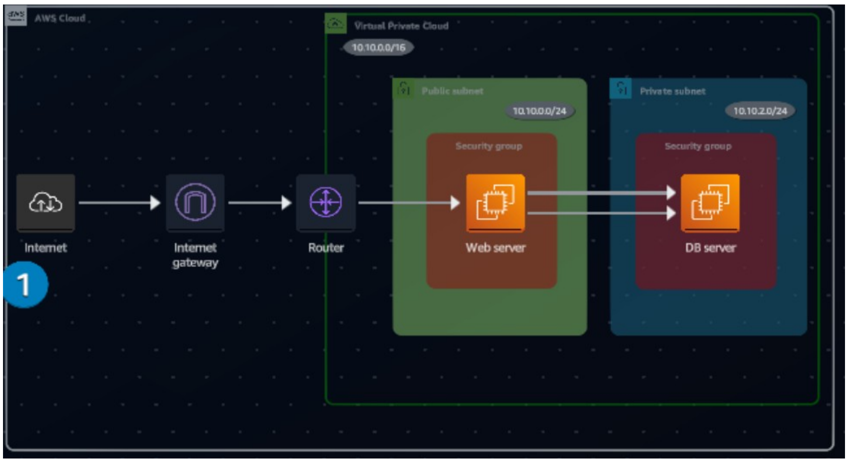
AMAZON VPC: BUILDING AND CONFIGURING YOUR VIRTUAL NETWORK

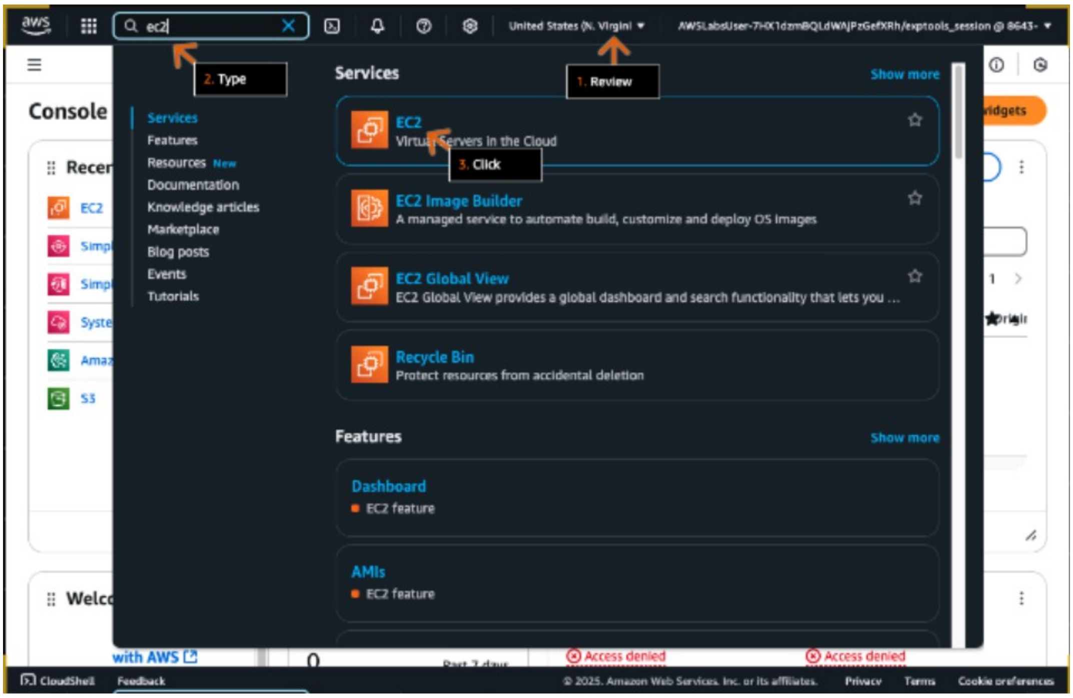
Objectives:

Explore the components that comprise a virtual private cloud (VPC).
Configure a route table attached to a subnet within a VPC.
Configure a route table to direct internet-bound traffic to the internet gateway.
Configure inbound rules within a security group to control access.



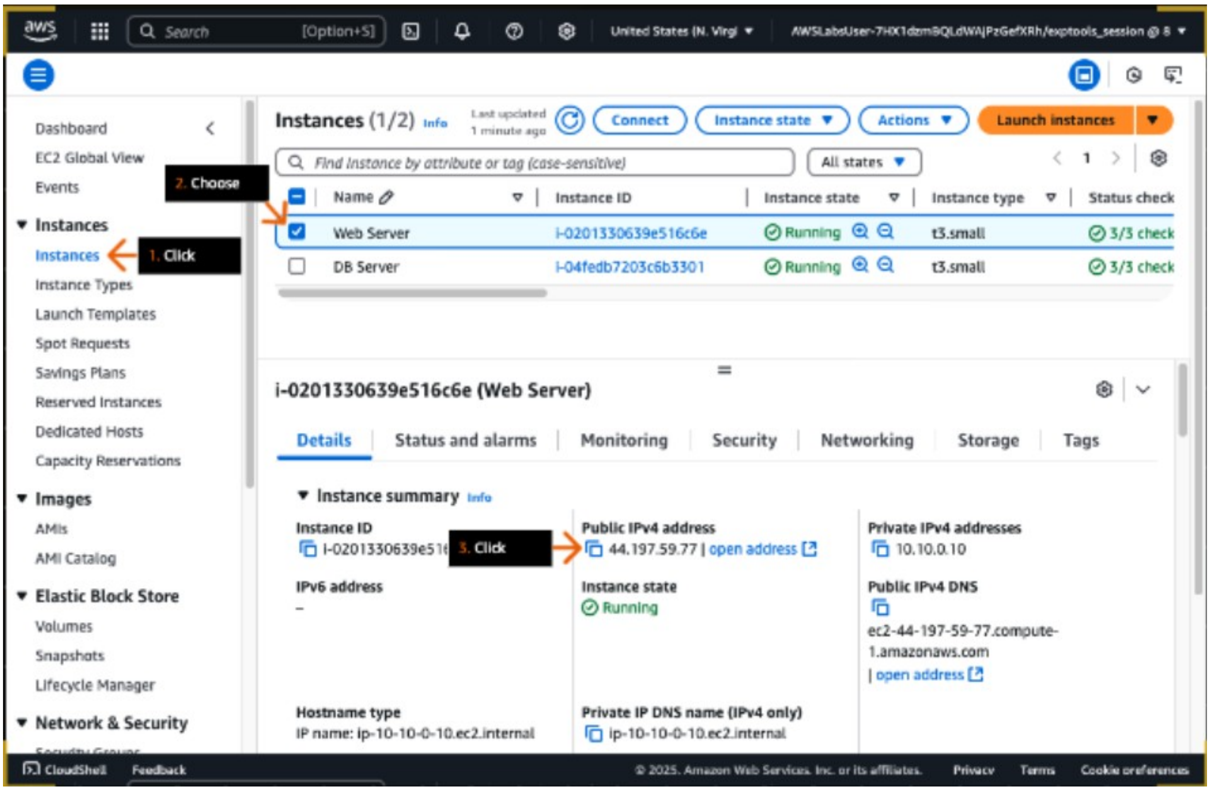
Steps / Procedures / Instructions:

- On the top navigation bar, review the Region selector to confirm that the Region is set to N. Virginia (us-east-1).
- In the Services search box, type: ec2
- In the search results, under Services, click EC2.


aws
ec2
United States (N. Virginia) ▾
AWSLabsUser-7HX1dzmBQLdWNJPzGefXRh/exptools_session @ 8643- ▾
2. Type
1. Review
3. Click
Console
Recent
EC2
S3
Welcome
Services
Features
Resources New
Documentation
Knowledge articles
Marketplace
Blog posts
Events
Tutorials
Services
Show more
EC2
Virtual Servers in the Cloud
EC2 Image Builder
A managed service to automate build, customize and deploy OS images
EC2 Global View
EC2 Global View provides a global dashboard and search functionality that lets you ...
Recycle Bin
Protect resources from accidental deletion
Features
Show more
Dashboard
EC2 feature
AMIs
EC2 feature
Widgets
with AWS
Access denied
Access denied
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

- In the left navigation pane, click Instances.

- In the Instances section, choose the check box to select the Web Server instance.
- On the Details tab, under Public IPv4 address, click the copy icon to copy the provided address.



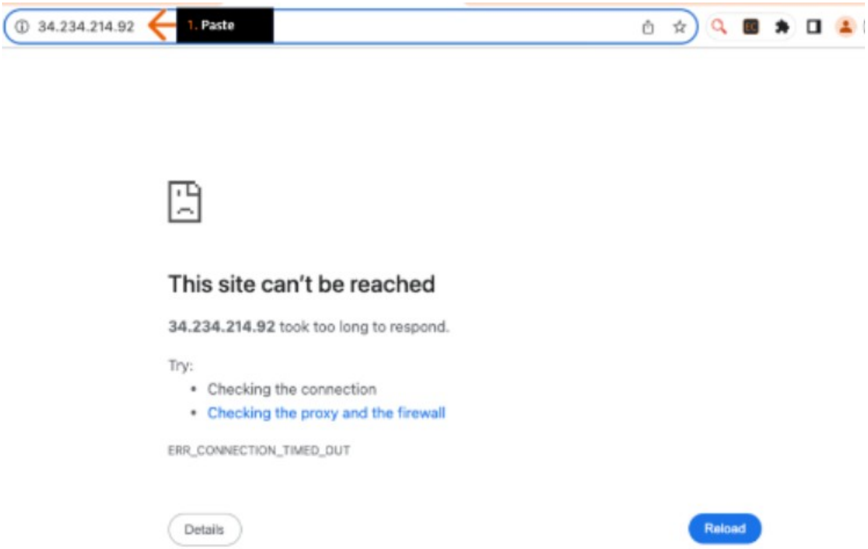
Name	Instance ID	Instance state	Instance type	Status check
☑ Web Server	i-0201330639e516c6e	Running	t3.small	3/3 check
□ DB Server	i-04fedb7203c6b3301	Running	t3.small	3/3 check

i-0201330639e516c6e (Web Server)

Instance ID: i-0201330639e516c6e
Public IPv4 address: 44.197.59.77 | open address
Private IPv4 addresses: 10.10.0.10
IPv6 address: –
Instance state: Running
Public IPv4 DNS: ec2-44-197-59-77.compute-1.amazonaws.com | open address
Hostname type: IP name: ip-10-10-0-10.ec2.internal
Private IP DNS name (IPv4 only): ip-10-10-0-10.ec2.internal

A public IP address is an IPv4 address that's reachable from the internet. You can use public addresses for communication between your instances and the internet.

- In a new browser tab (or window) address bar, paste the IP address that you just copied and press Enter.
  - After about a minute, a site timeout message should appear.



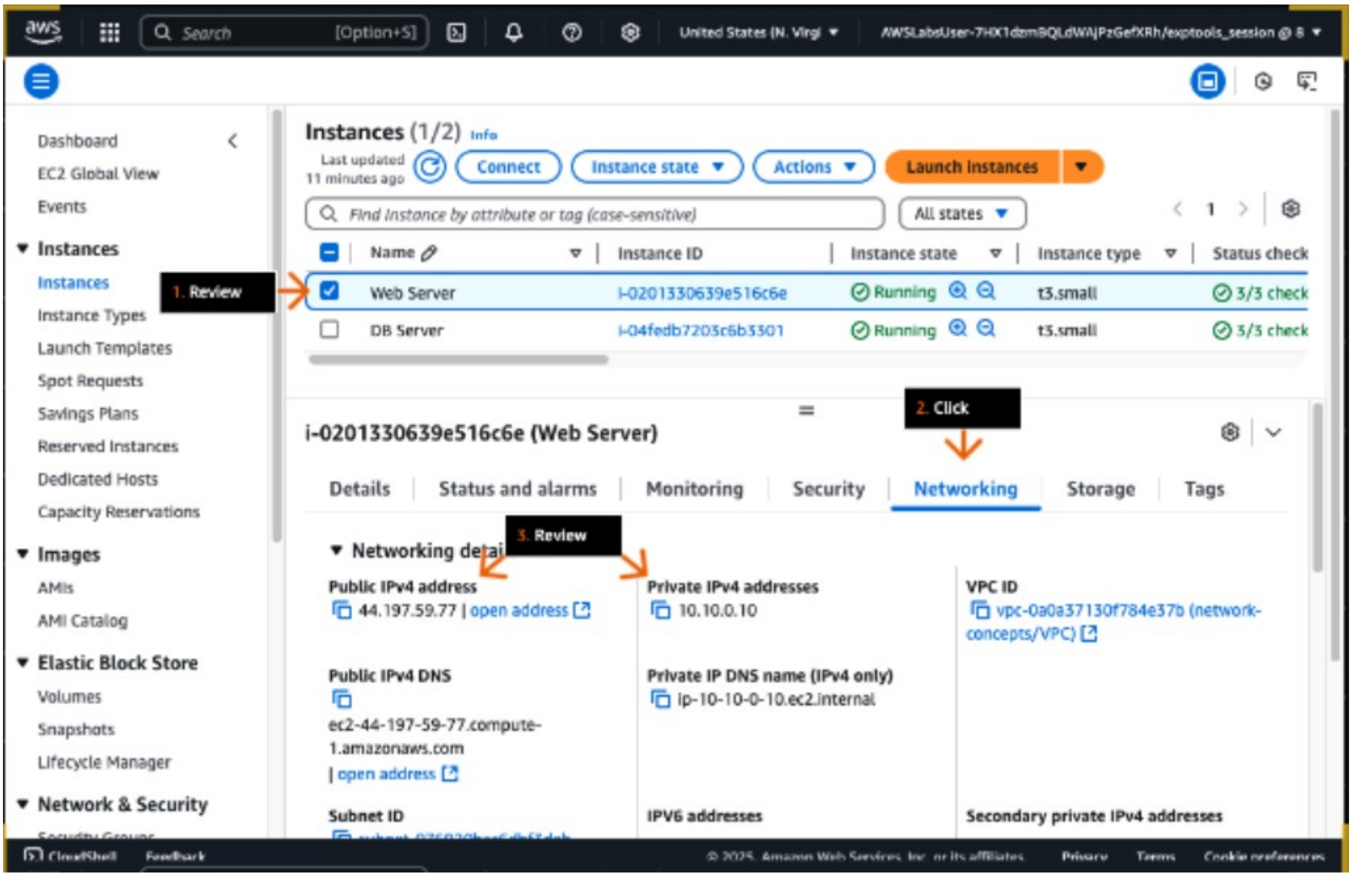
This site can't be reached

34.234.214.92 took too long to respond.

Try:
- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_TIMED_OUT

- To solve this issue, return to the Amazon EC2 console browser tab.
- Review to confirm that the Web Server instance is still selected.
- Click the Networking tab.
- Review the Public and Private IPv4 addresses.



	Name	Instance ID	Instance state	Instance type	Status check
☑	Web Server	i-0201330639e516c6e	Running	t3.small	3/3 check
□	DB Server	i-04fedb7203c6b3301	Running	t3.small	3/3 check

1. Review

i-0201330639e516c6e (Web Server)

2. Click

Networking details

3. Review

Public IPv4 address: 44.197.59.77 | open address

Private IPv4 addresses: 10.10.0.10

VPC ID: vpc-0a0a37130f784e37b (network-concepts/VPC)

Public IPv4 DNS: ec2-44-197-59-77.compute-1.amazonaws.com | open address

Private IP DNS name (IPv4 only): ip-10-10-0-10.ec2.internal

Subnet ID

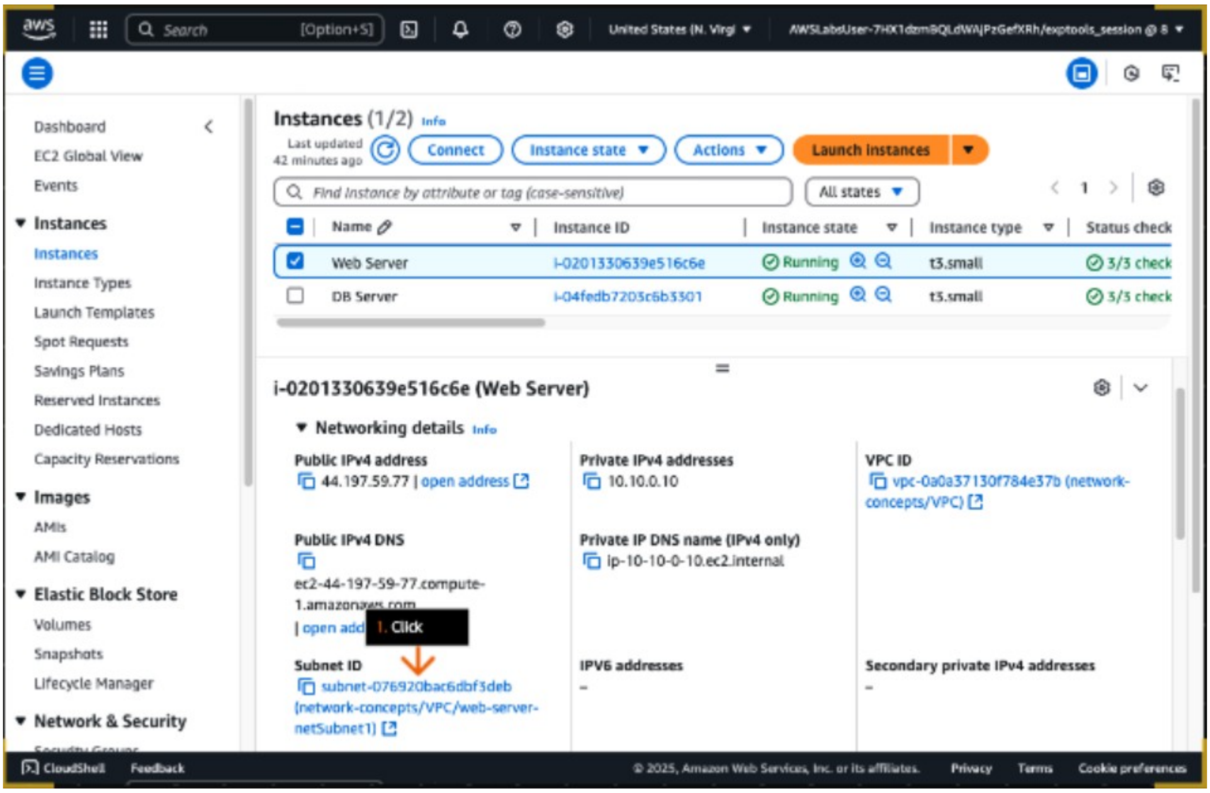
IPV6 addresses

Secondary private IPv4 addresses

Using Amazon Virtual Private Cloud (Amazon VPC), you can launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

- Under Subnet ID, click the provided ID.
  - The subnet ID opens the Amazon VPC console in a new browser tab (or window).

A subnet is a range of IP addresses in your VPC. You can launch AWS resources into a specified subnet. Each subnet must reside entirely within one Availability Zone and cannot span zones.



Instances (1/2) Info

Last updated 42 minutes ago

Find Instance by attribute or tag (case-sensitive)

	Name	Instance ID	Instance state	Instance type	Status check
☑	Web Server	i-0201330639e516c6e	Running	t3.small	3/3 check
□	DB Server	i-04fedb7203c6b3301	Running	t3.small	3/3 check

i-0201330639e516c6e (Web Server)

Networking details Info

Public IPv4 address: 44.197.59.77 | open address

Private IPv4 addresses: 10.10.0.10

VPC ID: vpc-0a0a37130f784e37b (network-concepts/VPC)

Public IPv4 DNS: ec2-44-197-59-77.compute-1.amazonaws.com | open add

Private IP DNS name (IPv4 only): ip-10-10-0-10.ec2.internal

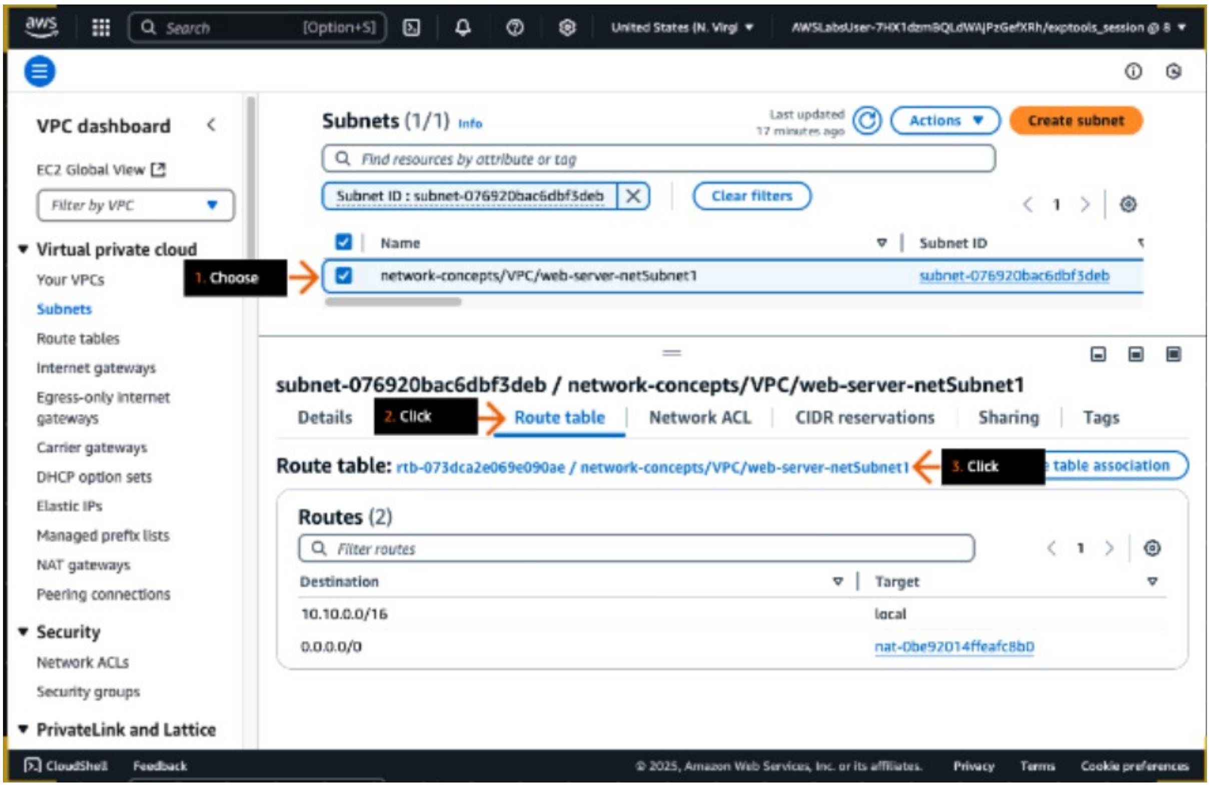
1. Click

Subnet ID: subnet-076920bac6dbf3deb (network-concepts/VPC/web-server-netSubnet1)

IPV6 addresses: –

Secondary private IPv4 addresses: –

- In the Subnets section, choose the check box to select the subnet name that starts with network-concepts.
- Click the Route table tab.
- Next to Route table, click the link name that contains web-server-netSubnet1.



Subnets (1/1) Info

Last updated 17 minutes ago

Find resources by attribute or tag

Subnet ID : subnet-076920bac6dbf3deb

1. Choose

	Name	Subnet ID
☑	network-concepts/VPC/web-server-netSubnet1	subnet-076920bac6dbf3deb

subnet-076920bac6dbf3deb / network-concepts/VPC/web-server-netSubnet1

2. Click

Route table: rtb-073dca2e069e090ae / network-concepts/VPC/web-server-netSubnet1

3. Click

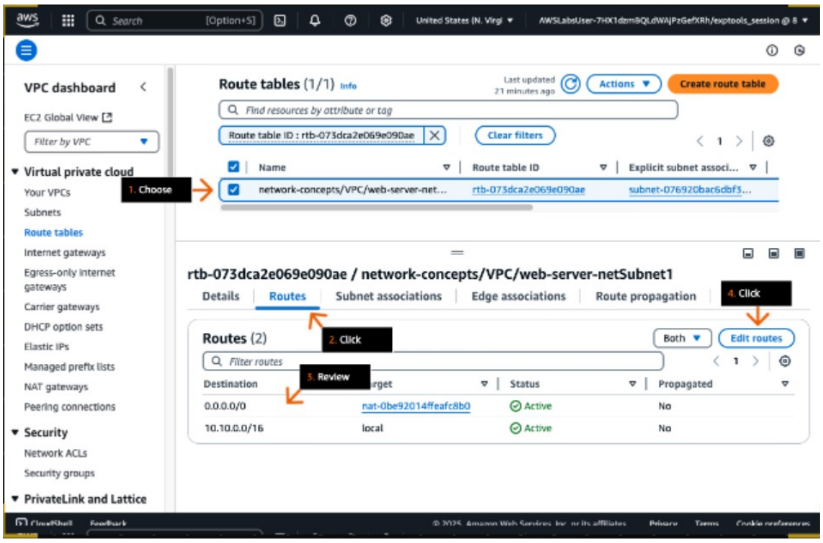
Routes (2)

Filter routes

Destination	Target
10.10.0.0/16	local
0.0.0.0/0	nat-0be92014ffeafc8b0

A route table contains a set of rules, named routes, that are used to determine where network traffic from your subnet or gateway is directed. Use a public subnet for internet-connected resources and a private subnet for resources not connected to the internet.

- In the Route tables section, choose the check box to select the route table name that starts with network-concepts.
- Click the Routes tab.
- Review the two route table entries.
    - One route sends local traffic to the local network only.
    - The other route sends all other traffic to the internet through a NAT gateway.
- Click Edit routes.



Route tables (1/1) Info

Route table ID : rtb-073dca2e069e090ae

☑	Name	Route table ID	Explicit subnet associ...
☑	network-concepts/VPC/web-server-net...	rtb-073dca2e069e090ae	subnet-076920bac6dbf3...

1. Choose

rtb-073dca2e069e090ae / network-concepts/VPC/web-server-netSubnet1

2. Click

Routes (2)

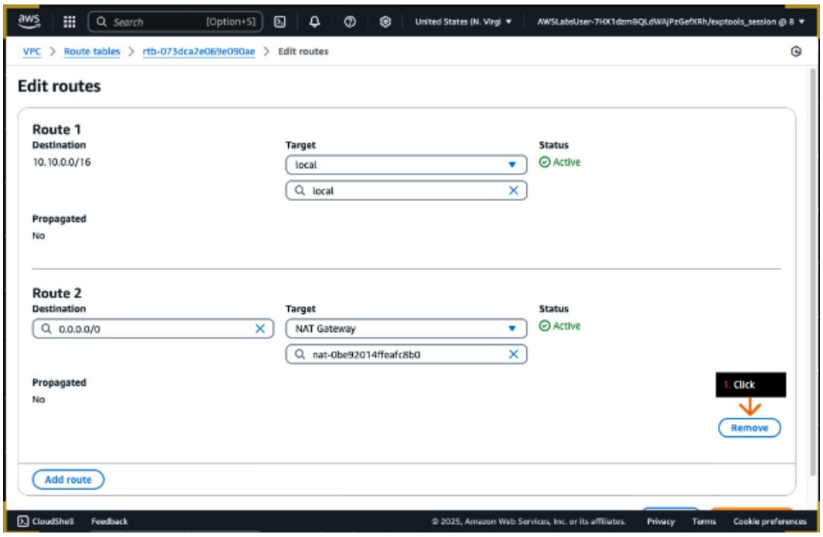
3. Review

Destination	Target	Status	Propagated
0.0.0.0/0	nat-0be92014ffeafc8b0	Active	No
10.10.0.0/16	local	Active	No

4. Click

A NAT gateway is a network address translation (NAT) service. With a NAT gateway, instances in a private subnet can connect to services outside your VPC. External services, however, cannot initiate a connection with those instances.

- To delete the NAT gateway from the route table, click Remove.
    - By removing this route, the instances in this subnet can no longer connect to external services.



aws
Search [Option+S]
United States (N. Virgi
AWSLabsUser-7HX1dzmBQLdWAjPzGefXRh/exptools_session @ 8
VPC > Route tables > rtb-073dca2e069e090ae > Edit routes
Remove
Add route
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Edit routes

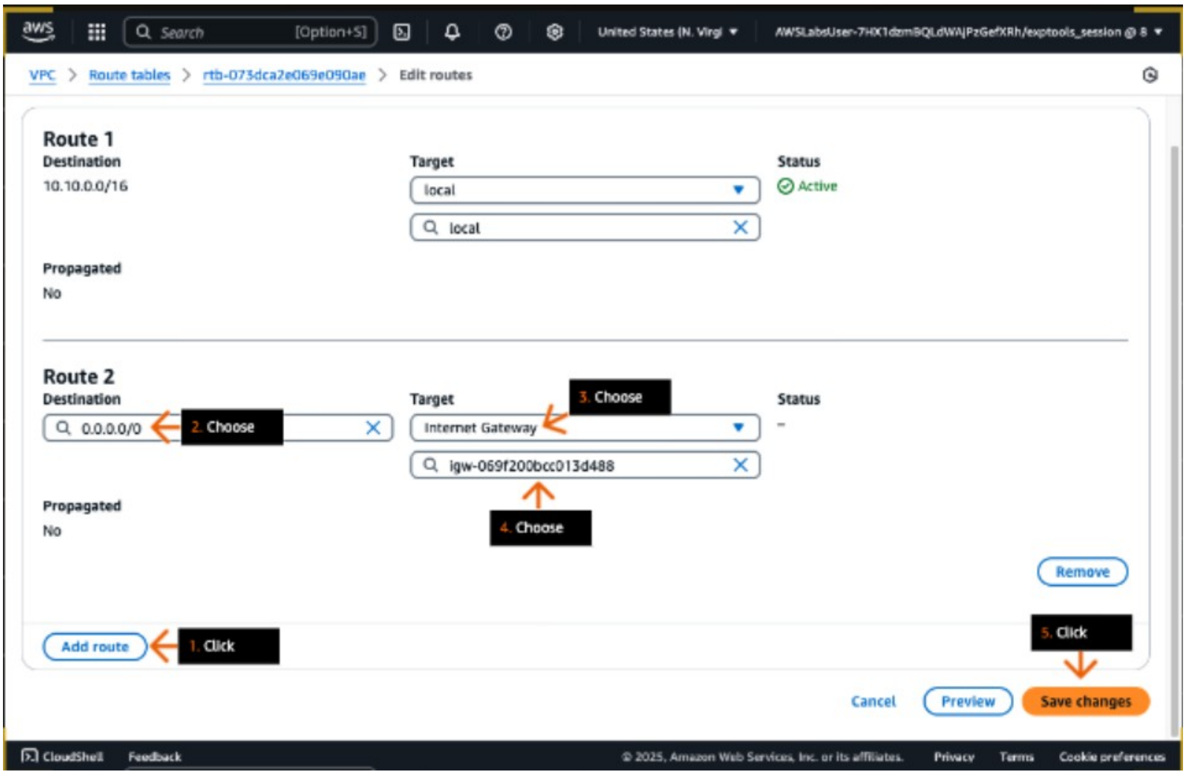
Route 1
Destination: 10.10.0.0/16
Target: local
local
Status: Active
Propagated: No

Route 2
Destination: 0.0.0.0/0
Target: NAT Gateway
nat-0be92014ffeafc8b0
Status: Active
Propagated: No

1. Click

The CIDR naming convention 0.0.0.0/0 represents all possible IPv4 addresses (::/0 for IPv6).

- Now, Click Add route.
- For Destination, on the dropdown list, choose 0.0.0.0/0.
- For Target, choose Internet Gateway.
- Below that, choose igw-xxxxxxx.
- Click Save changes.



VPC > Route tables > rtb-073dca2e069e090ae > Edit routes

Route 1

Destination: 10.10.0.0/16

Target: local

local

Status: Active

Propagated: No

Route 2

Destination: 0.0.0.0/0

2. Choose

Target: Internet Gateway

3. Choose

igw-069f200bcc013d488

4. Choose

Status: -

Propagated: No

1. Click

5. Click

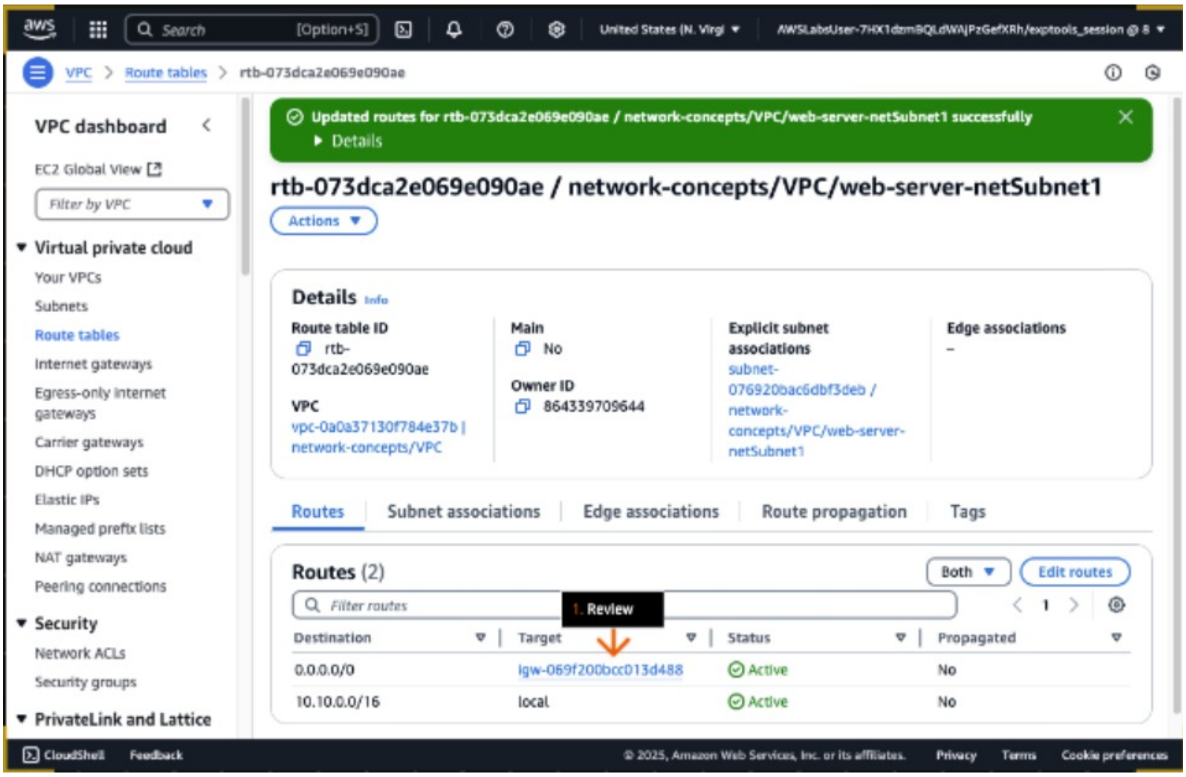
An internet gateway serves two purposes:

- Provide a target in your VPC route tables for internet-routable traffic.
- Perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.

- On the Routes tab, under Target, review the new internet gateway association.
  - The subnet is now reachable from the internet.
- Return to the Amazon EC2 console in the other browser tab.

An Internet gateway is horizontally scaled, redundant, and highly available, imposing no availability risks or bandwidth constraints on network traffic. There's no additional charge for having an internet gateway in your account. It serves two main purposes:

- Provide a target in VPC route tables for internet-routable traffic.
- Perform network address translation (NAT) for instances with public IPv4 addresses.



Updated routes for rtb-073dca2e069e090ae / network-concepts/VPC/web-server-netSubnet1 successfully

▸ Details

rtb-073dca2e069e090ae / network-concepts/VPC/web-server-netSubnet1

Details Info

Route table ID: rtb-073dca2e069e090ae

Main: No

Explicit subnet associations: subnet-076920bac6dbf3deb / network-concepts/VPC/web-server-netSubnet1

Edge associations: –

VPC: vpc-0a0a37130f784e37b | network-concepts/VPC

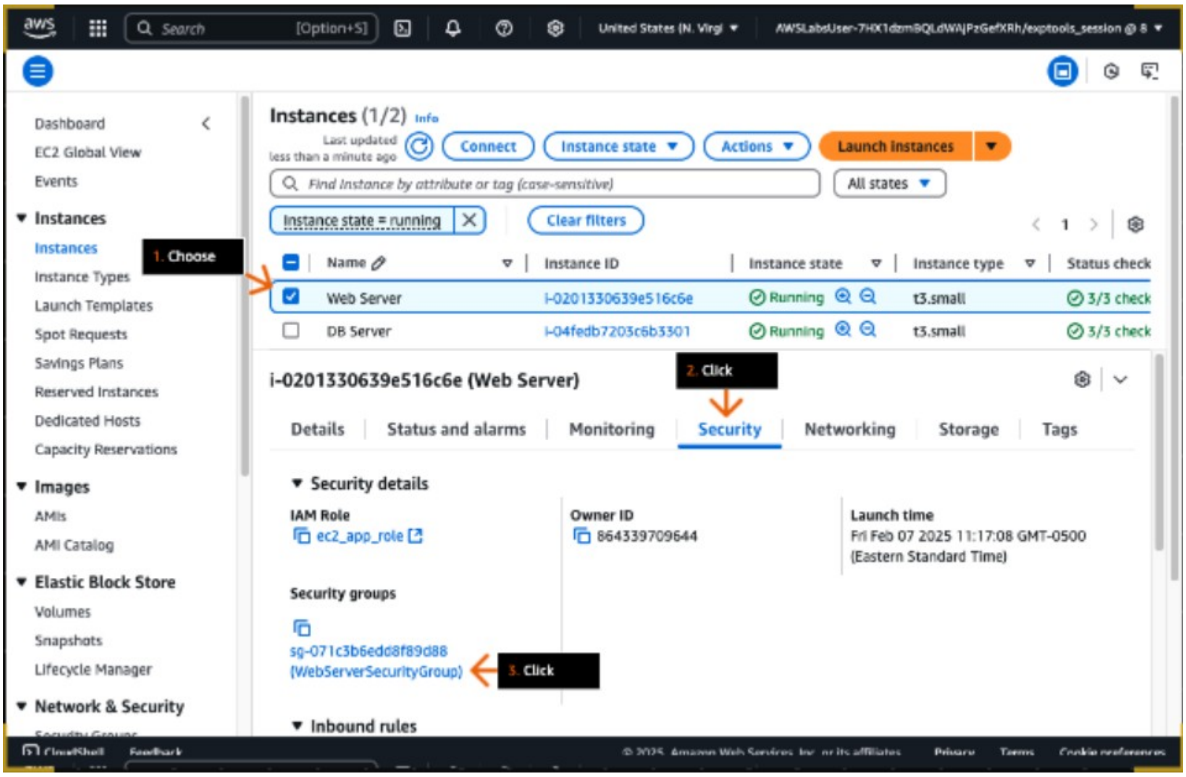
Owner ID: 864339709644

Routes (2)

1. Review

Destination	Target	Status	Propagated
0.0.0.0/0	igw-069f200bcc013d488	Active	No
10.10.0.0/16	local	Active	No

- In the Instances section, choose the check box to select the Web Server instance.
- Click the Security tab.
- Under Security groups, click WebServerSecurityGroup.



Instances (1/2) Info

Last updated less than a minute ago

1. Choose

☐	Name	Instance ID	Instance state	Instance type	Status check
☑	Web Server	i-0201330639e516c6e	Running	t3.small	3/3 check
☐	DB Server	i-04fedb7203c6b3301	Running	t3.small	3/3 check

i-0201330639e516c6e (Web Server)

2. Click

Security details

IAM Role: ec2_app_role

Owner ID: 864339709644

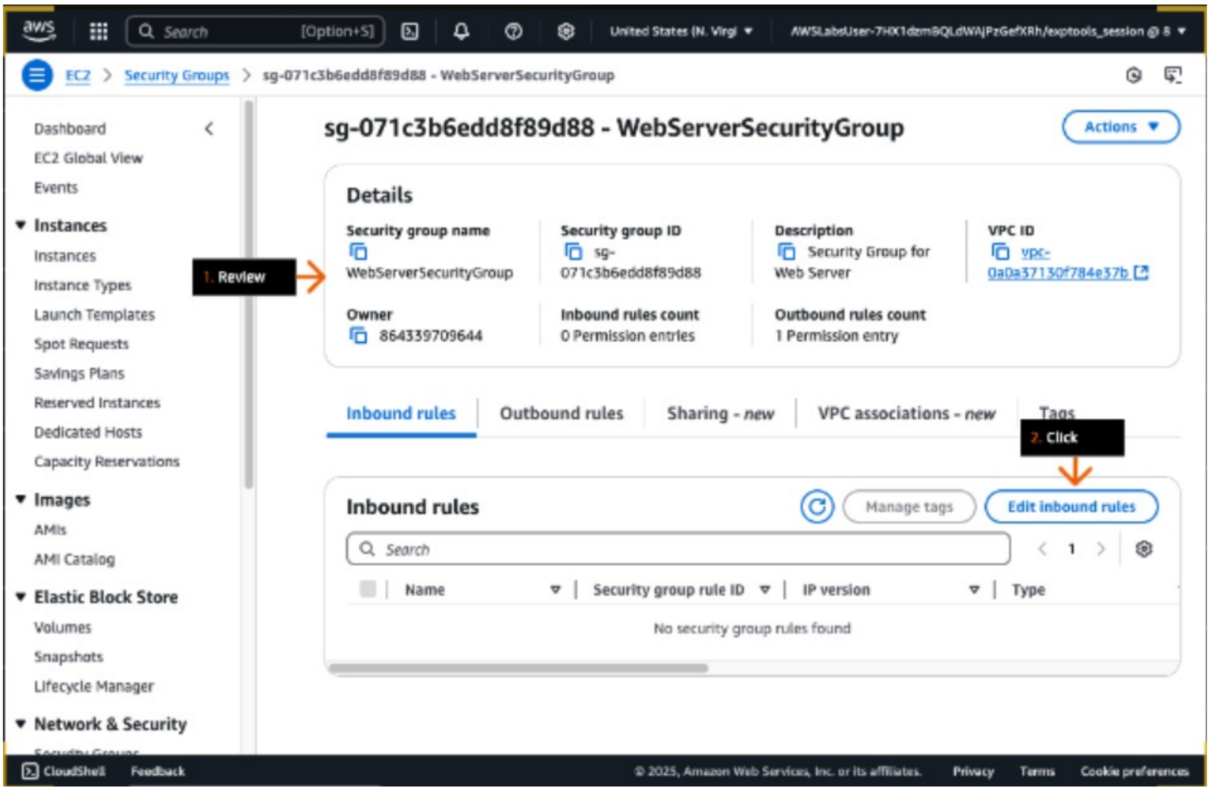
Launch time: Fri Feb 07 2025 11:17:08 GMT-0500 (Eastern Standard Time)

Security groups: sg-071c3b6edd8f89d88 (WebServerSecurityGroup)

3. Click

A Security group is a virtual firewall that controls traffic to and form AWS resources.

- In the Details section, review the security group details.
- On the Inbound rules tab, click Edit inbound rules.



sg-071c3b6edd8f89d88 - WebServerSecurityGroup

Details

Security group name: WebServerSecurityGroup

Security group ID: sg-071c3b6edd8f89d88

Description: Security Group for Web Server

VPC ID: vpc-0a0a37130f784e37b

Owner: 864339709644

Inbound rules count: 0 Permission entries

Outbound rules count: 1 Permission entry

Inbound rules

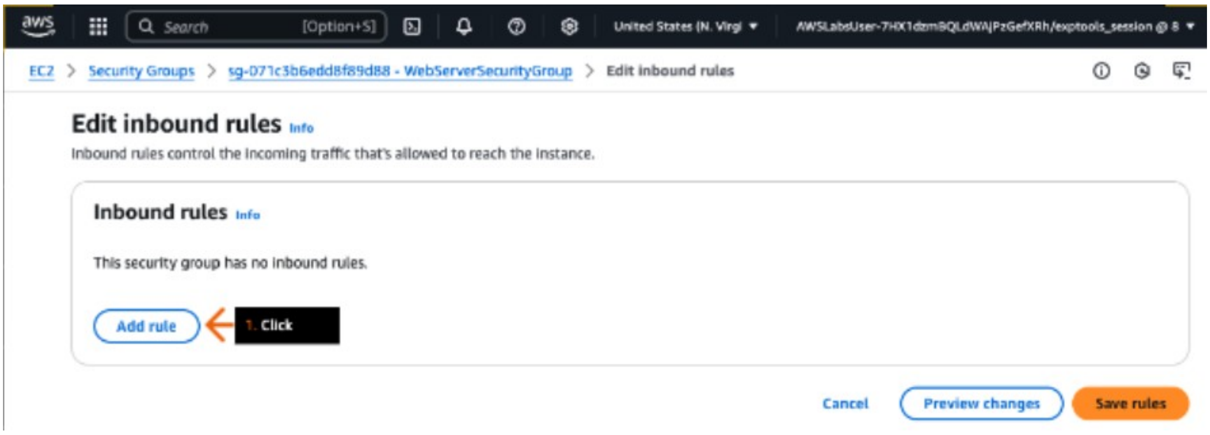
Name	Security group rule ID	IP version	Type

No security group rules found

For each security group, you can add rules that control the traffic based on protocols and port numbers. Separate sets of rules exist for inbound traffic and outbound traffic.

When you create a VPC, it comes with a default security group. You can create additional security groups for each VPC.

- Click Add rule.


Search [Option+S]
United States (N. Virgi ▾
AWSLabsUser-7HX1dzmBQLdWAjPzGefXRh/exptools_session @ 8 ▾
EC2 > Security Groups > sg-071c3b6edd8f89d88 - WebServerSecurityGroup > Edit inbound rules
Info
Add rule
1. Click
Cancel
Preview changes
Save rules

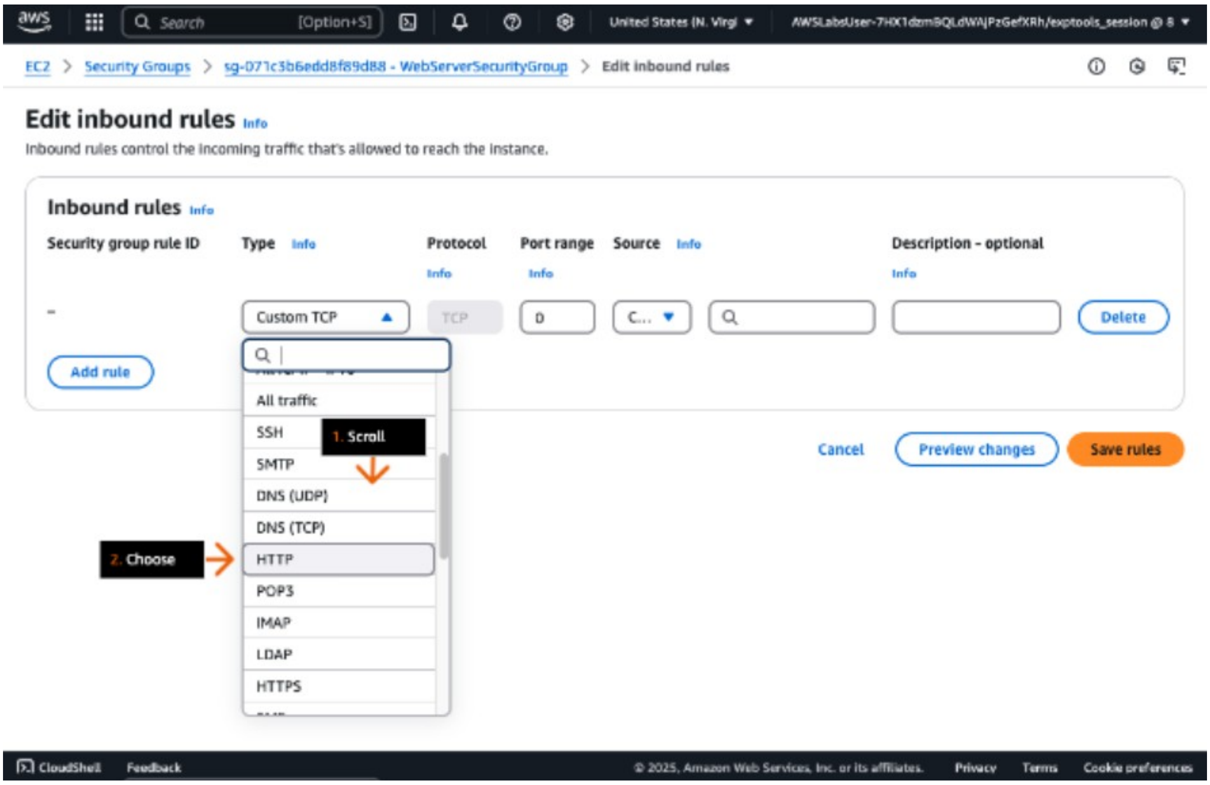
Edit inbound rules

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules

This security group has no inbound rules.

- For Type, on the dropdown list, scroll down to see the various available predefined protocols.
- Choose HTTP.
    - Make sure you did not choose HTTPS.



EC2 > Security Groups > sg-071c3b6edd8f89d88 - WebServerSecurityGroup > Edit inbound rules

Edit inbound rules Info

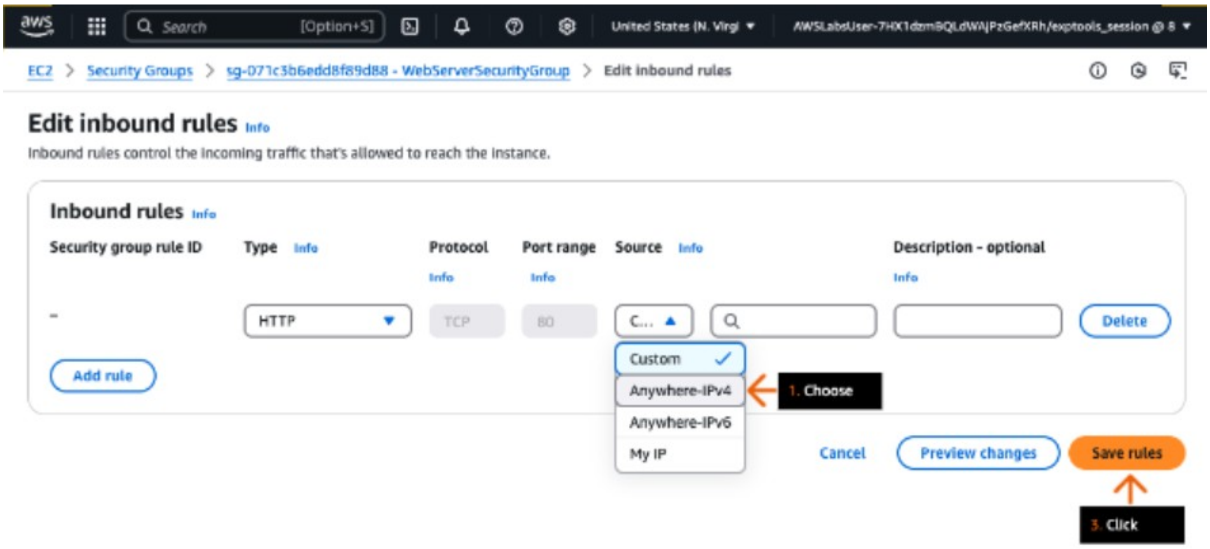
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
-	Custom TCP	TCP	0	C...	

You can create a security group and add rules that reflect the role of the instance that is associated with the security group. For example, an instance that is configured as a web server needs security group rules that allow inbound HTTP and HTTPS access. Likewise, a database instance needs rules that allow access for the type of database, such as access over port 3306 for MySQL.

- For Source, choose Anywhere-IPv4.
- In the warning alert, review the recommended setting.
- Click Save rules.



EC2 > Security Groups > sg-071c3b6edd8f89d88 - WebServerSecurityGroup > Edit inbound rules

Edit inbound rules Info

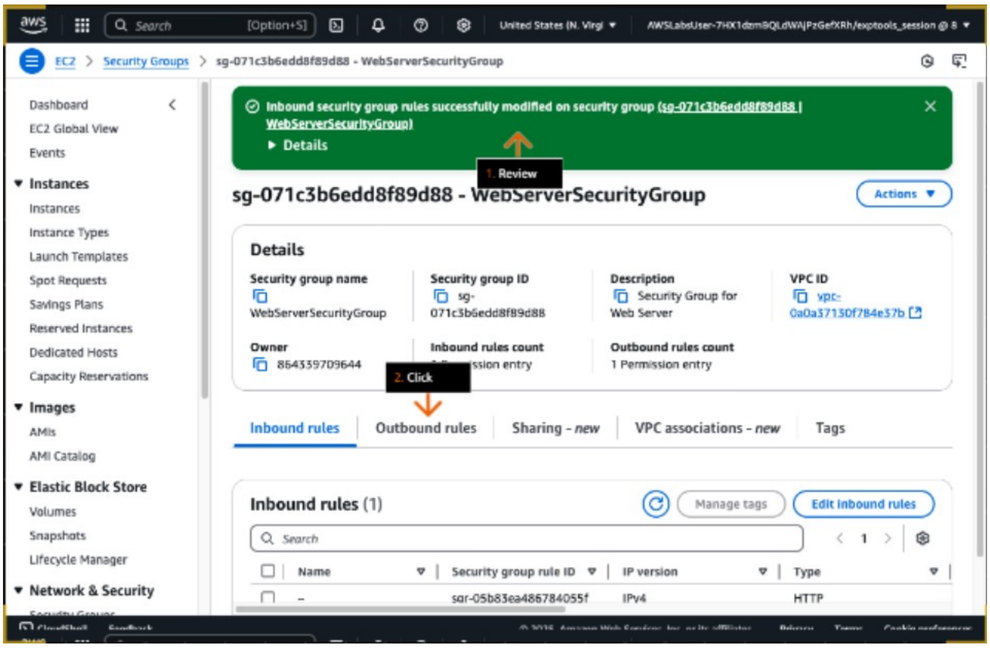
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
-	HTTP	TCP	80	C...	

Security groups are stateful, meaning they retain information about their interactions over time. For example, if you send a request from an instance, the response traffic for that request is allowed to reach the instance regardless of the inbound security group rules. Responses to allowed inbound traffic are allowed to leave the instance, regardless of the outbound rules.

- In the success alert, review the message.
- In the tab ribbon, click Outbound rules.



Inbound security group rules successfully modified on security group (sg-071c3b6edd8f89d88 | WebServerSecurityGroup)

▶ Details

sg-071c3b6edd8f89d88 - WebServerSecurityGroup

Details

Security group name: WebServerSecurityGroup

Security group ID: sg-071c3b6edd8f89d88

Description: Security Group for Web Server

VPC ID: vpc-0a0a37130f784e37b

Owner: 864339709644

Inbound rules count: 1 Permission entry

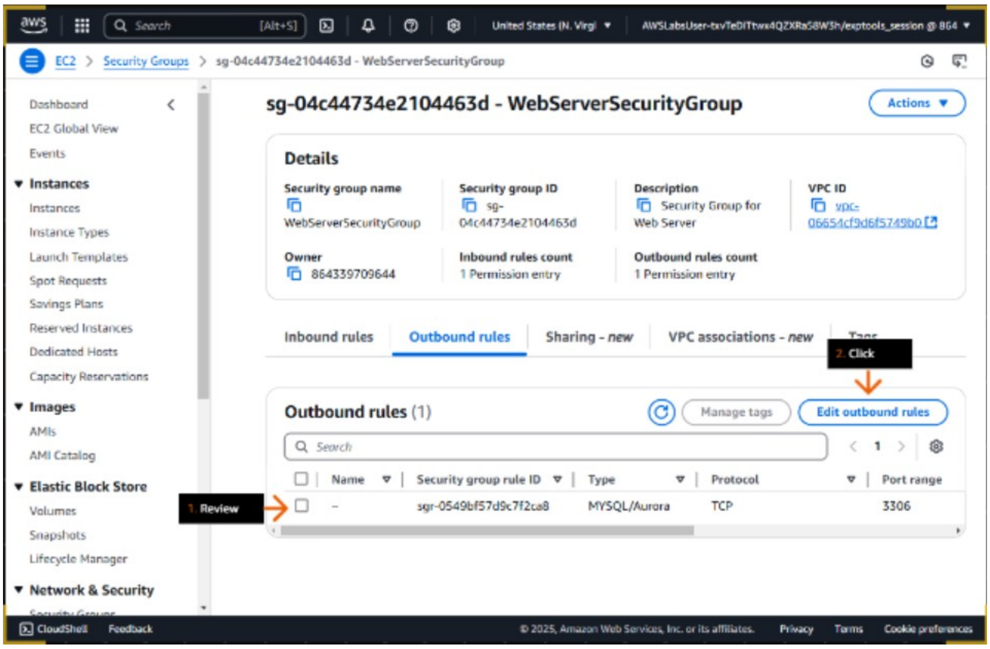
Outbound rules count: 1 Permission entry

Inbound rules (1)

	Name	Security group rule ID	IP version	Type
□	–	sgr-05b83ea486784055f	IPv4	HTTP

For better security, you should only allow incoming connections from specific network addresses (like certain computers or your office network), instead of allowing connections from anywhere on the internet.

- Review that an existing outbound rule exist allowing traffic on port 3306
  - o 3306 is the default port used by MySQL database server.
- Click Edit outbound rules.



sg-04c44734e2104463d - WebServerSecurityGroup

Details

Security group name: WebServerSecurityGroup

Security group ID: sg-04c44734e2104463d

Description: Security Group for Web Server

VPC ID: vpc-06654cf9d6f57490b0

Owner: 864339709644

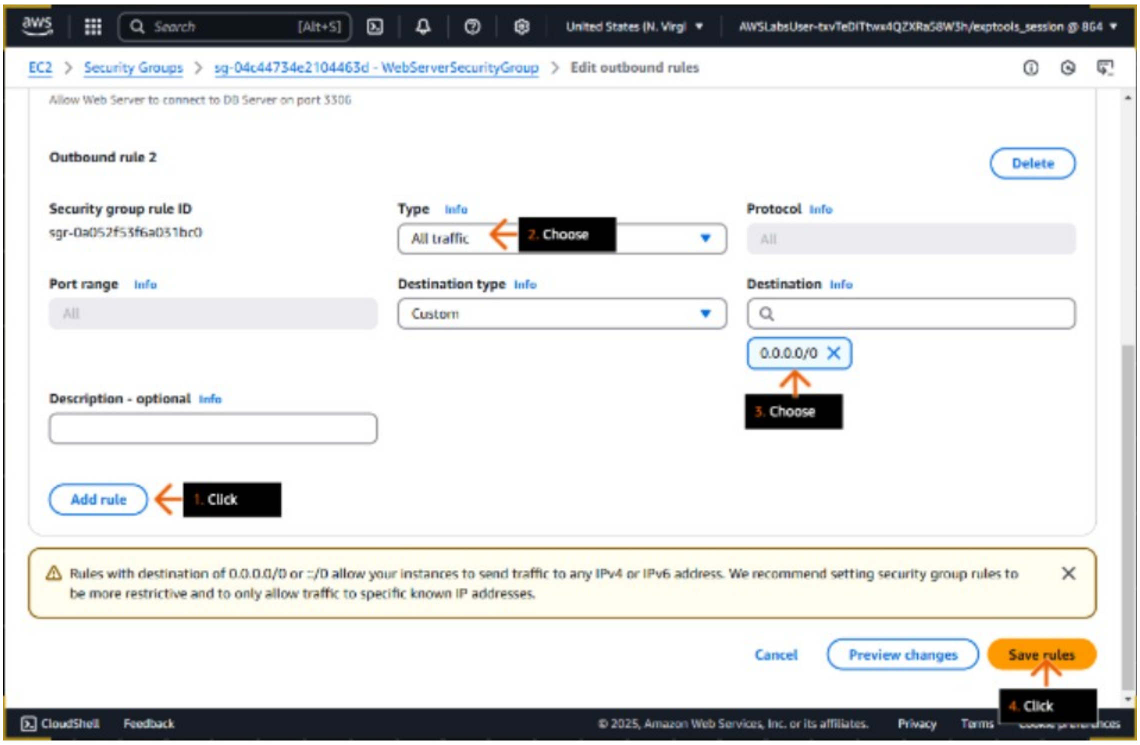
Inbound rules count: 1 Permission entry

Outbound rules count: 1 Permission entry

Outbound rules (1)

	Name	Security group rule ID	Type	Protocol	Port range
□	–	sgr-0549bf57d9c7f2ca8	MYSQL/Aurora	TCP	3306

- Click Add rule.
- For Type, use the dropdown to choose All traffic.
- For Destination, use the dropdown to choose the CIDR range 0.0.0.0/0.
- Click Save rules.



EC2 > Security Groups > sg-04c44734e2104463d - WebServerSecurityGroup > Edit outbound rules

Allow Web Server to connect to DB Server on port 3306

Outbound rule 2

Security group rule ID: sgr-0a052f53f6a031bc0

Type: All traffic

Protocol: All

Port range: All

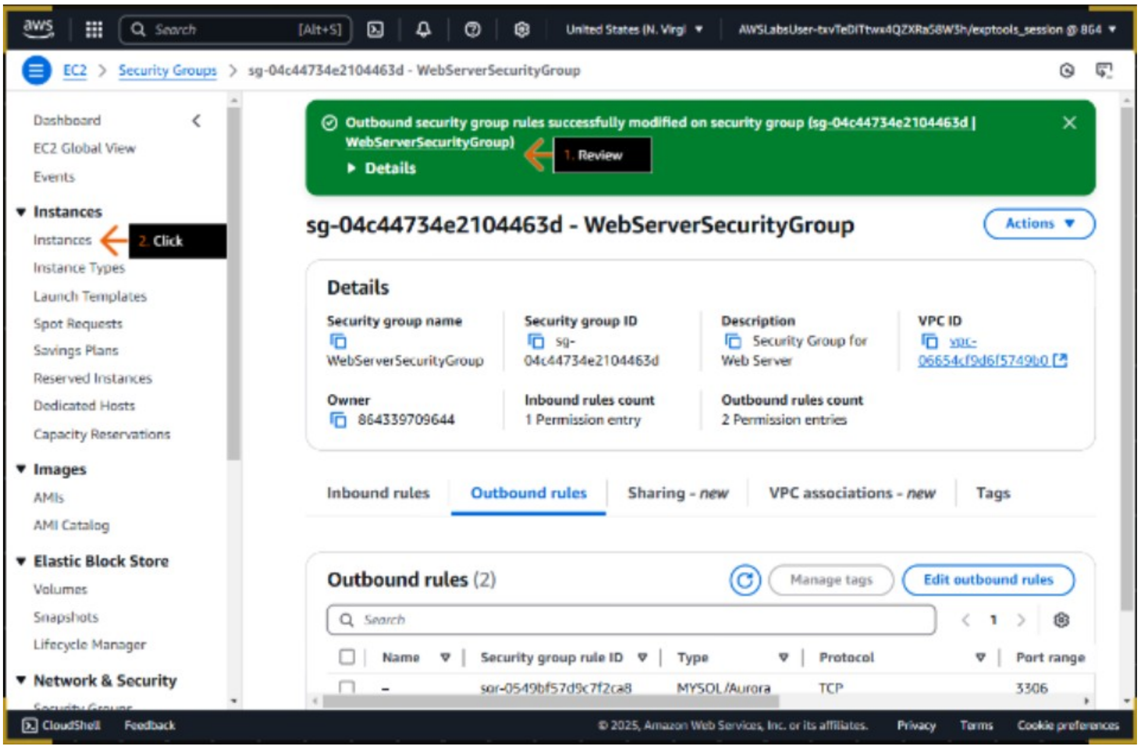
Destination type: Custom

Destination: 0.0.0.0/0

Description - optional:

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.

- Review that the Outbound security group rules were updated successfully.
- In the left navigation pane, click Instances.



EC2 > Security Groups > sg-04c44734e2104463d - WebServerSecurityGroup

Outbound security group rules successfully modified on security group (sg-04c44734e2104463d | WebServerSecurityGroup)

sg-04c44734e2104463d - WebServerSecurityGroup

Details

Security group name: WebServerSecurityGroup

Security group ID: sg-04c44734e2104463d

Description: Security Group for Web Server

VPC ID: vpc-06654cf9d6f5749b0

Owner: 864339709644

Inbound rules count: 1 Permission entry

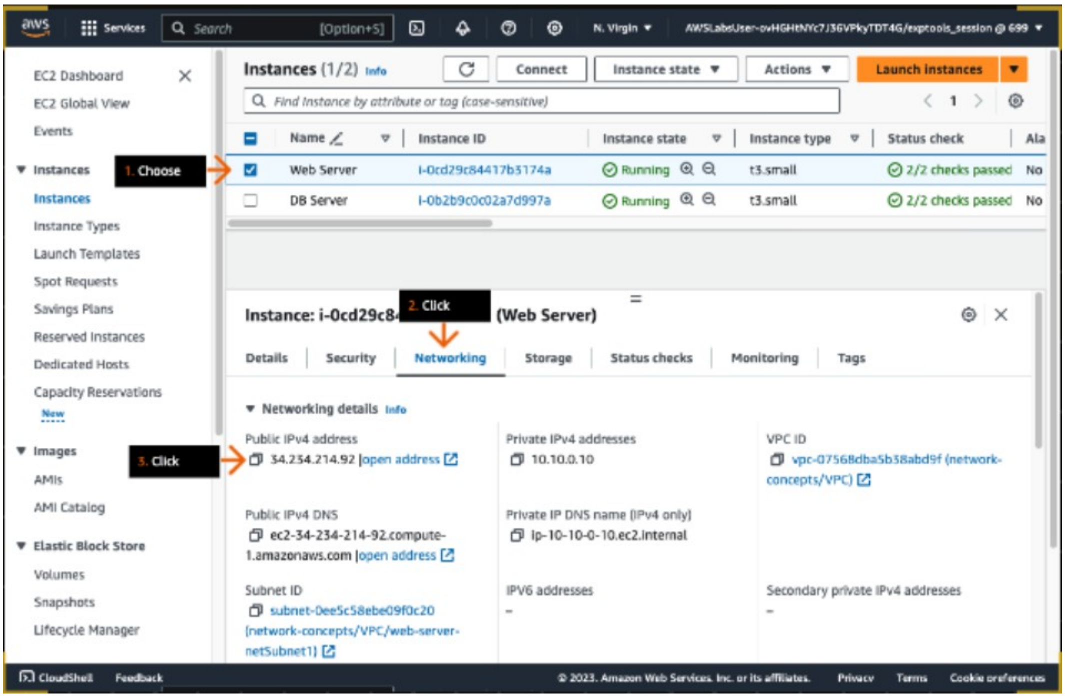
Outbound rules count: 2 Permission entries

Outbound rules (2)

Name	Security group rule ID	Type	Protocol	Port range
–	sgr-0549bf57d5c7f2ca8	MYSQL/Aurora	TCP	3306

- In the Instances section, choose the check box to select the Web Server instance.

- Click the Networking tab.
- Under Public IPv4 address, click the copy icon to copy the provided address.
    - Do not click open address or the page will not load.



1. Choose
2. Click
3. Click

Instances (1/2)

	Name	Instance ID	Instance state	Instance type	Status check	Ala
☑	Web Server	i-0cd29c84417b5174a	Running	t3.small	2/2 checks passed	No
□	DB Server	i-0b2b9c0c02a7d997a	Running	t3.small	2/2 checks passed	No

Instance: i-0cd29c84… (Web Server)

Networking details

Public IPv4 address: 34.234.214.92 | open address

Private IPv4 addresses: 10.10.0.10

VPC ID: vpc-07568dba5b38abd9f (network-concepts/VPC)

Public IPv4 DNS: ec2-34-234-214-92.compute-1.amazonaws.com | open address

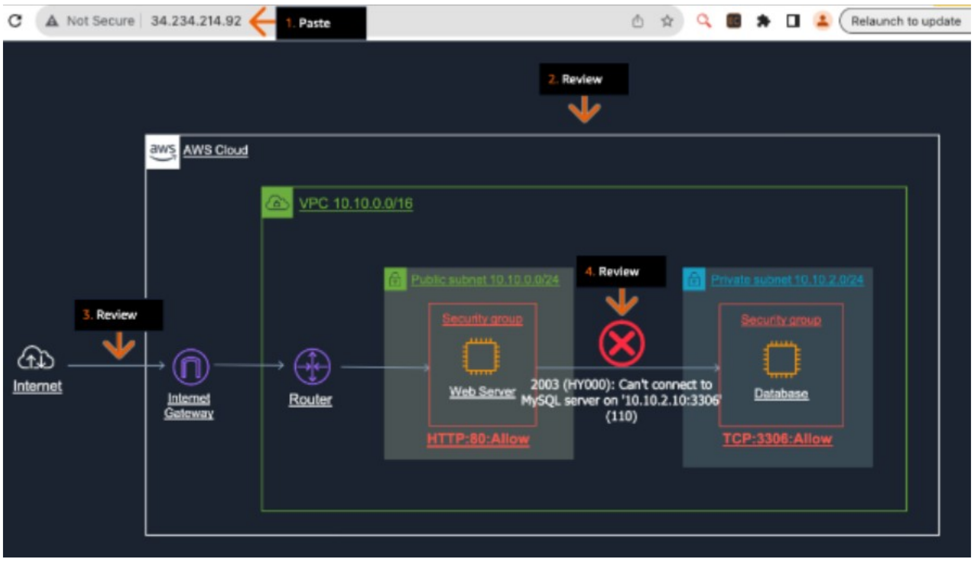
Private IP DNS name (IPv4 only): ip-10-10-0-10.ec2.internal

Subnet ID: subnet-0ee5c58ebe09f0c20 (network-concepts/VPC/web-server-netSubnet1)

IPV6 addresses: –

Secondary private IPv4 addresses: –

- In a new browser tab (or window) address bar, paste the instance IP address that you just copied and press Enter.
    - Make sure you use HTTP, not HTTPS.
    - The address should look similar to this: http://xxx.xxx.xxx.xxx
- Review the diagram that loads from the public IP address.
- Review the connection from the internet to the web server.
    - A connection should be established.
- Review the connection from the web server to the database (DB server).
    - The connection should display as failed.



1. Paste
2. Review
3. Review
4. Review

2003 (HY000): Can't connect to MySQL server on '10.10.2.10:3306' (110)

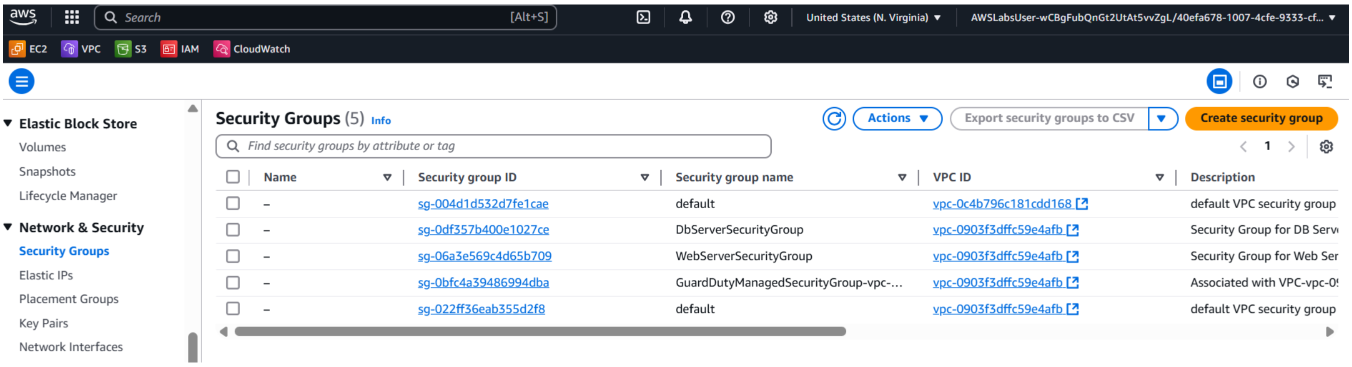
To deploy a working internet gateway, the following must be completed:

- The internet gateway must be attached to a VPC.
- Route tables associated with your public subnet must have a route to your internet gateway.
- Security groups associated with your VPC must allow traffic to/from the internet.
- Any instances in the VPC must have a public IP or Elastic IP address assigned.

To enable communication between the web server and the DB server, you need to modify the security group associated with the DB server (`DbServerSecurityGroup`) to allow incoming traffic on the necessary port from the web server's security group (`WebServerSecurityGroup`).

Steps to Update Security Group Rules:

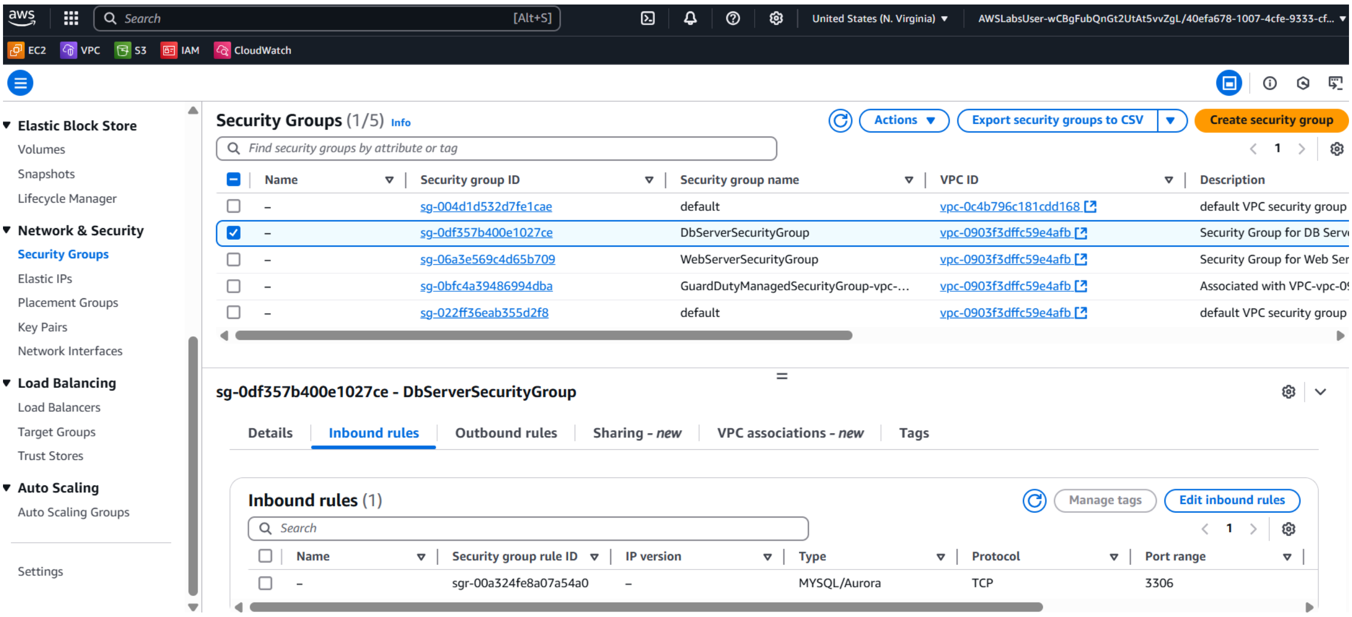
- Navigate to the EC2 console and select **Security Groups**.



Security Groups (5) Info

□	Name	Security group ID	Security group name	VPC ID	Description
□	–	sg-004d1d532d7fe1cae	default	vpc-0c4b796c181cdd168	default VPC security group
□	–	sg-0df357b400e1027ce	DbServerSecurityGroup	vpc-0903f3dffc59e4afb	Security Group for DB Serv
□	–	sg-06a3e569c4d65b709	WebServerSecurityGroup	vpc-0903f3dffc59e4afb	Security Group for Web Ser
□	–	sg-0bfc4a39486994dba	GuardDutyManagedSecurityGroup-vpc-…	vpc-0903f3dffc59e4afb	Associated with VPC-vpc-0
□	–	sg-022ff36eab355d2f8	default	vpc-0903f3dffc59e4afb	default VPC security group

- Locate and select the security group associated with your DB server (e.g., `DbServerSecurityGroup`).
- Find the option to edit **Inbound rules**.



Security Groups (1/5) Info

☐	Name	Security group ID	Security group name	VPC ID	Description
□	–	sg-004d1d532d7fe1cae	default	vpc-0c4b796c181cdd168	default VPC security group
☑	–	sg-0df357b400e1027ce	DbServerSecurityGroup	vpc-0903f3dffc59e4afb	Security Group for DB Serv
□	–	sg-06a3e569c4d65b709	WebServerSecurityGroup	vpc-0903f3dffc59e4afb	Security Group for Web Ser
□	–	sg-0bfc4a39486994dba	GuardDutyManagedSecurityGroup-vpc-…	vpc-0903f3dffc59e4afb	Associated with VPC-vpc-0
□	–	sg-022ff36eab355d2f8	default	vpc-0903f3dffc59e4afb	default VPC security group

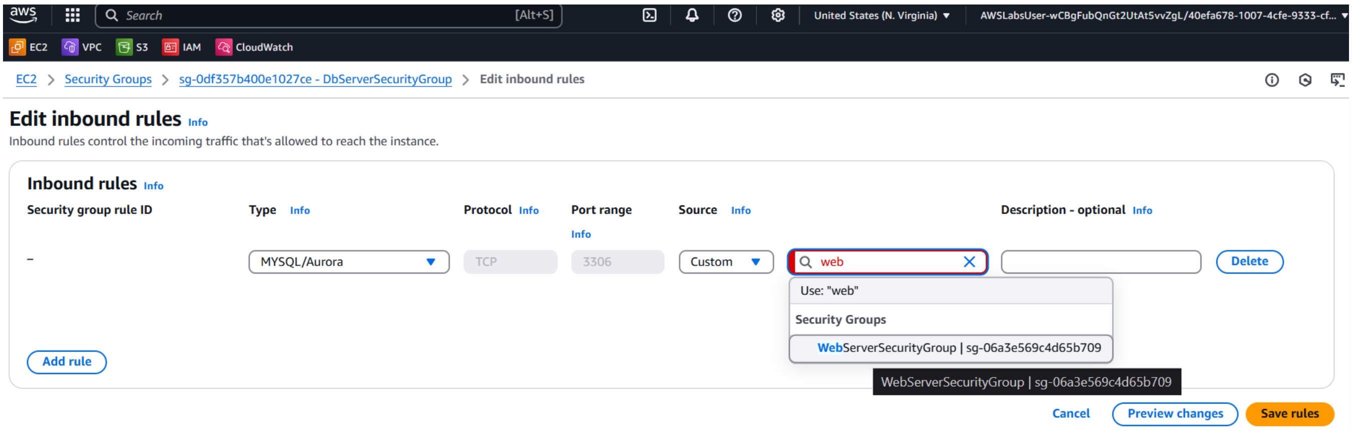
sg-0df357b400e1027ce - DbServerSecurityGroup

Inbound rules (1)

□	Name	Security group rule ID	IP version	Type	Protocol	Port range
□	–	sgr-00a324fe8a07a54a0	–	MYSQL/Aurora	TCP	3306

- Add a new **Inbound Rule** with the following settings:

- **Type:** Select the appropriate database type (e.g., `MySQL/Aurora`). This will automatically populate the protocol and port range.
- **Protocol:** Ensure **TCP** is selected.
- **Port Range:** Ensure **3306** is specified.
- **Source:** Here, instead of specifying IP addresses, select the security group associated with your web server (e.g., `WebServerSecurityGroup`). This allows any instance in the web server's security group to connect to the DB server on port 3306.



aws Search [Alt+S] United States (N. Virginia) ▼ AWSLabsUser-wCBgFubQnGt2UtAt5vvZgL/40efa678-1007-4cfe-9333-cf... ▼

EC2 VPC S3 IAM CloudWatch

EC2 > Security Groups > sg-0df357b400e1027ce - DbServerSecurityGroup > 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	
–	MYSQL/Aurora ▼	TCP	3306	Custom ▼	web ✕		Delete

Use: "web"

Security Groups

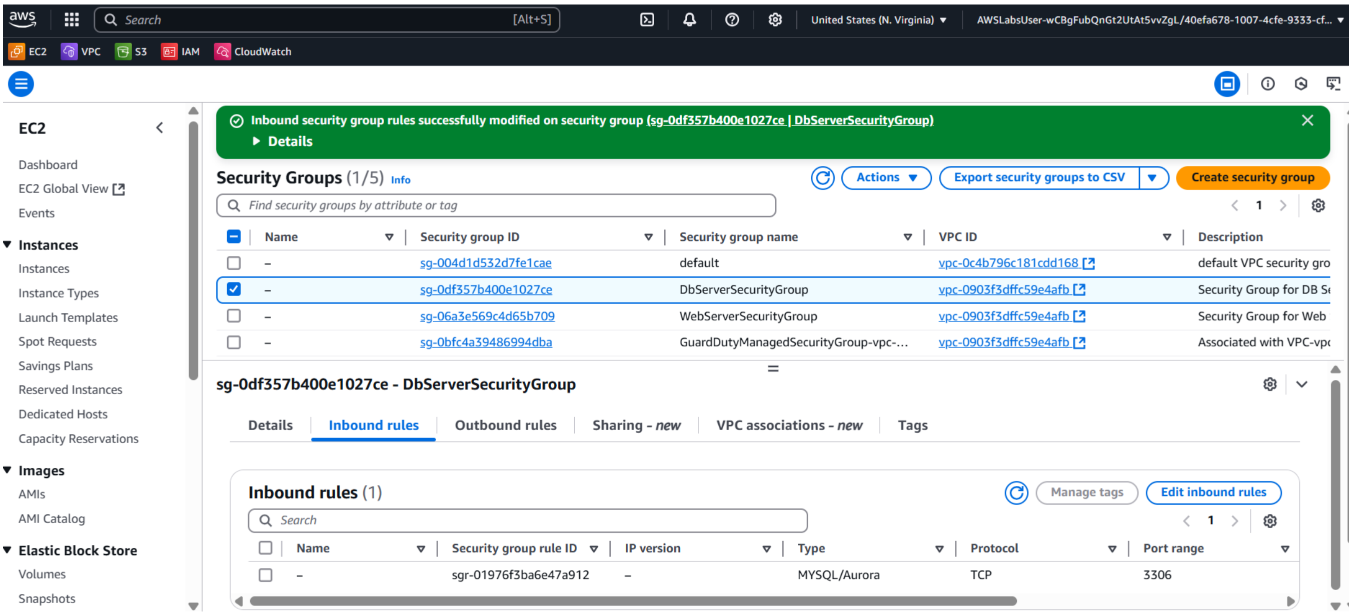
WebServerSecurityGroup | sg-06a3e569c4d65b709

WebServerSecurityGroup | sg-06a3e569c4d65b709

Add rule

Cancel Preview changes Save rules

- Save the updated inbound rules.
- A confirmation message, such as "Inbound security group rules successfully modified on security group (DbServerSecurityGroup)," indicating that your rule changes have been saved.



aws Search [Alt+S] United States (N. Virginia) ▼ AWSLabsUser-wCBgFubQnGt2UtAt5vvZgL/40efa678-1007-4cfe-9333-cf... ▼

EC2 VPC S3 IAM CloudWatch

EC2

Dashboard
EC2 Global View
Events

▼ Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations

▼ Images
AMIs
AMI Catalog

▼ Elastic Block Store
Volumes
Snapshots

Inbound security group rules successfully modified on security group (sg-0df357b400e1027ce | DbServerSecurityGroup) ✕

▶ Details

Security Groups (1/5) Info

Actions ▼ Export security groups to CSV ▼ Create security group

Find security groups by attribute or tag

	Name	Security group ID	Security group name	VPC ID	Description
□	–	sg-004d1d532d7fe1cae	default	vpc-0c4b796c181cdd168	default VPC security gro
☑	–	sg-0df357b400e1027ce	DbServerSecurityGroup	vpc-0903f3dffc59e4afb	Security Group for DB S
□	–	sg-06a3e569c4d65b709	WebServerSecurityGroup	vpc-0903f3dffc59e4afb	Security Group for Web
□	–	sg-0bfc4a39486994dba	GuardDutyManagedSecurityGroup-vpc-...	vpc-0903f3dffc59e4afb	Associated with VPC-vpc

sg-0df357b400e1027ce - DbServerSecurityGroup

Details | Inbound rules | Outbound rules | Sharing - new | VPC associations - new | Tags

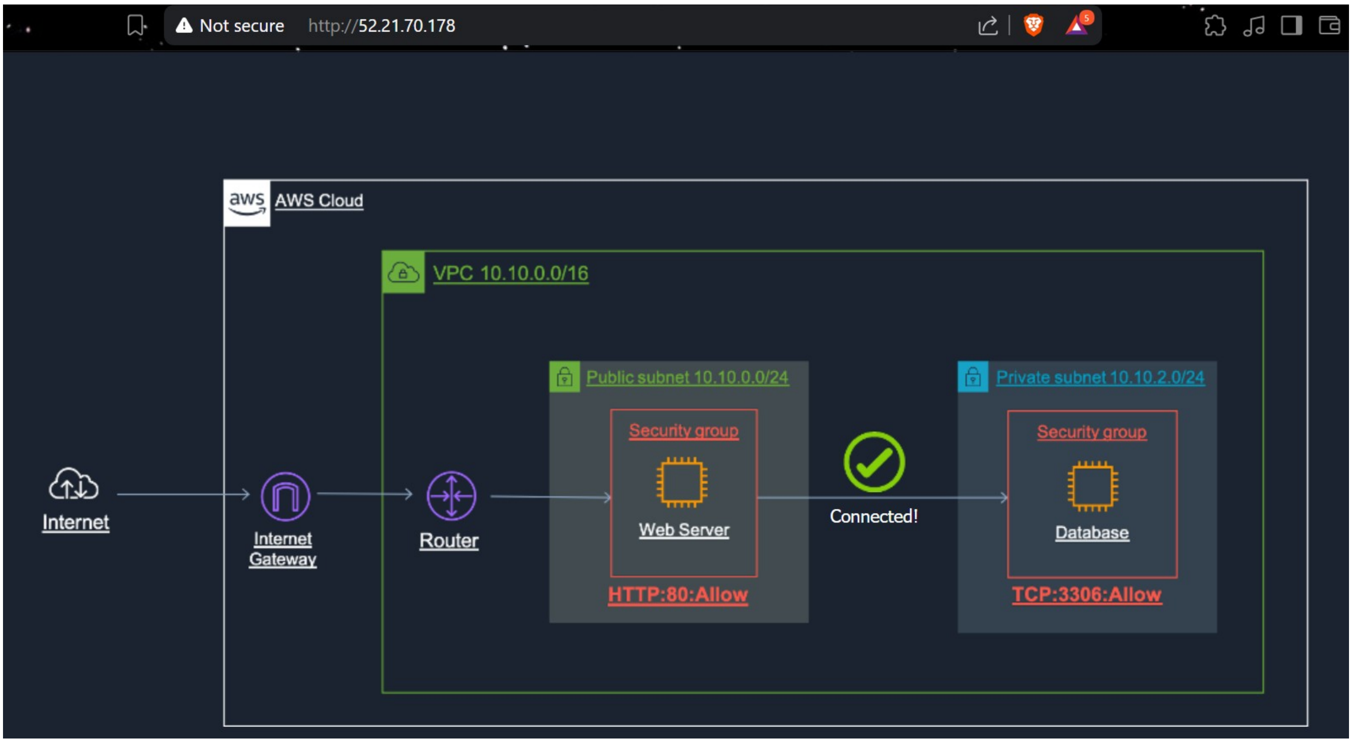
Inbound rules (1)

Manage tags Edit inbound rules

Search

	Name	Security group rule ID	IP version	Type	Protocol	Port range
□	–	sgr-01976f3ba6e47a912	–	MYSQL/Aurora	TCP	3306

- After updating the security group rules, review the network diagram or the connection status indicator in your lab environment.
- Allow a short moment for the rule changes to take effect.
- Confirm that the status between the Web server and the DB server in the diagram changes to **Connected**, visually confirming that the necessary traffic on port 3306 is now allowed.



Conclusion:

Upon achieving the outlined objectives, you have successfully explored the fundamental components of a Virtual Private Cloud (VPC). This includes gaining proficiency in configuring route tables attached to subnets to manage network traffic flow, specifically directing internet-bound traffic via an internet gateway. Furthermore, you have demonstrated the ability to configure inbound rules within a security group, effectively controlling access to resources within the VPC.