

AWS Secure Network

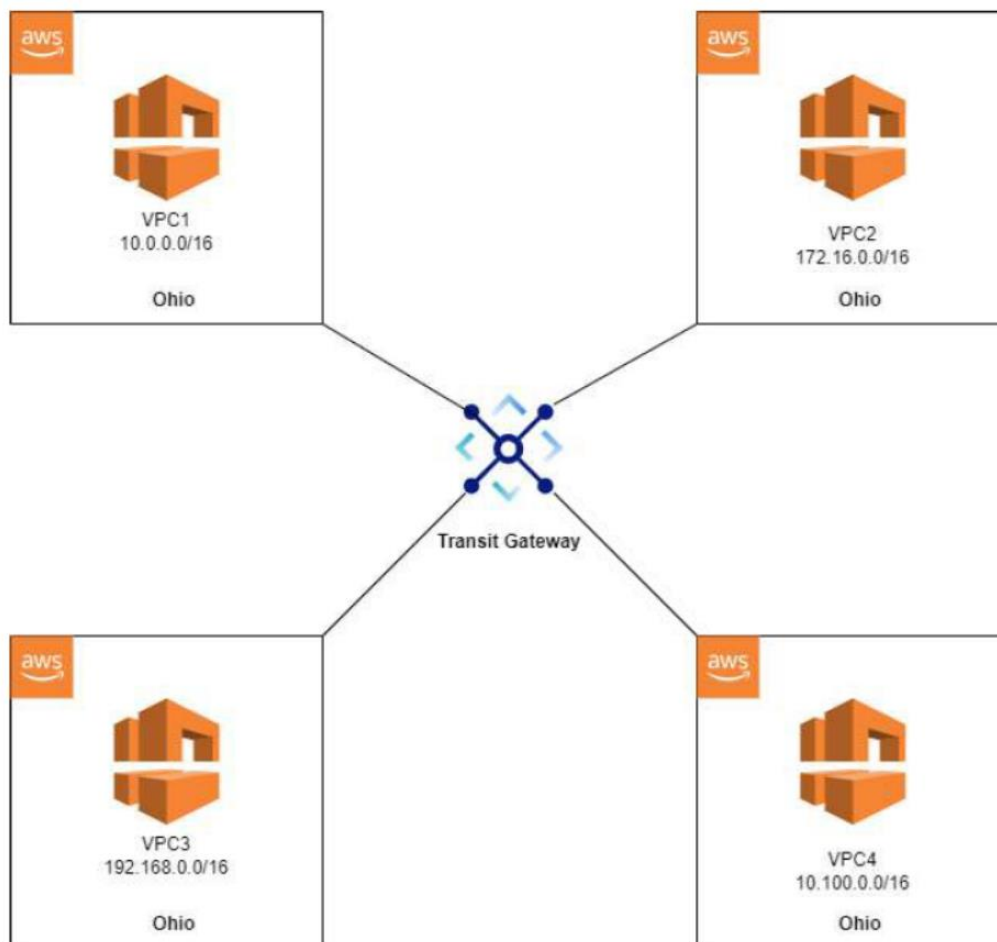


Table of Contents

I. Proposed Architecture	3
II. Security Groups	9
III. Identity and Access Management (IAM).....	14
IV. Remote Access to the instances.....	17
V. Security Hardening.....	20

The primary objective of this project is to develop a secure cloud network design that effectively mitigates the risks associated with unauthorized access, data breaches, and network vulnerabilities. By implementing industry best practices and leveraging state-of-the-art security technologies, this project aims to establish a robust security framework that ensures the confidentiality, integrity, and availability of data stored and transmitted within the cloud infrastructure of a small business.

I. Proposed Architecture



Here is our Network topology with 4 VPCs located in Ohio, each VPC is a different Network. A transit gateway interconnects all the VPCs.

- **VPC1: 10.0.0.0/16**
- **VPC2: 172.16.0.0/16**
- **VPC3: 192.168.0.0/16**
- **VPC4: 10.100.0.0/16**

us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#vpcs

Services Search [Alt+S]

VPC dashboard X

EC2 Global View New

Filter by VPC: Select a VPC

Virtual private cloud

Your VPCs [New](#)

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

Network ACLs

Security groups

Your VPCs (5) Info

Filter VPCs

Actions Create VPC

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP
<input type="checkbox"/>	VPC1	vpc-0abc2cec959abae7c	Available	10.0.0.0/16	-	dopt-0
<input type="checkbox"/>	VPC4	vpc-04a5e822cace94922	Available	10.100.0.0/16	-	dopt-0
<input type="checkbox"/>	VPC3	vpc-0bd6380f80786f536	Available	192.168.0.0/16	-	dopt-0
<input type="checkbox"/>	VPC2	vpc-0aafd337ceaf939dc	Available	172.16.0.0/16	-	dopt-0
<input type="checkbox"/>	-	vpc-0c91858b2a7120a02	Available	172.31.0.0/16	-	dopt-0

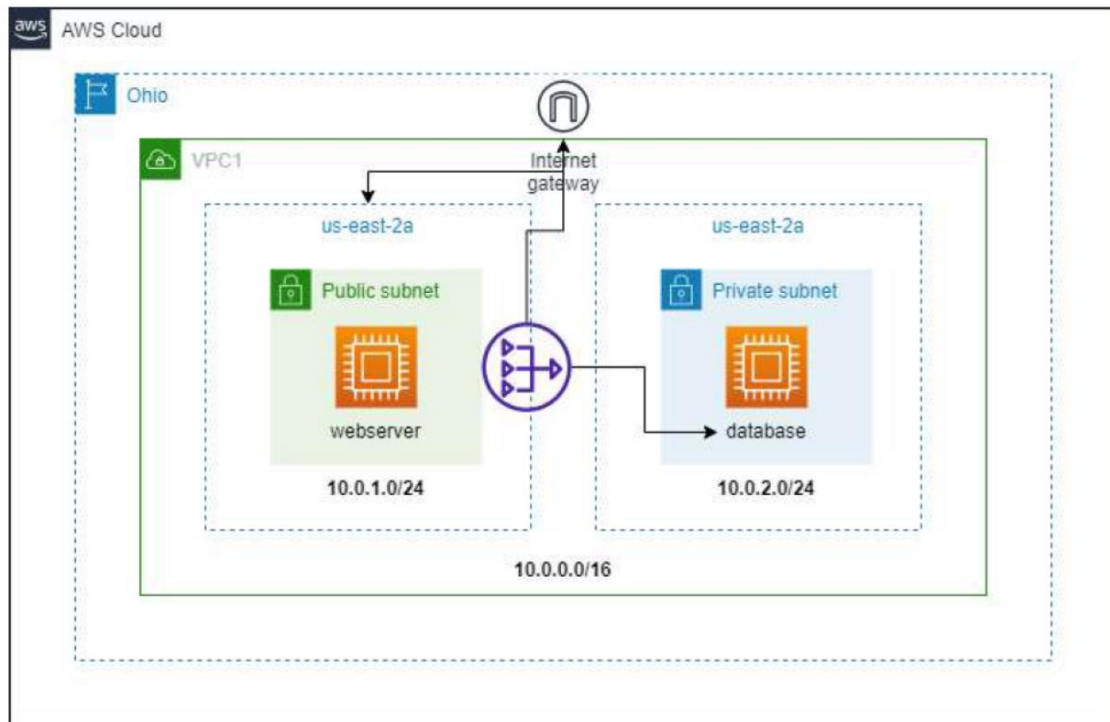
Select a VPC above

CloudShell Feedback Language

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Each VPC has purposes and objectives based on the business's needs and requirements.

VPC1 Diagram



The VPC1 have 2 subnets in the same availability zone which is **us-east-2a**.

Subnets (2/11) info

	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>	Private-VPC2	subnet-0f8ce5490ebbf04d	Available	vpc-0aafd337ceaf939dc VPC2	172.16.2.0/24	-
<input type="checkbox"/>	-	subnet-0b211cbb6c2e1746	Available	vpc-0c91858b2a7120a02	172.31.16.0/20	-
<input type="checkbox"/>	Private-VPC4	subnet-0ac6365a2fb052c2d	Available	vpc-04a5e822cace94922 VPC4	10.100.2.0/24	-
<input type="checkbox"/>	Public-VPC4	subnet-0acf3fc5b5b66c172	Available	vpc-04a5e822cace94922 VPC4	10.100.1.0/24	-
<input type="checkbox"/>	-	subnet-00564db393f8f2e74	Available	vpc-0c91858b2a7120a02	172.31.32.0/20	-
<input type="checkbox"/>	Public-VPC3	subnet-03f10cc106146fd75	Available	vpc-0bd6380f80786f536 VPC3	192.168.1.0/24	-
<input type="checkbox"/>	-	subnet-0ecd8e49c658be91a	Available	vpc-0c91858b2a7120a02	172.31.0.0/20	-
<input type="checkbox"/>	Public-VPC2	subnet-0ca75374b1545cc73	Available	vpc-0aafd337ceaf939dc VPC2	172.16.1.0/24	-
<input checked="" type="checkbox"/>	Public-VPC1	subnet-0844964fff95bb971	Available	vpc-0abc2cec959abae7c VPC1	10.0.1.0/24	-
<input checked="" type="checkbox"/>	Private-VPC1	subnet-039b4d78b56bd5438	Available	vpc-0abc2cec959abae7c VPC1	10.0.2.0/24	-
<input type="checkbox"/>	Private-VPC3	subnet-08f1837e55030027d	Available	vpc-0bd6380f80786f536 VPC3	192.168.2.0/24	-

Subnets: subnet-039b4d78b56bd5438, subnet-0844964fff95bb971

- **Public subnet: 10.0.1.0/24**

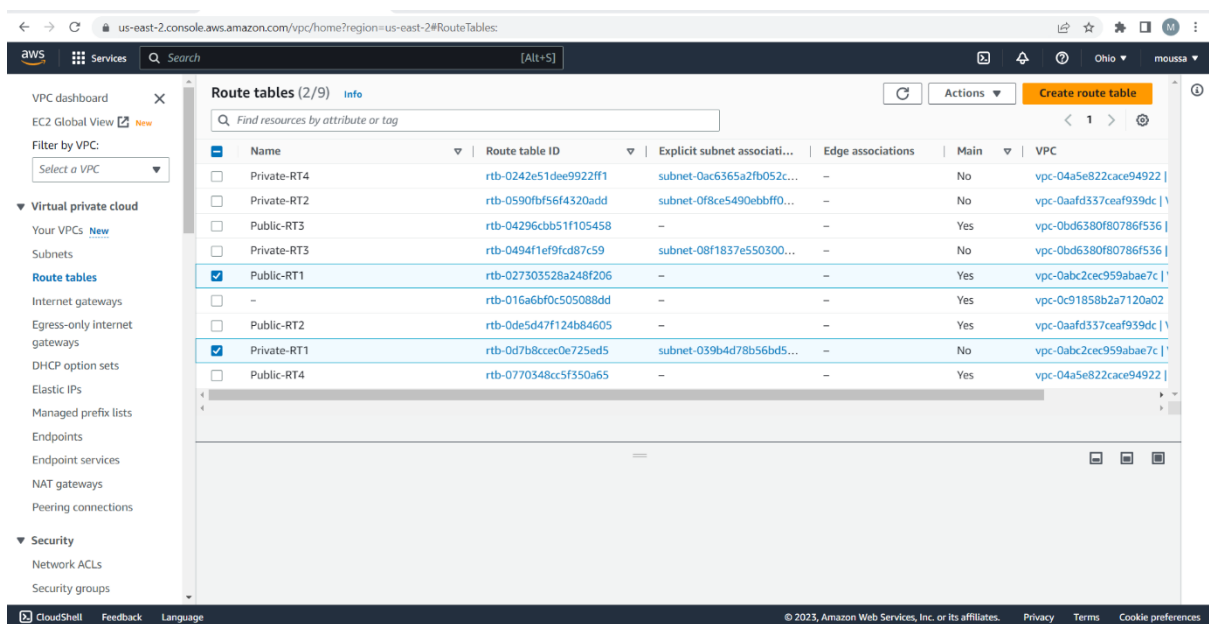
The public subnet contains an EC2 instance that we consider as a web server, the internet gateway enables this instance to have access to the internet and people from the internet access the instance. This makes instances in the public subnet expose to cyber threat.

- **Private subnet: 10.0.2.0/24**

The private subnet contains an EC2 instance that we consider as a database. The instances in the private subnet are not accessible from the internet that is why it is more secure than the public subnet. However, the instance in the private subnet might need to access to the internet. This will be possible by using the NAT gateway that is in the public subnet, so the private instance will be routed to the internet gateway and access the internet.

We will isolate the others VPC for future purposes.

- **VPC1 route tables:** VPC1 have two route table **Public-RT1** for the public subnet and **Private-RT1** the private subnet.



The screenshot shows the AWS Management Console interface for the 'Route tables (2/9)' page. The left sidebar contains navigation links for VPC dashboard, EC2 Global View, and various VPC resources. The main content area displays a table of route tables. The table has columns for Name, Route table ID, Explicit subnet associations, Edge associations, Main status, and VPC. Two route tables are selected: 'Public-RT1' (rtb-027303528a248f206) and 'Private-RT1' (rtb-0d7b8ccce0e725ed5). Both are associated with VPC 'vpc-04a5e822cace94922'.

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
<input type="checkbox"/> Private-RT4	rtb-0242e51dee9922ff1	subnet-0ac6365a2fb052c...	-	No	vpc-04a5e822cace94922
<input type="checkbox"/> Private-RT2	rtb-0590fbf56f4320add	subnet-0f8ce5490ebbf0...	-	No	vpc-0aafd337ceaf939dc
<input type="checkbox"/> Public-RT3	rtb-04296cbb51f105458	-	-	Yes	vpc-0bd6380f80786f536
<input type="checkbox"/> Private-RT3	rtb-0494f1ef9fcd87c59	subnet-08f1837e550300...	-	No	vpc-0bd6380f80786f536
<input checked="" type="checkbox"/> Public-RT1	rtb-027303528a248f206	-	-	Yes	vpc-04a5e822cace94922
<input type="checkbox"/> -	rtb-016a6bf0c505088dd	-	-	Yes	vpc-0c91858b2a7120a02
<input type="checkbox"/> Public-RT2	rtb-0de5d47f124b84605	-	-	Yes	vpc-0aafd337ceaf939dc
<input checked="" type="checkbox"/> Private-RT1	rtb-0d7b8ccce0e725ed5	subnet-039b4d78b56bd5...	-	No	vpc-04a5e822cace94922
<input type="checkbox"/> Public-RT4	rtb-0770348ccf350a65	-	-	Yes	vpc-04a5e822cace94922

Public-RT1

The screenshot shows the AWS Management Console for the us-east-2 region, specifically the Route Tables page. The left sidebar shows the VPC dashboard with options for VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, and Peering connections. The main content area displays a list of route tables for the selected VPC (vpc-04a5e822cace94922). The table has columns for Name, Route table ID, Explicit subnet associations, Edge associations, Main, and VPC. The route table Public-RT1 (rtb-027303528a248f206) is selected. Below the table, the routes for Public-RT1 are shown in a table with columns for Destination, Target, Status, and Propagated.

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
Private-RT4	rtb-0242e51dee9922ff1	subnet-0ac6365a2fb052c...	-	No	vpc-04a5e822cace94922
Private-RT2	rtb-0590fbf56f4320add	subnet-0f8ce5490ebbff0...	-	No	vpc-0aafd337ceaf939dc
Public-RT3	rtb-04296cbb51f105458	-	-	Yes	vpc-0bd6380f80786f536
Private-RT3	rtb-0494f1ef9fcd87c59	subnet-08f1837e550300...	-	No	vpc-0bd6380f80786f536
Public-RT1	rtb-027303528a248f206	-	-	Yes	vpc-0abc2cec959abae7c
-	rtb-016a6bf0c505088dd	-	-	Yes	vpc-0c91858b2a7120a02
Public-RT2	rtb-0de5d47f124b84605	-	-	Yes	vpc-0aafd337ceaf939dc
Private-RT1	rtb-0d7b8ccce0e725ed5	subnet-039b4d78b56bd5...	-	No	vpc-0abc2cec959abae7c
Public-RT4	rtb-0770348cc5f350a65	-	-	Yes	vpc-04a5e822cace94922

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0adbea8dfc0bda2c7	Active	No
10.0.0.0/16	local	Active	No

Public-RT1 have a route for communication within the VPC and a route to the internet thanks to the internet gateway. The public subnet can access to the internet and from the internet we can access the public subnet.

Private-RT1

The screenshot shows the AWS Management Console for the us-east-2 region, specifically the Route Tables page. The left sidebar shows the VPC dashboard with options for VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, and Peering connections. The main content area displays a list of route tables for the selected VPC (vpc-04a5e822cace94922). The table has columns for Name, Route table ID, Explicit subnet associations, Edge associations, Main, and VPC. The route table Private-RT1 (rtb-0d7b8ccce0e725ed5) is selected. Below the table, the routes for Private-RT1 are shown in a table with columns for Destination, Target, Status, and Propagated.

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
Private-RT4	rtb-0242e51dee9922ff1	subnet-0ac6365a2fb052c...	-	No	vpc-04a5e822cace94922
Private-RT2	rtb-0590fbf56f4320add	subnet-0f8ce5490ebbff0...	-	No	vpc-0aafd337ceaf939dc
Public-RT3	rtb-04296cbb51f105458	-	-	Yes	vpc-0bd6380f80786f536
Private-RT3	rtb-0494f1ef9fcd87c59	subnet-08f1837e550300...	-	No	vpc-0bd6380f80786f536
Public-RT1	rtb-027303528a248f206	-	-	Yes	vpc-0abc2cec959abae7c
-	rtb-016a6bf0c505088dd	-	-	Yes	vpc-0c91858b2a7120a02
Public-RT2	rtb-0de5d47f124b84605	-	-	Yes	vpc-0aafd337ceaf939dc
Private-RT1	rtb-0d7b8ccce0e725ed5	subnet-039b4d78b56bd5...	-	No	vpc-0abc2cec959abae7c
Public-RT4	rtb-0770348cc5f350a65	-	-	Yes	vpc-04a5e822cace94922

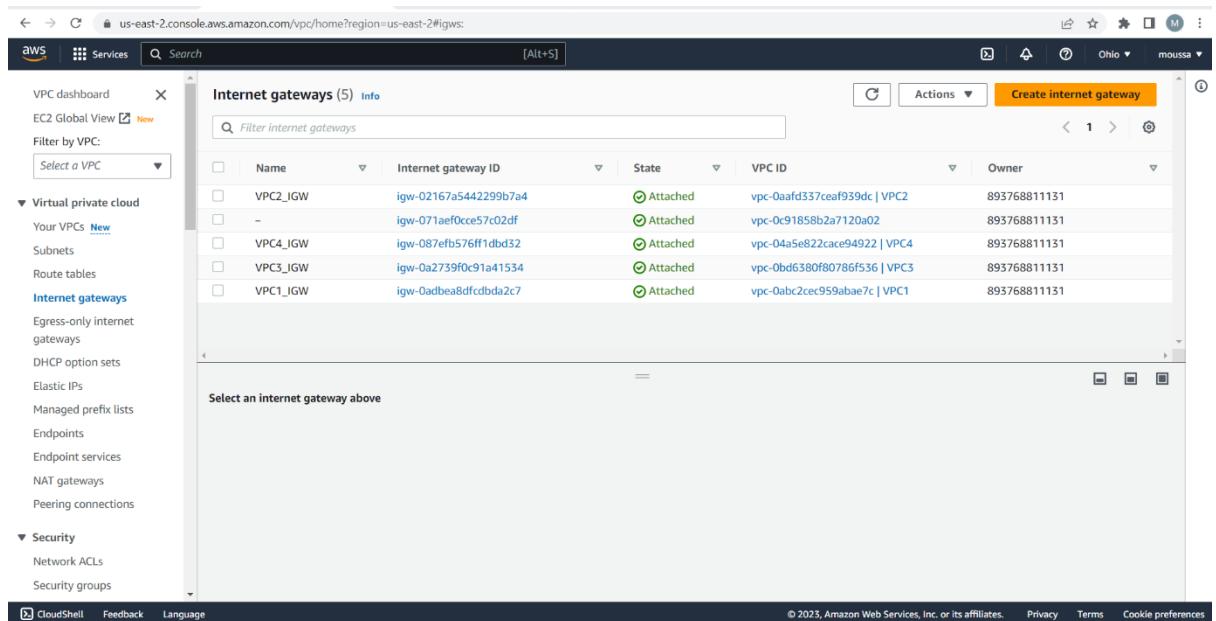
Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

Private-RT1 has a route for communication within the VPC, can access the internet thanks to a NAT gateway in the public subnet but we cannot access it from the internet that make the private subnet more secure.

- **Internet access**

An internet gateway enables resources in your public subnets (such as EC2 instances) to connect to the internet if the resource has a public IPv4 address or an IPv6 address. Similarly, resources on the internet can initiate a connection to resources in your subnet using the public IPv4 address or IPv6 address. For example, an internet gateway enables you to connect to an EC2 instance in AWS using your local computer.

The internet gateway is only for the public subnets.



II. Security Groups

AWS Security Groups are virtual firewalls that control inbound and outbound traffic for Amazon EC2 instances, allowing you to define rules to permit or deny traffic based on protocol, port, and source/destination IP addresses

Web server security group rules:

Inbound Rule for HTTP (Port 80):

Type: HTTP

Protocol: TCP

Port Range: 80

Source: 0.0.0.0/0 (allowing access from any IP address)

Description: Allow inbound HTTP traffic to the web server.

Inbound Rule for HTTPS (Port 443):

Type: HTTPS

Protocol: TCP

Port Range: 443

Source: 0.0.0.0/0 (allowing access from any IP address)

Description: Allow inbound HTTPS traffic to the web server.

Inbound Rule for SSH (Secure Shell) access (Port 22):

Type: SSH

Protocol: TCP

Port Range: 22

Source: 0.0.0.0/0

Description: Allow inbound SSH traffic only from our all IP address. The EC2 instance private key is required so This rule ensures secure remote access to the server.

Inbound Rule for ICMP (Ping) requests:

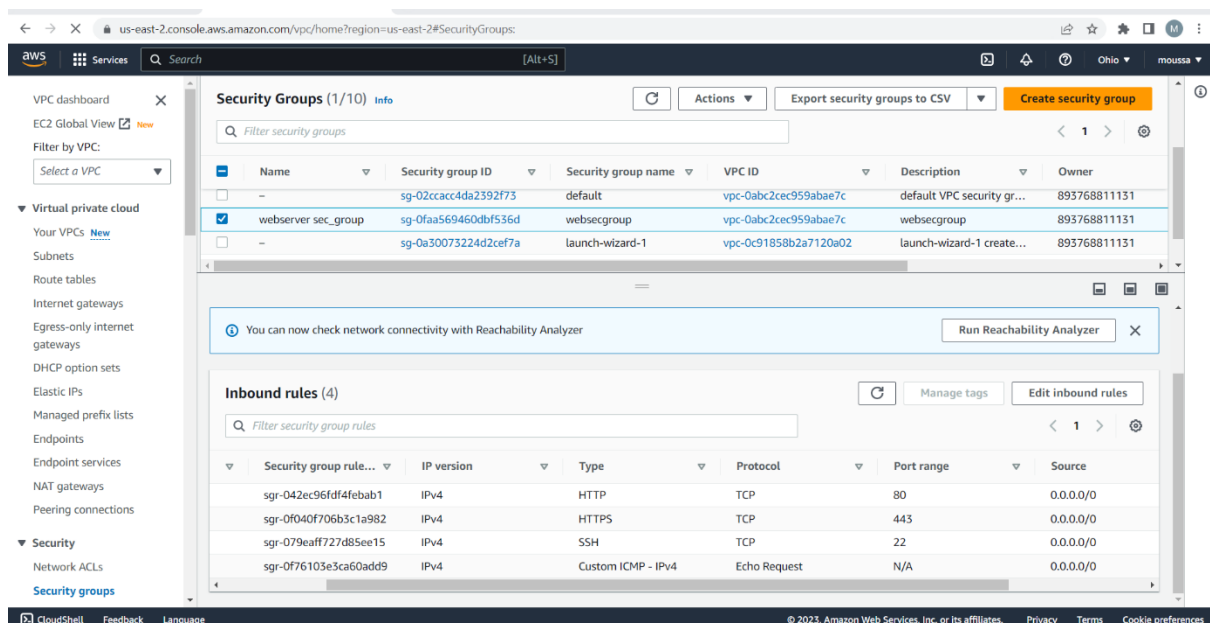
Type: ICMP (IPv4)

Protocol: ICMP

Port Range: N/A

Source: 0.0.0.0/0 (allowing access from any IP address)

Description: Allow inbound ICMP requests, such as ping, for troubleshooting purposes.



The screenshot shows the AWS Management Console for the 'us-east-2' region. The 'Security Groups (1/10)' page is active. A table lists three security groups: 'default', 'webserver sec_group', and 'launch-wizard-1'. The 'webserver sec_group' is selected. Below the table, a notification banner for 'Reachability Analyzer' is visible. The 'Inbound rules (4)' section is expanded, showing a table of rules. The rule for 'Custom ICMP - IPv4' is highlighted.

Name	Security group ID	Security group name	VPC ID	Description	Owner
default	sg-02ccacc4da2392f73	default	vpc-0abc2cec959abae7c	default VPC security gr...	893768811131
webserver sec_group	sg-0faa569460dbf536d	websecgroup	vpc-0abc2cec959abae7c	websecgroup	893768811131
launch-wizard-1	sg-0a30073224d2cef7a	launch-wizard-1	vpc-0c91858b2a7120a02	launch-wizard-1 create...	893768811131

Security group rule...	IP version	Type	Protocol	Port range	Source
sgr-042ec96fdf4febab1	IPv4	HTTP	TCP	80	0.0.0.0/0
sgr-0f040f706b3c1a982	IPv4	HTTPS	TCP	443	0.0.0.0/0
sgr-079eaff727d85ee15	IPv4	SSH	TCP	22	0.0.0.0/0
sgr-0f76103e3ca60add9	IPv4	Custom ICMP - IPv4	Echo Request	N/A	0.0.0.0/0

Outbound Rule for All Traffic:

Type: All Traffic

Protocol: All

Port Range: All

Destination: 0.0.0.0/0

Description: Allow all outbound traffic from the web server to any destination. This rule ensures that the server can communicate with other services or resources it requires.

← → ↻

us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#SecurityGroups

🔖 ☆ ⚙️ 👤 M

aws

Services

Search

[Alt+S]

📄 🔄 ⌛ Ohio moussa

New EC2 Experience

Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Limits

▼ 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

Security Groups (1/10) Info

🔄 Actions ▼ Export security groups to CSV Create security group

🔍 Filter security groups

<input type="checkbox"/>	Name	Security group ID	Security group name	VPC ID	Description	Owner
<input type="checkbox"/>	-	sg-010511a05c3d0e6ea	default	vpc-04a5e822cace94922	default VPC security gr...	893768811131
<input type="checkbox"/>	Database sec_gro...	sg-021dba19fb8ffdf18d	dbsecgroup	vpc-0abc2cec959abae7c	dbsecgroup	893768811131
<input checked="" type="checkbox"/>	webserver sec_g...	sg-0faa569460dbf536d	websecgroup	vpc-0abc2cec959abae7c	websecgroup	893768811131

sg-0faa569460dbf536d - websecgroup

Details Inbound rules Outbound rules Tags

Outbound rules (1)

🔄 Manage tags Edit outbound rules

🔍 Filter security group rules

▼	Security group rule...	IP version	Type	Protocol	Port range	Destination
◀	sgr-07c3ca206fb0bf7fc	IPv4	All traffic	All	All	0.0.0.0/0

https://us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#SecurityGroups...

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- **Database security group rules:**

Inbound Rule for MySQL (Port 3306):

Type: MySQL/Aurora

Protocol: TCP

Port Range: 3306

Source: [sg-0faa569460dbf536d](#) (web server security group ID)

Description: Allow inbound MySQL traffic from the security group associated with the web server. This rule allows the web server to connect to the database.

Inbound Rule for SSH (Secure Shell) access (Port 22):

Type: SSH

Protocol: TCP

Port Range: 22

Source: 0.0.0.0/0

Description: Allow inbound SSH traffic only from the public subnet. This rule ensures secure remote access to the database server for administrative purposes.

The screenshot displays the AWS Management Console interface for Security Groups in the us-east-2 region. The left sidebar shows the navigation menu with 'Security groups' selected under the 'Security' category. The main content area shows a list of security groups, with 'Database sec_group' (sg-021dba19fb8ffd18d) selected. Below the list, the 'Inbound rules' tab is active, showing two rules:

Security group rule...	IP version	Type	Protocol	Port range	Source
sgr-0b76e5e5f194915a8	--	MySQL/Aurora	TCP	3306	sg-0faa569460dbf536d...
sgr-0dd32a11c945c2ecb	IPv4	SSH	TCP	22	0.0.0.0/0

The bottom of the console shows the footer with copyright information: © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Outbound Rule for All Traffic:

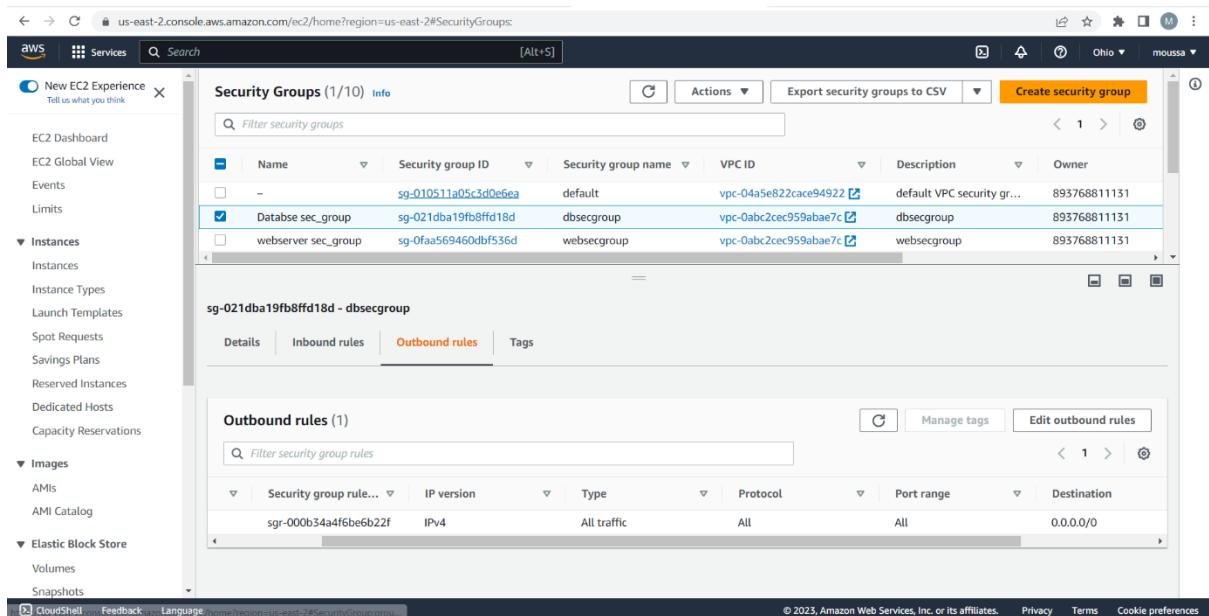
Type: All Traffic

Protocol: All

Port Range: All

Destination: 0.0.0.0/0

Description: Allow all outbound traffic from the database server to any destination. This rule ensures that the database server can communicate with other services or resources it requires.



The screenshot displays the AWS Management Console interface for the 'Security Groups' section. The left-hand navigation pane includes links to various AWS services like EC2 Dashboard, Events, Limits, Instances, Images, and Elastic Block Store. The main content area is titled 'Security Groups (1/10) Info' and features a table listing security groups. The 'Database sec_group' is selected, and its details are shown below. The 'Outbound rules' tab is active, displaying a single rule that allows all traffic to the destination 0.0.0.0/0.

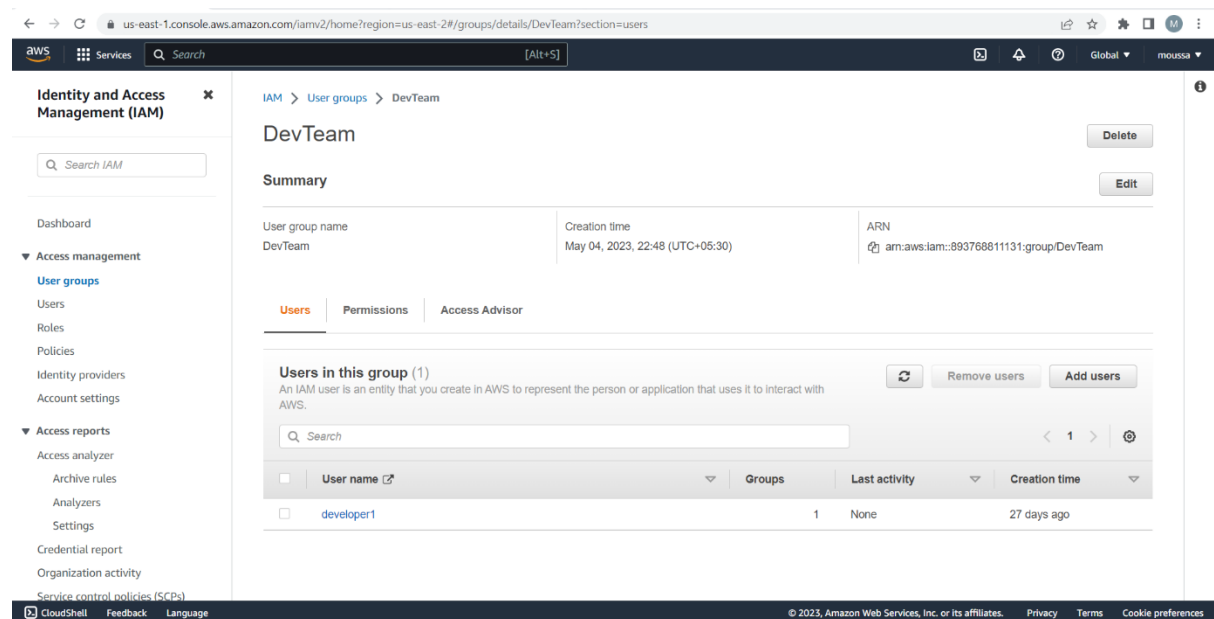
Name	Security group ID	Security group name	VPC ID	Description	Owner
-	sg-010511a05c3d0e5ea	default	vpc-04a5e822ace94922	default VPC security gr...	893768811131
Database sec_group	sg-021dba19fb8ffd18d	dbsecgroup	vpc-0abc2cec959abae7c	dbsecgroup	893768811131
webserver sec_group	sg-0faa569460dbf536d	websecgroup	vpc-0abc2cec959abae7c	websecgroup	893768811131

Security group rule...	IP version	Type	Protocol	Port range	Destination
sgr-000b34a4f6be6b22f	IPv4	All traffic	All	All	0.0.0.0/0

III. Identity and Access Management (IAM)

AWS IAM (Identity and Access Management) is a web service provided by Amazon Web Services (AWS) that enables you to securely control access to AWS services and resources. It helps you manage users, groups, roles, and permissions within your AWS environment.

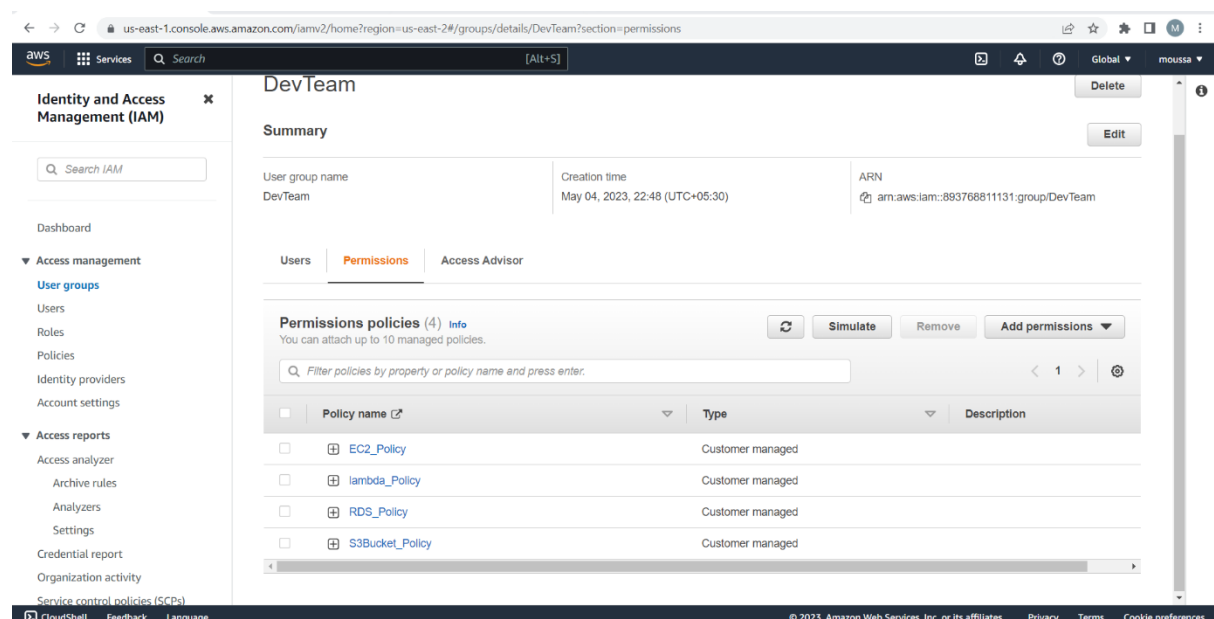
Instead of assigning permissions to each user we have created a group called **DevTeam** so the permissions will be assigned to the group. This will make the management of the users easier.



The screenshot shows the AWS IAM console interface. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and Service control policies (SCPs). The main content area displays the details for the 'DevTeam' user group. The 'Summary' tab is active, showing the user group name 'DevTeam', creation time 'May 04, 2023, 22:48 (UTC+05:30)', and ARN 'arn:aws:iam::893768811131:group/DevTeam'. Below the summary, there are tabs for 'Users', 'Permissions', and 'Access Advisor'. The 'Users' tab is selected, showing a table with one user: 'developer1'. The table has columns for 'User name', 'Groups', 'Last activity', and 'Creation time'.

User name	Groups	Last activity	Creation time
developer1	1	None	27 days ago

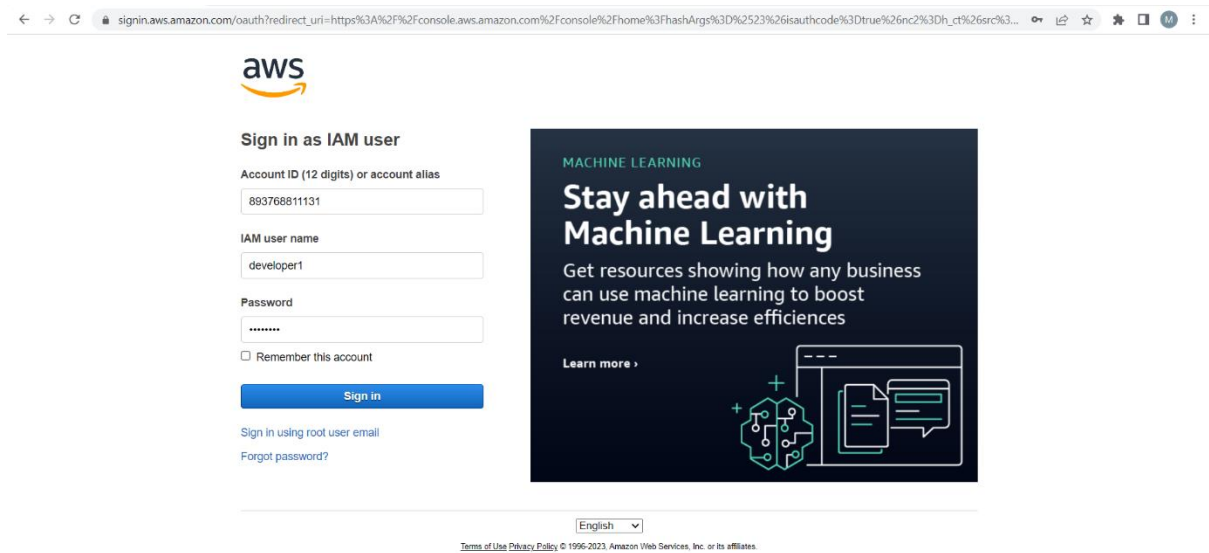
DevTeam is a development team so we suppose that developers may need these few policies including:



The screenshot shows the AWS IAM console interface, specifically the 'Permissions' tab for the 'DevTeam' user group. The 'Summary' tab is still active, showing the user group name 'DevTeam', creation time 'May 04, 2023, 22:48 (UTC+05:30)', and ARN 'arn:aws:iam::893768811131:group/DevTeam'. Below the summary, there are tabs for 'Users', 'Permissions', and 'Access Advisor'. The 'Permissions' tab is selected, showing a table with four policies: 'EC2_Policy', 'lambda_Policy', 'RDS_Policy', and 'S3Bucket_Policy'. The table has columns for 'Policy name', 'Type', and 'Description'.

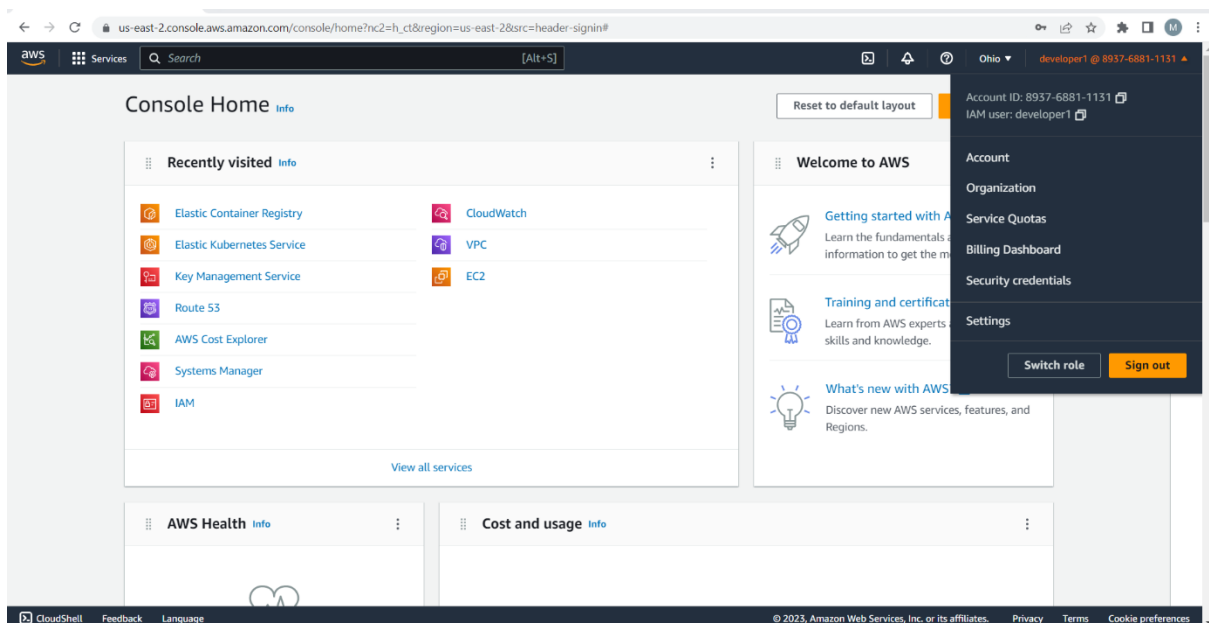
Policy name	Type	Description
EC2_Policy	Customer managed	
lambda_Policy	Customer managed	
RDS_Policy	Customer managed	
S3Bucket_Policy	Customer managed	

We connect to that user account by using his username and password.



The screenshot shows the AWS IAM console sign-in page. The browser address bar displays a URL with a long redirect path. The page features the AWS logo at the top left. Below it, the heading "Sign in as IAM user" is followed by a form with three input fields: "Account ID (12 digits) or account alias" (containing "893768811131"), "IAM user name" (containing "developer1"), and "Password" (masked with dots). A checkbox for "Remember this account" is present below the password field. A blue "Sign in" button is at the bottom of the form. To the right of the form is a promotional banner for "MACHINE LEARNING" with the text "Stay ahead with Machine Learning" and "Get resources showing how any business can use machine learning to boost revenue and increase efficiencies". Below the banner is a "Learn more" link and an illustration of a brain with circuitry. At the bottom of the page, there is a language selector set to "English" and a link to the "Terms of Use Privacy Policy".

Now we have logged as developer1



The screenshot shows the AWS Management Console home page. The browser address bar displays the URL "us-east-2.console.aws.amazon.com/console/home?nc2=h_ct®ion=us-east-2&src=header-signin#". The page has a dark header bar with the AWS logo, a search bar, and a user profile dropdown menu. The user profile shows "developer1" with the account ID "8937-6881-1131". The main content area is titled "Console Home" and features a "Recently visited" section with links to Elastic Container Registry, Elastic Kubernetes Service, Key Management Service, Route 53, AWS Cost Explorer, Systems Manager, IAM, CloudWatch, VPC, and EC2. There is also a "Welcome to AWS" section with links to "Getting started with AWS", "Training and certification", and "What's new with AWS". At the bottom of the page, there is a footer with links to "CloudShell", "Feedback", "Language", "© 2023, Amazon Web Services, Inc. or its affiliates.", "Privacy", "Terms", and "Cookie preferences".

Developer1 is only authorized to perform certain tasks, we can see that his not authorized to access the VPCs.

The screenshot shows the AWS VPC dashboard in the us-east-2 region. A red error banner at the top states: "An error occurred. You are not authorized to perform this operation." The left sidebar contains navigation links for "Virtual private cloud" and "Security". The main content area, titled "Resources by Region", lists various VPC resources in a grid. Each resource card includes a link to "See all regions" and a "retry?" button. The resources listed are: VPCs, NAT Gateways, Subnets, VPC Peering Connections, Route Tables, Network ACLs, Internet Gateways, Security Groups, Egress-only Internet Gateways, Customer Gateways, DHCP option sets, Virtual Private Gateways, Elastic IPs, and Site-to-Site VPN Connections. On the right side, there are sections for "Settings" (with links to Zones and Console Experiments), "Additional Information" (with links to VPC Documentation, All VPC Resources, Forums, and Report an Issue), "AWS Network Manager" (with a link to Get started with Network Manager), and "Site-to-Site VPN Connections". The footer of the page includes "CloudShell", "Feedback", "Language", and copyright information for Amazon Web Services, Inc. or its affiliates, along with links to Privacy, Terms, and Cookie preferences.

Resources by Region	
VPCs See all regions	NAT Gateways See all regions
Subnets See all regions	VPC Peering Connections See all regions
Route Tables See all regions	Network ACLs See all regions
Internet Gateways See all regions	Security Groups See all regions
Egress-only Internet Gateways See all regions	Customer Gateways See all regions
DHCP option sets See all regions	Virtual Private Gateways See all regions
Elastic IPs See all regions	Site-to-Site VPN Connections See all regions


```

ubuntu@ip-10-0-1-43:~$ whoami
ubuntu
ubuntu@ip-10-0-1-43:~$ S ping google.com
PING google.com (142.250.191.238) 56(84) bytes of data:
64 bytes from ord38532-ln-f14.1e100.net (142.250.191.238): icmp_seq=1 ttl=47 time=17.7 ms
64 bytes from ord38532-ln-f14.1e100.net (142.250.191.238): icmp_seq=2 ttl=47 time=17.7 ms
64 bytes from ord38532-ln-f14.1e100.net (142.250.191.238): icmp_seq=3 ttl=47 time=17.6 ms
64 bytes from ord38532-ln-f14.1e100.net (142.250.191.238): icmp_seq=4 ttl=47 time=17.7 ms
64 bytes from ord38532-ln-f14.1e100.net (142.250.191.238): icmp_seq=5 ttl=47 time=17.7 ms
64 bytes from ord38532-ln-f14.1e100.net (142.250.191.238): icmp_seq=6 ttl=47 time=17.5 ms
64 bytes from ord38532-ln-f14.1e100.net (142.250.191.238): icmp_seq=7 ttl=47 time=17.7 ms
64 bytes from ord38532-ln-f14.1e100.net (142.250.191.238): icmp_seq=8 ttl=47 time=17.7 ms
64 bytes from ord38532-ln-f14.1e100.net (142.250.191.238): icmp_seq=9 ttl=47 time=17.7 ms
64 bytes from ord38532-ln-f14.1e100.net (142.250.191.238): icmp_seq=10 ttl=47 time=17.7 ms
64 bytes from ord38532-ln-f14.1e100.net (142.250.191.238): icmp_seq=11 ttl=47 time=17.6 ms
64 bytes from ord38532-ln-f14.1e100.net (142.250.191.238): icmp_seq=12 ttl=47 time=17.6 ms
^C
[1]: Stopped ping google.com

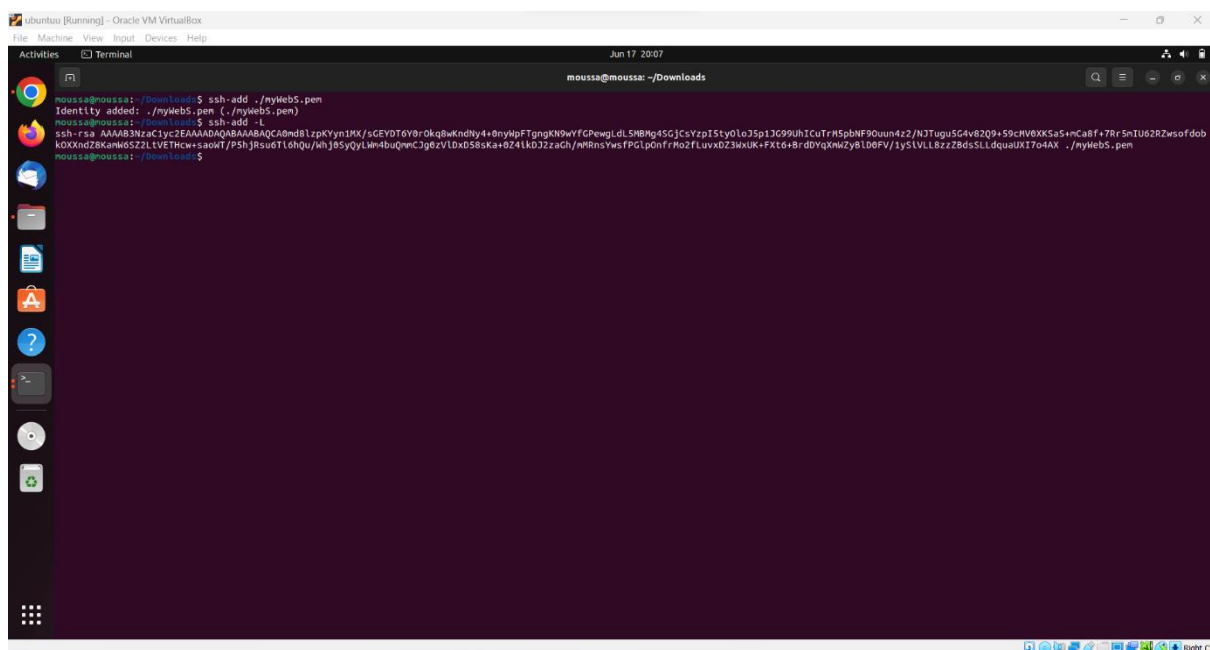
```

2. Access to the database

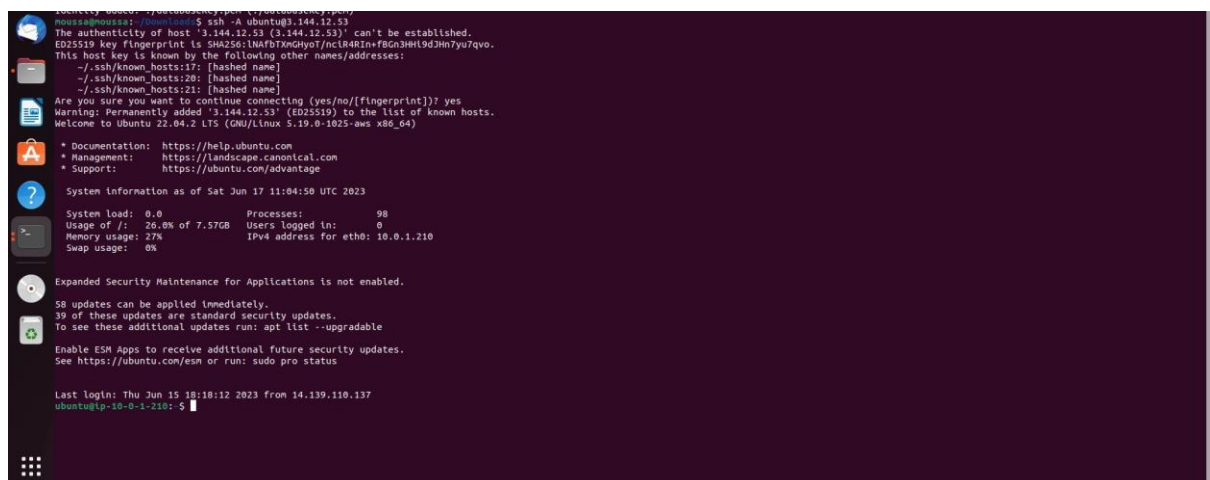
To access the database, one of the most secure ways is by SSH forwarding also known as SSH bastion host.

This method involves using an intermediate server (our web server instance), often called a "bastion host" or "jump host," that is publicly accessible and acts as a bridge to connect to the private EC2 instance. The bastion host resides in a public subnet and has SSH access to both the public and private subnets. You establish an SSH connection to the bastion host first and then use that connection to SSH into the private EC2 instance.

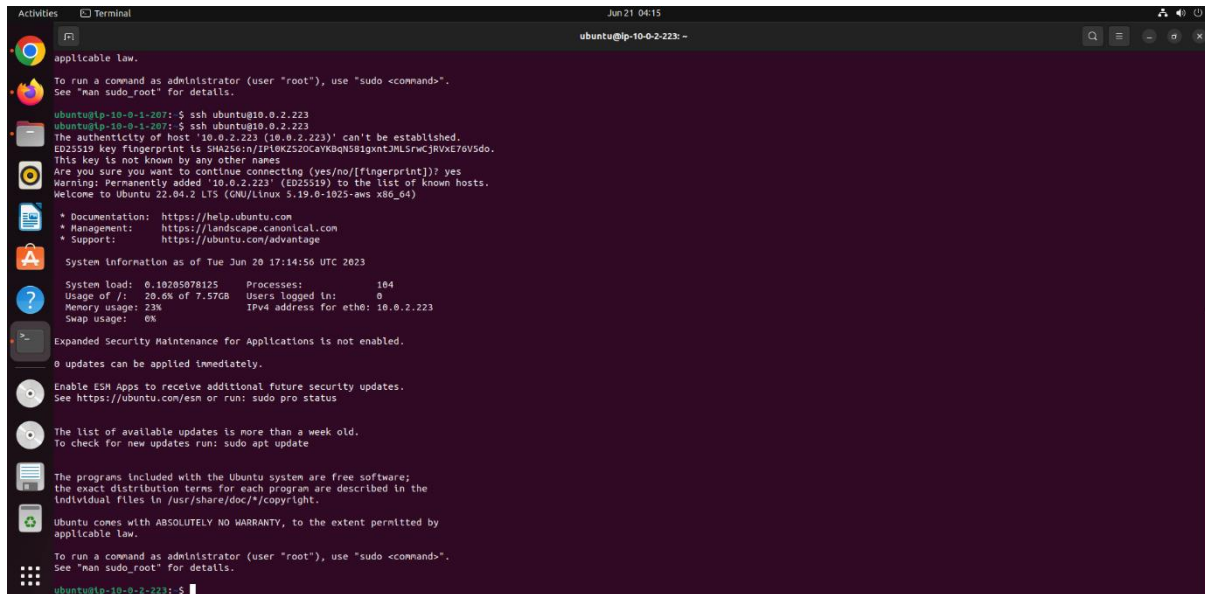
Adding of our private to the ssh agent



Here we are in the bastion host and we did not specify the private key



Thanks to the agent forwarding we are able to access to the private instance without specifying the private key



The image shows a terminal window titled "Terminal" with a dark background. The window displays the output of an SSH command. The prompt is "ubuntu@ip-10-0-2-223: ~". The output shows the SSH client version "OpenSSH_8.2p1 Ubuntu-0ubuntu0.2", the Ubuntu logo, and the system information "Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-105-aws x86_64)". The system information includes the system load, usage of /, memory usage, swap usage, and the number of processes and users logged in. The output also shows the SSH key fingerprint and the warning "Warning: Permanently added '10.0.2.223' (ED25519) to the list of known hosts." The prompt is "ubuntu@ip-10-0-2-223: ~".

```
ubuntu@ip-10-0-2-223: ~  
OpenSSH_8.2p1 Ubuntu-0ubuntu0.2, OpenSSL 3.0.2 3 Jun 2023  
ubuntu@ip-10-0-2-223: ~  
The authenticity of host '10.0.2.223 (10.0.2.223)' can't be established.  
ED25519 key fingerprint is SHA256:n1P10K2520Ca1Kq581gxt2ML5rwcJRVxE70V5do.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.0.2.223' (ED25519) to the list of known hosts.  
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-105-aws x86_64)  
  
 * Documentation:  https://help.ubuntu.com  
 * Management:    https://landscape.canonical.com  
 * Support:       https://ubuntu.com/advantage  
  
System Information as of Tue Jun 20 17:14:56 UTC 2023  
  
System load: 0.10205078125      Processes:      164  
Usage of /: 20.0% of 7.57GB      Users logged in: 0  
Memory usage: 23%              IPv4 address for eth0: 10.0.2.223  
Swap usage: 0%  
  
Expanded Security Maintenance for Applications is not enabled.  
  
0 updates can be applied immediately.  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/*copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
ubuntu@ip-10-0-2-223: ~
```

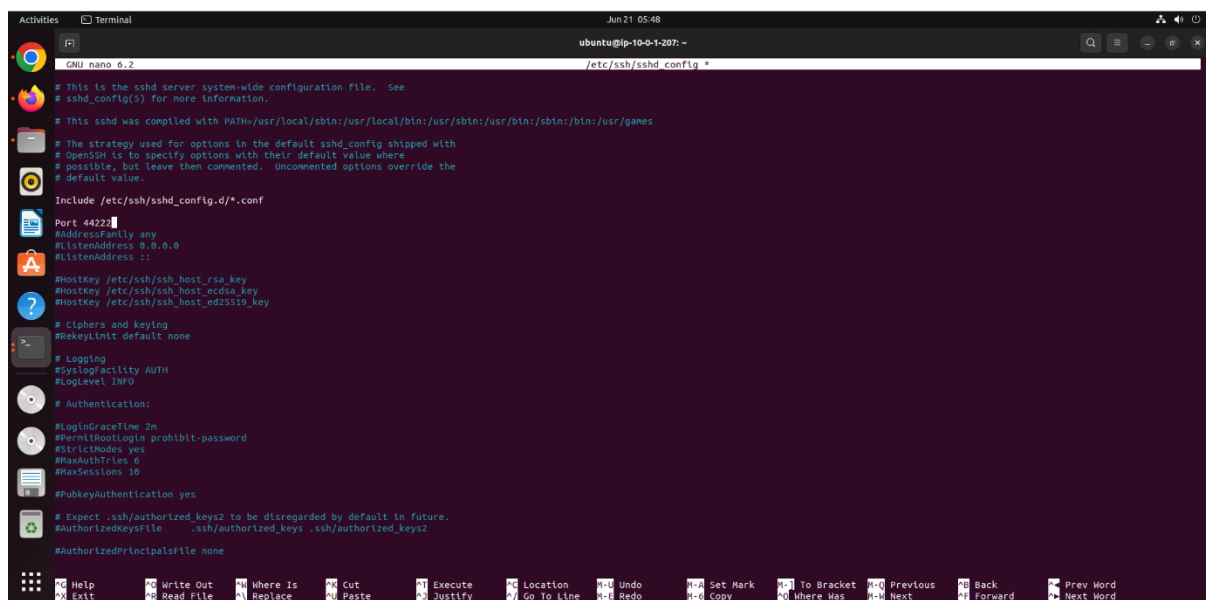
V. Security Hardening

- **SSH connexion**

To enforce the security of the SSH service, Changing the default port number of SSH (Secure Shell) is considered a security best practice. By default, SSH uses port 22 for communication, which is well-known and often targeted by malicious actors for brute-force attacks and automated scanning.

Changing the default SSH port can make it harder for attackers to find and target your SSH service. It adds an extra layer of security through "security through obscurity." While it shouldn't be relied upon as the sole security measure, it can be an effective deterrent against automated attacks.

We have changed the SSH port 22 to 4422.



```
GNU nano 0.2 /etc/ssh/sshd_config
# This is the sshd server system-wide configuration file. See
# sshd_config(8) for more information.
# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.
Include /etc/ssh/sshd_config.d/*.conf

Port 4422
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
#AuthorizedPrincipalsFile none
```

- **Hide apache2 server banner**

The Apache banner refers to the server identification information that is typically included in the HTTP response headers sent by an Apache web server. It provides details about the version of Apache being used and may also include additional information such as the operating system and other server software.

From our first nmap scan we can see the apache banner information



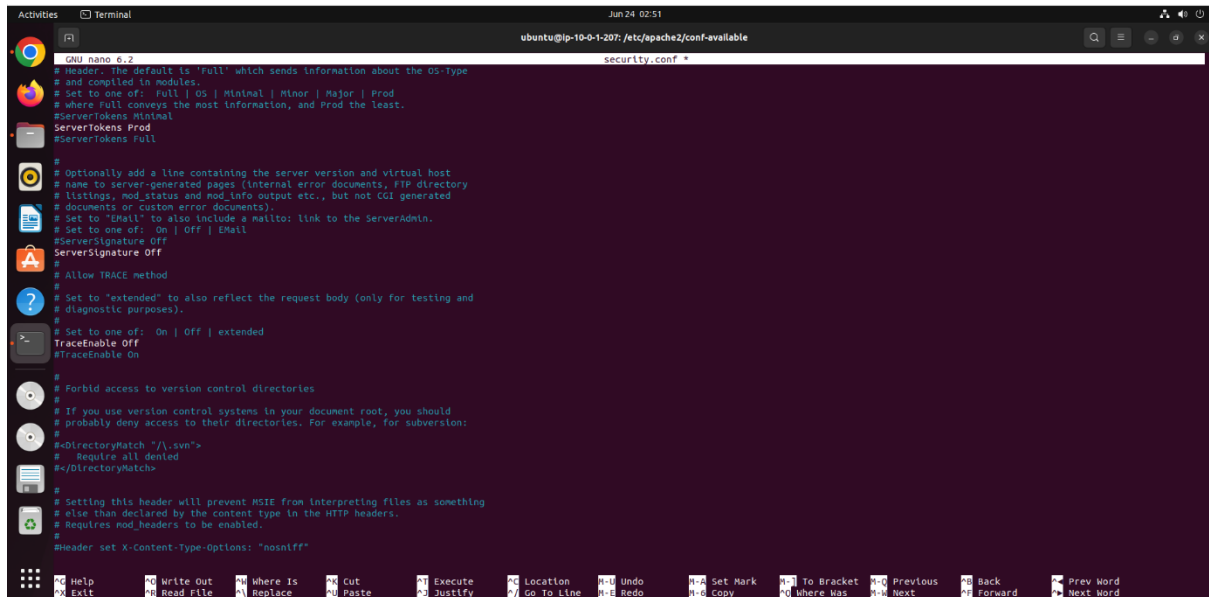
```
ubuntu [Running] - Oracle VM VirtualBox
Jun 18 15:47
moussa@moussa: ~
moussa@moussa:~$ sudo nmap -A 18.221.7.97
[sudo] password for moussa:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-06-18 15:38 IST
Nmap scan report for ec2-18-221-7-97.us-east-2.compute.amazonaws.com (18.221.7.97)
Host is up (0.034s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  ssl/http
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
```

To hide the banner, we need to configure the file `/etc/apache2/apache2.conf` and add the following:

ServerTokens Prod

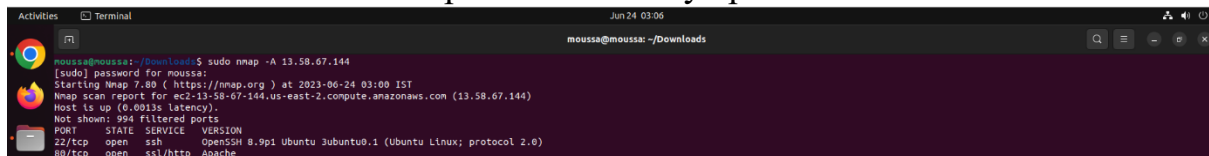
ServerSignature Off

TraceEnable Off



```
GNU nano 6.2 security.conf
#
# The default is 'Full' which sends information about the OS-type
# and compiled-in modules.
# Set to one of: Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#ServerTokens Minimal
ServerTokens Prod
#ServerTokens Full
#
# optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, /flp directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to 'On' to also include a mailto: link to the ServerAdmin.
# Set to one of: On | Off | Email
#ServerSignature Off
ServerSignature Off
#
# Allow TRACE method
#
# Set to 'extended' to also reflect the request body (only for testing and
# diagnostic purposes).
#
# Set to one of: On | Off | extended
TraceEnable Off
#TraceEnable On
#
# Forbid access to version control directories
#
# If you use version control systems in your document root, you should
# probably deny access to their directories. For example, for Subversion:
#
#DirectoryMatch "/\..svn">
#    Require all denied
#</DirectoryMatch>
#
# Setting this header will prevent MSIE from interpreting files as something
# else than declared by the content type in the HTTP headers.
# Requires mod_headers to be enabled.
#
#Header set X-Content-Type-Options: "nosniff"
```

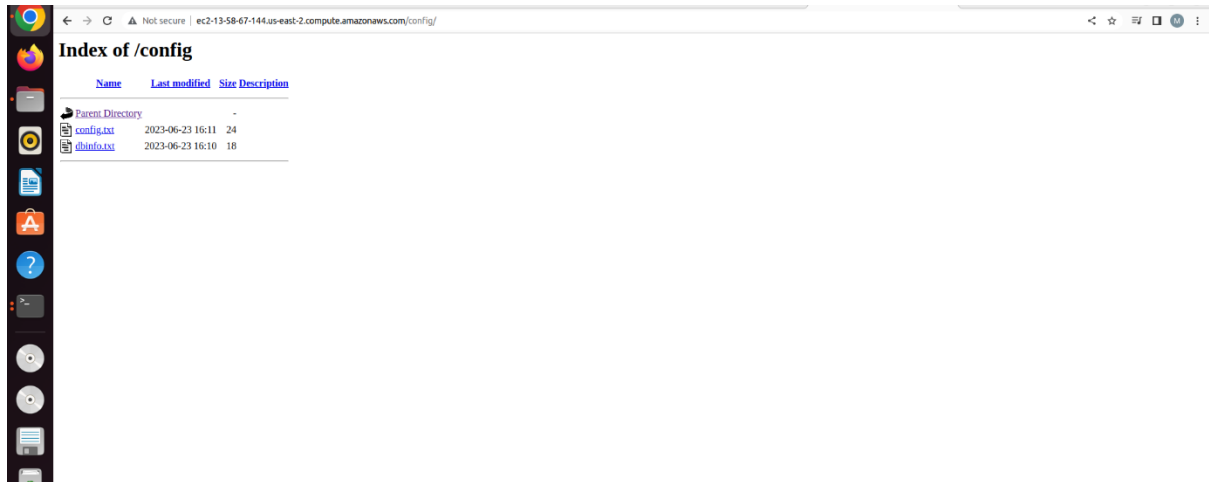
Now we can see that the nmap scan show only apache



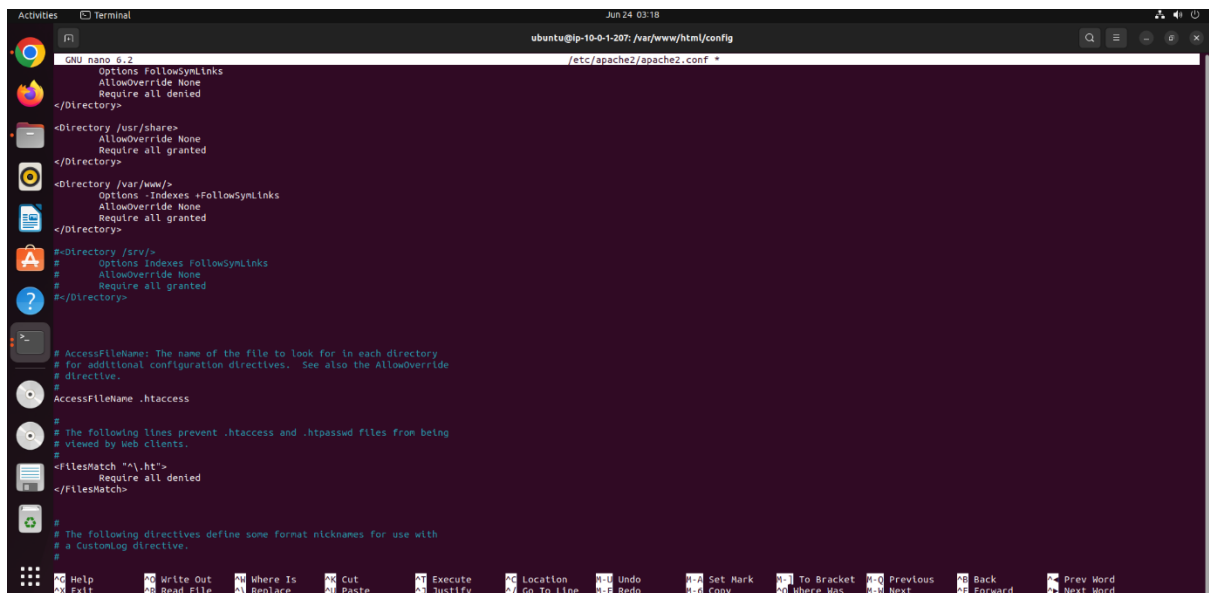
```
moussa@moussa: ~/Downloads
[sudo] password for moussa:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-06-24 03:00 IST
Nmap scan report for ec2-13-58-67-144.us-east-2.compute.amazonaws.com (13.58.67.144)
Host is up (0.0013s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  ssl/http Apache
```

- **Disable Apache directory browsing**

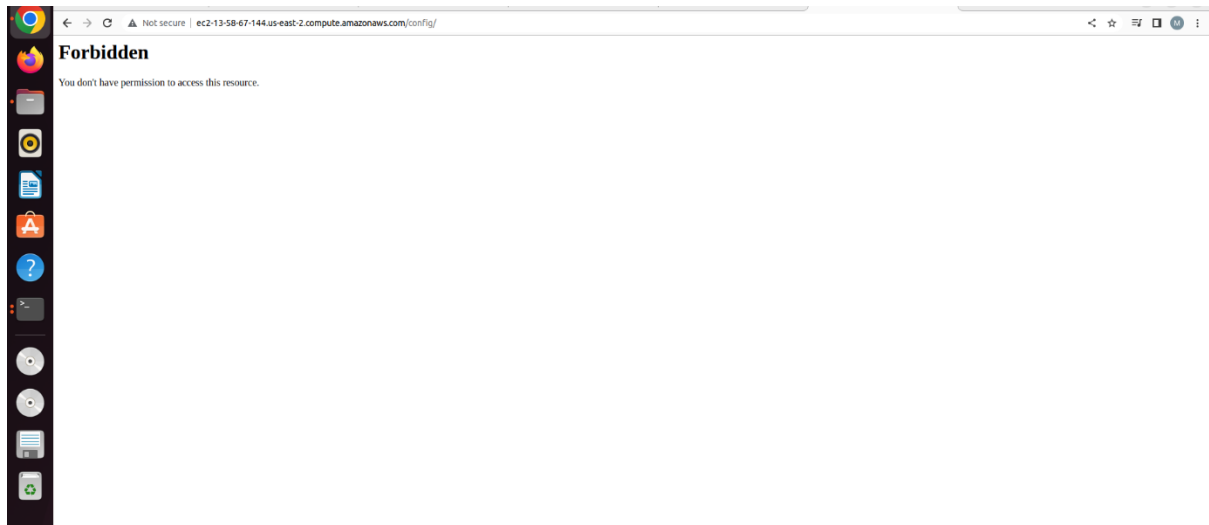
Directory browsing is a feature that can be enabled on a web server, which allows users to view the directory structure of a website without the need to enter any credentials. It is typically enabled on web servers to allow users to easily access files that they need, without having to know the precise path.



To disable the directory browsing we modify the file `/etc/apache2/apache2.conf` by adding “-” to Options -Indexes.



We can see that now we are not able to access the directory



This work is done by simply following AWS configuration best practices. It can be more enhanced by using others tools such as:

- **AWS WAF (Web Application Firewall)**
- **AWS Inspector**
- **AWS CloudWatch**
- **Amazon GuardDuty**
- **AWS Key Management Service (KMS)**
- **Etc...**