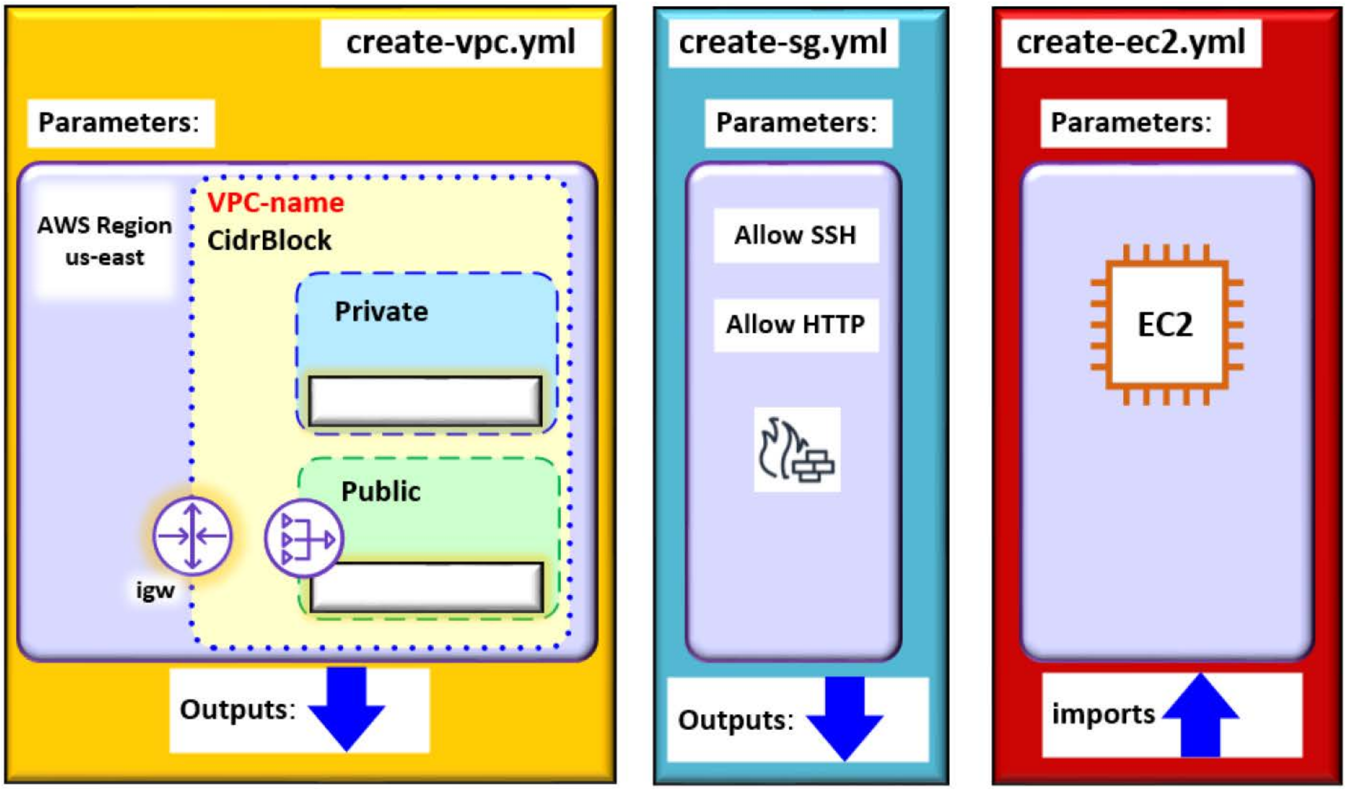
Author: Frank Ekwomadu. C

Tech Stack: AWS CloudFormation

VISUAL OF THE INFRASTRUCTURE

Challenge: Using AWS's CloudFormation, provision the infrastructure below.



Challenge Requirements:

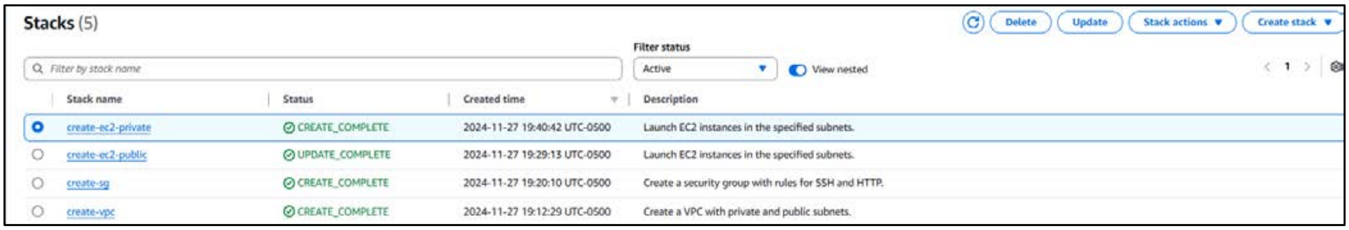
a. create-vpc.yml: Creates a VPC with **private** and **public subnets**. A **NAT Gateway** should be attached to the public subnet to enable the private subnet to access the internet.

b. create-sg.yml: Creates a security group with rules for **SSH** and **HTTP**. These rules should permit traffic from anywhere.

c. create-ec2.yml: Launches EC2 instances in the subnets (private or public) specified by the user. They should **make use of the VPC and SG created in (a) and (b)**.

MY SOLUTION VISUALS

Stacks Display:

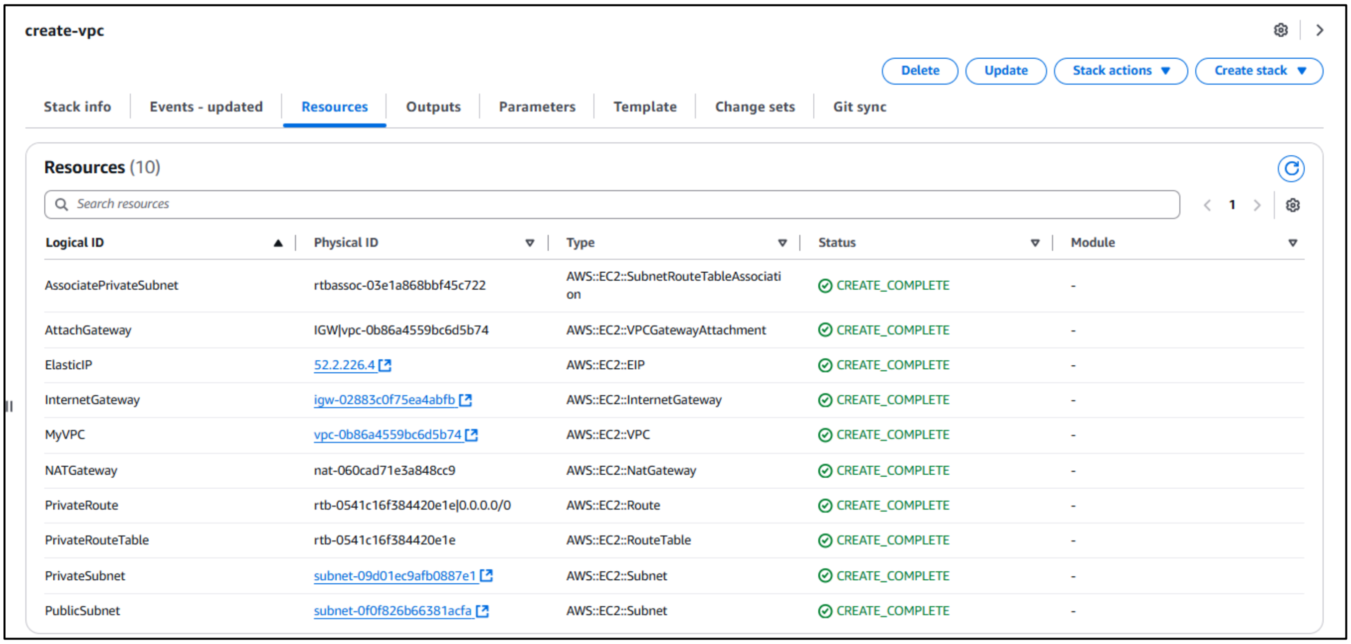


Stacks (5)

	Stack name	Status	Created time	Description
●	create-ec2-private	CREATE_COMPLETE	2024-11-27 19:40:42 UTC-0500	Launch EC2 instances in the specified subnets.
○	create-ec2-public	UPDATE_COMPLETE	2024-11-27 19:29:13 UTC-0500	Launch EC2 instances in the specified subnets.
○	create-sg	CREATE_COMPLETE	2024-11-27 19:20:10 UTC-0500	Create a security group with rules for SSH and HTTP.
○	create-vpc	CREATE_COMPLETE	2024-11-27 19:12:29 UTC-0500	Create a VPC with private and public subnets.

A. create-vpc.yml

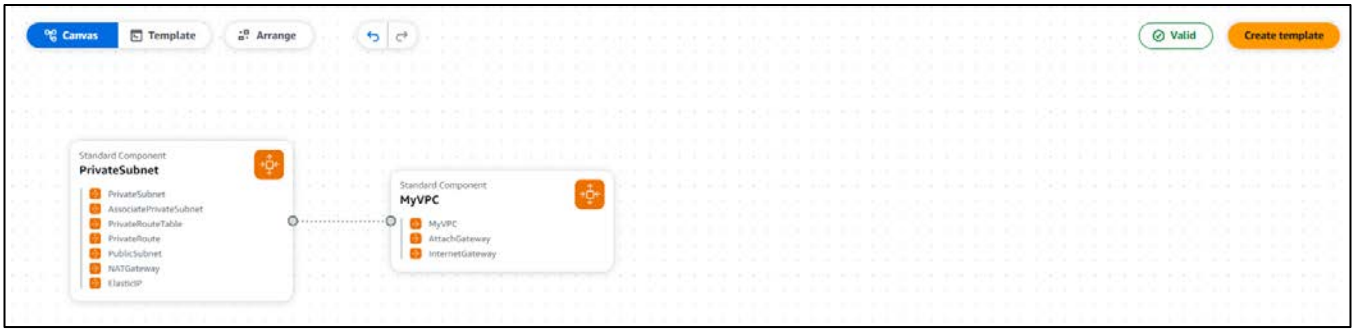
Resources Created:



Resources (10)

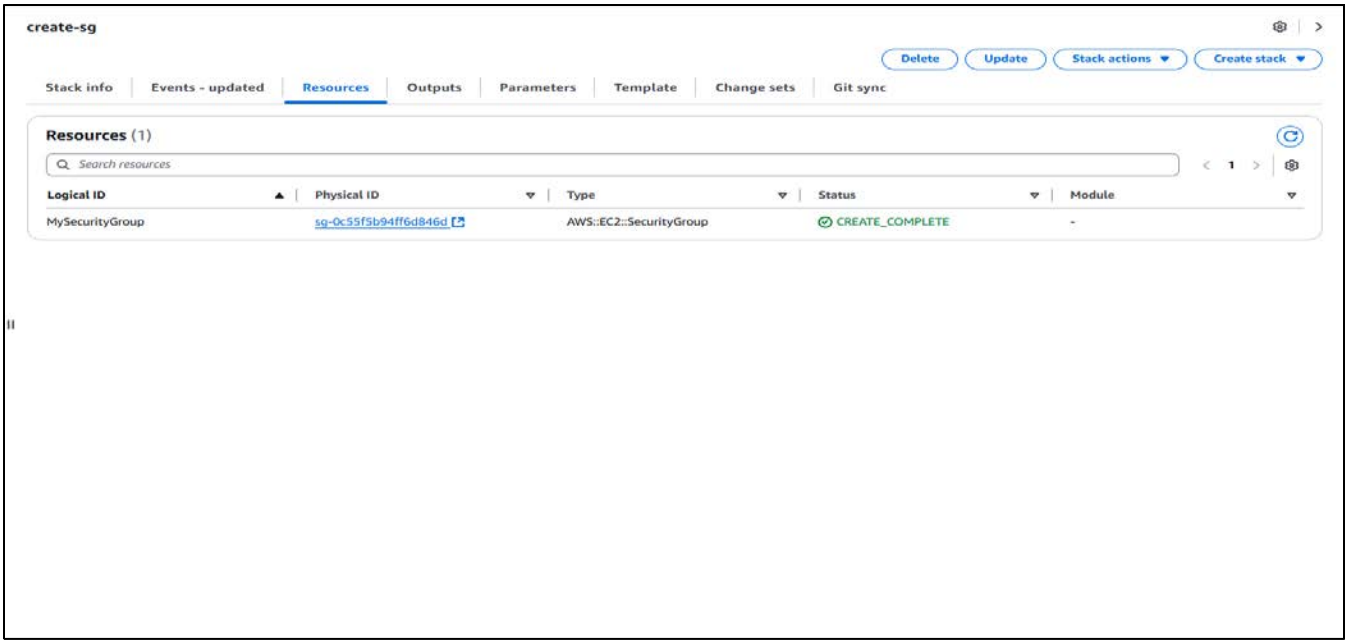
Logical ID	Physical ID	Type	Status	Module
AssociatePrivateSubnet	rtbassoc-03e1a868bbf45c722	AWS::EC2::SubnetRouteTableAssociation	CREATE_COMPLETE	-
AttachGateway	IGW|vpc-0b86a4559bc6d5b74	AWS::EC2::VPCGatewayAttachment	CREATE_COMPLETE	-
ElasticIP	52.2.226.4	AWS::EC2::EIP	CREATE_COMPLETE	-
InternetGateway	igw-02883c0f75ea4abfb	AWS::EC2::InternetGateway	CREATE_COMPLETE	-
MyVPC	vpc-0b86a4559bc6d5b74	AWS::EC2::VPC	CREATE_COMPLETE	-
NATGateway	nat-060cad71e3a848cc9	AWS::EC2::NatGateway	CREATE_COMPLETE	-
PrivateRoute	rtb-0541c16f384420e1e|0.0.0.0/0	AWS::EC2::Route	CREATE_COMPLETE	-
PrivateRouteTable	rtb-0541c16f384420e1e	AWS::EC2::RouteTable	CREATE_COMPLETE	-
PrivateSubnet	subnet-09d01ec9afb0887e1	AWS::EC2::Subnet	CREATE_COMPLETE	-
PublicSubnet	subnet-0f0f826b66381acfa	AWS::EC2::Subnet	CREATE_COMPLETE	-

Canvas Display of Created Resources:



B. create-sg.yml

Resources Created:

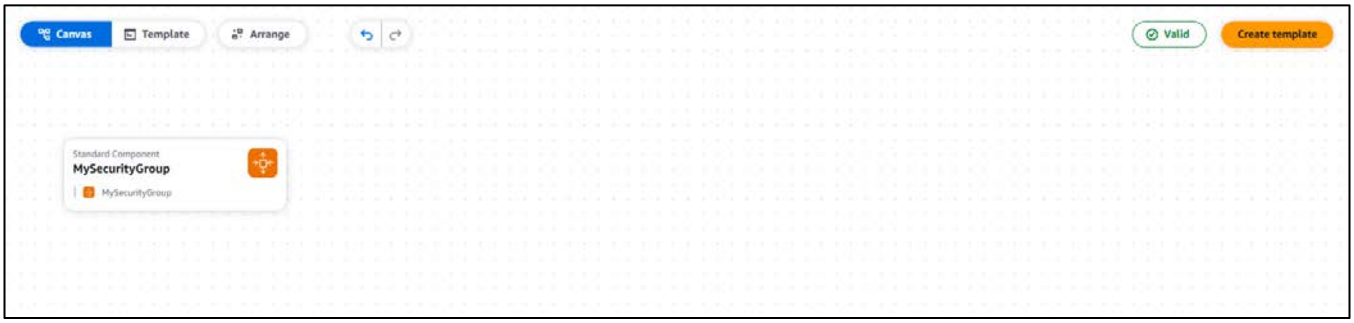


create-sg

Resources (1)

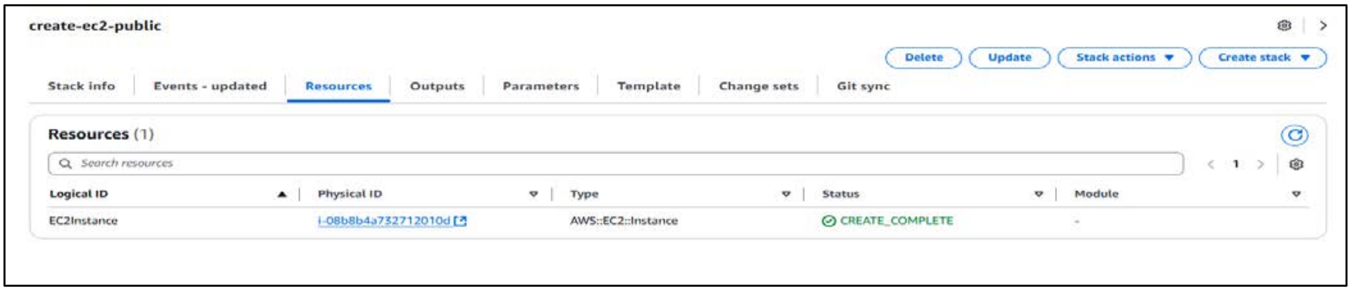
Logical ID	Physical ID	Type	Status	Module
MySecurityGroup	sg-0c55f5b94ff6d846d	AWS::EC2::SecurityGroup	CREATE_COMPLETE	-

Canvas Display of Created Resources:



C. create-ec2.yml

Resouces Created - Public ec2

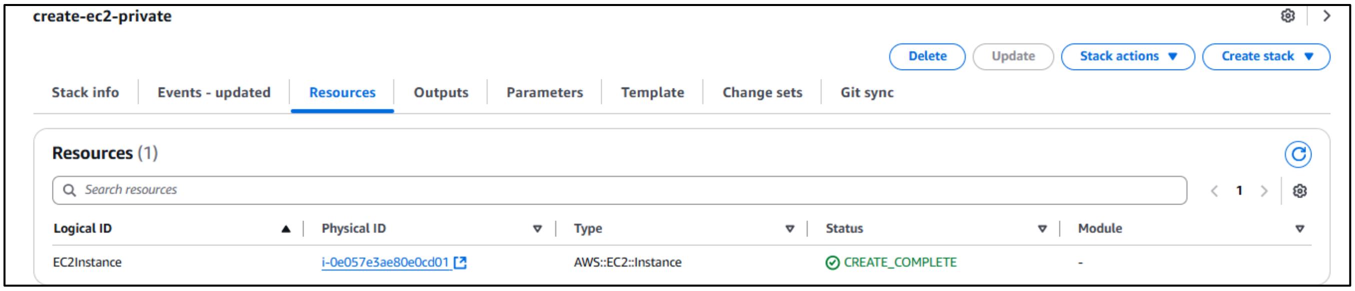


create-ec2-public

Resources (1)

Logical ID	Physical ID	Type	Status	Module
EC2Instance	i-08b8b4a732712010d	AWS::EC2::Instance	CREATE_COMPLETE	-

Resouces Created - Private ec2

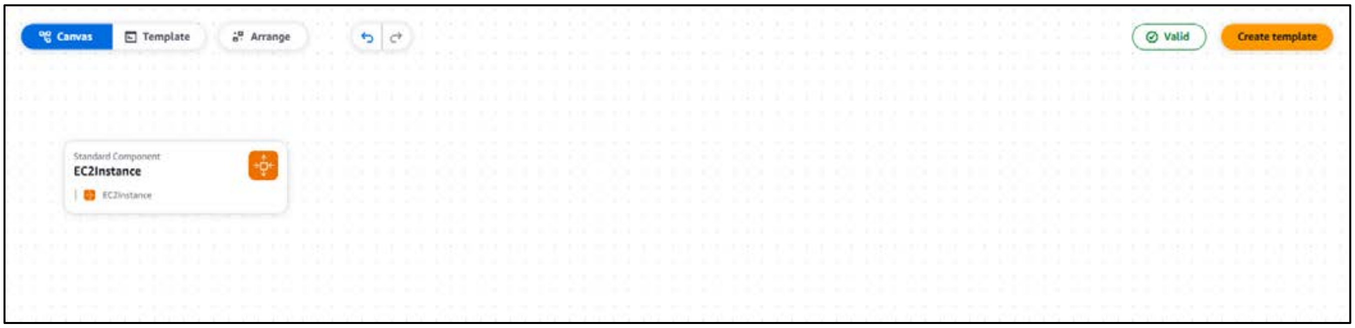


Resources (1)

Search resources

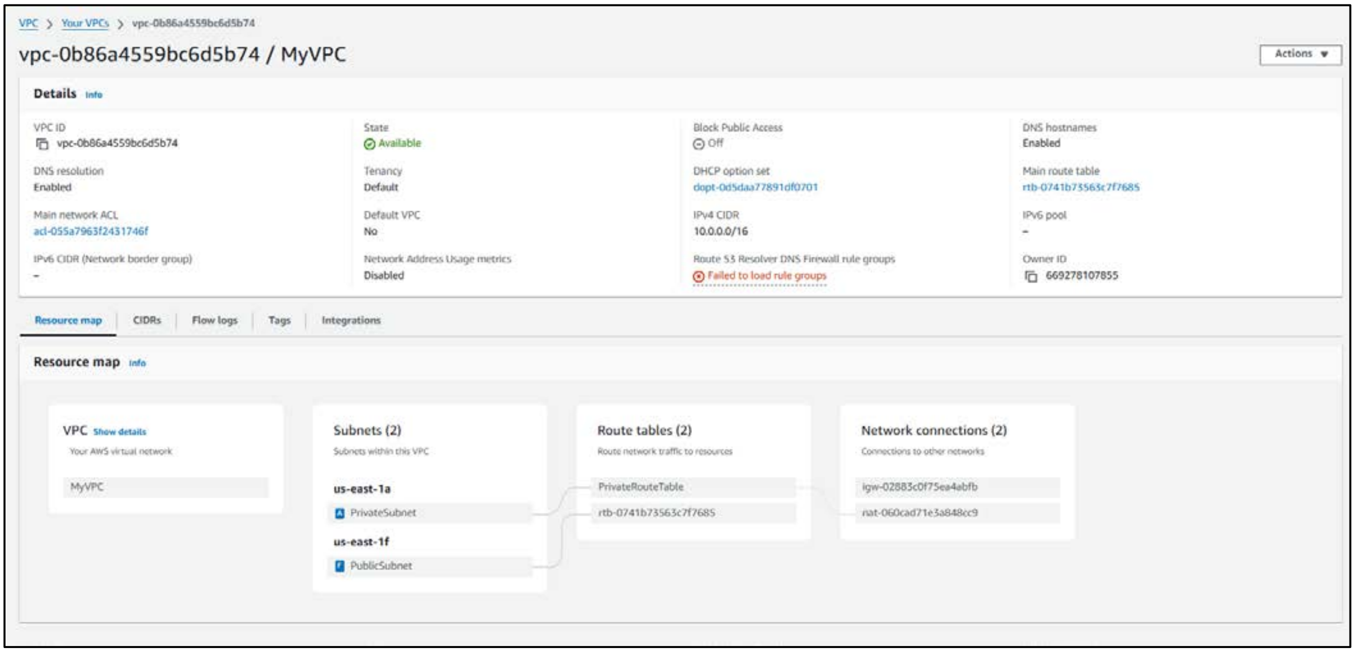
Logical ID	Physical ID	Type	Status	Module
EC2Instance	i-0e057e3ae80e0cd01	AWS::EC2::Instance	✓ CREATE_COMPLETE	-

Canvas Display of Created Resources:



D. VPC, IGW, and Public & Private Subnet with CIDR block

VPC:



vpc-0b86a4559bc6d5b74 / MyVPC

Details Info

VPC ID
vpc-0b86a4559bc6d5b74

State
Available

Block Public Access
Off

DNS hostnames
Enabled

DNS resolution
Enabled

Tenancy
Default

DHCP option set
dopt-0d5daa77891df0701

Main route table
rtb-0741b73563c7f7685

Main network ACL
acl-055a7963f2431746f

Default VPC
No

IPv4 CIDR
10.0.0.0/16

IPv6 pool
-

IPv6 CIDR (Network border group)
-

Network Address Usage metrics
Disabled

Route 53 Resolver DNS Firewall rule groups
Failed to load rule groups

Owner ID
669278107855

Resource map Info

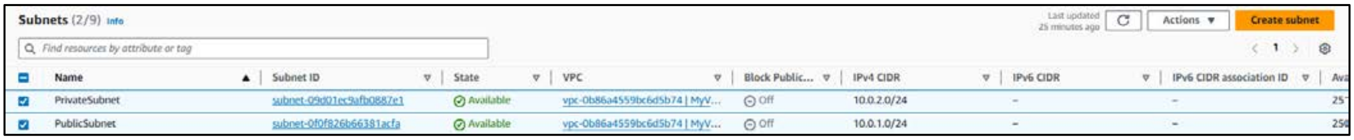
VPC Show details
Your AWS virtual network
MyVPC

Subnets (2)
Subnets within this VPC
us-east-1a
PrivateSubnet
us-east-1f
PublicSubnet

Route tables (2)
Route network traffic to resources
PrivateRouteTable
rtb-0741b73563c7f7685

Network connections (2)
Connections to other networks
igw-02883c0f75ea4abfb
nat-060cad71e3a848cc9

Public & Private Subnet:

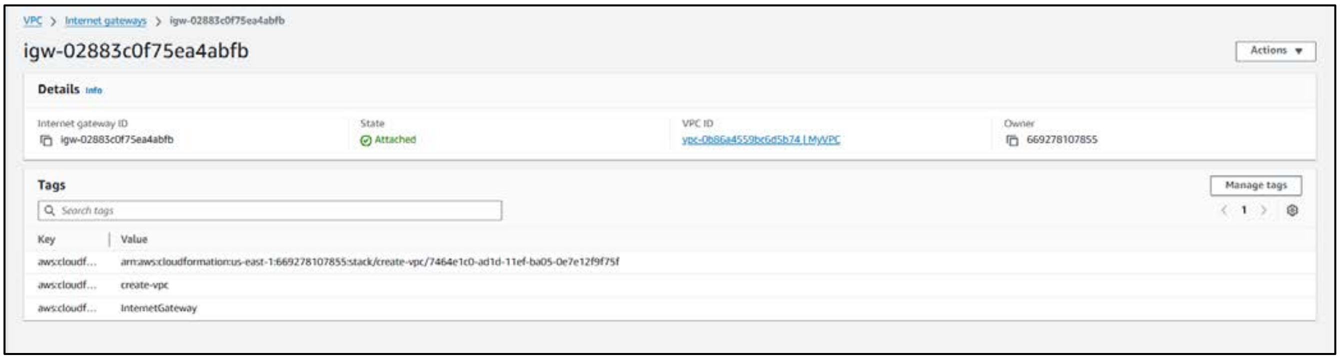


Subnets (2/9) Info

Last updated 25 minutes ago

☑	Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR association ID	Ava
☑	PrivateSubnet	subnet-09d01ec9afb0887e1	✓ Available	vpc-0b86a4559bc6d5b74 | MyV...	⊖ Off	10.0.2.0/24	–	–	25
☑	PublicSubnet	subnet-0f0f826b66381acfa	✓ Available	vpc-0b86a4559bc6d5b74 | MyV...	⊖ Off	10.0.1.0/24	–	–	25

IGW:



VPC > Internet gateways > igw-02883c0f75ea4abfb

igw-02883c0f75ea4abfb

Details Info

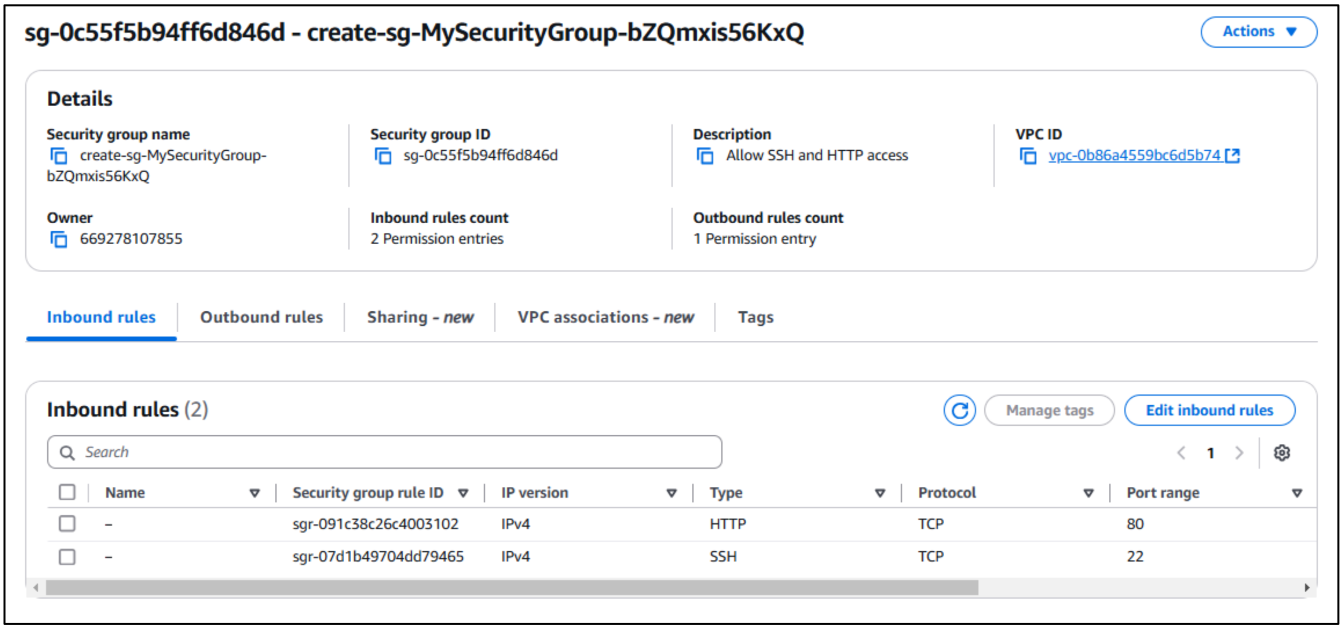
Internet gateway ID	State	VPC ID	Owner
igw-02883c0f75ea4abfb	✓ Attached	vpc-0b86a4559bc6d5b74 | MyVPC	669278107855

Tags

Key	Value
aws:cloudf...	arn:aws:cloudformation:us-east-1:669278107855:stack/create-vpc/7464e1c0-ad1d-11ef-ba05-0e7e12f9f75f
aws:cloudf...	create-vpc
aws:cloudf...	InternetGateway

E. **EC2 with the given SG configuration in the public subnet created**

SG:



sg-0c55f5b94ff6d846d - create-sg-MySecurityGroup-bZQmxis56KxQ

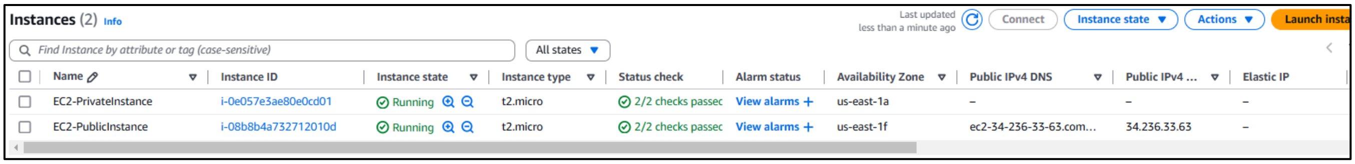
Details

Security group name	Security group ID	Description	VPC ID
create-sg-MySecurityGroup-bZQmxis56KxQ	sg-0c55f5b94ff6d846d	Allow SSH and HTTP access	vpc-0b86a4559bc6d5b74
Owner	**Inbound rules count**	**Outbound rules count**	
669278107855	2 Permission entries	1 Permission entry	

Inbound rules (2)

□	Name	Security group rule ID	IP version	Type	Protocol	Port range
□	–	sgr-091c38c26c4003102	IPv4	HTTP	TCP	80
□	–	sgr-07d1b49704dd79465	IPv4	SSH	TCP	22

Running Instances:

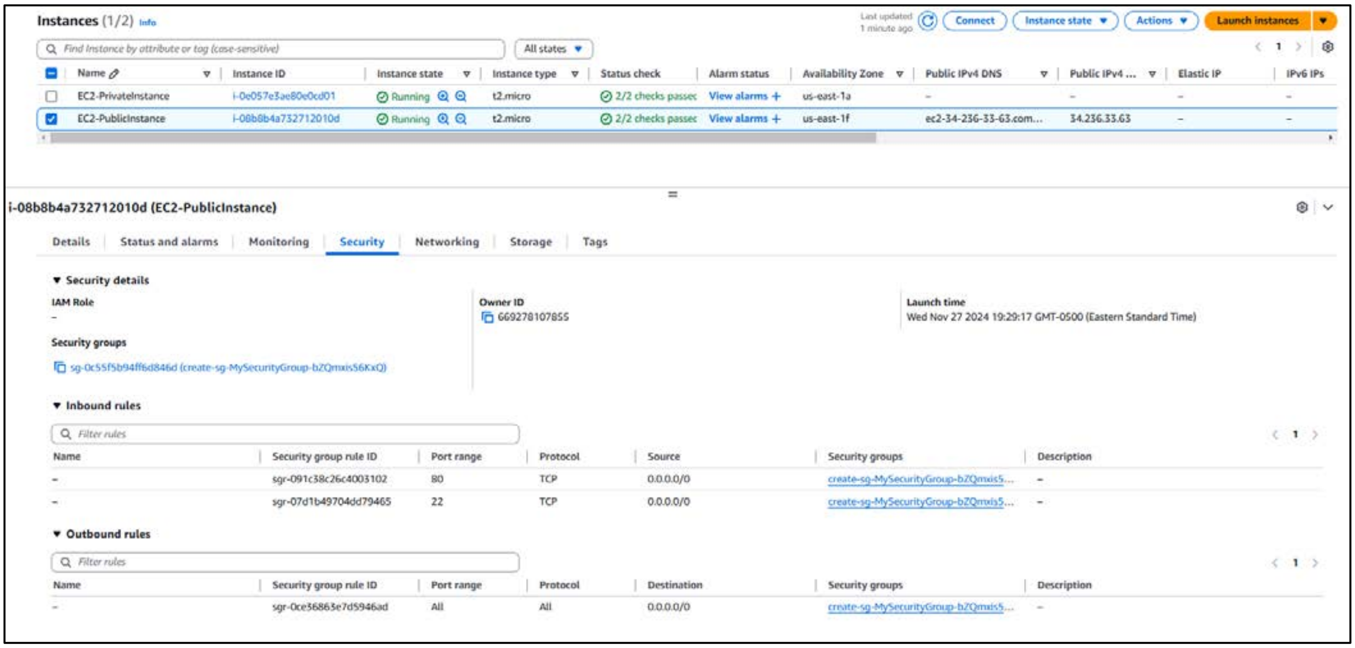


Instances (2) Info

Last updated less than a minute ago

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
□	EC2-PrivateInstance	i-0e057e3ae80e0cd01	Running	t2.micro	2/2 checks passec	View alarms +	us-east-1a	–	–	–
□	EC2-PublicInstance	i-08b8b4a732712010d	Running	t2.micro	2/2 checks passec	View alarms +	us-east-1f	ec2-34-236-33-63.com...	34.236.33.63	–

SG config in the public subnet:



Instances (1/2) Info

Last updated 1 minute ago

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
□	EC2-PrivateInstance	i-0e057e3ae80e0cd01	Running	t2.micro	2/2 checks passec	View alarms +	us-east-1a	–	–	–	–
☑	EC2-PublicInstance	i-08b8b4a732712010d	Running	t2.micro	2/2 checks passec	View alarms +	us-east-1f	ec2-34-236-33-63.com...	34.236.33.63	–	–

i-08b8b4a732712010d (EC2-PublicInstance)

▼ **Security details**

IAM Role
–

Owner ID
669278107855

Launch time
Wed Nov 27 2024 19:29:17 GMT-0500 (Eastern Standard Time)

Security groups
sg-0c55f5b94ff6d846d (create-sg-MySecurityGroup-bZQmxis56KxQ)

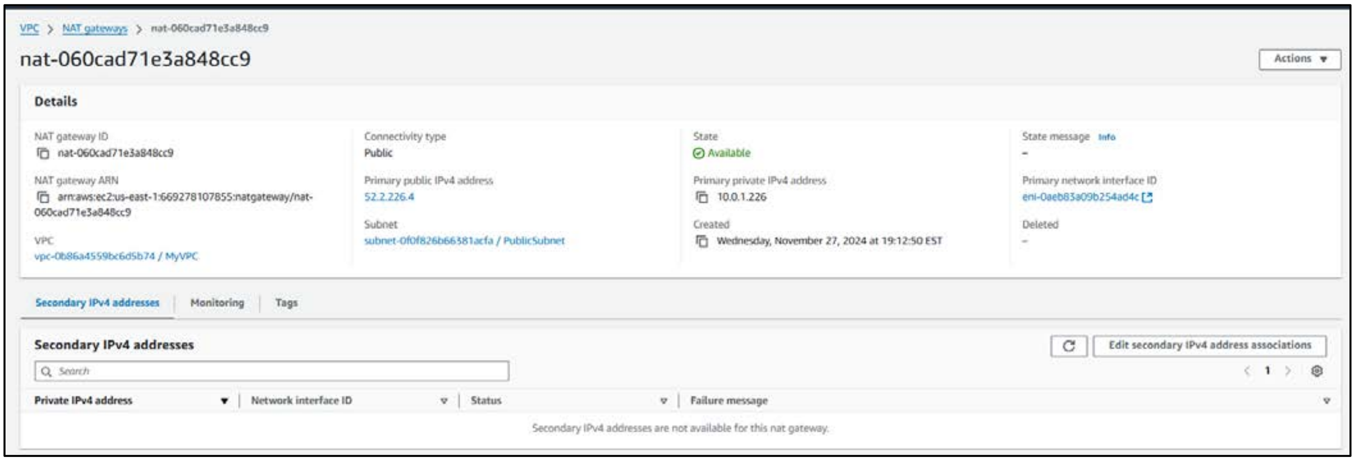
▼ **Inbound rules**

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
–	sgr-091c38c26c4003102	80	TCP	0.0.0.0/0	create-sg-MySecurityGroup-bZQmxis5...	–
–	sgr-07d1b49704dd79465	22	TCP	0.0.0.0/0	create-sg-MySecurityGroup-bZQmxis5...	–

▼ **Outbound rules**

Name	Security group rule ID	Port range	Protocol	Destination	Security groups	Description
–	sgr-0ce36863e7d5946ad	All	All	0.0.0.0/0	create-sg-MySecurityGroup-bZQmxis5...	–

NAT Gateway



VPC > NAT gateways > nat-060cad71e3a848cc9

nat-060cad71e3a848cc9

Details

NAT gateway ID
nat-060cad71e3a848cc9

NAT gateway ARN
arn:aws:ec2:us-east-1:669278107855:natgateway/nat-060cad71e3a848cc9

VPC
vpc-0b86a4559bc6d5b74 / MyVPC

Connectivity type
Public

Primary public IPv4 address
52.2.226.4

Subnet
subnet-0f0f826b66381acfa / PublicSubnet

State
Available

Primary private IPv4 address
10.0.1.226

Created
Wednesday, November 27, 2024 at 19:12:50 EST

State message Info
–

Primary network interface ID
eni-0aeb83a09b254ad4c

Deleted
–

Secondary IPv4 addresses

Private IPv4 address	Network interface ID	Status	Failure message

Secondary IPv4 addresses are not available for this nat gateway.