

Automatic snapshot deletion using AWS Lambda

➤ *Conditions to be applied for snapshot deletion.*

- **Running and Stopped state Instances**
 1. Retain last 30days snapshots.
 2. Snapshots with specific tags shouldn't be deleted.
- **Terminated state instances**
 1. Retain latest snapshots and delete remaining.
 2. Snapshots with specific tags shouldn't be deleted.

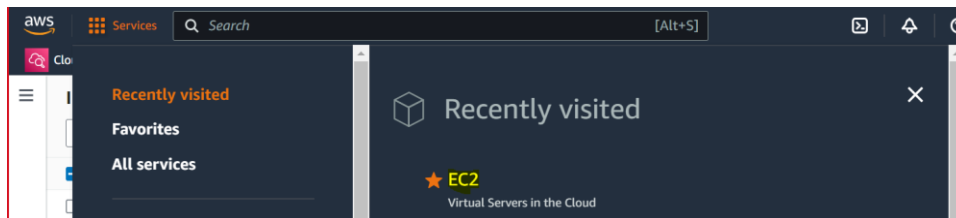
Step1: - Create EC2 Instance

Sign into the AWS Management Console:

Log in to your AWS account.

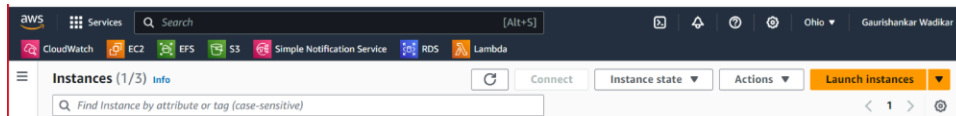
Navigate to the EC2 Dashboard:

In the AWS Management Console, find and select the "EC2" service.



Launch Instance:

Click on the "Instances" option on the left sidebar and then click the "Launch Instance" button.



Choose an Amazon Machine Image (AMI):

- Select an AMI that best suits your needs (Amazon Linux, Ubuntu, Windows Server, etc.).

▼ 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

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

Free tier eligible

ami-06d4b7182ac3480fa (64-bit (x86)) / ami-0090be1905998682a (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.2.20231113.0 x86_64 HVM kernel-6.1

Architecture

AMI ID

64-bit (x86)

ami-06d4b7182ac3480fa

Verified provider

Choose an Instance Type:

- Select the instance type based on your workload requirements (e.g., t2.micro, t3.medium, etc.). Instance types vary in terms of CPU, memory, storage, and networking capacity.

▼ Instance type
Info

Instance type

t2.micro

Free tier eligible

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

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

Key Pair:

- Select an existing key pair or create a new one. This key pair will be used to SSH/RDP into your instance securely.

▼ 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

Configure Instance:

- Configure instance details like the number of instances you want to launch, network settings (VPC, subnet), IAM role, etc.

▼
Network settings
Info

VPC - required
Info

vpc-0fca942f81ea0bd9f
172.31.0.0/16

(default) ▼

↻

Subnet
Info

No preference

▼

↻

Create new subnet

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

Add Storage:

- Define the storage requirements for your instance. You can add or modify the default storage settings (EBS volumes) based on your needs.

Configure Security Group:

- Create a new security group or choose an existing one. Security groups act as virtual firewalls controlling inbound and outbound traffic to your instance.

Inbound
Security Group
Rules

▼
Security group rule 1 (All, All, 0.0.0.0/0)

Remove

Type
Info

All traffic

▼

Protocol
Info

All

Port range
Info

All

Source type
Info

Anywhere

▼

Source
Info

Add CIDR, prefix list or secur

0.0.0.0/0

✕

Description - optional
Info

e.g. SSH for admin desktop

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

✕

Add security group rule

Review and Launch:

- Review the configuration details of your instance.
- You can modify any settings at this stage if needed.

Launch Instance:

- Click the "Launch" button.
- AWS will prompt you to select or create a key pair if you haven't already. This key pair will be used for securely accessing your instance.

▶
Advanced details
Info

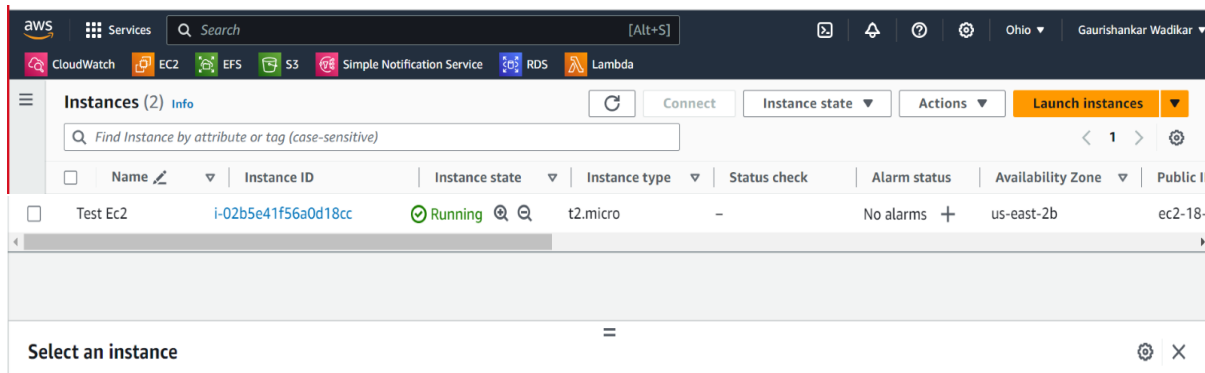
Cancel

Launch instance

Review commands

View Instances:

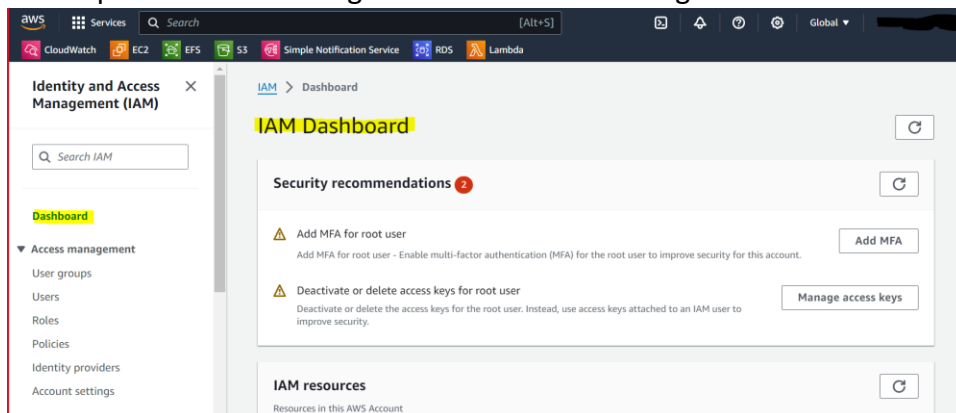
- After launching, go back to the EC2 dashboard and click on "Instances" to view the status of your newly created instance.



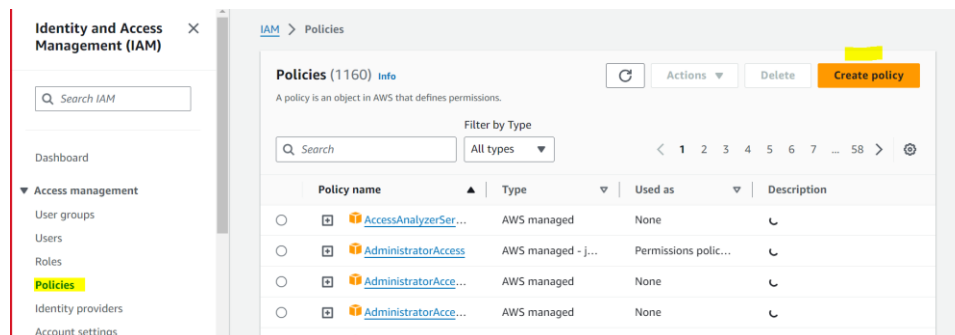
Steps2: - Create IAM Policies and Rules

A) Create Policy: -

- Open the AWS Management Console and navigate to the IAM dashboard.



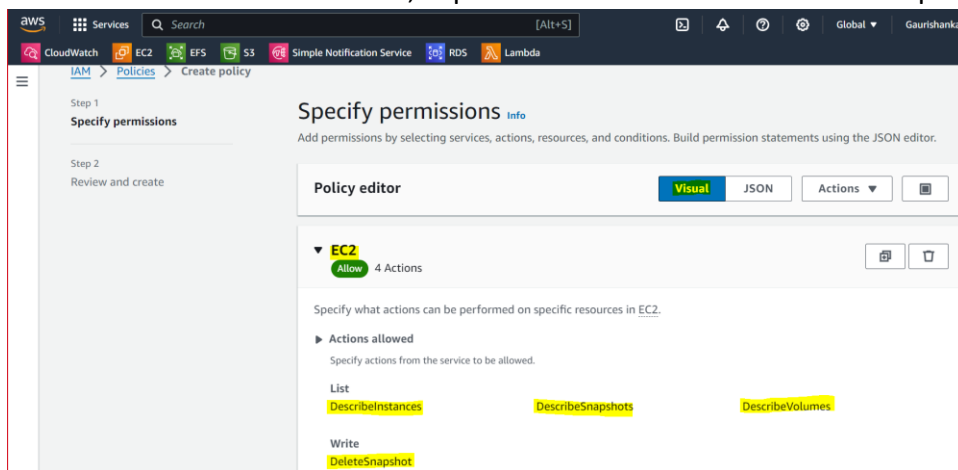
- In the left navigation pane, choose "Policies" and then click on the "Create policy" button.



- Choose the "Visual editor" tab.

- Click on the "Service" field, search for and select "EC2."

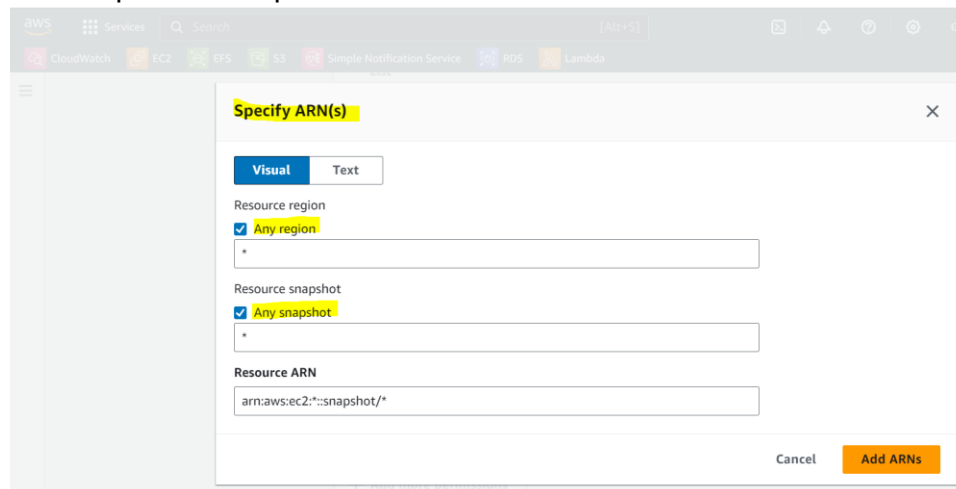
- In the "Actions" section, expand "Read" and select "DescribeSnapshots" and "DescribeVolumes."
- In the "Actions" section, expand "Write" and select "DeleteSnapshot."



- In the "Resources" section, click on the "Add ARN" button.
For each action, configure the resource ARN. You can use * for all resources or specify the ARNs of the specific resources you want to allow.

Example ARNs:

- For DescribeSnapshots, DescribeInstances and DescribeVolumes:
`arn:aws:ec2:region:account-id:*`
- For DeleteSnapshot: `arn:aws:ec2:region:account-id:snapshot/snapshot-id`



- Click on the "Review policy" button.
➤ Enter a name and description for the policy, and then click "Create policy."

IAM > Policies > Create policy

Step 1
[Specify permissions](#)

Step 2
Review and create

Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

automaticsnapshotdeletion

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

Description - optional
Add a short explanation for this policy.

Delete the Snapshots

Maximum 1,000 characters. Use alphanumeric and '+', '@', '-' characters.

Cancel Previous **Create policy**

Once our policy has been created, on the left-hand side click on **Roles** and then click on the orange button title ***Create roles***.

▼ Access management

- User groups
- Users
- Roles**
- Policies

IAM > Roles

Roles (9) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

↻ Delete **Create role**

Select the **AWS Service** for **Trusted entity type** and **Lambda** for **Use case**, then click on **next**.

Trusted entity type

☒ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ **Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

Choose a use case for the specified service.
 Use case
☒ **Lambda**
 Allows Lambda functions to call AWS services on your behalf.

Cancel **Next**

search and select the **policy** created in the steps above then click next.

Add permissions info

Permissions policies (1/906) info
 Choose one or more policies to attach to your new role.

Filter by Type
 All types 1 match

<input checked="" type="checkbox"/>	Policy name	Type	Description
<input checked="" type="checkbox"/>	automaticsnapshotdeletion	Customer managed	Delete the Snapshots

► Set permissions boundary - optional

Cancel Previous **Next**

create a name and click on **“Create role”**.

Name, review, and create

Role details

Role name
 Enter a meaningful name to identify this role.

 Maximum 64 characters. Use alphanumeric and '+@_.' characters.

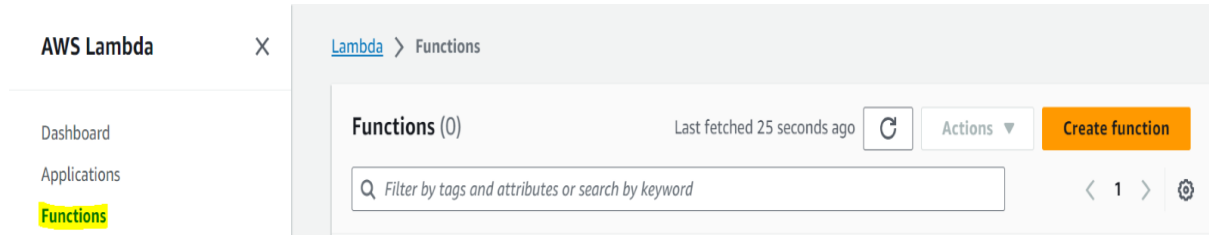
Description
 Add a short explanation for this role.

 Maximum 1000 characters. Use alphanumeric and '+@_.' characters.

Cancel Previous **Create role**

Step 3:- Lambda Functions Creation

Once the Lambda dashboard is displayed, on the right-hand side click on the orange button title **“Create functions”**.

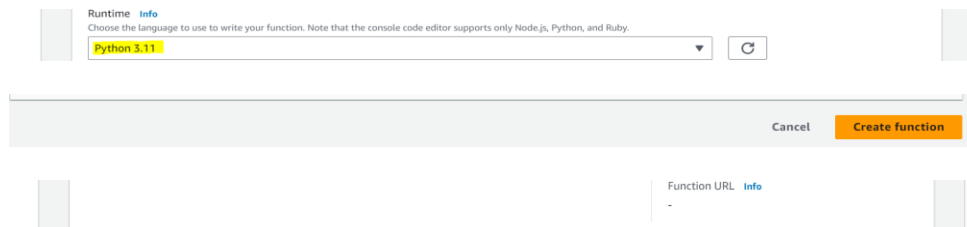


Create a name for our function.

Select **“Python 3.11”** for our runtime.

Select the role we created earlier under the **“Change default execution role”** option.

Then click on **“Create functions”** for **stop** running ec2 Instance



➤ After creating Lambda function, we can add the required code as per your requirement.

