

1. EC2 Basics Lab

- **Objective:** To understand the process of setting up and managing an Amazon EC2 instance.
- **Approach:** Students will start by launching a new EC2 instance, selecting an appropriate instance type and configuring the instance details. They will then create and configure a new Security Group, and allocate an Elastic IP address to the instance. The lab will also include connecting to the instance via SSH.
- **Goal:** By the end of this lab, students should be able to launch and manage an EC2 instance, understand instance types, security groups, and IP addressing in AWS.

=====

BASIC STEPS

1. Open the AWS Console and click EC2

Give the EC2 instance name

following the simple steps below.

Name and tags [Info](#)


Name

[Add additional tags](#)

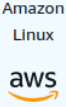
2. Select OS images and AMI


▼ Application and OS Images (Amazon Machine Image) [Info](#)


An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below


 Search our full catalog including 1000s of application and OS Images


Quick Start


**Amazon Linux**


**macOS**

**Ubuntu**

**Windows**

**Red Hat**

**SUSE Linux**

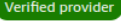

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI Free tier eligible ▼
ami-0e9107ed11be76fde (64-bit (x86), uefi-preferred) / ami-0cb6fec6f40971379 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.3.20240117.0 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	
64-bit (x86) ▼	uefi-preferred	ami-0e9107ed11be76fde	

3. Select instance type as t2.micro

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.0716 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

☒ All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Select



[Create new key pair](#)

Select key pair login

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

vockey



[Create new key pair](#)

4. Select create security group and edit the rules

▼ Network settings

Info

Edit

Network

Info

vpc-00e811aee63173e5d

Subnet

Info

No preference (Default subnet in any availability zone)

Auto-assign public IP

Info

Enable

Firewall (security groups)

Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group
 ☐ Select existing security group

5. Disable auto assign public ip

Auto-assign public IP

Info

Disable

▼

Firewall (security groups)

Info

6. Click launch instance to create new EC2 instance

Cancel

Launch instance

Review commands

7. The instance is now created

Instances (1)

Info

↺

Connect

Instance st

Find Instance by attribute or tag (case-sensitive)

Any state ▼

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	techcraftinsta...	i-0a283d1a1c82bc1b4	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1b


8. Not assign any ip for the EC2 instance

Instance: i-0a283d1a1c82bc1b4 (techcraftinstance)

[Details](#) | [Status and alarms ^{New}](#) | [Monitoring](#) | [Security](#) | [Networking](#) | [Storage](#) | [Tags](#)

▼ Instance summary [Info](#)

Instance ID

 i-0a283d1a1c82bc1b4 (techcraftinstance)

IPv6 address

—

Hostname type

IP name: ip-172-31-40-203.ec2.internal

Answer private resource DNS name

IPv4 (A)

[Auto-assign IP address](#)

Public IPv4 address

—

Instance state

 **Running**

Private IP DNS name (IPv4 only)

 ip-172-31-40-203.ec2.internal

Instance type

t2.micro

[View IP](#)

Private IPv4 addresses

 172.31.40.203

Public IPv4 DNS

—

Elastic IP addresses

—

[AWS Compute Optimizer findings](#)

- Now assigning the Elastic IP address
- Select Elastic IPs


[Security Groups](#)


[Elastic IPs](#)

[Placement Groups](#)

[Key Pairs](#)

- Select Allocate Elastic IP address

 **Actions** ▼ **Allocate Elastic IP address**

< 1 > 

Order	Associated instance ID	Private IP address
IP addresses found in this Region		

- Select IPv4 to set IP address

Allocate Elastic IP address [Info](#)

Elastic IP address settings [Info](#)

Network Border Group [Info](#)

us-east-1

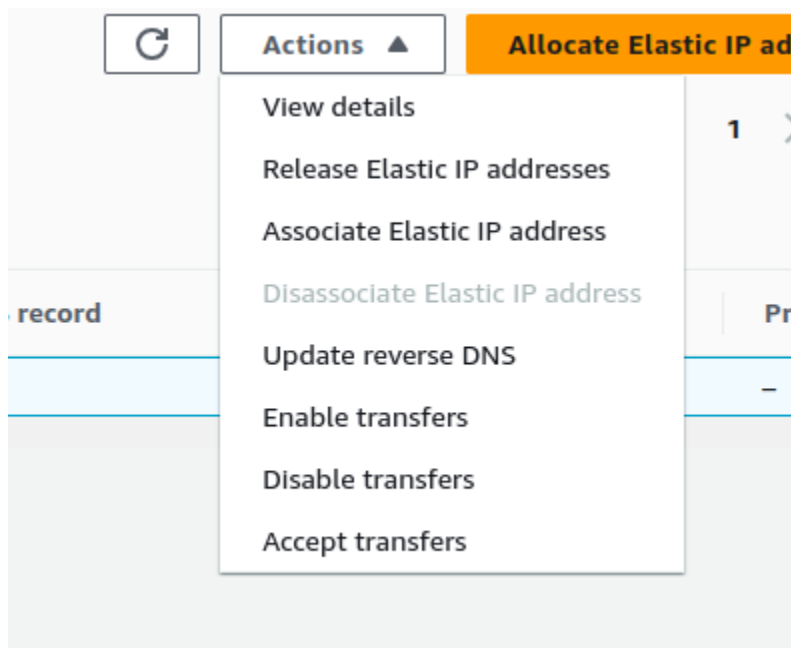
Public IPv4 address pool

- ☒ Amazon's pool of IPv4 addresses
- ☐ Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) [Learn more](#)
- ☐ Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (option disabled because no customer owned pools found) [Learn more](#)

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. To

12. Keep the created ipv4 selected and click action and select associate elastic ip address



13. Select the EC2 instance and click associate

Choose the instance or network interface to associate to this Elastic IP address (34.202.134.119)

Elastic IP address: 34.202.134.119

Resource type
Choose the type of resource with which to associate the Elastic IP address.

☒ Instance

☐ Network Interface

⚠ If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. [Learn more](#)

If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

Instance



Private IP address
The private IP address with which to associate the Elastic IP address.

Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.


☐ Allow this Elastic IP address to be reassociated

14. Now we can see the EC2 is assign an IP

Public IPv4 address

 34.202.134.119 | [open address](#) 

Instance state

 **Running**

15. To connect to the ec2 instance via ssh download the pem file in the aws details

No running instance

SSH key

AWS SSO

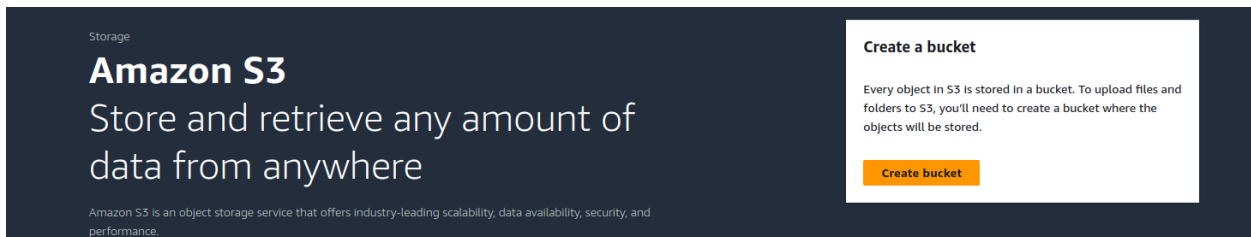
2. S3 Storage Fundamentals Lab

- **Objective:** To gain hands-on experience with Amazon S3 by performing basic storage operations.
- **Approach:** This lab involves creating an S3 bucket, uploading files to it, and setting up bucket policies for access control. Students will explore the S3 management console, learn about object storage, and understand the concepts of buckets and objects.
- **Goal:** Students will understand how to use S3 for storing and managing data, learn about S3 security and permissions, and become familiar with S3's user interface.

#####

BASIC STEPS

1. Go to the AWS Console Management and select S3
Click create bucket to create the S3 bucket



2. Choose the bucket name the bucket name must be unique

General configuration

AWS Region

US East (N. Virginia) us-east-1

Bucket type [Info](#)

☒ General purpose

Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ Directory - *New*

Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)

myfirstbucketat

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix

3. Click create bucket

to the bucket, and configure additional bucket settings.

Cancel

Create bucket

4. Bucket is now created

[General purpose buckets](#) [Directory buckets](#)

General purpose buckets (1) [Info](#)

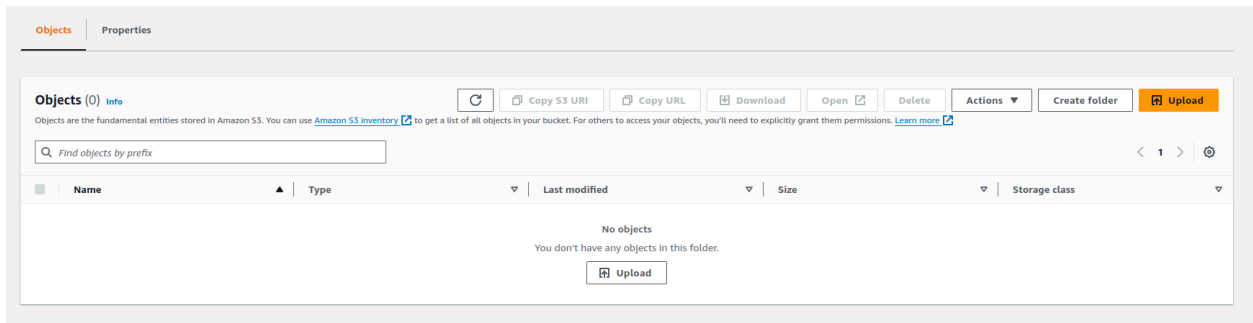
[Buckets are containers for data stored in S3. \[Learn more\]\(#\)](#)

[Refresh](#) [Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

< 1 > [Filter](#)

Name	AWS Region	Access	Creation date
<input type="radio"/> myfirstbucketat	US East (N. Virginia) us-east-1	Objects can be public	January 22, 2024, 16:55:10 (UTC+05:45)

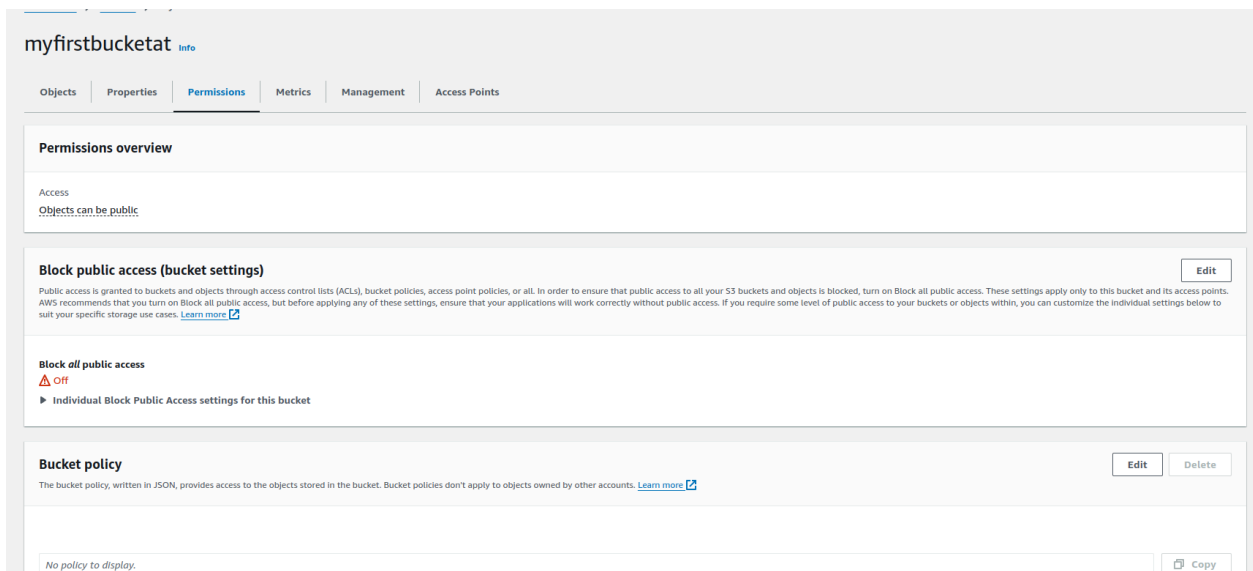
5. Click upload to upload the file



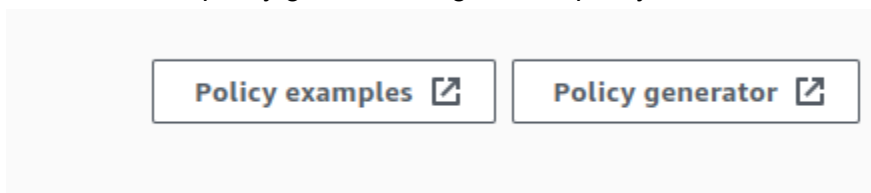
6. File is uploaded

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	labsuser.pem	pem	January 22, 2024, 16:58:55 (UTC+05:45)	1.6 KB	Standard

- To set the policies click the bucket name and select permission tab and you can see the Bucket policy now click edit to set the polices to the bucket



8. Click to policy generator to generate policy



9. Add necessary policy and click to add Statement

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to [Amazon Web Services \(AWS\)](#) products and resources. For more information about [concepts in Using AWS Identity and Access Management](#). Here are [sample policies](#).

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See [a description of elements](#) that you can use in statements.

Effect ☒ Allow ☐ Deny

Principal
Use a comma to separate multiple values.

AWS Service Amazon S3 ☐ All Services (*)
Use multiple statements to add permissions for more than one service.

Actions 1 Action(s) Selected ☐ All Actions (*)

Amazon Resource Name (ARN) arn:aws:s3::myfirstbucketat
ARN should follow the following format: arn:aws:s3:::{BucketName}/{Key(KeyName)}.
Use a comma to separate multiple values.

[Add Conditions \(Optional\)](#)

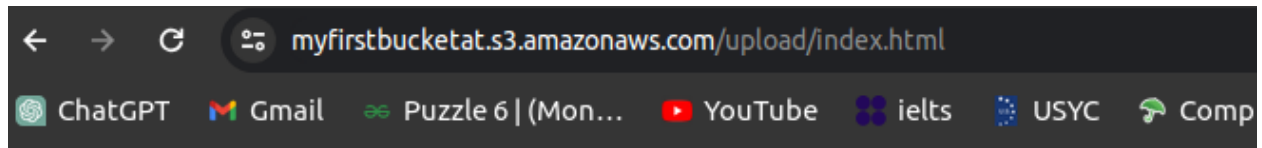
10. Now place the generated JSON in the policy and click save changes

```
1 {  
2   "Id": "Policy1705933731096",  
3   "Version": "2012-10-17",  
4   "Statement": [  
5     {  
6       "Sid": "Stmnt1705933707120",  
7       "Action": [  
8         "s3:GetObject"  
9       ],  
10      "Effect": "Allow",  
11      "Resource": "arn:aws:s3:::myfirstbucketat",  
12      "Principal": ""  
13    }  
14  ]  
15 }
```

Edit statement

Select an element

11. Now access the bucket through public URL



Hello Amazon Web Services (AWS)

This is a simple HTML page to greet AWS!

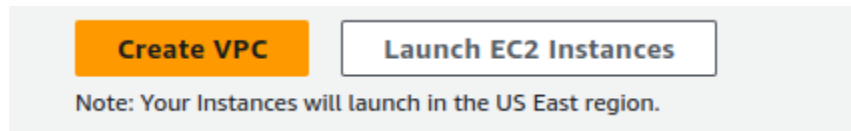
3. VPC Configuration Lab

- **Objective:** To understand the fundamentals of AWS networking through the configuration of a Virtual Private Cloud (VPC).
- **Approach:** Students will create a new VPC, add subnets, set up an Internet Gateway, and configure route tables. The lab might also include setting up a simple EC2 instance within this VPC to demonstrate how resources are deployed in a custom network environment.
- **Goal:** By the end of this lab, students should be able to create and configure a VPC, understand subnetting, and the role of route tables and internet gateways in AWS.

#####

BASIC STEPS

1. Open AWS Console and search for VPC and click create VPC



2. Configure the VPC details in the *VPC settings* panel on the left:

Click VPC and more

Choose VPC and more.

Under Name tag auto-generation, keep *Auto-generate* selected, however change the value from project to lab.

Keep the IPv4 CIDR block set to 10.0.0.0/16

For Number of Availability Zones, choose 1.

For Number of *public* subnets, keep the 1 setting.

For Number of *private* subnets, keep the 1 setting.

Name tag auto-generation [Info](#)

Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☒ Auto-generate

lab

IPv4 CIDR block [Info](#)

Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16

65,536 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block

☐ Amazon-provided IPv6 CIDR block

Tenancy [Info](#)

Default

Number of Availability Zones (AZs) [Info](#)

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1

2

3

► Customize AZs

Number of public subnets [Info](#)

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0

1

Number of private subnets [Info](#)

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0

1

2

3. Expand the Customize subnets CIDR blocks section

Change Public subnet CIDR block in us-east-1a to 10.0.0.0/24

Change Private subnet CIDR block in us-east-1a to 10.0.1.0/24

Set NAT gateways to In 1 AZ.

Set VPC endpoints to None.

Keep both DNS hostnames and DNS resolution *enabled*.

▼ Customize subnets CIDR blocks

Public subnet CIDR block in us-east-1a

10.0.0.0/24

256 IPs

< > ^ v

Private subnet CIDR block in us-east-1a

10.0.1.0/24

256 IPs

NAT gateways (\$) [Info](#)

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None

In 1 AZ

1 per AZ

VPC endpoints [Info](#)

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None

S3 Gateway

DNS options [Info](#)

☒ Enable DNS hostnames

☒ Enable DNS resolution

4. Now click to create VPC the VPC will be created after some time

VPC > Your VPCs > vpc-02a527fc1c9ef3602

vpc-02a527fc1c9ef3602 / lab-vpc

Details [Info](#)

VPC ID vpc-02a527fc1c9ef3602	State Available	DNS hostnames Enabled
Tenancy Default	DHCP option set dopt-07906611f00af17a1	Main route table rtb-0c672f0a4af9d38d6
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -

5. To add subnet click to subnet in left panel


Subnets

Route tables

Internet gateways

Egress-only internet

6. Click to create subnet



Actions ▾

Create subnet

< 1 > ⚙

▼	IPv6 CIDR	▼	Available IPv4
---	-----------	---	----------------

7.

7. Select the created VPC

VPC ID

Create subnets in this VPC.

vpc-02a527fc1c9ef3602 (lab-vpc) ▾

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

8. Now give subnet name, availability zone, and add the IPv4-CIDR subnet

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block [Info](#)

Choose the IPv4 VPC CIDR block to create a subnet in.

IPv4 subnet CIDR block

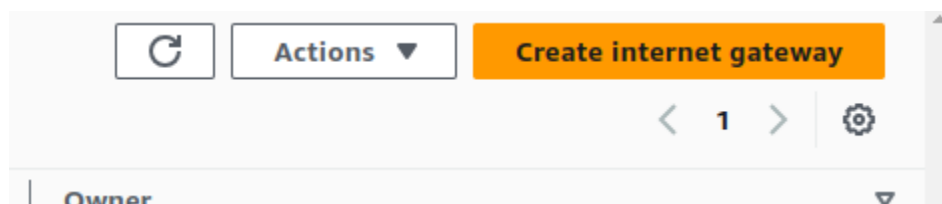
< > ^ v

▼ Tags - optional

Again do same to create another subnet for with different CIDR block id you can see newly created private and public subnet

<input type="checkbox"/>	lab-subnet-private1-us-east-1a	subnet-0c603c3
<input type="checkbox"/>	lab-subnet-public1-us-east-1a	subnet-03188ab
<input type="checkbox"/>	lab-subnet_public2	subnet-022f5c2
<input type="checkbox"/>	lab-subnetprivate2	subnet-04b0887

9. To setup the internet gateway select my vpc and in the left bar click internet gateway click create gateway to create



10. Now to configure the route table click route tables in the left navigation panel and select lab-rtb-private1-us-east-1a

<input checked="" type="checkbox"/>	lab-rtb-private1-us-east-1a	rtb-0d119cc37267cb54f	subnet-0c603c33bd12c4...
-------------------------------------	-----------------------------	---------------------------------------	--

11. In the lower panel choose routes

rtb-0d119cc37267cb54f / lab-rtb-private1-us-east-1a

Details	Routes	Subnet associations	Edge associations	Route propagation	Tags
----------------	--------	---------------------	-------------------	-------------------	------

12. Choose subnet association and click edit subnet association and click explicit subnet association

Details	Routes	Subnet associations	Edge associations	Route propagation	Tags
Explicit subnet associations (1)					
<input type="text" value="Find subnet association"/>					
<div>1</div>					
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR		
lab-subnet-private1-us-east-1a	subnet-0c603c33bd12c43c1	10.0.1.0/24	-		

13. Leave lab-rtb-private1-us-east-1a selected and select lab-subnetprivate2 and do same for public subnet

<input type="text" value="Filter subnet associations"/>			
<input type="checkbox"/>	lab-subnet_public2	subnet-022f5c2900d527d83	10.0.2.0/24
<input checked="" type="checkbox"/>	lab-subnet-private1-us-east-1a	subnet-0c603c33bd12c43c1	10.0.1.0/24
<input type="checkbox"/>	lab-subnet-public1-us-east-1a	subnet-03188ab975a79163e	10.0.0.0/24
<input checked="" type="checkbox"/>	lab-subnetprivate2	subnet-04b088789261c30cd	10.0.3.0/24
Selected subnets			

14. Create security group with necessary rule for the vpc

VPC > Security Groups > sg-065c508b012ddd605 - mywebgroup

sg-065c508b012ddd605 - mywebgroup

Details

Security group name mywebgroup	Security group ID sg-065c508b012ddd605	Description Enable HTTP access	VPC ID vpc-02a527fc1c9ef3602
Owner 866388144037	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules

Outbound rules

Tags

15. Now create a EC2 instance with the created security group and the vpc
And launch by some code in user data box and go back to the cretated
instance when status shows 2 check pass select the instance and get the
public IP

	mytestinstance	i-0bb102c4024244ff8		t2.micro		View alarms	us-east-1b	ec2-54-80-250-63.com...	54.80...
--	----------------	---------------------	--	----------	--	-----------------------------	------------	-------------------------	----------

4. IAM Users and Roles Lab

- **Objective:** To understand AWS Identity and Access Management (IAM) by creating and managing users, groups, and roles.
- **Approach:** Students will create new IAM users, assign them to groups, and apply policies to manage permissions. The lab will also involve creating roles for AWS services and understanding the use of IAM roles for cross-service access.
- **Goal:** Students will learn about user and permission management in AWS, the importance of roles for security and best practices for IAM.

#####

BASIC STEPS

We Can’t create any groups and assign the policy, so I used the foundation course lab to assign the user with groups

1. Create a IAM User first, to create this, open the AWS Console Management tab and search for IAM. Click the User on the left side and create IAM user with necessary attribute

Specify user details

User details


User name

helloworld

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☐ Provide user access to the AWS Management Console - *optional*

If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Cent

 If you are creating programmatic access through access keys or service-specific credentials f

2. Attach the policy for that user, you have to select attach policies directly radio button to do so

Permissions options

☐ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.


☒ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.





Permissions policies (1178)

Choose one or more policies to attach to your new user.

Filter by Type

All types

< 1 2 3 4 5 6 7 ... 59 > 

<input type="checkbox"/>	Policy name 	Type	Attached entities
<input type="checkbox"/>	 AccessAnalyzerServiceRolePolicy	AWS managed	0
<input type="checkbox"/>	 AdministratorAccess	AWS managed - job function	.1
<input type="checkbox"/>	 AdministratorAccess-Amplify	AWS managed	0

3. Click to create user to create user

Cancel

Previous

Create user

These are the users

<input type="checkbox"/>	user-1	/spl66/	0	-	-	✓ 13 minutes	-	Active - AKIA
<input type="checkbox"/>	user-2	/spl66/	0	-	-	✓ 13 minutes	-	Active - AKIA
<input type="checkbox"/>	user-3	/spl66/	0	-	-	✓ 13 minutes	-	Active - AKIA

4. For creating groups, click the group section in the left nav bar and select create groups

[IAM](#) > [User groups](#) > Create user group

Create user group

Name the group

User group name
Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.

Add users to the group - *Optional* (4) [Info](#)











An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

< 1 >

☐ User name [✎](#)

▲ Groups | Last activity ▼ | Creation ti

Again for the group we can assign policy directly by selecting the available policy

<input type="text" value="Search"/>		<input type="text" value="All types"/>		<div>< 1 2 3 4 5 6 7 ... 46 ></div>	
<input type="checkbox"/>	Policy name	Type	Used as	Description	
<input type="checkbox"/>	 AdministratorAccess	AWS managed - job function	Permissions policy (1)	Provides full access to AWS services ar	
<input type="checkbox"/>	 AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permis	
<input type="checkbox"/>	 AdministratorAccess-AWSElas...	AWS managed	None	Grants account administrative permis	
<input type="checkbox"/>	 AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaFc	
<input type="checkbox"/>	 AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness	
<input type="checkbox"/>	 AlexaForBusinessGatewayExe...	AWS managed	None	Provide gateway execution access to A	
<input type="checkbox"/>	 AlexaForBusinessLifeseDele...	AWS managed	None	Provide access to Lifesize AVS devices	
<input type="checkbox"/>	 AlexaForBusinessPolyDelegat...	AWS managed	None	Provide access to Poly AVS devices	
<input type="checkbox"/>	 AlexaForBusinessReadOnlyAc...	AWS managed	None	Provide read only access to AlexaForB.	
<input type="checkbox"/>	 AmazonAPIGatewayAdministr...	AWS managed	None	Provides full access to create/edit/del	

These are the pre created group, now we have to assign the users to it

[IAM](#) > User groups

User groups (3) [Info](#)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

< 1 > ⚙

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	EC2-Admin	0	Defined	8 minutes ago
<input type="checkbox"/>	EC2-Support	0	Defined	9 minutes ago
<input type="checkbox"/>	S3-Support	0	Defined	9 minutes ago

- Go to the user group which is under the users in the left panel,click the group name

[IAM](#) > [User groups](#) > EC2-Support

EC2-Support [Info](#) Delete

Summary Edit

User group name EC2-Support	Creation time February 12, 2024, 21:51 (UTC+05:45)	ARN arn:aws:iam::376615524342:group/spl66/EC2-Support
--------------------------------	---	--

[Users](#) | **[Permissions](#)** | [Access Advisor](#)

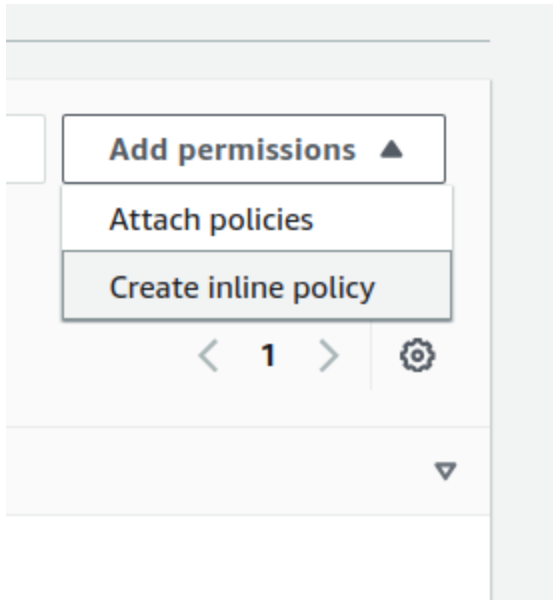
Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

Filter by Type All types < 1 > ⚙

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AmazonEC2ReadOnlyAccess	AWS managed	1

Now click the permission tab as you can see the group has read only. We can again reassign the policy by clicking add permission but here we are not allowed to do that



6. Now click the user tab and click add user

EC2-Support [Info](#) Delete

Summary Edit

User group name	Creation time	ARN
EC2-Support	February 12, 2024, 21:51 (UTC+05:45)	arn:aws:iam::376615524342:group/spl66/EC2-Support

[Users](#) | [Permissions](#) | [Access Advisor](#)

Users in this group (0) Refresh Remove Add users

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

< 1 > Settings

<input type="checkbox"/>	User name ?	Groups	Last activity	Creation time
No resources to display				

And select the user you want to assign to the particular group, after selecting the user click add user

[IAM](#) > [User groups](#) > [EC2-Support](#) > Add users

Add users to EC2-Support [Info](#)

Other users in this account (1/4) Refresh

< 1 > Settings

<input type="checkbox"/>	User name ?	Groups	Last activity	Creation time
<input type="checkbox"/>	awsstudent	0	None	16 minutes ago
<input type="checkbox"/>	user-1	0	None	16 minutes ago
<input checked="" type="checkbox"/>	user-2	0	None	16 minutes ago
<input type="checkbox"/>	user-3	0	None	16 minutes ago

Cancel Add users

You can see the user is added to the group

1 user added to this group.

IAM > User groups > EC2-Support

EC2-Support [Info](#)

[Delete](#)

Summary [Edit](#)

User group name	Creation time	ARN
EC2-Support	February 12, 2024, 21:51 (UTC+05:45)	arn:aws:iam::376615524342:group/spl66/EC2-Support

[Users \(1\)](#) | [Permissions](#) | [Access Advisor](#)

Users in this group (1)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

< 1 >

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	user-2	1	None	17 minutes ago

Now we can signout from aws and use the created user as a userid,generated password and login with the assign roles within a group using the

☒ Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

Do you want to provide console access to a person?
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications. To do so, sign into the console by using the credentials of the management account in AWS Organizations, and then enable Identity Center. If you aren't the management account owner, contact the owner to perform this task.

Console password

☒ Autogenerated password
You can view the password after you create the user.

☐ Custom password
Enter a custom password for the user.

☐ Show password

☒ Users must create a new password at next sign-in - Recommended
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

[Cancel](#) [Next](#)

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

We can auto generate password or use custom password when creating the user