



**KESHAV MEMORIAL INSTITUTE OF TECHNOLOGY
(AN AUTONOMOUS INSTITUTION)**



Accredited by NBA & NAAC, Approved by AICTE, Affiliated to JNTUH,
Narayanguda, Hyderabad – 500029



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

LAB RECORD

CLOUD COMPUTING LAB

B.Tech. III YEAR II SEM (KR20)

ACADEMIC YEAR 2022-23



KESHAV MEMORIAL INSTITUTE OF TECHNOLOGY
(AN AUTONOMOUS INSTITUTE)



Accredited by NBA & NAAC, Approved by AICTE, Affiliated to JNTUH, Hyderabad
Department of Computer Science & Engineering

Certificate

This is to certify that following is a Bonafide Record of the workbook task done by

_____ bearing Roll No _____ of _____

Branch of _____ year B.Tech Course in the _____

Subject during the Academic year _____ & _____ under our supervision.

Number of week tasks completed: _____

Signature of Staff Member Incharge

Signature of Head of the Dept.



KESHAV MEMORIAL INSTITUTE OF TECHNOLOGY (AN AUTONOMOUS INSTITUTE)



Accredited by NBA & NAAC, Approved by AICTE, Affiliated to JNTUH, Hyderabad
Department of Computer Science & Engineering

Daily Laboratory Assessment Sheet

Name of the Lab:

Name of the Student:

Class:

HT.No:

	TOTAL						

Faculty Incharge

INDEX

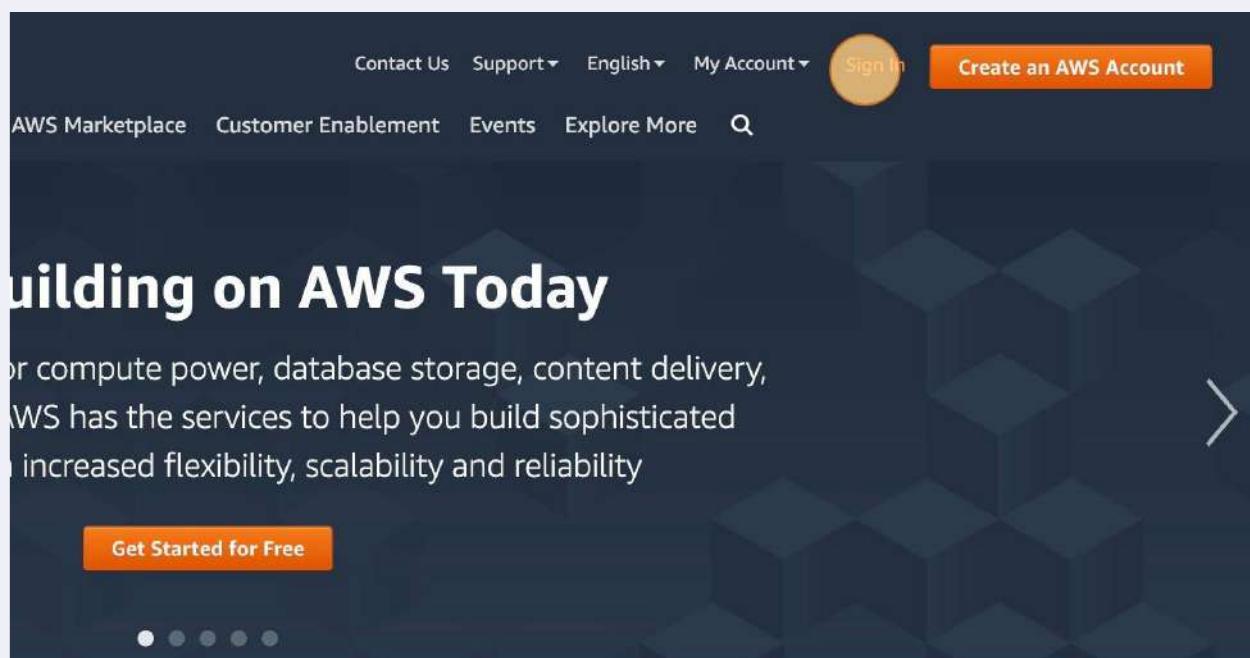
S.NO	CONTENTS	PAGE NO
1	Establish an AWS account. Use the AWS Management Console to launch an EC2 instance and connect to it.	1
2	Create your First AWS S3 Bucket and Upload Content to Bucket and Manage their Access and Create Static Website using AWS S3	19
3.	Create and configure storage services and upload files and objects using Amazon EBS	36
4	Create and configure storage services and upload files and objects using Amazon EFS	53
5	Creation of Amazon Lex Chat bot	86
6	Creation of S3 bucket and trigger by lambda to dynamo DB	95
7	Pull the image from Docker to EC2 Instance and access it publicly.	105
8	Creation of S3 bucket and make it available with Cloud Front	110
9	Creation of Dynamo DB	113
10	Create image recognition capability application using AWS Amazon Recognition.	125

EXPERIMENT 1

Establish an AWS account. Use the AWS Management Console to launch an EC2 instance and connect to it.

- 1 Navigate to <https://aws.amazon.com/>

- 2 Click "Sign In"



- 3** Click the "Root user" radio button.

Root user
Account owner that performs tasks requiring unrestricted access. [Learn more](#)

IAM user
User within an account that performs daily tasks. [Learn more](#)

Root user email address

Next

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

New to AWS?

Create a new AWS account



- 4** Type "Username you have registered for free tier"

IAM user
User within an account that performs daily tasks. [Learn more](#)

Root user email address

Next

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

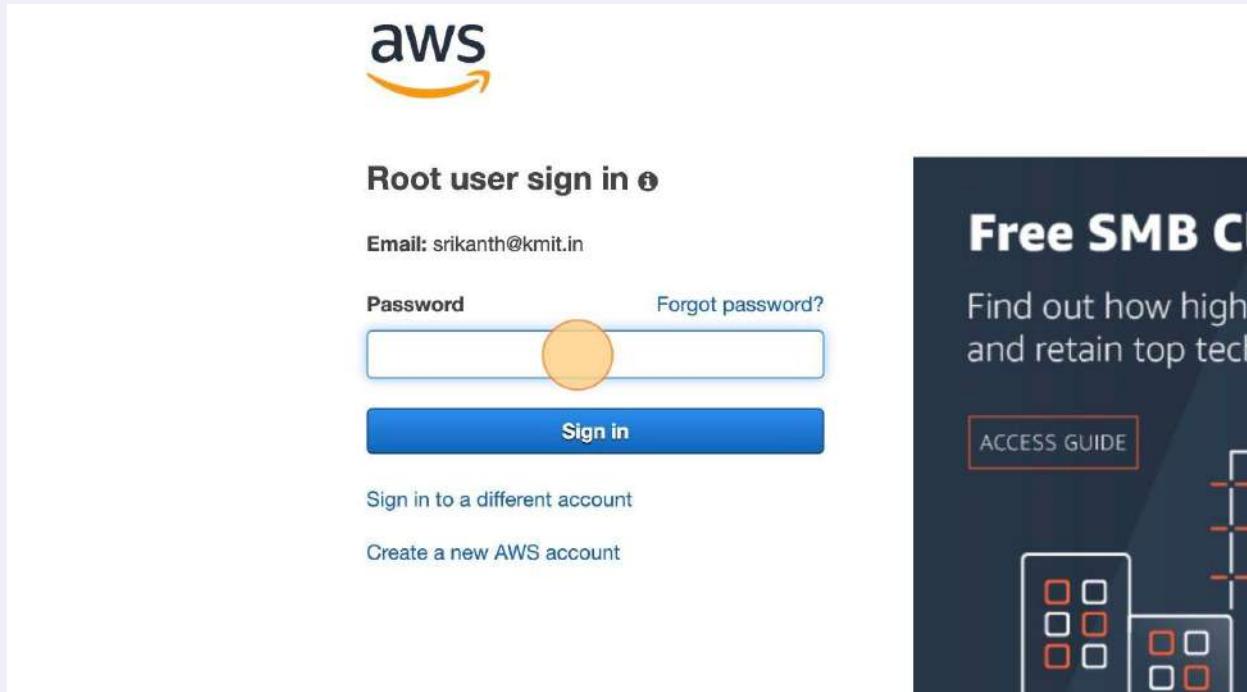
New to AWS?

Create a new AWS account

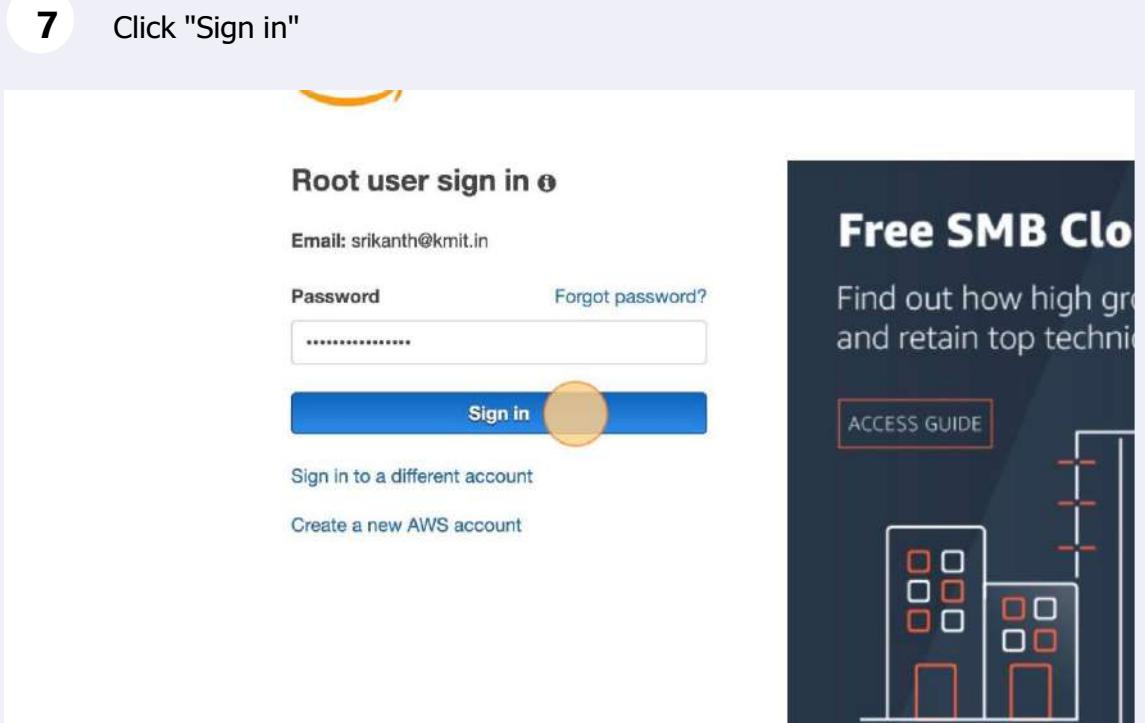


- 5** Click "Next"

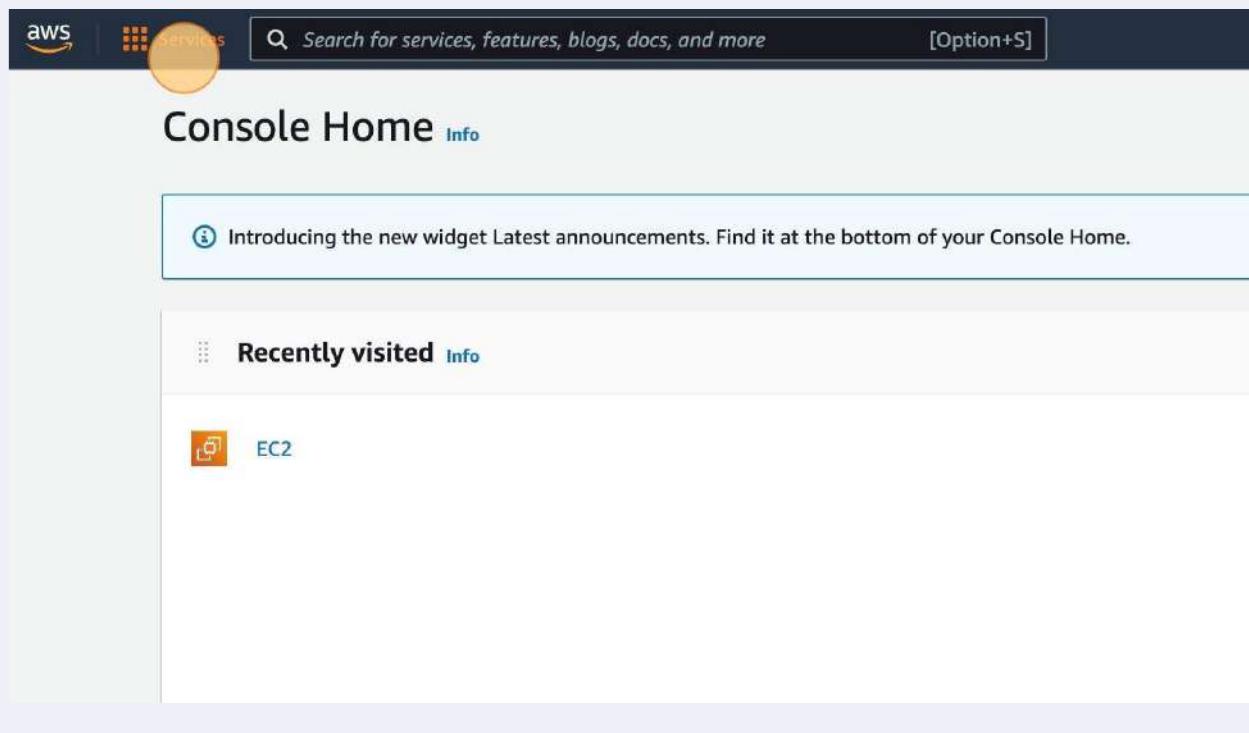
- 6** Click this password field.



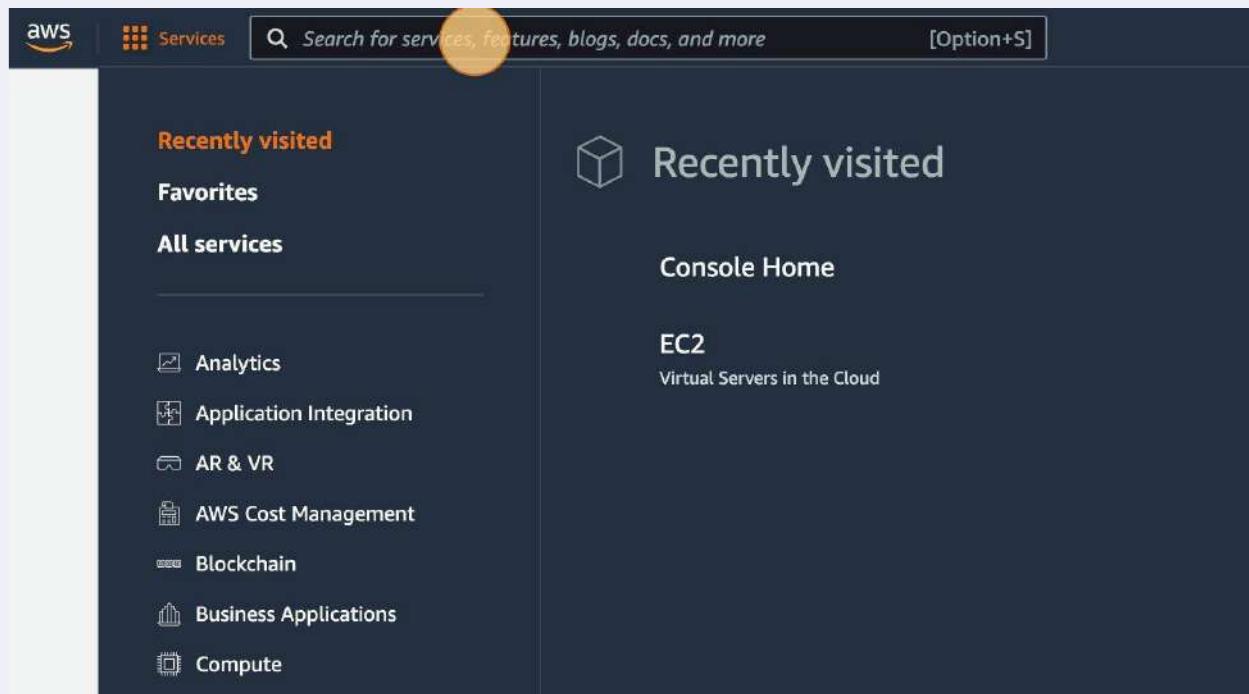
- 7** Click "Sign in"



8 Click "Services"



9 Click the "Search for services, features, blogs, docs, and more" field.



10 Type "EC2 [[enter]]"

11 Click "Instances"

The screenshot shows the AWS EC2 Dashboard. On the left sidebar, under the 'Instances' section, the 'Instances' link is highlighted with a yellow circle. The main content area displays various EC2 resources with counts: Instances (running) 0, Dedicated Hosts 0, Elastic IPs 0, Instances 0, Key pairs 1, Load balancers 0, Placement groups 0, Security groups 2, and Volumes 0. A callout box points to the 'Launch instance' button, which is described as easily sizing, configuring, and deploying Microsoft SQL Server Always On availability groups using the AWS Launch Wizard for SQL Server. To the right, there is a 'Service health' section with a status indicator.

12 Click "Launch instances"

The screenshot shows the AWS EC2 Instances page. At the top, there is a toolbar with a search bar labeled '[Option+S]', filter icons (grid, connect, instance state, actions), and a prominent orange 'Launch instances' button. Below the toolbar is a table header with columns: Instance state, Instance type, Status check, Alarm status, Availability Zone, and Pulse. Underneath the header, there is one row of data for an instance: Running (t2.micro), 2/2 checks passed, No alarms, us-east-2b, and ec2. The 'Launch instances' button is circled in yellow.

- 13** Click the "Name" field.

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

e.g. My Web Server



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

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

- 14** Click the "Name" field.



Services

Search for services, features, blogs, docs, and more

[Option+S]

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

AWS EC2 Instance



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

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

15 Type " [[enter]]"

16 Click here.

The screenshot shows the AWS Marketplace interface. At the top is a search bar with placeholder text: "Search our full catalog including 1000s of application and OS images". Below the search bar are two tabs: "Recents" and "Quick Start", with "Quick Start" being the active tab. Underneath the tabs are five quick-start links: Amazon Linux (with AWS logo), Ubuntu, Windows, Red Hat, and SUSE Linux. To the right of these links is a search icon and a link to "Browse more AMIs", which includes a note about including AMIs from AWS, Marketplace, and the Community. Below this section, a specific AMI is highlighted: "Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type". The details for this AMI are: ami-02d1e544b84bf7502 (64-bit (x86)) / ami-05e57de632660544c (64-bit (Arm)). It is noted as "Free tier eligible". A dropdown arrow is shown to the right of the AMI details. Below the highlighted AMI, there is a "Description" section containing the text: "Amazon Linux 2 Kernel 5.10 AMI 2 0 20220606 1 x86_64 HVM gn2".

17 Click "Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type"

The screenshot shows the AWS Quick Start interface. At the top, there are tabs for 'Recents' and 'Quick Start'. Below these are several AMI icons: Amazon Linux (selected), Ubuntu, Windows, Red Hat, SUSE Linux, and a search icon. A button labeled 'Browse more AMIs' is also present. The main content area displays the selected AMI: 'Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type'. It includes details like the AMI ID (ami-02d1e544b84bf7502), Virtualization type (hvm), ENA enabled status (true), and Root device type (ebs). A 'Free tier eligible' badge is shown. Below this, sections for 'Description' and 'Architecture' are visible, with the architecture dropdown set to '64-bit (x86)'.

18 Select 64-bit architecture.

This screenshot continues from the previous one, showing the selection of the 64-bit architecture. The 'Architecture' dropdown menu is open, displaying three options: '64-bit (x86)', '64-bit (x86)', and '64-bit (Arm)'. The first option is highlighted with a blue selection bar, and a yellow circle highlights the second option. The AMI ID 'ami-02d1e544b84bf7502' is also visible next to the selected architecture.

19 Click here.

▼ Instance type [Info](#)

Instance type

t2.micro Family: t2 1 vCPU 1 GiB Memory On-Demand Linux pricing: 0.0116 USD per Hour On-Demand Windows pricing: 0.0162 USD per Hour	Free tier eligible	Compare instance types
-----------------------------------------------------------------------------------------------------------------------------------------------------	--------------------	----------------------------------------

▼ 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

Looking for language selection? Find it in the new [Unified Settings](#)

[Create new key pair](#)

© 2022, Amazon

20 Click here.

aws Services [Search for services, features, blogs, docs, and more](#) [Option+S]

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type

ami-02d1e544b84bf7502 (64-bit (x86)) / ami-03e57de632660544c (64-bit (Arm))

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

Free tier eligible

<input type="text"/>
t2.nano Family: t2 1 vCPU 0.5 GiB Memory On-Demand Linux pricing: 0.0058 USD per Hour On-Demand Windows pricing: 0.0081 USD per Hour
t2.micro Family: t2 1 vCPU 1 GiB Memory On-Demand Linux pricing: 0.0116 USD per Hour On-Demand Windows pricing: 0.0162 USD per Hour
Free tier eligible
t2.small Family: t2 1 vCPU 2 GiB Memory On-Demand Linux pricing: 0.023 USD per Hour On-Demand Windows pricing: 0.032 USD per Hour
t2.medium Family: t2 2 vCPU 4 GiB Memory On-Demand Linux pricing: 0.0464 USD per Hour On-Demand Windows pricing: 0.0644 USD per Hour
t2.micro Family: t2 1 vCPU 1 GiB Memory On-Demand Linux pricing: 0.0116 USD per Hour
Free tier eligible

Compare instance types

21 Click here.

ux pricing: 0.0116 USD per Hour
ndows pricing: 0.0162 USD per Hour

(login) Info
key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch

required

Create new key pair

settings

Edit

Default subnet in any availability zone

Free tier: In your first 12 months of t2.micro usage, you get 1,000 hours of free instance usage on each Region in which you run an instance. Usage after this period is charged at the standard rate.

Cancel

22 Click here.

▼ 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

Proceed without a key pair (Not recommended) Default value

kmit
Type: rsa

test
Type: rsa

vpc-06979b155ac7b42d6

Subnet

No preference (Default subnet in any availability zone)

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022

23 Click the "Select existing security group" field.

vpc-06979b155ac7b42d6
Subnet
No preference (Default subnet in any availability zone)
Auto-assign public IP
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-3' with the following rules:
 Allow SSH traffic from Anywhere
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

24 Click "Select security groups"

difference (Default subnet in any availability zone)
sign public IP
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
Select security groups Info
Compare security group rules
groups that you add or remove here will be added to or removed from all your network interfaces.
Configure storage Info Advanced
GiB - gp2 Root volume
or language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Serv

26 Edit the "8" field.

The screenshot shows the 'Configure storage' section of the AWS Lambda console. At the top, there is a dropdown menu labeled 'Select security groups' with 'default sg-0092bd8cc91b732bf' selected and a VPC dropdown below it. To the right, there is a 'group rules' button. Below this, a note states: 'Security groups that you add or remove here will be added to or removed from all your network interfaces.' In the main configuration area, there is a heading 'Configure storage' with an 'Info' link and an 'Advanced' link. Underneath, there is a row for the root volume: '1x 8 GiB gp2'. The '8' value is highlighted with a yellow circle. To the right of this row is the label 'Root volume'. Below this row, there is a message: 'Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage' with a close button. At the bottom, there is a 'Add new volume' button and a section for file systems with a '0 x File systems' count and an 'Edit' link.

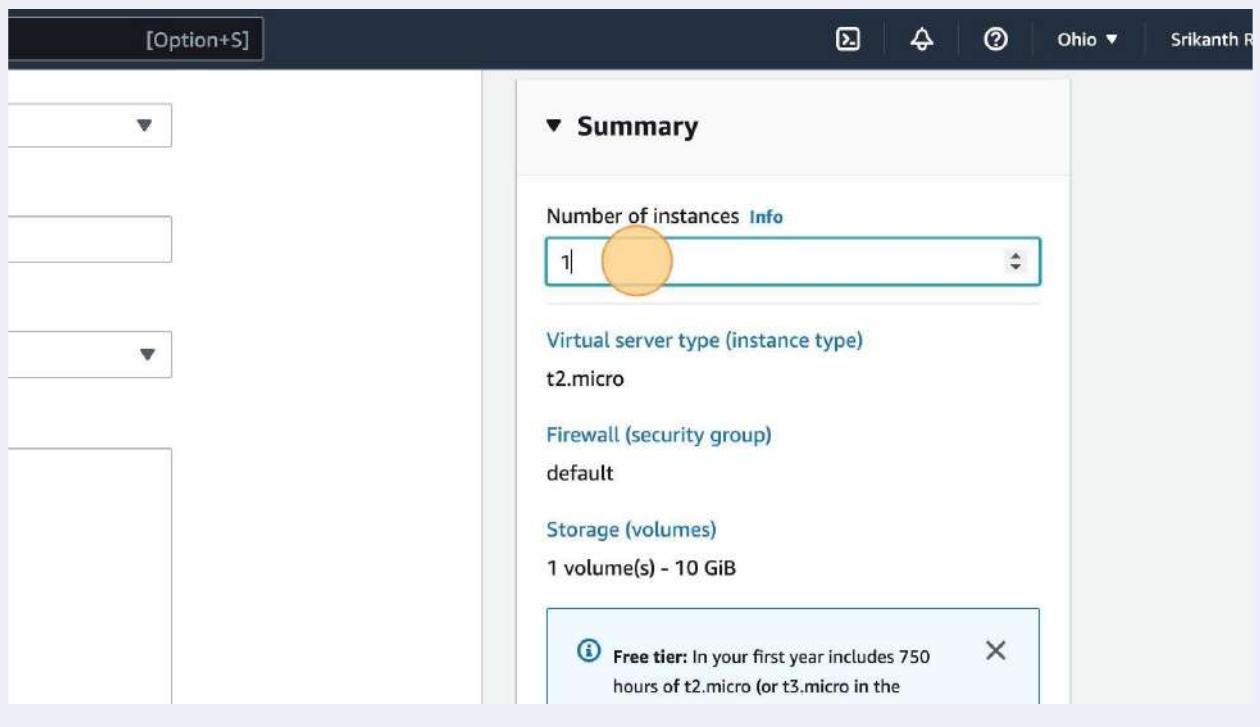
27 Type 10 GB for root volume.

The screenshot shows the 'Configure storage' section of the AWS Lambda setup. A yellow circle highlights the '10 GiB gp2' configuration for the root volume. An information box states: 'Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage'. Below this, there's an 'Add new volume' button and a section for file systems. At the bottom, a blue circle highlights the 'Advanced details' link.

28 Click "Advanced details Info" and leave as it is.

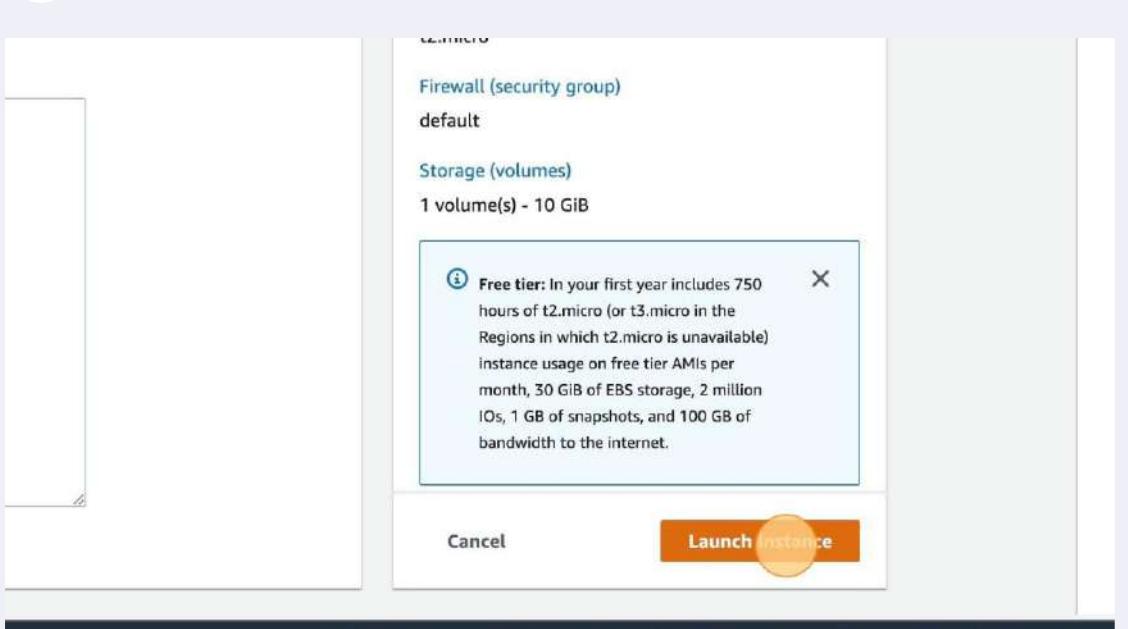
The screenshot shows the same 'Configure storage' section as the previous step, but with a yellow circle highlighting the 'Advanced details' link. The rest of the interface is identical to the previous screenshot.

29 Click the "Number of instances Info" field.

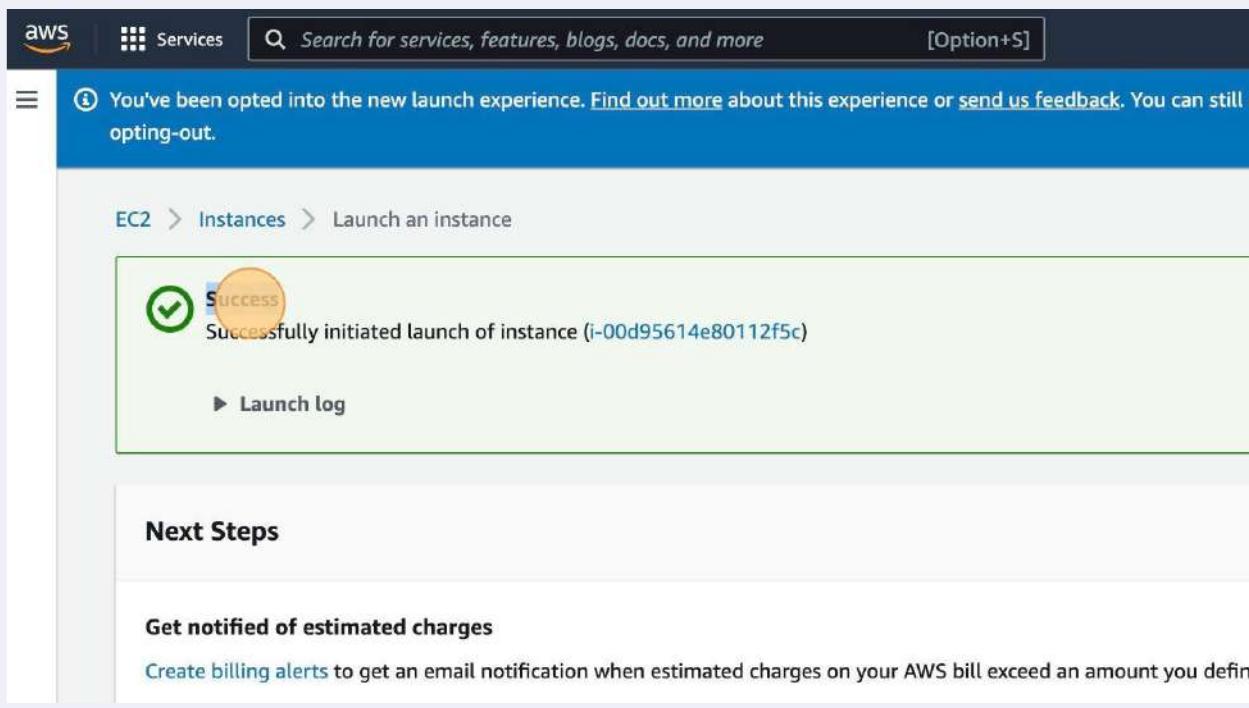


30 Type " [[Backspace]] 1 [[enter]]"

31 Click "Launch instance"

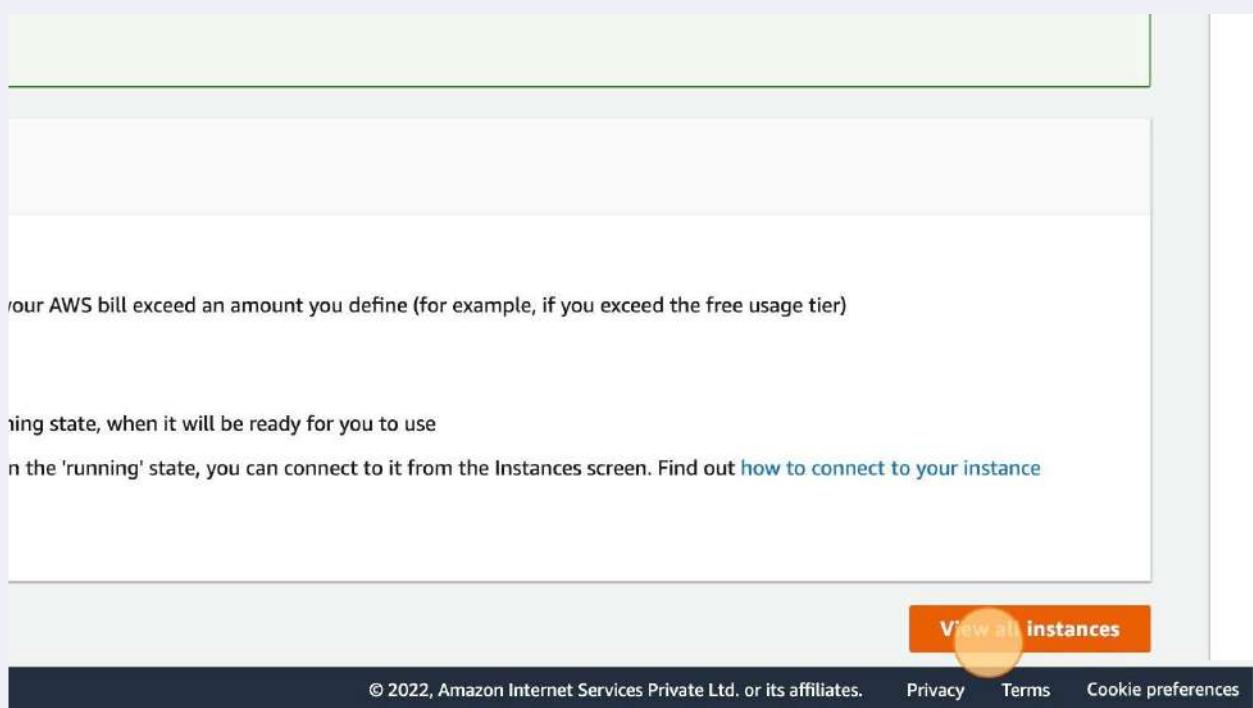


32 Created EC2 instance "Success"



The screenshot shows the AWS EC2 Instances Launch an instance page. At the top, there's a success message: "Successfully initiated launch of instance (i-00d95614e80112f5c)". Below it is a "Launch log" button. A "Next Steps" section follows, containing a "Get notified of estimated charges" link and a note about creating billing alerts.

33 Click "View all instances"



The screenshot shows the AWS EC2 Instances View all instances page. It features a large search bar at the top and a "View all instances" button at the bottom right. The main content area displays a message about estimated charges and a note about connecting to instances.

34 Right Click on the instance name.

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with options like EC2 Dashboard, EC2 Global View, Events, Tags, Limits, and Instances. Under Instances, there are links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, and Reserved Instances. The main area shows a table titled 'Instances (1/1)'. A single row is selected, with the 'Name' column containing 'AWS EC2 I...' highlighted by a yellow circle. Below the table, a section titled 'Instance: i-012ebd2c367f4ea45' is expanded, showing tabs for Details, Security, Networking, Storage, Status checks, and Monitoring. The 'Details' tab is active. At the bottom of the main area, there's a '▼ Instance summary' section and a 'Info' link.

35 Click "Connect"

This screenshot is similar to the previous one, showing the AWS EC2 Instances page. The sidebar and main table structure are identical. However, a context menu has been opened over the 'Name' field of the selected instance ('AWS EC2 I...'). The menu items listed are: Launch instances, Launch instance from template, Migrate a server, Connect (highlighted with a yellow circle), Stop instance, Start instance, Reboot instance, Hibernate instance, Terminate instance, Instance settings, Networking, Instance ID, Storage, Status checks, and Monitoring. The 'Details' tab is still active at the bottom.

36 Click "EC2 Instance Connect"

The screenshot shows the AWS EC2 Instance Connect interface. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, a search bar containing 'Search for services, features, blogs, docs, and more', and a keyboard shortcut '[Option+S]'. Below the navigation is a breadcrumb trail: 'EC2 > Instances > i-012ebd2c367f4ea45 > Connect to instance'. The main section is titled 'Connect to instance' with an 'Info' link. It says 'Connect to your instance i-012ebd2c367f4ea45 (AWS EC2 Instance) using any of these options'. There are four tabs: 'EC2 Instance Connect' (which is highlighted with a yellow circle), 'Session Manager', 'SSH client', and 'EC2 Serial Console'. Under 'EC2 Instance Connect', the 'Instance ID' is listed as 'i-012ebd2c367f4ea45 (AWS EC2 Instance)'. The 'Public IP address' is '3.17.141.196'. The 'User name' is 'ec2-user'. A note below says 'Connect using a custom user name, or use the default user name ec2-user for the AMI used to launch the instance.'

37 Click "Connect"

A modal dialog box is displayed, asking for confirmation to connect. It contains the text: 'user name ec2-user for the AMI used to launch the instance.' Below this, a note says 'Name is correct. However, read your AMI usage instructions to check if : AMI user name.' At the bottom of the dialog are two buttons: 'Cancel' and a large orange 'Connect' button, which is also highlighted with a yellow circle.

38 Instance will open in browser.

```
Last login: Thu Jun 16 06:46:41 2022 from ec2-3-16-146-2.us-east-2.compute.amazonaws.com  
[ec2-user@ip-172-31-31-32 ~]$ ls  
Amazon Linux 2 AMI  
[ec2-user@ip-172-31-31-32 ~]$ https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-172-31-31-32 ~]$ pwd  
/home/ec2-user  
[ec2-user@ip-172-31-31-32 ~]$ [REDACTED]
```

39 You can now start interacting with the instance.

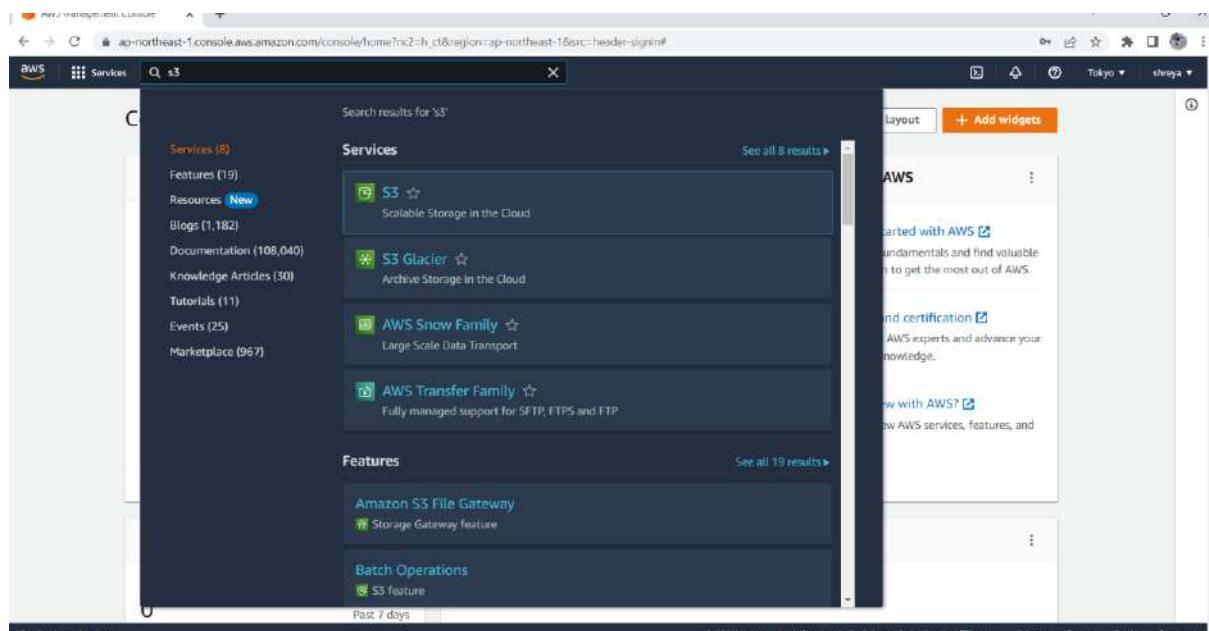
```
Last login: Thu Jun 16 06:46:41 2022 from ec2-3-16-146-2.us-east-2.compute.amazonaws.com  
[ec2-user@ip-172-31-31-32 ~]$ ls  
Amazon Linux 2 AMI  
[ec2-user@ip-172-31-31-32 ~]$ https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-172-31-31-32 ~]$ pwd  
/home/ec2-user  
[ec2-user@ip-172-31-31-32 ~]$ [REDACTED]
```

EXPERIMENT 2

Create your First AWS S3 Bucket and Upload Content to Bucket and Manage their Access and Create Static Website using AWS S3

Procedure to create S3 bucket:

- 1.Click on S3 services.
2. Provide bucket name and enable the acl's enabled.
3. Unblock all the public access settings for the bucket
- 4.Check box the acknowledgement, disable bucket versioning.
- 5.Provide default encryption as amazon s3-managed keys and bucket key as enable and click on create bucket.
- 6.Bucket is successfully created.**
7. After creation of bucket ,click on the bucket and go to permission tab, enable the ACL's permission to list and read.
8. Now right click on the bucket created, click **on upload to upload A file** here I uploaded kmit.Jpg
- 9.Click on upload and the file is **uploaded successfully**.
10. After upload of file once again go to permission tab of object check whether ACL's permission to list and read is enabled or not.
- 11.Now go back to the file been uploaded into the bucket
- 12.Right click onto the file and **go to properties**, Copy the object url and paste in browser,will be able to see the object uploaded publicly.



The screenshot shows the AWS S3 Management Console homepage. The main heading is "Amazon S3" with the subtext "Store and retrieve any amount of data from anywhere". Below this, a brief description states: "Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance." To the right, there are three main sections: "Create a bucket", "Pricing", and "Resources". The "Create a bucket" section contains a button labeled "Create Bucket". The "Pricing" section notes that there are no minimum fees and provides links to an AWS Simple Monthly Calculator and pricing details. The "Resources" section is currently empty. At the bottom, there are standard browser navigation and search bars, along with system status icons.

CLICK ON CREATE BUCKET

The screenshot shows the "Create bucket" configuration page. The top navigation bar includes "Services" and the current path "Amazon S3 > Buckets > Create bucket". The main section is titled "Create bucket" with a "Info" link. It explains that buckets are containers for data stored in S3. The "General configuration" section requires entering a "Bucket name" (e.g., "myawsbucket") and selecting an "AWS Region" (e.g., "Asia Pacific (Tokyo) ap-northeast-1"). There is also a "Copy settings from existing bucket - optional" section with a "Choose bucket" button. The "Object Ownership" section allows choosing between "ACLs disabled (recommended)" (selected) and "ACLs enabled". Both options provide detailed descriptions of how object ownership and access control will be managed. The bottom of the page includes standard browser navigation and search bars, along with system status icons.

PROVIDE BUCKET NAME AND CHANGE AWS REGION TO US EAST(OHIO)

The screenshot shows the AWS S3 'Create bucket' interface. In the 'General configuration' section, the 'Bucket name' is set to 'cseb' and the 'AWS Region' is set to 'US East (Ohio) us-east-2'. Under 'Object Ownership', 'ACLs disabled (recommended)' is selected. The bottom navigation bar includes links for 'Feedback', 'Language', and the current date '© 2023'.

UNBLOCK ALL THE PUBLIC ACCESS SETTINGS FOR THE BUCKET

The screenshot shows the 'Block Public Access settings for this bucket' page. It lists four settings under 'Block all public access': 'Block public access to buckets and objects granted through new access control lists (ACLS)', 'Block public access to buckets and objects granted through any access control lists (ACLS)', 'Block public access to buckets and objects granted through new public bucket or access point policies', and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies'. A warning message states: 'Turning off block all public access might result in this bucket and the objects within becoming public. AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.' A checkbox at the bottom acknowledges this risk. The bottom navigation bar includes links for 'Feedback', 'Language', and the copyright notice '© 2023, Amazon Web Services'.

CHECK BOX THE ACKNOWLEDGEMENT

The screenshot shows the 'Block public access' section of the AWS S3 Bucket Properties page. It contains two checkboxes:

- Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

A warning message in a red-bordered box states: "Turning off block all public access might result in this bucket and the objects within becoming public. AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting." Below it is a checkbox: " I acknowledge that the current settings might result in this bucket and the objects within becoming public."

A blue-bordered box contains a notice: "Upcoming permission changes to disable any Block Public Access setting. Starting in April 2023, to disable any Block Public Access setting when creating buckets by using the S3 console, you must have the s3:PutBucketPublicAccessBlock permission. [Learn more](#)"

Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

ENABLE THE BUCKET VERSIONING

Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning
 Disable
 Enable

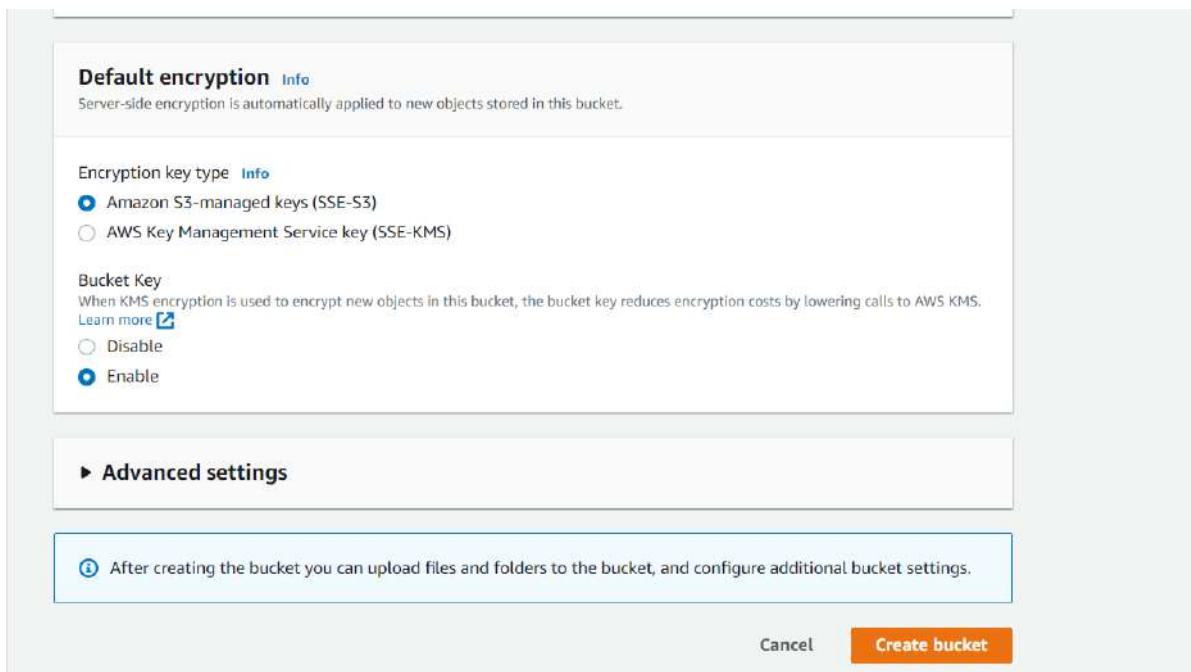
Tags (0) - optional
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

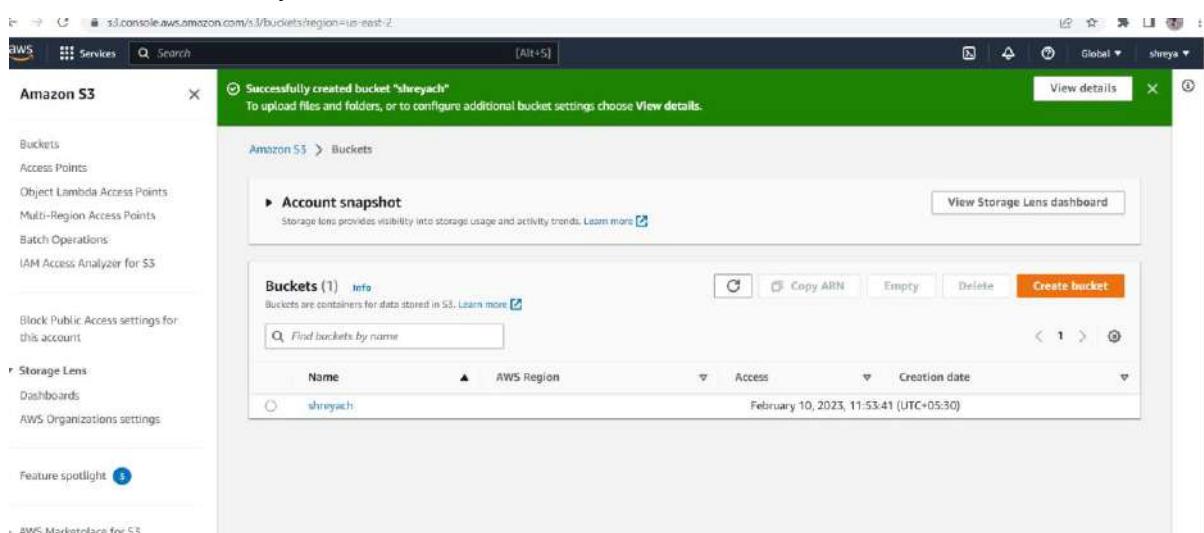
[Add tag](#)

PROVIDE DEFAULT ENCRYPTION AS Amazon S3-managed keys and bucket key as enable and

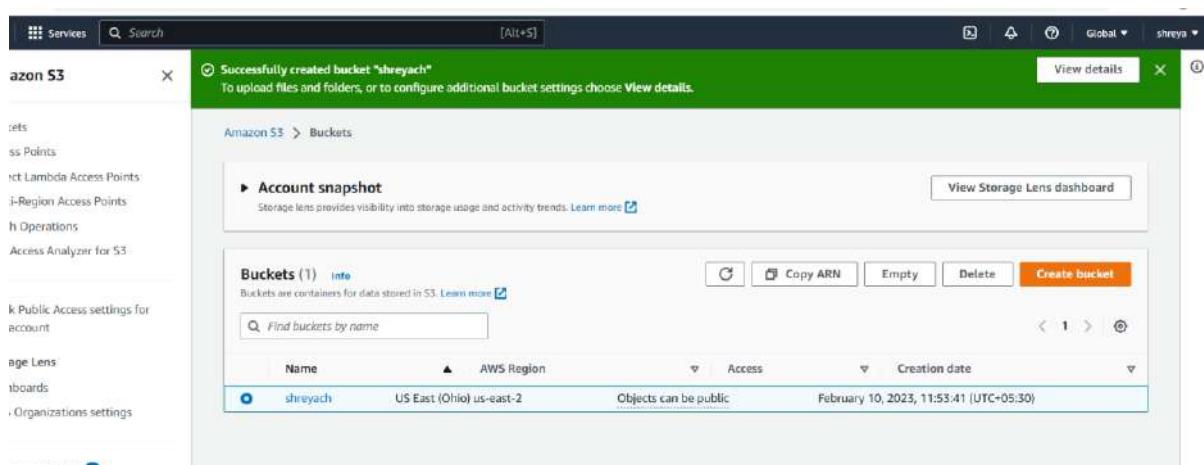
click on create bucket.



Bucket is successfully created.



Now right click on the bucket created



Click on upload to upload a file.

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with tabs: Objects (which is selected), Properties, Permissions, Metrics, Management, and Access Points. Below the navigation bar, the main area is titled "Objects (0)". A sub-instruction says: "Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory [?] to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more [?]" Below this, there's a toolbar with buttons for Copy S3 URI, Copy URL, Download, Open, Delete, Actions, Create folder, and Upload. There's also a search bar labeled "Find objects by prefix" and a "Show versions" checkbox. A pagination indicator shows page 1 of 1. The main table header includes columns for Name, Type, Last modified, Size, and Storage class. The table body displays a message: "No objects" and "You don't have any objects in this bucket." At the bottom right of the table area is another "Upload" button.

Here I uploaded kmit.jpg

The screenshot shows the AWS S3 console interface for uploading files. The title is "Upload [Info]". A sub-instruction says: "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 [?]" Below this is a large dashed box with the placeholder text: "Drag and drop files and folders you want to upload here, or choose Add files, or Add folders." Underneath is a table titled "Files and folders (1 Total, 7.0 KB)". It shows one item: "kmit.jpg" (image/jpeg, 7.0 KB). There are "Remove", "Add files", and "Add folder" buttons above the table. A search bar labeled "Find by name" and a pagination indicator are also present. The "Destination" section below the table shows the destination as "s3://shreyach". A "Destination details" section provides information about bucket settings.

Click on upload and the file is uploaded successfully.

The screenshot shows the AWS S3 console with a green header bar indicating "Upload succeeded". Below it, a summary table shows the destination bucket "shreyach" with 1 succeeded file (7.0 KB) and 0 failed files (0 B). A "Close" button is in the top right. Below the summary is a "Files and folders" section with one item: "kmit.jpg" (1 Total, 7.0 KB). A search bar and navigation icons are at the bottom.

Now go back to the file been uploaded into the bucket

The screenshot shows the AWS S3 console with the bucket "shreyach" selected. The "Objects" tab is active, displaying one object: "kmit.jpg" (Type: jpg, Last modified: February 10, 2023, 11:57:21 (UTC+05:30), Size: 7.0 KB, Storage class: Standard). The "Actions" menu is open, showing options like Copy S3 URI, Copy URL, Download, Open, Delete, Create folder, and Upload. A search bar and navigation icons are at the bottom.

Right click onto the file and go to properties

The screenshot shows the AWS S3 console with the bucket "shreyach" selected. The "Objects" tab is active, displaying one object: "kmit.jpg" (Type: jpg, Last modified: February 10, 2023, 11:57:21 (UTC+05:30), Size: 7.0 KB, Storage class: Standard). The "Actions" menu is open, showing options like Copy S3 URI, Copy URL, Download, Open, Delete, Create folder, and Upload. A search bar and navigation icons are at the bottom. The file "kmit.jpg" has a checked checkbox next to its name.

Copy the Object URL

Object overview

Owner: 319df62ce57eddc9306340/b2eb1bf32dd22fc98223599730c951618fa09c0

AWS Region: US East (Ohio) us-east-2

Last modified: February 10, 2023, 11:57:21 (UTC+05:30)

Size: 7.0 KB

Type: jpg

Key: kmit.jpg

S3 URI: s3://shreyach/kmit.jpg

Amazon Resource Name (ARN): arn:aws:s3:::shreyach/kmit.jpg

Entity tag (Etag): a0448e49ae2e779932520afb35d03c9a

Object URL: https://shreyach.s3.us-east-2.amazonaws.com/kmit.jpg

Paste it in another tab, it pops out error.

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>SYRHA0480HNP4EC4</RequestId>
<HostId>122001107a2y6YDv902NaH8tLFRGIBc6R966Q21SQwcc</HostId>
</Error>
```

Now go back ton S3 bucket

Bucket overview

AWS Region : US East (Ohio) us-east-2	Amazon Resource Name (ARN) : arn:aws:s3:::shreyach	Creation date : February 10, 2023, 11:53:41 (UTC+05:30)
----------------------------------------------	-----------------------------------------------------------	----------------------------------------------------------------

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more [\[\]](#)

Edit

Bucket Versioning: Enabled

Multi-factor authentication (MFA) delete: An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more [\[\]](#)

Disabled

Go to the uploaded file inside the bucket

The screenshot shows the AWS S3 console. In the top navigation bar, it says 'Amazon S3 > Buckets > shreyach'. Below the navigation, there's a tab bar with 'Objects' (which is selected), 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. Under the 'Objects' tab, it says 'Objects (1)'. A note below states: 'Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions.' There are several buttons at the top of the object list: 'Copy', 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'. A search bar says 'Find objects by prefix'. Below the search bar is a table with columns: Name, Type, Last modified, Size, and Storage class. One object is listed: 'kmit.jpg' (Type: jpg, Last modified: February 10, 2023, 11:57:21 (UTC+05:30), Size: 7.0 KB, Storage class: Standard).

Go to the permissions of bucket

The screenshot shows the 'Permissions' tab selected in the S3 console. It displays the 'Permissions overview' section, which includes a note: 'Objects can be public'. Below this is the 'Block public access (bucket settings)' section. It explains that public access is granted through ACLs, bucket policies, or access point policies. It recommends turning on 'Block all public access' to ensure no public access. It also notes that individual settings can be customized. An 'Edit' button is available. The 'Block all public access' setting is currently 'Off'. A note below says: 'Individual Block Public Access settings for this bucket'.

Now go to the Object Ownership

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.

[Edit](#)

Object Ownership

Bucket owner enforced

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

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

[Edit](#)

This bucket has the bucket owner enforced setting applied for Object Ownership

When bucket owner enforced is applied, use bucket policies to control access. [Learn more](#)

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account)	List, Write	Read, Write
Canonical ID: 319df62ce57edde9306340fb2eb1bf32dd22fcc98223399730c951618fba09ce		
Everyone (public access)		

Click on edit of the Object Ownership

Amazon S3 > Buckets > shreyach > Edit Object Ownership

Edit Object Ownership [Info](#)

Object Ownership

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

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

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

Object Ownership
Bucket owner enforced

[Cancel](#) [Save changes](#)

Check ACLS enabled and save the changes

Edit Object Ownership [Info](#)

Object Ownership

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

ACLs disabled (recommended)

All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

ACLs enabled

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



Enabling ACLs turns off the bucket owner enforced setting for Object Ownership

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

I acknowledge that ACLs will be restored.

Object Ownership

Bucket owner preferred

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

Object writer

The object writer remains the object owner.



If you want to enforce object ownership for new objects only, your bucket policy must specify that the

© 2022 Amazon Web Services India Private Limited. All Rights Reserved.

The changes are successfully saved

The screenshot shows the AWS S3 Bucket Permissions page for the bucket 'shreyach'. A green success bar at the top indicates 'Successfully edited Object Ownership.' The 'Permissions' tab is selected. In the 'Permissions overview' section, there is a single item under 'Access': a circular arrow icon. Below this is a section titled 'Block public access (bucket settings)' with a note about public access settings. At the bottom left, there is a small circular icon with a question mark.

Now edit the block public access

Edit Block public access (bucket settings) Info

Block public access (bucket settings)

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

Block all public access

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

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

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

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

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

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

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

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

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

Confirm the edits

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 within, you can customize the individual settings below to suit your specific storage use cases.

Edit Block public access (bucket settings)

Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, enter *confirm* in the field.

Cancel

Confirm

The changes are successfully done.

The screenshot shows the AWS S3 console. In the top navigation bar, there is a green banner message: "Successfully edited Block Public Access settings for this bucket." Below the banner, the URL is "Amazon S3 > Buckets > shreyach". The main navigation tabs are "Objects", "Properties", "Permissions" (which is highlighted in orange), "Metrics", "Management", and "Access Points". Under the "Permissions" tab, there is a section titled "Permissions overview" with a sub-section "Access".

Now edit the edit access control list(ACL)

The screenshot shows the "Edit access control list (ACL)" page. At the top, it says "Access control list (ACL)". Below that, it says "Grant basic read/write permissions to other AWS accounts. Learn more" with a link icon.

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account)	<input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Canonical ID: 319df62ce5 7eddc9306340fb2eb1bf32dd2 2fcc98223399730c951618fba0 9ce		
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	<input type="checkbox"/> List <input checked="" type="checkbox"/> Write	<input type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	<input type="checkbox"/> List <input checked="" type="checkbox"/> Write	<input type="checkbox"/> Read <input checked="" type="checkbox"/> Write
S3 log delivery group	<input type="checkbox"/> List	<input type="checkbox"/> Read

At the bottom, it says "© 2023, Amazon Web Services India Private Limited" and shows a taskbar with various icons.

Check the list and read near Everyone(public access)

Grant basic read/write permissions to other AWS accounts. Learn more		
Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: 319df62ce5 7eddc9306340fb2eb1bf32dd2 2fcc98223399730c951618fba0 9ce	<input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	<input checked="" type="checkbox"/> List <input type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write

When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can

Check box the option to make the changes.

Group: http://acs.amazonaws.com/groups/s3/LogDelivery	<input type="checkbox"/> Write	<input type="checkbox"/> Write
When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access the objects in this bucket. Learn more		
<input checked="" type="checkbox"/> I understand the effects of these changes on my objects and buckets.		
Access for other AWS accounts		
No other AWS accounts associated with the resource.		
Add grantee		

The changes are successfully made

Successfully edited access control list.

Amazon S3 > Buckets > shreyach

shreyach [Info](#)

Permissions

Objects Properties Permissions Metrics Management Access Points

Permissions overview

Now go to the uploaded file permissions to edit those permissions

The screenshot shows the AWS S3 console interface. At the top, the path is Amazon S3 > Buckets > shreyach > kmit.jpg. Below the path, there are four buttons: Copy S3 URI, Download, Open, and Object actions. Under the file name, there are three tabs: Properties, Permissions (which is selected), and Versions. In the Permissions section, there is a heading "Access control list (ACL)" with a link to "Grant basic read/write permissions to AWS accounts". A "Edit" button is located in the top right corner of this section. The main table lists grants for the object:

Grantee	Object	Object ACL
Object owner (your AWS account) Canonical ID: 319df62ce57eddc9306340fb2eb1bf32dd22fc98223399730c951618fba09ce	Read	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-

In the edit access control list provide both read permissions near everyone (public access)

The screenshot shows the "Edit access control list" page for the file kmit.jpg. The URL in the address bar is Amazon S3 > Buckets > shreyach > kmit.jpg > Edit access control list. The page title is "Edit access control list". The "Access control list (ACL)" section includes a link to "Grant basic read/write permissions to AWS accounts". The main table allows editing of permissions for different groups:

Grantee	Objects	Object ACL
Object owner (your AWS account) Canonical ID: 319df62ce57eddc9306340fb2eb1bf32dd22fc98223399730c951618fba09ce	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	<input checked="" type="checkbox"/> ⚠️ Read <input type="checkbox"/> Write	<input checked="" type="checkbox"/> ⚠️ Read <input type="checkbox"/> Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	<input type="checkbox"/> Read <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write

Check the box to make the changes

⚠️ When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.

[Learn more](#)

I understand the effects of these changes on this object.

Access for other AWS accounts

No other AWS accounts associated with the resource.

[Add grantee](#)

Specified objects

The changes are successfully made

Successfully edited access control list for object "kmit.jpg".

Amazon S3 > Buckets > shreyach > kmit.jpg

kmit.jpg [Info](#)

[Copy S3 URI](#) [Download](#) [Open](#) [Object actions](#)

Now go back to the properties of the file uploaded inside s3 bucket and copy the url

Successfully edited access control list for object "kmit.jpg".

Amazon S3 > Buckets > shreyach > kmit.jpg

kmit.jpg [Info](#)

[Properties](#) [Permissions](#) [Versions](#)

Object overview

Owner	S3 URI
319df62ce57eddc9306340fb2eb1bf32dd22fcc98223399730c951618fba09ce	s3://shreyach/kmit.jpg
AWS Region	Amazon Resource Name (ARN)
US East (Ohio) us-east-2	arn:aws:s3:::shreyach/kmit.jpg
Last modified	Entity tag (Etag)
February 10, 2023, 11:57:21 (UTC+05:30)	a0448e49ae2e779952320afb33d05c9a
Size	Object URL
7.0 KB	https://shreyach.s3.us-east-2.amazonaws.com/kmit.jpg
Type	
jpg	

The URL is successfully copied.

SWS Services Search [Alt+F5] Global shreyach

Successfully edited access control list for object 'kmit.jpg'.

Amazon S3 > Buckets > shreyach > kmit.jpg

kmit.jpg [Info](#)

[Copy S3 URI](#) [Download](#) [Open](#) [Object actions](#)

[Properties](#) [Permissions](#) [Versions](#)

Object overview

Owner: 319df62cce57eddc9306340fb2eb1bf32dd22fcc98225399730c951618fb09ce

AWS Region: US East (Ohio) us-east-2

Last modified: February 10, 2023, 11:57:21 (UTC+05:30)

Size: 7.0 KB

Type: jpg

S3 URI: s3://shreyach/kmit.jpg

Amazon Resource Name (ARN): arnaws:s3::shreyach/kmit.jpg

Entity tag (Etag): a0448e49ac0e779952320afb53d03c9a

Object URL Copied

<https://shreyach.s3.us-east-2.amazonaws.com/kmit.jpg>

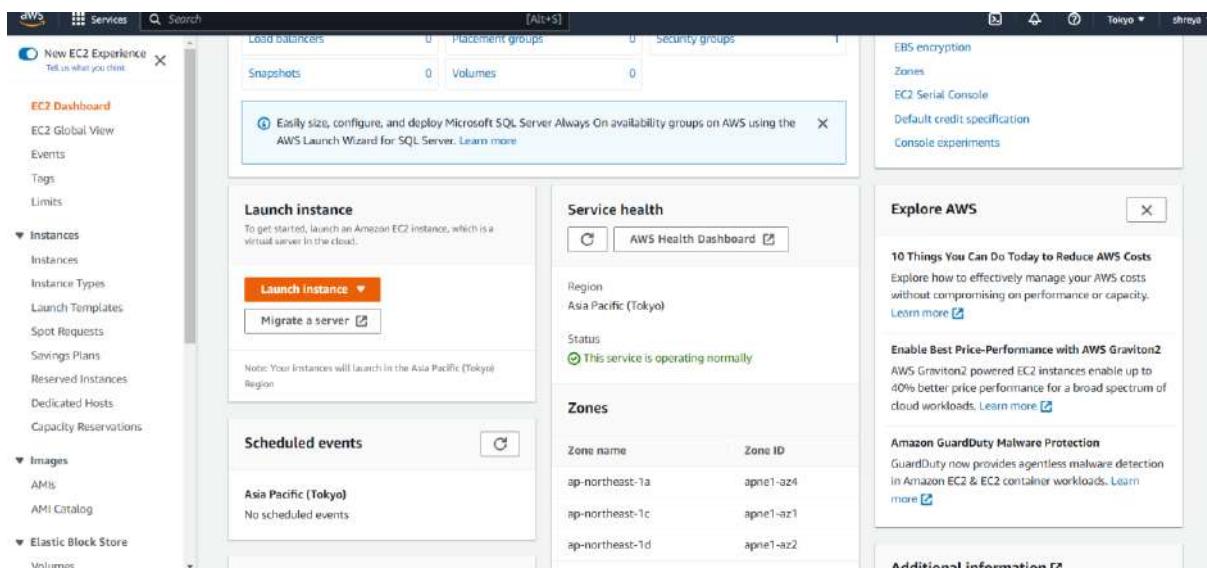
Paste the URL in another tab to obtain the output as follows.



EXPERIMENT 3

Create and configure storage services and upload files and objects using Amazon EBS.

1. Open the Amazon EC2 console and Launch Ec2 Instance .
2. In the Left navigation pane, choose Elastic Block store..select **Volumes**.
3. Choose **Create volume**.
4. For **Volume type**, choose the type of volume to create select default ssd
5. For **Size**, enter the size of the volume, in GiB example 15GB.
6. For **Availability Zone**, choose the Availability Zone in which to create the volume. A volume can be attached only to an instance that is in the same Availability Zone.
7. Choose **Create volume** and in actions selct attach and connect to the Running instance.
8. **Note :** The volume is ready for use when the **Volume state is available**.
9. 8. Again In the left navigation pane, choose **Volumes**.
10. 9. Select the volume which was created with 15GB ,enable it and choose **Actions , Attach volume**.
11. **Note :** You can attach only volumes that are in the Available state.
12. 10. For **Instance**, enter the ID of the instance or select the instance from the list of options.
13. **Note :** The volume must be attached to an instance in the same Availability Zone.
14. 11. For **Device name**, enter a supported device name for the volume. This device name is used by Amazon EC2..
15. 12. Choose **Attach volume**
16. 13. Connect to the instance and mount the volume.
17. 14. After that go t the instance dash board and click on storage then you will be able to see the attached EBS volume to the instance.



The screenshot shows the AWS EC2 'Launch an instance' configuration page. Key fields include:

- Name and tags**: Name is set to "e.g. My Web Server".
- Software Image (AMI)**: Set to "Amazon Linux 2 Kernel 5.10 AMI...".
- Virtual server type (instance type)**: Set to "t2.micro".
- Storage (volumes)**: 1 volume(s) - 8 GB.

A tooltip for "Free tier" indicates it includes 750 hours of t2.micro or t3.micro usage in regions where t2.micro is unavailable, plus 30 GB of EBS storage per month. The "Launch Instance" button is visible at the bottom right.

This screenshot shows a more detailed view of the EC2 instance launch configuration:

- Name and tags**: Name is set to "shreya".
- Application and OS Images (Amazon Machine Image)**: Shows a search bar and a "Quick Start" section with various OS icons (Amazon Linux, macOS, Ubuntu, Windows, Red Hat, etc.).
- Amazon Machine Image (AMI)**: A specific AMI is selected: "Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type".
- Virtual server type (instance type)**: Set to "t2.micro".
- Storage (volumes)**: 1 volume(s) - 8 GB.

A tooltip for "Free tier" is displayed again, stating it includes 750 hours of t2.micro or t3.micro usage in regions where t2.micro is unavailable, plus 30 GB of EBS storage per month. The "Launch Instance" button is at the bottom right.

The screenshot shows the AWS EC2 console with the URL ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#LaunchInstances. The page is titled "Launch an instance | EC2 Manager".

Name and tags: A text input field where "shreya" has been typed. There is also a "Add additional tags" button.

Application and OS Images (Amazon Machine Image): A section listing various AMI categories: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, and others. A search bar is present above the list.

Quick Start: A grid of icons representing different AMIs: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, and others. A "Browse more AMIs" link is available.

Summary: A summary of the launch configuration:

- Number of instances: 1
- Software Image (AMI): Canonical, Ubuntu, 22.04 LTS, ami-0b828c1ca5acff13ae
- Virtual server type (instance type): t2.micro
- Firewall (security group): New security group
- Storage (volumes): 1 volume(s) - 8 GiB

A tooltip for the "Free tier" is displayed: "In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage."

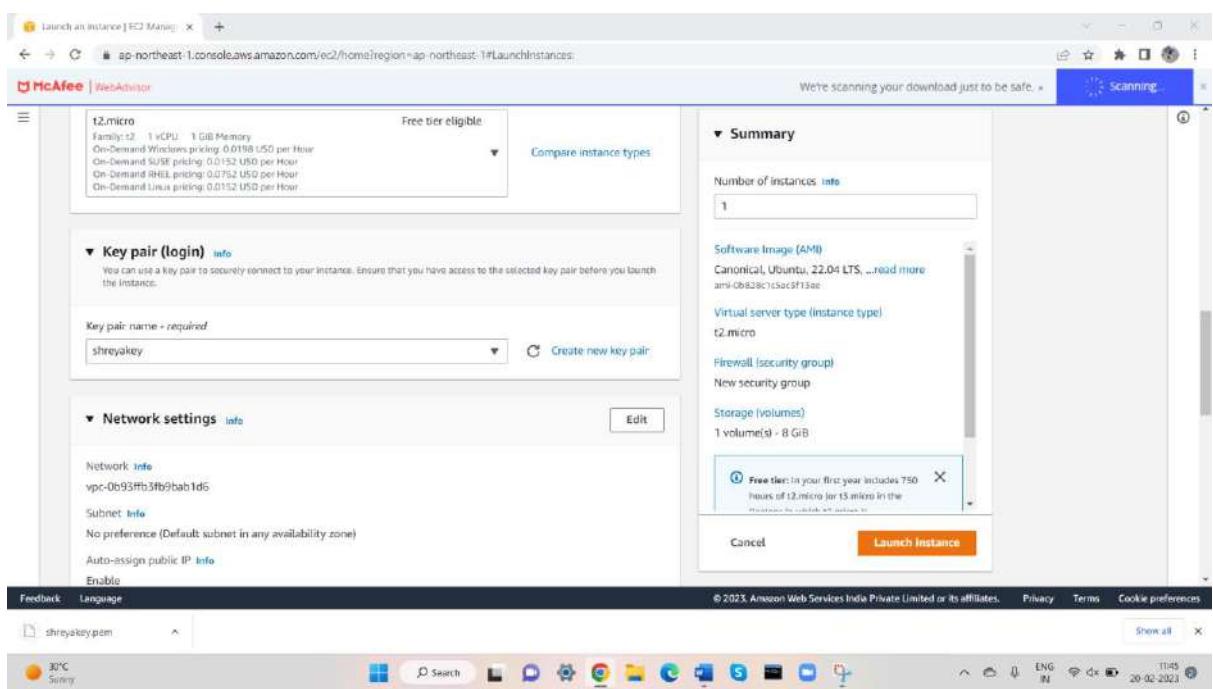
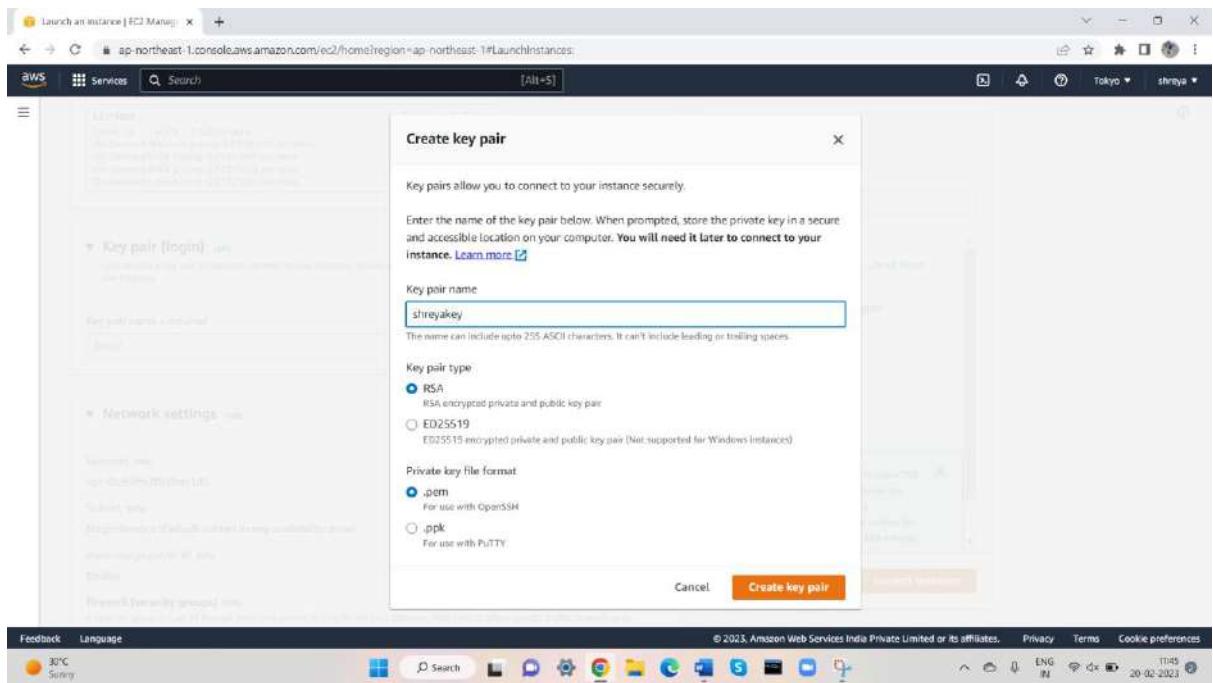
Buttons: "Cancel" and "Launch Instance" (highlighted in orange).

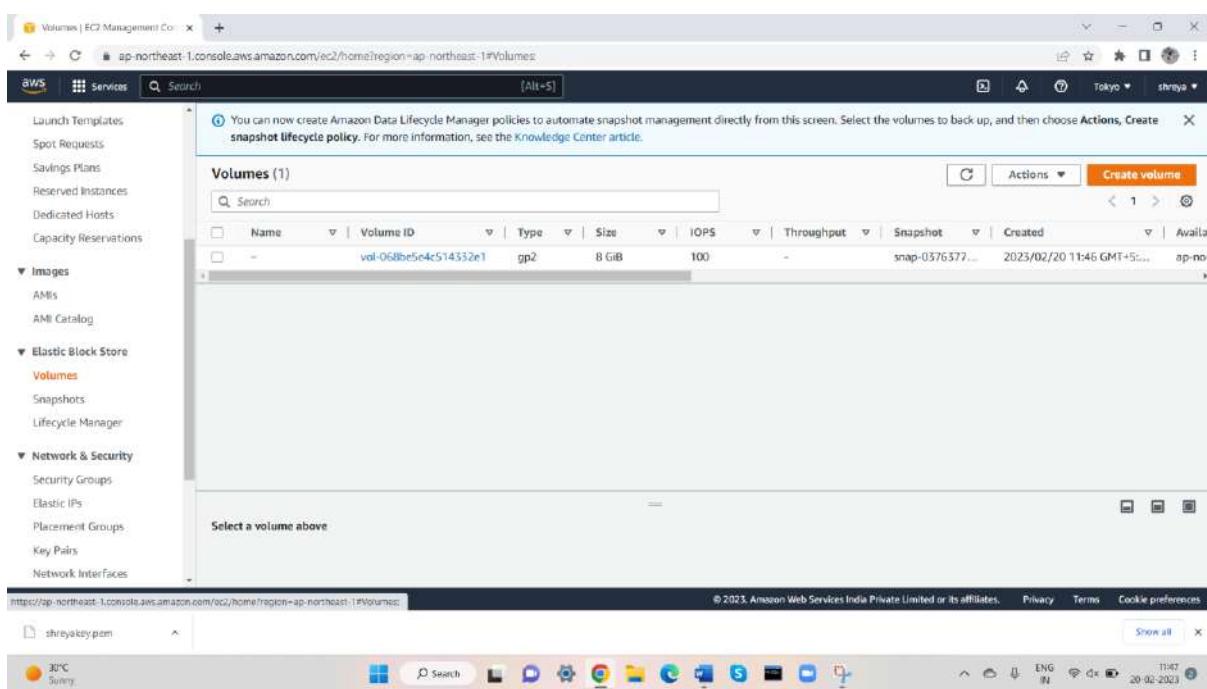
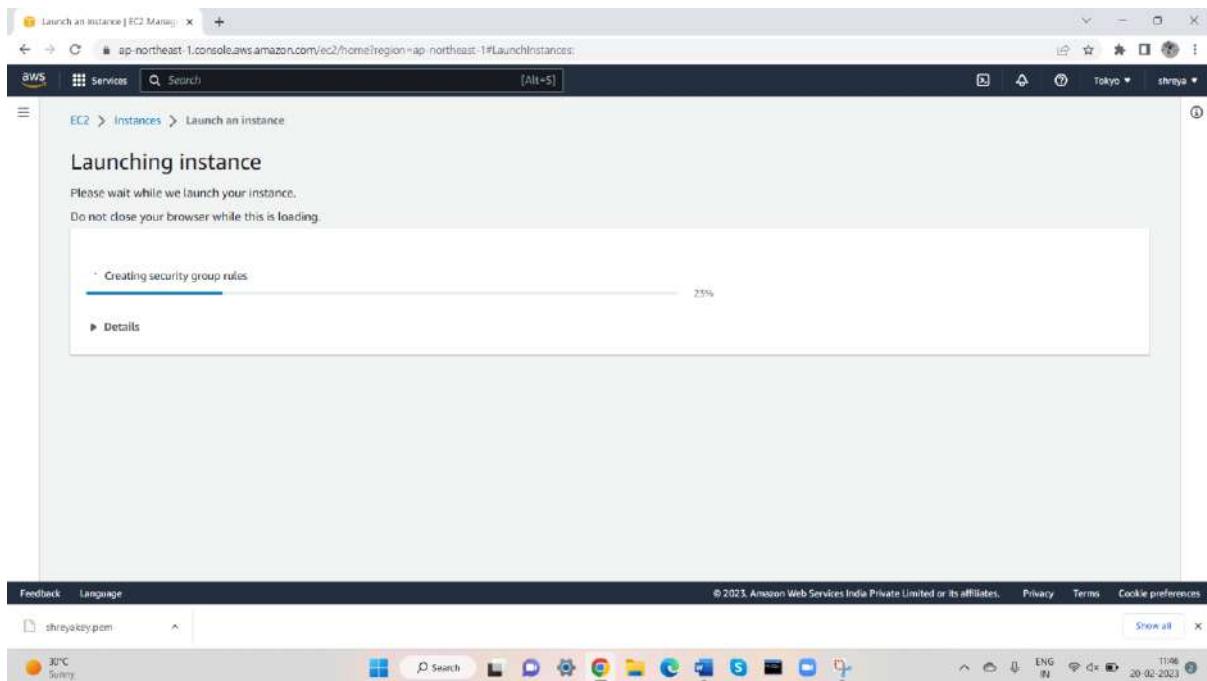
The screenshot shows the AWS EC2 console with the URL ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#LaunchInstances. The page is titled "Launch an instance | EC2 Manager".

Create key pair: A modal dialog box with the following fields:

- Key pair name:** An input field with the placeholder "Enter key pair name".
- Key pair type:** A radio button selected for "RSA" (RSA encrypted private and public key pair). There is also an option for "ED25519" (Ed25519 encrypted private and public key pair, not supported for Windows instances).
- Private key file format:** A radio button selected for ".pem" (For use with OpenSSH). There is also an option for ".ppk" (For use with PuTTY).

Buttons: "Cancel" and "Create key pair" (highlighted in orange).





The screenshot shows the 'Create volume' page in the AWS EC2 Management console. The 'Volume settings' section is open, displaying the following configuration:

- Volume type:** General Purpose SSD (gp2)
- Size (GB):** 100 (with a note: Min: 1 GB, Max: 16384 GB)
- IOPS:** 300 / 3000 (Baseline of 3 IOPS per GB with a minimum of 100 IOPS, burstable to 3000 IOPS)
- Throughput (MB/s):** Not applicable
- Availability Zone:** ap-northeast-1a

At the bottom of the page, there are links for Feedback, Language, and cookie preferences, along with a status bar showing the user's name (shreya) and the date (20-02-2023).

This screenshot shows the same 'Create volume' page with additional settings visible:

- Volume type:** General Purpose SSD (gp2)
- Size (GB):** 10 (with a note: Min: 1 GB, Max: 16384 GB)
- IOPS:** 100 / 3000 (Baseline of 3 IOPS per GB with a minimum of 100 IOPS, burstable to 3000 IOPS)
- Throughput (MB/s):** Not applicable
- Availability Zone:** ap-northeast-1a
- Snapshot ID - optional:** Don't create volume from a snapshot

The interface includes standard AWS navigation elements like Services, Search, and the AWS logo at the top, and a status bar at the bottom.

Create volume | EC2 Management

ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#CreateVolume:

Volume type [Info](#)
General Purpose SSD (gp2)

Size (GB) [Info](#)
10
Min: 1 GB, Max: 16384 GB. The value must be an integer.

IOPS [Info](#)
100 / 3000
Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS.

Throughput (MiB/s) [Info](#)
Not applicable

Availability Zone [Info](#)
ap-northeast-1c

Snapshot ID - optional [Info](#)
Don't create volume from a snapshot

Encryption [Info](#)
Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.
 Encrypt this volume

Feedback Language Show all

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

shreyakay.pem

30°C Sunny

11:52 20-02-2023

Volumes | EC2 Management

ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#Volumes:

New EC2 Experience Tell us what you think

Successfully created volume vol-051bbd130b95fc1a9

You can now create Amazon Data Lifecycle Manager policies to automate snapshot management directly from this screen. Select the volumes to back up, and then choose **Actions**, **Create snapshot lifecycle policy**. For more information, see the [Knowledge Center article](#).

Volumes (2)

Search

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created	Available
-	vol-051bbd130b95fc1a9	gp2	10 GB	100	-	-	2023/02/20 11:48 GMT+5...	ap-nor
-	vol-068be5a4c514332e1	gp2	8 GB	100	-	snap-0376377...	2023/02/20 11:46 GMT+5...	ap-nor

Select a volume above

Feedback Language Show all

shreyakay.pem

30°C Sunny

11:48 20-02-2023

Screenshots showing the AWS EC2 Management Console - Volumes page after creating a volume.

The top screenshot shows the main Volumes list with two volumes:

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created	Available
-	vol-051bbd130b95fc1a9	gp2	10 GB	100	-	-	2023/02/20 11:48 GMT+5....	ap-nor
-	vol-068be5e4c514332e1	gp2	8 GB	100	-	snap-037657... (1)	2023/02/20 11:46 GMT+5....	ap-nor

The bottom screenshot shows the "Actions" dropdown menu for the first volume (vol-051bbd130b95fc1a9). The "Modify volume" option is selected.

- Actions ▾
- Modify volume
- Create snapshot
- Create snapshot lifecycle policy
- Delete volume
- Attach volume
- Detach volume
- Force detach volume
- Manage auto-enabled I/O
- Manage tags
- Fault injection

Screenshots showing the AWS EC2 Management Console - Volumes page after creating a volume.

The top screenshot shows the main Volumes list with two volumes:

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created	Available
-	vol-051bbd130b95fc1a9	gp2	10 GB	100	-	-	2023/02/20 11:48 GMT+5....	ap-nor
-	vol-068be5e4c514332e1	gp2	8 GB	100	-	-	2023/02/20 11:46 GMT+5....	ap-nor

The bottom screenshot shows the "Actions" dropdown menu for the first volume (vol-051bbd130b95fc1a9). The "Modify volume" option is selected.

- Actions ▾
- Modify volume
- Create snapshot
- Create snapshot lifecycle policy
- Delete volume
- Attach volume
- Detach volume
- Force detach volume
- Manage auto-enabled I/O
- Manage tags
- Fault injection

The screenshot shows the 'Attach volume' page in the AWS EC2 Management console. The URL is ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#AttachVolumevolumeId=vol-051bbd130b95fc1a9. The page title is 'Attach volume'. It displays basic details for the volume, including its ID (vol-051bbd130b95fc1a9) and availability zone (ap-northeast-1a). The 'Instance info' dropdown is set to 'Only instances in the same Availability Zone as the selected volume are displayed.' The 'Device name' field is empty. At the bottom right is the 'Attach volume' button.

The screenshot shows the 'Attach volume' page in the AWS EC2 Management console. The URL is ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#AttachVolumevolumeId=vol-0c8825616475829bb. The page title is 'Attach volume'. It displays basic details for the volume, including its ID (vol-0c8825616475829bb) and availability zone (ap-northeast-1c). The 'Instance info' dropdown is populated with the instance ID 'i-0d19493a5cbf7077c' and the label '(shreyal training)'. At the bottom right is the 'Attach volume' button.

Attach volume | EC2 Management

ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#AttachVolumevolume/d=vol-0c8825616475829bb

Services Search [Alt+S]

Basic details

Volume ID: vol-0c8825616475829bb

Availability Zone: ap-northeast-1c

INSTANCE INFO: i-0d19493a5cbf7077c

Device name: /dev/sdf

Recommended device names for Linux: /dev/xvda1 for root volume, /dev/sdf[1] for data volumes.

INFO: Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdः internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.

Cancel Attach volume

Feedback Language shreyakay.pem Show all © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

80°F Sunny 11:55 20-02-2023

Volumes | EC2 Management

ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#Volumes

New EC2 Experience Tell what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Feedback Language shreyakay.pem Show all © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

80°F Sunny 11:55 20-02-2023

Successfully attached volume vol-0c8825616475829bb to instance i-0d19493a5cbf7077c

You can now create Amazon Data Lifecycle Manager policies to automate snapshot management directly from this screen. Select the volumes to back up, and then choose Actions, Create snapshot lifecycle policy. For more information, see the Knowledge Center article.

Volumes (2)

Actions Create volume

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created	Available
-	vol-068be5e4c514332e1	gp2	8 GiB	100	-	snap-0376377...	2023/02/20 11:46 GMT+5...	ap-nor
-	vol-0c8825616475829bb	gp2	10 GiB	100	-	-	2023/02/20 11:55 GMT+5...	ap-nor

Select a volume above

Dashboard | EC2 Management < + ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#Home: https://ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#Home:

New EC2 Experience Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances Instances Types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts Capacity Reservations

Images AMIs AMI Catalog

Launch Instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch Instance Migrate a server

Note: Your instances will launch in the Asia Pacific (Tokyo) Region

Scheduled events

Asia Pacific (Tokyo) No scheduled events

Migrate a server

Service health

AWS Health Dashboard

Region Asia Pacific (Tokyo)

Status This service is operating normally.

Zones

Zone name	Zone ID
ap-northeast-1a	apne1-az4
ap-northeast-1c	apne1-az1
ap-northeast-1d	apne1-az2

Enable additional Zones

Default credit specification

Console experiments

Explore AWS

Enable Best Price-Performance with AWS Graviton2

AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads. Learn more

Amazon GuardDuty Malware Protection

GuardDuty now provides agentless malware detection in Amazon EC2 & EC2 container workloads. Learn more

Save up to 90% on EC2 with Spot Instances

Optimize price-performance by combining EC2 purchase options in a single EC2 ASG. Learn more

Additional information

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences Show all

shreyakey.pem

80°F Sunny

11:55 20-02-2023

Instances | EC2 Management Con X + ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#Instances: https://ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#Instances:

New EC2 Experience Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances Instances Types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts Capacity Reservations

Images AMIs AMI Catalog

Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
shreya	i-0d19493a5cbf7077c	Running	t2.micro	2/2 checks passed	No alarms	ap-northeast-1c	ec2-3-115-19-22

Instance: i-0d19493a5cbf7077c (shreya)

Details Security Networking Storage Status checks Monitoring Tags

Root device details

Root device name /dev/sda1 Root device type EBS EBS optimization disabled

Block devices

Filter block devices

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences Show all

shreyakey.pem

80°F Sunny

11:56 20-02-2023

The screenshot shows the AWS EC2 Management Console. On the left, there's a sidebar with navigation links for EC2 Dashboard, Global View, Events, Tags, Limits, Instances (with sub-links for Instances Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations), and Images (AMIs, Catalog). The main content area is titled 'Instances (1/1) Info'. It lists one instance: 'shreya' (i-0d19493a5cbf7077c), which is 'Running' on an 't2.micro' instance type. The 'Actions' dropdown menu is open, showing options like Launch instances, Stop instance, Start instance, and Terminate instance. Below the instance list, there's a table for 'Filter block devices' and a section for 'Recent root volume replacement tasks'.

DELETION

This screenshot is similar to the previous one, showing the AWS EC2 Management Console. The 'shreya' instance is still running. The Actions dropdown menu is open, and the 'Terminate instance' option is highlighted with a yellow background. Other options like Launch instances, Stop instance, and Start instance are also visible.

EC2 Management Console

ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#Instances:

New EC2 Experience Tell what you think

Instances (1/1) Info

Stop instance?

Instance IDs
i-0d19493a5cbf7077c (shreya)

To confirm that you want to stop the instance, choose the Stop button below.

Cancel Stop

Details Security Networking Metrics

Instance summary info

Instance ID i-0d19493a5cbf7077c (shreya)

Public IPv4 address 3.115.19.226 | open address

Private IPv4 addresses 172.31.12.170

InstanceState Stopping

Instance type t2.micro

Status checks 2/2 checks passed

Alarm status No alarms

Availability Zone ap-northeast-1c

Public IPv4 DNS ec2-3-115-19-226.ap-northeast-1.compute.amazonaws.com | open address

Feedback Language

shreya.pem

80°F Sunny

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Show all

11:58 20-02-2023

EC2 Management Console

ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#Instances:

New EC2 Experience Tell what you think

Instances (1/1) Info

Successfully stopped i-0d19493a5cbf7077c

Instances (1/1) Info

Instance: i-0d19493a5cbf7077c (shreya)

Details Security Networking Storage Status checks Monitoring Tags

Instance summary info

Instance ID i-0d19493a5cbf7077c (shreya)

Public IPv4 address 3.115.19.226 | open address

Private IPv4 addresses 172.31.12.170

IPv6 address -

InstanceState Running

Hostname type

Private IP DNS name (IPv4 only)

Feedback Language

shreya.pem

80°F Sunny

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Show all

11:58 20-02-2023

Screenshot of the AWS EC2 Management Console showing the Instances page. An instance named 'shreya' (ID: i-0d19493a5cbf7077c) is selected. A context menu is open over the instance row, with 'Terminate instance' highlighted.

Instances (1/1) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
shreya	i-0d19493a5cbf7077c	Stopped	t2.micro	-	No alarms	ap-northeast-1c	-

Instance: i-0d19493a5cbf7077c (shreya)

Details | Security | Networking | Storage

Instance summary

Instance ID	i-0d19493a5cbf7077c (shreya)
IPv6 address	-
Hostname type	Private IP DNS name (IPv4 only)
IP name	ip-172-31-12-170.ap-northeast-1.compute.internal
IP name	ip-172-31-12-170.ap-northeast-1.compute.internal

Networking

Security

Image and templates

Monitor and troubleshoot

Tags

Private IPv4 addresses: 172.31.12.170
Public IPv4 DNS:

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Screenshot of the AWS EC2 Management Console showing the Instances page. A confirmation dialog box titled 'Terminate instance?' is displayed.

Terminate instance?

On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost.

Are you sure you want to terminate these instances?
i-0d19493a5cbf7077c (shreya)

Clean up associated resources

Associated resources may incur costs after these instances are terminated.

► Delete EBS volumes

To confirm that you want to terminate the instances, choose the terminate button below. Terminating the instance cannot be undone.

Cancel | **Terminate**

Instances (1/1) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
shreya	i-0d19493a5cbf7077c	Terminating	t2.micro	-	No alarms	ap-northeast-1c	-

Instance summary

Instance ID	i-0d19493a5cbf7077c (shreya)
IPv6 address	-
Hostname type	Private IP DNS name (IPv4 only)
IP name	ip-172-31-12-170.ap-northeast-1.compute.internal
IP name	ip-172-31-12-170.ap-northeast-1.compute.internal

Networking

Security

Image and templates

Monitor and troubleshoot

Tags

Private IPv4 addresses: 172.31.12.170
Public IPv4 DNS:

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Instances | EC2 Management Con

ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#Instances:

New EC2 Experience Tell what you think

EC2 Dashboard EC2 Global View Events Tags Limits Instances Instances Types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts Capacity Reservations Images AMIs AMI Catalog Feedback Language shreyakey.pem

Successfully terminated i-0d19493a5cbf7077c

Instances (1/1) Info Connect Instance state Actions Launch instances

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
shreya	i-0d19493a5cbf7077c	Shutting-down	t2.micro	-	No alarms	ap-northeast-1c	-

Instance: i-0d19493a5cbf7077c (shreya)

Details Security Networking Storage Status checks Monitoring Tags

Instance summary

Instance ID	Public IPv4 address	Private IPv4 addresses
i-0d19493a5cbf7077c (shreya)	-	172.31.12.170

IPv6 address Instance state Public IPv4 DNS

Hostname type Private IP DNS name (IPv4 only)

IP name: ip-172-31-12-170.ap-northeast-1.compute.internal IP: ip-172-31-12-170.ap-northeast-1.compute.internal

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences Show all

80°F Sunny 11:59 20-02-2023

Volumes | EC2 Management Con

ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#Volumes:

AMIs AMI Catalog

Elastic Block Store Volumes Snapshots Lifecycle Manager

Network & Security Security Groups Elastic IPs Placement Groups Key Pairs Network Interfaces

Load Balancing Load Balancers Target Groups

Auto Scaling Launch Configurations Auto Scaling Groups

You can now create Amazon Data Lifecycle Manager policies to automate snapshot management directly from this screen. Select the volumes to back up, and then choose Actions, Create snapshot lifecycle policy. For more information, see the Knowledge Center article.

Volumes (1)

Create volume

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created	Available
-	vol-0e825616475829bb	gp2	10 GB	100	-	-	2023/02/20 11:55 GMT+5...	ap-nor

Select a volume above

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences Show all

80°F Sunny 12:00 20-02-2023

Screenshots of the AWS Management Console showing the Volumes page for the 'ap-northeast-1' region. The left sidebar shows navigation links for AMIs, Services, and various AWS services like Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling.

The main content area displays a table titled 'Volumes (1/1)'. A single volume is listed:

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created	Available
vol-0c8825616475829bb	gp2	10 GiB	100	-	-	-	2023/02/20 11:53 GMT+5:30	ap-northeast-1

A context menu is open over this volume, listing options: Create volume, Modify volume, Create snapshot, Create snapshot lifecycle policy, Delete volume, Attach volume, Detach volume, Force detach volume, Manage auto-enabled I/O, Manage tags, and Fault injection.

Below the table, a message says: "You can now create Amazon Data Lifecycle Manager policies to automate snapshot management directly from this screen. Select the volumes to back up, and then choose Actions, Create snapshot lifecycle policy. For more information, see the Knowledge Center article."

At the bottom of the page, there are tabs for Details, Status checks, Monitoring, and Tags. The Details tab is selected.

Screenshot of the AWS Management Console showing a confirmation dialog box titled 'Delete vol-0c8825616475829bb?'.

The dialog contains the following text:

After you delete a volume, its data is permanently deleted and the volume can no longer be attached to an instance.
Are you sure that you want to delete vol-0c8825616475829bb?

At the bottom right of the dialog are two buttons: 'Cancel' and 'Delete'.

The background shows the same Volumes page as the previous screenshot, with the volume 'vol-0c8825616475829bb' still listed.

The screenshot shows the AWS EC2 Management Console with the URL ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#Volumes. The left sidebar includes sections for AMIs, Elastic Block Store (selected), Snapshots, Lifecycle Manager, Network & Security, Load Balancing, and Auto Scaling. A success message at the top states: "Successfully deleted volume vol-0c8825616475829bb". Below it, a note says: "You can now create Amazon Data Lifecycle Manager policies to automate snapshot management directly from this screen. Select the volumes to back up, and then choose **Actions, Create snapshot lifecycle policy**. For more information, see the [Knowledge Center article](#)." The main area is titled "Volumes" and displays a table with columns: Name, Volume ID, Type, Size, IOPS, Throughput, Snapshot, Created, and Available. A search bar and an "Actions" dropdown menu are at the top of the table. A message below the table says: "You currently have no volumes in this region". At the bottom of the page, there are links for Feedback, Language, Privacy, Terms, and Cookie preferences. The taskbar at the bottom of the browser window shows various pinned icons and the date/time as 20 02-2023 12:01.

EXPERIMENT 4

Create and configure storage services and upload files and objects using Amazon EFS

Note: Select OS Linux while doing EFS , use same security group and key pair for both instances and select the subnet id for second instance other than first instance while creating security group

(1) Creating first instance and note down the availability zone and security group

- Create the first instance by launching the Instance
- Name the first instance to be launched as efs1
- Select The operating System as AWS Linux
- Create a Key pair and name it as nfs
- Create the key pair.
- Configure the network settings
- Provide all the permissions as shown by checking the boxes.
- Configure the storage from 8GB to 10GB
- Now Launch the instance.
- Instance 1 named efs1 is successfully launched.

(2)Creating Second instance and adding same security group, keypair and different availability zone

- Go back to the Dashboard of EC2 instance to create another instance.
- Check the availability zone and Security group in another tab so that for the second instance the availability zone should be different and security group to be the same.
- Repeat the same process and create another instance with name as efs2 same as the previous instance and use same key and security group for instance 2.
- Checking the Security group in another tab so that to apply it same to the instance 2 that we are creating.
- Changing the security group as wizard2 as it was in instance1
- Now edit the same for the second instance2
- Select the existing security group for instance2
- Launch the instance2
- Instance 2 is also successfully launched
- The availability zones are different.

(3) Adding security group New Rule with NFS

- The Security groups are same, if we add both instances can be reflected.
- Select the first instance efs1
- Click on the security tab in dashboard of instance of efs1 click on the security groups

- Now select the inbound rules and edit the inbound rules,in the edit inbound rules click on add rule
- Add the rule , Select NFS and anywhere in IPV4.
- Save the changes and the saved changes will be successful.

(4) Creating EFS Service

- Go back to the dashboard and search for EFS, Now click on create file system
- Provide name to the file system something as efsdemo ,Let VPC be default and Storage class as Standard and click on customize
- Click on Next and Removed all the previous provided Security Groups Network access.
- Apply the security group name same as the EC2 instances security group
- Click on next, Now click on Create.
- EFS created successfully.

(5)Mounting the EFS with instances from console

- Go back to instances
- Now go to efs1 i.e, instance 1 and right click the instance and connect to the instance.
- Connect to the instance, by Click on connect to establish connection
- Connection is being established
- After connection is established, Same step must be repeated for the second instance efs2 and connection must be established.
- After connection is established, Type the below all commands in two instance consoles
 - 1) sudo su
 - 2) mkdir efs
 - 3) yum install-y amazon-efs-utils
- Go back to the amazon aws console , in the services go back to efs service, right click on created efs i.e. efsdemo
- Click on attach to mount efs,We are ,mounting via DNS ,Copying the command and pste in two consoles.

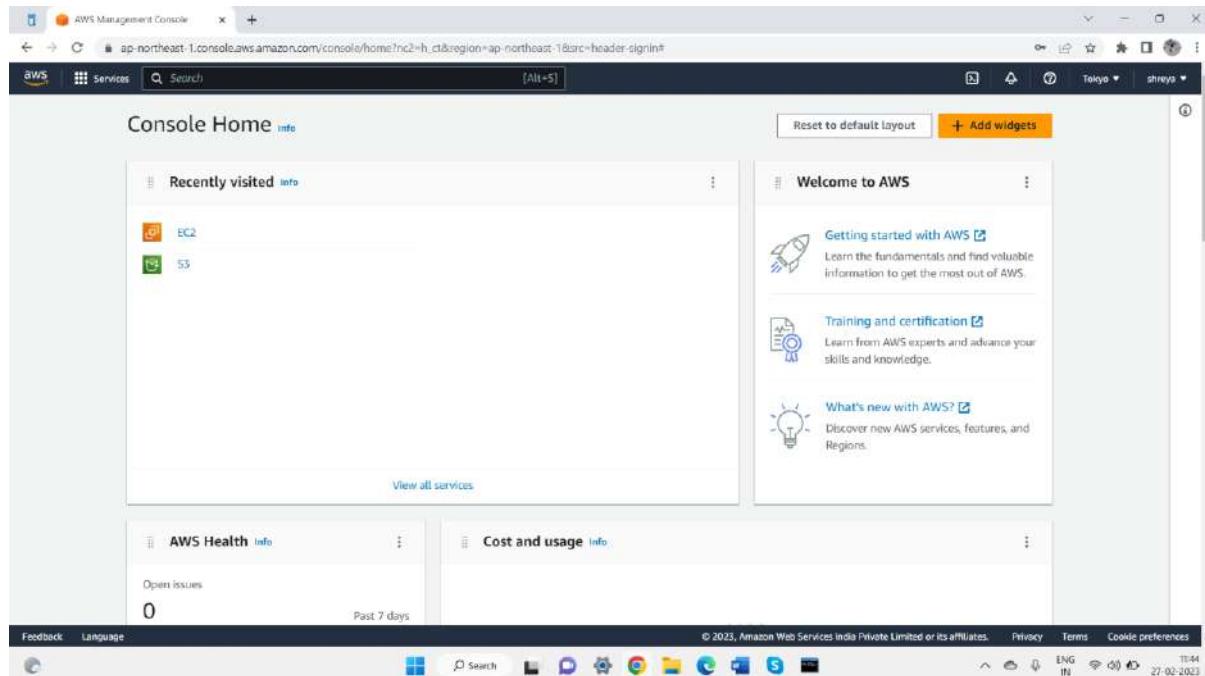
(6) Creating EFS directory and files

- Type the commands in two consoles
 - ls
 - cd efs
- Now create a file in any **one of the ec2 instance** such that **it must reflect in another instance** even. For example create file in instance1 must reflect in instance 2
- Type the command in one console
 - touch file1 file2
 - ls in any one of the instance.
- Touch file1 file2 to create files and ls to list the created files.

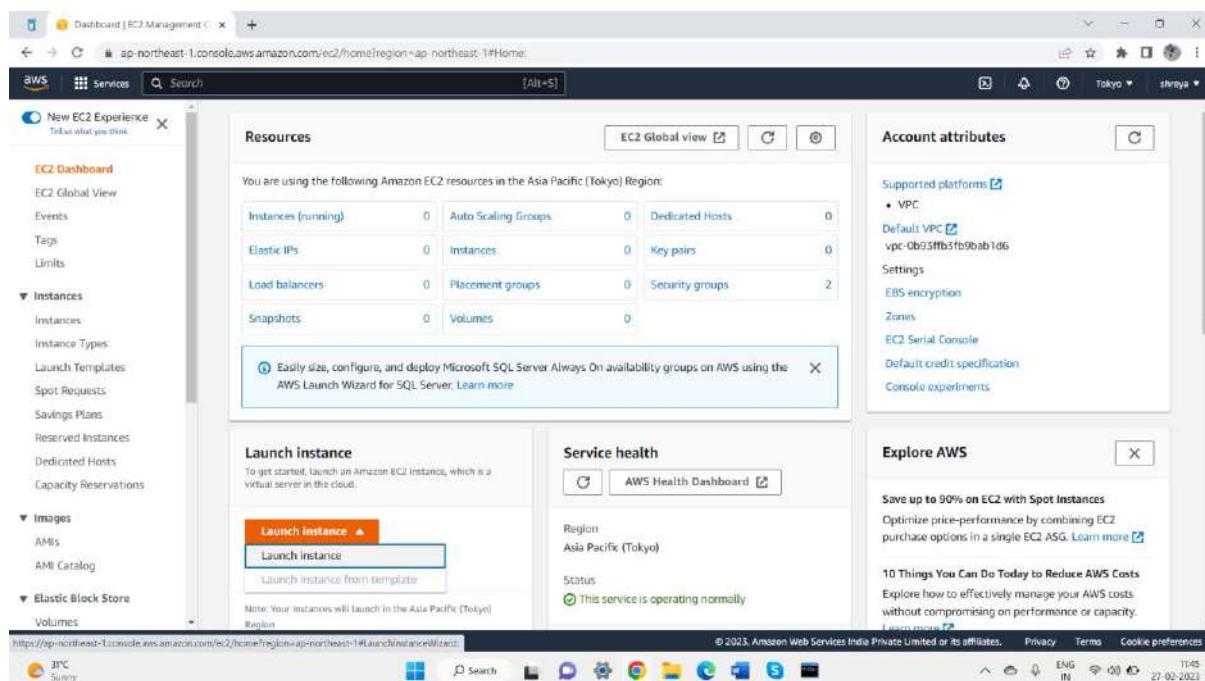
- In another instance(instance where touch command not used) type ls. It shows the created files l1 and l2
- In the other instance ,to remove the file type the command
 - rm file1
 - ls

Check the same ls command in the instance where we have created file1 and file2 after removal of file1. It shows only file2 In this process Efs can be shared among ec2 instances with in the regions

In the console home of the AWS dashboard open EC2 instance.



Create the first instance by launching the Instance



Name the first instance to be launched as efs1

Name and tags

Name: efs1

Application and OS Images (Amazon Machine Image)

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 | S | Browse more AMIs

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2 Kernel 5.10 AMI...read more
ami-0ffac3e16dc16665e

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month. 30 GiB of EBS storage.

Cancel | Launch instance

Select The operating System as AWS Linux

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-0ffac3e16dc16665e (64-bit [x86]) / ami-0b6f8fb486fb0ccac (64-bit [Arm])
Virtualization: hvm | ENA enabled: true | Root device type: ebs

Free tier eligible

Description: Amazon Linux 2 Kernel 5.10 AMI 2.0.20230207.0 x86_64 HVM gp2.

Architecture: 64-bit (x86) | AMI ID: ami-0ffac3e16dc16665e | Verified provider

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2 Kernel 5.10 AMI...read more
ami-0ffac3e16dc16665e

Virtual server type (instance type): t2.micro

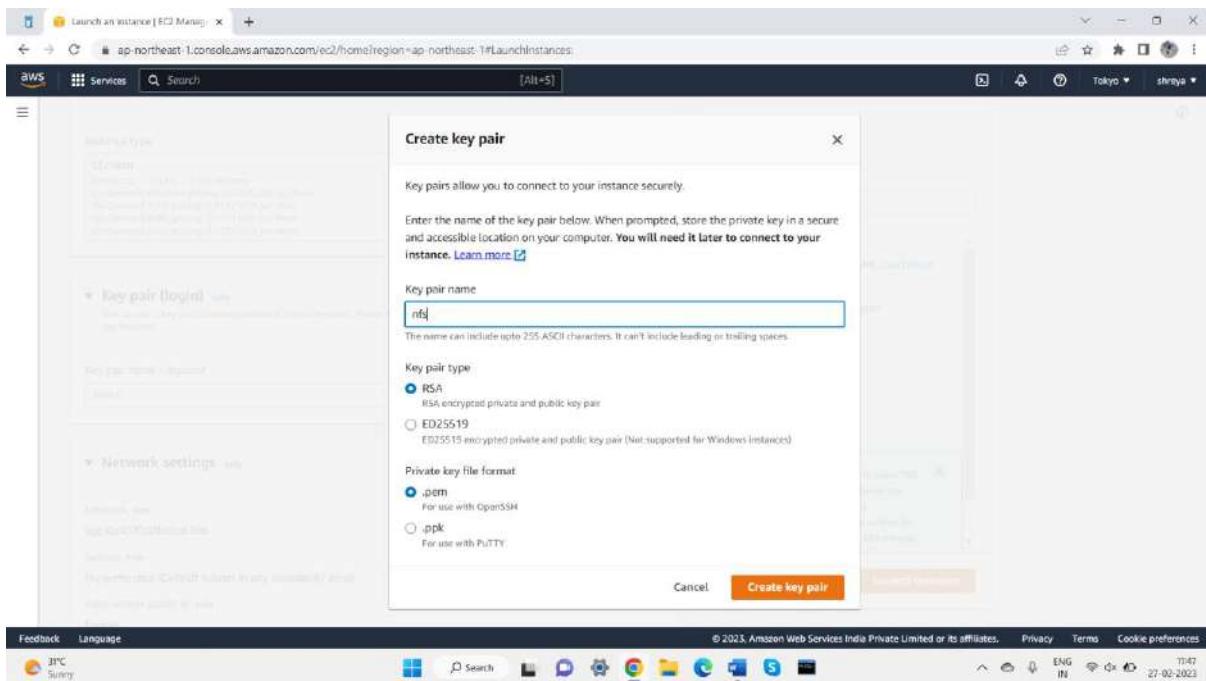
Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

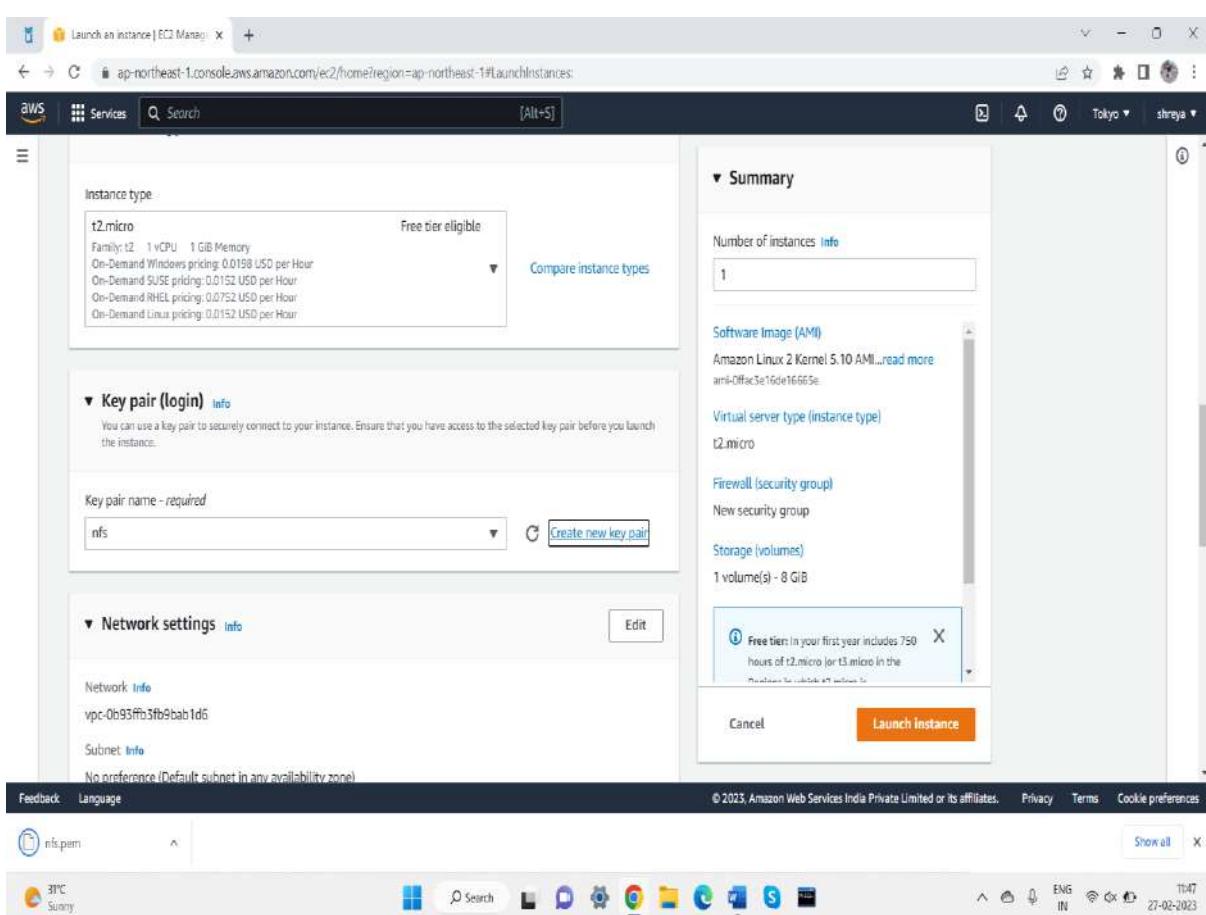
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month. 30 GiB of EBS storage.

Cancel | Launch instance

Create a Key pair and name it as nfs



Create the key pair.



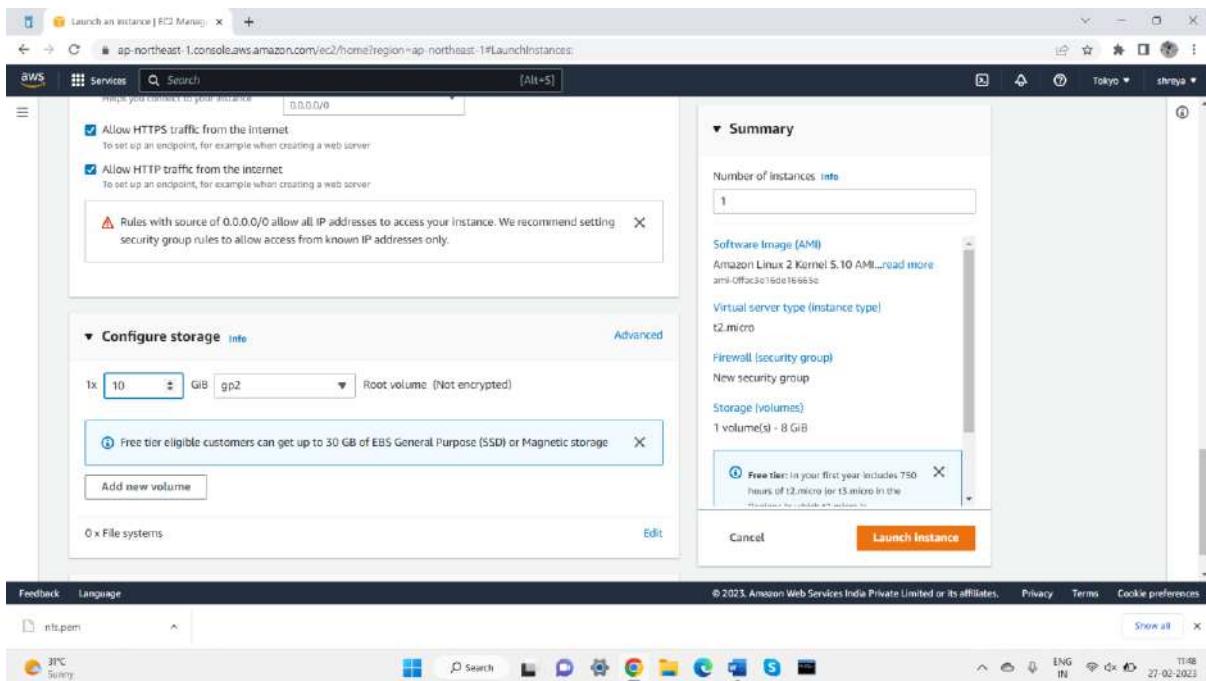
Configure the network settings

The screenshot shows the AWS EC2 Launch Instance wizard. In the 'Network settings' section, under 'Firewall (security groups)', there are three checked boxes: 'Allow SSH traffic from Anywhere (0.0.0.0/0)', 'Allow HTTPS traffic from the internet', and 'Allow HTTP traffic from the internet'. A tooltip for the free tier is displayed, stating: 'Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Free tier) on demand for 1 instance'. The 'Launch Instance' button is highlighted.

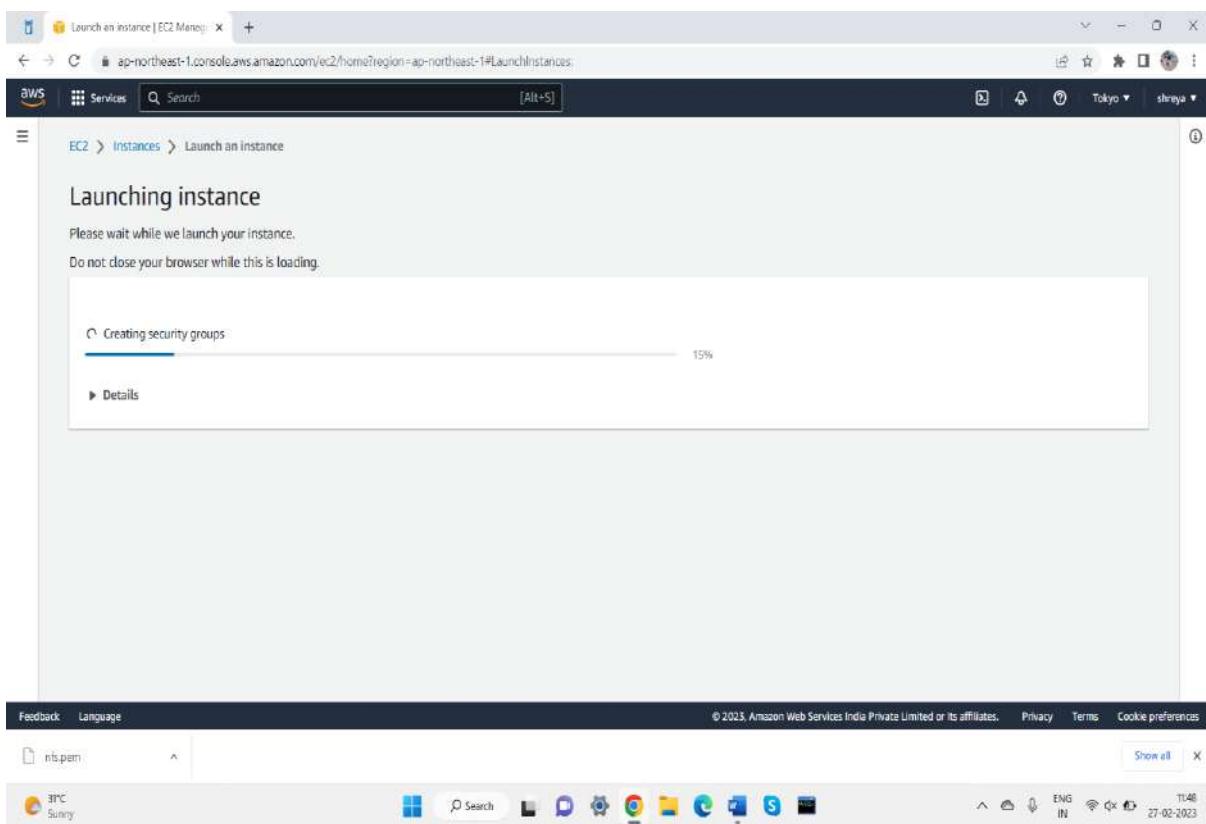
Provide all the permissions as shown by checking the boxes.

The screenshot shows the AWS EC2 Launch Instance wizard. In the 'Network settings' section, under 'Firewall (security groups)', all three checkboxes are now checked: 'Allow SSH traffic from Anywhere (0.0.0.0/0)', 'Allow HTTPS traffic from the internet', and 'Allow HTTP traffic from the internet'. A tooltip for the free tier is displayed, stating: 'Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Free tier) on demand for 1 instance'. The 'Launch Instance' button is highlighted.

Configure the storage from 8GB to 10GB



Now Launch the instance.



Instance 1 named efs1 is successfully launched.

The screenshot shows the AWS EC2 'Launch an instance' success page. At the top, there's a green checkmark icon and the word 'Success'. Below it, a message says 'Successfully initiated launch of instance (i-095c0806739615856)'. There's a link to 'Launch log'. Under 'Next Steps', there are three main sections: 'Create billing and free tier usage alerts', 'Connect to your instance', and 'Connect an RDS database'. Each section contains descriptive text and a button or link for further action.

Go back to the Dashboard of EC2 instance to create another instance.

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with various navigation options like 'EC2 Dashboard', 'Instances', 'Images', etc. The main area has sections for 'Resources' (listing Instances (running), Auto Scaling Groups, Dedicated Hosts, etc.) and 'Account attributes' (listing Supported platforms, Default VPC, Settings, etc.). A central 'Launch instance' button is also visible.

Check the availability zone and Security group in another tab so that for the second instance the availability zone should be different and security group to be the same.

The screenshot shows the AWS EC2 Management Console. On the left, the navigation pane includes 'Instances', 'Images', 'Elastic Block Store', and 'Network & Security'. The main content area displays a table of instances with one entry: 'ec2' (Running, t2.micro, Initializing, No alarms, ap-northeast-1c, ec2-43-207-47-11.ap-n...). Below the table, a modal window titled 'Select an instance' lists the same instance 'ec2'.

Repeat the same process and create another instance with name as ec2 same as the previous instance and use same key and security group for instance 2.

The screenshot shows the 'Launch Instances' wizard. In the 'Network settings' step, the 'Select existing security group' dropdown is open, showing 'launch-wizard-1' and 'launch-wizard-2'. Other configuration options include 'Number of instances' (1), 'Software Image (AMI)' (Amazon Linux 2 Kernel 5.10 AMI), 'Virtual server type (instance type)' (t2.micro), and 'Storage (volumes)' (1 volume(s) - 8 GiB). A 'Launch Instance' button is visible at the bottom.

Checking the Security group in another tab so that to apply it same to the instance 2 that we are creating.

EC2 Management Console Instances | EC2 Management Console [Alt+5] Instances (1) Info

Find Instance By attribute or tag (case-sensitive)

Availability Zone	Public IPv4 DNS	Public IPv4 IP	Elastic IP	IPv6 IPs	Monitoring	Security group name	Key name
ap-northeast-1c	ec2-43-207-47-11.ap-northeast-1.compute.amazonaws.com	43.207.47.11	-	-	disabled	launch-wizard-2	nfs

Select an instance

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences Show all ENG IN 27-02-2023

Changing the security group as wizard2 as it was in instance1

EC2 Management Console Instances | EC2 Management Console [Alt+5] Instances | EC2 Management Console [Alt+5]

Number of instances: 1

Software Image (AMI): Amazon Linux 2 Kernel 5.10 AMI...read more
ami-0ffcc5e16de1666se

Virtual server type (instance type): t2.micro

Firewall (security group): launch-wizard-2

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: in your first year includes 750 hours of t2.micro (or t3.micro in the non-aws GovCloud (US) Region) for a total of 475 hours per month.

Cancel Launch instance

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences Show all ENG IN 27-02-2023

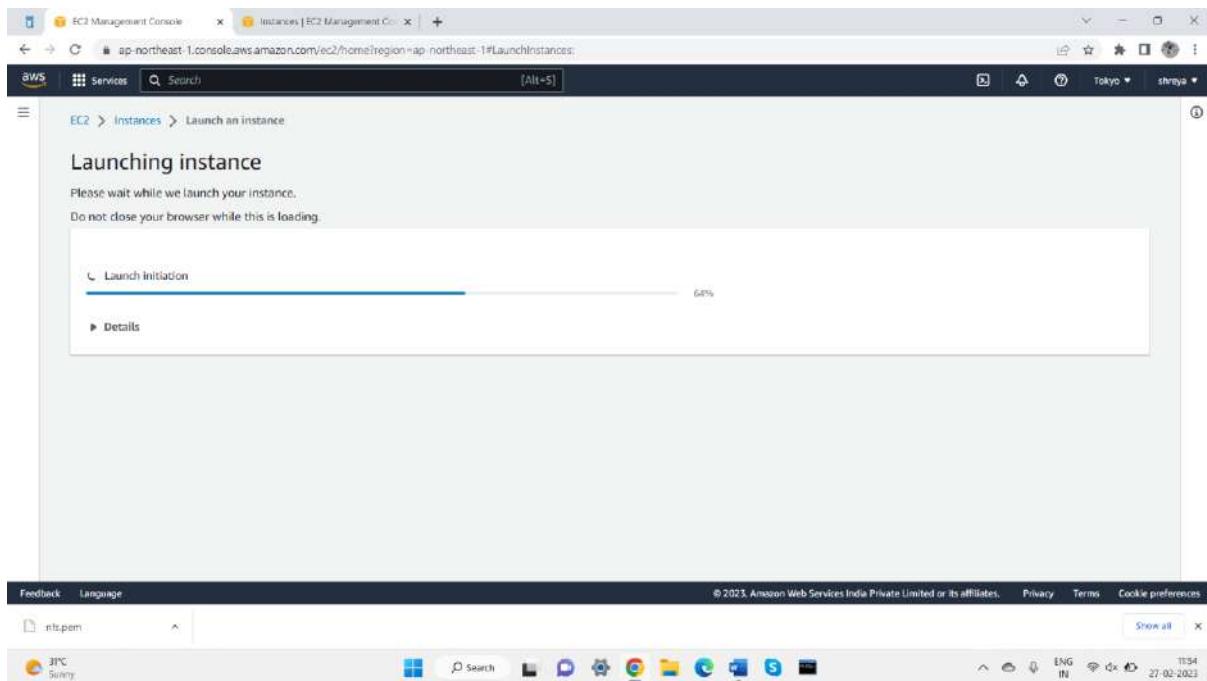
Now edit the same for the second instance2

The screenshot shows the AWS EC2 Management Console interface. In the 'Network settings' section, a VPC dropdown is set to 'vpc-0b93ff3fb9bab1d6' (default). Below it, a 'Subnet' dropdown shows 'No preference' selected. A list of subnets is visible: subnet-09ee98057113516bd, subnet-0d57baff110f71c18, and subnet-035a4528070fe579. The 'Summary' section on the right indicates 1 instance will be launched with an 'Amazon Linux 2 Kernel 5.10 AMI', 't2.micro' instance type, and 1 volume(s) - 10 GiB. A 'Launch Instance' button is present.

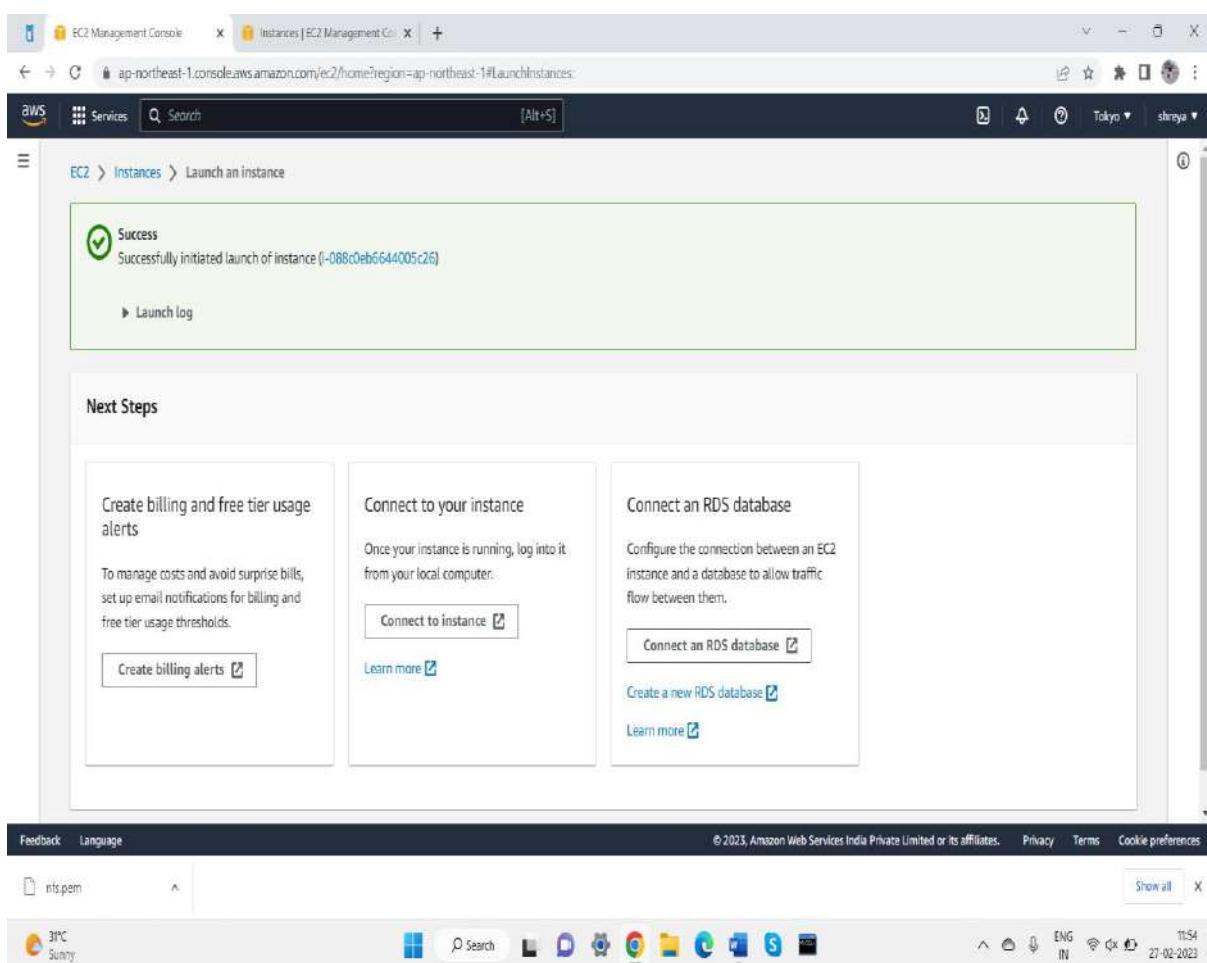
Select the existing security group for instance2

The screenshot shows the AWS EC2 Management Console interface. In the 'Firewall (security groups)' section, 'Auto-assign public IP' is set to 'Enable'. The 'Select existing security group' button is highlighted. The 'Summary' section on the right indicates 1 instance will be launched with an 'Amazon Linux 2 Kernel 5.10 AMI', 't2.micro' instance type, and 1 volume(s) - 10 GiB. A 'Launch Instance' button is present.

Launch the instance2



Instance 2 is also successfully launched



The availability zones are different.

The screenshot shows the AWS EC2 Management Console interface. The left sidebar is collapsed, and the main area displays the 'Instances' table. The table has columns for Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, Public IPv4 IP, and Elastic IP. There are three rows:

Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 IP	Elastic IP
Running	t2.micro	Initializing	No alarms	ap-northeast-1a	ec2-54-95-109-164.ap...	54.95.109.164	-
Terminated	t2.micro	-	No alarms	ap-northeast-1c	-	-	-
Running	t2.micro	2/2 checks passed	No alarms	ap-northeast-1c	ec2-43-207-47-11.ap...	43.207.47.11	-

The Security group names are same

The screenshot shows the AWS EC2 Management Console interface. The left sidebar is collapsed, and the main area displays the 'Instances' table. The table has columns for Public IPv4 DNS, Public IPv4 IP, Elastic IP, IPv6 IPs, Monitoring, Security group name, Key name, and Launch time. There are two rows:

Public IPv4 DNS	Public IPv4 IP	Elastic IP	IPv6 IPs	Monitoring	Security group name	Key name	Launch time
2-54-95-109-164.ap...	54.95.109.164	-	-	disabled	launch-wizard-2	nfs	2023/02/27 12:02 GMT+5
2-43-207-47-11.ap...	43.207.47.11	-	-	disabled	launch-wizard-2	nfs	2023/02/27 11:54 GMT+5

Select the first instance efs1

The screenshot shows the AWS EC2 Management Console. The left sidebar is collapsed. The main area displays a table of instances. The first two rows are for terminated instances named 'efs2'. The third row is for a running instance named 'efs1' with the ID 'i-095c0806739615856'. The 'Actions' column for 'efs1' has a 'Launch Instances' button. Below the table, a modal window titled 'Instance: i-095c0806739615856 (efs1)' is open, showing the 'Details' tab. The 'Security' tab is also visible. The status bar at the bottom right shows '12:34 27-02-2023'.

Click on the security of efs1 click on the security groups

The screenshot shows the AWS EC2 Management Console. The left sidebar is collapsed. The main area displays a table of instances. The first two rows are for terminated instances named 'efs2'. The third row is for a running instance named 'efs1' with the ID 'i-095c0806739615856'. The 'Actions' column for 'efs1' has a 'Launch Instances' button. Below the table, a modal window titled 'Instance: i-095c0806739615856 (efs1)' is open, showing the 'Security' tab. The 'Details' tab is also visible. The 'Security' tab displays 'Security details' (IAM Role: -, Owner ID: 106244561508) and 'Inbound rules' (Security group: sg-0c137eff48ae547b6 (launch-wizard-2)). The status bar at the bottom right shows '12:34 27-02-2023'.

click on the security groups

EC2 > Security Groups > sg-0c137eff48ae547b6 - launch-wizard-2

Details

Security group name	Security group ID	Description	VPC ID
launch-wizard-2	sg-0c137eff48ae547b6	launched-wizard-2 created 2023-02-27T06:16:13.213Z	vpc-0b93fffb3fb9bab1d6
Owner	Inbound rules count	Outbound rules count	
106244561508	3 Permission entries	1 Permission entry	

Inbound rules | Outbound rules | Tags

You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer

Now select the inbound rules and edit the inbound rules

EC2 > Security Groups > sg-0c137eff48ae547b6 - launch-wizard-2 > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-000c78a746a27ed78	SSH	TCP	22	Custom	0.0.0.0/0
sgr-009fe3ec23076a7d7	HTTPS	TCP	443	Custom	0.0.0.0/0
sgr-07872976429f936af	HTTP	TCP	80	Custom	0.0.0.0/0

Add rule

Cancel | Preview changes | Save rules

In the edit inbound rules click on add rule

Inbound rules [Info](#)

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
sgr-000c78a746a27ed78	SSH	TCP	22	Custom	<input type="text"/> 0.0.0.0 X
sgr-009fe5ec23076a7d7	HTTPS	TCP	443	Custom	<input type="text"/> 0.0.0.0 X
sgr-07872976429f936af	HTTP	TCP	80	Custom	<input type="text"/> 0.0.0.0 X
-	Custom TCP	TCP	0	Custom	<input type="text"/> 0.0.0.0 X

[Add rule](#)

[Cancel](#) [Preview changes](#) [Save rules](#)

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 31°C Sunny ENG IN 12:16 27-02-2023

Change the custom TCP to NFS

Inbound rules [Info](#)

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
sgr-000c78a746a27ed78	SSH	TCP	22	Custom	<input type="text"/> 0.0.0.0 X
sgr-009fe5ec23076a7d7	HTTPS	TCP	443	Custom	<input type="text"/> 0.0.0.0 X
sgr-07872976429f936af	HTTP	TCP	80	Custom	<input type="text"/> 0.0.0.0 X
-	NFS	TCP	2049	Custom	<input type="text"/> 0.0.0.0 X

[Add rule](#)

[Cancel](#) [Preview changes](#) [Save rules](#)

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 31°C Sunny ENG IN 12:16 27-02-2023

Change the source from custom to anywhere in ipv4

The screenshot shows the 'Edit inbound rules' section of the AWS EC2 Management Console. A table displays five existing rules:

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-000c78a746a27ed78	SSH	TCP	22	Custom	0.0.0.0/0
sgr-009fe5cc23076a7d7	HTTPS	TCP	443	Custom	0.0.0.0/0
sgr-0782976429f936ef	HTTP	TCP	80	Custom	0.0.0.0/0
-	NPS	TCP	2049	Anywhere	0.0.0.0/0

An 'Add rule' button is located at the bottom left of the table.

Save the changes and the saved changes will be successful.

The screenshot shows a success message: "Inbound security group rules successfully modified on security group (sg-0c137eff48ae547b6 | launch-wizard-2)". Below this, the security group details are displayed:

Security group name	Security group ID	Description	VPC ID
launch-wizard-2	sg-0c137eff48ae547b6	launch-wizard-2 created 2023-02-27T06:15:21Z	vpc-0b93fb3fb2bab1d6

The 'Inbound rules' tab is selected. A message at the bottom says: "You can now check network connectivity with Reachability Analyzer". A "Run Reachability Analyzer" button is available. At the bottom right, there is an "Edit inbound rules" button.

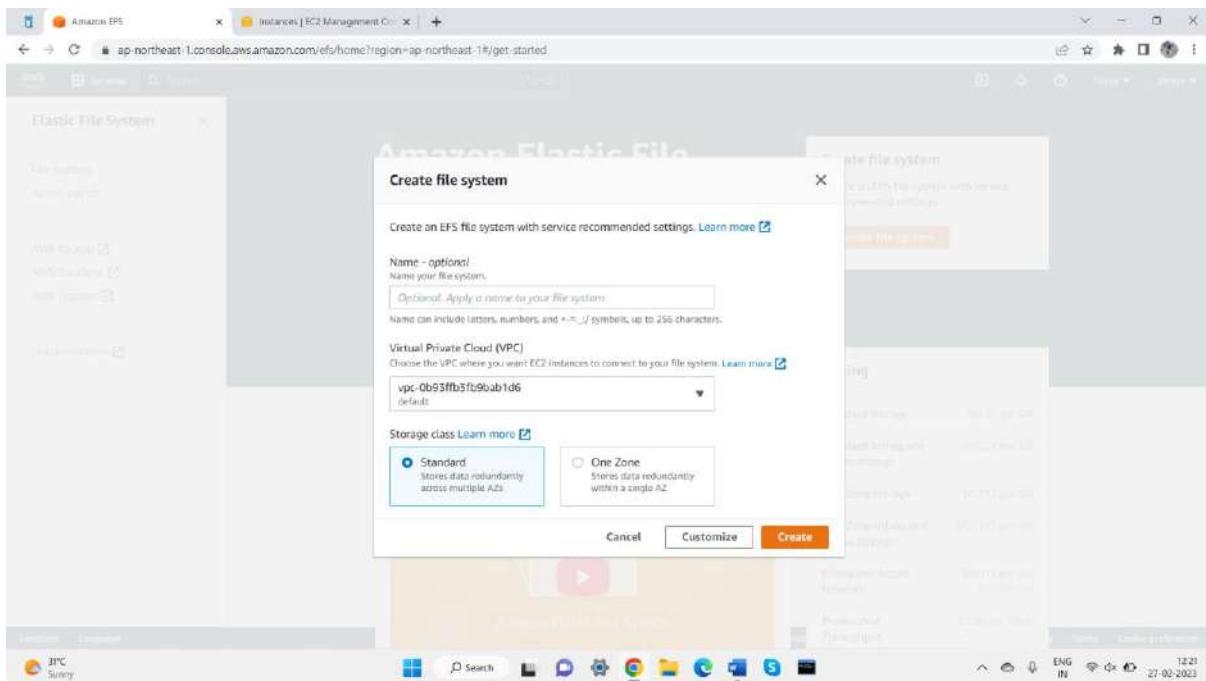
Go back to the dashboard and search for EFS and click on efs service.

The screenshot shows the AWS Services search results for 'EFS'. The search bar at the top right contains the query 'EFS'. Below it, the 'Services' section lists several services, with 'EFS' highlighted in blue. Other listed services include DataSync, MediaStore, and Elastic Kubernetes Service. The 'Features' section below shows 'Access points' and 'File systems' under the EFS feature. On the right side, there's a sidebar titled 'Account attributes' which includes sections for Supported platforms (VPC), Default VPC (vpc-0b93fb3fb9bab1d6), Settings, EBS encryption, Zones, EC2 Serial Console, Default credit specification, and Console experiments. There are also 'Explore AWS' sections for Amazon GuardDuty Malware Protection and 10 Things You Can Do Today to Reduce AWS Costs.

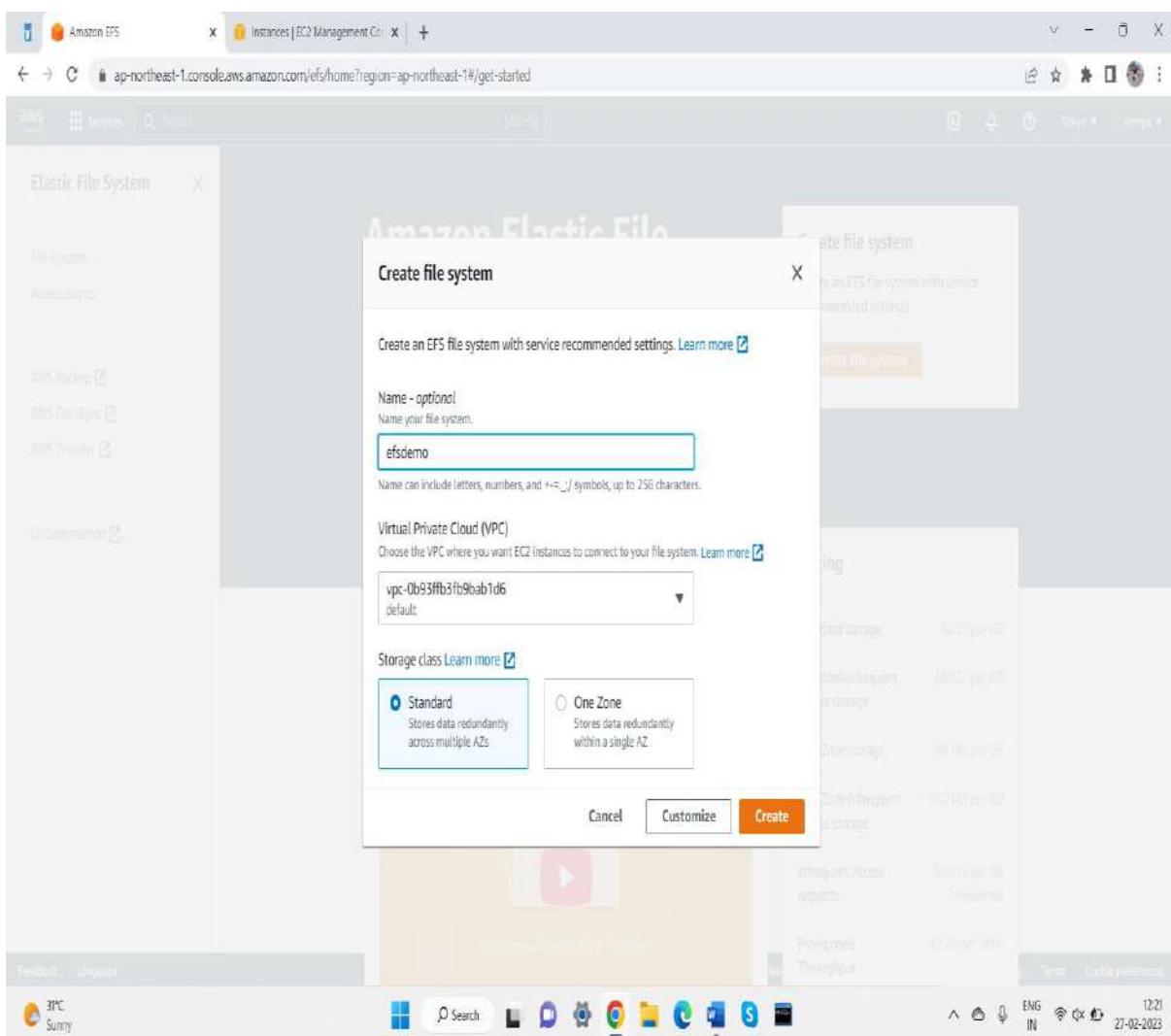
The dashboard resembles as shown. Now click on create file system

The screenshot shows the Amazon Elastic File System (Amazon EFS) landing page. The left sidebar has links for 'File systems', 'Access points', 'AWS Backup', 'AWS DataSync', 'AWS Transfer', and 'Documentation'. The main content area features a large title 'Amazon Elastic File System' with the subtitle 'Scalable, elastic, cloud-native NFS file system'. It includes a brief description of what Amazon EFS is and a video player with the text 'Amazon Elastic File System - Scalable, Elasti...'. To the right, there's a 'Create file system' button and a 'Pricing' table. The table lists storage types and their costs: Standard storage (\$0.36 per GB), Standard-Infrequent Access storage (\$0.027 per GB), One Zone storage (\$0.192 per GB), One Zone-Infrequent Access storage (\$0.0145 per GB), and Infrequent Access requests (\$0.012 per GB transferred).

Provide name to the file system something as efsdemo



Let VPC be default and Storage class as Standard and click on customize



Storage class as Standard and automatic backups to be enabled

File system settings

General

Name - optional
Name your file system.
efsdemo

Storage class [Learn more](#)

Standard Stores data redundantly across multiple AZs

One Zone Stores data redundantly within a single AZ

Automatic backups Automatically backup your file system data with AWS Backup using recommended settings. Additional pricing applies. [Learn more](#)

Enable automatic backups

Lifecycle management EFS Intelligent-Tiering uses Lifecycle Management to automatically achieve the right price and performance trade-off for your application by moving your files between the Standard and Standard-Infrequent Access storage classes. [Learn more](#)

Transition into IA Transition files from Standard to Standard-Infrequent Access.

30 days(s) since last access

Transition out of IA Transition files from Standard-Infrequent Access to Standard.

None

Encryption Close to enable encryption of your file system's data at rest. Uses the AWS KMS service key (aws/mountfilesystem) by default. [Learn more](#)

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

31°C Sunny ENG IN 12:21 27-02-2023

Click on Next and apply the security group same as the instances security group

Mount target settings

A mount target provides an NFSv4 endpoint at which you can mount an Amazon EFS file system. We recommend creating one mount target per Availability Zone. [Learn more](#)

Availability zone	Subnet ID	IP address	Security groups
ap-northeast-1a	subnet-09ee980571...	Automatic	Choose security groups Remove
ap-northeast-1c	subnet-0d57baff10f...	Automatic	Choose security groups Remove
ap-northeast-1d	subnet-030a452807...	Automatic	Choose security groups Remove

Add mount target

You can only create one mount target per Availability Zone.

Cancel Previous Next

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

31°C Sunny ENG IN 12:23 27-02-2023

Removed all the previous provided Security Groups Network access

Step 1
File system settings

Step 2
Network access

Step 3 - optional
File system policy

Step 4
Review and create

Network

Virtual Private Cloud (VPC)
Choose the VPC where you want EC2 instances to connect to your file system. Learn more [\[?\]](#)

vpc-0b93ffb3fb9bab1d6
default

Mount targets

A mount target provides an NFSv4 endpoint at which you can mount an Amazon EFS file system. We recommend creating one mount target per Availability Zone. Learn more [\[?\]](#)

Availability zone	Subnet ID	IP address	Security groups	Remove
ap-northeast-1a	subnet-09ee980571...	Automatic	Choose security groups [?]	Remove
ap-northeast-1c	subnet-0d57baff10f...	Automatic	Choose security groups [?]	Remove
ap-northeast-1d	subnet-030a452807...	Automatic	Choose security groups [?]	Remove

Add mount target

You can only create one mount target per Availability Zone.

Cancel Previous Next

Adding the security group same as the instances security group

Feedback Language

Amazon EFS - Create a file system X Instances | EC2 Management Con X +

ap-northeast-1.console.aws.amazon.com/efs/home?region=ap-northeast-1#/file-systems/create?name=efsdemo&vpc=vpc-0b93ffb3fb9bab1d6&az=

31°C Sunny

ENG IN 12:23 27-02-2023

Step 3 - optional
File system policy

Step 4
Review and create

Virtual Private Cloud (VPC)
Choose the VPC where you want EC2 instances to connect to your file system. Learn more [\[?\]](#)

vpc-0b93ffb3fb9bab1d6
default

Mount targets

A mount target provides an NFSv4 endpoint at which you can mount an Amazon EFS file system. We recommend creating one mount target per Availability Zone. Learn more [\[?\]](#)

Availability zone	Subnet ID	IP address	Security groups	Remove
ap-northeast-1a	subnet-09ee980571...	Automatic	Choose security groups [?]	Remove
ap-northeast-1c	subnet-0d57baff10f...	Automatic	Choose security groups [?]	Remove
ap-northeast-1d	subnet-030a452807...	Automatic	Choose security groups [?]	Remove

sg-0c137eff48ae547b6
launch-wizard-2

sg-0c137eff48ae547b6
launch-wizard-2

sg-0c137eff48ae547b6
launch-wizard-2

Add mount target

You can only create one mount target per Availability Zone.

Feedback Language

Amazon EFS - Create a file system X Instances | EC2 Management Con X +

ap-northeast-1.console.aws.amazon.com/efs/home?region=ap-northeast-1#/file-systems/create?name=efsdemo&vpc=vpc-0b93ffb3fb9bab1d6&az=

31°C Sunny

ENG IN 12:23 27-02-2023

Click on next

Step 1
File system settings

Step 2
Network access

Step 3 - optional
File system policy

Step 4
Review and create

File system policy - optional

Policy options

Select one or more of these common policy options, or create a custom policy using the editor. [Learn more](#)

Prevent root access by default*

Enforce read-only access by default*

Prevent anonymous access

Enforce in-transit encryption for all clients

* Identity-based policies can override these default permissions.

Grant additional permissions

Policy editor (JSON)

1

Manual changes will prevent the use of the policy options on the left until the editor is cleared.

Cancel Previous Next

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences



Search

ENG IN 12:25 27-02-2023

Again click on next without any changes

Step 2: Network access

Mount targets

Availability zone	Subnet	IP address	Security groups
ap-northeast-1a	subnet-09ee98057113516bd	-	sg-0c137eff48ae547b6
ap-northeast-1c	subnet-0d57bafff10f71c18	-	sg-0c137eff48ae547b6
ap-northeast-1d	subnet-030a4528070f0e579	-	sg-0c137eff48ae547b6

Step 3: File system policy

File system policy

1

Edit Next

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

31°C Sunny Search ENG IN 12:25 27-02-2023

Now click on Create

EFS is in process to create

The screenshot shows the AWS EFS Management Console. A modal window titled "File system (fs-06208766c4d740d31) is creating" is displayed over the main interface. The main area shows a table of file systems with one entry: "efsdemo" (File system ID: fs-06208766c4d740d31), which is currently "Creating". The status bar at the bottom indicates the file system is available.

Name	File system ID	Encrypted	Total size	Size in Standard / One Zone	Size in Standard-IA / One Zone-IA	Provisioned Throughput (MiB/s)	File system state	Create time
efsdemo	fs-06208766c4d740d31	Encrypted	0 Bytes	0 Bytes	0 Bytes	-	Creating	Mon, 2023 06:54 GMT

EFS created successfully

The screenshot shows the AWS EFS Management Console. A green success message box is prominently displayed: "Success! File system fs-06208766c4d740d31 is available." The main interface shows the same table of file systems, where "efsdemo" is now listed as "Available". The status bar at the bottom indicates the file system is available.

Name	File system ID	Encrypted	Total size	Size in Standard / One Zone	Size in Standard-IA / One Zone-IA	Provisioned Throughput (MiB/s)	File system state	Create time
efsdemo	fs-06208766c4d740d31	Encrypted	6.00 KiB	6.00 KiB	0 Bytes	-	Available	Mon, 2023 06:56 GMT

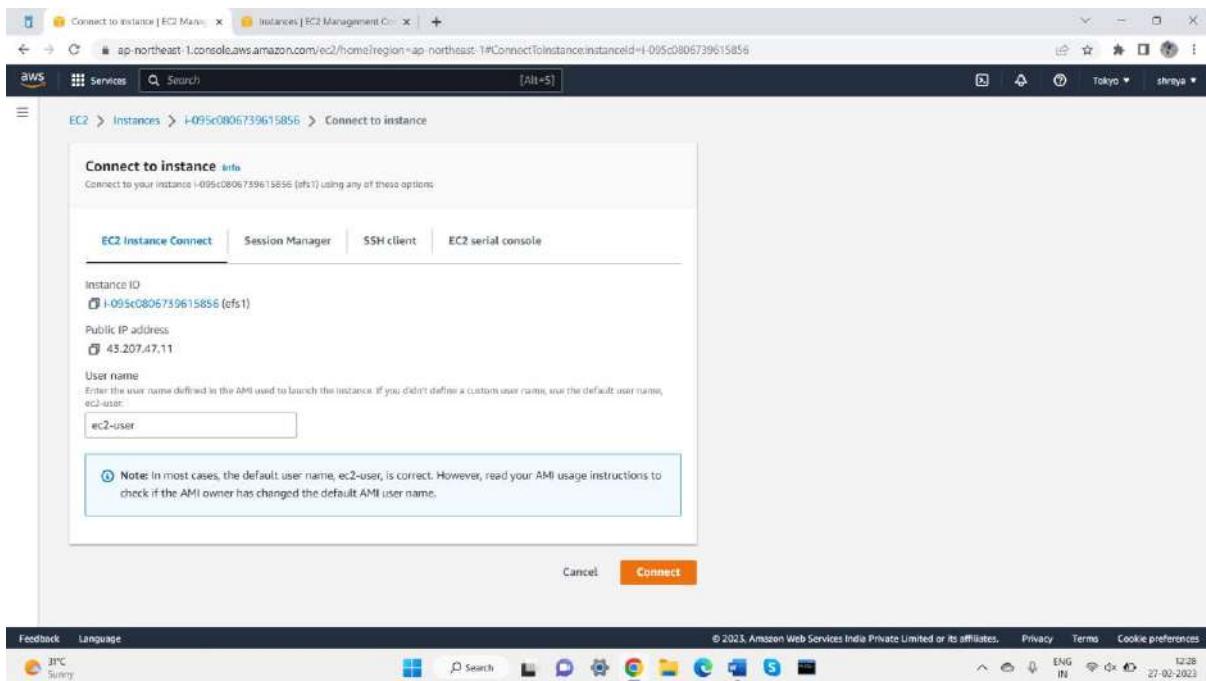
Go back to instances

The screenshot shows the AWS EC2 Management Console interface. On the left, a sidebar menu includes options like EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), and Elastic Block Store (Volumes). The main content area displays a table titled "Instances (3) Info" with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. The table lists three instances: "efs2" (Running, t2.micro), "efs2" (Terminated, t2.micro), and "efs1" (Running, t2.micro). The "efs1" row is highlighted. A modal window titled "Select an instance" is open over the table, indicating the user has selected the "efs1" instance.

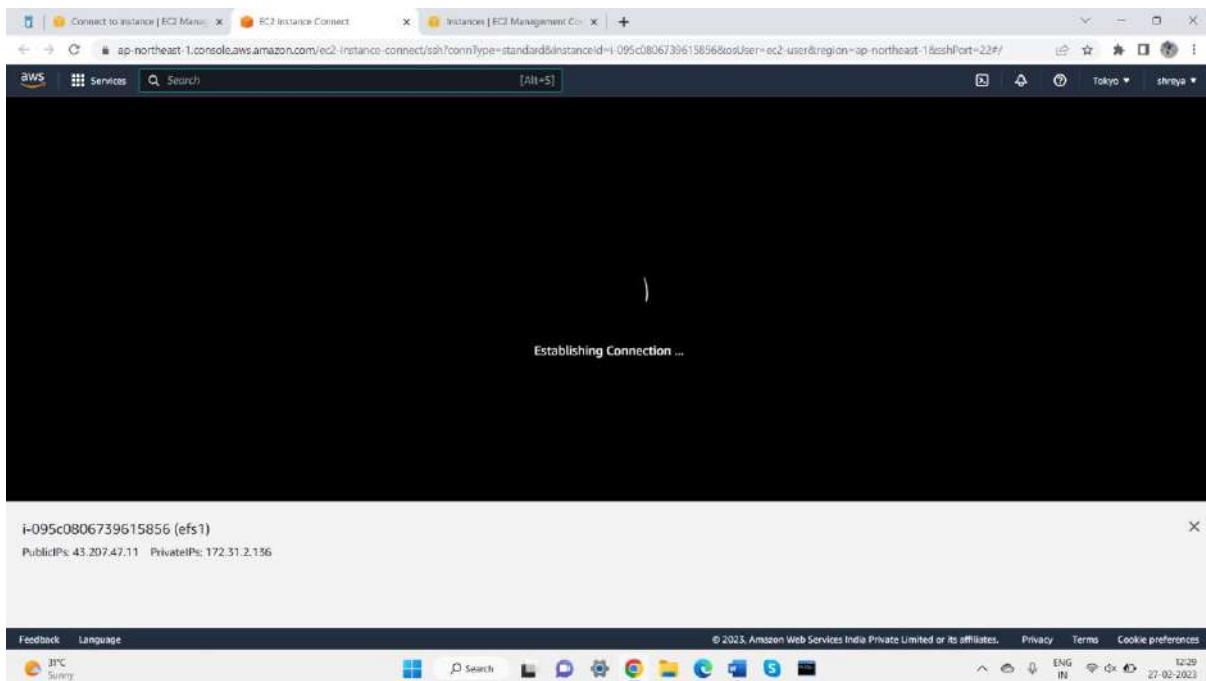
Now go to efs1 i.e, instance 1 and right click the instance and connect to the instance.

The screenshot shows the AWS EC2 Management Console interface, similar to the previous one but with a context menu open over the "efs1" instance row. The menu items include "Launch instances", "Launch instance from template", "Migrate a server", "Connect" (which is highlighted in blue), "Stop instance", "Start instance" (with the value "5856 (efs1)" entered), "Reboot instance", "Hibernate instance", "Terminate instance", "Instance settings", "Networking", "Security", "Image and templates", "Monitor and troubleshoot", "Private IP DNS name (IPv4 only)", and "IP name: ip-172-31-2-136.ap-northeast-1.compute.internal". The "Connect" button is the primary focus, suggesting the next step is to click it to establish a connection.

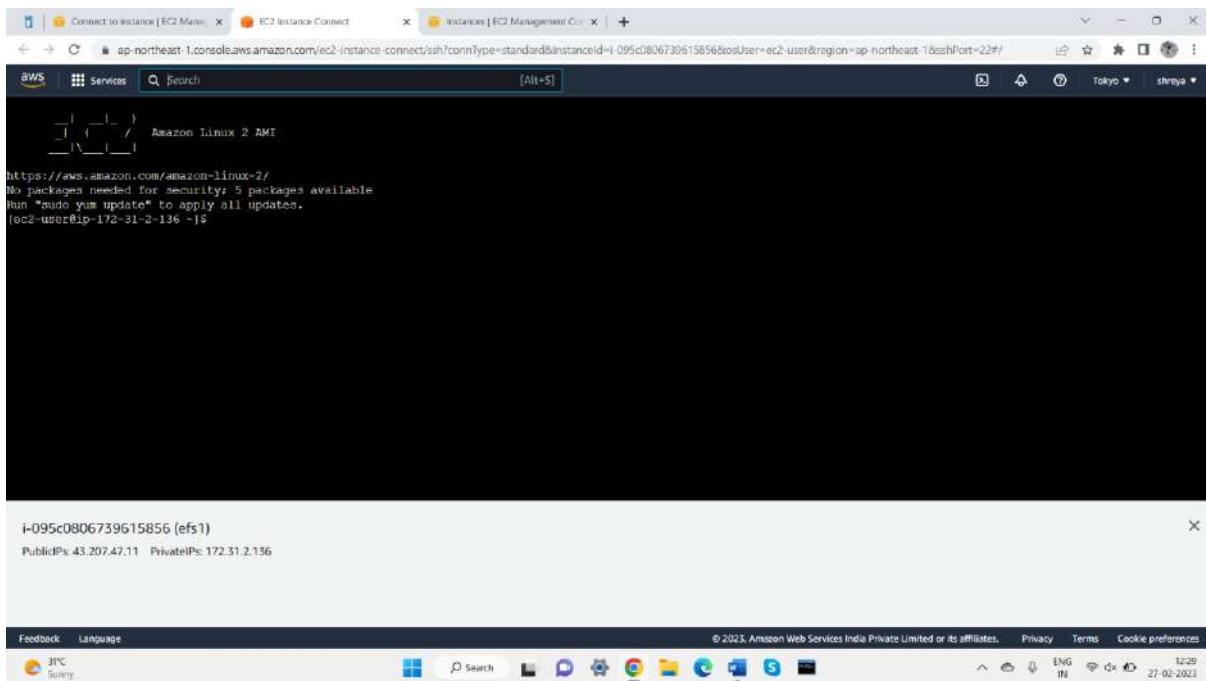
Connect to the instance, by Click on connect to establish connection



Connection is being established



After connection is established, the output for efs1 (instance1) will be as follows.



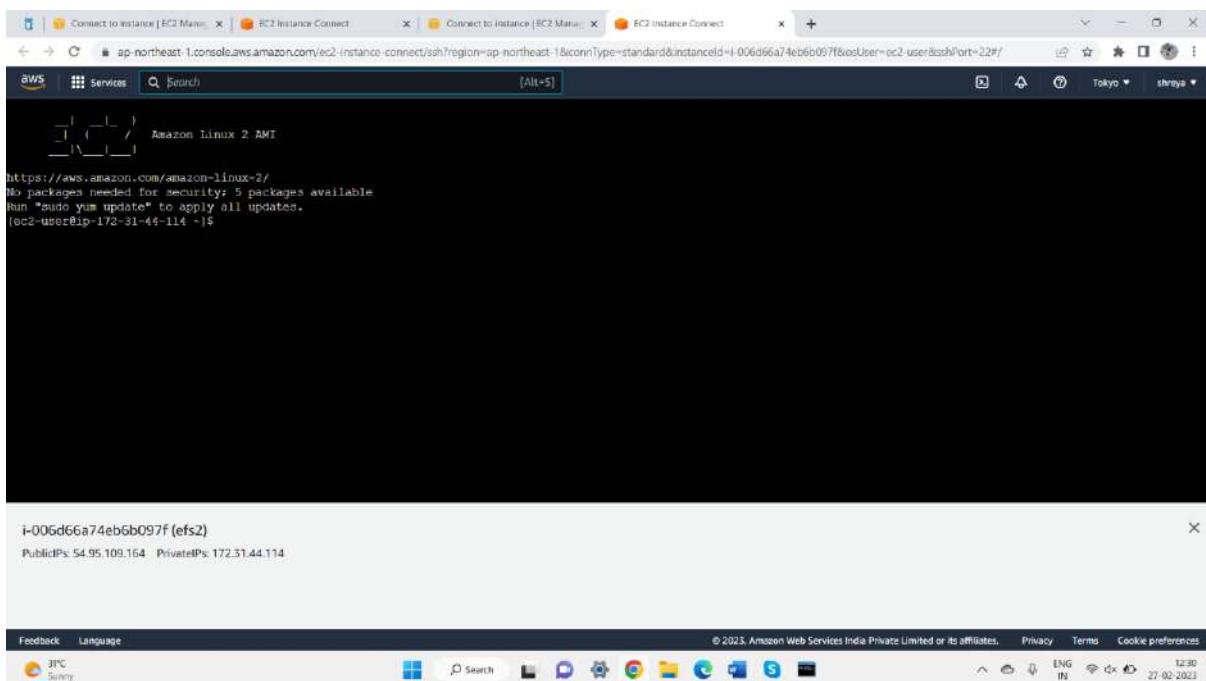
```
https://aws.amazon.com/amazon-linux-2/
No packages needed for security; 5 packages available
Run "sudo yum update" to apply all updates.
(ec2-user@ip-172-31-2-136 ~)$
```

i-095c0806739615856 (efs1)
PublicIPs: 43.207.47.11 PrivateIPs: 172.31.2.136

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences ENG IN 12:29 27-02-2023

Same step must be repeated for the second instance efs2 and connection must be established.

After connection is established, the output for efs2 (instance2) will be as follows.



```
https://aws.amazon.com/amazon-linux-2/
No packages needed for security; 5 packages available
Run "sudo yum update" to apply all updates.
(ec2-user@ip-172-31-46-114 ~)$
```

i-006d66a74eb6b097f (efs2)
PublicIPs: 54.95.109.164 PrivateIPs: 172.31.44.114

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences ENG IN 12:30 27-02-2023

Type the commands sudo su and mkdir efs in both of the connected instance

i-095c0806739615856 (efs1)
PublicIPs: 43.207.47.11 PrivateIPs: 172.31.2.136

Type the command `yum install-y amazon-efs-utils` in both of the connected instances

i-095c0806739615856 (efs1)
PublicIPs: 43.207.47.11 PrivateIPs: 172.31.2.136

Click on enter, The required statements will be imported.

```

No packages needed for security; 5 packages available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-2-136 ~]$ sudo su
[ec2-user@ip-172-31-2-136 ec2-user]$ mkdir efs
[ec2-user@ip-172-31-2-136 ec2-user]$ yum install -y amazon-efs-utils
[ec2-user@ip-172-31-2-136 ec2-user]$ yum install -y amazon-efs-utils
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
No such command: install-y. Please use /bin/yum --help
[ec2-user@ip-172-31-2-136 ec2-user]$ yum install -y amazon-efs-utils
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
Resolving Dependencies
--> Running transaction check
--> Package amazon-efs-utils.noarch 0:1.34.5-1.amzn2 will be installed
--> Processing Dependency: stunnel5 for package: amazon-efs-utils-1.34.5-1.amzn2.noarch
--> Running transaction check
--> Package stunnel5.x86_64 0:5.58-1.amzn2.0.1 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

Transaction Summary
  Install  1 Package

  Total size: 3.7 kB
  Is this ok [y/n]: y
  Public IPs: 43.207.47.11 Private IPs: 172.31.2.136

  i-095c0806739615856 (efs1)

```

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences ENG IN 12:39 27-02-2023

Go back to the amazon aws console , in the services go back to efs service, right click on created efs i.e. efsdemo

Name	File system ID	Encrypted	Total size	Size in Standard / One Zone	Size in Standard-IA / One Zone-IA	Provisioned Throughput (MiB/s)	File system state	Create time
efsdemo	fs-06208766c4d740d31	Encrypted	6.00 KB	6.00 KB	0 Bytes	-	Available	Mon, 2023-02-27 06:51 GMT

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences ENG IN 12:41 27-02-2023

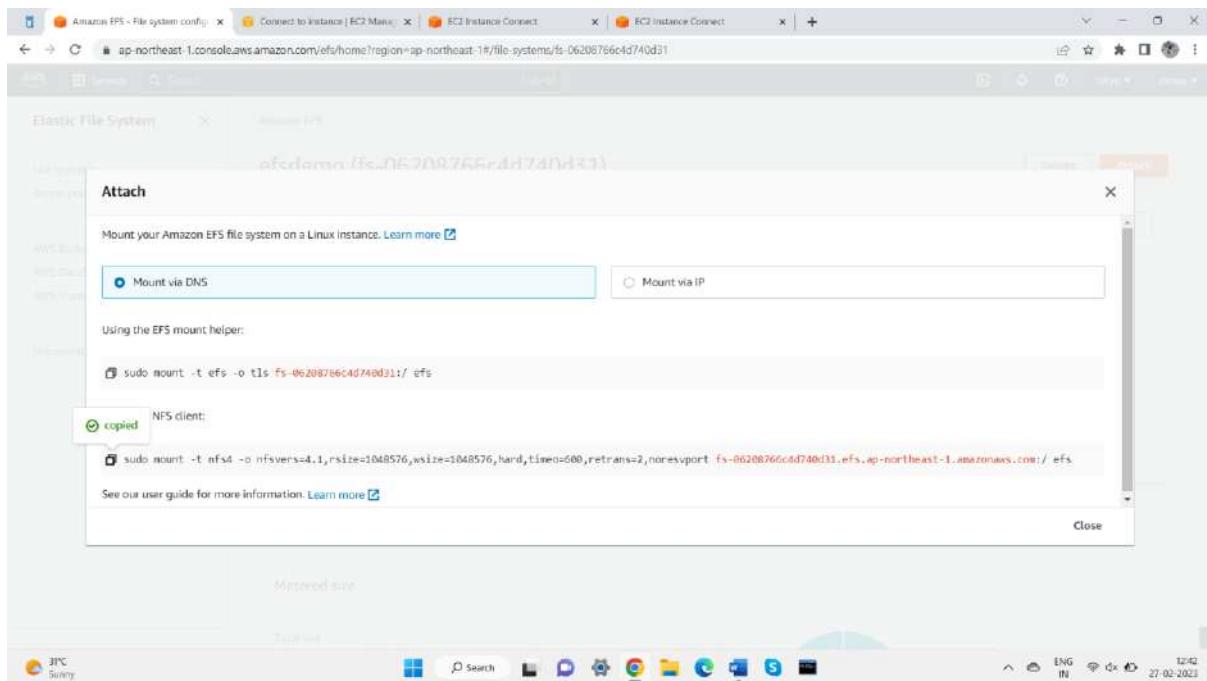
Click on attach to mount efs

The screenshot shows the AWS EFS console with the 'efsdemo' file system selected. The 'General' tab is active, displaying details such as Performance mode (General Purpose), Encryption (Enabled), and DNS name (fs-06208766c4d740d31.efs.ap-northeast-1.amazonaws.com). Other tabs include Metered size, Monitoring, Tags, File system policy, Access points, Network, and Replication.

We are mounting via DNS

The screenshot shows the 'Attach' dialog box for the 'efsdemo' file system. It provides two mounting options: 'Mount via DNS' (selected) and 'Mount via IP'. Below these options, there are examples of command snippets for both methods. A 'Close' button is at the bottom right of the dialog.

Copying the command to copy in both the remote servers. The link is copied



Copy the command in both the connections

```
Install 1 Package (+1 Dependent package)

Total download size: 221 k
Installed size: 526 k
Downloading packages:
(1/2): amazon-efs-utils-1.34.5-1.amzn2.noarch.rpm           | 56 KB  00:00:00
(2/2): stunnel5-5.58-1.amzn2.0.1.x86_64.rpm                | 165 KB 00:00:00
Total                                         679 kB/s | 221 kB 00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : stunnel5-5.58-1.amzn2.0.1.x86_64          1/2
    Installing : amazon-efs-utils-1.34.5-1.amzn2.noarch   2/2
      Verifying : amazon-efs-utils-1.34.5-1.amzn2.noarch  1/2
      Verifying : stunnel5-5.58-1.amzn2.0.1.x86_64        2/2

Installed:
  amazon-efs-utils.noarch 0:1.34.5-1.amzn2

Dependency Installed:
  stunnel5.x86_64 0:5.58-1.amzn2.0.1

Complete!
[root@ip-172-31-2-136 ec2-user]# sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noremount fs-06208766c4d740d31.efs.ap-northeast-1.amazonaws.com:/ efs
```

The terminal window shows the user running a `yum update` command to install the `amazon-efs-utils` package. The output details the download and installation of the package along with its dependencies, including `stunnel5` and `libcurl`. The final command shown is `sudo mount` to mount the EFS file system.

Type ls and cd efs in both the instance connects

```

Amazon EFS - File system config | Connect to Instance | EC2 Main | EC2 Instance Connect
ap-northeast-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=ap-northeast-1&connType=standard&instanceId=i-095c0806739615856&osUser=ec2-user&sshPort=22#/
AWS Services Search [Alt+5] Tokyo shreya

Installed size: 526 k
Downloading packages:
(1/2): amazon-efs-utils-1.34.5-1.amzn2.noarch.rpm | 56 kB 00:00:00
(2/2): stunnel15-5.58-1.amzn2.0.1.x86_64.rpm | 165 kB 00:00:00
Total 679 kB/s | 221 kB 00:00:00

Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : stunnel15-5.58-1.amzn2.0.1.x86_64 1/2
  Installing : amazon-efs-utils-1.34.5-1.amzn2.noarch 2/2
  Verifying  : amazon-efs-utils-1.34.5-1.amzn2.noarch 1/2
  Verifying  : stunnel15-5.58-1.amzn2.0.1.x86_64 2/2

Installed:
  amazon-efs-utils.noarch 0:1.34.5-1.amzn2

Dependency Installed:
  stunnel15.x86_64 0:5.58-1.amzn2.0.1

Complete!
[root@ip-172-31-2-136 ec2-user]# sudo mount -t nfs4 -o nfsv4=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport fs-06208766c4d740d31.efs.ap-northeast-1.amazonaws.com:/efs
[root@ip-172-31-2-136 ec2-user]# ls
efs
[root@ip-172-31-2-136 ec2-user]# cd efs
[root@ip-172-31-2-136 efs]# i-095c0806739615856 (efs1)
PublicIPs: 43.207.47.11 PrivateIPs: 172.31.2.136

```

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 32°C Sunny ENG IN 12:49 27-02-2023

Now create a file in any one of the ec2 instance such that it must reflect in another instance even. For example create file in instance1 must reflect in instance 2

Type touch file1 file2 and ls in any one of the instance.

Touch file1 file2 to create files and ls to list the created files.

```

Amazon EFS - File system config | Connect to Instance | EC2 Main | EC2 Instance Connect
ap-northeast-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=ap-northeast-1&connType=standard&instanceId=i-095c0806739615856&osUser=ec2-user&sshPort=22#/
AWS Services Search [Alt+5] Tokyo shreya

(2/2): stunnel15-5.58-1.amzn2.0.1.x86_64.rpm | 165 kB 00:00:00
Total 679 kB/s | 221 kB 00:00:00

Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : stunnel15-5.58-1.amzn2.0.1.x86_64 1/2
  Installing : amazon-efs-utils-1.34.5-1.amzn2.noarch 2/2
  Verifying  : amazon-efs-utils-1.34.5-1.amzn2.noarch 1/2
  Verifying  : stunnel15-5.58-1.amzn2.0.1.x86_64 2/2

Installed:
  amazon-efs-utils.noarch 0:1.34.5-1.amzn2

Dependency Installed:
  stunnel15.x86_64 0:5.58-1.amzn2.0.1

Complete!
[root@ip-172-31-2-136 ec2-user]# sudo mount -t nfs4 -o nfsv4=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport fs-06208766c4d740d31.efs.ap-northeast-1.amazonaws.com:/efs
[root@ip-172-31-2-136 ec2-user]# ls
efs
[root@ip-172-31-2-136 ec2-user]# cd efs
[root@ip-172-31-2-136 efs]# touch file1 file2
[root@ip-172-31-2-136 efs]# ls
file1 file2
[root@ip-172-31-2-136 efs]# i-095c0806739615856 (efs1)
PublicIPs: 43.207.47.11 PrivateIPs: 172.31.2.136

```

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 32°C Sunny ENG IN 12:53 27-02-2023

In another instance(instance where touch command not used) type ls. It shows the created files 11 and 12

```

Amazon EFS - File system config | Connect to instance | EC2 Main... | EC2 Instance Connect | EC2 Instance Connect
← → C ap-northeast-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=ap-northeast-1&connType=standard&instanceId=i-006d66a74eb6b097&osUser=ec2-user&sshPort=22#/ [Alt+5]

(1/2) amazon-efs-utils-1.34.5-1.amzn2.noarch.rpm
(2/2) stunnel5-5.58-1.amzn2.0.1.x86_64.rpm

Total 650 KB/s | 221 KB 00:00:00
| 56 KB 00:00:00
| 165 KB 00:00:00

Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : stunnel5-5.58-1.amzn2.0.1.x86_64 1/2
  Installing : amazon-efs-utils-1.34.5-1.amzn2.noarch 2/2
  Verifying  : amazon-efs-utils-1.34.5-1.amzn2.noarch 1/2
  Verifying  : stunnel5-5.58-1.amzn2.0.1.x86_64 2/2

Installed:
  amazon-efs-utils.noarch 0:1.34.5-1.amzn2

Dependency Installed:
  stunnel5.x86_64 0:5.58-1.amzn2.0.1

Complete!
[root@ip-172-31-44-114 ec2-user]# sudo mount -t nfs4 -o nfsversion=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport fs-06208766c4d740d31.efs.ap-northeast-1.amazonaws.com:/efs
[root@ip-172-31-44-114 ec2-user]# ls
efs
[root@ip-172-31-44-114 efs]# ls
file1  file2
[root@ip-172-31-44-114 efs]# rm file1
i-006d66a74eb6b097 (efs2)
PublicIPs: 54.95.109.164 PrivateIPs: 172.31.44.114

```

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 32°C Sunny ENG IN 12:33 27-02-2023

In the same instance connect type the command rm file1 which removes the file.

Type command ls to show the existing files present(shows only file2)

```

Amazon EFS - File system config | Connect to instance | EC2 Main... | EC2 Instance Connect | EC2 Instance Connect
← → C ap-northeast-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=ap-northeast-1&connType=standard&instanceId=i-095c0806739615856&osUser=ec2-user&sshPort=22#/ [Alt+5]

Running transaction test
Transaction test succeeded
Running transaction
  Installing : stunnel5-5.58-1.amzn2.0.1.x86_64 1/2
  Installing : amazon-efs-utils-1.34.5-1.amzn2.noarch 2/2
  Verifying  : amazon-efs-utils-1.34.5-1.amzn2.noarch 1/2
  Verifying  : stunnel5-5.58-1.amzn2.0.1.x86_64 2/2

Installed:
  amazon-efs-utils.noarch 0:1.34.5-1.amzn2

Dependency Installed:
  stunnel5.x86_64 0:5.58-1.amzn2.0.1

Complete!
[root@ip-172-31-2-136 ec2-user]# sudo mount -t nfs4 -o nfsversion=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport fs-06208766c4d740d31.efs.ap-northeast-1.amazonaws.com:/efs
[root@ip-172-31-2-136 ec2-user]# ls
efs
[root@ip-172-31-2-136 efs]# cd efs
[root@ip-172-31-2-136 efs]# touch file1 file2
[root@ip-172-31-2-136 efs]# ls
file1  file2
[root@ip-172-31-2-136 efs]# rm file1
rm: remove regular empty file 'file1'? Y
[root@ip-172-31-2-136 efs]# ls
file2
[root@ip-172-31-2-136 efs]# rm file1
i-095c0806739615856 (efs1)
PublicIPs: 43.207.47.11 PrivateIPs: 172.31.2.136

```

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 32°C Sunny ENG IN 12:54 27-02-2023

Check the same ls command in the instance where we have created file1 and file2 after removal of file1.

It shows only file2

```
Total  
Running transaction check  
Running transaction test  
Transaction test succeeded  
Running transaction  
  Installing : stunnel5-5.58-1.amzn2.0.1.x86_64 1/2  
  Installing : amazon-efs-utils-1.34.5-1.amzn2.noarch 2/2  
  Verifying   : stunnel5-5.58-1.amzn2.0.1.x86_64 1/2  
  Verifying   : amazon-efs-utils-1.34.5-1.amzn2.noarch 2/2  
Installed:  
  amazon-efs-utils.noarch 0:1.34.5-1.amzn2  
Dependency Installed:  
  stunnel5.x86_64 0:5.58-1.amzn2.0.1  
Complete!  
[root@ip-172-31-44-114 ec2-user]# sudo mount -t nfs4 -o nfovers=4.1,rsize=1048576,wsize=1048576,hard,timeout=600,retrans=2,noresvport fs-06208766c4d740d31.efs.ap-northeast-1.amazonaws.com:/efs  
[root@ip-172-31-44-114 ec2-user]# ls  
efs  
[root@ip-172-31-44-114 ec2-user]# cd efs  
[root@ip-172-31-44-114 efs]# ls  
file1  
file2  
[root@ip-172-31-44-114 efs]# ls  
[root@ip-172-31-44-114 efs]#  
i-006d66a74eb6b097f (efs2)  
PublicIPs: 54.95.109.164 PrivateIPs: 172.31.44.114
```

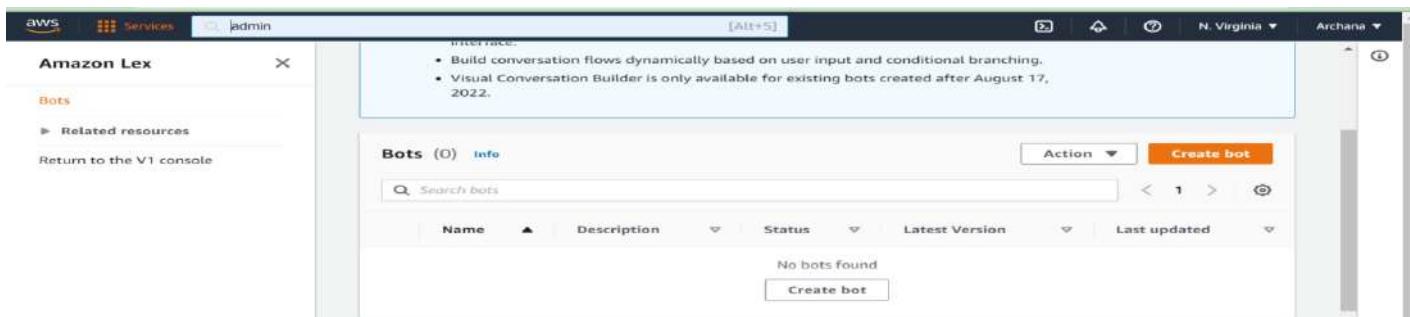
In this process Efs can be shared among ec2 instances with in the regions

EXPERIMENT 5

Creation of Amazon Lex chat bot

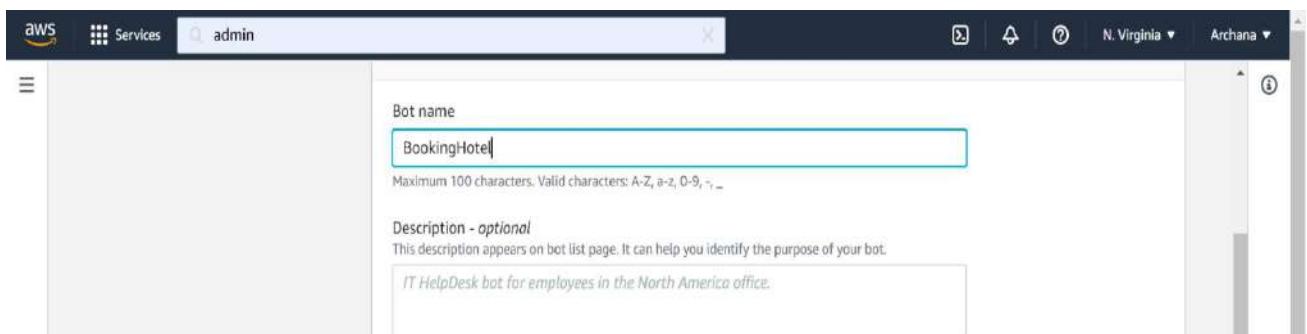


No here click on -> create bot



Here we have to select the Create a blank bot

Give the name to the Bot here I have given BookingHotel



we have select the create a role with basic Amazon Lex permission

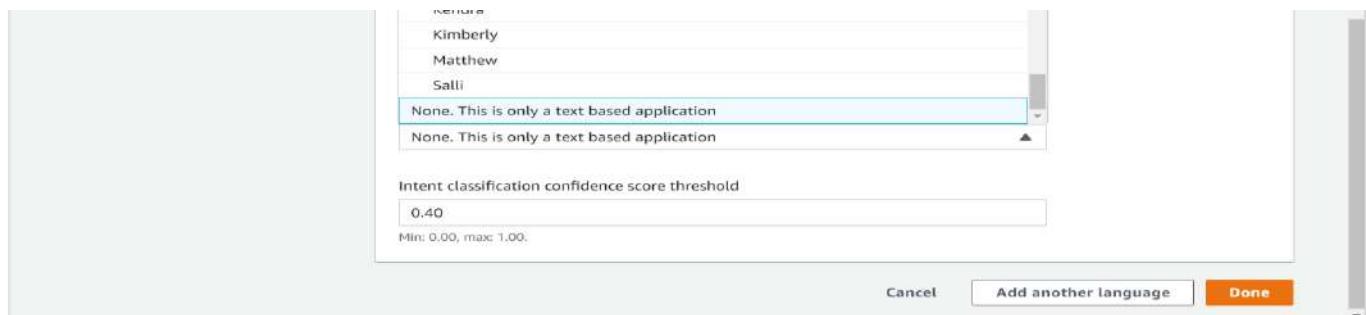


we have to give the children online privacy protection Act as No



Select the language as English US

We have different options ,here we select the “This is only text based application”



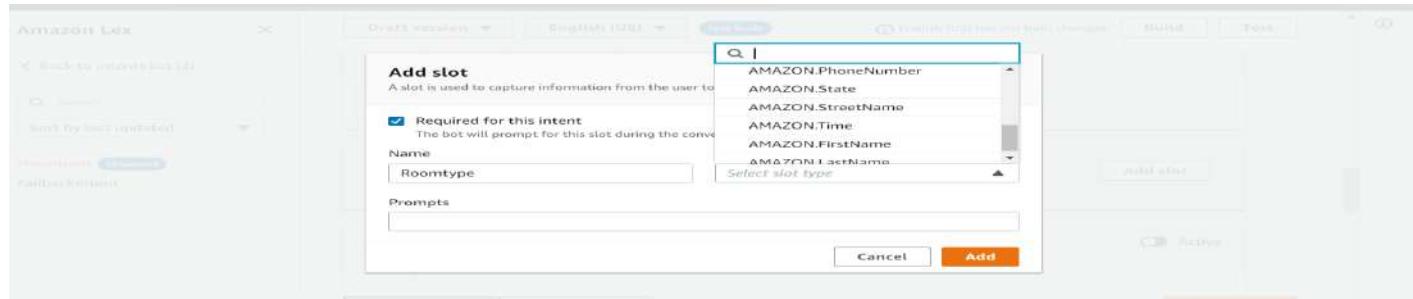
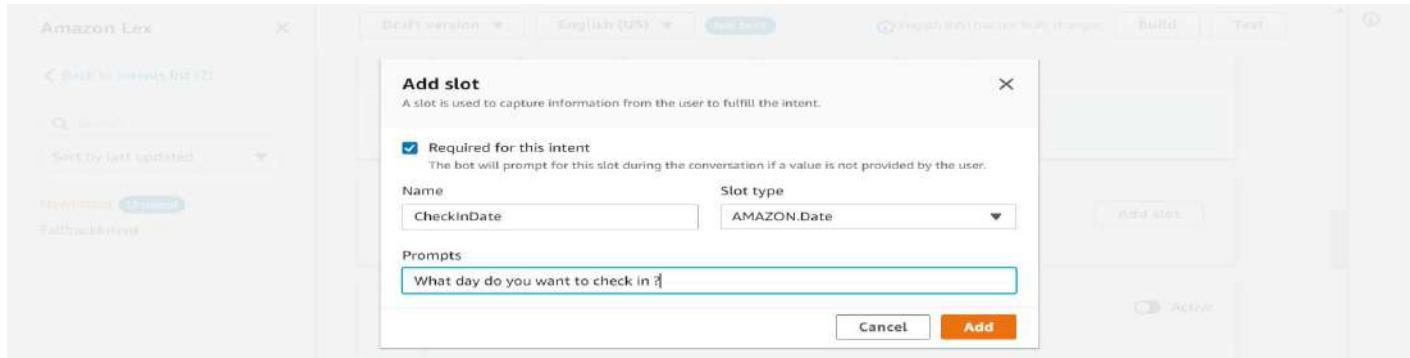
We give the name

Here we will give the prompts for utterances

The screenshot shows the AWS Lambda interface. At the top, it says "Successfully created bot: BookingHotel". Below this, there are buttons for "Draft version", "English (US)", and "Not built". A message indicates "English (US) has not built changes." with "Build" and "Test" buttons. On the left, there's a sidebar with "Amazon Lex" and a link to "Back to intents list (2)". The main area shows an intent named "BookHotel" with a note about character limits. At the bottom, there are links for "Newintent" and "FallbackIntent".

The screenshot shows the AWS Lambda interface. It displays a slot configuration for "Lacation" (note the misspelling). The "Slot type" is set to "AMAZON.City". A checkbox labeled "Required for this intent" is checked, with a note explaining it prompts for the slot if no value is provided. The "Name" field is "Lacation" and the "Slot type" is "AMAZON.City". Under "Prompts", the message "What city will you be staying in ?" is listed. A note at the bottom says "You can use the advanced options setting to configure rich messages such a custom payload, card groups, and SSML." An "Advanced options" button is also present.

We can add more extra questions by adding in ADD SlotHere we are trying to add extra slot , where it is not predefined



We can create the our own slot by creating the slot types

Go to intend ,slot types-> we click on Add Slot types

The screenshot shows the 'Slot types' configuration page in the Amazon Lex console. The left sidebar lists a single slot type named 'Roomtype' (status: Unsaved). The main area is titled 'Slot value resolution' with the sub-instruction: 'Amazon Lex resolves the slot values in an utterance to only the values you provide, or it expands the resolution to related or similar values.' Two radio button options are shown: 'Expand values (default)' (Values used as training data.) and 'Restrict to slot values' (Use only values provided.). The 'Restrict to slot values' option is selected.

Here we give the slot type

The screenshot shows a modal dialog titled 'Add blank slot type' with the instruction 'Create a custom slot type for your bot.'. A 'Slot type name' input field contains the text 'Roomtype'. Below the input field is a note: 'Maximum 100 characters. Valid characters: A-Z, a-z, 0-9, -, _'. At the bottom right of the dialog are 'Cancel' and 'Add' buttons, with 'Add' being highlighted.

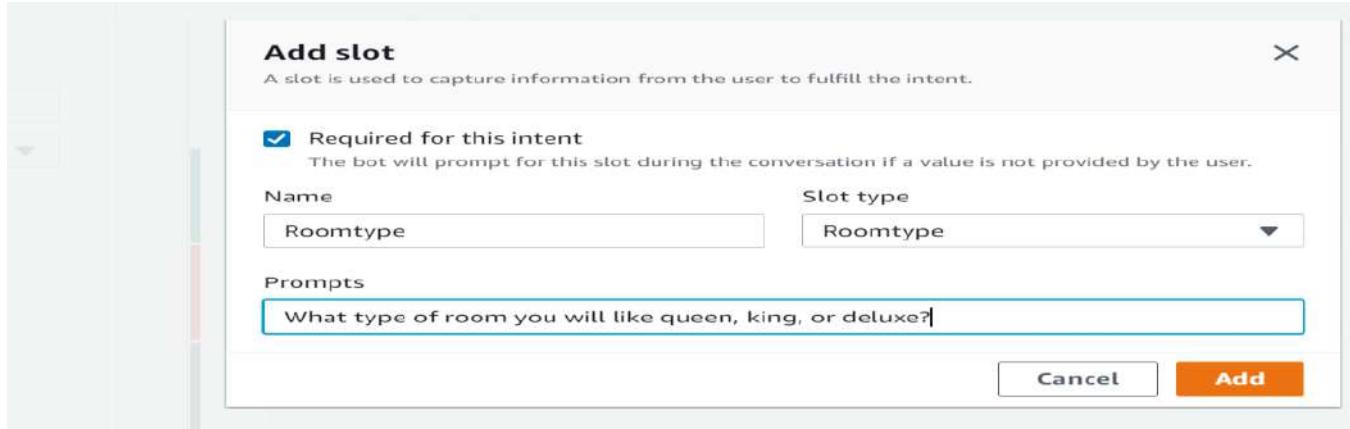
After giving the name for the slot here we go for restrict to slot values -> means it take those values which we have given to them Here we give the values for the slot type ,and click on create slot

The screenshot shows the 'Slot type values' configuration page for the 'Roomtype' slot. It lists three values: 'King', 'Queen', and 'Delux', each with a corresponding 'Value' input field and a 'Tab or ; for new value' field to its right. At the bottom is a note: 'Maximum 140 characters. Valid characters: A-Z, a-z, 0-9, @, #, \$'. A 'Add value' button is located at the bottom right.

Now come to the intend, go to slots click on add slot

The screenshot shows the 'Intents' configuration page for the 'Bookhotel' intent. It includes sections for 'Response to acknowledge the user's request' (Message: -), 'Slots (3) - optional' (Information: 'Information that a bot needs to fulfill the intent. The bot prompts for slots required for intent fulfillment, in priority order below.'), and 'Confirmation' (Info: 'Prompts help to clarify whether the user wants to fulfill the intent or cancel it.', Active status). An 'Add slot' button is located in the 'Slots (3) - optional' section.

Here we can see the our slot type which we have created ,add prompts also



After adding all the required slots we can click on save intend

Here will get the preview after saving the intend, n build the intend

After that build it ,we go for test option ,right side panel will be created with chat

The screenshot shows the AWS Lambda function configuration page for the 'BookingHotel' bot. The top navigation bar includes the AWS logo, Services, admin, and N. Virginia regions. The main title is 'Amazon Lex' with a green success message: 'Successfully built language English (US) in bot: BookingHotel'. Below this are dropdowns for 'Draft version' (set to 'Draft'), 'English (US)', and a green button labeled 'Successfully built'. A search bar and a 'Sort by last updated' dropdown are also present. On the right, there's an 'Inspect' button and a note about the last build being submitted 1 minute ago. The central area displays three utterances: 'Book a Hotel', 'I want a make hotel reservations', and 'Book a [Nights] nights stay in [location]'. Each utterance has a small edit icon.

Now we can give any one of the utterance here, I gave here Book Hotel, you see response also.In response to Book a hotel we get the replay from bot, in this way will get the responses

The screenshot shows the same AWS Lambda function configuration page for the 'BookingHotel' bot. The interface is identical to the previous one, with the 'Successfully built' message at the top. On the right, a simulated conversation is shown in a chat window. The user says 'book hotel' and the bot responds with 'What city will you be staying in ?'. This indicates that the bot has triggered the 'Book a Hotel' intent and is awaiting further input from the user.

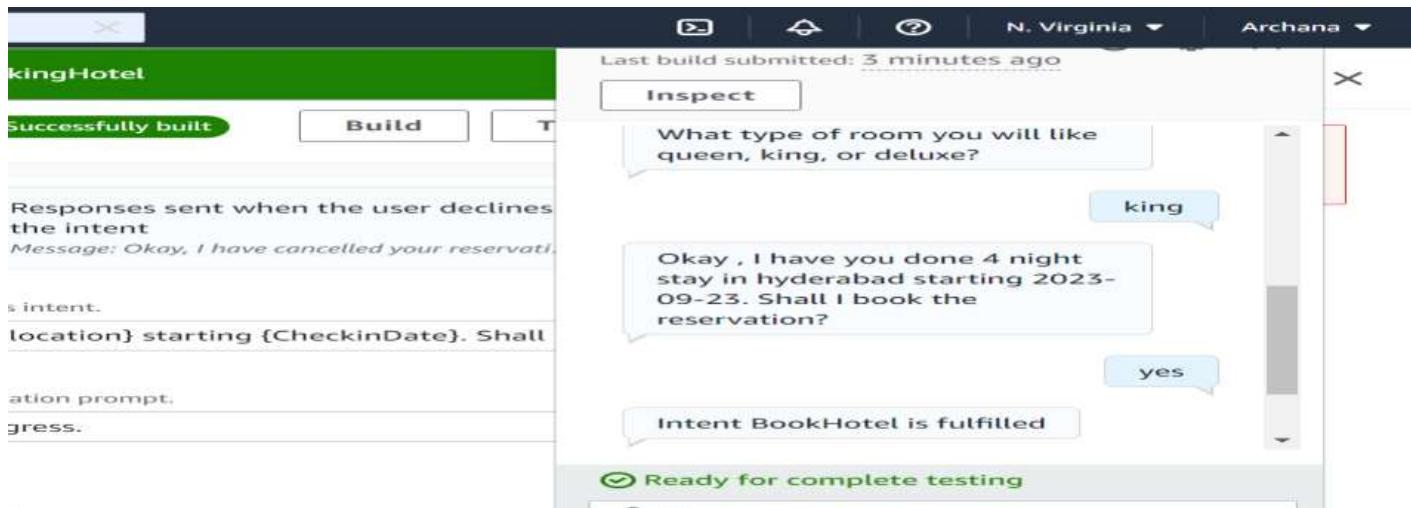
At last we get intend BookHotel is fulfilled, in spite of this message we change it .

The screenshot shows the AWS Lambda interface for the 'BookingHotel' bot. At the top, a green banner indicates 'Successfully built language English (US) in bot: BookingHotel'. Below this, there are tabs for 'Draft version' and 'English (US)', with 'Successfully built' highlighted. A search bar and a 'Sort by added (ascending)' button are also present. On the left, a sidebar lists intents: 'BookHotel' (selected) and 'FallbackIntent'. The main area displays three examples of user input: 'Book a Hotel', 'I want to make hotel reservations', and 'Book a [Nights] nights stay in [location]'. To the right, a conversation window shows a user message 'What type of room you will like queen, king, or deluxe?' followed by a bot response 'delux'. Below the conversation, a message says 'Intent BookHotel is fulfilled'. At the bottom right, a green checkmark indicates 'Ready for complete testing'.

Go to the intend ,à confirmation à prompts à confirmation prompts à type your message
Save the intend ,build it and test it again

The screenshot shows the AWS Lambda interface for the 'BookingHotel' bot. The top banner indicates 'Successfully built language English (US) in bot: BookingHotel'. Below this, there are tabs for 'Draft version' and 'English (US)', with 'Successfully built' highlighted. On the right, there are 'Build' and 'Test' buttons. The main area is divided into sections for 'Prompts to confirm the intent' and 'Responses sent when the user declines the intent'. Under 'Prompts to confirm the intent', a message is shown: 'Message: Okay, I have you done {Nights} night stay in...'. Under 'Responses sent when the user declines the intent', another message is shown: 'Message: Okay, I have cancelled your reservation in pr...'. Below these, there are sections for 'Confirmation prompt' (with a placeholder message 'Okay, I have you done {Nights} night stay in {location} starting {CheckinDate}. Shall I book the reservation?') and 'Decline response' (with a placeholder message 'Okay, I have cancelled your reservation in progress.'). A note at the bottom states: 'What will the bot say if the user says NO to the confirmation prompt.' followed by the same decline message.

Now we can see the confirmation message is displayed here



EXPERIMENT 6

Creation of S3 bucket and trigger by lambda to dynamo DB

Go to IAM service à create a role

The screenshot shows the AWS IAM service interface. The top navigation bar has 'Services' selected, and the search bar contains 'iam'. The main content area displays a search result for 'iam' with two items: 'IAM' (Manage access to AWS resources) and 'IAM Identity Center (successor to AWS Single Sign-On)'. Below this, the 'Identity and Access Management (IAM)' section is open, showing 'Access management' with 'User groups' listed. On the right, the 'Roles' page is displayed, showing 16 roles. A blue banner at the top of the 'Roles' page says 'Now! Securely access AWS services from your data center with IAM Roles Anywhere. Learn more'. A 'Create role' button is visible on the right side of the 'Roles' page.

Select the AWS Service and enable Lambda à click on Next

The screenshot shows the 'Create role' wizard, Step 1: Select trusted entity. The title is 'Select trusted entity' with an 'Info' link. It shows three options under 'Trusted entity type': 'AWS service' (selected), 'AWS account', and 'Web identity'. The 'AWS service' option is described as allowing AWS services like EC2, Lambda, or others to perform actions in the account. The 'AWS account' option is described as allowing entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account. The 'Web identity' option is described as allowing users federated by the specified external web identity provider to assume this role to perform actions in this account. Below this, there are sections for 'Use case' (with a note about allowing EC2 or Lambda to call AWS services) and 'Common use cases' (with options for EC2 and Lambda). At the bottom are 'Cancel' and 'Next' buttons.

Select the role as AWS DynamoDBFullAccess ànext

The screenshot shows the 'Add permissions' step of the IAM role creation wizard. On the left, a sidebar lists three steps: Step 1 (Select trusted entity), Step 2 (Add permissions), and Step 3 (Name, review, and create). Step 2 is currently selected. The main area is titled 'Permissions policies (815)' and contains a search bar with the query '"dynamodb"'. A table lists one policy: 'AmazonDynamoDBFullAccess' (Type: AWS managed policy, Description: Provides full access to Amazon DynamoDB via the AWS Management Console and AWS SDKs). There are buttons for 'Create policy' and 'Clear filters'.

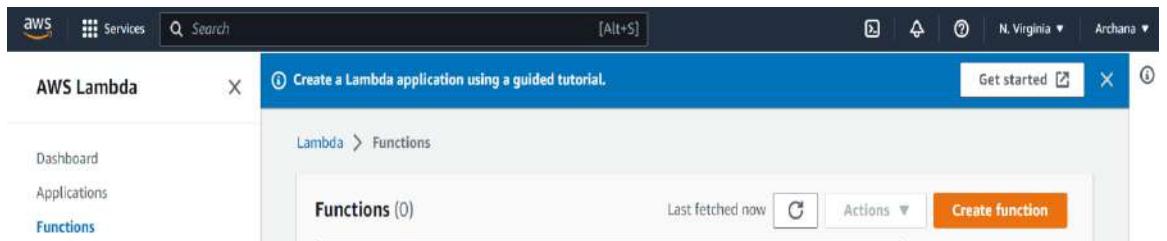
Give the name to the role here -àcreate role

The screenshot shows the 'Name, review, and create' step of the IAM role creation wizard. The sidebar shows Step 1 (Select trusted entity), Step 2 (Add permissions), and Step 3 (Name, review, and create). Step 3 is selected. The main area has a title 'Role details' and a 'Role name' input field containing 'iam_for_dynamodb'. Below it is a note: 'Maximum 64 characters. Use alphanumeric and '-' characters.' There is also an 'Add tag' button and a note: 'You can add up to 50 more tags.' At the bottom are 'Cancel', 'Previous', and 'Create role' buttons.

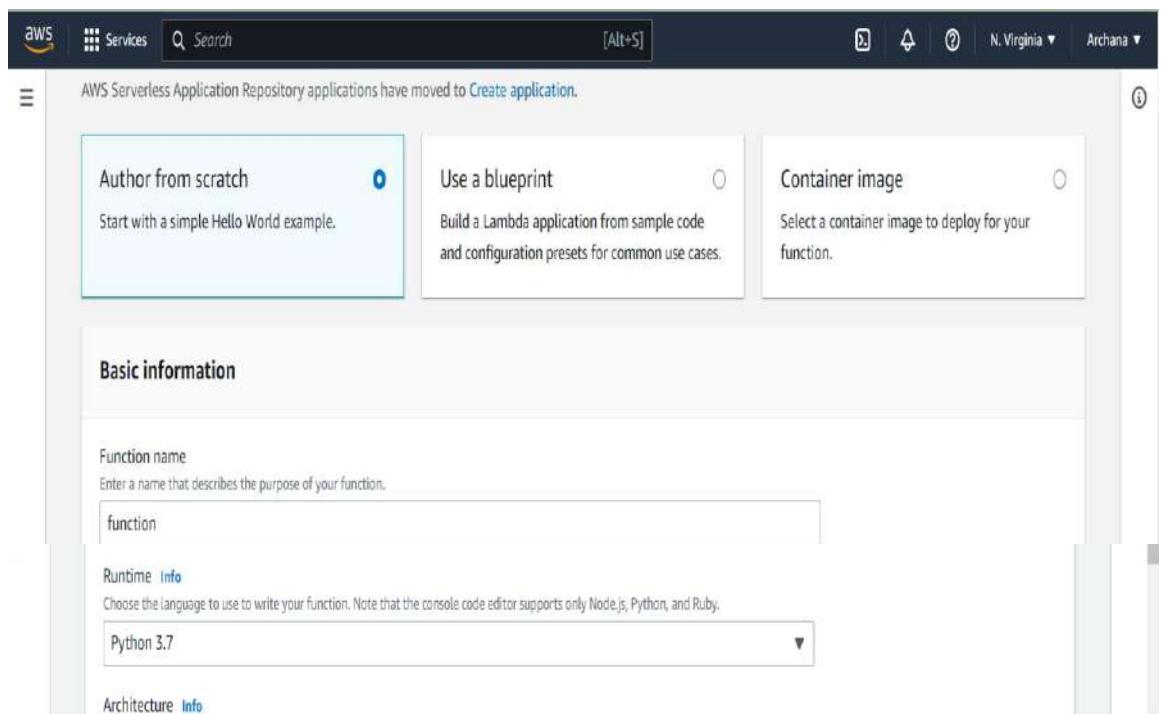
Role is successfully created

The screenshot shows the IAM Roles page. The sidebar says 'Identity and Access Management (IAM)'. The main area displays a green success message: 'Role iamfordynamodb created.' with a 'View role' button. Navigation links include 'Search IAM' and 'IAM > Roles'. A blue banner at the top says 'New! Securely access AWS services from your data center with IAM Roles Anywhere. Learn more.'

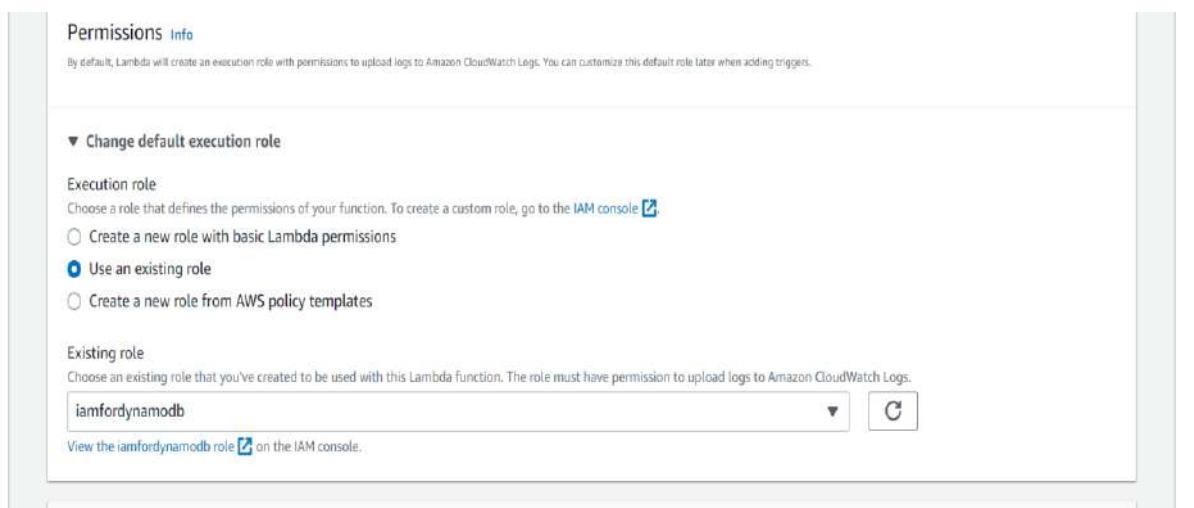
Now go to the Lambda service ,and create the function



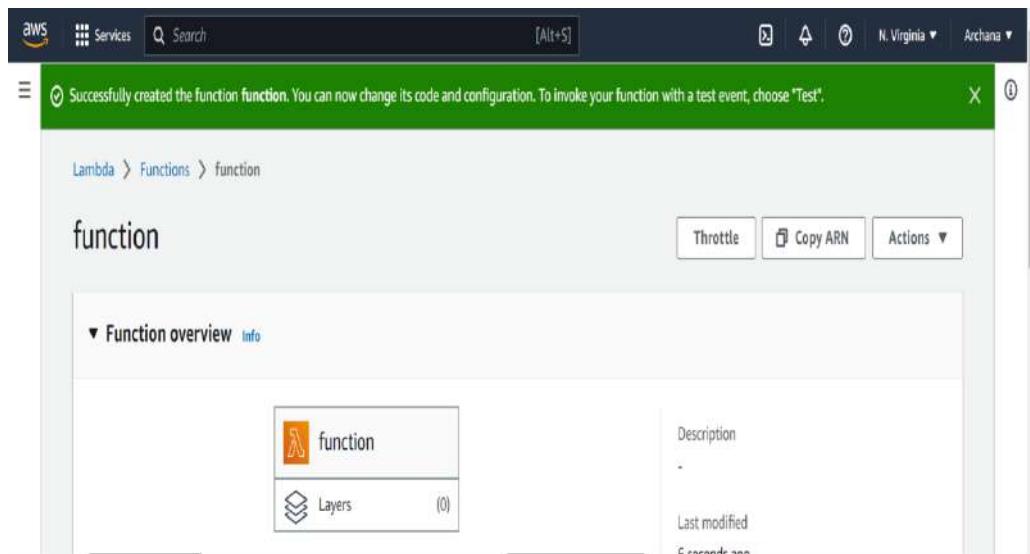
Choose the option Author from scratch ,give function name and select the language as python 3.7



In permissions à change default execution role à select the use an existing role à create function



Function is successfully created



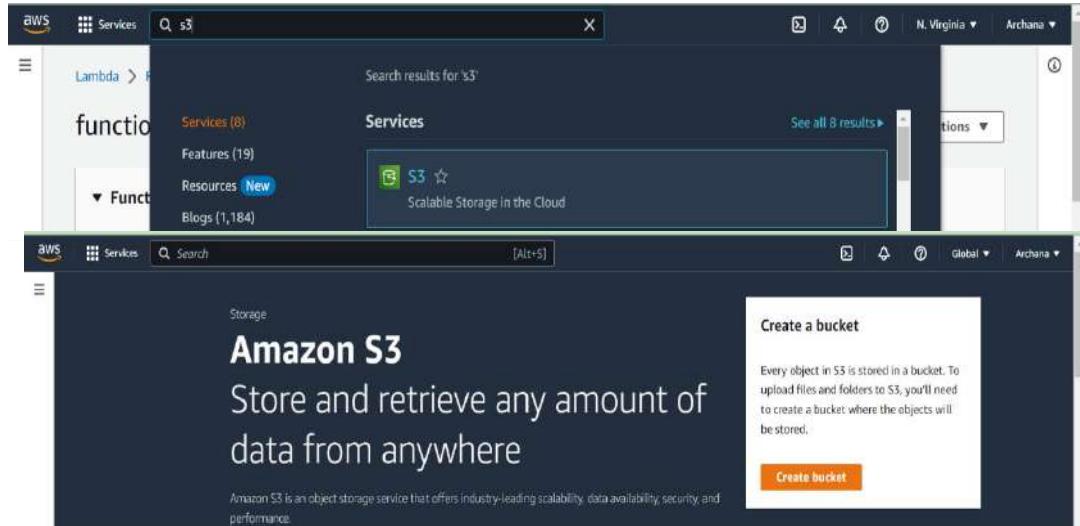
Click on code à copy the code in code area -à click on Deploy

The screenshot shows the AWS Lambda function editor interface. The top navigation bar includes tabs for Code, Test, Monitor, Configuration, Aliases, and Versions. The Code tab is selected. Below the tabs is a toolbar with File, Edit, Find, View, Go, Tools, Window, Test, Deploy, and a status message 'Changes not deployed'. On the far right of the toolbar are settings and gear icons. A search bar at the top says 'Go to Anything (Ctrl-P)'. The main area is titled 'lambda_function' and contains a code editor with the following Python code:

```
1 import boto3
2 from uuid import uuid4
3 def lambda_handler(event, context):
4     s3 = boto3.client("s3")
5     dynamodb = boto3.resource('dynamodb')
6     for record in event['Records']:
7         bucket_name = record['s3']['bucket']['name']
8         object_key = record['s3']['object']['key']
9         size = record['s3']['object'].get('size', -1)
10        event_name = record['eventName']
11        event_time = record['eventTime']
12        dynamoTable = dynamodb.Table('newtable')
13        dynamoTable.put_item(
14            Item={'unique': str(uuid4()), 'Bucket': bucket_name, 'Object': object_key, 'Size': size, 'Event': event_name, 'EventTime': event_time})
```

The screenshot shows the AWS Lambda function editor interface after deployment. A green notification bar at the top states 'Successfully updated the function function.' The interface is identical to the previous screenshot, with the same tabs, toolbar, and code editor. The code in the editor remains the same as shown above.

Go to S3 service and create bucket



Give the bucket name globally unique

A screenshot of the 'Create a new bucket' configuration page. The top navigation bar includes the AWS logo, 'Services' button, and a search bar with the placeholder 'Search' and keyboard shortcut '[Alt+S]'. Below the search bar, a message states 'Buckets are containers for data stored in S3. Learn more' with a link icon. The main form is titled 'General configuration'. It has two main sections: 'Bucket name' and 'AWS Region'. In the 'Bucket name' section, the input field contains the value 'lambdadynamodb'. A note below the field says 'Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming' with a link icon. In the 'AWS Region' section, a dropdown menu is open, showing 'US East (N. Virginia) us-east-1' as the selected option. There is also a link 'Copy settings from existing bucket - optional' at the bottom of the configuration form.

Uncheck the block all public access, and acknowledge it à create bucket

The screenshot shows the 'Block all public access' settings for an S3 bucket. There are four checkboxes:

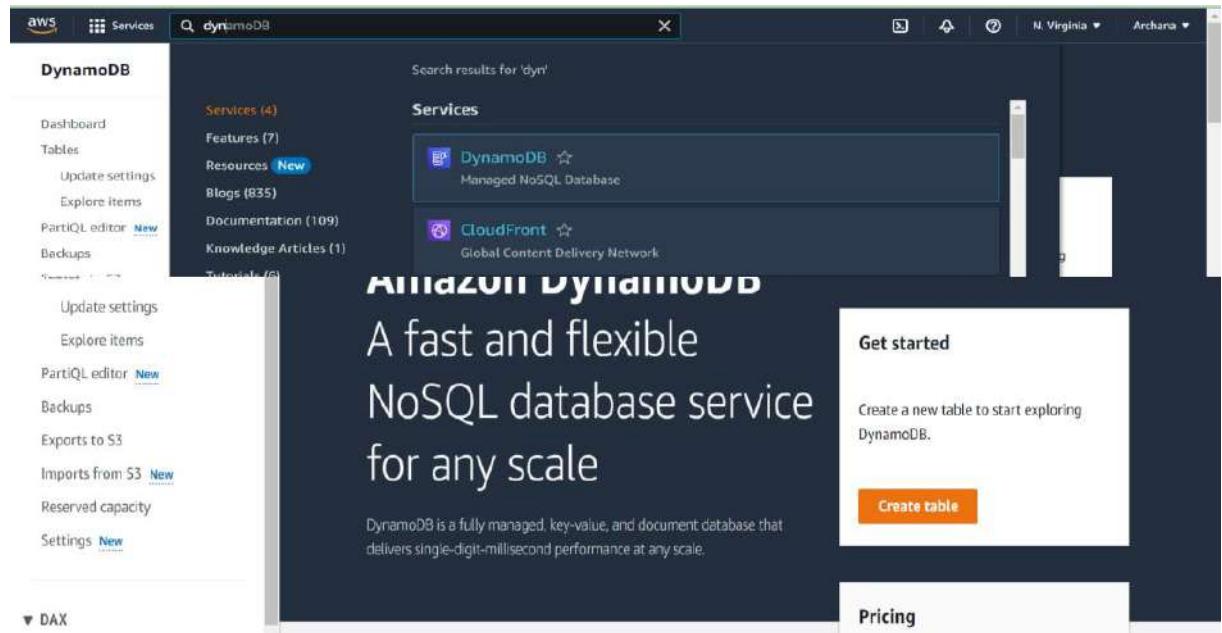
- Block all public access**: Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
- Block public access to buckets and objects granted through new access control lists (ACLs)**: S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**: S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**: S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**: S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

A warning message at the bottom states: "Turning off block all public access might result in this bucket and the objects within becoming public. AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting." A checkbox below it says: "I acknowledge that the current settings might result in this bucket and the objects within becoming public." The checkbox is checked.

The screenshot shows the 'Buckets' page in the AWS S3 console. A green banner at the top says: "Successfully created bucket 'lambdadynamodb123'. To upload files and folders, or to configure additional bucket settings choose View details." Below the banner, there's an 'Account snapshot' section with a 'View Storage Lens dashboard' button. The main area shows a table of buckets:

Name	AWS Region	Access	Creation date
lambdadynamodb123	US East (N. Virginia) us-east-1	Objects can be public	February 7, 2023, 20:22:42 (UTC+05:30)

Go to service DynamoDB and create the table



Give the table as newtable and partition key as unique which we provided in the code à create table

This screenshot shows the 'Create table' wizard on the 'Set table details' step. The 'Table name' field is filled with 'newtable'. The 'Partition key' field contains 'unique' with a dropdown menu showing 'String'. Below these fields, there are sections for 'Sort key - optional' (disabled) and 'Tags' (disabled). At the bottom right are 'Cancel' and 'Create table' buttons.

Go lambda function à Add trigger -à Select the service à select the bucket à Select the All object create events

The screenshot shows the 'Add trigger' step for a Lambda function. In the top navigation bar, 'S3' is selected under the 'aws storage' category. The 'Bucket' section is set to 's3/lambdadynamodb123'. The 'Event type' dropdown is set to 'All object create events'. A note below the bucket selection states: 'Please select the S3 bucket that serves as the event source. The bucket must be in the same region as the function.' and 'Select the events that you want to have trigger the Lambda function. You can optionally set up a prefix or suffix for an event. However, for each bucket, individual events cannot have multiple configurations with overlapping prefixes or suffixes that could match the same object key.'

Acknowledge it à add

This screenshot shows the 'Acknowledge' step. It includes a note about recursive invocation: 'If your function writes objects to an S3 bucket, ensure that you are using different S3 buckets for input and output. Writing to the same bucket increases the risk of creating a recursive invocation, which can result in increased Lambda usage and increased costs.' Below this is a checked checkbox: 'I acknowledge that using the same S3 bucket for both input and output is not recommended and that this configuration can cause recursive invocations, increased Lambda usage, and increased costs.' A note below the checkbox states: 'Lambda will add the necessary permissions for AWS S3 to invoke your Lambda function from this trigger.' A red error message box contains the text: '☒ An error occurred when creating the trigger: Please correct the errors above.' At the bottom right are 'Cancel' and 'Add' buttons.

Go to S3 and upload file in the bucket

The screenshot shows the Amazon S3 console. A green success banner at the top reads: 'Successfully created bucket "lambdadynamodb123". To upload files and folders, or to configure additional bucket settings choose View details.' On the left sidebar, 'Buckets' is selected. The main area displays an 'Account snapshot' with a 'View Storage Lens dashboard' button. Below it is a 'Buckets (1)' table with one item: 'lambdadynamodb123'. The table includes columns for Name, AWS Region, Access, and Creation date. The 'Name' column shows 'lambdadynamodb123', 'AWS Region' shows 'US East (N. Virginia) us-east-1', 'Access' shows 'Objects can be public', and 'Creation date' shows 'February 7, 2023, 20:22:42 (UTC+05:30)'. Action buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket' are also visible.

Here we have uploaded the file

The screenshot shows two consecutive screenshots of the AWS S3 console. The top screenshot displays a table titled 'Files and folders (1 Total, 657.0 B)' with one item: 'lambda code.txt' (text/plain, 657.0 B). Below it is a search bar and buttons for 'Remove', 'Add files', and 'Add folder'. The bottom screenshot shows a green success message: 'Upload succeeded' with a link to 'View details below.' It also shows the 'Upload: status' section with a note about session expiration and a 'Summary' table.

Come to DynamoDB here we can see in explore items ,the details of s3 has been updated

The screenshot shows the AWS DynamoDB 'Explore items' interface. On the left, the navigation pane includes 'Dashboard', 'Tables', 'Explore items' (which is selected), 'PartiQL editor', 'Backups', 'Exports to S3', 'Imports from S3', 'Reserved capacity', and 'Settings'. Under 'DAX', there are 'Clusters' and 'Subnet groups'. The main area shows a table named 'newtable' with one item: 'unique' (Bucket: lambdadyn..., Event: ObjectCreate..., EventTime: 2023-01-16T11:45:00Z).

EXPERIMENT 7

Pull the image from Docker to EC2 Instance and access it publicly.

Create the EC2 instance and connect with EC2 Console.

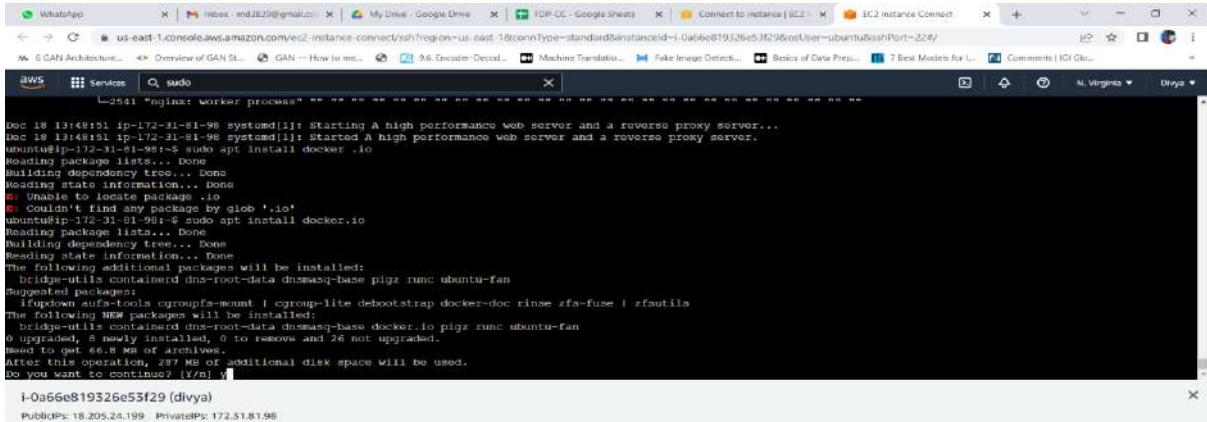
- In the opened Console of EC2, Type the following commands to pull the image from docker
 - sudo apt update / sudo apt-get update
 - sudo apt install docker.io / sudo apt-get install docker .io
 - sudo docker version
 - sudo docker image ls (it shows the images list present in our Instance)

Note: we don't have images in the instance because we didn't pulled the image from docker

- sudo docker pull scott2srikanth/fileshare_docker-fdp (pull the image)
- sudo docker image ls (shows the image pulled in the list)
- sudo docker run -d -p 3000:3000 scott2srikanth/fsdreactdemo

Note: 3000:3000 first is inbound values we change it but right isde 3000 value is docker bound values we cant change that,example we can give 3008:3000

```
No containers need to be restarted.  
No user sessions are running outdated binaries.  
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
ubuntu@ip-172-31-81-98:~$ sudo systemctl start nginx  
ubuntu@ip-172-31-81-98:~$ sudo systemctl status nginx  
● nginx.service - A high performance web server and a reverse proxy server  
  Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)  
  Active: active (running) since Sun 2022-12-18 13:48:51 UTC; 1min 4s ago  
    Docs: man:nginx(8)  
    Process: 2444 ExecStartPre=/usr/sbin/nginx -t -g daemon on; master_process on; (code=exited, status=0/SUCCESS)  
    Process: 2445 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)  
   Main PID: 2538 (nginx)  
     Tasks: 2 (limit: 1143)  
    Memory: 4.6M  
      CPU: 23ms  
     CGroup: /system.slice/nginx.service  
           ├─2538 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"  
           └─2541 "nginx: worker process"  
Dec 18 13:48:51 ip-172-31-81-98 systemd[1]: Starting A high performance web server and a reverse proxy server...  
Dec 18 13:48:51 ip-172-31-81-98 systemd[1]: Started A high performance web server and a reverse proxy server.  
ubuntu@ip-172-31-81-98:~$ sudo apt install docker.io  
i-0a66e819326e53f29 (divy)  
PublicIPs: 18.205.24.199 PrivateIPs: 172.31.81.98
```

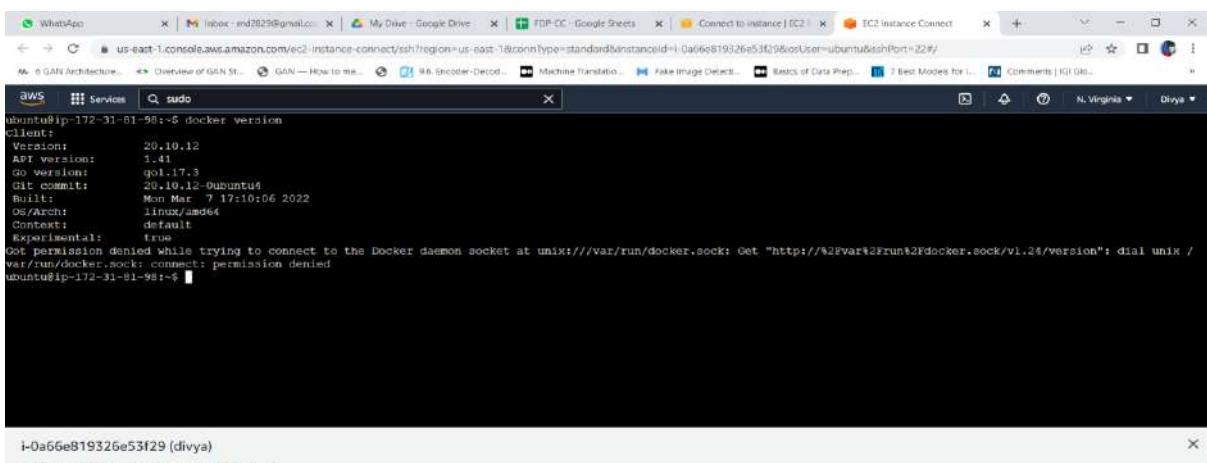


```
i-0a66e819326e53f29 "nginx: worker process" ""
```

```
Dec 18 13:48:51 ip-172-31-81-98 systemd[1]: Starting A high performance web server and a reverse proxy server...
Dec 18 13:48:51 ip-172-31-81-98 systemd[1]: Started A high performance web server and a reverse proxy server.
ubuntu@ip-172-31-81-98:~$ sudo apt install docker.io
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package .io
ubuntu@ip-172-31-81-98:~$ sudo apt install docker.io
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
bridge-utils containerd dns-root-data dnsmasq-base liblz4-1 liblzo2-2 libnftnl0 librktls0 libubntu-fan
recommended packages:
ifupdown auto-tools cgroupsfs-mount libcrypt-lite debootstrap docker-doc rinse zfs-fuse | rfautofs
The following NEW packages will be installed:
bridge-utils containerd dns-root-data dnsmasq-base docker.io liblz4-1 liblzo2-2 libnftnl0 librktls0 libubntu-fan
0 upgraded, 8 newly installed, 0 to remove and 26 not upgraded.
Need to get 66.8 MB of archives.
After this operation, 287 MB of additional disk space will be used.
Do you want to continue? [Y/n] i
```

i-0a66e819326e53f29 (divya)

PublicIPs: 18.205.24.199 PrivateIPs: 172.31.81.98



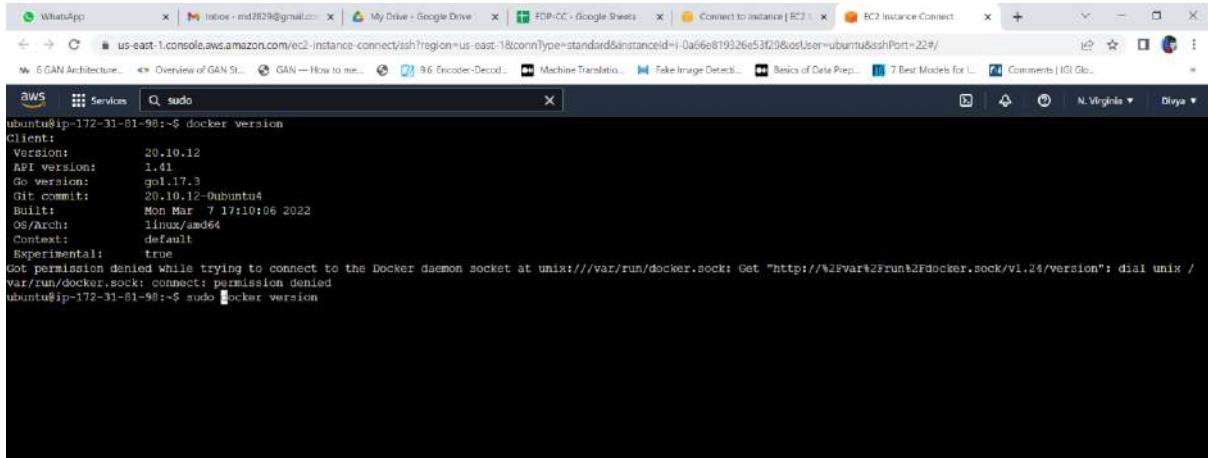
```
i-0a66e819326e53f29 "nginx: worker process" ""
```

```
ubuntu@ip-172-31-81-98:~$ docker version
Client:
 Version: 20.10.12
 API version: 1.41
 Go version: go1.17.3
 Git commit: 20.10.12-0ubuntu4
 Built: Mon Mar  7 17:10:06 2022
 OS/Arch: linux/amd64
 Context: default
 Experimental: true
Get permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/v1.24/version": dial unix /
var/run/docker.sock: connect: permission denied
ubuntu@ip-172-31-81-98:~$
```

i-0a66e819326e53f29 (divya)

PublicIPs: 18.205.24.199 PrivateIPs: 172.31.81.98

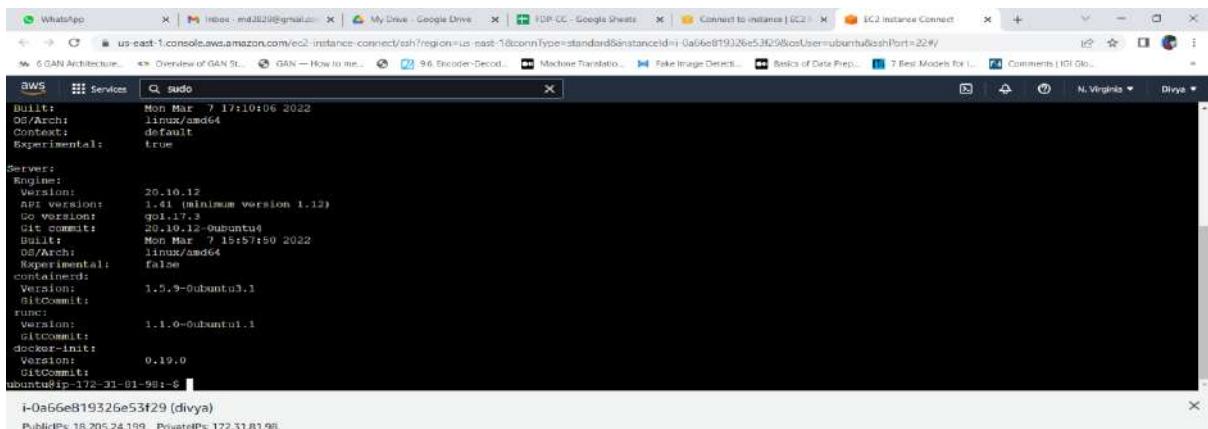




```
ubuntu@ip-172-31-81-98:~$ docker version
Client:
  Version:          20.10.12
  API version:      1.41
  Go version:       go1.17.3
  Git commit:       20.10.12-0ubuntu4
  Built:            Mon Mar  7 17:10:06 2022
  OS/Arch:          linux/amd64
  Context:          default
  Experimental:    true
Got permission denied while trying to connect to the docker daemon socket at unix:///var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/v1.24/version": dial unix /var/run/docker.sock: connect: permission denied
ubuntu@ip-172-31-81-98:~$ sudo docker version
```

i-0a56e819326e53f29 (divya)

PublicIPs: 18.205.24.199 PrivateIPs: 172.31.81.98



```
ubuntu@ip-172-31-81-98:~$ docker version
Client:
  Version:          20.10.12
  API version:      1.41 (minimum version 1.12)
  Go version:       go1.17.3
  Git commit:       20.10.12-0ubuntu4
  Built:            Mon Mar  7 15:57:50 2022
  OS/Arch:          linux/amd64
  Context:          default
  Experimental:    false
Server:
  Engine:
    Version:          20.10.12
    API version:      1.41 (minimum version 1.12)
    Go version:       go1.17.3
    Git commit:       20.10.12-0ubuntu4
    Built:            Mon Mar  7 15:57:50 2022
    OS/Arch:          linux/amd64
    Experimental:    false
  containerd:
    Version:          1.5.9-0ubuntu0.3.1
    GitCommit:        774f23d7b01fe9e9c97d8df61b44a070
    OSErr:             None
  runc:
    Version:          1.1.0-0ubuntu0.1
    GitCommit:        9af07a005e455a058d89273f939a3a74
  docker-init:
    Version:          0.19.0
    GitCommit:        9935703
ubuntu@ip-172-31-81-98:~$
```

i-0a56e819326e53f29 (divya)

PublicIPs: 18.205.24.199 PrivateIPs: 172.31.81.98



```
WhatsApp X Inbox - md32020 X My Drive - Google X Connect to insta... X EC2 Instance Con... X Docker Hub X docker image bu... X
← C os-east-1.console.aws.amazon.com/ec2/instance-connect/ssr?region=us-east-1&connType=standard&instanceId=i-0a66e819326e53f298ccUser=ubuntu&sshPort=22/
6 GAN Architecture... Overview of GAN... GAN - How to me... 9.6 Decoder-Decou... Machine Translat... False Image Detect... Basics of Data Prep... 7 Best Models for L... Comments | IOT Obj...
AWS Services Q sudo
ubuntu@ip-172-31-81-98:~$ sudo docker pull scott2srikanth/fileshare_docker_fdp
Using default tag: latest
Error response from daemon: pull access denied for scott2srikanth/fileshare_docker_fdp, repository does not exist or may require 'docker login': denied: requested access to the resource is denied
ubuntu@ip-172-31-81-98:~$ sudo docker pull scott2srikanth/fileshare_docker-fdp
Using default tag: latest
latest: Pulling from scott2srikanth/fileshare_docker-fdp
10cff8997b4d: Extracting [====] 25.62MB/53.69MB
4c9f2abf674dc: Download complete
daa253bf7db: Download complete
ad1603b1024ec: Download complete
d1214141: Download complete
dfe3e54a67b3: Download complete
25917ca5aa021: Download complete
2ea5a9ef7047: Download complete
285fafc7b4ec: Download complete
2da2b6c10e99: Download complete
c841125e0eacfc: Download complete
ef0d9b90675: Download complete
3755232175e0: Download complete


```

i-0a66e819326e53f29 (divya)

PublicIP: 18.205.24.199 PrivateIP: 172.31.81.98

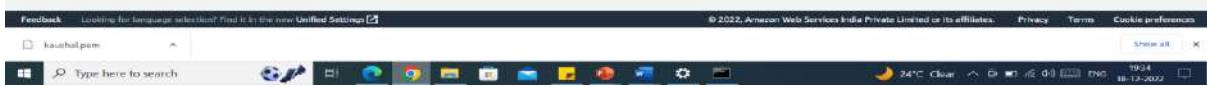


```
WhatsApp X Inbox - md32020 X My Drive - Google X Connect to insta... X EC2 Instance Con... X Docker Hub X docker image bu... X
← C os-east-1.console.aws.amazon.com/ec2/instance-connect/ssr?region=us-east-1&connType=standard&instanceId=i-0a66e819326e53f298ccUser=ubuntu&sshPort=22/
6 GAN Architecture... Overview of GAN... GAN - How to me... 9.6 Decoder-Decou... Machine Translat... False Image Detect... Basics of Data Prep... 7 Best Models for L... Comments | IOT Obj...
AWS Services Q sudo
statust Downloaded newer image for scott2srikanth/fileshare_docker-fdp:latest
docker.io/scott2srikanth/fileshare_docker-fdp:latest
ubuntu@ip-172-31-81-98:~$ docker image
Usage: docker image COMMAND

Manage images

Commands:
build      Build an image from a Dockerfile
history   Show the history of an image
import    Import the contents from a tarball to create a filesystem image
inspect   Display detailed information on one or more images
load      Load an image from a tar archive or STDIN
ls        List images
prune     Remove unused images
pull      Pull an image or a repository from a registry
push      Push an image or a repository to a registry
rm       Remove one or more images
save     Save one or more images to a tar archive (stremmed to STDOUT by default)
tag       Create a tag TARGET_IMAGE that refers to SOURCE_IMAGE

Run 'docker image COMMAND --help' for more information on a command.
ubuntu@ip-172-31-81-98:~$ sudo docker image
i-0a66e819326e53f29 (divya)
PublicIP: 18.205.24.199 PrivateIP: 172.31.81.98
```



```
WhatsApp X Inbox - md32020 X My Drive - Google X Connect to insta... X EC2 Instance Con... X Docker Hub X docker image bu... X
← C os-east-1.console.aws.amazon.com/ec2/instance-connect/ssr?region=us-east-1&connType=standard&instanceId=i-0a66e819326e53f298ccUser=ubuntu&sshPort=22/
6 GAN Architecture... Overview of GAN... GAN - How to me... 9.6 Decoder-Decou... Machine Translat... False Image Detect... Basics of Data Prep... 7 Best Models for L... Comments | IOT Obj...
AWS Services Q sudo
Usage: docker image COMMAND

Manage images

Commands:
build      Build an image from a Dockerfile
history   Show the history of an image
import    Import the contents from a tarball to create a filesystem image
inspect   Display detailed information on one or more images
load      Load an image from a tar archive or STDIN
ls        List images
prune     Remove unused images
pull      Pull an image or a repository from a registry
push      Push an image or a repository to a registry
rm       Remove one or more images
save     Save one or more images to a tar archive (stremmed to STDOUT by default)
tag       Create a tag TARGET_IMAGE that refers to SOURCE_IMAGE

Run 'docker image COMMAND --help' for more information on a command.
ubuntu@ip-172-31-81-98:~$ sudo docker image ls
REPOSITORY          TAG      IMAGE ID      CREATED     SIZE
scott2srikanth/fileshare_docker-fdp  latest  ad519b868f39  2 months ago  973MB
ubuntu@ip-172-31-81-98:~$ i-0a66e819326e53f29 (divya)
PublicIP: 18.205.24.199 PrivateIP: 172.31.81.98
```



WhatsApp | Inbox - md2022@gmail.com | My Drive - Google Sheets | FDF-CC - Google Sheets | Connect to instance | EC2 Instance Connect | Docker Hub | +

os-east-1.console.aws.amazon.com/ec2-instance-connect/sshd?region=us-east-1&connType=standard&instanceId=i-0a66e819326a53f298ccUser=ubuntu&sshPort=224/

6 GAN Architecture... Overview of GAN... GAN — How to me... 9.6 Decoder-Decoupler Machine Translation... False Image Detection... Basics of Data Prepr... 7 Best Models for L... Comments | DOI | Obj...

N. Virginia Dives...

AWS Services Q sudo

Usage: docker image COMMAND

Manage images

Commands:

```

build      build an image from a dockerfile
history    Show the history of an image
import     Import the contents from a tarball to create a filesystem image
inspect   Display detailed information on one or more images
load      Load an image from a tar archive or STDIN
ls       List images
prime     Remove unused images
pull      Pull an image or a repository from a registry
push      Push an image or a repository to a registry
rm       Remove one or more images
save      Save one or more images to a tar archive (streamed to STDOUT by default)
tag       Create a tag TARGET_IMAGE that refers to SOURCE_IMAGE

```

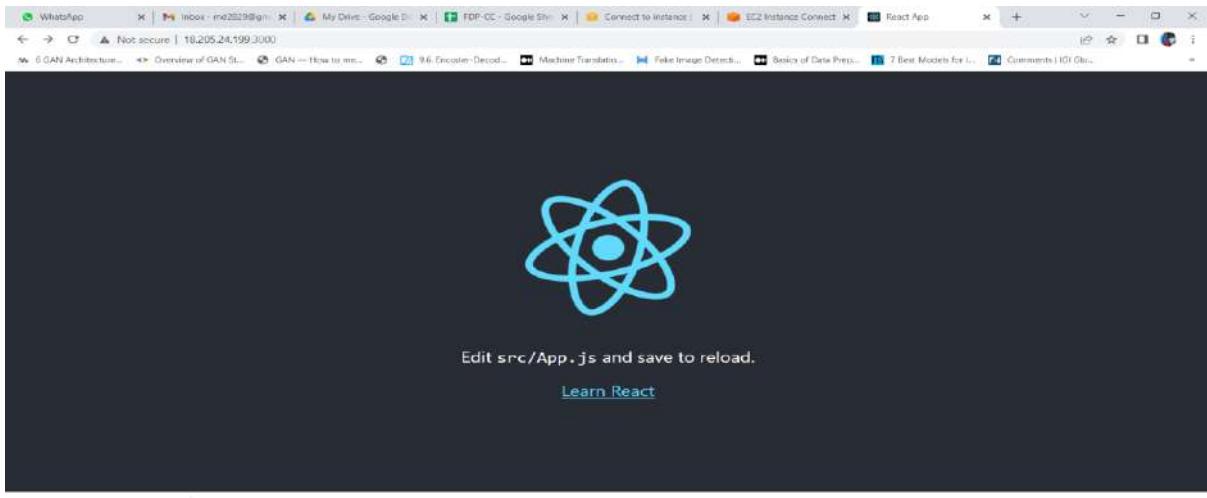
Run 'docker image COMMAND --help' for more information on a command.

```

ubuntu@ip-172-31-81-98:~$ sudo docker image ls
REPOSITORY          TAG      IMAGE ID      CREATED        SIZE
scott2rikanth/fileshare docker-rdp latest   a35198658f39  2 months ago  973MB
ubuntu@ip-172-31-81-98:~$ sudo docker run -d -p 3000:3000 scott2rikanth/reactapp
i-0a66e819326a53f29 (divya)

```

PublicIP: 18.205.24.199 PrivateIP: 172.31.81.98



EXPERIMENT 8

Creation of S3 bucket and make it available with Cloud Front

1. Create S3 Bucket
2. Give Bucket Name
3. ACL should be disabled
4. **Uncheck** Block all public access
5. **Check** the box for *I acknowledge that the current settings*
6. **Create Bucket**
7. Amazon S3 → Buckets → **bucket name** (give your bucket name here)
8. Choose Properties → Edit Static website hosting
9. **Enable static website hosting**
10. Enter index.html for Name of Index Document
11. Save Changes
12. Upload the Files **index.html**
13. Copy the URL
14. Test the URL
15. Create basic HTML page with body and head
16. Create Cloud front Distribution

The screenshot shows the AWS CloudFront Distributions page. The left sidebar has a 'CloudFront' tab selected, along with links for 'Distributions', 'Policies', 'Functions', 'What's new', 'Telemetry', 'Monitoring', 'Alarms', 'Logs', 'Reports & analytics', 'Cache statistics', 'Popular objects', 'Top referrers', 'Usage', and 'Viewers'. The main content area is titled 'CloudFront > Distributions' and shows a table of distributions. The table has columns for 'ID', 'Description', 'Type', and 'Domain name'. There are two entries: one with ID 'E2F4V2XK2QE06F' and domain 'd1zp4pdskmiff.cloudfront.net', and another with ID 'E16MA043ID6LJX' and domain 'd2j2p8uposkj7b.cloudfront.net'. A 'Create distribution' button is at the top right of the table.

ID	Description	Type	Domain name
E2F4V2XK2QE06F	-	Production	d1zp4pdskmiff.cloudfront.net
E16MA043ID6LJX	-	Production	d2j2p8uposkj7b.cloudfront.net

The screenshot shows the 'Create distribution' wizard in the AWS CloudFront Management Console. On the 'Origin' configuration page, the 'Origin domain' field contains 'buck4cfs3.ap-south-1.amazonaws.com'. A warning message states: 'This S3 bucket has static web hosting enabled. If you plan to use this distribution as a website, we recommend using the S3 website endpoint rather than the bucket endpoint.' Below this, there is a 'Use website endpoint' button. The 'Origin path - optional' field is empty. The status bar at the bottom indicates 'Feedback Language Type here to search' and shows system information like '22°C' and '10:48 PM 3/21/2023'.

This screenshot shows the same 'Create distribution' wizard, but now the 'Name' field under 'Origin' contains 'buck4cfs3-website.ap-south-1.amazonaws.com'. The rest of the configuration remains the same as the previous screenshot. The status bar at the bottom indicates 'Feedback Language Type here to search' and shows '22°C' and '11:01 PM 3/21/2023'.

This screenshot shows the 'HTTP/S' configuration step in the 'Create distribution' wizard. It includes sections for 'Default root object - optional' (empty), 'Standard logging' (with 'Off' selected), 'IPv6' (with 'On' selected), and a 'Description - optional' field (empty). At the bottom right are 'Cancel' and 'Create distribution' buttons. The status bar at the bottom indicates 'Feedback Language Type here to search' and shows '22°C' and '10:52 PM 3/21/2023'.

The screenshot shows the AWS CloudFront Management Console. A green success message at the top states "Successfully created new distribution." Below it, the distribution details for "E2Q81ZNG29DNQB" are displayed. The "General" tab is selected. Key information includes:

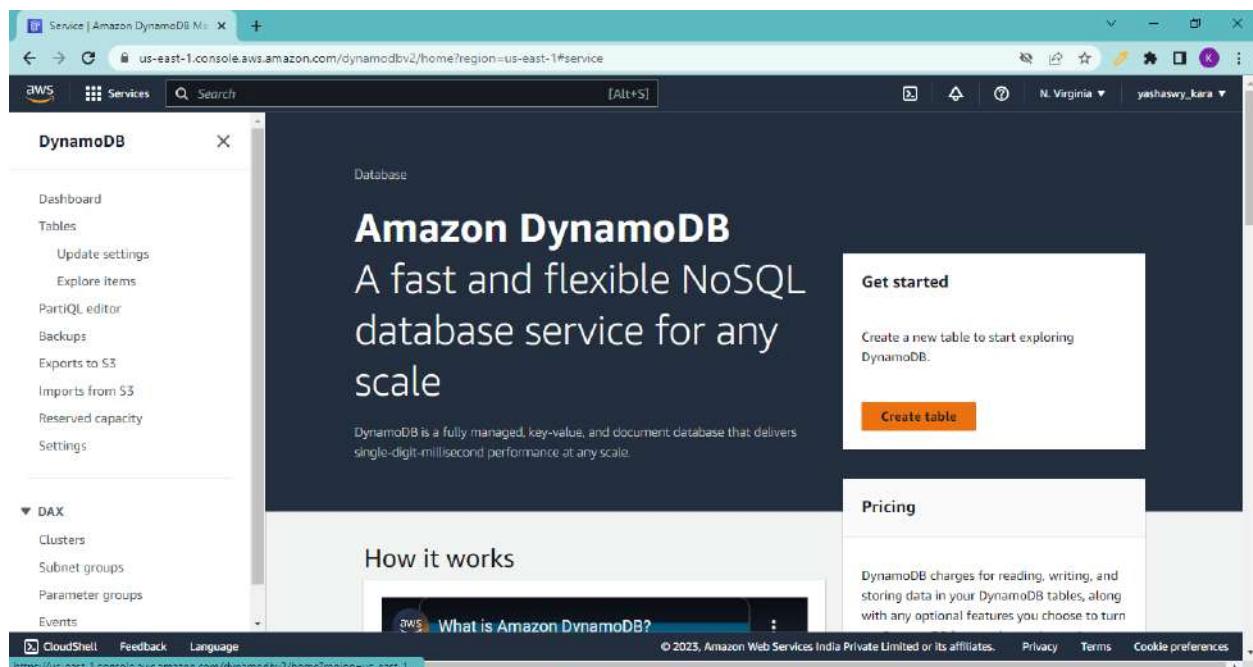
- Distribution domain name: drat4eqsc14uz.cloudfront.net
- ARN: arn:aws:cloudfront::038211148739:distribution/E2Q81ZNG29DNQB
- Last modified: Deploying

The "Settings" tab is also visible, showing options for Description, Alternate domain names, and Standard logging.

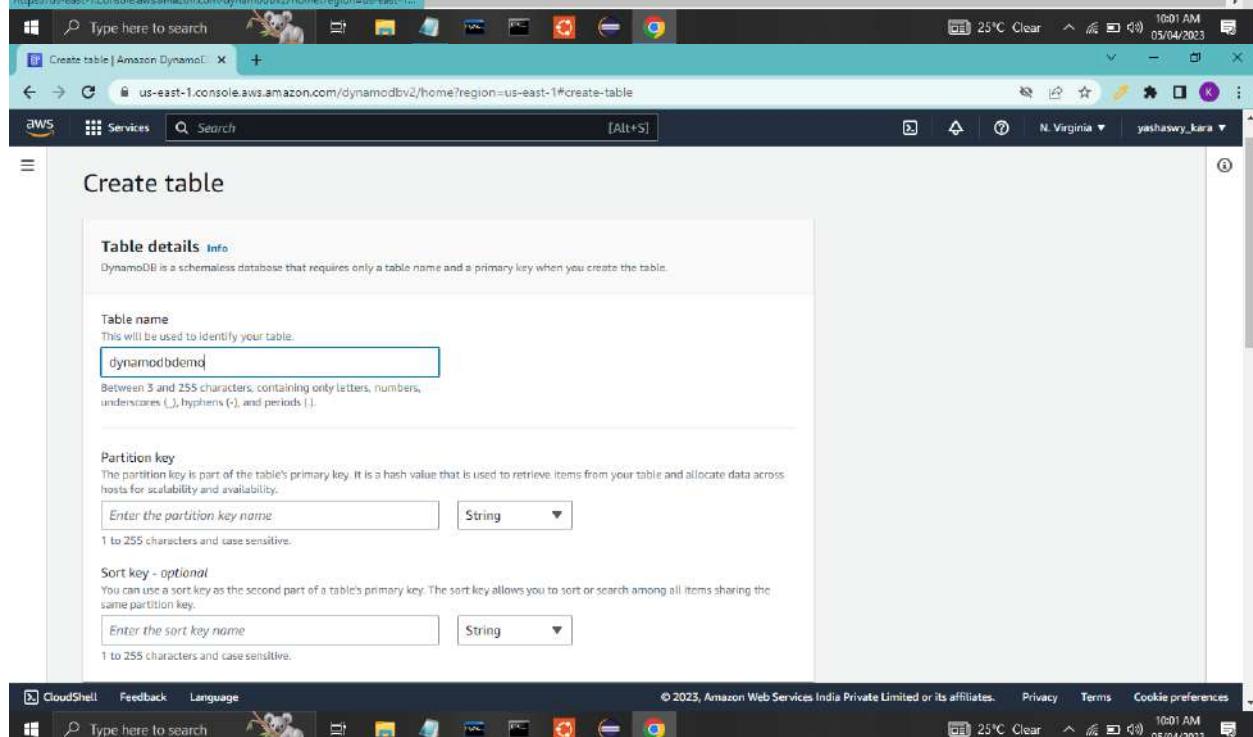


EXPERIMENT 9

Creation of Dynamo DB



The screenshot shows the Amazon DynamoDB console homepage. The main heading is "Amazon DynamoDB: A fast and flexible NoSQL database service for any scale". Below it, a sub-section titled "How it works" is visible. On the right side, there is a "Get started" box with a "Create table" button. The left sidebar contains links for Dashboard, Tables, Update settings, Explore items, PartiQL editor, Backups, Exports to S3, Imports from S3, Reserved capacity, and Settings. A "DAX" section is also present. The bottom of the page includes standard AWS navigation links like CloudShell, Feedback, Language, and copyright information.



The screenshot shows the "Create table" wizard. The first step, "Table details", is displayed. It asks for a "Table name" which is set to "dynamodbdbdemo". It also asks for a "Partition key" and a "Sort key - optional". Both fields have dropdown menus set to "String". Below each input field is a note about character limits and case sensitivity. The bottom of the page includes standard AWS navigation links like CloudShell, Feedback, Language, and copyright information.

Create table | Amazon DynamoDB

us-east-1.console.aws.amazon.com/dynamodbv2/home?region=us-east-1#create-table

Table details Info

DynamoDB is a schemaless database that requires only a table name and a primary key when you create the table.

Table name
 This will be used to identify your table.
 Between 3 and 255 characters, containing only letters, numbers, underscores (_), hyphens (-), and periods (.)

Partition key
 The partition key is part of the table's primary key. It is a hash value that is used to retrieve items from your table and allocate data across hosts for scalability and availability.
 String

Sort key - optional
 You can use a sort key as the second part of a table's primary key. The sort key allows you to sort or search among all items sharing the same partition key.
 String

1 to 255 characters and case sensitive.

CloudShell Feedback Language

Type here to search

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

10:02 AM 25°C Clear 05/04/2023

Create table | Amazon DynamoDB

us-east-1.console.aws.amazon.com/dynamodbv2/home?region=us-east-1#create-table

Table settings

Default settings
 The fastest way to create your table. You can modify these settings now or after your table has been created.

Customize settings
 Use these advanced features to make DynamoDB work better for your needs.

Default table settings
 These are the default settings for your new table. You can change some of these settings after creating the table.

Setting	Value	Editable after creation
Capacity mode	Provisioned	Yes
Read capacity	5 RCU	Yes
Write capacity	5 WCU	Yes
Auto scaling	On	Yes
Local secondary indexes	-	No
Global secondary indexes	-	Yes

CloudShell Feedback Language

Type here to search

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

10:03 AM 25°C Clear 05/04/2023

Create table | Amazon DynamoDB

us-east-1.console.aws.amazon.com/dynamodbv2/home?region=us-east-1#create-table

N. Virginia N. Virginia yashaswy_kara

Local secondary indexes	-	No
Global secondary indexes	-	Yes
Encryption key management	Owned by Amazon DynamoDB	Yes
Table class	DynamoDB Standard	Yes
Deletion protection - new	Off	Yes

Tags
Tags are pairs of keys and optional values, that you can assign to AWS resources. You can use tags to control access to your resources or track your AWS spending.

No tags are associated with the resource.

Add new tag
You can add 50 more tags.

Cancel Create table

List tables | Amazon DynamoDB

us-east-1.console.aws.amazon.com/dynamodbv2/home?region=us-east-1#tables

N. Virginia N. Virginia yashaswy_kara

DynamoDB

Creating the dynamodbdemo table. It will be available for use shortly.

DynamoDB > Tables

Tables (1) Info

Name	Status	Partition key	Sort key	Indexes	Deletion protection	Read capacity mode
dynamodbdemo	Creating	name (S)	subject (S)	0	Off	Provisioned with aut

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 10:03 AM 25°C Clear 05/04/2023

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 10:04 AM 25°C Clear 05/04/2023

List tables | Amazon DynamoDB

us-east-1.console.aws.amazon.com/dynamodbv2/home?region=us-east-1#tables

The dynamodbdemo table was created successfully.

DynamoDB > Tables

Tables (1) Info

Find tables by table name Any table tag

Name	Status	Partition key	Sort key	Indexes	Deletion protection	Read capacity mode
dynamodbdemo	Active	name (S)	subject (S)	0	Off	Provisioned with auto

Actions Delete Create table

Dashboard Tables Update settings Explore items PartiQL editor Backups Exports to S3 Imports from S3 Reserved capacity Settings

DAX Clusters Subnet groups Parameter groups Events

CloudShell Feedback Language

Type here to search

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

1004 AM 25°C Clear 05/04/2023

List tables | Amazon DynamoDB

us-east-1.console.aws.amazon.com/dynamodbv2/home?region=us-east-1#tables

DynamoDB > Tables

Tables (1) Info

Find tables by table name Any table tag

Name	Status	Partition key	Sort key	Indexes	Deletion protection	Read capacity mode
dynamodbdemo	Active	name (S)	subject (S)	0	Off	Provisioned with auto

Actions Delete Create table

Dashboard Tables Update settings Explore items PartiQL editor Backups Exports to S3 Imports from S3 Reserved capacity Settings

DAX Clusters Subnet groups Parameter groups Events

https://us-east-1.console.aws.amazon.com/dynamodbv2/home?region=us-east-1...

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

1004 AM 25°C Clear 05/04/2023

Screenshot of the AWS DynamoDB console showing the 'dynamodbdemo' table details.

General Information:

- Partition key: name (String)
- Sort key: subject (String)
- Capacity mode: Provisioned
- Table status: Active

Create Item Form:

Attribute name	Value	Type
name - Partition key	Empty value	String
subject - Sort key	Empty value	String

Actions:

- Form
- JSON view
- Add new attribute
- Cancel
- Create Item

Edit item | Amazon DynamoDB +

us-east-1.console.aws.amazon.com/dynamodbv2/home?region=us-east-1#edit-item?table=dynamodbdemo&route=ROUTE_ITEM_EXPLORER&itemMo...

DynamoDB Services Search [Alt+S] N. Virginia yashaswy_kara

DynamoDB > Items: dynamodbdemo > Edit item

Create item

You can add, remove, or edit the attributes of an item. You can nest attributes inside other attributes up to 32 levels deep. [Learn more](#)

Attributes		Add new attribute ▾
Attribute name	Value	Type
name - Partition key	Empty value	String
subject - Sort key	Empty value	String
marks	0	Number
Grade	Empty value	String

Cancel Create Item

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 10:06 AM 25°C Clear 05/04/2023

Edit item | Amazon DynamoDB +

us-east-1.console.aws.amazon.com/dynamodbv2/home?region=us-east-1#edit-item?table=dynamodbdemo&route=ROUTE_ITEM_EXPLORER&itemMo...

DynamoDB Services Search [Alt+S] N. Virginia yashaswy_kara

DynamoDB > Items: dynamodbdemo > Edit item

Create item

You can add, remove, or edit the attributes of an item. You can nest attributes inside other attributes up to 32 levels deep. [Learn more](#)

Attributes		Add new attribute ▾
Attribute name	Value	Type
name - Partition key	A	String
subject - Sort key	CC	String
marks	99	Number
Grade	A	String

Cancel Create Item

Items | Amazon DynamoDB Main +

us-east-1.console.aws.amazon.com/dynamodbv2/home?region=us-east-1#item-explorer?table=dynamodbdemo

DynamoDB dynamodbdemo

Select a table or index: Table - dynamodbdemo

Select attribute projection: All attributes

Filters

Run Reset

Completed. Read capacity units consumed: 0.5

Items returned (1)

	name	subject	Grade	marks
<input type="checkbox"/>	A	CC	A	99

https://us-east-1.console.aws.amazon.com/dynamodbv2/home?region=us-east-1...

Type here to search

Edit item | Amazon DynamoDB +

us-east-1.console.aws.amazon.com/dynamodbv2/home?region=us-east-1#edit-item?table=dynamodbdemo&route=ROUTE_ITEM_EXPLORER&itemMo...

DynamoDB Services Search [Alt+S]

Items: dynamodbdemo > Edit item

Create item

You can add, remove, or edit the attributes of an item. You can nest attributes inside other attributes up to 32 levels deep. Learn more ↗

Attributes

Attribute name	Value	Type	Action
name - Partition key	B	String	Remove
subject - Sort key	FEWD	String	Remove
marks	100	Number	Remove
Grade	A	String	Remove

Add new attribute ▾

Cancel Create Item

CloudShell Feedback Language

Type here to search

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

10:07 AM 25°C Clear 05/04/2023

Items | Amazon DynamoDB Main + us-east-1.console.aws.amazon.com/dynamodbv2/home?region=us-east-1#item-explorer?table=dynamodbdemo

N. Virginia N. Virginia yashaswy_kara

DynamoDB

Dashboard

Tables

Update settings

Explore items

PartiQL editor

Backups

Exports to S3

Imports from S3

Reserved capacity

Settings

DAX

Clusters

Subnet groups

Parameter groups

Events

Table - dynamodbdemo All attributes

Filters

Run Reset

Completed. Read capacity units consumed: 0.5

Items returned (2)

	name	subject	Grade	marks
<input type="checkbox"/>	B	FEWD	A	100
<input type="checkbox"/>	A	CC	A	99

CloudShell Feedback Language Type here to search © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 10:08 AM 25°C Clear 05/04/2023

Items | Amazon DynamoDB Main + us-east-1.console.aws.amazon.com/dynamodbv2/home?region=us-east-1#item-explorer?table=dynamodbdemo

N. Virginia N. Virginia yashaswy_kara

DynamoDB

Dashboard

Tables

Update settings

Explore items

PartiQL editor

Backups

Exports to S3

Imports from S3

Reserved capacity

Settings

DAX

Clusters

Subnet groups

Parameter groups

Events

DynamoDB > Items > dynamodbdemo

Tables (1) dynamodbdemo

Any table tag Find tables by table name

dynamodbdemo

Autopreview View table details

Scan or query items

Scan Query

Select a table or index Table - dynamodbdemo Select attribute projection All attributes

name (Partition key) Enter partition key value

subject (Sort key) Equal to Enter sort key value Sort descending

Filters

The item has been saved successfully.

CloudShell Feedback Language Type here to search © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 10:08 AM 25°C Clear 05/04/2023

The image consists of three vertically stacked screenshots of the AWS DynamoDB console. Each screenshot shows the 'Scan or query items' interface for a table named 'dynamodbdemo'. The interface includes fields for selecting a table (set to 'Table - dynamodbdemo'), choosing an attribute projection ('All attributes'), and defining a query. In the first two screenshots, the 'Query' tab is selected, while in the third, the 'Scan' tab is selected. The results pane shows a single item with the partition key 'B' and sort key 'Enter sort key value'. The left sidebar of the console is visible in all three frames.

The image consists of three vertically stacked screenshots of the AWS DynamoDB console, illustrating the creation and execution of a scan operation on a table named `dynamodbdemo`.

Screenshot 1: Table Overview

This screenshot shows the `DynamoDB > Tables` page. A table named `dynamodbdemo` is listed, showing its status as `Active`, partition key as `name (S)`, sort key as `subject (S)`, and deletion protection set to `Off`. The table is provisioned with auto scaling.

Name	Status	Partition key	Sort key	Indexes	Deletion protection	Read capacity mode
<code>dynamodbdemo</code>	<code>Active</code>	<code>name (S)</code>	<code>subject (S)</code>	0	<code>Off</code>	<code>Provisioned with auto</code>

Screenshot 2: Item Creation Confirmation

This screenshot shows the `DynamoDB > Items > dynamodbdemo` page. A success message indicates that an item has been saved successfully. The table `dynamodbdemo` is selected for scanning.

Screenshot 3: Scan Execution Result

This screenshot shows the results of a scan operation on the `dynamodbdemo` table. The results indicate that 0.5 read capacity units were consumed. The table selection dropdown shows `Table - dynamodbdemo` and the attribute projection dropdown shows `All attributes`.

The screenshot shows the AWS DynamoDB console. On the left, a sidebar menu for 'DynamoDB' includes options like Dashboard, Tables, Update settings, Explore items, PartiQL editor, Backups, Exports to S3, Imports from S3, Reserved capacity, and Settings. Under 'Tables', there is a table listing with one item:

Name	Status	Partition key	Sort key	Indexes	Deletion protection	Read capacity mode
dynamodbdemo	Active	name (S)	subject (S)	0	Off	Provisioned with auto

The screenshot shows the 'Delete table' confirmation dialog. It asks if you want to permanently delete the 'dynamodbdemo' table in US East (N. Virginia). The dialog includes a warning message, two checkboxes for CloudWatch alarms and on-demand backups, and a text input field for confirmation.

Delete table **dynamodbdemo** in US East (N. Virginia) permanently? This action cannot be undone.

⚠ Proceeding with this action will delete the table and you won't be able to retrieve this data.

Delete all CloudWatch alarms for **dynamodbdemo**.

Create an on-demand backup of **dynamodbdemo** before deletion.
You can create an on-demand backup of your table for long-term retention and data archiving. You can then use this backup to restore your data to its exact state before table deletion. Additional charges apply for on-demand backup and restore. For more information see [Pricing](#).

To avoid unintentional deletions, we ask you to provide additional confirmation.

Enter "confirm" to agree.

confirm

Cancel Delete

The screenshot shows two consecutive screenshots of the AWS DynamoDB console.

Screenshot 1: Delete table Confirmation Dialog

A modal dialog titled "Delete table" is displayed. It asks, "Delete table dynamodbdemo in US East (N. Virginia) permanently? This action cannot be undone." Below this is a warning message: "Proceeding with this action will delete the table and you won't be able to retrieve this data." There are two checkboxes: one checked ("Delete all CloudWatch alarms for dynamodbdemo") and one unchecked ("Create an on-demand backup of dynamodbdemo before deletion"). A note explains that backups can be used for restore. A text field prompts the user to "Enter 'confirm' to agree." The "Delete" button is highlighted in orange.

Screenshot 2: Successful Deletion Confirmation

The main DynamoDB dashboard shows a success message: "The request to delete the 'dynamodbdemo' table has been submitted successfully." The "Tables" section shows "Tables (0)" and a message: "You have no tables in this account in this AWS Region." The "Create table" button is visible.

EXPERIMENT 10

Create image recognition capability application using AWS Amazon Recognition

The screenshot shows two browser windows. The top window displays the AWS search results for 'iam'. It lists several services under 'Services' and 'Features'. The 'IAM' service is highlighted, showing its description: 'Manage access to AWS resources'. Below it are other services like 'IAM Identity Center', 'Resource Access Manager', and 'Serverless Application Repository'. The bottom window shows the 'Roles' page in the IAM Management Console. It lists five existing roles, each with a checkbox, role name, trusted entity, and last updated date. A 'Create role' button is visible at the top right. A 'Roles Anywhere' section is also present.

Role name	Trusted entities	Last updated
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS Service: dynamodb application-autoscaling (Service-Linked Role)	54 days ago
AWSServiceRoleForLexV2Bots_3RXWR95B94V	AWS Service: lexv2 (Service-Linked Role)	-
AWSServiceRoleForLexV2Bots_4VVM9CZLA06	AWS Service: lexv2 (Service-Linked Role)	-
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-

IAM Management Console us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles/create?step=selectEntities

Services Search [Alt+S]

IAM > Roles > Create role

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

Select trusted entity Info

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 Creates 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.

Common use cases

- EC2 Allows EC2 instances to call AWS services on your behalf.

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 10:19 AM 25°C Clear 05/04/2023

IAM Management Console us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles/create?step=selectEntities

Services Search [Alt+S]

Step 3 Name, review, and create

Select trusted entity Info

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 Creates 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.

Common use cases

- EC2 Allows EC2 instances to call AWS services on your behalf.
- Lambda Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

Choose a service to view use case

Cancel Next

IAM Management Console us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles/create?commonUseCase=Lambda&step=addPermission&trustedEntityType=AWS_... Global yashaswy_kara

Add permissions Step 1 Select trusted entity Step 2 Add permissions Step 3 Name, review, and create

Permissions policies (843) Choose one or more policies to attach to your new role.

Policy name	Type	Description
AdministratorAccess	AWS managed policy	Provides full access to AWS services and resources.
PowerUserAccess	AWS managed policy	Provides full access to AWS services and resources, but does not allow management of other users.
ReadOnlyAccess	AWS managed policy	Provides read-only access to AWS services and resources.
AWSCloudFormationFullAccess	AWS managed policy	Provides access to AWS CloudFormation via the AWS Management Console and AWS CLI.
CloudFrontFullAccess	AWS managed policy	Provides full access to the CloudFront console plus the ability to list Amazon CloudFront distributions.
AWSCloudHSMFullAccess	AWS managed policy	Provides full access to all CloudHSM resources.
AWSCloudHSMReadOnlyAccess	AWS managed policy	Provides read only access to all CloudHSM resources.
ResourceGroupsFullAccess	AWS managed policy	Provides full access to Resource Groups and Tag Editor.

CloudShell Feedback Language Type here to search IAM Management Console us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles/create?commonUseCase=Lambda&step=addPermission&trustedEntityType=AWS_... Global yashaswy_kara

IAM > Roles > Create role Step 1 Select trusted entity Step 2 Add permissions Step 3 Name, review, and create

Add permissions Step 1 Select trusted entity Step 2 Add permissions Step 3 Name, review, and create

Permissions policies (843) Choose one or more policies to attach to your new role.

Policy name	Type	Description
AWSLambdaExecute	AWS managed policy	Provides Put, Get access to S3 and full access to CloudWatch Logs.

Set permissions boundary - optional Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Cancel Previous Next

IAM Management Console

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles/create?commonUseCase=Lambda&step=addPermission&trustedEntityType=AWS_...

Services Search [Alt+S]

IAM > Roles > Create role

Step 1: Select trusted entity

Step 2: Add permissions

Step 3: Name, review, and create

Add permissions Info

Permissions policies (Selected 1/843) Info
Choose one or more policies to attach to your new role.

Filter policies by property or policy name and press enter. 1 match < 1 > Clear filters

"AwsLambdaExecute" X

Policy name	Type	Description
AWSLambdaExecute	AWS m...	Provides Put, Get access to S3 and full access to CloudWatch Logs.

Set permissions boundary - optional Info
Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Cancel Previous Next

CloudShell Feedback Language

Type here to search

IAM Management Console

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles/create?commonUseCase=Lambda&step=addPermission&trustedEntityType=AWS_...

Services Search [Alt+S]

IAM > Roles > Create role

Step 1: Select trusted entity

Step 2: Add permissions

Step 3: Name, review, and create

Add permissions Info

Permissions policies (Selected 2/843) Info
Choose one or more policies to attach to your new role.

Filter policies by property or policy name and press enter. 1 match < 1 > Clear filters

"AmazonRekognitionFullAccess" X

Policy name	Type	Description
AmazonRekognition...	AWS m...	Access to all Amazon Rekognition APIs

Set permissions boundary - optional Info
Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Cancel Previous Next

IAM Management Console us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles/create?commonUseCase=Lambda&step=addPermission&trustedEntityType=AWS_... Global yashaswy_kara

IAM > Roles > Create role

Step 1: Select trusted entity

Step 2: Add permissions

Step 3: Name, review, and create

Add permissions Info

Permissions policies (Selected 3/843) Info
Choose one or more policies to attach to your new role.

Filter policies by property or policy name and press enter. 1 match < 1 > Clear filters

s3fullaccess Policy name Type Description

 AmazonS3FullAccess AWS m... Provides full access to all buckets via the AWS Management Console.

Set permissions boundary - optional Info
Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 10:26 AM 25°C Clear 05/04/2023

IAM Management Console us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles/create?commonUseCase=Lambda&policies=arn%3Aaws%3Aiam%3Aaws%3A... Global yashaswy_kara

IAM > Roles > Create role

Step 1: Select trusted entity

Step 2: Add permissions

Step 3: Name, review, and create

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.
Allows Lambda functions to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and "+-, @-, _" characters.

Step 1: Select trusted entities Edit

```
1 * [ ]  
2 "Version": "2012-10-17",
```

IAM Management Console

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles/create?commonUseCase=Lambda&policies=am%3Aaws%3Aiam%3Aaws%3A...

Services Search [Alt+S]

Name, review, and create

Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

Role details

Role name Enter a meaningful name to identify this role
sampled

Description Add a short explanation for this role.
Allows Lambda functions to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '-' characters.

Step 1: Select trusted entities Edit

```
1+ {
2+   "Version": "2012-10-17",
3+   "Statement": [
4+     {
5+       "Effect": "Allow",
6+       "Action": [
7+         "sts:AssumeRole"

```

CloudShell Feedback Language

Type here to search

IAM Management Console

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles/create?commonUseCase=Lambda&policies=am%3Aaws%3Aiam%3Aaws%3A...

Services Search [Alt+S]

Permissions policy summary

Policy name	Type	Attached as
AmazonS3FullAccess	AWS managed	Permissions policy
AmazonRekognitionFullAccess	AWS managed	Permissions policy
AWSLambdaExecute	AWS managed	Permissions policy

Tags

Add tags - optional Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add tag

You can add up to 50 more tags.

Cancel Previous Create role

The screenshot shows the AWS IAM Management Console. The left sidebar is titled "Identity and Access Management (IAM)" and includes sections for Dashboard, User groups, Users, Roles (selected), Policies, Identity providers, and Account settings. The main content area is titled "Roles (6) Info" and contains a table of roles:

Role name	Trusted entities	Last updated
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS Service: dynamodb.application-autoscaling (Service-Linked Role)	54 days ago
AWSServiceRoleForLexV2Bots_3RXWR95B84V	AWS Service: lexv2 (Service-Linked Role)	-
AWSServiceRoleForLexV2Bots_4VVM9CZLA06	AWS Service: lexv2 (Service-Linked Role)	-
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
sample	AWS Service: lambda	-

At the top right of the main content area, there are "View role" and "Create role" buttons.

The screenshot shows the AWS S3 Management Console. The left sidebar is titled "Storage" and lists "Amazon S3". The main content area has a large heading "Amazon S3" and sub-headline "Store and retrieve any amount of data from anywhere". Below this, a paragraph explains that Amazon S3 is an object storage service. On the right, there is a "Create a bucket" section with a "Create bucket" button. At the bottom, there is a "Pricing" section with information about costs and a link to the AWS Simple Monthly Calculator.

The screenshot shows the AWS S3 Bucket creation interface. In the 'General configuration' section, the bucket name is set to 'csee1'. The AWS Region is selected as 'US East (N. Virginia) us-east-1'. Under 'Object Ownership', 'ACLs enabled' is selected, and a note states: 'Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.' A warning message below advises against enabling ACLs unless needed for individual object access or sharing with external users. The 'Bucket owner preferred' option is selected under 'Object Ownership'.

General configuration

Bucket name: csee1

AWS Region: US East (N. Virginia) us-east-1

Object Ownership

ACLs disabled (recommended)

ACLs enabled

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

Bucket owner preferred

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

Object writer

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

S3 bucket x +

s3.console.aws.amazon.com/s3/bucket/create?region=us-east-1

Block Public Access settings for this bucket

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 this bucket and its 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 this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

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

- Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning
 Disable
 Enable

Tags (0) - optional

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 10:32 AM 25°C Clear 05/04/2023

The image consists of three vertically stacked screenshots of the AWS S3 Bucket creation interface.

Screenshot 1: Bucket Versioning

Bucket Versioning:

- Disable
- Enable

Tags (0) - optional

You can use bucket tags to track storage costs and organize buckets. Learn more [\[Link\]](#)

No tags associated with this bucket.

[Add tag](#)

Default encryption [Info](#)

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

Encryption key type [Info](#)

- Amazon S3 managed keys (SSE-S3)
- AWS Key Management Service key (SSE-KMS)

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS.

[Learn more \[Link\]](#)

- 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](#)

Screenshot 2: Default encryption

Default encryption [Info](#)

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

Encryption key type [Info](#)

- Amazon S3 managed keys (SSE-S3)
- AWS Key Management Service key (SSE-KMS)

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS.

[Learn more \[Link\]](#)

- 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](#)

Screenshot 3: Summary Step

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

[Cancel](#) [Create bucket](#)

The screenshot shows the AWS S3 console interface for the 'csee1' bucket. The left sidebar includes links for Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings for this account, Storage Lens, Dashboards, AWS Organizations settings, and Feature spotlight.

The main content area displays the 'Permissions overview' section, which states that objects can be public. Below this is the 'Block public access (bucket settings)' section, which is currently set to 'Bucket owner preferred'. A note indicates that if new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner; otherwise, they are owned by the object writer.

At the bottom, there is an 'Access control list (ACL)' section with a note about combined access grants for duplicate grantees. It lists one grantee: 'Bucket owner (your AWS account)' with Canonical ID e028143a24b478708fd05db49573dbdf256177daa3ea2a75e1053eb4446278, having 'List, Write' permissions under 'Bucket ACL'.

The image consists of three vertically stacked screenshots of the AWS S3 'Edit access control list (ACL)' page. Each screenshot shows a different configuration of grants for a bucket named 'csee1'.

Screenshot 1 (Top): Shows grants for 'Bucket owner (your AWS account)', 'Everyone (public access)', and 'Authenticated users group'. The 'Bucket owner' has 'List', 'Read', and 'Write' permissions. 'Everyone' has 'List' and 'Read' permissions. 'Authenticated users group' has 'Read' and 'Write' permissions.

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account)	<input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access)	<input checked="" type="checkbox"/> List <input type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write
Authenticated users group (anyone with an AWS account)	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write

Screenshot 2 (Middle): Shows grants for 'Bucket owner (your AWS account)' and 'S3 log delivery group'. The 'Bucket owner' has 'List', 'Read', and 'Write' permissions. The 'S3 log delivery group' has 'List' and 'Write' permissions.

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account)	<input type="checkbox"/> List <input type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
S3 log delivery group	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write

Screenshot 3 (Bottom): Shows grants for 'Bucket owner (your AWS account)'. The 'Bucket owner' has 'List', 'Read', and 'Write' permissions.

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account)	<input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write

A warning message in the middle screenshot states: "⚠️ When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access the objects in this bucket." A checkbox below it says "I understand the effects of these changes on my objects and buckets."

The image consists of three vertically stacked screenshots of the AWS S3 console, illustrating the management of a bucket named 'csee1'.

Screenshot 1: Bucket Permissions

This screenshot shows the 'Permissions' tab for the 'csee1' bucket. It indicates that the bucket is 'Publicly accessible'. The 'Access' section shows a red warning icon next to 'Public'. Below this, the 'Block public access (bucket settings)' section is visible, containing a note about granting public access through ACLs, policies, or access points. A link to learn more is provided.

Screenshot 2: Object Management

This screenshot shows the 'Objects' tab for the 'csee1' bucket. It displays a table with one row: 'No objects'. A large orange 'Upload' button is prominently displayed at the top of the list.

Screenshot 3: Object Details

This screenshot shows a detailed view of an object within the 'csee1' bucket. The object name is 'index.html'. It shows the object's type as 'File', size as '0 B', and storage class as 'Standard'. The 'Actions' dropdown menu is open, showing options like 'Edit', 'Delete', and 'Copy'.

The image shows two screenshots of the AWS Management Console.

The top screenshot displays the "Bucket policy" section for the "csee1" bucket. It shows a message stating "No policy to display." with a "Copy" button. There are "Edit" and "Delete" buttons at the top of the policy area.

The bottom screenshot shows the "Upload" page for the "csee1" bucket. It includes a search bar, navigation links for CloudShell, Feedback, Language, Privacy, Terms, and Cookie preferences, and a status bar showing 25°C Clear, 10:33 AM, and 05/04/2023. The main area has a heading "Upload" with a "Info" link, instructions about file upload limits, and a large dashed box for dragging files. Below this is a table titled "Files and folders (0)" with columns for Name, Folder, Type, and Size. A search bar and pagination controls are also present. A message at the bottom states "No files or folders." and "You have not chosen any files or folders to upload."

S3 Management Console

s3.console.aws.amazon.com/s3/upload/csee1?region=us-east-1

Services Search [Alt+S]

Amazon S3 > Buckets > csee1 > Upload

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 [\[Link\]](#)

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

Files and folders (1 Total, 41.5 KB)
All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	WhatsApp Image 2023-03-01 at 12.02.16 (1).jpeg	-	image/jpeg	41.5 KB

Destination

Destination URL: <s3://csee1>

Destination details
Bucket settings that impact new objects stored in the specified destination.

Permissions
Grant public access and access to other AWS accounts.

Properties
Specify storage class, encryption settings, tags, and more.

Cancel **Upload**

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 10:34 AM 25°C Clear 05/04/2023

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 10:34 AM 25°C Clear 05/04/2023

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 10:34 AM 25°C Clear 05/04/2023

S3 Management Console

s3.console.aws.amazon.com/s3/upload/csee1?region=us-east-1

Upload succeeded

View details below.

Upload: status

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

Summary	
Destination	Succeeded s3://csee1 1 file, 41.5 KB (100.00%)
Failed	0 files, 0 B (0%)

Files and folders Configuration

Files and folders (1 Total, 41.5 KB)

Find by name

Name	Folder	Type	Size	Status	Error
WhatsApp Image 2023-03-01 at 12.02.16 (1).jpeg	-	image/jpeg	41.5 KB	Succeeded	-

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 10:34 AM 25°C Clear 05/04/2023

S3 Management Console

s3.console.aws.amazon.com/s3/upload/csee1?region=us-east-1

Upload succeeded

View details below.

Upload: status

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

Summary	
Destination	Succeeded s3://csee1 1 file, 41.5 KB (100.00%)
Failed	0 files, 0 B (0%)

Files and folders Configuration

Files and folders (1 Total, 41.5 KB)

Find by name

Name	Folder	Type	Size	Status	Error
WhatsApp Image 2023-03-01 at 12.02.16 (1).jpeg	-	image/jpeg	41.5 KB	Succeeded	-

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 10:35 AM 25°C Clear 05/04/2023

S3 Management Console

s3.console.aws.amazon.com/s3/upload/csee1?region=us-east-1

Services Lambda

Upload

Services (7)

Features (2)

Resources New

Blogs (959)

Documentation (7,182)

Knowledge Articles (16)

Tutorials (6)

Events (13)

Marketplace (460)

Summary

Destination s3://csee1

Files and F

Find by name

Search results for 'lambda'

Services

See all 7 results ▾

Lambda Run code without thinking about servers

CodeBuild Build and Test Code

AWS Signer Ensuring trust and integrity of your code

Amazon Inspector Continual vulnerability management at scale

Features

Local processing IoT Core feature

Close

This screenshot shows the AWS S3 Management Console interface. A message at the top indicates a successful upload to a Lambda function. The search bar has 'lambda' typed into it. Below the search bar, there's a list of services, with 'Lambda' being the first item. To the right of the Lambda entry is a green rectangular box containing the text 'Run code without thinking about servers'. Other services listed include CodeBuild, AWS Signer, and Amazon Inspector. Below the service list, there's a section titled 'Features' with a single item: 'Local processing' under the 'IoT Core feature' category.

https://us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1

Type here to search

Dashboard - Lambda

us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#discover

AWS Lambda

Services

Search

[Alt+S]

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

23°C Clear 10:35 AM 05/04/2023

AWS Lambda

Dashboard

Applications

Functions

Additional resources

Code signing configurations

Layers

Replicas

Related AWS resources

Step Functions state machines

Resources for US East (N. Virginia)

Create function

Lambda function(s) 0

Code storage 0 byte (0% of 75.0 GB)

Full account concurrency 10

Unreserved account concurrency 10

Account-level metrics

The charts below show metrics across all your Lambda functions in this AWS Region.

Error count and success rate (%)

1h 3h 12h 1d 3d 1w Custom

Waiting for miquoddy@execute-api.us-east-1.amazonaws.com...

Type here to search

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

23°C Clear 10:35 AM 05/04/2023

This screenshot shows the AWS Lambda dashboard for the US East (N. Virginia) region. On the left, there's a sidebar with links for Dashboard, Applications, Functions, Additional resources, Related AWS resources, and Step Functions state machines. The main area displays 'Resources for US East (N. Virginia)' with a summary table. The table shows 0 Lambda functions, 0 bytes of code storage (0% of the 75.0 GB limit), and 10 units of both full account concurrency and unreserved account concurrency. Below this, there's a section titled 'Account-level metrics' featuring three line charts for 'Error count and success rate (%)'. At the bottom of the page, there's a status bar with the text 'Waiting for miquoddy@execute-api.us-east-1.amazonaws.com...'.

Create function [Info](#)

AWS Serverless Application Repository applications have moved to [Create application](#).

Author from scratch
Start with a simple Hello World example.

Use a blueprint
Build a Lambda application from sample code and configuration presets for common use cases.

Container image
Select a container image to deploy for your function.

Basic information

Function name
Enter a name that describes the purpose of your function.

Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime [Info](#)
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.

Architecture [Info](#)
Choose the instruction set architecture you want for your function code.
 x86_64

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 10:35 AM 25°C Clear 05/04/2023

Type here to search

Create function - Lambda [Info](#)

us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/create/function

Services Search [Alt+S]

N. Virginia yashaswy_kara

Basic information

Java 8 on Amazon Linux 2

Node.js 12.x

Node.js 14.x

Node.js 16.x

Python 3.7

Python 3.8

Python 3.9

Custom runtime

Use default bootstrap on Amazon Linux 1

Provide your own bootstrap on Amazon Linux 2

Container image
a container image to deploy for your function.

Architecture [Info](#)
Choose the instruction set architecture you want for your function code.
 x86_64
 arm64

Permissions [Info](#)
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

The screenshot shows the 'Create Function' wizard in the AWS Lambda console. The 'Basic information' step is selected. The function name is set to 'lambda'. The runtime is chosen as 'Python 3.7'. The architecture is set to 'x86_64'. Under permissions, it is noted that Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs.

Basic information

Function name
Enter a name that describes the purpose of your function.

Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime [Info](#)
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.

Architecture [Info](#)
Choose the instruction set architecture you want for your function code.
 x86_64
 arm64

Permissions [Info](#)
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

The screenshot shows the 'Create function' wizard continuing through the steps. It has passed the 'Basic information' and 'Permissions' steps and is now at the 'Advanced settings' step. The 'Execution role' section shows 'sample' selected. At the bottom, there are 'Cancel' and 'Create function' buttons.

Advanced settings

Execution role
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.

Create function

The screenshot shows the AWS Lambda console. At the top, a green banner says "Successfully created the function lambda. You can now change its code and configuration. To invoke your function with a test event, choose 'Test'." Below this, the function name "lambda" is displayed. On the left, there's a sidebar with "Lambda > Functions > lambda". On the right, there are buttons for "Throttle", "Copy ARN", and "Actions". Under "Function overview", there's a section for triggers and destinations. A large button at the bottom left says "+ Add trigger" and another at the bottom right says "+ Add destination". To the right of these buttons are sections for "Description", "Last modified", "Function ARN", and "Function URL".

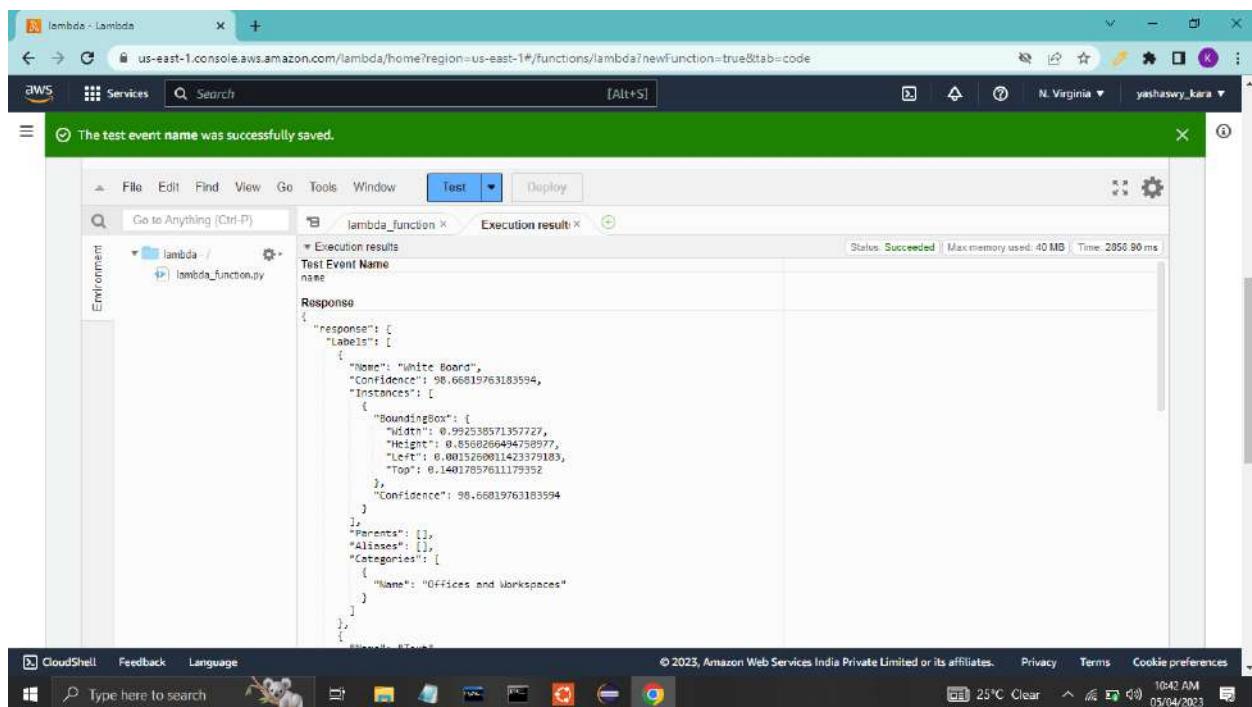
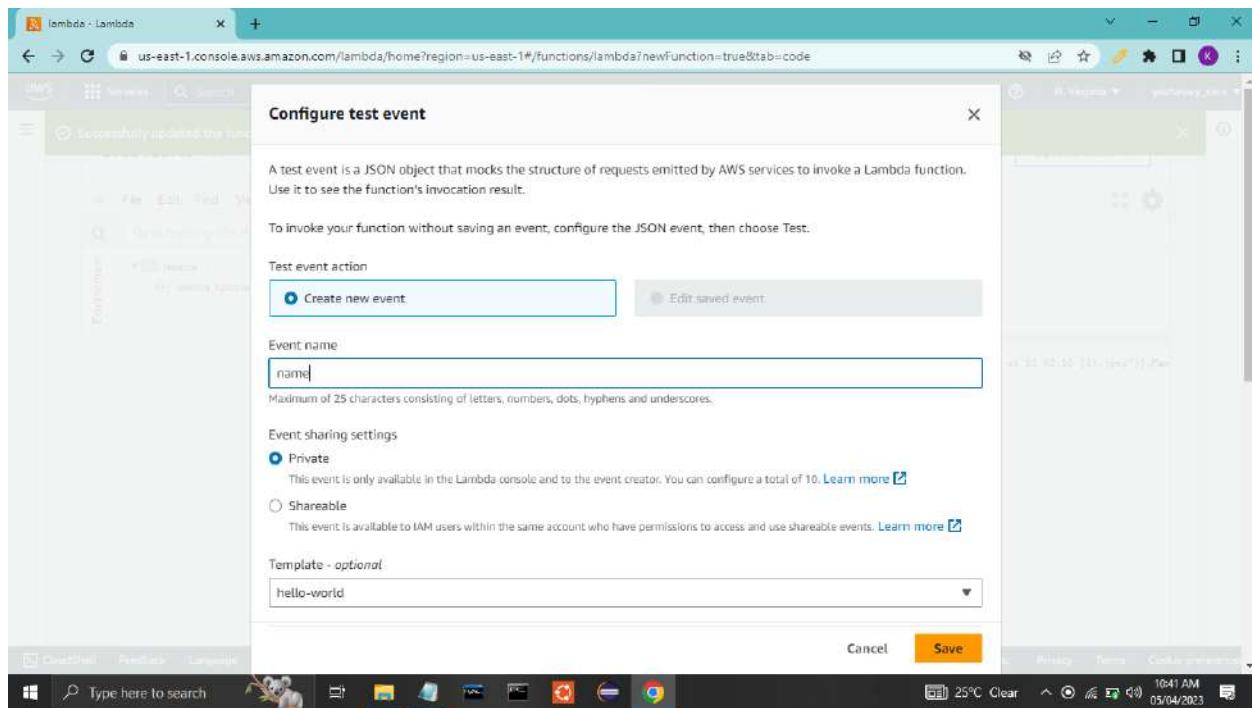
The screenshot shows the "Code" tab of the Lambda function configuration. At the top, a green banner says "Successfully created the function lambda. You can now change its code and configuration. To invoke your function with a test event, choose 'Test'." Below this, there are tabs for "Code", "Test", "Monitor", "Configuration", "Aliases", and "Versions". The "Code" tab is selected. In the main area, there's a "Code source" section with an "Upload from" button. Below it, a large Lambda logo is shown with the text "Loading your function..." underneath.

The screenshot shows the AWS Lambda function editor. The code source tab is selected, displaying the following Python code:

```
1 import json
2 import boto3
3
4 def lambda_handler(event,context):
5     client = boto3.client("rekognition")
6     s3=boto3.client("s3")
7     fileObj = s3.get_object(Bucket = "cseel", Key="WhatsApp Image 2023-03-01 at 12.01.16 (1).jpeg")
8     file_content=fileObj["Body"].read()
9     response = client.detect_labels(Image= {"S3Object": {"Bucket": "cseel", "Name": "WhatsApp Image 2023-03-01 at 12.02.16 (1).jpeg"}},MaxResults=10)
10    print(response)
11    return {
12        'response': response,
13        'statusCode':200,
14        'body':json.dumps('Hello From Lambda')
15    }
16
```

The screenshot shows the AWS Lambda function editor. The code source tab is selected, displaying the same Python code as the previous screenshot:

```
1 import json
2 import boto3
3
4 def lambda_handler(event,context):
5     client = boto3.client("rekognition")
6     s3=boto3.client("s3")
7     fileObj = s3.get_object(Bucket = "cseel", Key="WhatsApp Image 2023-03-01 at 12.01.16 (1).jpeg")
8     file_content=fileObj["Body"].read()
9     response = client.detect_labels(Image= {"S3Object": {"Bucket": "cseel", "Name": "WhatsApp Image 2023-03-01 at 12.02.16 (1).jpeg"}},MaxResults=10)
10    print(response)
11    return {
12        'response': response,
13        'statusCode':200,
14        'body':json.dumps('Hello From Lambda')
15    }
16
```



The screenshot shows the AWS Lambda Functions page. At the top, there's a search bar and a navigation bar with 'Services' and 'Search'. The main area displays a table titled 'Functions (1/1)'. The table has columns for 'Function name', 'Description', 'Package type', 'Runtime', and 'Last modified'. A single row is shown for a function named 'lambda', which is packaged as a Zip file and runs on Python 3.7. The 'Last modified' column shows '10 minutes ago'. To the right of the table, there's a sidebar titled 'Lambda functions' with instructions on how to filter and perform actions on functions. At the bottom, there's a status bar with 'CloudShell', 'Feedback', 'Language', and a search bar.

This screenshot shows a confirmation dialog box titled 'Delete 1 functions'. It contains a warning message: '⚠ Deleting a function permanently removes the function code. The related logs, roles, test event schemas, and triggers are retained in your account.' Below the message, there's a list of the selected function: 'lambda'. A text input field at the bottom contains the word 'delete'. On the right side of the dialog, there are 'Cancel' and 'Delete' buttons. The background shows the same AWS Lambda interface as the previous screenshot.

The screenshot shows the AWS Lambda console with a search bar at the top containing 's3'. The search results are displayed under two sections: 'Services' and 'Features'.

Services (7 results):

- S3: Scalable Storage in the Cloud
- S3 Glacier: Archive Storage in the Cloud
- AWS Snow Family: Large Scale Data Transport
- AWS Transfer Family: Fully managed support for SFTP, FTPS and FTP

Features (19 results):

- Documentation (17,486)
- Blogs (1,226)
- Knowledge Articles (24)
- Tutorials (12)
- Events (26)
- Marketplace (1,107)

The right sidebar contains information about Lambda functions, including a note about recently created functions appearing in the list, filtering options, and instructions for performing actions on functions.

The screenshot shows the AWS S3 Management Console with a search bar at the top containing 's3'. The main view displays an account snapshot and a list of buckets.

Account snapshot: Storage Lens provides visibility into storage usage and activity trends. [Learn more](#)

Buckets (1):

Name	AWS Region	Access	Creation date
csee1	US East (N. Virginia) us-east-1	Public	May 4, 2023, 10:32:28 (UTC+05:30)

The left sidebar includes links for Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings for this account, Storage Lens (Dashboards, AWS Organizations settings), and Feature spotlight.

The bottom navigation bar shows the URL <https://s3.console.aws.amazon.com/s3/buckets/csee1?region=us-east-1>.

The screenshot shows the AWS S3 console for the bucket 'csee1'. The 'Objects' tab is selected. There is one object listed:

Name	Type	Last modified	Size	Storage class
WhatsApp Image 2023-03-01 at 12.02.16 (1).jpeg	jpeg	May 4, 2023, 10:34:38 (UTC+05:30)	41.5 KB	Standard

The screenshot shows the AWS S3 console with a delete confirmation dialog open over the object list.

Specified objects

Name	Type	Last modified	Size
WhatsApp Image 2023-03-01 at 12.02.16 (1).jpeg	jpeg	May 4, 2023, 10:34:38 (UTC+05:30)	41.5 KB

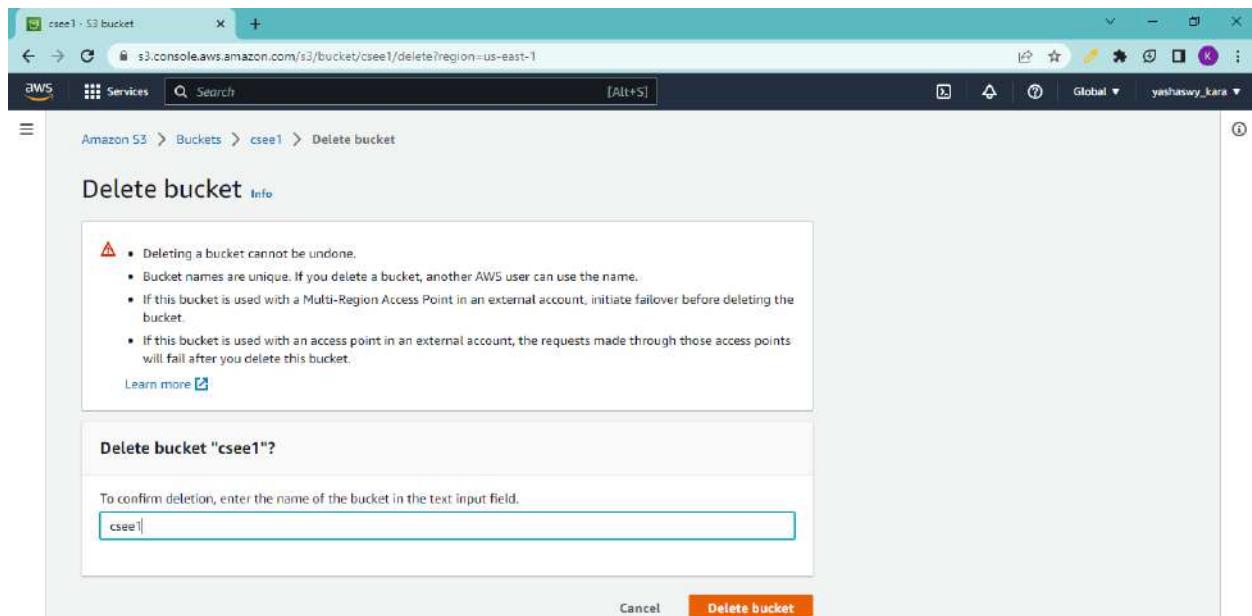
Permanently delete objects?

To confirm deletion, type *permanently delete* in the text input field.

Delete objects

The screenshot shows the AWS Lambda console interface. At the top, there's a search bar and a navigation bar with 'Services' and 'Search'. Below that, the main area has a title 'Lambda > Functions' and a sub-section 'Functions (1/1)'. A table lists one function: 'lambda'. The table columns include 'Function name', 'Description', 'Package type', 'Runtime', and 'Last modified'. The 'Delete' button in the 'Actions' column is highlighted with a blue border. The function details show it's a 'Zip' package type, runs on 'Python 3.7', and was last modified '10 minutes ago'. To the right of the table, there's a sidebar titled 'Lambda functions' with descriptive text about filtering and performing actions on functions.

The screenshot shows the AWS S3 Management Console. At the top, there's a search bar and a navigation bar with 'Services' and 'Search'. Below that, the main area has a title 'Amazon S3 > Buckets' and a sub-section 'Buckets (1)'. A table lists one bucket: 'csee1'. The table columns include 'Name', 'AWS Region', 'Access', and 'Creation date'. The bucket 'csee1' is located in 'US East (N. Virginia)' with 'us-east-1' as its region. The 'Access' column shows a red warning icon followed by 'Public'. The 'Creation date' is 'May 4, 2023, 10:32:28 (UTC+05:30)'. To the left, there's a sidebar with links for 'Buckets', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', 'IAM Access Analyzer for S3', 'Block Public Access settings for this account', 'Storage Lens', 'Dashboards', and 'AWS Organizations settings'. The status bar at the bottom shows the date as 05/04/2023 and the time as 10:51 AM.



Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings

IAM > Roles

Roles (Selected 1/6) 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.

[Create role](#)

Role name	Trusted entities	Last updated
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS Service: dynamodb application-autoscaling (Service-Linked Role)	54 days ago
AWSServiceRoleForLexV2Bots_3RXWR95B84V	AWS Service: lexv2 (Service-Linked Role)	-
AWSServiceRoleForLexV2Bots_4VVM9CZLA06	AWS Service: lexv2 (Service-Linked Role)	-
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
sample	AWS Service: lambda	-

Roles Anywhere Info

Authenticate your own AWS workloads and securely provide access to AWS services.

[Manage](#)

The screenshot shows the AWS IAM Management Console. In the top-left corner, there's a sidebar titled "Identity and Access Management (IAM)" with options like "Dashboard", "Access management", "Access reports", and "Roles". The "Roles" option is selected. The main area shows a list of roles with one row highlighted for "sample". A modal dialog box titled "Delete sample?" is open over the list. It contains a confirmation message: "Delete sample permanently? This will also delete all its inline policies and any attached instance profiles." Below this, it says "Role name" and "sample". A note below the role name states: "Recent activity usually appears within 4 hours. Data is stored for a maximum of 365 days, depending when your region began supporting this feature." There's a "Note" link. Below the note, it says "This action cannot be undone." At the bottom of the modal, there's a text input field containing "sample", a "Cancel" button, and a "Delete" button.

Role deleted sample.

The screenshot shows the same IAM console after the deletion. A green success message at the top left says "Role deleted sample." The main table now lists five roles: "AWSServiceRoleForApplicationAutoScaling_DynamoDBTable", "AWSServiceRoleForLexV2Bots_3RXWR96B84V", "AWSServiceRoleForLexV2Bots_4VVM9CZLA05", "AWSServiceRoleForSupport", and "AWSServiceRoleForTrustedAdvisor". Each role has its "Trusted entities" listed next to it. The table includes columns for "Role name", "Trusted entities", and "Last activity".

The screenshot shows the AWS S3 console interface. At the top, a green banner indicates "Successfully deleted objects". Below this, a modal window titled "Delete objects: status" displays a message: "The information below will no longer be available after you navigate away from this page." The "Summary" section shows the following details:

Source	Successfully deleted	Failed to delete
s3://csee1	1 object, 41.5 KB	0 objects

Below the summary, there are tabs for "Failed to delete" (which is selected) and "Configuration". Under "Failed to delete", it says "(0)". A search bar at the bottom of this section contains the placeholder text "Find objects by name". The browser's address bar shows the URL: s3.console.aws.amazon.com/s3/buckets/csee1/object/delete?region=us-east-1&showversions=false. The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray indicating the date and time.