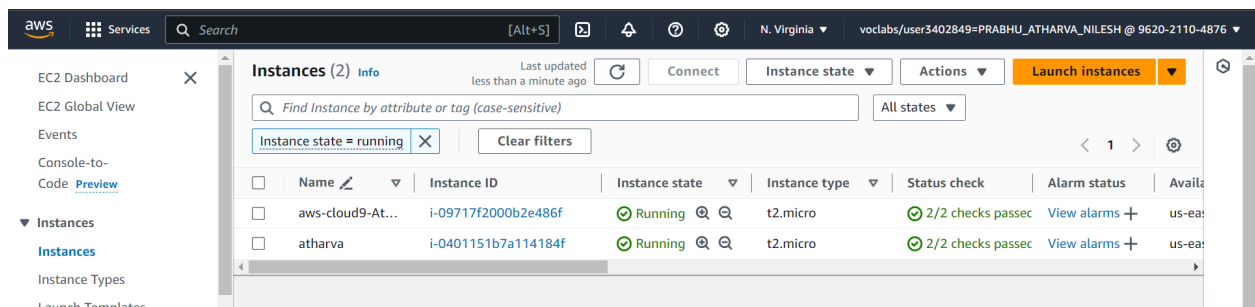
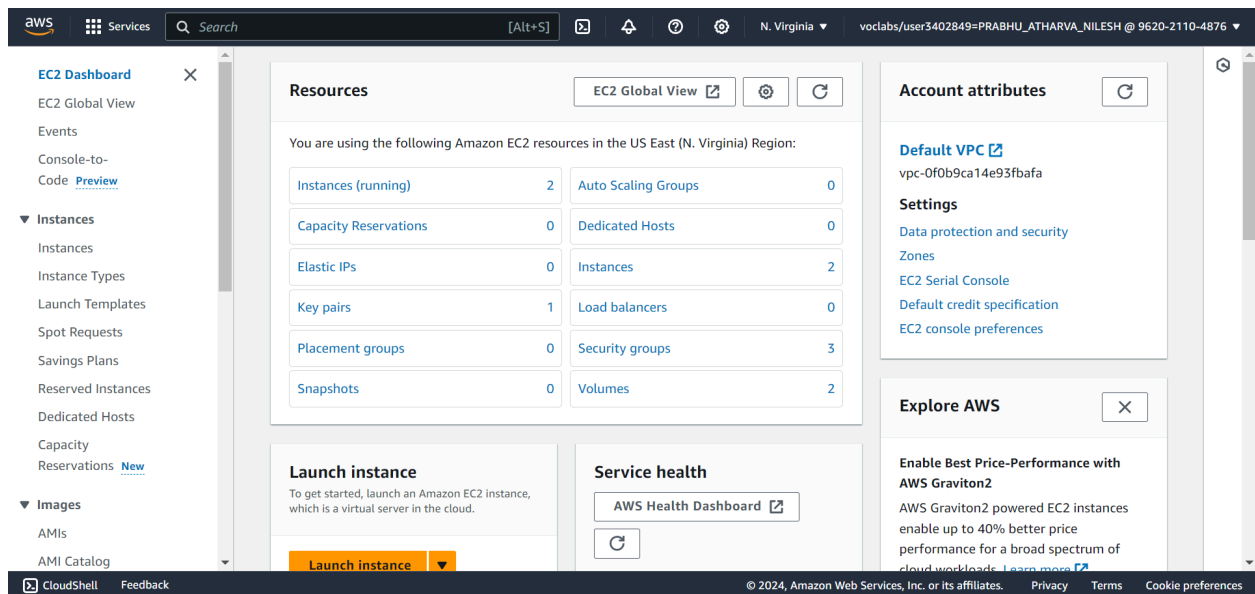
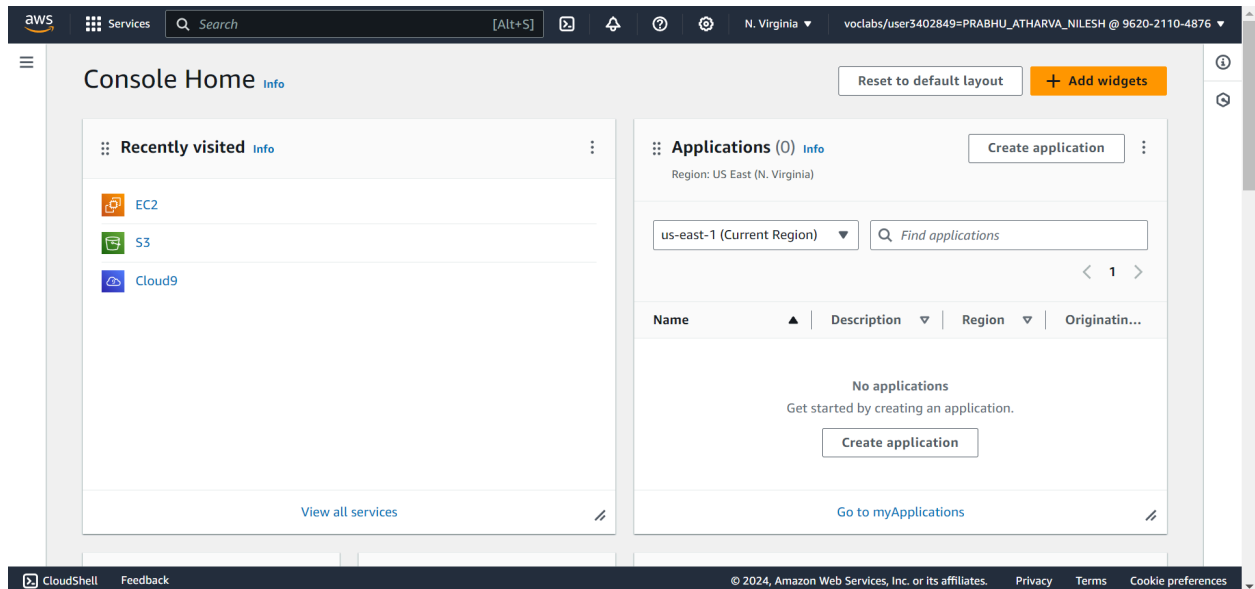


Experiment 1

Atharva Prabhu

D15A 43

1. Open AWS Academia and select launch instance



2. Execute the following commands in the aws console.

Commands :

sudo su

sudo apt install

sudo apt-get update

apt install apache2

systemctl status apache2

cd /var/www/html/

```
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1009-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/pro

System information as of Sun Aug 25 03:11:28 UTC 2024

System load:  0.09           Processes:    105
Usage of /:   23.4% of 6.71GB Users logged in:  0
Memory usage: 19%          IPv4 address for enX0: 172.31.82.107
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

Last login: Thu Aug 22 05:23:58 2024 from 18.206.107.29
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-82-107:~$ sudo su
root@ip-172-31-82-107:/home/ubuntu# sudo apt install
Reading package lists... Done
```

i-0401151b7a114184f (atharva)

PublicIPs: 54.234.233.3 PrivateIPs: 172.31.82.107

```
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@ip-172-31-82-107:/home/ubuntu# ^[[200~sudo apt-get update
sudo: command not found
root@ip-172-31-82-107:/home/ubuntu# ^[[200~sudo apt-get update
sudo: command not found
root@ip-172-31-82-107:/home/ubuntu# sudo apt-get update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [323 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [463 kB]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [114 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [7192 B]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [337 kB]
Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [142 kB]
Get:19 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [45.0 kB]
Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [13.6 kB]
Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [280 kB]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [54.8 kB]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 c-n-f Metadata [416 B]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [14.1 kB]
```

i-0401151b7a114184f (atharva)

PublicIPs: 54.234.233.3 PrivateIPs: 172.31.82.107

```
aws Services Search [Alt+S] N. Virginia voclabs/user3402849=PRABHU_ATHARVA_NILESH @ 9620-2110-487

Get:25 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [3608 B]
Get:26 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [212 B]
Get:27 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 c-n-f Metadata [532 B]
Get:28 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Get:29 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 c-n-f Metadata [112 B]
Get:30 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Packages [10.3 kB]
Get:31 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe Translation-en [10.5 kB]
Get:32 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [17.6 kB]
Get:33 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 c-n-f Metadata [1016 B]
Get:34 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:35 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 c-n-f Metadata [116 B]
Get:36 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Get:37 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 c-n-f Metadata [116 B]
Get:38 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [73.1 kB]
Get:39 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [4220 B]
Get:40 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [252 kB]
Get:41 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [109 kB]
Get:42 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [1632 B]
Get:43 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [9756 B]
Get:44 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [280 kB]
Get:45 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [54.8 kB]
Get:46 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 c-n-f Metadata [420 B]
Get:47 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Packages [10.6 kB]
Get:48 http://security.ubuntu.com/ubuntu noble-security/multiverse Translation-en [2808 B]
Get:49 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Get:50 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [344 B]
Patched 28.6 MB in 6s (5118 kB/s)
Reading package lists... Done
root@ip-172-31-82-107:/home/ubuntu# ^[[200-apt install apache2
apt: command not found
root@ip-172-31-82-107:/home/ubuntu# apt install apache2
Reading package lists... Done

i-0401151b7a114184f (atharva)
PublicIPs: 54.234.233.3 PrivateIPs: 172.31.82.107
```

```
aws Services Search [Alt+S] N. Virginia voclabs/user3402849=PRABHU_ATHARVA_NILESH @ 9620-2110-487

Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libaprilt64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64 liblua5.4-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libaprilt64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64 liblua5.4-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 100 not upgraded.
Need to get 2083 kB of archives.
After this operation, 8094 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprilt64 amd64 1.7.2-3.1build2 [107 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1t64 amd64 1.6.3-1.lubuntu7 [91.9 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.3-1.lubuntu7 [11.2 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-ldap amd64 1.6.3-1.lubuntu7 [9116 B]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 liblua5.4-0 amd64 5.4.6-3build2 [166 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-bin amd64 2.4.58-1ubuntu8.4 [1329 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-data all 2.4.58-1ubuntu8.4 [163 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-utils amd64 2.4.58-1ubuntu8.4 [97.1 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2 amd64 2.4.58-1ubuntu8.4 [90.2 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 ssl-cert all 1.1.2ubuntu1 [17.8 kB]
Patched 2083 kB in 0s (34.4 MB/s)
Preconfiguring packages ...
Selecting previously unselected package libaprilt64:amd64.
(Reading database ... 67739 files and directories currently installed.)
Preparing to unpack .../0-libaprilt64_1.7.2-3.1build2_amd64.deb ...
Unpacking libaprilt64:amd64 (1.7.2-3.1build2) ...
Selecting previously unselected package libaprutil1t64:amd64.
Preparing to unpack .../1-libaprutil1t64_1.6.3-1.lubuntu7_amd64.deb ...
Unpacking libaprutil1t64:amd64 (1.6.3-1.lubuntu7) ...
Selecting previously unselected package libaprutil1-dbd-sqlite3:amd64.
```

```
Preparing to unpack .../2-libaprutil1-dbd-sqlite3 1.6.3-1.lubuntu7_amd64.deb ...
Unpacking libaprutil1-dbd-sqlite3:amd64 (1.6.3-1.lubuntu7) ...
Selecting previously unselected package libaprutil1-ldap:amd64.
Preparing to unpack .../3-libaprutil1-ldap 1.6.3-1.lubuntu7_amd64.deb ...
Unpacking libaprutil1-ldap:amd64 (1.6.3-1.lubuntu7) ...
Selecting previously unselected package liblua5.4-0:amd64.
Preparing to unpack .../4-liblua5.4-0 5.4.6-3build2_amd64.deb ...
Unpacking liblua5.4-0:amd64 (5.4.6-3build2) ...
Selecting previously unselected package apache2-bin.
Preparing to unpack .../5-apache2-bin 2.4.58-lubuntu8.4_amd64.deb ...
Unpacking apache2-bin (2.4.58-lubuntu8.4) ...
Selecting previously unselected package apache2-data.
Preparing to unpack .../6-apache2-data 2.4.58-lubuntu8.4_all.deb ...
Unpacking apache2-data (2.4.58-lubuntu8.4) ...
Selecting previously unselected package apache2-utils.
Preparing to unpack .../7-apache2-utils 2.4.58-lubuntu8.4_amd64.deb ...
Unpacking apache2-utils (2.4.58-lubuntu8.4) ...
Selecting previously unselected package apache2.
Preparing to unpack .../8-apache2 2.4.58-lubuntu8.4_amd64.deb ...
Unpacking apache2 (2.4.58-lubuntu8.4) ...
Selecting previously unselected package ssl-cert.
Preparing to unpack .../9-ssl-cert 1.1.2ubuntu1_all.deb ...
Unpacking ssl-cert (1.1.2ubuntu1) ...
Setting up ssl-cert (1.1.2ubuntu1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/ssl-cert.service → /usr/lib/systemd/system/ssl-cert.service.
Setting up libapr1t64:amd64 (1.7.2-3.1build2) ...
Setting up liblua5.4-0:amd64 (5.4.6-3build2) ...
Setting up apache2-data (2.4.58-lubuntu8.4) ...
Setting up libaprutil1t64:amd64 (1.6.3-1.lubuntu7) ...
Setting up libaprutil1-ldap:amd64 (1.6.3-1.lubuntu7) ...
Setting up libaprutil1-dbd-sqlite3:amd64 (1.6.3-1.lubuntu7) ...
Setting up apache2-utils (2.4.58-lubuntu8.4) ...
Setting up apache2-bin (2.4.58-lubuntu8.4) ...
```

i-0401151b7a114184f (atharva)

PublicIPs: 54.234.233.3 PrivateIPs: 172.31.82.107

```
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@ip-172-31-82-107:/home/ubuntu# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Sun 2024-08-25 03:15:58 UTC; 1min 50s ago
     Docs: https://httpd.apache.org/docs/2.4/
  Main PID: 2310 (apache2)
    Tasks: 55 (limit: 1130)
   Memory: 5.3M (peak: 5.4M)
      CPU: 41ms
   CGroup: /system.slice/apache2.service
           └─2310 /usr/sbin/apache2 -k start
             └─2312 /usr/sbin/apache2 -k start
               └─2314 /usr/sbin/apache2 -k start

Aug 25 03:15:58 ip-172-31-82-107 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Aug 25 03:15:58 ip-172-31-82-107 systemd[1]: Started apache2.service - The Apache HTTP Server.
root@ip-172-31-82-107:/home/ubuntu# cd /var/www/html/
root@ip-172-31-82-107:/var/www/html#
```

i-0401151b7a114184f (atharva)

PublicIPs: 54.234.233.3 PrivateIPs: 172.31.82.107

3.Edit the inbound and outbound rules.

EC2 Dashboard

EC2 Global View

Events

Console-to-Code

Preview

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity

Reservations

New

▼ Images

AMIs

AMI Catalog

▼ Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

EC2 > Security Groups > sg-027fc9d1716e3904f - launch-wizard-1

sg-027fc9d1716e3904f - launch-wizard-1

Actions

Details

Security group name

launch-wizard-1

Security group ID

sg-027fc9d1716e3904f

Description

launch-wizard-1 created 2024-08-01T09:31:31.596Z

VPC ID

vpc-0f0b9ca14e93fbafa

Owner

962021104876

Inbound rules count

1 Permission entry

Outbound rules count

1 Permission entry

Inbound rules

Outbound rules

Tags

Inbound rules (1)

Manage tags

Edit inbound rules

Search

< 1 > ⌕

<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range	Source
<input type="checkbox"/>	-	sgr-0a294f7b728e86bb4	IPv4	HTTP	TCP	80	0.0.0.0/0

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

EC2 Dashboard

EC2 Global View

Events

Console-to-Code

Preview

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity

Reservations

New

▼ Images

AMIs

AMI Catalog

▼ Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

EC2 > Security Groups > sg-027fc9d1716e3904f - launch-wizard-1

sg-027fc9d1716e3904f - launch-wizard-1

Actions

Details

Security group name

launch-wizard-1

Security group ID

sg-027fc9d1716e3904f

Description

launch-wizard-1 created 2024-08-01T09:31:31.596Z

VPC ID

vpc-0f0b9ca14e93fbafa

Owner

962021104876

Inbound rules count

1 Permission entry

Outbound rules count

1 Permission entry

Inbound rules

Outbound rules

Tags

Outbound rules (1)

Manage tags

Edit outbound rules

Search

< 1 > ⌕

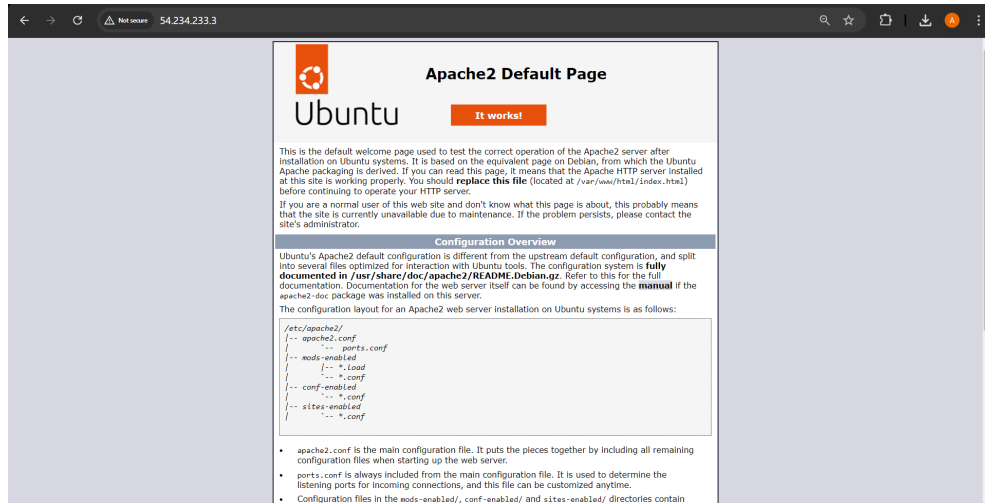
<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range	Destination
<input type="checkbox"/>	-	sgr-0875dd8762f2a189c	IPv4	HTTP	TCP	80	0.0.0.0/0

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

4. This is the hosted Static Website.



Static Site Hosting using S3 bucket

1. Visit S3 under the developer tools and create a Bucket. Click on the Edit Static Website Hosting under the properties tab

Amazon S3 > Buckets > atharva45554 > Edit static website hosting

Edit static website hosting [Info](#)

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

☐ Disable

☒ Enable

Hosting type

☒ Host a static website

Use the bucket endpoint as the web address. [Learn more](#)

☐ Redirect requests for an object

Redirect requests to another bucket or domain. [Learn more](#)

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#)

Index document

Specify the home or default page of the website.

index.html

Error document - *optional*

This is returned when an error occurs.

404.html

2. Upload a file

Upload succeeded

View details below.

Upload: status

Close

The information below will no longer be available after you navigate away from this page.

Summary

Destination

s3://atharva45554

Succeeded

1 file, 2.8 KB (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration


Files and folders (1 Total, 2.8 KB)

Find by name

< 1 >

Name	Folder	Type	Size	Status	Error
index.html	-	text/html	2.8 KB	Succeeded	-

3. Click on the Edit block public access under the Permissions tab



[Amazon S3](#) > [Buckets](#) > [atharva45554](#) > Edit Block public access (bucket settings)

Edit Block public access (bucket settings) [Info](#)

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☐

Block *all* public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐

Block public access to buckets and objects granted through *new* access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐

Block public access to buckets and objects granted through *any* access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

☐

Block public access to buckets and objects granted through *new* public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐


Block public and cross-account access to buckets and objects through *any* public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Cancel

Save changes

4. Click on Object Ownership under Permission Tab




Edit Object Ownership [Info](#)


Object Ownership

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☐ **ACLs disabled (recommended)**
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☒ **ACLs enabled**
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

 We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.



 **Enabling ACLs turns off the bucket owner enforced setting for Object Ownership**
Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.

☐ I acknowledge that ACLs will be restored.

Object Ownership

☒ **Bucket owner preferred**
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

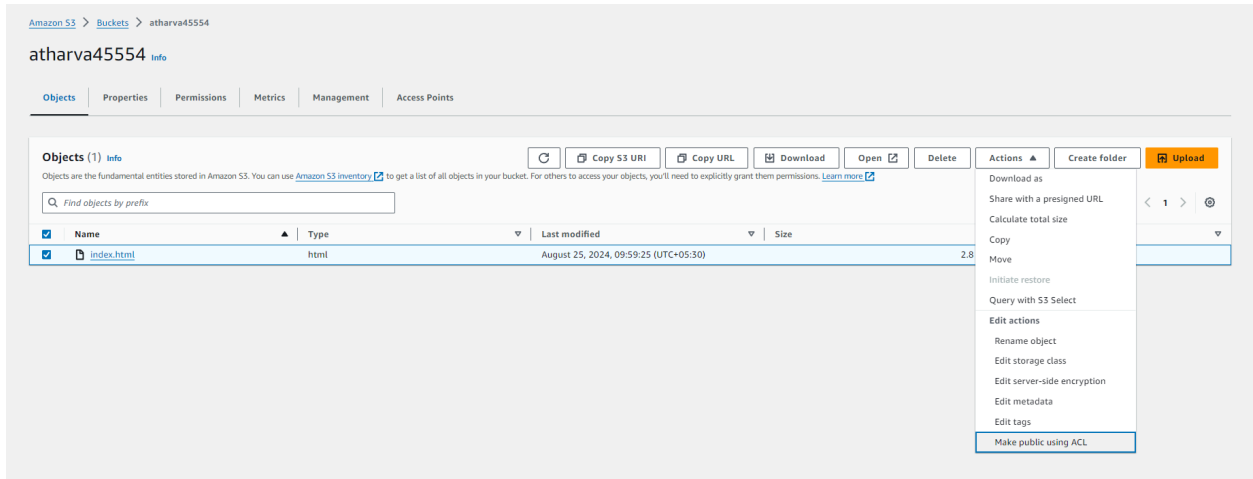
☐ **Object writer**
The object writer remains the object owner.

 If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#) 

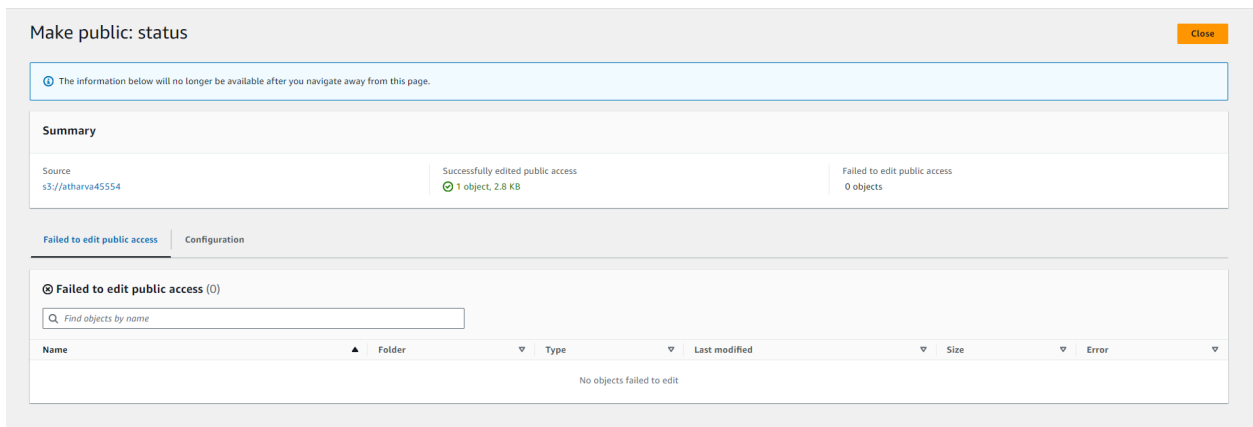
Cancel

Save changes

5. Select the file and click on Actions and select the option Make Public using ACL from the dropdown



6. Select on Make Public



7. Visit the domain and the website hosted.



Custom T-Shirt Order Form

T-Shirt Details

Tagline on the Shirt: Color: Size: Quantity: Delivery Date:

Delivery Details

Recipient's Name: Address: Email: Phone Number:

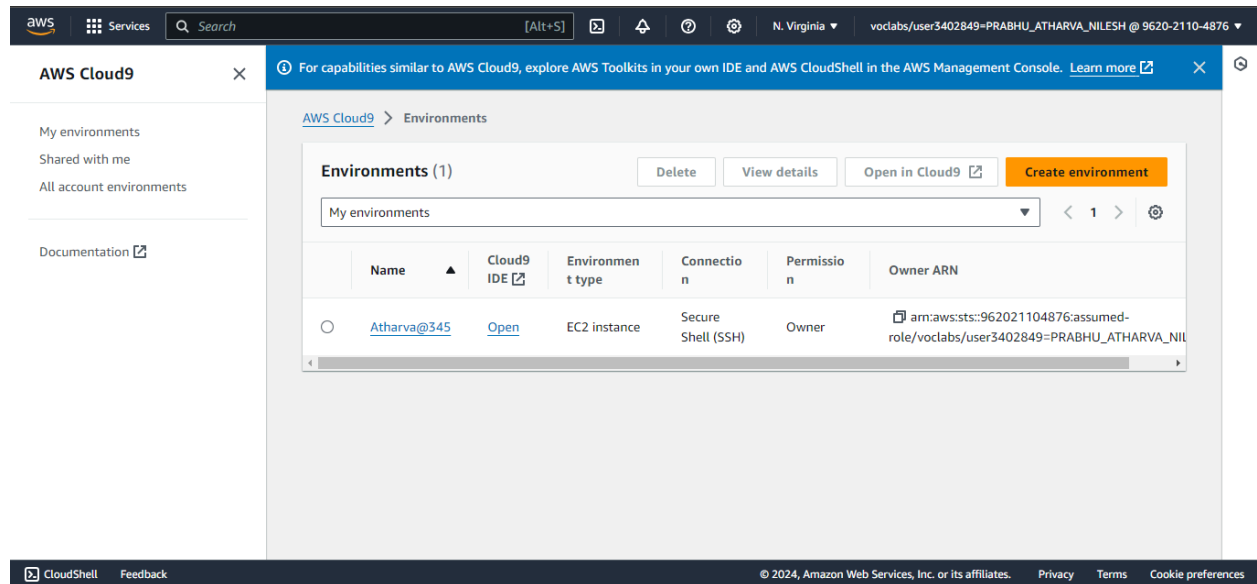
Additional Comments:

Place Order

Reset Form

Cloud 9 IDE Site Hosting

Step 1: Create Environment



Step 2 :Open the Environment IDE and add the code and run the code

