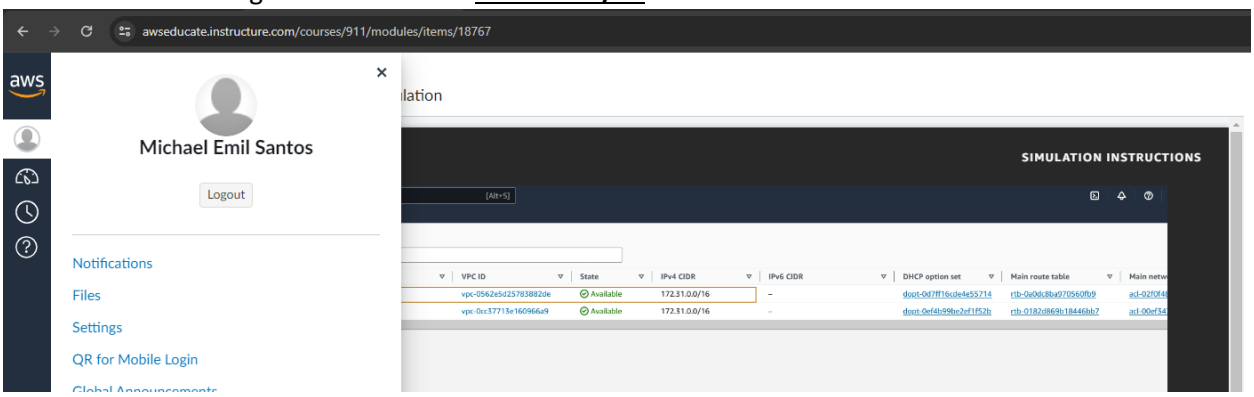
- Verified network connectivity by accessing public IPs and confirming internet access through the internet gateway, ensuring correct VPC and route table settings.

3. Challenges and Solutions

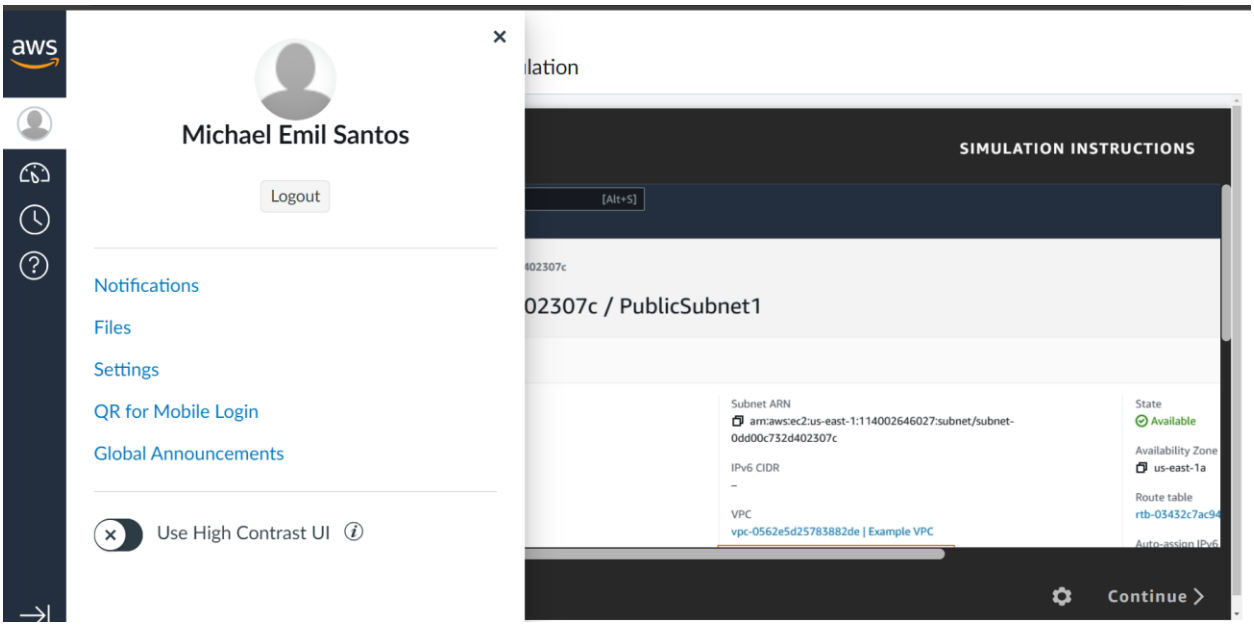
- Challenge: Ensuring accurate configuration between the internet gateway and subnets.
- Solution: Regular checks and adjustments in the routing tables and security groups to confirm connectivity.

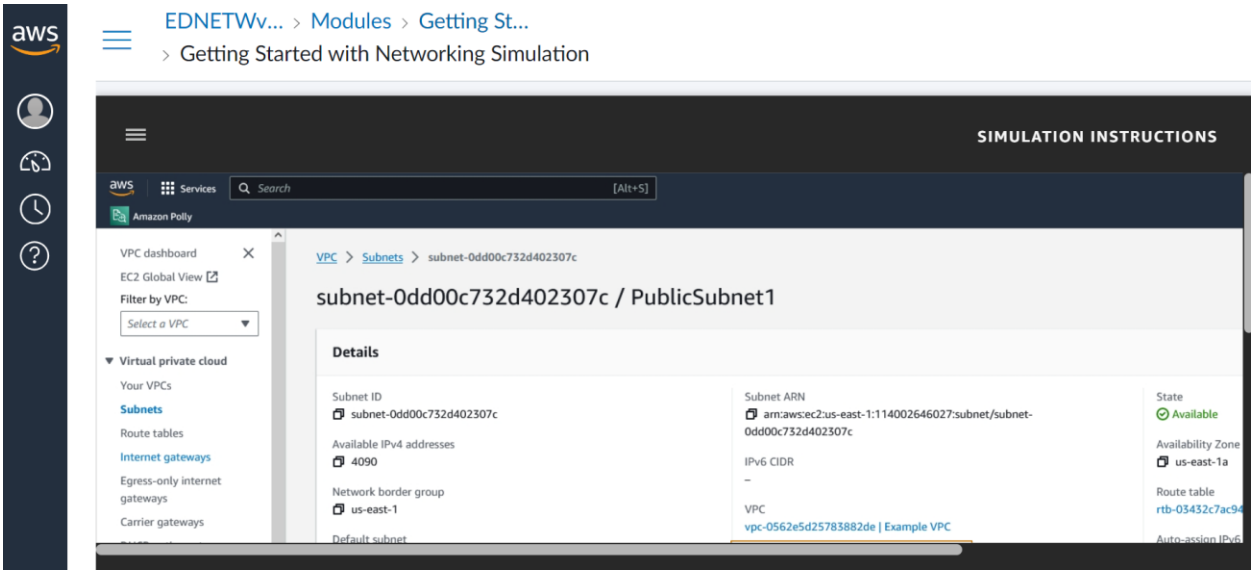
1 - EC2 in Default VPC

1. What is the CIDR range of default VPC? **172.31.0.0/16**



2. Give the range of IP addresses in this VPC? **172.31.0.0 to 172.31.255.255 = 65,536 addresses**
3. Attach Screenshot Default Subnet here.



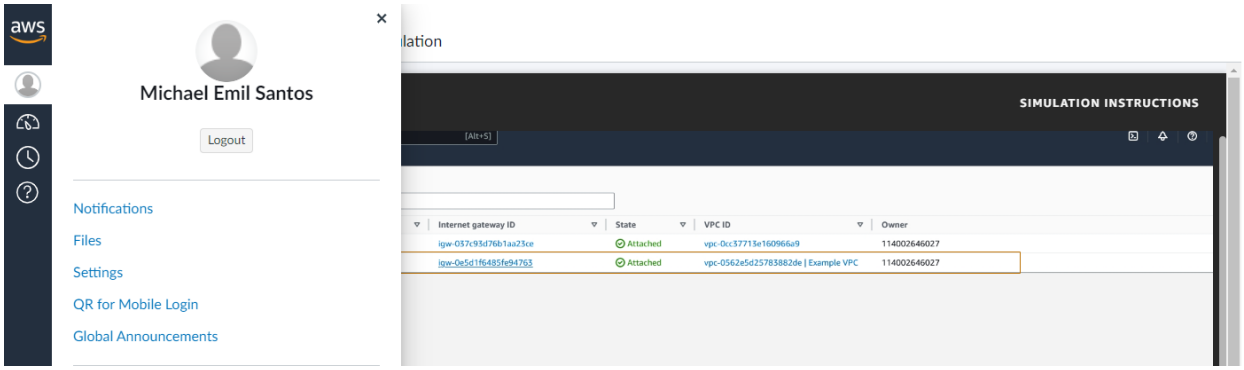


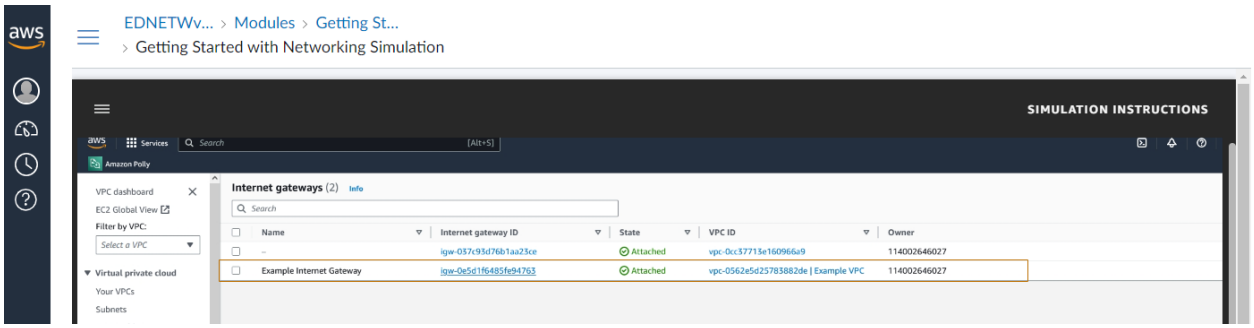
4. What is the CIDR range of default Subnet?

   172.31.0.0/20

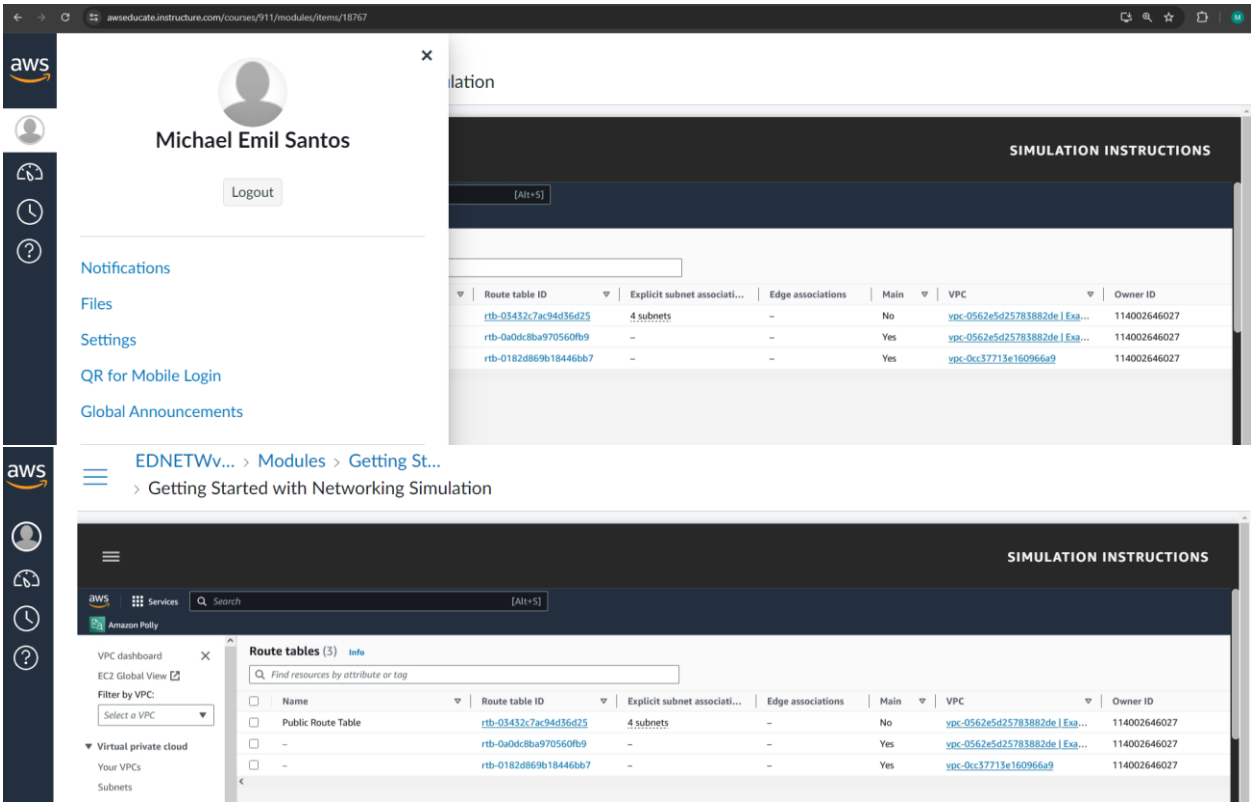
   The VPC has a CIDR block of 172.31.0.0/16, which includes all 172.31.x.x IP addresses. This subnet has a CIDR block of 172.31.0.0/20, which includes addresses 172.31.0.0–172.31.15.255. These CIDR ranges might look similar, but the subnet is smaller than the VPC because of the /20 in the CIDR range. This subnet uses the first 4,096 addresses available in the VPC. The console shows that only 4,091 addresses are available to use because AWS always reserves five addresses in each subnet for IP networking purposes.

5. Attach Screenshot Internet Gateway in the default VPC

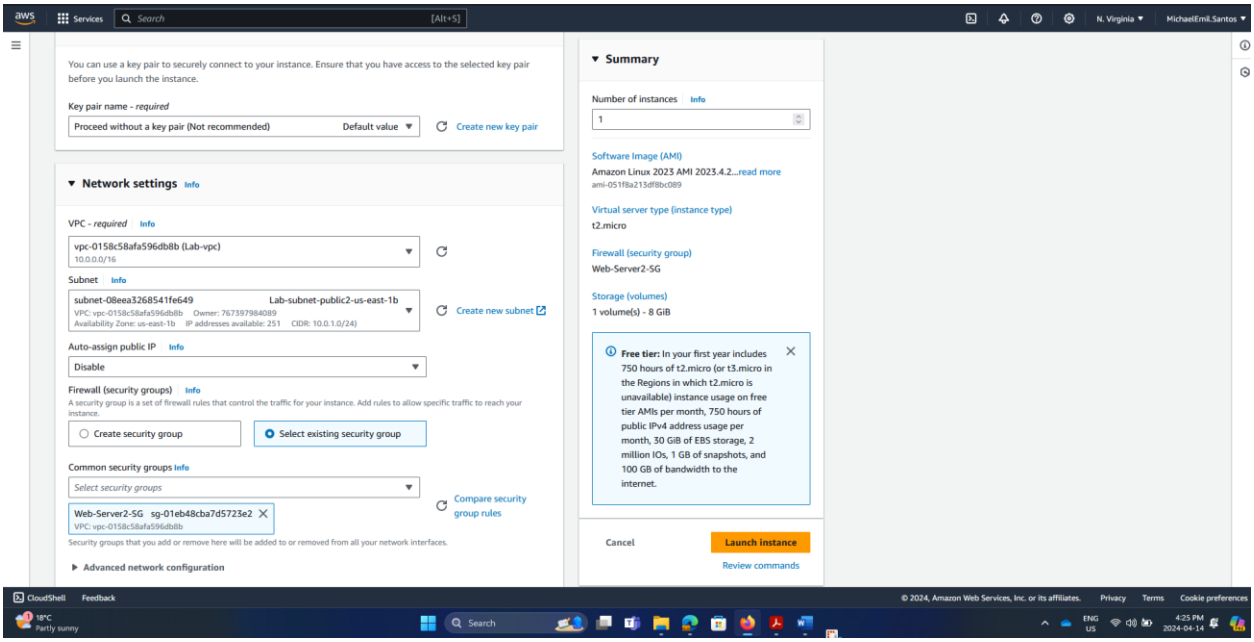


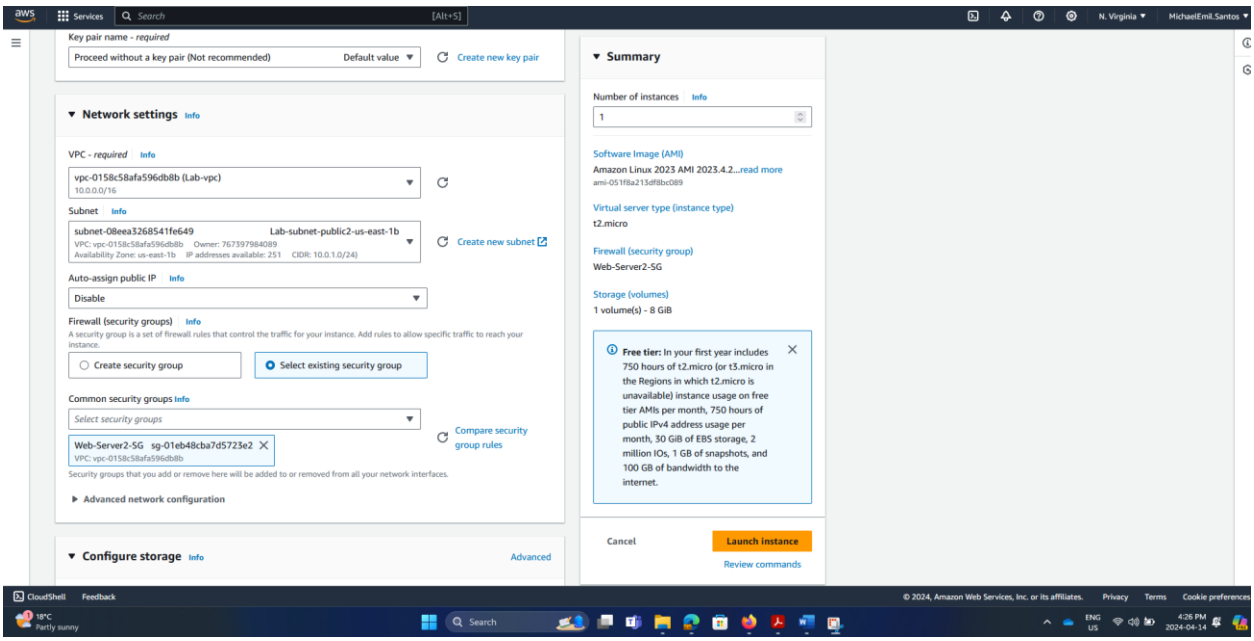


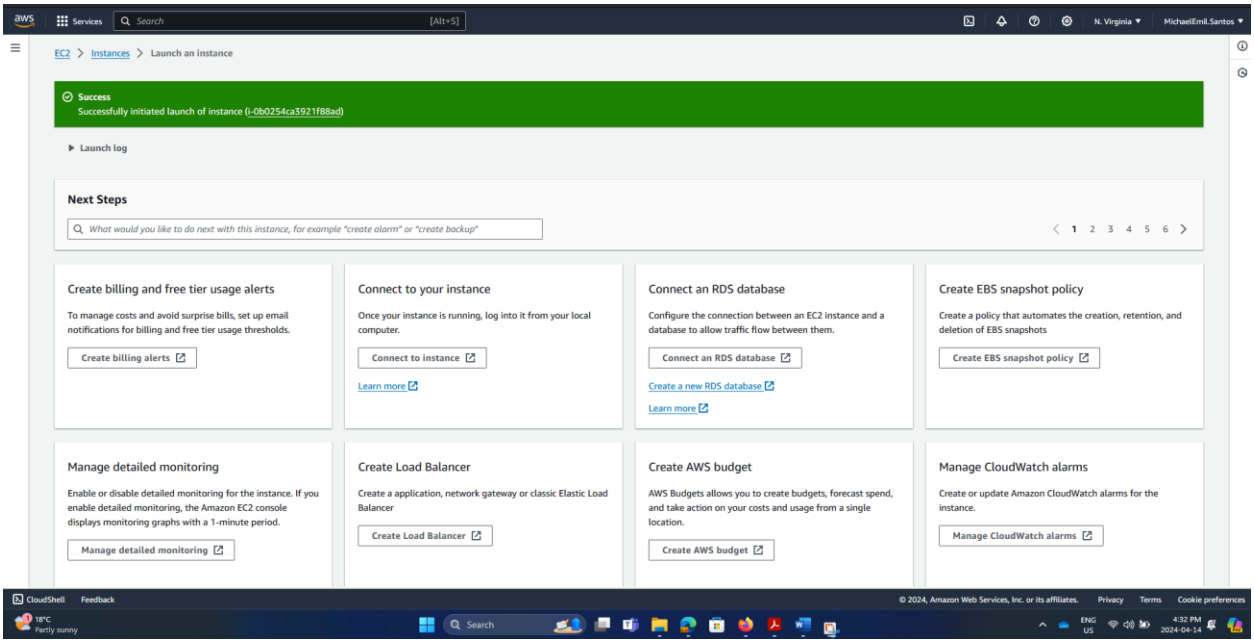
6. What is the Internet Gateway ID?
   igw-037c93d76b1aa23ce
   igw-035d1f6485fe94763 - Example VPC
7. What is the VPC ID?
   vpc-0cc37713e160966a9
   vpc-0562e5d25783882de – Example VPC
8. Attach screenshot of route table showing the default route allow internet access from the VPC

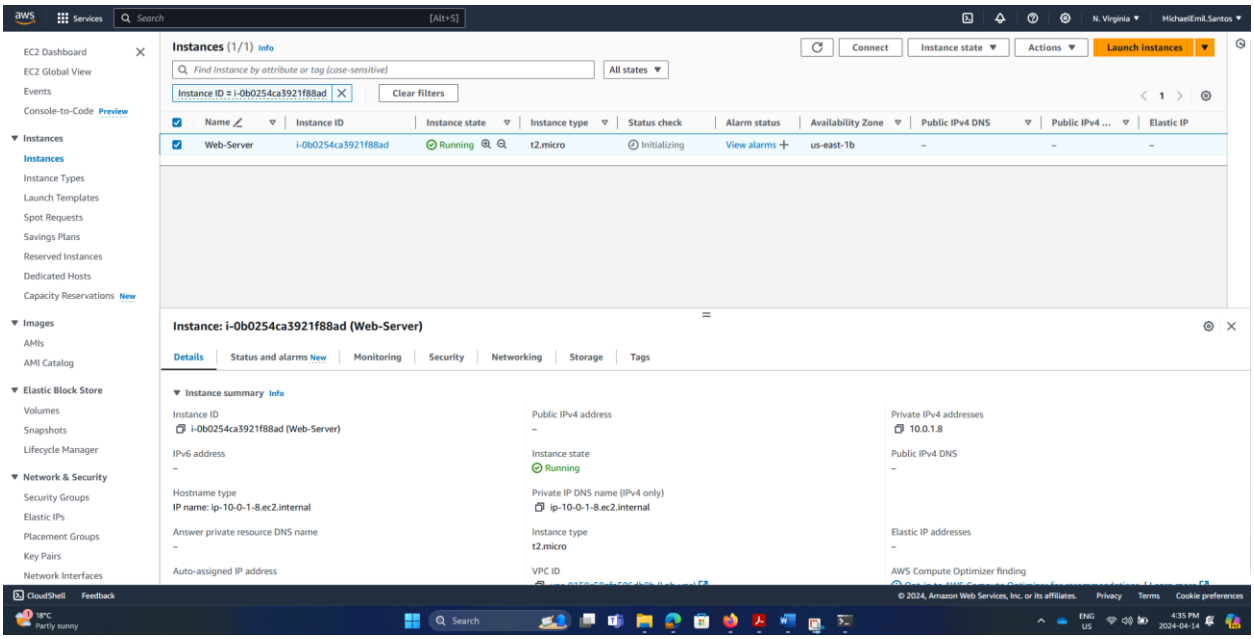


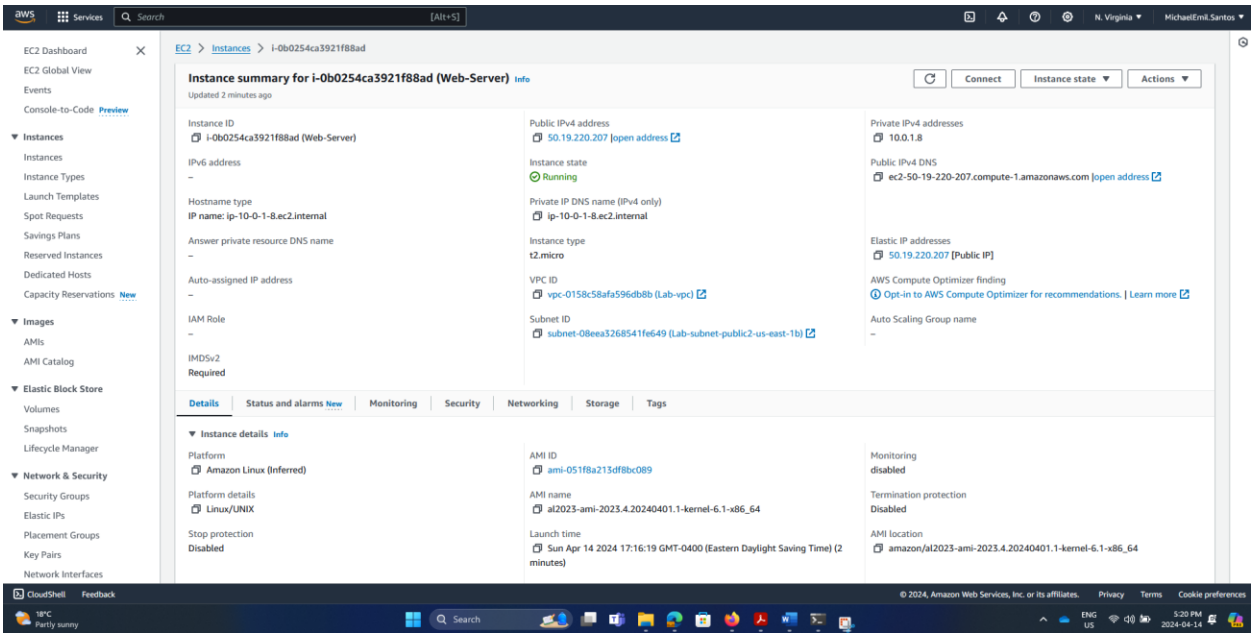
9. Attach the EC2 instance page of the AWS portal showing the EC2 in default VPC


Services
Search
[Alt+S]
N. Virginia
MichaelEmil.Santos
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-0158c58afa596db8b (Lab-vpc)
10.0.0.0/16
Subnet Info
subnet-08eea3268541fe649 Lab-subnet-public2-us-east-1b
VPC: vpc-0158c58afa596db8b Owner: 767397984089
Availability Zone: us-east-1b IP addresses available: 251 CIDR: 10.0.1.0/24)
Create new subnet
Auto-assign public IP Info
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
Web-Server2-SG sg-01eb48cba7d5723e2
VPC: vpc-0158c58afa596db8b
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
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.4.2...read more
ami-051f8a213df8bc089
Virtual server type (instance type)
t2.micro
Firewall (security group)
Web-Server2-SG
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
18°C
Partly sunny
Search
ENG
US
4:25 PM
2024-04-14

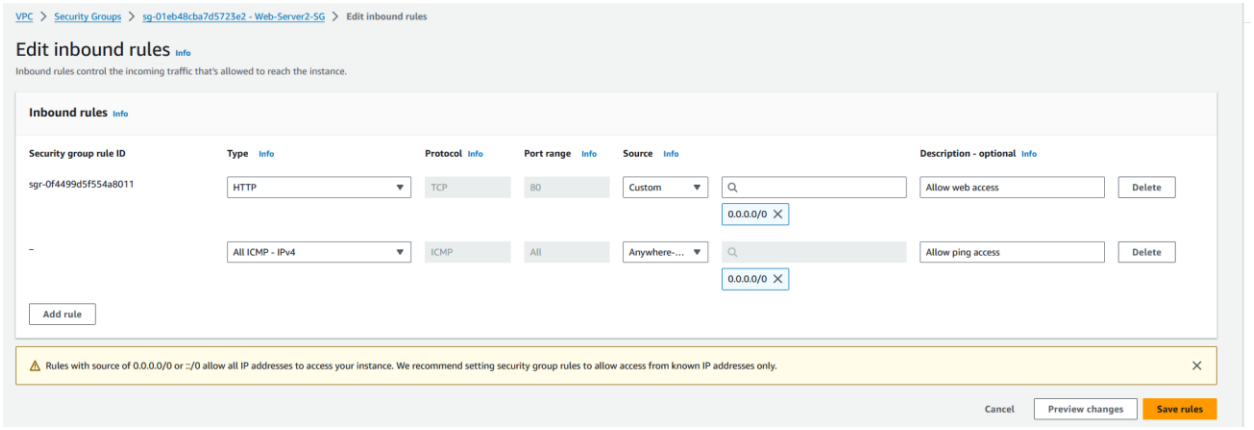

Services
Search
[Alt+S]
N. Virginia
MichaelEmil.Santos
Key pair name - required
Proceed without a key pair (Not recommended)
Default value
Create new key pair
Network settings Info
VPC - required Info
vpc-0158c58afa596db8b (Lab-vpc)
10.0.0.0/16
Subnet Info
subnet-08eea3268541fe649 Lab-subnet-public2-us-east-1b
VPC: vpc-0158c58afa596db8b Owner: 767397984089
Availability Zone: us-east-1b IP addresses available: 251 CIDR: 10.0.1.0/24)
Create new subnet
Auto-assign public IP Info
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
Web-Server2-SG sg-01eb48cba7d5723e2
VPC: vpc-0158c58afa596db8b
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
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.4.2...read more
ami-051f8a213df8bc089
Virtual server type (instance type)
t2.micro
Firewall (security group)
Web-Server2-SG
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
18°C
Partly sunny
Search
ENG
US
4:26 PM
2024-04-14

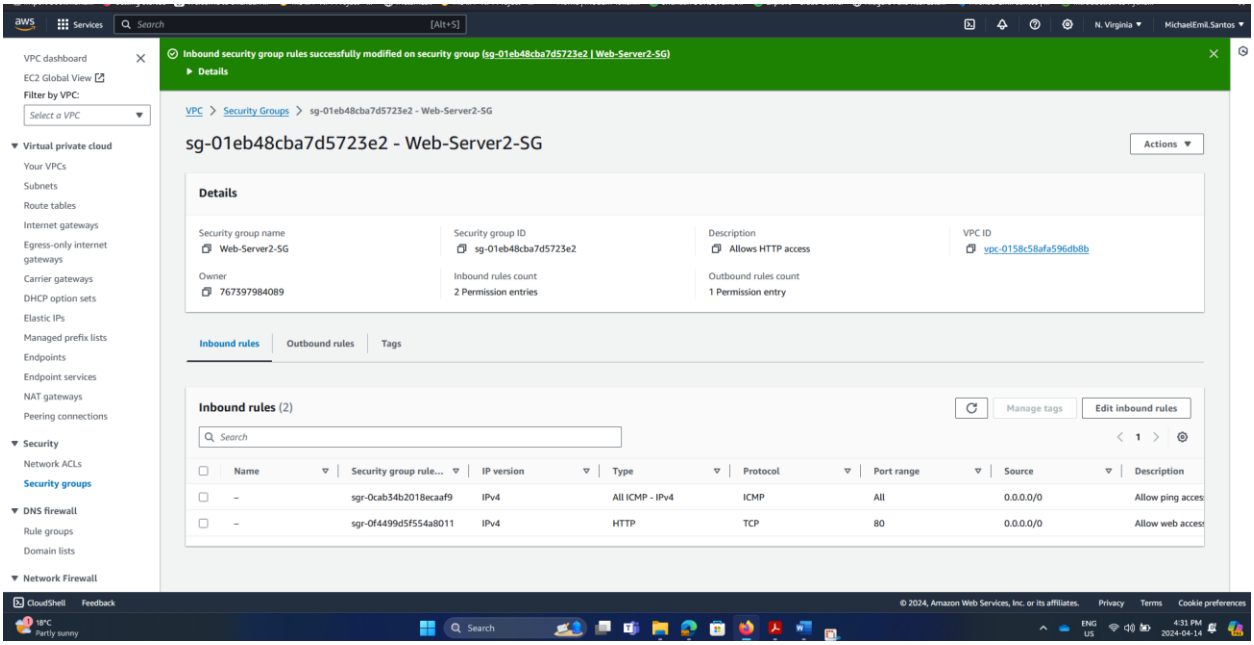

Services
Search
[Alt+S]
N. Virginia
MichaelEmil.Santos
EC2 > Instances > Launch an instance
Success
Successfully initiated launch of instance (i-0b0254ca3921f88ad)
Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
Create billing alerts
Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more
Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more
Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy
Manage detailed monitoring
Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.
Manage detailed monitoring
Create Load Balancer
Create a application, network gateway or classic Elastic Load Balancer
Create Load Balancer
Create AWS budget
AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.
Create AWS budget
Manage CloudWatch alarms
Create or update Amazon CloudWatch alarms for the instance.
Manage CloudWatch alarms
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

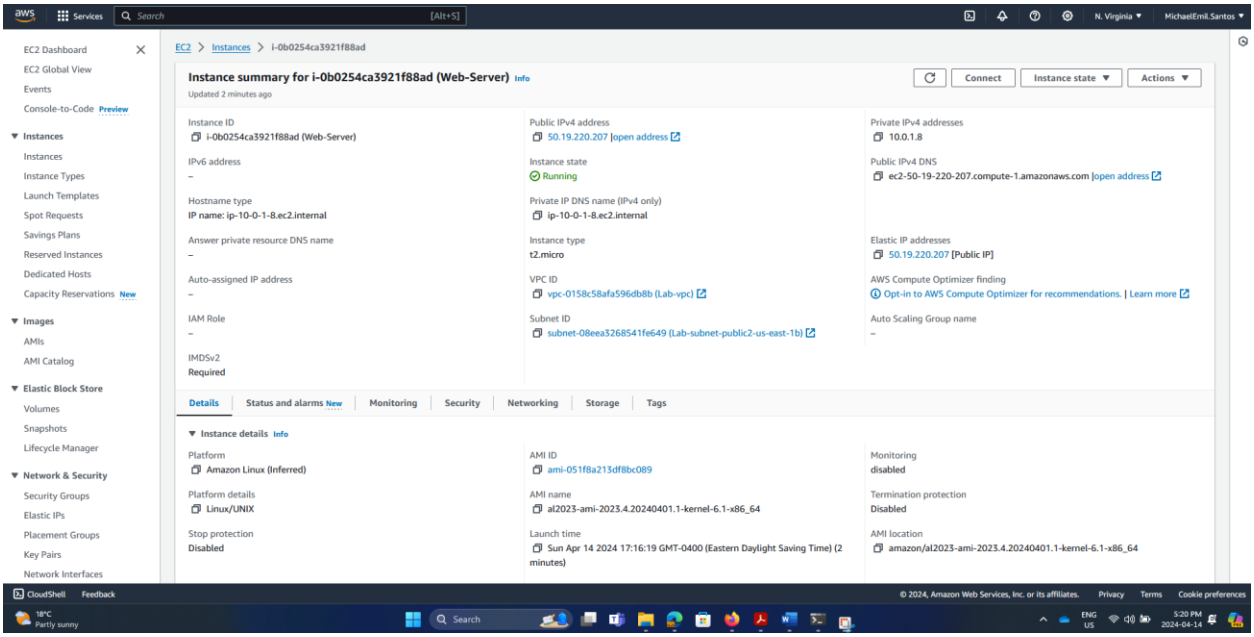

Services
Search
[Alt+S]
N. Virginia
MichaelEmil.Santos
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Instance ID = i-0b0254ca3921f88ad
Clear filters
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic IP
Web-Server
i-0b0254ca3921f88ad
Running
t2.micro
Initializing
View alarms
us-east-1b
Instance: i-0b0254ca3921f88ad (Web-Server)
Details
Status and alarms New
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-0b0254ca3921f88ad (Web-Server)
IPv6 address
Hostname type
IP name: ip-10-0-1-8.ec2.internal
Answer private resource DNS name
Auto-assigned IP address
Public IPv4 address
Instance state
Running
Private IP DNS name (IPv4 only)
ip-10-0-1-8.ec2.internal
Instance type
t2.micro
VPC ID
Private IPv4 addresses
10.0.1.8
Public IPv4 DNS
Elastic IP addresses
AWS Compute Optimizer finding
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

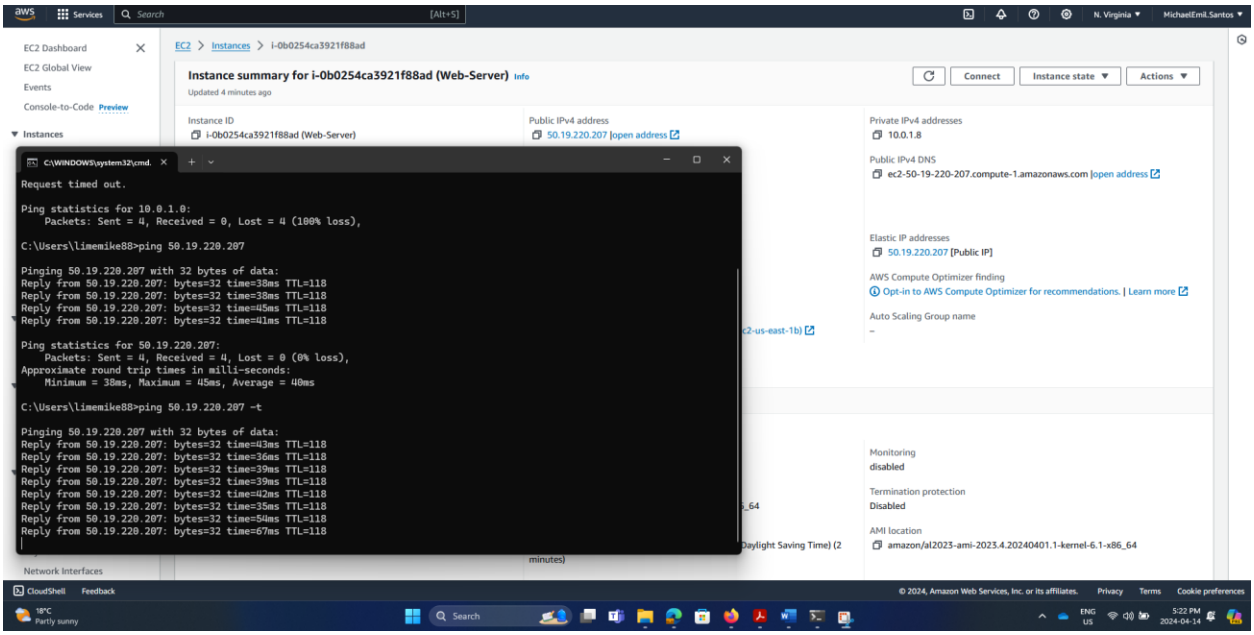


10. Screenshot of Pinging public IP of EC2 in default VPC



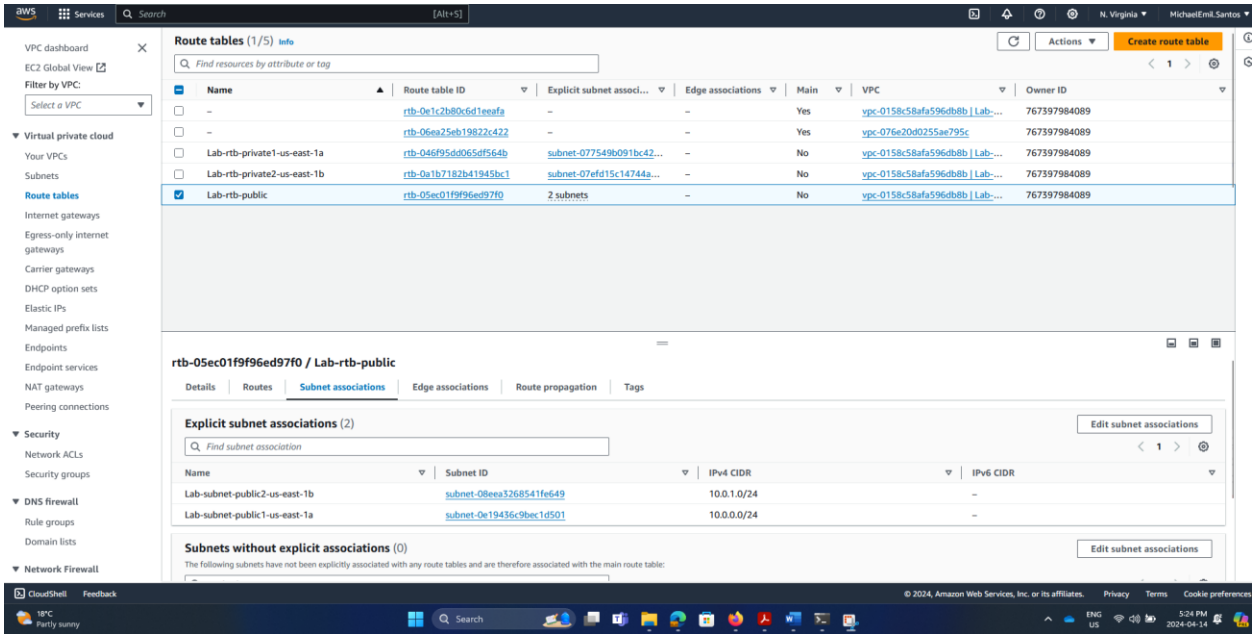

Inbound security group rules successfully modified on security group (sg-01eb48cba7d5723e2 | Web-Server2-SG)
Details
VPC > Security Groups > sg-01eb48cba7d5723e2 - Web-Server2-SG
sg-01eb48cba7d5723e2 - Web-Server2-SG
Actions
Details
Security group name
Web-Server2-SG
Security group ID
sg-01eb48cba7d5723e2
Description
Allows HTTP access
VPC ID
vpc-0158c58afa596db8b
Owner
767397984089
Inbound rules count
2 Permission entries
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Tags
Inbound rules (2)
Manage tags
Edit inbound rules
Name
Security group rule...
IP version
Type
Protocol
Port range
Source
Description
sgr-0cab34b2018ecaaf9
IPv4
All ICMP - IPv4
ICMP
All
0.0.0.0/0
sgr-0f4499d5f554a8011
IPv4
HTTP
TCP
80
0.0.0.0/0

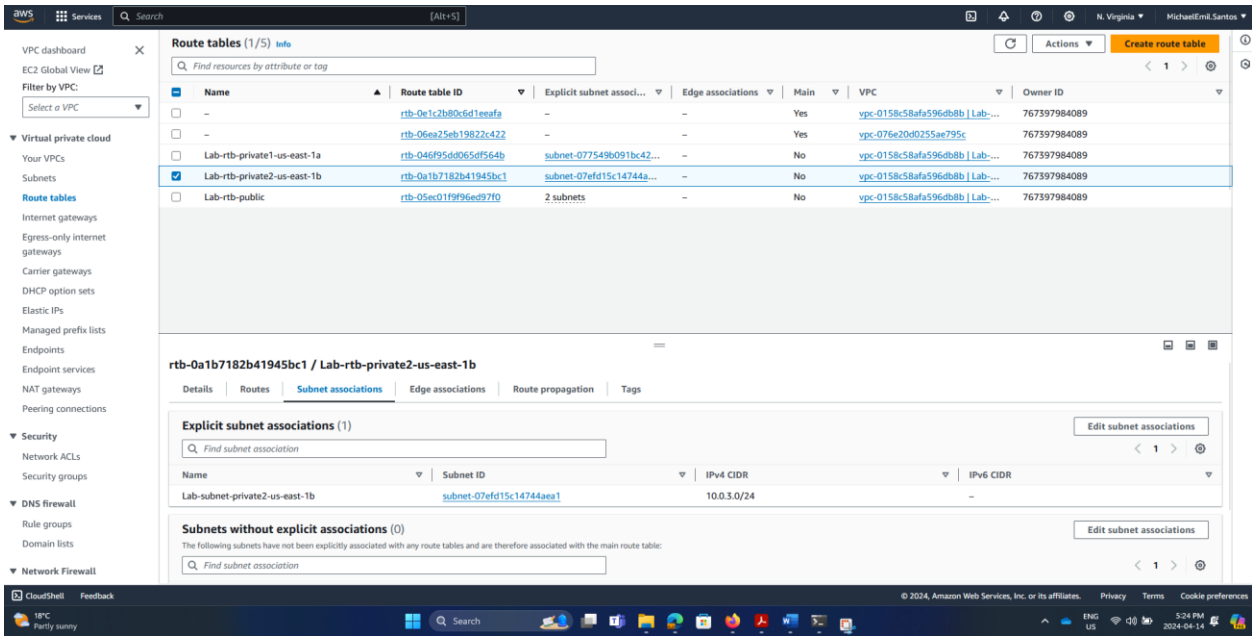

EC2 > Instances > i-0b0254ca3921f88ad
Instance summary for i-0b0254ca3921f88ad (Web-Server)
Updated 2 minutes ago
Connect
Instance state
Actions
Instance ID
i-0b0254ca3921f88ad (Web-Server)
Public IPv4 address
50.19.220.207 |open address
Private IPv4 addresses
10.0.1.8
IPv6 address
Instance state
Running
Public IPv4 DNS
ec2-50-19-220-207.compute-1.amazonaws.com |open address
Hostname type
IP name: ip-10-0-1-8.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-0-1-8.ec2.internal
Answer private resource DNS name
Instance type
t2.micro
Elastic IP addresses
50.19.220.207 [Public IP]
Auto-assigned IP address
VPC ID
vpc-0158c58afa596db8b (Lab-vpc)
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more
IAM Role
Subnet ID
subnet-08eea3268541fe649 (Lab-subnet-public2-us-east-1b)
Auto Scaling Group name
IMDSv2
Required
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance details
Platform
Amazon Linux (Inferred)
AMI ID
ami-051f8a213df8bc089
Monitoring
disabled
Platform details
Linux/UNIX
AMI name
al2023-ami-2023.4.20240401.1-kernel-6.1-x86_64
Termination protection
Disabled
Stop protection
Disabled
Launch time
Sun Apr 14 2024 17:16:19 GMT-0400 (Eastern Daylight Saving Time) (2 minutes)
AMI location
amazon/al2023-ami-2023.4.20240401.1-kernel-6.1-x86_64

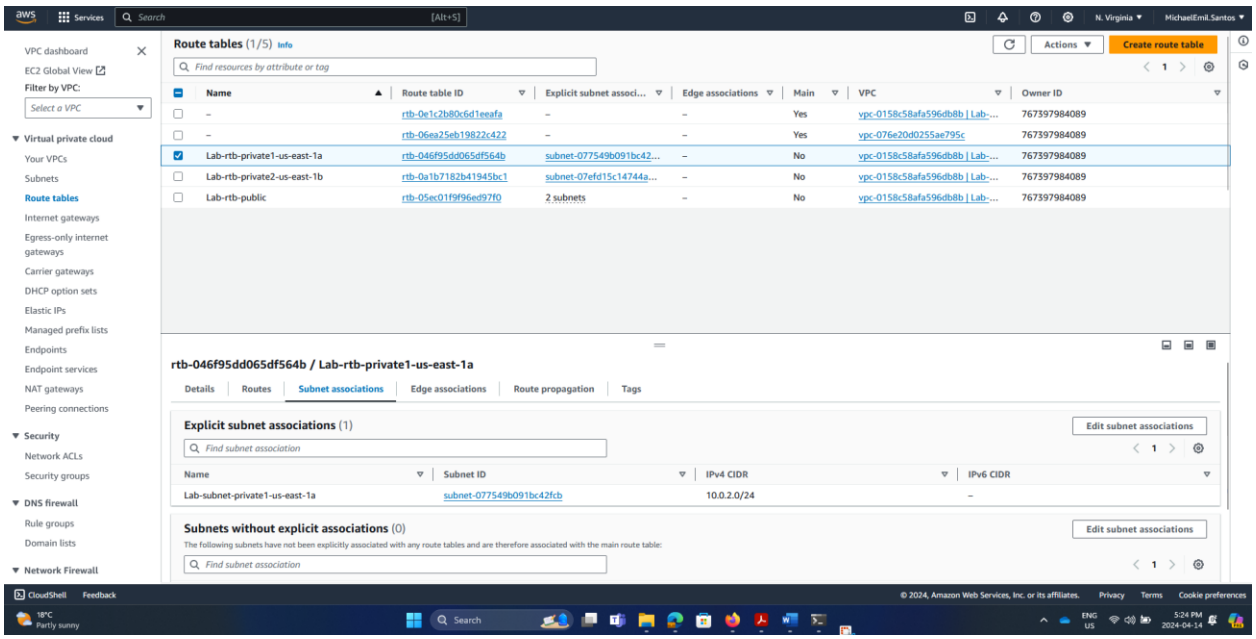


Part 2 - EC2 in Customer VPC

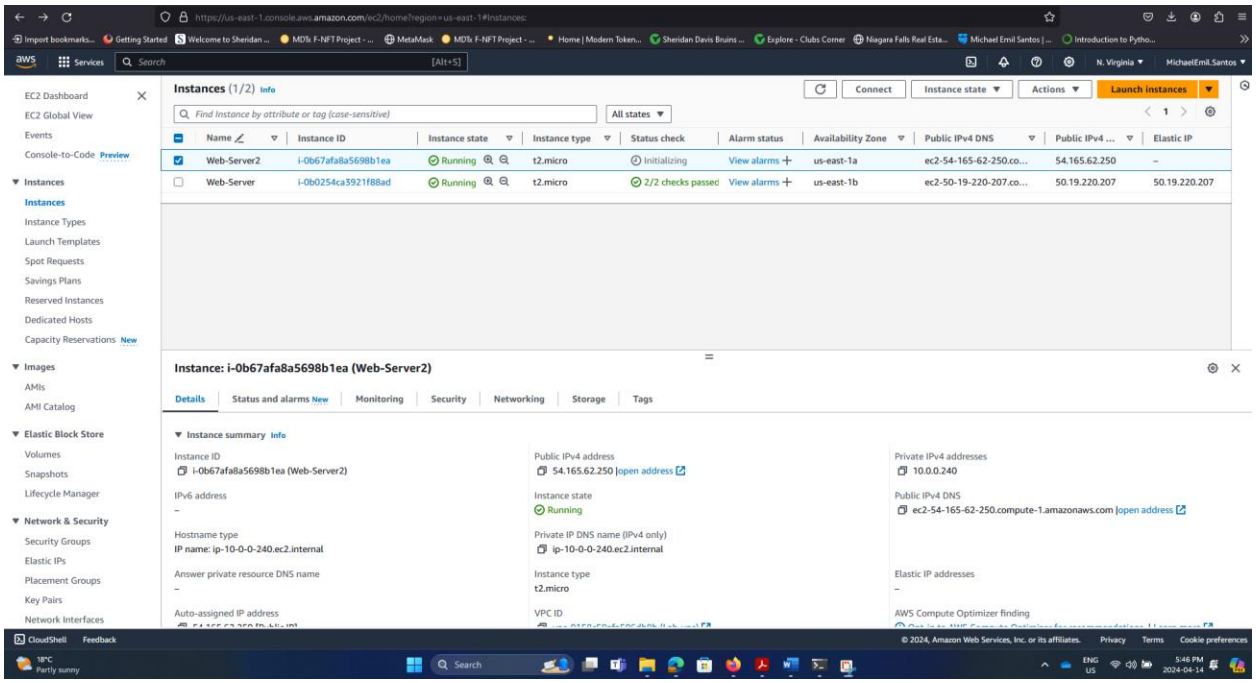
1. Screenshots of custom VPC and subnets

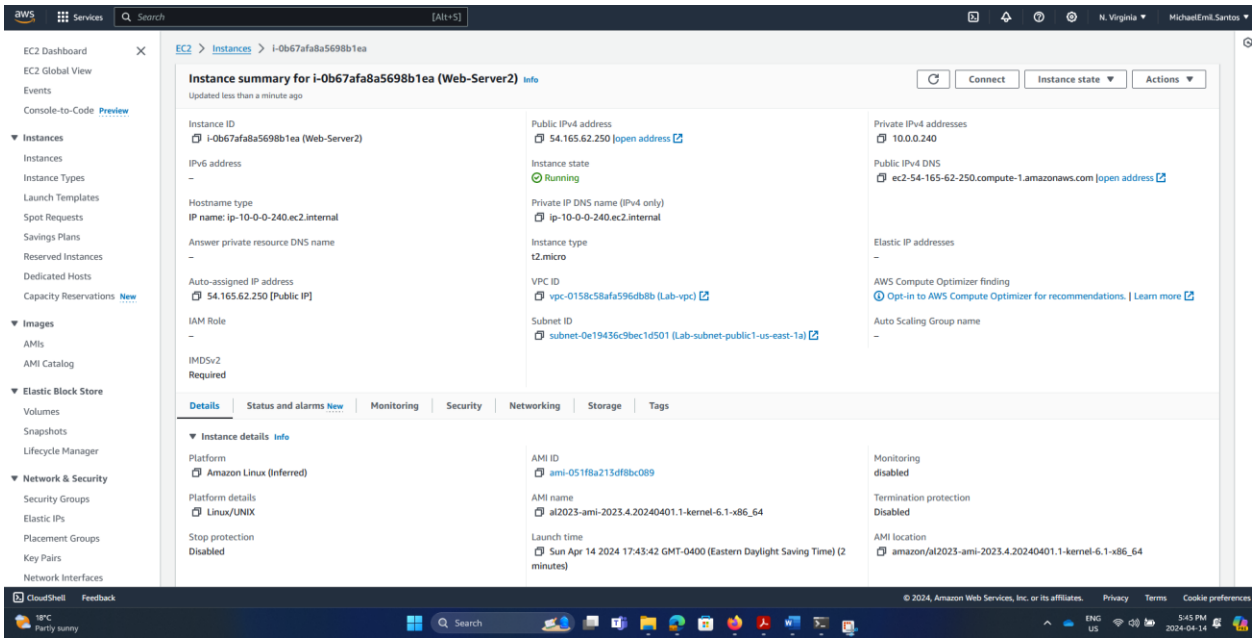


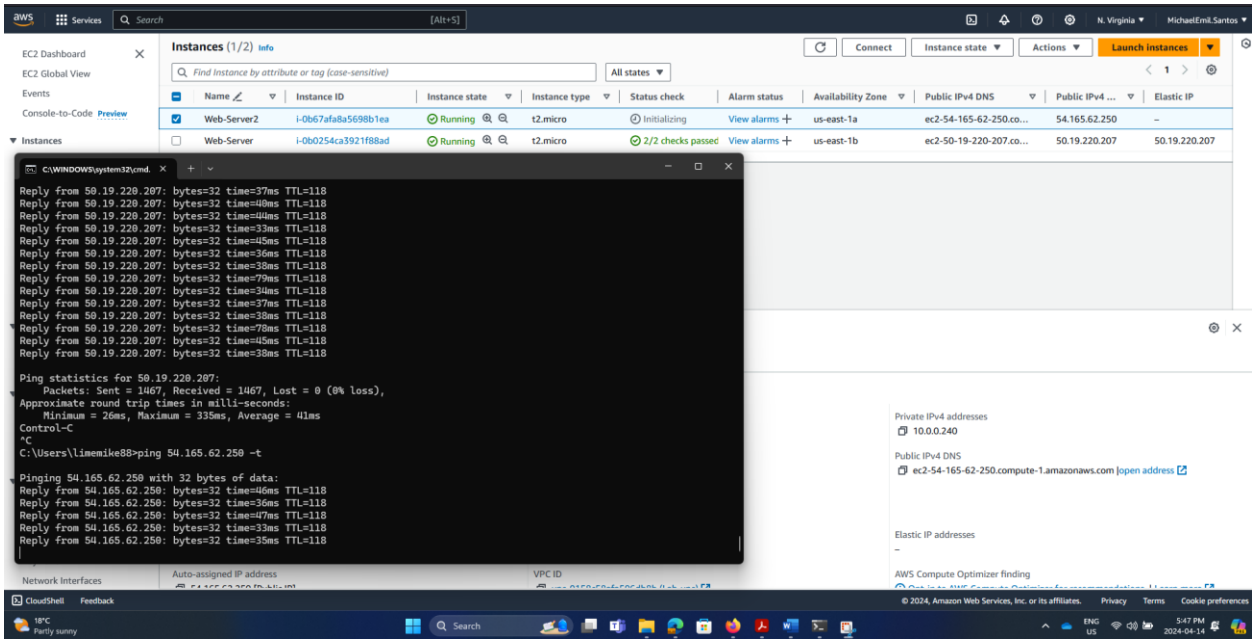


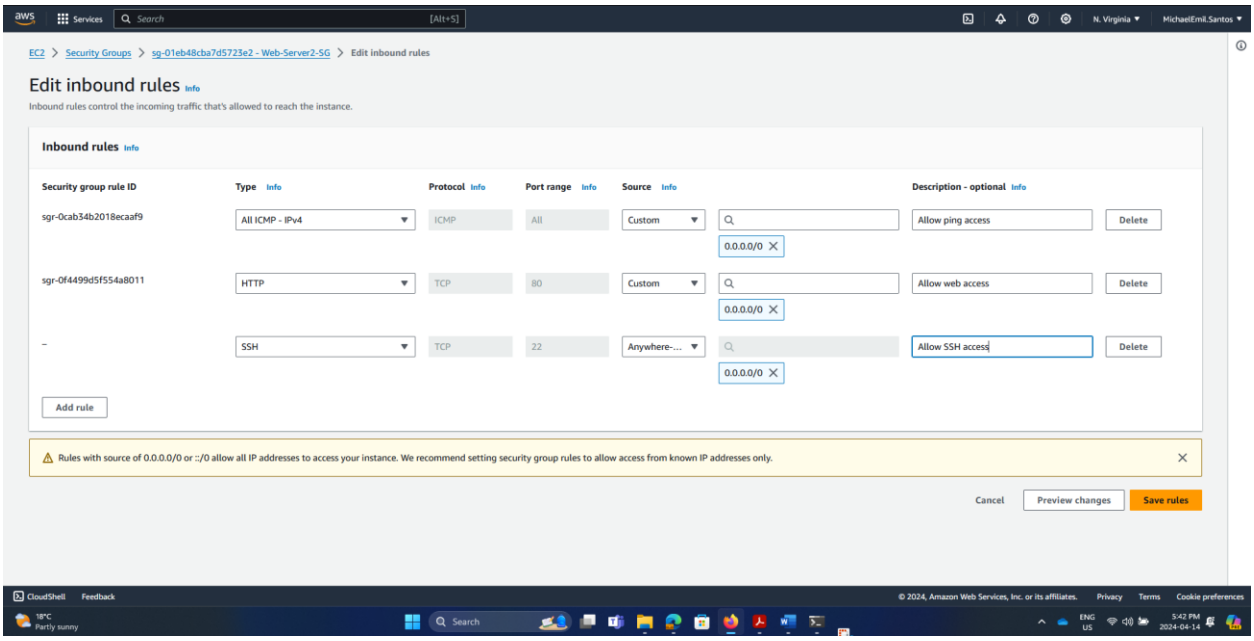


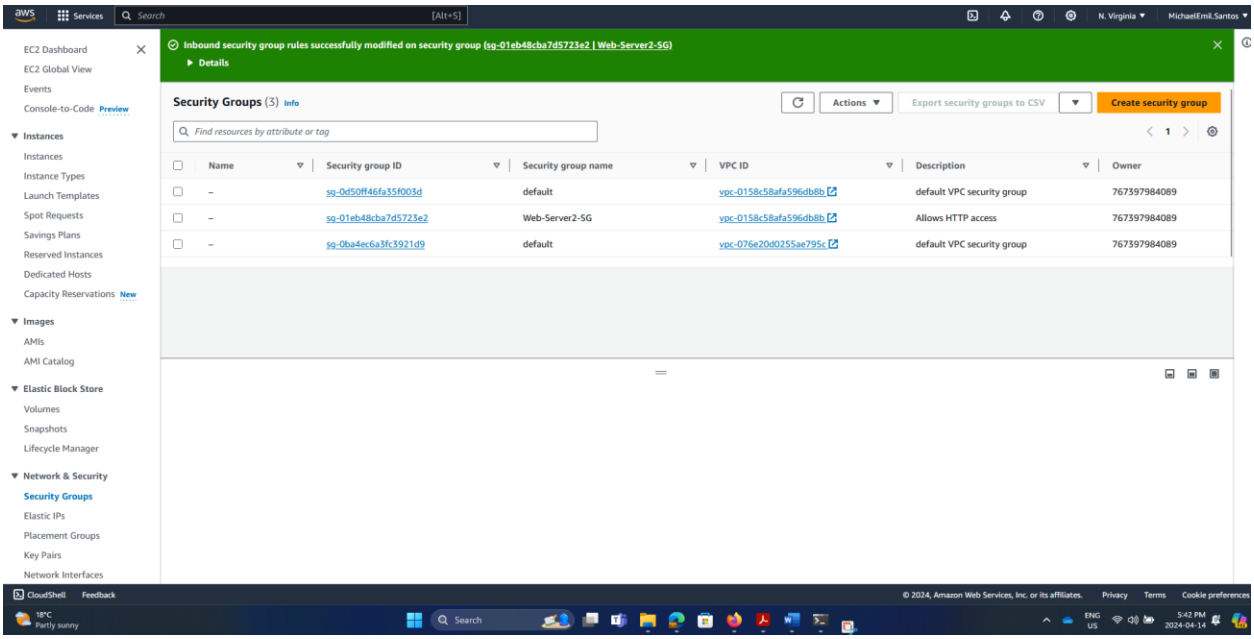
2. Attach the EC2 instance page of the AWS portal showing the EC2 in Custom VPC


Instances (1/2) Info
Connect
Instance state
Actions
Launch instances
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic IP
Web-Server2
i-0b67afa8a5698b1ea
Running
t2.micro
Initializing
View alarms
us-east-1a
ec2-54-165-62-250.co...
54.165.62.250
Web-Server
i-0b0254ca3921f88ad
Running
t2.micro
2/2 checks passed
View alarms
us-east-1b
ec2-50-19-220-207.co...
50.19.220.207
50.19.220.207
Instance: i-0b67afa8a5698b1ea (Web-Server2)
Details
Status and alarms New
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-0b67afa8a5698b1ea (Web-Server2)
Public IPv4 address
54.165.62.250 |open address
Private IPv4 addresses
10.0.0.240
IPv6 address
Instance state
Running
Public IPv4 DNS
ec2-54-165-62-250.compute-1.amazonaws.com |open address
Hostname type
IP name: ip-10-0-0-240.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-0-0-240.ec2.internal
Answer private resource DNS name
Instance type
t2.micro
Elastic IP addresses
Auto-assigned IP address
VPC ID
AWS Compute Optimizer finding
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

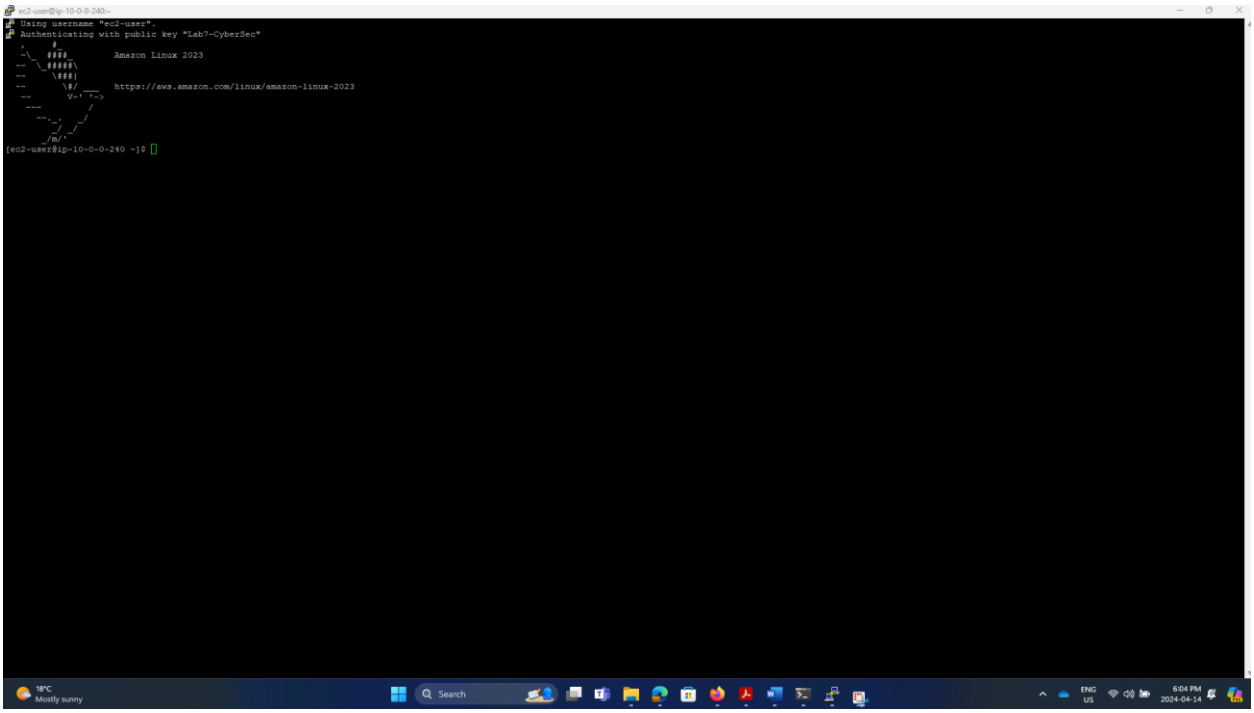

EC2 > Instances > i-0b67afa8a5698b1ea
Instance summary for i-0b67afa8a5698b1ea (Web-Server2) Info
Updated less than a minute ago
Connect
Instance state
Actions
Instance ID
i-0b67afa8a5698b1ea (Web-Server2)
Public IPv4 address
54.165.62.250 |open address
Private IPv4 addresses
10.0.0.240
IPv6 address
Instance state
Running
Public IPv4 DNS
ec2-54-165-62-250.compute-1.amazonaws.com |open address
Hostname type
IP name: ip-10-0-0-240.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-0-0-240.ec2.internal
Answer private resource DNS name
Instance type
t2.micro
Elastic IP addresses
Auto-assigned IP address
54.165.62.250 [Public IP]
VPC ID
vpc-0158c58afa596db8b (Lab-vpc)
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more
IAM Role
Subnet ID
subnet-0e19436c9bec1d501 (Lab-subnet-public1-us-east-1a)
Auto Scaling Group name
IMDSv2
Required
Details
Status and alarms New
Monitoring
Security
Networking
Storage
Tags
Instance details Info
Platform
Amazon Linux (Inferred)
AMI ID
ami-051f8a213df8bc089
Monitoring
disabled
Platform details
Linux/UNIX
AMI name
al2023-ami-2023.4.20240401.1-kernel-6.1-x86_64
Termination protection
Disabled
Stop protection
Disabled
Launch time
Sun Apr 14 2024 17:43:42 GMT-0400 (Eastern Daylight Saving Time) (2 minutes)
AMI location
amazon/al2023-ami-2023.4.20240401.1-kernel-6.1-x86_64
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

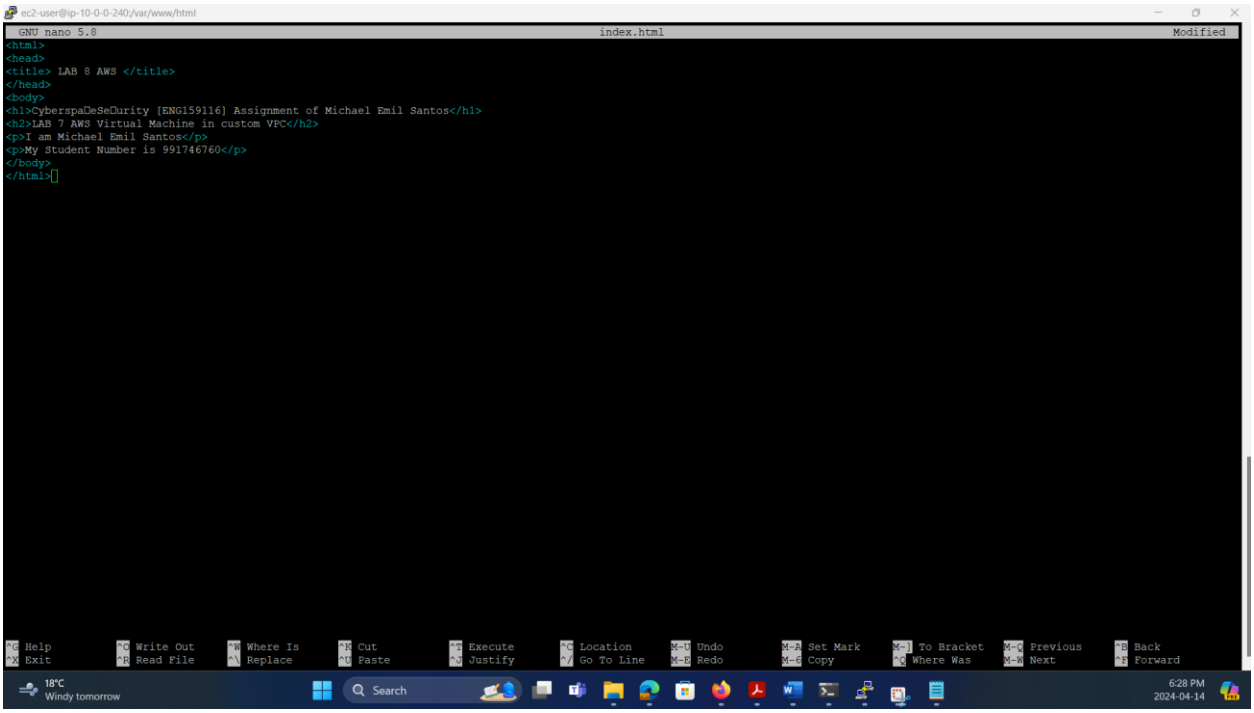

Instances (1/2) Info
Web-Server2 i-0b67afa8a5698b1ea Running t2.micro Initializing us-east-1a ec2-54-165-62-250.co... 54.165.62.250
Web-Server i-0b0254ca3921f88ad Running t2.micro 2/2 checks passed us-east-1b ec2-50-19-220-207.co... 50.19.220.207 50.19.220.207
C:\WINDOWS\system32\cmd.
Reply from 50.19.220.207: bytes=32 time=37ms TTL=118
Reply from 50.19.220.207: bytes=32 time=40ms TTL=118
Reply from 50.19.220.207: bytes=32 time=44ms TTL=118
Reply from 50.19.220.207: bytes=32 time=33ms TTL=118
Reply from 50.19.220.207: bytes=32 time=45ms TTL=118
Reply from 50.19.220.207: bytes=32 time=36ms TTL=118
Reply from 50.19.220.207: bytes=32 time=38ms TTL=118
Reply from 50.19.220.207: bytes=32 time=79ms TTL=118
Reply from 50.19.220.207: bytes=32 time=34ms TTL=118
Reply from 50.19.220.207: bytes=32 time=37ms TTL=118
Reply from 50.19.220.207: bytes=32 time=38ms TTL=118
Reply from 50.19.220.207: bytes=32 time=78ms TTL=118
Reply from 50.19.220.207: bytes=32 time=45ms TTL=118
Reply from 50.19.220.207: bytes=32 time=38ms TTL=118
Ping statistics for 50.19.220.207:
Packets: Sent = 1467, Received = 1467, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 26ms, Maximum = 335ms, Average = 41ms
Control-C
^C
C:\Users\limemike88>ping 54.165.62.250 -t
Pinging 54.165.62.250 with 32 bytes of data:
Reply from 54.165.62.250: bytes=32 time=46ms TTL=118
Reply from 54.165.62.250: bytes=32 time=36ms TTL=118
Reply from 54.165.62.250: bytes=32 time=47ms TTL=118
Reply from 54.165.62.250: bytes=32 time=33ms TTL=118
Reply from 54.165.62.250: bytes=32 time=35ms TTL=118
Private IPv4 addresses
10.0.0.240
Public IPv4 DNS
ec2-54-165-62-250.compute-1.amazonaws.com open address
Elastic IP addresses
AWS Compute Optimizer finding

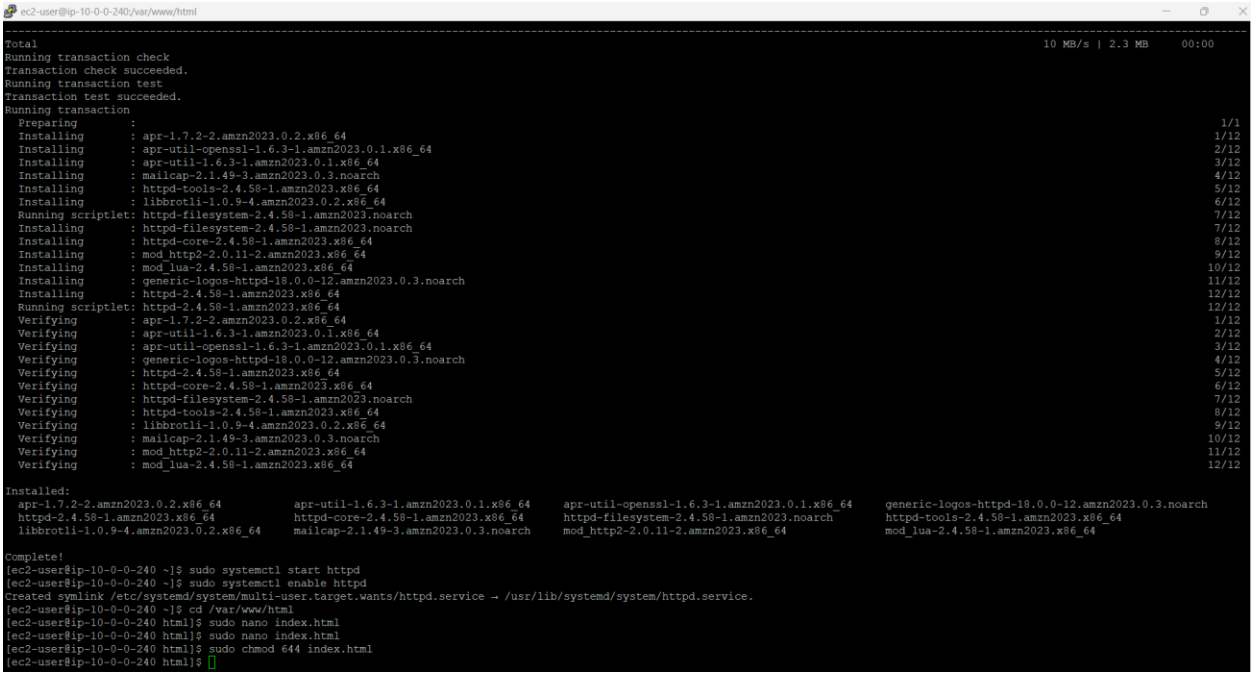

EC2 > Security Groups > sg-01eb48cba7d5723e2 - Web-Server2-SG > Edit inbound rules
Edit inbound rules Info
Inbound rules control the incoming traffic that's allowed to reach the instance.
Inbound rules Info
Security group rule ID
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
sgr-0cab34b2018ecaaf9 All ICMP - IPv4 ICMP All Custom 0.0.0.0/0 Allow ping access Delete
sgr-0f4499d5f554a8011 HTTP TCP 80 Custom 0.0.0.0/0 Allow web access Delete
- SSH TCP 22 Anywhere-... 0.0.0.0/0 Allow SSH access 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.
Cancel
Preview changes
Save rules



3. Screen shot of the web page from the virtual machine in custom VPC




ec2-user@ip-10-0-0-240:/var/www/html
GNU nano 5.8 index.html Modified
<html>
<head>
<title> LAB 8 AWS </title>
</head>
<body>
<h1>CyberspaDeSeDurity [ENG159116] Assignment of Michael Emil Santos</h1>
<h2>LAB 7 AWS Virtual Machine in custom VPC</h2>
I am Michael Emil Santos
My Student Number is 991746760
</body>
</html>
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-Q Previous ^B Back
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was M-W Next ^F Forward
18°C
Windy tomorrow
Search
6:28 PM
2024-04-14


ec2-user@ip-10-0-0-240:/var/www/html
Total 10 MB/s | 2.3 MB 00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : 1/1
Installing : apr-1.7.2-2.amzn2023.0.2.x86_64 1/12
Installing : apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64 2/12
Installing : apr-util-1.6.3-1.amzn2023.0.1.x86_64 3/12
Installing : mailcap-2.1.49-3.amzn2023.0.3.noarch 4/12
Installing : httpd-tools-2.4.58-1.amzn2023.x86_64 5/12
Installing : libbrotli-1.0.9-4.amzn2023.0.2.x86_64 6/12
Running scriptlet: httpd-filesystem-2.4.58-1.amzn2023.noarch 7/12
Installing : httpd-filesystem-2.4.58-1.amzn2023.noarch 7/12
Installing : httpd-core-2.4.58-1.amzn2023.x86_64 8/12
Installing : mod_http2-2.0.11-2.amzn2023.x86_64 9/12
Installing : mod_lua-2.4.58-1.amzn2023.x86_64 10/12
Installing : generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch 11/12
Installing : httpd-2.4.58-1.amzn2023.x86_64 12/12
Running scriptlet: httpd-2.4.58-1.amzn2023.x86_64 12/12
Verifying : apr-1.7.2-2.amzn2023.0.2.x86_64 1/12
Verifying : apr-util-1.6.3-1.amzn2023.0.1.x86_64 2/12
Verifying : apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64 3/12
Verifying : generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch 4/12
Verifying : httpd-2.4.58-1.amzn2023.x86_64 5/12
Verifying : httpd-core-2.4.58-1.amzn2023.x86_64 6/12
Verifying : httpd-filesystem-2.4.58-1.amzn2023.noarch 7/12
Verifying : httpd-tools-2.4.58-1.amzn2023.x86_64 8/12
Verifying : libbrotli-1.0.9-4.amzn2023.0.2.x86_64 9/12
Verifying : mailcap-2.1.49-3.amzn2023.0.3.noarch 10/12
Verifying : mod_http2-2.0.11-2.amzn2023.x86_64 11/12
Verifying : mod_lua-2.4.58-1.amzn2023.x86_64 12/12
Installed:
apr-1.7.2-2.amzn2023.0.2.x86_64 apr-util-1.6.3-1.amzn2023.0.1.x86_64 apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64 generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch
httpd-2.4.58-1.amzn2023.x86_64 httpd-core-2.4.58-1.amzn2023.x86_64 httpd-filesystem-2.4.58-1.amzn2023.noarch httpd-tools-2.4.58-1.amzn2023.x86_64
libbrotli-1.0.9-4.amzn2023.0.2.x86_64 mailcap-2.1.49-3.amzn2023.0.3.noarch mod_http2-2.0.11-2.amzn2023.x86_64 mod_lua-2.4.58-1.amzn2023.x86_64
Complete!
[ec2-user@ip-10-0-0-240 ~]$ sudo systemctl start httpd
[ec2-user@ip-10-0-0-240 ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[ec2-user@ip-10-0-0-240 ~]$ cd /var/www/html
[ec2-user@ip-10-0-0-240 html]$ sudo nano index.html
[ec2-user@ip-10-0-0-240 html]$ sudo nano index.html
[ec2-user@ip-10-0-0-240 html]$ sudo chmod 644 index.html
[ec2-user@ip-10-0-0-240 html]$

Conclusion

This project offered an in-depth look at cloud networking through AWS, from initial configuration to deployment and connectivity testing. By working with both the default and custom VPCs, I gained practical experience in AWS's networking capabilities, including setting up isolated subnets, configuring secure internet access, and deploying EC2 instances.

Configuring a custom VPC allowed me to create a tailored environment with unique IP addressing and enhanced security controls, showcasing the flexibility and scalability of cloud networks. Testing connectivity and troubleshooting internet access strengthened my understanding of routing tables, internet gateways, and the critical role of security groups in maintaining secure yet accessible resources.

Ultimately, this project underscored the importance of network segmentation and secure configurations in cloud environments. These skills are foundational for designing and managing robust cloud infrastructures, where reliability, scalability, and security are paramount. This hands-on experience with AWS networking provides a solid foundation for future cloud architecture projects, ensuring I can design secure, efficient, and resilient cloud environments to meet diverse business needs.