

# 020 Practical

**Network ACL - 08 Mar 2022**

The screenshot shows the AWS VPC Management console interface. On the left, a navigation sidebar under 'VIRTUAL PRIVATE CLOUD' has 'Your VPCs' selected, indicated by a red box. The main area displays 'Your VPCs (1/2)' with a table showing one entry:

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
-	vpc-0d530da491583e01c	Available	172.31.0.0/16	-
<b>devops-VPC</b>	<b>vpc-0e1ea03ae4ce0d752</b>	<b>Available</b>	<b>10.10.0.0/16</b>	-

A detailed view of the selected VPC ('devops-VPC') is shown below, with its VPC ID 'vpc-0e1ea03ae4ce0d752' highlighted by a red box. The IPv4 CIDR '10.10.0.0/16' is also highlighted by a red box in the details panel.

VPC ID vpc-0e1ea03ae4ce0d752	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-0abdddae61d15017c	Main route table rtb-0ce45cd7130c22a95	Main network ACL acl-0c1d6fc4d05d6d57d
Default VPC No	IPv4 CIDR <b>10.10.0.0/16</b>	IPv6 pool -	IPv6 CIDR -
Route 53 Resolver DNS Firewall rule groups -	Owner ID 876283541003		

At the bottom, the footer includes links for Feedback, English (US), Privacy, Terms, and Cookie preferences, along with system status icons like weather and battery level.

- Here I have created one VPC

The screenshot shows the AWS VPC Subnets page. On the left sidebar, under the 'Subnets' section, the 'Subnets' link is highlighted with a red box. In the main content area, the 'Subnets (1/5)' table is displayed. A single row for a 'Public-Subnet' is selected and highlighted with a red box. The table columns include Name, Subnet ID, State, VPC, and IPv4 CIDR. The selected subnet has a Subnet ID of 'subnet-00c1a5d0a1e14e5fe', is in an 'Available' state, belongs to VPC 'vpc-0e1ea03ae4ce0d752 | dev...', and has an IPv4 CIDR of '10.10.1.0/24'. The 'Details' pane on the right shows more information about the selected subnet, including its VPC (vpc-0e1ea03ae4ce0d752 | dev-), Subnet ARN, State (Available), IPv4 CIDR (10.10.1.0/24), and Route table (rtb-06f83db7355a8ad75 | Public-Routing).

Name	Subnet ID	State	VPC	IPv4 CIDR
-	subnet-0a84a11858506eb19	Available	vpc-0d530da491583e01c	172.31.32.0/20
<input checked="" type="checkbox"/> Public-Subnet	subnet-00c1a5d0a1e14e5fe	Available	vpc-0e1ea03ae4ce0d752   dev...	10.10.1.0/24

**Details**

Subnet ID subnet-00c1a5d0a1e14e5fe	Subnet ARN arn:aws:ec2:us-east-2:876283541003:subnet/subnet-00c1a5d0a1e14e5fe	State Available	IPv4 CIDR 10.10.1.0/24
Available IPv4 addresses 249	IPv6 CIDR -	Availability Zone us-east-2a	Availability Zone ID use2-az1
VPC vpc-0e1ea03ae4ce0d752   dev- VPC	Route table rtb-06f83db7355a8ad75   Public-Routing	Network ACL acl-0c1d6fc4d05d6d57d	Default subnet No
Auto-assign public IPv4 address		Auto-assign customer-owned IPv4 address	Customer-owned IPv4 pool -

- Here I have created one Public Subnet in my VPC

The screenshot shows the AWS VPC Route Tables page. On the left sidebar, under the 'Route Tables' section, the 'Route Tables' link is highlighted with a red box. In the main content area, the 'Route tables (1/3) Info' section displays a table with one row. The row for 'Public-Routing' has a checked checkbox and is also highlighted with a red box. The table columns include Name, Route table ID, Explicit subnet associations, Edge associations, Main, and VPC. The 'Details' panel on the right shows the Route table ID as rtb-06f83db7355a8ad75, the VPC as vpc-0e1ea03ae4ce0d752 | devops- VPC, and the explicit subnet associations as subnet-00c1a5d0a1e14e5fe / Public-Subnet.

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
Public-Routing	rtb-06f83db7355a8ad75	subnet-00c1a5d0a1e14e5fe / Public-Subnet	-	No	vpc-0e1ea03ae4ce0d752

**Details**

Route table ID rtb-06f83db7355a8ad75	Main No	Explicit subnet associations subnet-00c1a5d0a1e14e5fe / Public-Subnet
VPC vpc-0e1ea03ae4ce0d752   devops- VPC	Owner ID 876283541003	Edge associations -

- Here I have created one Public Route Table in my VPC

The screenshot shows the AWS VPC Internet Gateways page. On the left sidebar, under the 'Internet Gateways' section, the 'Devops-IGW' entry is selected and highlighted with a red box. In the main content area, the table lists two Internet Gateways:

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-034f938d902beb887	Attached	vpc-0d530da491583e01c	876283541003
<input checked="" type="checkbox"/> Devops-IGW	igw-0aec85fb3ccf20d7b	Attached	vpc-0e1ea03ae4ce0d752   devops-VPC	876283541003

Below the table, the details for the selected gateway (igw-0aec85fb3ccf20d7b / Devops-IGW) are shown. The 'Details' tab is selected, and the 'VPC ID' field, containing the value 'vpc-0e1ea03ae4ce0d752 | devops-VPC', is also highlighted with a red box.

- Here I have created one Internet Gateway and attached it to my VPC

**Now we have to create Network ACL**

The screenshot shows the AWS Management Console interface for Network ACLs. The left sidebar navigation includes options like Elastic IPs, Managed Prefix Lists, Endpoints, Endpoint Services, NAT Gateways, Peering Connections, SECURITY (Network ACLs selected), NETWORK ANALYSIS, DNS FIREWALL, and NETWORK FIREWALL. The main content area displays a table titled "Network ACLs (2) Info" with two entries:

Name	Network ACL ID	Associated with	Default	VPC ID
-	acl-0c906de5a149adf1e	3 Subnets	Yes	vpc-0d530da491583e01c
-	acl-0c1d6fc4d05d6d57d	2 Subnets	Yes	vpc-0e1ea03ae4ce0d752 / dev

A red box highlights the "Create network ACL" button in the top right corner of the table header.

At the bottom of the screen, there is a toolbar with various icons and status information, including weather (31°C Partly sunny), system icons (Windows, search, file, browser, messaging, calendar, etc.), and system status (ENG IN, 4:38 PM, 3/11/2022).

- Go to Network ACLs
- Click on Create Network ACL

The screenshot shows the AWS VPC Management Console with the URL [us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#CreateNetworkAcl](https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#CreateNetworkAcl). The page is titled "Network ACL settings". It has two main sections: "Name - optional" (with input field "Devops-NACL") and "VPC" (with dropdown menu showing "vpc-0e1ea03ae4ce0d752 (devops-VPC)". Both the Name and VPC fields are highlighted with red boxes. Below these is a "Tags" section with a key-value pair ("Name" : "Devops-NACL") and an "Add new tag" button. The "Create network ACL" button at the bottom is also highlighted with a red box. The browser's address bar and various AWS services in the top navigation bar are visible.

- Give name
- Select our VPC
- Click on Create Network ACL

The screenshot shows the AWS VPC Network ACLs page. At the top, there is a success message: "You successfully created acl-0638aa5cc7139fd44 / Devops-NACL." Below this, the "Network ACLs (1/3)" section displays a table with one row. The table has columns: Name, Network ACL ID, Associated with, Default, and VPC ID. The single row shows "Devops-NACL" as the Name, "acl-0638aa5cc7139fd44" as the Network ACL ID, "-" as the Associated with value, "No" as the Default value, and "vpc-0e1ea03ae4ce0d752 / devops-VPC" as the VPC ID. The "VPC ID" column is highlighted with a red box. The left sidebar shows navigation links for various AWS services like Elastic IPs, Managed Prefix Lists, and Network ACLs.

Name	Network ACL ID	Associated with	Default	VPC ID
Devops-NACL	acl-0638aa5cc7139fd44	-	No	vpc-0e1ea03ae4ce0d752 / devops-VPC

**Details**

Network ACL ID acl-0638aa5cc7139fd44	Associated with -	Default No	VPC ID vpc-0e1ea03ae4ce0d752 / devops-VPC
Owner 876283541003			

- Network ACL is Created Successfully.

The screenshot shows the AWS VPC Network ACLs page. On the left sidebar, under the 'SECURITY' section, 'Network ACLs' is selected. In the main content area, a table lists 'Network ACLs (1/3)'. The first row, 'Devops-NACL', is selected and highlighted with a red box. Below the table, a sub-section titled 'acl-0638aa5cc7139fd44 / Devops-NACL' is shown. The 'Subnet associations' tab is active, indicated by a red box around its title. A large red box highlights the 'Edit subnet associations' button. The bottom of the screen shows the standard AWS navigation bar with links for Feedback, English (US), Privacy, Terms, and Cookie preferences, along with system status icons.

- Now select our NACL
- Click on Subnet Associations
- Click on Edit Subnet Associations

The screenshot shows the AWS VPC Network ACL subnet associations editor. The URL in the browser is [us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#EditNetworkAclSubnetAssociations:networkAclId=acl-0638aa5cc7139fd44](https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#EditNetworkAclSubnetAssociations:networkAclId=acl-0638aa5cc7139fd44). The page title is "Edit subnet associations".

**Available subnets (1/2)**

Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR
<input checked="" type="checkbox"/> Public-Subnet	subnet-00c1a5d0a1e14e5fe	acl-0c1d6fc4d05d6d57d	us-east-2a	10.10.1.0/24	-
<input type="checkbox"/> Private-Subnet	subnet-0c11c8dc0b1c4f38e	acl-0c1d6fc4d05d6d57d	us-east-2b	10.10.2.0/24	-

**Selected subnets**

subnet-00c1a5d0a1e14e5fe / Public-Subnet X

Buttons: Cancel, Save changes

Page footer: Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences 31°C Partly sunny ENG IN 4:41 PM 3/11/2022

- Select Public Subnet
- Click on Save Changes

The screenshot shows the AWS VPC Network ACLs page. A prominent green success message at the top states: "You have successfully updated subnet associations for acl-0638aa5cc7139fd44 / Devops-NACL." Below this, the "Network ACLs" table lists one item: "Devops-NACL" associated with "subnet-00c1a5d0a1e14e5fe / Public-Subnet". The "Associated with" column shows the subnet ID and name. The "Actions" dropdown menu for this row has been opened, revealing options like "Edit", "Delete", and "Associate with subnet". Below the main table, the "Filter subnet associations" search bar is visible, along with another table showing a single association between "Public-Subnet" and "acl-0638aa5cc7139fd44 / Devops-NACL". The left sidebar contains navigation links for various VPC services like New VPC Experience, Elastic IPs, Managed Prefix Lists, and security-related options like Network ACLs, Security Groups, and Network Firewall.

Name	Network ACL ID	Associated with	Default	VPC ID
Devops-NACL	acl-0638aa5cc7139fd44	subnet-00c1a5d0a1e14e5fe / Public-Subnet	No	vpc-0e1ea03ae4ce0d752 / d

Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR
Public-Subnet	subnet-00c1a5d0a1e14e5fe	acl-0638aa5cc7139fd44 / Devops-NACL	us-east-2a	10.10.1.0/24	-

- Here we have updated our Subnet Successfully.

**Now Launch one instance in our VPC inside  
public subnet.**

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with sections like EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (with 'Instances New' highlighted), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances (New), Dedicated Hosts, and Capacity Reservations. Below that is the Images section with 'AMIs New'. The main content area has tabs for Instances and Info, with the Instances tab selected. It shows a search bar, a filter for 'Instance state = running' (which is also highlighted with a red box), and a 'Clear filters' button. A table header includes columns for Name, Instance ID, Instance state, Instance type, and Status. A message below the table says 'No matching instances found'. At the top right of the main area, there are buttons for Actions, Instance state, and Launch instances (which is also highlighted with a red box). Below the main table is a modal window titled 'Select an instance'.

- Go to Instances
- Click on Launch Instances

Step 3: Configure Instance Details

Number of instances  Launch into Auto Scaling Group [i](#)

Purchasing option [i](#)  Request Spot instances

Network [i](#)  [Create new VPC](#)

Subnet [i](#)  [Create new subnet](#)  
251 IP Addresses available

Auto-assign Public IP [i](#)

Hostname type [i](#)

DNS Hostname [i](#)

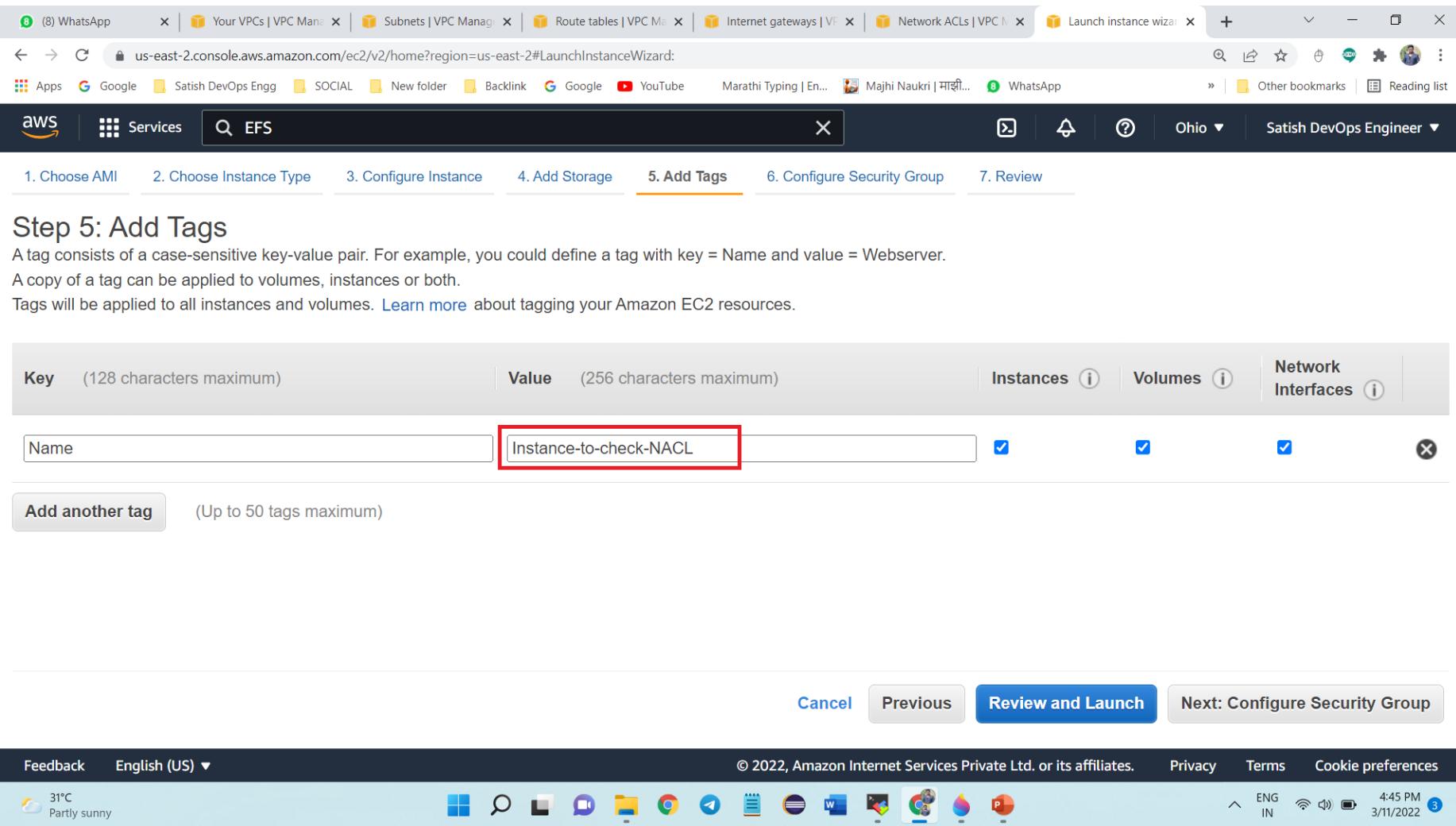
- Enable IP name IPv4 (A record) DNS requests
- Enable resource-based IPv4 (A record) DNS requests
- Enable resource-based IPv6 (AAAA record) DNS requests

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

31°C Partly sunny ENG IN 4:44 PM 3/11/2022

- Select our VPC
- Select Public Subnet
- Enable Public IP



The screenshot shows the AWS Launch Instance Wizard at Step 5: Add Tags. The URL in the browser is [us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard](https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard). The search bar at the top has 'EFS' typed into it. Below the search bar, the steps are numbered 1 through 7: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags (which is the current step), 6. Configure Security Group, and 7. Review.

**Step 5: Add Tags**

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

The 'Value' field is highlighted with a red box and contains the text "Instance-to-check-NACL".

Below the input fields, there is a button labeled "Add another tag" and a note "(Up to 50 tags maximum)".

At the bottom, there are navigation buttons: "Cancel", "Previous", "Review and Launch" (which is highlighted in blue), and "Next: Configure Security Group".

The browser's footer includes links for Feedback, English (US) dropdown, © 2022, Amazon Internet Services Private Ltd. or its affiliates, Privacy, Terms, and Cookie preferences. It also shows the weather (31°C, Partly sunny), system icons (ENG IN, battery, signal), and the date/time (4:45 PM, 3/11/2022).

- Give proper Tags

8 (8) WhatsApp | Your VPCs | VPC Manager | Subnets | VPC Manager | Route tables | VPC Manager | Internet gateways | VPC Manager | Network ACLs | VPC Manager | Launch instance wizard | + | - | X

us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:

Apps Google SOCIAL New folder Backlink Google YouTube Marathi Typing | En... Majhi Naukri | माझी... WhatsApp

Ohio | Satisfy DevOps Engineer

**EFS**

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

## Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group:  Create a **new** security group  
 Select an **existing** security group

**Security group name:** SSH-Only-11

**Description:** SSH-Only-11

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Anywhere	0.0.0.0/0, ::/0

**Add Rule**

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

Cancel Previous **Review and Launch**

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

31°C Partly sunny

ENG IN 4:46 PM 3/11/2022

- Select SSH 22 in Security Group

The screenshot shows the AWS Launch Instance Wizard at Step 7: Review Instance Launch. A modal window titled "Select an existing key pair or create a new key pair" is displayed. It contains a note about key pairs and a dropdown menu for selecting a key pair, which has "ohio-instance | RSA" selected. There is also a checkbox for acknowledging access to the private key file. The background shows the instance details (Amazon Linux 2 AMI (HVM) - Kernel 5.10), instance type (t2.micro), and a summary of the launch process.

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to previous steps or proceed to the next step.

**AMI Details**

**Amazon Linux 2 AMI (HVM) - Kernel 5.10**

Free tier eligible

Amazon Linux 2 comes with five years support and access to over 2,000 software packages through extras. This AMI includes the latest version of Python 3.9, Java 11, MySQL 8.0, PostgreSQL 12, MariaDB 10.5, and Redis 6.0. It also includes the latest versions of Apache, Nginx, and PHP.

Root Device Type: ebs Virtualization type: hvm

**Instance Type**

Instance Type	ECUs	vCPUs
t2.micro	-	1

**Select an existing key pair or create a new key pair**

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

Select a key pair

ohio-instance | RSA

I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

Network Performance

Low to Moderate

Feedback English (US) ▾

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

31°C Partly sunny

ENG IN 4:46 PM 3/11/2022

- Select Key Pair and Launch Instnace

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with various navigation options like EC2 Dashboard, Events, Tags, and Limits. The main area displays a table of instances. A single instance is selected, highlighted with a red box. The instance details are shown in a modal window. The 'Details' tab is selected, showing the instance summary. The 'Public IPv4 address' field contains '3.15.11.240' with a link to 'open address'. The 'Connect' button at the top of the main table is also highlighted with a red box.

Name	Instance ID	Instance state	Instance type	Status check
Instance-to-check-NACL	i-0b65c5ea53fd70be8	Running	t2.micro	Initializing

**Instance: i-0b65c5ea53fd70be8 (Instance-to-check-NACL)**

Details	Security	Networking	Storage	Status checks	Monitoring	Tags
<b>Instance summary</b>						
Instance ID i-0b65c5ea53fd70be8 (Instance-to-check-NACL)	Public IPv4 address 3.15.11.240   <a href="#">open address</a>	Private IPv4 addresses 10.10.1.12				
IPv6 address -	Instance state Running	Public IPv4 DNS -				
Hostname type IP name: ip-10-10-1-12.us-east-2.compute.internal	Private IP DNS name (IPv4 only) ip-10-10-1-12.us-east-2.compute.internal	Answer private resource DNS name IPv4 (A)				
Instance type t2.micro	Elastic IP addresses -	VPC ID -				

- Here our instance is Running fine.
- Now we will try to connect it. So click on Connect

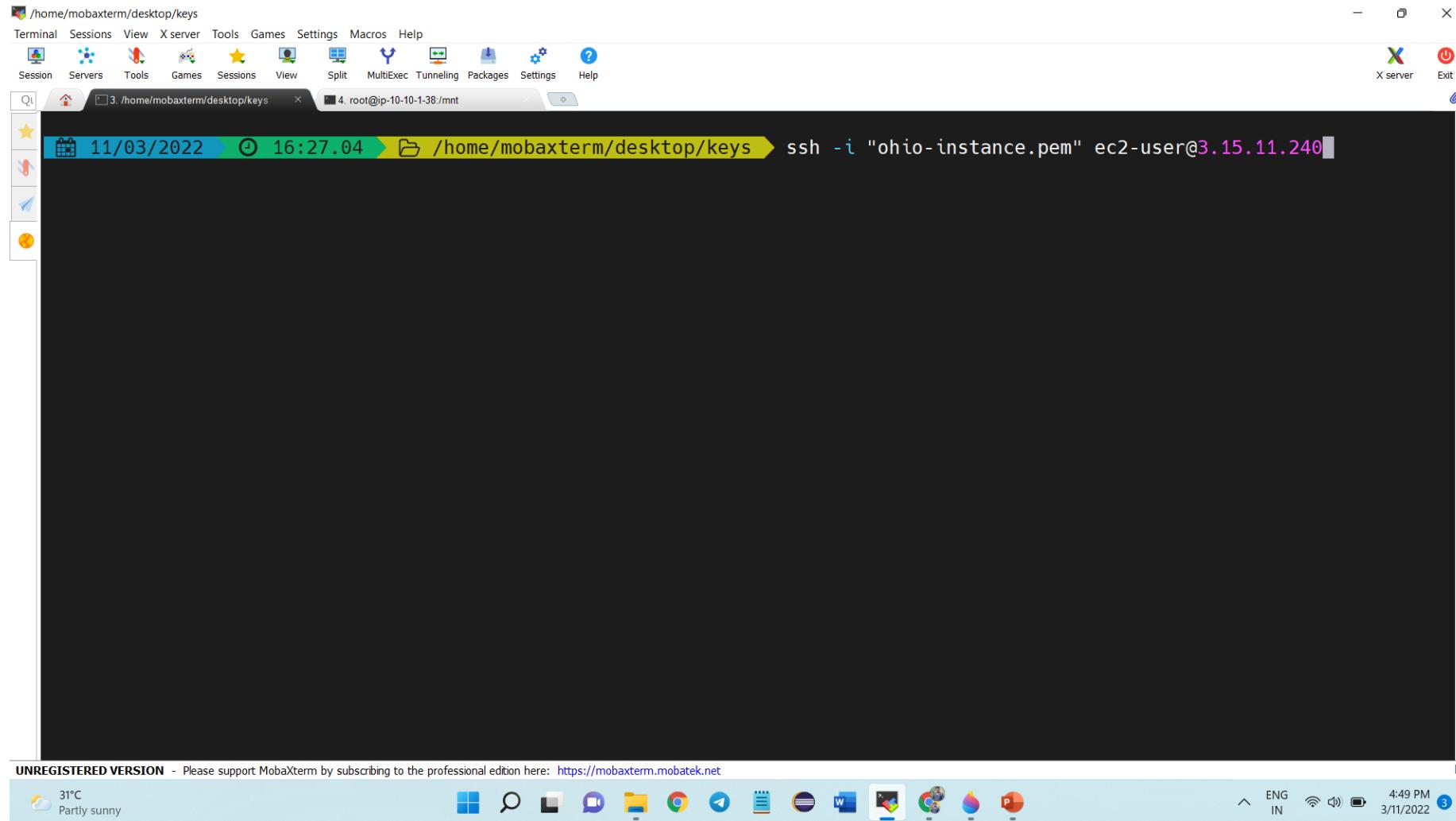
The screenshot shows the AWS EC2 Connect to instance page for an instance with ID `i-0b65c5ea53fd70be8`. The `SSH client` tab is selected. A tooltip `Command copied` is displayed above a red box containing the copied command:

```
ssh -i "ohio-instance.pem" ec2-user@3.15.11.240
```

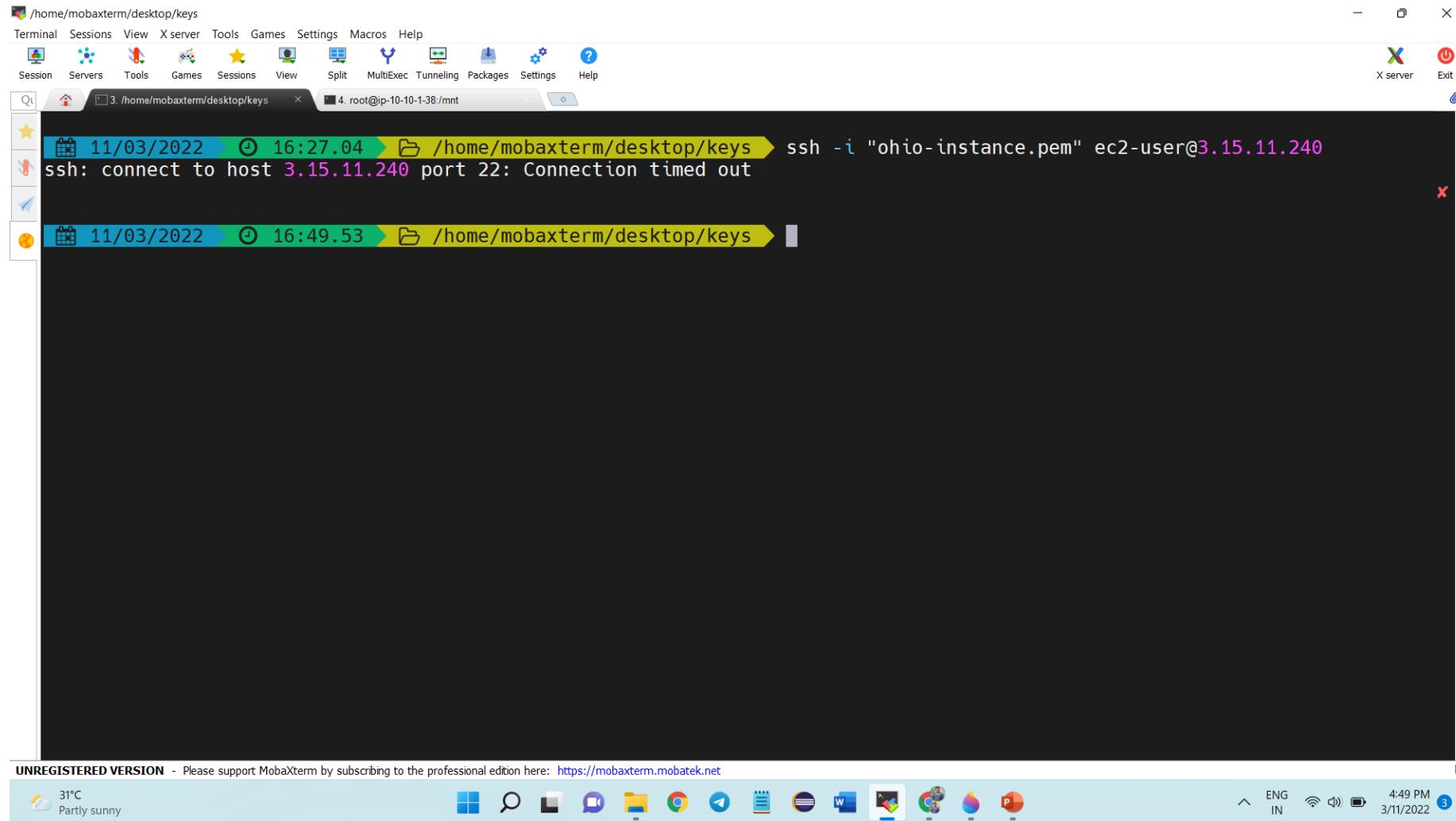
A note below the command states: `Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.`

At the bottom of the browser window, the status bar displays: `Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences`. The weather icon shows `31°C Partly sunny`. The system tray shows `ENG IN 4:48 PM 3/11/2022`.

- Copy the Last Command



- Paste in MobaxTerm
- Press Enter



- Here we can see that it shows connection time out.
- **Because we have not set Inbound and Outbound Rules into Network ACL**

The screenshot shows the AWS VPC Network ACLs page. The left sidebar is collapsed, and the main content area displays the 'Network ACLs (1/3)' table. A red box highlights the 'Devops-NACL' row, which is selected. Another red box highlights the 'Inbound rules' tab under the 'acl-0638aa5cc7139fd44 / Devops-NACL' section. A third red box highlights the 'Edit inbound rules' button in the top right corner of the Inbound rules table.

Name	Network ACL ID	Associated with	Default	VPC ID
Devops-NACL	acl-0638aa5cc7139fd44	subnet-00c1a5d0a1e14e5fe / Public-Subnet	No	vpc-0e1ea03ae4ce0d752 / devops-VPC
	acl-0c906de5a149adf1e	3 Subnets	Yes	vpc-0d530da491583e01c

**Inbound rules (1)**

Rule number	Type	Protocol	Port range	Source	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	Deny

- So go to Network ACL and Select our NACL
- Click to Inbound Rules
- Click on Edit Inbound Rules

The screenshot shows the AWS VPC Management Console with the URL [us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#EditInboundRules:networkAclId=acl-0638aa5cc7139fd44](https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#EditInboundRules:networkAclId=acl-0638aa5cc7139fd44). The page title is "Edit inbound rules". The main content area displays a table with columns: Rule number, Type, Protocol, Port range, Source, and Allow/Deny. A single row is shown with values: Rule number \* (highlighted with a red box), Type All traffic, Protocol All, Port range All, Source 0.0.0.0, and Allow/Deny Deny. Below the table are two buttons: "Add new rule" (highlighted with a red box) and "Sort by rule number". At the bottom right are "Cancel", "Preview changes", and "Save changes" buttons. The status bar at the bottom includes weather information (31°C, Partly sunny), system icons, and the date/time (3/11/2022, 4:51 PM).

- Click on Add Rule

The screenshot shows the AWS VPC Network ACL inbound rules editor. The URL in the browser is <https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#EditInboundRules:networkAclId=acl-0638aa5cc7139fd44>. The page displays two inbound rules:

Rule number	Type	Protocol	Port range	Source	Allow/Deny
1	SSH (22)	TCP (6)	22	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

At the bottom right, there are 'Cancel', 'Preview changes', and 'Save changes' buttons. The 'Save changes' button is highlighted with a red box.

- Select SSH 22 and Allow it
- Click on Save Changes

The screenshot shows the AWS VPC Network ACLs page. A green success message at the top states: "You have successfully updated inbound rules for acl-0638aa5cc7139fd44 / Devops-NACL". The "Inbound rules" tab is selected, displaying two rules:

Rule number	Type	Protocol	Port range	Source	Allow/Deny
1	SSH (22)	TCP (6)	22	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

The "Devops-NACL" row in the main table is highlighted with a red box. The "Edit inbound rules" button is visible above the rules table.

- Here our Inbound Rules are Saved.

**Now Change the Outbound Rules**

The screenshot shows the AWS VPC Network ACLs page. On the left sidebar, under the 'SECURITY' section, 'Network ACLs' is selected. In the main content area, the 'Outbound rules' tab is active. A red box highlights the 'Edit outbound rules' button. Another red box highlights the 'Devops-NACL' row in the table below.

Name	Network ACL ID	Associated with	Default	VPC ID
Devops-NACL	acl-0638aa5cc7139fd44	subnet-00c1a5d0a1e14e5fe / Public-Subnet	No	vpc-0e1ea03ae4ce0d752 / devops-VPC
-	acl-0c906de5a149adf1e	3 Subnets	Yes	vpc-0d530da491583e01c

**Outbound rules (1)**

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	Deny

- Select our Network ACL
- Click on Outbound Rules
- Click on Edit Outbound Rules

The screenshot shows the AWS VPC Management Console with the URL [us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#EditOutboundRules:networkAclId=acl-0638aa5cc7139fd44](https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#EditOutboundRules:networkAclId=acl-0638aa5cc7139fd44). The page title is "Edit outbound rules" under "acl-0638aa5cc7139fd44 / Devops-NACL". The main content area displays a table for defining outbound rules. The first row of the table has the following values:

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
*	All traffic	All	All	0.0.0.0	Deny

Below the table are two buttons: "Add new rule" (highlighted with a red box) and "Sort by rule number". At the bottom right are three buttons: "Cancel", "Preview changes", and "Save changes".

- Click on Add New Rule

The screenshot shows the AWS VPC Management Console with the URL <https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#EditOutboundRules:networkAclId=acl-0638aa5cc7139fd44>. The page title is "Edit outbound rules". The main content area displays a table of outbound rules:

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
1	Custom TCP	TCP (6)	0-65535	0.0.0.0/0	Allow

Below the table are buttons for "Add new rule" and "Sort by rule number". At the bottom right are "Cancel", "Preview changes", and a large orange "Save changes" button.

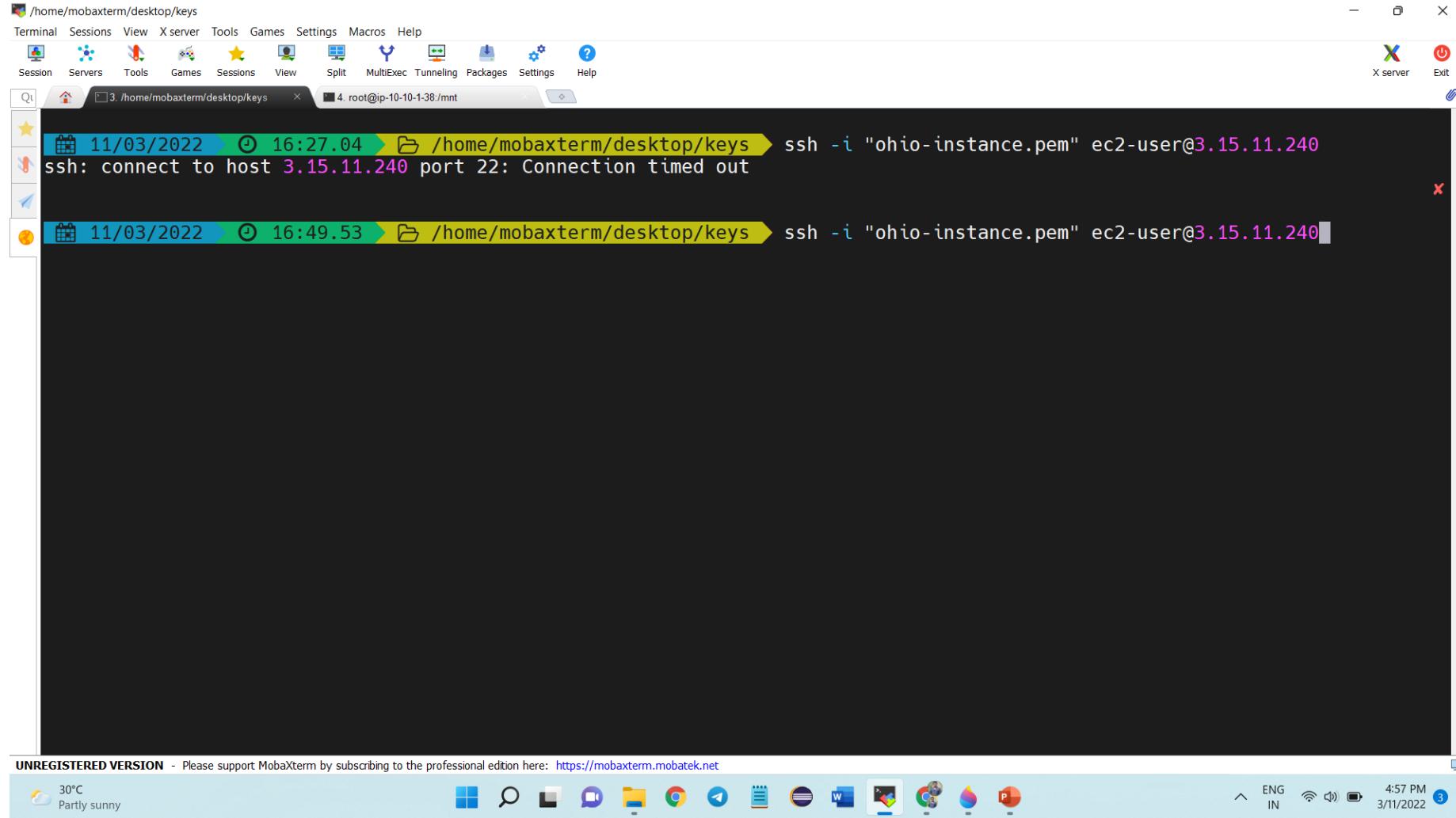
- Select Custom TCP and Port Range as 0-65535
- Click on Save Changes

The screenshot shows the AWS VPC Network ACLs page. A green success message at the top states: "You have successfully updated outbound rules for acl-0638aa5cc7139fd44 / Devops-NACL". The main table lists one Network ACL named "Devops-NACL" associated with subnet-00c1a5d0a1e14e5fe / Public-Subnet. The "Outbound rules" tab is selected, showing two rules. Rule 1 is for All TCP traffic (Protocol TCP (6), Port range All, Destination 0.0.0.0/0) and is set to Allow. Rule \* is for All traffic (Protocol All, Port range All, Destination 0.0.0.0/0) and is set to Deny. The browser address bar shows the URL https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#acl:.

Name	Network ACL ID	Associated with	Default	VPC ID
Devops-NACL	acl-0638aa5cc7139fd44	subnet-00c1a5d0a1e14e5fe / Public-Subnet	No	vpc-0e1ea03ae4ce0d752 / devops-VPC

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
1	All TCP	TCP (6)	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

- Here we can see that our outbound rules are saved successfully



- Now go inside MobaxTerm and run our Connect Command Again
- Press Enter

The screenshot shows a MobaXterm window titled "ec2-user@ip-10-10-1-12:~". The interface includes a top menu bar with options like Terminal, Sessions, View, Xserver, Tools, Games, Settings, Macros, and Help. Below the menu is a toolbar with icons for Session, Servers, Tools, Games, Sessions, View, Split, MultiExec, Tunneling, Packages, Settings, and Help. The main window contains two terminal sessions:

- Session 3:** Displays the command "ssh -i "ohio-instance.pem" ec2-user@3.15.11.240" followed by the error message "ssh: connect to host 3.15.11.240 port 22: Connection timed out".
- Session 4:** Displays the command "ssh -i "ohio-instance.pem" ec2-user@3.15.11.240" followed by the output:
  - "Warning: Permanently added '3.15.11.240' (RSA) to the list of known hosts."
  - "X11 forwarding request failed on channel 0"

Below the sessions, the terminal prompt shows the URL <https://aws.amazon.com/amazon-linux-2/> and the command "[ec2-user@ip-10-10-1-12 ~]\$".

The status bar at the bottom indicates an unregistered version, weather (30°C, Partly sunny), system icons (Windows Start, Search, Task View, File Explorer, Google Chrome, Mail, Calendar, Taskbar, Paint 3D, Photos, File History, Power), and system information (ENG IN, WiFi, Battery, 4:57 PM, 3/11/2022).

- Here now we can see that we are able to do ssh to our machine.

- So here we have seen that how **Network ACL** works as a 1<sup>st</sup> layer of firewall at Subnet level.
- Also we have to specify Inbound rules and Outbound rules Separately.

**Thanks for Doing Practical with Us**