

Basic Labs

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.

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.

3. VPC Configuration Lab

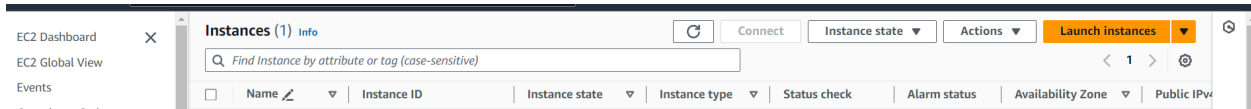
- **Objective:** To understand the fundamentals of AWS networking through the configuration of a Virtual Private Cloud (VPC).
- **Approach:** Students will create a new VPC, add subnets, set up an Internet Gateway, and configure route tables. The lab might also include setting up a simple EC2 instance 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.

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.

EC2 Basics Lab:

Launching EC2 instance:



Add name of the instance:

Name and tags [Info](#)

Name

[Add additional tags](#)

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

Select required AMI

below

Quick Start

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE Li

[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

ami-0005e0cfe09cc9050 (64-bit (x86), uefi-preferred) / ami-0730971bf8e0532d6 (64-bit (Arm), uefi)

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Select instance type:

▼ **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](#)

Select the default key pair, this will required to connect through the SSH and download the ppm file:

▼ **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](#)

Create the security group:

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-2' with the following rules:

☒ Allow SSH traffic from Anywhere
0.0.0.0/0
 Helps you connect to your instance

☐ 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

Required storage configuration:

▼ **Configure storage** [Info](#) [Advanced](#)

1x GiB Root volume (Not encrypted)

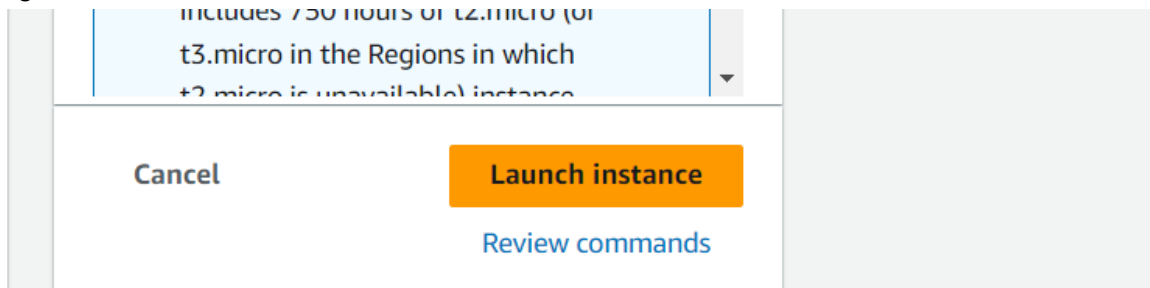
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

From the network setting disable assign public IP

Auto-assign public IP [Info](#)

Firewall (security groups) [Info](#)

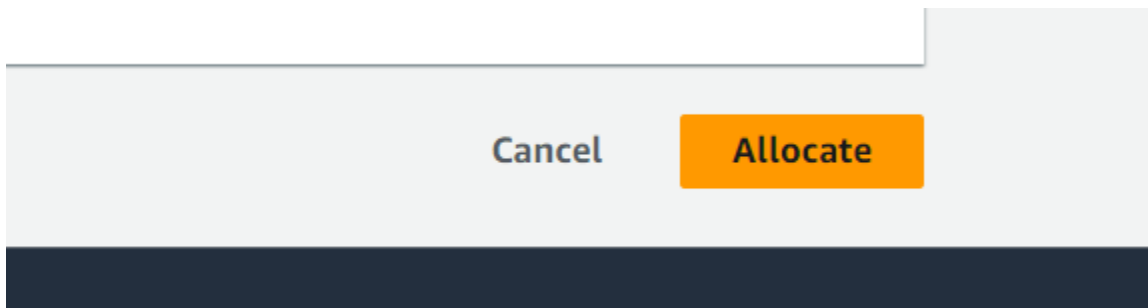
Launching the instance:



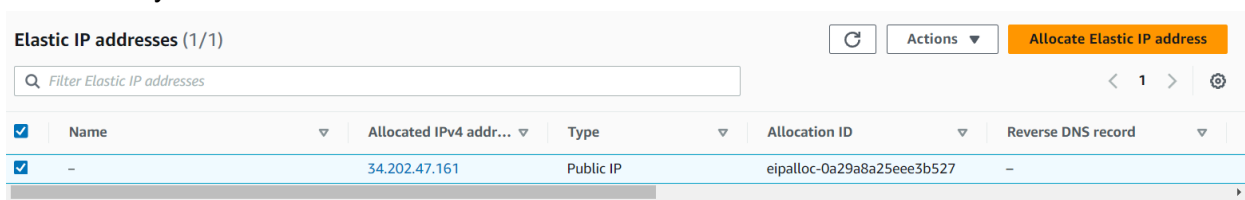
Waiting the instance to be running:



Allocate the default elastic IP:

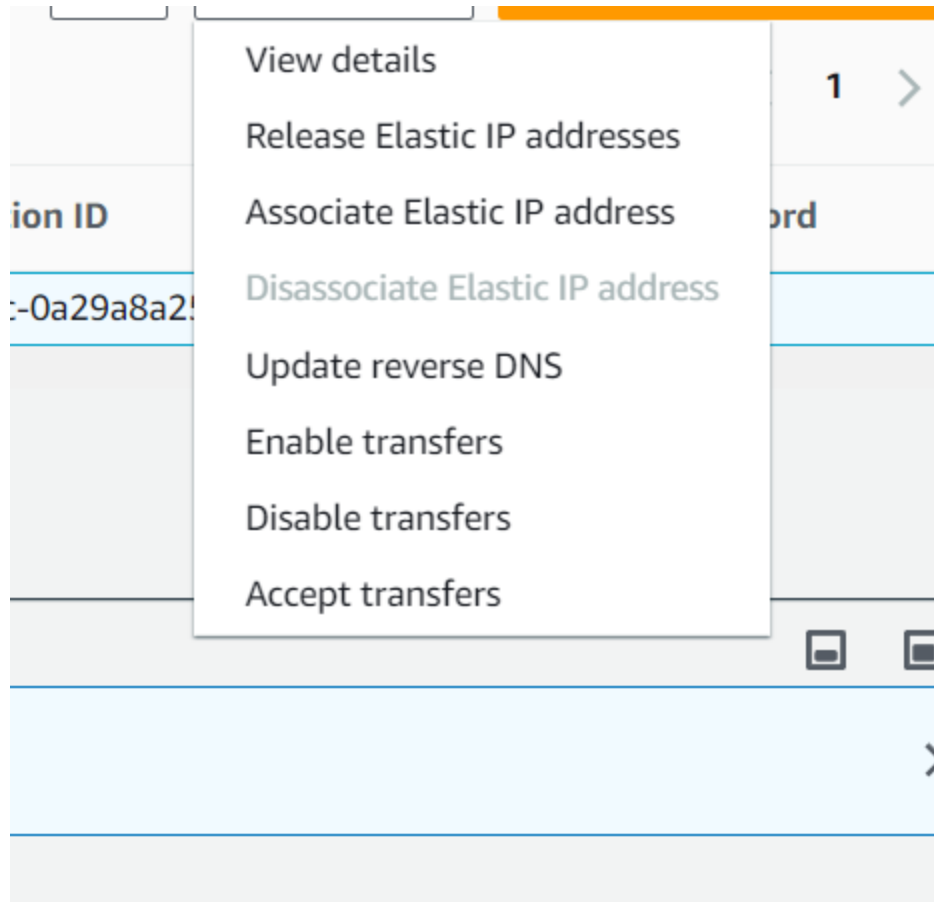


Now select your allocated elastic IP:



Go to action:

And choose associate elastic IP



Choose your EC2 instance:

Instance

Q i-03060d86eeb441df8

Private IP address

Then associate:

Cancel Associate

Connection through web browser:


EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID


 i-017eaaf1e9b09f68c (myinstanceconnectssh1)

Connection Type

☒ Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.


☐ Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.


Public IP address


 34.230.14.161

Username

Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ec2-user.

 ec2-user



 **Note:** In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

Cancel

Connect

Shell Feedback

Creating new security group:

▼ Security

Network ACLs

Security groups

▼ DNS firewall

Rule groups

Domain lists

Outbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info	
HTTP ▼	TCP	80	Anyw... ▼ 0.0.0.0/0 ✕		Delete
<button>Add rule</button>					

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

✕

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 tags.

[Cancel](#) [Create security group](#)

Basic details

Security group name [Info](#)

secgroup1

Name cannot be edited after creation.

Description [Info](#)

allow Http request

VPC [Info](#)

vpc-08f24abb23db1b34b ▼

Assigning the security group to ec2:

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

Q |

<input type="checkbox"/>	default	sg-019ee512ae412f8eb
	VPC: vpc-08f24abb23db1b34b	
<input type="checkbox"/>	secgroup1	sg-046f7b9a9c399d38b
	VPC: vpc-08f24abb23db1b34b	
<input type="checkbox"/>	launch-wizard-2	sg-0e04270dae5e0ca2b
	VPC: vpc-08f24abb23db1b34b	
<input type="checkbox"/>	launch-wizard-3	sg-03f149b159b23637e

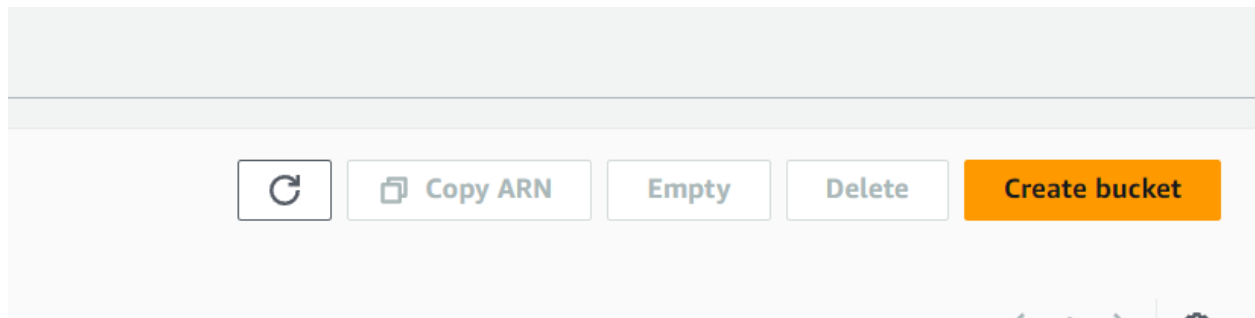
[Compare security group rules](#)

erfaces.

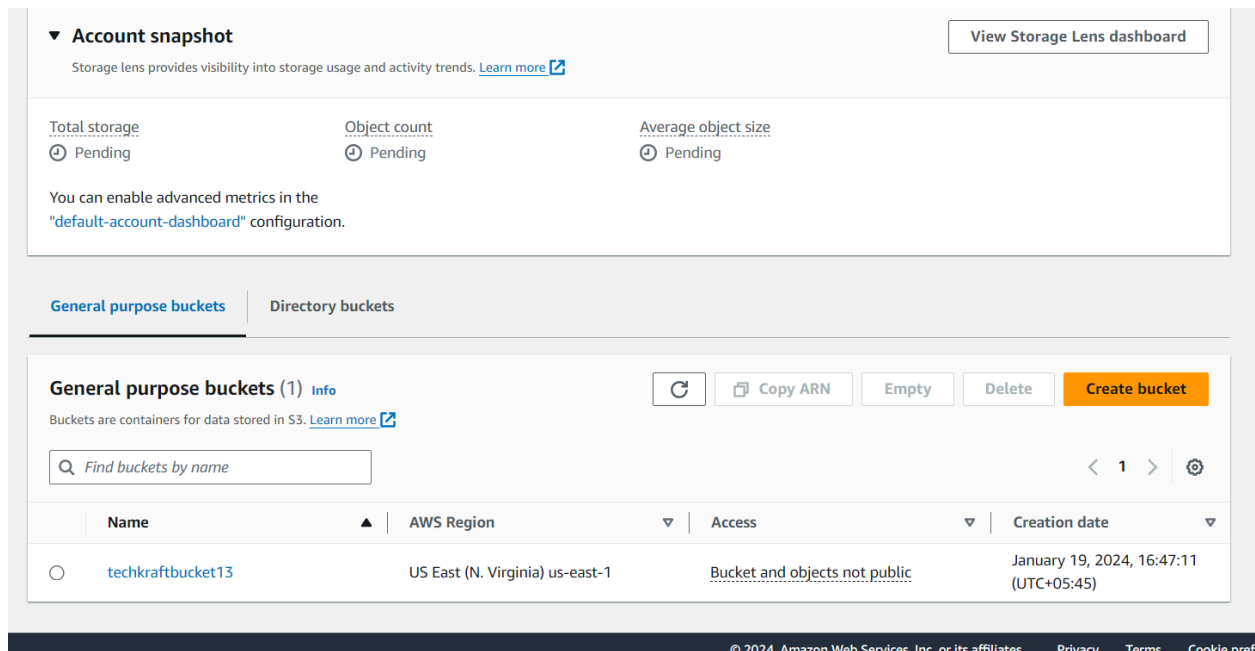
[Advanced](#)

S3 Storage Fundamentals Lab

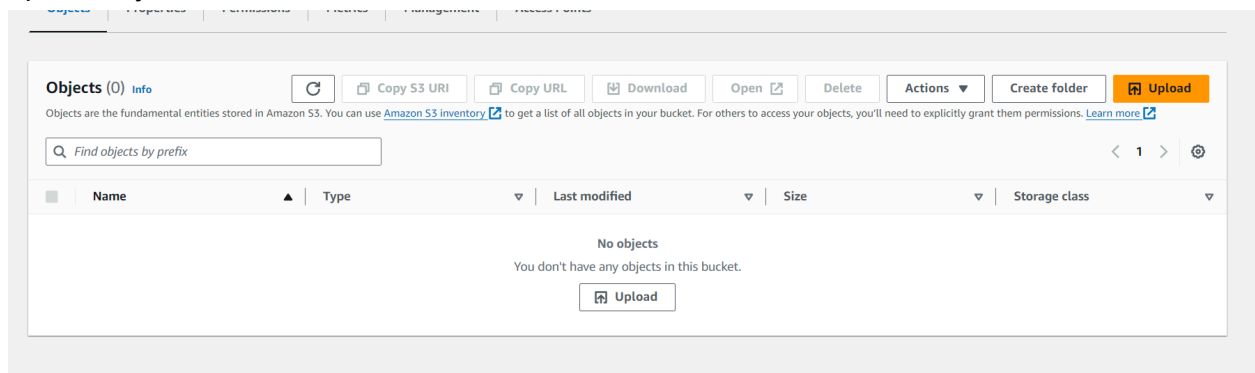
Create S3 bucket:



S3 management console:



Upload object file to s3 bucket:



Uploaded file:

Files and folders (1 Total, 45.0 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	Type
<input type="checkbox"/>	index.html	-	text/html

Enable static website hosting

Static website hosting

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

Static website hosting

Disabled

Setting bucket policy:

arn:aws:s3:::hostingst13


Policy

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "PublicReadGetObject",
6       "Effect": "Allow",
7       "Principal": "*",
8       "Action": [
9         "s3:GetObject"
10      ],
11      "Resource": [
12        "arn:aws:s3:::hostingst13/*"
13      ]
14    }
15  ]
16 }
```

HOsted static website:

Static website hosting

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

Static website hosting

Enabled

Hosting type

Bucket hosting

Bucket website endpoint

When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket.

 <http://hostingst13.s3-website-us-east-1.amazonaws.com> 

VPC Configuration Lab:

Creating VPC:

Create VPC

Launch EC2 Instances

Note: Your Instances will launch in the US East region.

Resources by Region

Refresh Resources

You are using the following Amazon VPC resources

VPCs

US East 2

NAT Gateways

See all regions ▼

See all regions ▼

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

DNS options

Info

☒ Enable DNS hostnames

☒ Enable DNS resolution

Additional tags

Cancel

Create VPC

Creating subnet;

VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways

Subnets (9) Info
Find resources by attribute or tag

	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	-	subnet-04d60bbc2e34d2b75	Available	vpc-035e0434f2845b45b	172.31.48.0/20
<input type="checkbox"/>	Work Public Subnet	subnet-06a45345fbdbf83b2	Available	vpc-019fabf0073781c84 Work...	10.0.0.0/24
<input type="checkbox"/>	-	subnet-0af93780ed48e4372	Available	vpc-035e0434f2845b45b	172.31.64.0/20
<input type="checkbox"/>	-	subnet-07202f09d432867a2	Available	vpc-035e0434f2845b45b	172.31.16.0/20
<input type="checkbox"/>	-	subnet-01871c80ef1f1c7ae	Available	vpc-035e0434f2845b45b	172.31.0.0/20
<input type="checkbox"/>	-	subnet-04a4b384923f4433e	Available	vpc-035e0434f2845b45b	172.31.80.0/20

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the 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
 256 IPs

< > ^ v

Tags - optional

Key	Value - optional	
<input type="text" value="Name"/>	<input type="text" value="subnet-public2"/>	Remove

Add new tag
You can add 49 more tags.

Remove

Add new subnet

Cancel Create subnet

Public subnet created:

Subnets (1) [Info](#)

Find resources by attribute or tag

Subnet ID : subnet-016027ab057befafb [X](#) [Clear filters](#)

< 1 > [Settings](#)

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	public-sub2	subnet-016027ab057befafb	Available	vpc-0c61382d1121902b4 myv...	10.0.2.0/24

Creating private 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

256 IPs

< > ^ v

▼ **Tags - optional**

Key	Value - optional	
<input type="text" value="Name"/> X	<input type="text" value="private-sub2"/> X	Remove
Add new tag		
You can add 49 more tags.		
Remove		
Add new subnet		

[Cancel](#) [Create subnet](#)

Subnet association:

<input type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	private-sub2	subnet-06ab34a735839e000	10.0.3.0/24	–	Main (rtb-01f47172adde597cd)
<input type="checkbox"/>	public-sub2	subnet-016027ab057befaf	10.0.2.0/24	–	Main (rtb-01f47172adde597cd)
<input type="checkbox"/>	myvpc1-subnet-public1-us-east...	subnet-060e897444a8e8218	10.0.0.0/24	–	rtb-0880ef4c8bba7e6e4 / myvpc1-
<input checked="" type="checkbox"/>	myvpc1-subnet-private1-us-eas...	subnet-095e08ba67a2935bd	10.0.1.0/24	–	rtb-0fe5035db3565f5ef / myvpc1-

IAM Users and Roles Lab

Create user:

Users (1) Info

Refresh

Delete

Create user

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Search

< 1 > ⚙

<input type="checkbox"/>	User name	Path	Group	Last activity	MFA	Password age
<input type="checkbox"/>	awsstudent	/	0	-	-	-

User details

User name

dipesh

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 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.

Silence!

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * () _ + - (hyphen) = [] { } | ' "

☒ 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

Not authorize to create a user:

⊗ User was not created.

User: arn:aws:sts::562976937128:assumed-role/voclabs/user2999740=tripathidipesh13@gmail.com is not authorized to perform: iam:CreateUser on resource: arn:aws:iam::562976937128:user/dipesh because no identity-based policy allows the iam:CreateUser action

Step 4

Retrieve password

dipesh

Custom password

No

Permissions summary

< 1 >

Name	Type	Used as
No resources		

18

Groups

Name the group

User group name

Enter a meaningful name to identify this group.

admin

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

Add users to the group - *Optional* (1) [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.

Q Search

<input type="checkbox"/>	User name ✕	▲	Groups	Last activity ▼	Creation time
<input type="checkbox"/>	awsstudent		0	None	1 hour ago

Attach permissions policies - *Optional* (1/908) [Info](#)

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Q Search

Filter by Type

All types [▼](#)

<input type="checkbox"/>	Policy name	▲	Type	▼	Used as	▼	Description
<input checked="" type="checkbox"/>	AdministratorAccess		AWS managed - job function		Permissions policy (1)		Provides full access to AWS services and resources.

AdministratorAccess

ⓘ

User group was not created.

✕

User: am:aws sts::562976937128:assumed-role/voclabs/user2999740-tripathidipesh13@gmail.com is not authorized to perform: iam:CreateGroup on resource: am:aws iam::562976937128:group/admin because no identity-based policy allows the iam:CreateGroup action

ⓘ

🔍

<input type="checkbox"/>	AdministratorAccess-...	AWS managed	None	Grants account administrative permissions. Explicitly allows developers and administrators to gain direct access to reso...
<input type="checkbox"/>	AlexaForBusinessDevi...	AWS managed	None	Provide device setup access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessFullA...	AWS managed	None	Grants full access to AlexaForBusiness resources and access to related AWS Services
<input type="checkbox"/>	AlexaForBusinessGate...	AWS managed	None	Provide gateway execution access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessLifes...	AWS managed	None	Provide access to Lifesize AVS devices
<input type="checkbox"/>	AlexaForBusinessPoly...	AWS managed	None	Provide access to Poly AVS devices

19

IAM lab with cloud foundation course lab

Here are already created users i.e 3.

<input type="checkbox"/>	user-1	/spl66/	0	-	-	✔ 4 minutes	-	Active - AKIAWW43LP...	✔ 4 minutes
<input type="checkbox"/>	user-2	/spl66/	0	-	-	✔ 4 minutes	-	Active - AKIAWW43LP...	✔ 4 minutes
<input type="checkbox"/>	user-3	/spl66/	0	-	-	✔ 4 minutes	-	Active - AKIAWW43LP...	✔ 4 minutes

Already created user group:

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	EC2-Admin		⚠ 0 ✔ Defined	5 minutes ago
<input type="checkbox"/>	EC2-Support		⚠ 0 ✔ Defined	5 minutes ago
<input type="checkbox"/>	S3-Support		⚠ 0 ✔ Defined	5 minutes ago

Permission to the EC2-support group is

User group name
EC2-Support

Creation time
January 20

Users
Permissions
Access Advisor

Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

<input type="checkbox"/>	Policy name ↗	Type
<input type="checkbox"/>	AmazonEC2ReadOnlyAccess	AWS

JSON written policy:

```

AmazonEC2ReadOnlyAccess

Provides read only access to Amazon EC2 via the AWS Management Console.

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "ec2:Describe*",
7       "Resource": "*"
8     },
9     {
10      "Effect": "Allow",
11      "Action": "elasticloadbalancing:Describe*",
12      "Resource": "*"
13    },
14    {
15      "Effect": "Allow",
16      "Action": [
17        "cloudwatch:ListMetrics",
18        "cloudwatch:GetMetricStatistics",
19        "cloudwatch:Describe*"
20      ],

```

We need to set the following users to the user group:

User	In Group	Permissions
user-1	S3-Support	Read-Only access to Amazon S3
user-2	EC2-Support	Read-Only access to Amazon EC2
user-3	EC2-Admin	View, Start and Stop Amazon EC2 instances

For this add users to the user group:

S3-Support [info](#) Delete

Summary Edit

User group name S3-Support	Creation time January 20, 2024, 11:37 (UTC+05:45)	ARN arn:aws:iam::461497925345:group/spl66/S3-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 >

Select user 1

Add users to S3-Support [info](#) Refresh

Other users in this account (1/4)

< 1 >

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	awsstudent	0	None	10 minutes ago
<input checked="" type="checkbox"/>	user-1	0	None	10 minutes ago
<input type="checkbox"/>	user-2	0	None	10 minutes ago
<input type="checkbox"/>	user-3	0	None	10 minutes ago

Cancel Add users

This Concludes the completion of AWS Basic Labs