

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.

Process:

- Open Aws Console inside learners lab
- Search and find EC2 feature and launch instance

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

[Add additional tags](#)


▼ 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


Recents

Quick Start


Amazon Linux




macOS




Ubuntu




Windows




Red Hat



SUSE Linux





[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

- Name was given and Os images was assigned as linux

- T2 micro was selected as instance type to cut down cost for the bootcamp

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

Instance type

t2.micro

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

Free tier eligible

☒ All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

- Keyvalue was given and security was assigned

▼ 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*

vockey

[Create new key pair](#)

▼ Network settings [Info](#)

Network [Info](#)

vpc-012aa5a5c7d7d6fc3

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

We'll create a new security group called 'launch-wizard-4' with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

Anywhere

0.0.0.0/0

☒ Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

☒ Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server



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

- Finally launching

○ Launching Instance
Launch initiation

79%

- Allocating elastic IP

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. This can help improve the availability and latency for your user traffic by using the Amazon global network. [Learn more](#)

Create accelerator

Tags - *optional*

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag

You can add up to 50 more tag

Cancel

Allocate

Associate Elastic IP address^{Info}

Choose the instance or network interface to associate to this Elastic IP address (3.212.93.196)

Elastic IP address: 3.212.93.196

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

i-0399eed5284616279 (ec2_basic_instance) - running

i-0f30eed23f762ea37 (sushant_p) - running



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

Cancel

Associate

Instance: i-0399eed5284616279 (ec2_basic_instance)

Hostname type
IP name: ip-172-31-17-225.ec2.internal
Answer private resource DNS name
IPv4 (A)
Auto-assigned IP address
—
IAM Role
—
IMDSv2
Required

▼ Instance details ^{Info}
Platform

Private IP DNS name (IPv4 only)
ip-172-31-17-225.ec2.internal
Instance type
t2.micro
VPC ID
vpc-012aa5a5c7d7d6fc3
Subnet ID
subnet-0d2019c8c2b79acc8

AMI ID

Elastic IP addresses
3.212.93.196 [Public IP]
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | [Learn more](#)
Auto Scaling Group name
—

Monitoring

- Connecting to the instance via SSH

Create key pair [Info](#)

Key pair

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type [Info](#)

☒ RSA☐ ED25519

Private key file format

☒ .pem

For use with OpenSSH

☐ .ppk

For use with PuTTY

Tags - *optional*

No tags associated with the resource.

You can add up to 50 more tags.

[Cancel](#)

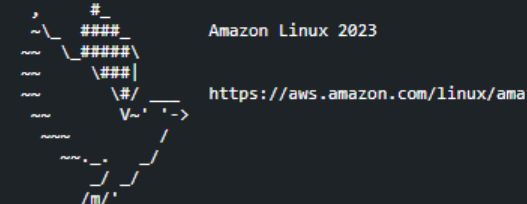
[Create key pair](#)

```
chmod 400 /path/to/your/private-key-file.pem
```

```
ssh -i /path/to/your/private-key-file.pem ec2-user@your-instance-public-dns
```


us-east-1

```
[cloudshell-user@ip-10-132-44-197 ~]$ chmod 400 new-key.pem  
[cloudshell-user@ip-10-132-44-197 ~]$ ssh -i "new-key.pem" ec2-user@ec2-3-212-93-196.compute-1.amazonaws.com  
  
ssh: connect to host ec2-3-212-93-196.compute-1.amazonaws.com port 22: Connection timed out  
[cloudshell-user@ip-10-132-44-197 ~]$  
[cloudshell-user@ip-10-132-44-197 ~]$ ssh -i "new-key.pem" ec2-user@ec2-3-212-93-196.compute-1.amazonaws.com  
^C  
[cloudshell-user@ip-10-132-44-197 ~]$ ssh -i "new-key.pem" ec2-user@ec2-54-90-80-47.compute-1.amazonaws.com  
The authenticity of host 'ec2-54-90-80-47.compute-1.amazonaws.com (54.90.80.47)' can't be established.  
ED25519 key fingerprint is SHA256:f5nrVihjJ4SJuCsMAeGzhH8I9rsLyzdEpU15jW+HrsE.  
This key is known by other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'ec2-54-90-80-47.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
```



```
#_
~\ #####      Amazon Linux 2023
~~ \#####\ 
~~   \|###|    
~~    \|##|   
~~~~ \|#/\     https://aws.amazon.com/linux/amazon-linux-2023
       V-' '->
           / 
          /  
         /___/
        /___/_m/'
```

```
Last login: Tue Feb 20 10:28:40 2024 from 18.206.107.27
[ec2-user@ip-172-31-25-67 ~]$ whoami
ec2-user
[ec2-user@ip-172-31-25-67 ~]$ █
```

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.

Create bucket Info

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

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

sushant-balti

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

Object Ownership Info

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.

Object Ownership

Bucket owner enforced

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)

☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)

☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the [Storage](#) tab of the [Amazon S3 pricing page](#). [↗](#)

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#) [↗](#)

☐ Disable

☒ Enable

► Advanced settings

ⓘ

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel

Create bucket

Uploading files to the bucket.

Upload [Info](#)

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#) [↗](#)

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (1 Total, 0 B)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

🔍 Find by name

< 1 >

<input type="checkbox"/>	Name	▼	Folder
<input type="checkbox"/>	hello.txt		-

Destination [Info](#)

Destination

s3://sushant-balti

Setting up bucket policies for access control.

sushant-balti

Objects

Properties

Permissions

Metrics

Management

Access Points

Permissions overview

Access

Objects can be public

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.

Block all public access

Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts.

EditDelete

Edit bucket policy

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts.

Policy examplesPolicy generator

Bucket ARN

arn:aws:s3::sushant-balti

Policy

1

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

Click policy generator

amazon

webservices

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 creating policies, see key 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 SQS Queue Policy.

Select Type of Policy

SQS Queue Policy

S3 Bucket Policy

VPC Endpoint Policy

IAM Policy

SNS Topic 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 SQS

All Services (*)

Use multiple statements to add permissions for more than one service.

Actions

-- Select Actions --

All Actions (*)

Amazon Resource Name (ARN)

ARN should follow the following format: arn:aws:sqs:(Region):(Account):(QueueName). Use a comma to separate multiple values.

Add Conditions (Optional)

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 creating policies, see [key 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 [SQS Queue Policy](#).

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 should follow the following format: arn:aws:s3:::{BucketName}/{KeyName}.
Use a comma to separate multiple values.

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

[Add Statement](#)


Now pasting the generated policy

Edit bucket policy [Info](#)

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

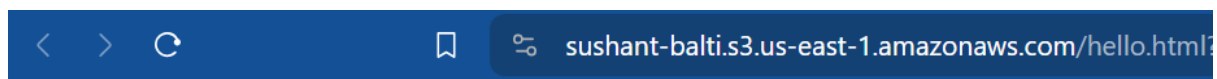
Bucket ARN

 arn:aws:s3::sushant-balti

Policy

```
1 {
2   "Id": "Policy1708535146418",
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "Stmnt1708535145290",
7       "Action": "s3:*",
8       "Effect": "Allow",
9       "Resource": "arn:aws:s3::sushant-balti",
10      "Principal": "*"
11    }
12  ]
13 }
```

Accessing the uploaded content



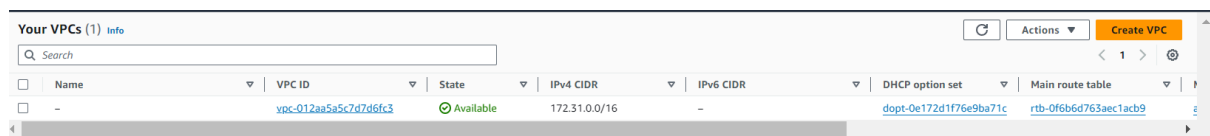
This is a heading

This is a paragraph.

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.

Creating a new VPC.



The screenshot shows the 'Your VPCs' page in the AWS Management Console. At the top, there is a search bar and a 'Create VPC' button. Below the search bar is a table with the following columns: Name, VPC ID, State, IPv4 CIDR, IPv6 CIDR, DHCP option set, and Main route table. A single VPC is listed in the table.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table
-	vpc-012aa5a5c7d7d6fc3	Available	172.31.0.0/16	-	dopt-0e172d1f76e9ba71c	rtb-0f6b6d763aec1acb9

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as

VPC settings

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

☐ VPC only

☒ VPC and more

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

basiclab

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
---	---	---

► **Customize subnets CIDR blocks**

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
------	------------

▼ **Customize subnets CIDR blocks**

Public subnet CIDR block in us-east-1a

10.0.0.0/24

256 IPs

Private subnet CIDR block in us-east-1a

10.0.1.0/24

256 IPs

< > ^ v

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

Create VPC workflow

Wait for NAT Gateways to activate

70%

Details

- ✓ Create VPC: [vpc-0e9fea6024ce8f27b](#)
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: [vpc-0e9fea6024ce8f27b](#)
- ✓ Create S3 endpoint: [vpce-0b33f11d7154ed7a0](#)
- ✓ Create subnet: [subnet-071aa08374f7720e2](#)
- ✓ Create subnet: [subnet-0ef1986e8d4dae2ee](#)
- ✓ Create internet gateway: [igw-09800f1d52e55189b](#)
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: [rtb-0a71f9920ec0a1c5e](#)
- ✓ Create route
- ✓ Associate route table
- ✓ Allocate elastic IP: [eipalloc-0f49544c45410339f](#)
- ✓ Create NAT gateway: [nat-0972249f2a3242231](#)
- ⋯ Wait for NAT Gateways to activate
- ⌚ Create route table
- ⌚ Create route
- ⌚ Associate route table
- ⌚ Verifying route table creation
- ⌚ Associate S3 endpoint with private subnet route tables: [vpce-0b33f11d7154ed7a0](#)

vpc-0e9fea6024ce8f27b / basiclab-vpc

Actions

Details

VPC ID vpc-0e9fea6024ce8f27b	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0e172d1f76e9ba71c	Main route table rtb-0a5fca5c08c2b377	Main network ACL acl-0fce440351d314619
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups Failed to load rule groups	Owner ID 133852355281	

Adding subnets.

VPC dashboard

EC2 Global View

Filter by VPC:
Select a VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Subnets (5)

Find resources by attribute or tag

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses
-	subnet-0d18fa231dd2bb593	Available	vpc-012aa5a5c7d7d6fc3	172.31.64.0/20	-	4091
-	subnet-00bcbf13a09c72fc	Available	vpc-012aa5a5c7d7d6fc3	172.31.80.0/20	-	4091
-	subnet-0da709092523209a9	Available	vpc-012aa5a5c7d7d6fc3	172.31.0.0/20	-	4091
-	subnet-09fd44e16d3629d9b	Available	vpc-012aa5a5c7d7d6fc3	172.31.48.0/20	-	4091
-	subnet-09cb9ede33e2889a1	Available	vpc-012aa5a5c7d7d6fc3	172.31.32.0/20	-	4091
-	subnet-0d2019c9c2b79ace8	Available	vpc-012aa5a5c7d7d6fc3	172.31.16.0/20	-	4089

Subnet 1 of 1

Subnet name

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

the_new_subnet_101

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.

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

IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.0.0.0/16

IPv4 subnet CIDR block

10.0.4.0/1665,536 IPs

< > ^ v

Tags - optional

Key

Value - optional

Q NameX

Q the_new_subnet_101X

Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

Cancel

Create subnet

Create multiple subnets

Subnets (10) [Info](#)

Find resources by attribute or tag

< 1 > ⌕

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses
<input type="checkbox"/>	-	subnet-09fd44e16d3629d9b	Available	vpc-012aa5a5c7d7d6fc3	172.31.48.0/20	-	4091
<input type="checkbox"/>	-	subnet-09cb9ede33e2889a1	Available	vpc-012aa5a5c7d7d6fc3	172.31.32.0/20	-	4091
<input type="checkbox"/>	-	subnet-0d2019c8c2b79ace8	Available	vpc-012aa5a5c7d7d6fc3	172.31.16.0/20	-	4089
<input type="checkbox"/>	the_new_subnet_101	subnet-00da8433da44bf76e	Available	vpc-0e9fea6024ce8f27b basicl...	10.0.10.0/24	-	251
<input type="checkbox"/>	basiclab-subnet-public1-us-east-1a	subnet-071aa08374f7720e2	Available	vpc-0e9fea6024ce8f27b basicl...	10.0.0.0/24	-	250
<input type="checkbox"/>	basiclab-subnet-private1-us-east-1a	subnet-0ef1986e8d4dae2ee	Available	vpc-0e9fea6024ce8f27b basicl...	10.0.1.0/24	-	251
<input type="checkbox"/>	basic_lab_new	subnet-0f82cb142778261b9	Available	vpc-0e9fea6024ce8f27b basicl...	10.0.11.0/24	-	251

Select subnet

=

Setting up an Internet Gateway.

VPC > Internet gateways > Create internet gateway

Create internet gateway [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

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

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
<input type="text" value="Name"/>	<input type="text" value="the_new_basic_gate"/>	<input type="button" value="Remove"/>
<input type="button" value="Add new tag"/>		

You can add 49 more tags.

Configuring route tables.

VPC dashboard X

EC2 Global View

Filter by VPC:

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

Route tables (1/5) [Info](#)

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner ID
<input type="checkbox"/>	-	rtb-0a62a2165c907b76a	-	-	Yes	vpc-03047434062641f1d new...	133852355281
<input type="checkbox"/>	-	rtb-0f6b6d763aec1acb9	-	-	Yes	vpc-012aa5a5c7d7d6fc3	133852355281
<input checked="" type="checkbox"/>	basiclab-rtb-private1-us-east-1a	rtb-0757937dba768ddd4	subnet-0ef1986e8d4dae2ee	-	No	vpc-0e9fea6024ce8f27b basicl...	133852355281
<input type="checkbox"/>	basiclab-rtb-public	rtb-0a71f9920ec0a1c5e	subnet-071aa08374f772...	-	No	vpc-0e9fea6024ce8f27b basicl...	133852355281
<input type="checkbox"/>	-	rtb-0a5fca5c08c2b377	-	-	Yes	vpc-0e9fea6024ce8f27b basicl...	133852355281

Select edit subnet association in the bottom panel

rtb-0757937dba768ddd4 / basiclab-rtb-private1-us-east-1a

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

Explicit subnet associations (1)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
basiclab-subnet-private1-us-east-1a	subnet-0ef1986e8d4dae2ee	10.0.1.0/24	-

Select the new subnet too

VPC > Route tables > rtb-0757937dba768ddd4 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)

<input type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	the_new_subnet_101	subnet-0dda8433da44bf76e	10.0.10.0/24	-	Main (rtb-0a5fca5c08c2b377)
<input type="checkbox"/>	basiclab-subnet-public1-us-east-1a	subnet-071aa08374f7720e2	10.0.0.0/24	-	rtb-0a71f9920ec0a1c5e basiclab-rtb-public
<input checked="" type="checkbox"/>	basiclab-subnet-private1-us-east-1a	subnet-0ef1986e8d4dae2ee	10.0.1.0/24	-	rtb-0757937dba768ddd4 / basiclab-rtb-private...
<input type="checkbox"/>	basic_lab_new	subnet-0f82cb142778261b9	10.0.11.0/24	-	Main (rtb-0a5fca5c08c2b377)

Selected subnets

Creating the security group

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

Network ACLs

Security groups

DNS firewall

Rule groups

Security Groups (7) Info

Find resources by attribute or tag

Export security groups to CSV

Create security group

< 1 >

	Name	Security group ID	Security group name	VPC ID	Description	Owner
<input type="checkbox"/>	-	sg-0e5d9506477740307	launch-wizard-2	vpc-012aa5a5c7d7d6fc3	launch-wizard-2 created 2024-01-22T...	133852355281
<input type="checkbox"/>	-	sg-037206bc223c9433b	launch-wizard-4	vpc-012aa5a5c7d7d6fc3	launch-wizard-4 created 2024-02-20T...	133852355281
<input type="checkbox"/>	-	sg-0bef19aad8028ed06	default	vpc-03047434062641f1d	default VPC security group	133852355281
<input type="checkbox"/>	-	sg-030c2554bd22f1545	default	vpc-012aa5a5c7d7d6fc3	default VPC security group	133852355281
<input type="checkbox"/>	-	sg-0e912ea826d56da16	launch-wizard-3	vpc-012aa5a5c7d7d6fc3	launch-wizard-3 created 2024-02-20T...	133852355281
<input type="checkbox"/>	-	sg-0eb520c3e84cab477	launch-wizard-1	vpc-012aa5a5c7d7d6fc3	launch-wizard-1 created 2024-01-22T...	133852355281

Inbound rules Info

Type Info

Protocol Info

Port range Info

Source Info

Description - optional Info

HTTP

TCP

80

Custom

Q

Delete

Add rule

Outbound rules Info

Type Info

Protocol Info

Port range Info

Destination Info

Description - optional Info

HTTP

TCP

80

Custom

Q

0.0.0.0/0 X

Delete

Add rule

Setting up a simple EC2 instance within the VPC.

▼ Network settings

Info

VPC - required

Info

vpc-0e9fea6024ce8f27b (basiclab-vpc)

10.0.0.0/16

▼

↻

Subnet

Info

subnet-00da8433da44bf76e

the_new_subnet_101

VPC: vpc-0e9fea6024ce8f27b Owner: 133852355281 Availability Zone: us-east-1a

IP addresses available: 251 CIDR: 10.0.10.0/24

▼

↻

Create new subnet

Auto-assign public IP

Info

Disable

▼

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

Common security groups

Info

Select security groups

▼

vpc-security sg-0724c5cd84287e744

×

VPC: vpc-0e9fea6024ce8f27b

↻

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

▶ Advanced network configuration

Instances (1)

Info

Find Instance by attribute or tag (case-sensitive)

Any state

Instance ID: i-0aa85f6ee583fe7ea

×

Clear filters

Connect

Instance state

Actions

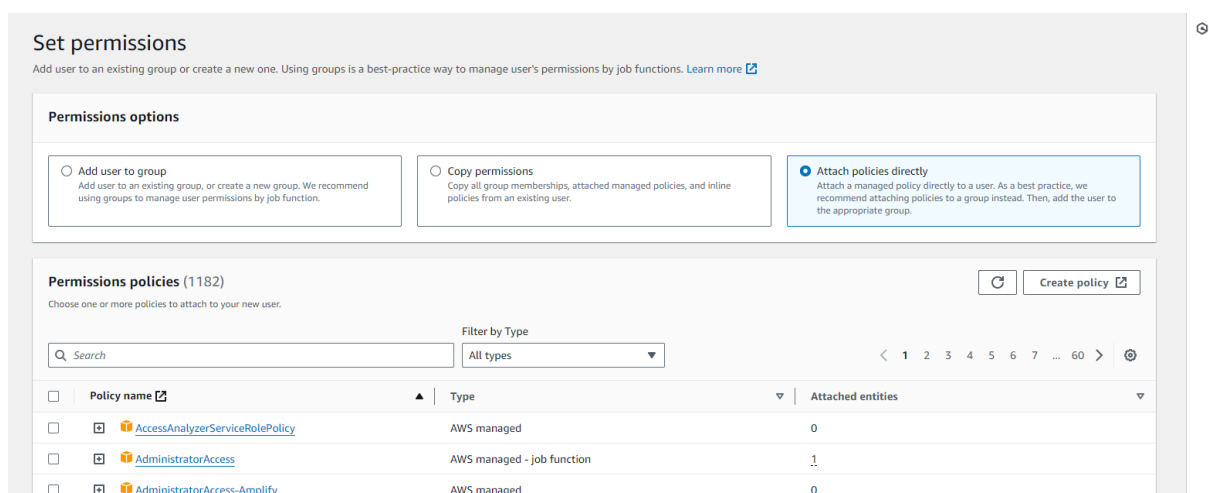
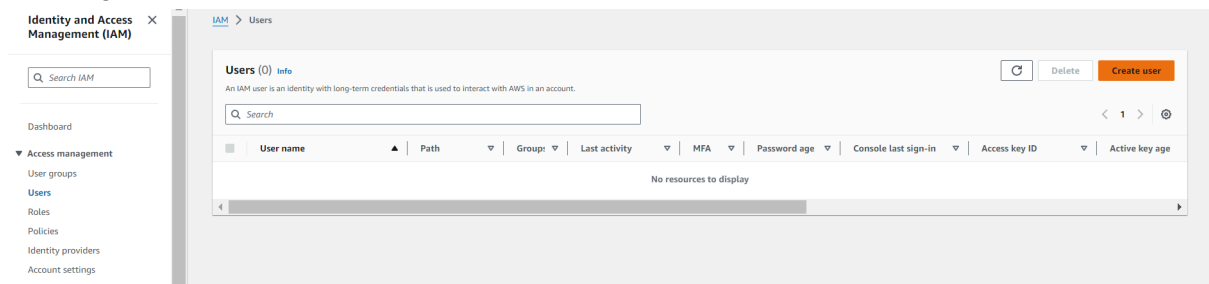
Launch instances

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input type="checkbox"/>	New VPC instance	i-0aa85f6ee583fe7ea	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	-	-	-

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.

Creating new IAM users.



Review and create


Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name sushant	Console password type None	Require password reset No
----------------------	-------------------------------	------------------------------

Permissions summary

< 1 >

Name 	Type	Used as
No resources		

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create user