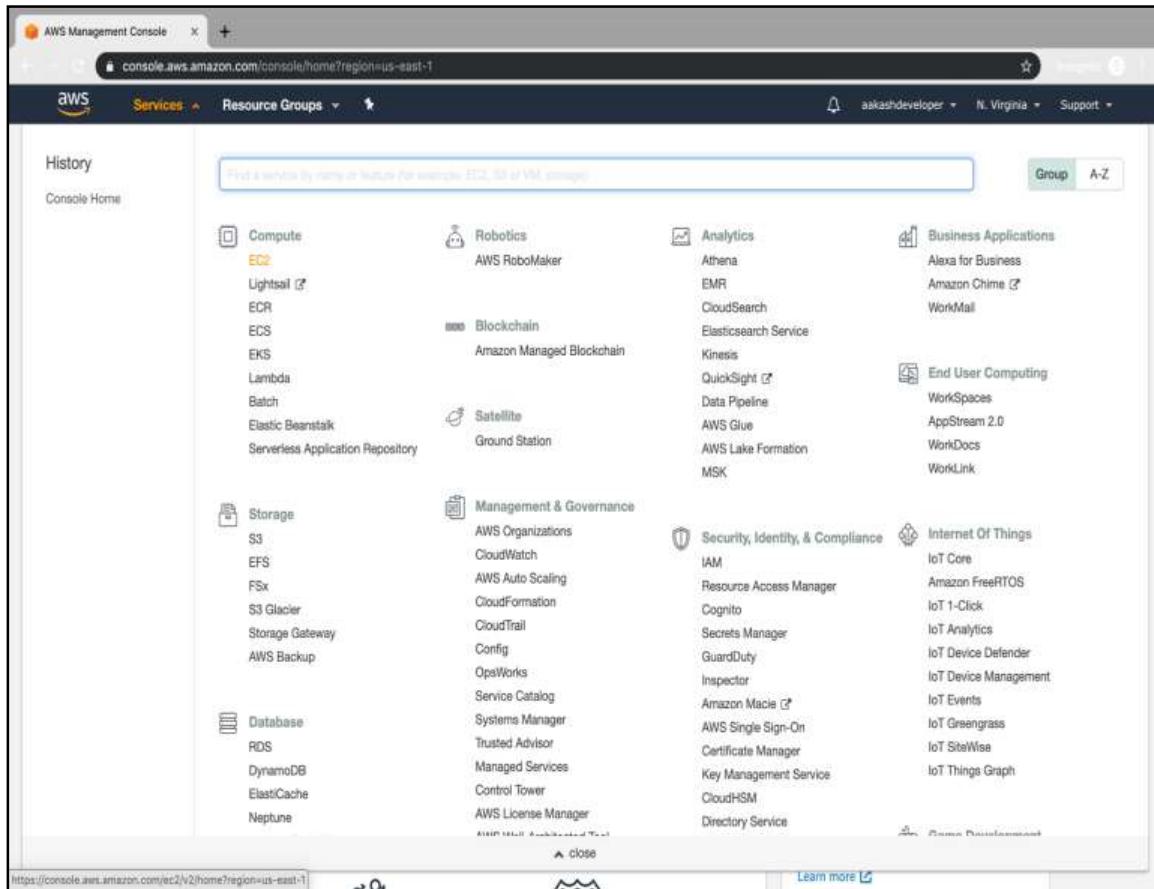


# 1.Launch and Connect to an EC2 Linux Instance.

## Step 1: Launching an EC2 instance

- Go to Amazon dashboard
- Select EC2



- Click on *launch instance* to run any instance

- Select the AMI

- Select t2. micro as the instance type

**Step 2: Choose an Instance Type**

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more about instance types and how they can meet your computing needs.](#)

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance	IPv6 Support
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
General purpose	<b>t2.micro</b> <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

Feedback English (US) © 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

- Specify the number of instances, networks, placement groups, and IAM roles and click *Next*

**Step 3: Configure Instance Details**

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 Launch into Auto Scaling Group

Purchasing option: Request Spot Instances

Network: vpc-4e244834 (default) Create new VPC

Subnet: No preference (default subnet in any Availability Zone) Create new subnet

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: Add instance to placement group

Capacity Reservation: Open Create new Capacity Reservation

IAM role: None Create new IAM role

Shutdown behavior: Stop Protect against accidental termination

Enable termination protection: Protect against accidental termination

Monitoring: Enable CloudWatch detailed monitoring Additional charges apply.

Tenancy: Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.

Elastic Inference: Add an Elastic Inference accelerator

Cancel Previous Review and Launch Next: Add Storage

Feedback English (US) © 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

- There is one volume attached to the instance by default

- In Linux, the default volume attached is 8 GB
- You can add more volume if required

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-05a19c3561abd794a	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Cancel Previous Review and Launch Next: Add Tags

- You can add a key-value pair to the instance

Key	Value	Instances	Volumes
linux	firstlinux	<input checked="" type="checkbox"/>	<input type="checkbox"/>
os	Ubuntu	<input type="checkbox"/>	<input type="checkbox"/>

Add another tag (Up to 50 tags maximum)

**Step 6: Configure Security Group**

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: [Create a new security group](#)

Select an existing security group

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop

[Add Rule](#)

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

[Cancel](#) [Previous](#) [Review and Launch](#)

- Attach the three policy groups depending on the type of access required

**Step 7: Review Instance Launch**

The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

Root Device Type: ebs Virtualization type: hvm

[Edit instance type](#)

**Instance Type**

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

[Edit security groups](#)

**Security Groups**

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	
HTTP	TCP	80	0.0.0.0/0	
HTTP	TCP	80	::/0	

[Edit instance details](#)

[Edit storage](#)

[Edit tags](#)

[Cancel](#) [Previous](#) [Launch](#)

- Select an existing key-value pair to launch the instance

The screenshot shows the AWS Launch Instance Wizard Step 7: Review Instance Launch. The main page displays instance configuration details and security group settings. A modal window titled "Select an existing key pair or create a new key pair" is open, showing three options: "Choose an existing key pair" (selected), "Create a new key pair" (highlighted in blue), and "Proceed without a key pair". A note below states: "A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance." Below the modal, there is an acknowledgment checkbox: "I acknowledge that I have access to the selected private key file (july\_aws\_batch.pem), and that without this file, I won't be able to log into my instance." At the bottom of the modal are "Cancel" and "Launch Instances" buttons.

- The instance is ready to use

The screenshot shows the AWS EC2 Management console. On the left, there's a sidebar with various navigation links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, AMIs, and Network & Security. The main area displays a table of instances. One instance is selected, showing its details: Name (i-0cbb6d6e60f077cbc), Instance ID (i-0cbb6d6e60f077cbc), Instance Type (t2.micro), Availability Zone (us-east-1b), Instance State (running), Status Checks (2/2 checks ...), Alarm Status (None), Public DNS (IPv4) (ec2-52-91-199-186.compute-1.amazonaws.com), and IPv4 Public IP (52.91.199.186). Below the table, a detailed view for the selected instance shows fields like Description, Status Checks, Monitoring, and Tags. The Status Checks tab is active, displaying the instance's state information.

- Click on *Connect* on EC2 dashboard
- Run the ssh command provided

```
Last login: Fri Sep 20 17:34:39 on ttys001
(base) Avyaans-MacBook-Pro:~ avi$ ssh -i "july_aws_batch.pem" ec2-user@ec2-52-91-199-186.compute-1.amazonaws.com
```

```
(base) Avyaans-MacBook-Pro:Downloads avi$ ssh -i "july_aws_batch.pem" ec2-user@ec2-52-91-199-186.compute-1.amazonaws.com
[ec2-user@ip-172-31-91-59 ~]$ ls
[ec2-user@ip-172-31-91-59 ~]$ cd /var/www/html
[ec2-user@ip-172-31-91-59 ~]$ curl https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
[ec2-user@ip-172-31-91-59 ~]$
```

## Step 2: Connecting to an EC2 instance

- Run the following command to launch a website over EC2:

```
yum install httpd -y
```

```
[command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C fd] [-D level] [-g groupname[#gid]] [-p prompt] [-u user name[#uid]] [-g
groupname[#gid]] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C fd] [-D level] [-g groupname[#gid]] [-p prompt] [-u user name[#uid]] file ...
[ec2-user@ip-172-31-91-59 ~]$ sudo su -
[root@ip-172-31-91-59 ~]# yum install httpd -y
Loaded plugins: priorities, update-motd, upgrade-helper
amzn-main                                         | 2.1 kB  00:00:00
amzn-updates                                      | 2.5 kB  00:00:00
Resolving Dependencies
--> Running transaction check
--> Package httpd.x86_64 0:2.2.34-1.16.amzn1 will be installed
--> Processing Dependency: httpd-tools = 2.2.34-1.16.amzn1 for package: httpd-2.2.34-1.16.amzn1.x86_64
--> Processing Dependency: apr-util-ldap for package: httpd-2.2.34-1.16.amzn1.x86_64
--> Processing Dependency: libaprutil-1.so.0()(64bit) for package: httpd-2.2.34-1.16.amzn1.x86_64
--> Processing Dependency: libapr-1.so.0()(64bit) for package: httpd-2.2.34-1.16.amzn1.x86_64
--> Running transaction check
--> Package apr.x86_64 0:1.5.2-5.13.amzn1 will be installed
--> Package apr-util.x86_64 0:1.5.4-6.18.amzn1 will be installed
--> Package apr-util-ldap.x86_64 0:1.5.4-6.18.amzn1 will be installed
--> Package httpd-tools.x86_64 0:2.2.34-1.16.amzn1 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package           Arch      Version       Repository   Size
=====
Installing:
httpd            x86_64    2.2.34-1.16.amzn1   amzn-main   1.2 M
Installing for dependencies:
apr               x86_64    1.5.2-5.13.amzn1   amzn-main   118 k
apr-util          x86_64    1.5.4-6.18.amzn1   amzn-main   99 k
apr-util-ldap    x86_64    1.5.4-6.18.amzn1   amzn-main   19 k
httpd-tools       x86_64    2.2.34-1.16.amzn1   amzn-main   80 k

Transaction Summary
=====
```

- Navigate to /var/www/html and create index.html file using command

```
vi index.html
```

```
Install 1 Package (+4 Dependent packages)

Total download size: 1.5 M
Installed size: 3.6 M
Downloading packages:
(1/5): apr-util-ldap-1.5.4-6.18.amzn1.x86_64.rpm | 19 kB 00:00:00
(2/5): apr-1.5.2-5.13.amzn1.x86_64.rpm | 118 kB 00:00:00
(3/5): apr-util-1.5.4-6.18.amzn1.x86_64.rpm | 99 kB 00:00:00
(4/5): httpd-tools-2.2.34-1.16.amzn1.x86_64.rpm | 80 kB 00:00:00
(5/5): httpd-2.2.34-1.16.amzn1.x86_64.rpm | 1.2 MB 00:00:00

Total                                         1.9 MB/s | 1.5 MB 00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : apr-1.5.2-5.13.amzn1.x86_64
  Installing : apr-util-1.5.4-6.18.amzn1.x86_64
  Installing : httpd-tools-2.2.34-1.16.amzn1.x86_64
  Installing : apr-util-ldap-1.5.4-6.18.amzn1.x86_64
  Installing : httpd-2.2.34-1.16.amzn1.x86_64
  Verifying   : httpd-tools-2.2.34-1.16.amzn1.x86_64
  Verifying   : apr-1.5.4-6.18.amzn1.x86_64
  Verifying   : httpd-2.2.34-1.16.amzn1.x86_64
  Verifying   : apr-1.5.2-5.13.amzn1.x86_64
  Verifying   : apr-util-ldap-1.5.4-6.18.amzn1.x86_64

Installed:
  httpd.x86_64 0:2.2.34-1.16.amzn1

Dependency Installed:
  apr.x86_64 0:1.5.2-5.13.amzn1           apr-util.x86_64 0:1.5.4-6.18.amzn1   apr-util-ldap.x86_64 0:1.5.4-6.18.amzn1
  httpd-tools.x86_64 0:2.2.34-1.16.amzn1

Complete!
[root@ip-172-31-91-59 ~]# cd /var/www/html/
```

- Enter *I* and start creating HTML file content
  - Once done, type :*wq!*

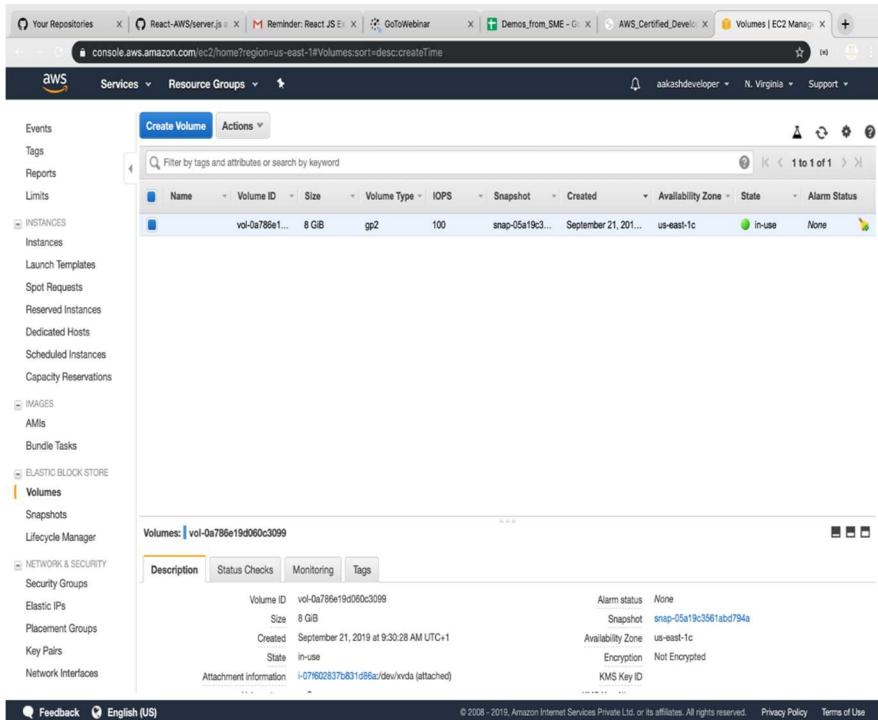
- Using public IP of EC2 instance, you can see your app running on the browser

```
[root@ip-172-31-91-59 html]# service httpd start
Starting httpd: [ OK ]
```



## 2.Change the Volume Size of an Instance.

**Step 1:** Creating the new volume which we want to add to an instance and clicking on **create volume**



The screenshot shows the AWS Management Console interface for managing EC2 volumes. The left sidebar navigation includes 'Your Repositories', 'React-AWS/server.js', 'Reminder: React JS E...', 'GoToWebinar', 'Demos\_from\_SME - 0...', 'AWS\_Certified\_Devel...', and 'Volumes | EC2 Manager'. The main menu bar has 'Services', 'Resource Groups', and 'Actions' dropdowns, along with user information 'aakashdeveloper', 'N. Virginia', and 'Support'. The 'VOLUMES' section is selected in the sidebar. A search bar at the top right says 'Filter by tags and attributes or search by keyword'. Below it is a table header with columns: Name, Volume ID, Size, Volume Type, IOPS, Snapshot, Created, Availability Zone, State, and Alarm Status. There is one row of data: 'vol-0a786e19d060c3099', 'vol-0a786e19d060c3099', '8 GiB', 'gp2', '100', 'snap-05a19c3...', 'September 21, 201...', 'us-east-1c', 'In-use', 'None'. At the bottom of the table, there are tabs for 'Description', 'Status Checks', 'Monitoring', and 'Tags', with 'Description' being the active tab. Detailed information for the volume is shown below the table: Volume ID (vol-0a786e19d060c3099), Size (8 GiB), Created (September 21, 2019 at 9:32:28 AM UTC+1), Availability Zone (us-east-1c), State (In-use), Attachment Information (i-07602837b831d96a/dev/xvda (attached)), Alarm status (None), Snapshot (snap-05a19c3561abd794a), Encryption (Not Encrypted), and KMS Key ID (None). The bottom of the page includes links for 'Feedback', 'English (US)', and legal notices: '© 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.', 'Privacy Policy', and 'Terms of Use'.

**Step 2:** Validating the Availability zone of the EC2 instance with which you want to add volume

The screenshot shows the AWS EC2 Instances Management console. The left sidebar navigation includes: Events, Tags, Reports, Limits, INSTANCES (with Instances selected), Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, IMAGES (with AMIs selected), and Bundle Tasks. The main content area displays a table of instances. A single instance is listed:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
	i-07f602837b831d86a	t2.micro	us-east-1c	running	2/2 checks ...	None	ec2-54-227-70-128.co...	54.227.70.128

Below the table, the instance details for i-07f602837b831d86a are shown. The Public DNS is ec2-54-227-70-128.compute-1.amazonaws.com. The detailed view shows the following information:

Description	Value	Description	Value
Instance ID	i-07f602837b831d86a	Public DNS (IPv4)	ec2-54-227-70-128.compute-1.amazonaws.com
Instance state	running	IPv4 Public IP	54.227.70.128
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-172-31-30-3.ec2.internal
Availability zone	us-east-1c	Private IPs	172.31.30.3

At the bottom, there are links for Feedback, English (US), and footer text: © 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use.

**Step 3:** Providing type, size, availability zone, and snapshot name on the **create volume** tab

Create Volume

Volume Type General Purpose SSD (gp2)

Size (GiB) 2  (Min: 1 GiB, Max: 16384 GiB)

IOPS 300 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)

Availability Zone\* us-east-1c

Throughput (MB/s) Not applicable

Snapshot ID Select a snapshot

Encryption  Encrypt this volume

Key (128 characters maximum) Value (256 characters maximum)

This resource currently has no tags  
Choose the Add tag button or [click to add a Name tag](#)

Add Tag 50 remaining (Up to 50 tags maximum)

\* Required

[Feedback](#) [English \(US\)](#) © 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

**Step 4:** Selecting newly created volume and clicking on the action to attach the volume to the instance

The screenshot shows the AWS EC2 Management Console with the 'Volumes' page selected. On the left, there's a sidebar with links like 'Create Volume', 'Actions', 'Events', 'Tags', 'Reports', 'Limits', 'Instances', 'Launch Templates', 'Spot Requests', 'Reserved Instances', 'Dedicated Hosts', and 'Scheduled Instances'. A context menu is open over a volume, with 'Attach Volume' highlighted. The main table lists two volumes:

Volume Type	IOPS	Snapshot	Created	Availability Zone	State	Alarm Status
gp2	100		September 21, 201...	us-east-1c	available	None
gp2	100	snap-05a19c3...	September 21, 201...	us-east-1c	in-use	None

**Step 5:** Selecting the instance of the same availability zone and attaching the volume in pop

The screenshot shows the 'Attach Volume' dialog box. On the left, there's a sidebar with links like 'Reserved Instances', 'Dedicated Hosts', 'Scheduled Instances', 'Capacity Reservations', 'AMIs', 'Bundle Tasks', 'Elastic Block Store' (with 'Volumes' selected), 'Snapshots', 'Lifecycle Manager', 'Network & Security' (with 'Security Groups' selected), and 'Elastic IPs'. The main area shows the 'Attach Volume' dialog with the following fields:

- Volume: vol-08837d74e970201a4 in us-east-1c
- Instance: i-07f602837b831d86a in us-east-1c
- Device: /dev/sdf

A note at the bottom states: "Note: Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdw internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp." The 'Attach' button is highlighted.

**Step 6:** Verifying the instance by adding one more device to the block device

The screenshot shows the AWS EC2 Instances Management console. On the left, there's a sidebar with navigation links for Events, Tags, Reports, Limits, Instances (selected), Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, Images (AMIs), Bundle Tasks, Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces). The main content area displays a table of instances. A single row is selected, showing details for an instance named 'i-07f602837b831d86a'. The instance is a 't2.micro' type, running in 'us-east-1c' availability zone, with a Public DNS of 'ec2-54-227-70-128.co...' and a Public IP of '54.227.70.128'. The table includes columns for Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, Public DNS (IPv4), and IPv4 Public IP. Below the table, detailed configuration settings for the instance are listed, including VPC ID, Subnet ID, Network interfaces, Source/dest. check, T2/T3 Unlimited, EBS-optimized, Root device type, Root device, Block devices, Elastic Graphics ID, Elastic Inference accelerator ID, Capacity Reservation, and Capacity Reservation Settings.

### 3.Launch an Instance in a Placement Group.

#### Step 1: Creating a placement group

- Click on *Create Placement Group*

The screenshot shows the AWS EC2 Management Console with the 'Placement Groups' section selected. The left sidebar lists various EC2 services like Instances, Images, and Auto Scaling. The main content area displays a message: 'You do not have any Placement groups in this region'. Below it is a sub-instruction: 'Click the Create Placement group button to create your first Placement group'. A prominent blue 'Create Placement Group' button is centered at the bottom of this section.

- Provide a name and strategy

The screenshot shows the 'Create Placement Group' wizard. The 'Name' field contains 'simplilearnApp'. The 'Strategy' dropdown is set to 'Cluster' and is currently being selected from a dropdown menu. The menu also lists 'Spread' and 'Partition'. At the bottom right of the form are 'Cancel' and 'Create' buttons.

## Step 2: Launching an instance in the placement group

- Launch the new EC2 instance

The screenshot shows the AWS EC2 Management Console Home page. On the left, there's a sidebar with various navigation links like EC2 Dashboard, Instances, Images, and Elastic Block Store. The main area displays 'Resources' for the US East (N. Virginia) region, showing 0 Running Instances, 0 Dedicated Hosts, 0 Volumes, 4 Key Pairs, 0 Elastic IPs, 0 Snapshots, 0 Load Balancers, and 42 Security Groups. Below this, there are sections for 'Create Instance' (with a 'Launch Instance' button), 'Service Health' (showing the US East (N. Virginia) region is healthy), and 'Scheduled Events' (showing 'No events'). On the right, there's an 'Account Attributes' section with details like 'Supported Platforms' (VPC), 'Default VPC' (vpc-e4e244834), and 'AWS Marketplace' with software like CloudEndure Migration and Matillion ETL for Amazon Redshift.

- Select the placement group

The screenshot shows the 'Launch Instance Wizard | EC2' step 3: 'Configure Instance Details'. It's a multi-step wizard with tabs at the top: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance (which is selected), 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review. The main form includes fields for 'Number of Instances' (1), 'Purchasing option' (Request Spot instances), 'Network' (vpc-e4e244834), 'Subnet' (No preference), 'Auto-assign Public IP' (Use subnet setting (Enable)), 'Placement group' (Add instance to placement group), 'Placement group name' (simpilearn), and 'Capacity Reservation' (simpilearn). A dropdown menu for 'Choose placement group' is open, showing a table with one entry: Name: simpilearn, Strategy: spread. At the bottom are buttons for 'Cancel', 'Previous', 'Review and Launch' (highlighted in blue), and 'Next: Add Storage'.

Launch instance wizard | EC2 | X

console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:

aakashdeveloper N. Virginia Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

**Step 3: Configure Instance Details**

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of Instances: 1 Launch into Auto Scaling Group

Purchasing option: Request Spot Instances

Network: vpc-4e244834 (default) Create new VPC

Subnet: No preference (default subnet in any Availability Zone) Create new subnet

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: Add instance to placement group

Placement group name: simplilearn (spread)

You can launch up to 7 more instances into this placement group. Spread placement groups can have up to seven running instances per Availability Zone. [Learn more](#)

Capacity Reservation: Open Create new Capacity Reservation

IAM role: None Create new IAM role

Shutdown behavior: Stop

Cancel Previous Review and Launch Next: Add Storage

Feedback English (US) © 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

- Verify the placement group of the instance

Instances | EC2 Management | Creating an Amazon EBS Volume

console.aws.amazon.com/ec2/v2/home?region=us-east-1#instances:sort=instanceId

aakashdeveloper N. Virginia Support

EC2 Dashboard Events Tags Reports Limits

**INSTANCES** Instances Launch Templates Spot Requests Reserved Instances Dedicated Hosts Scheduled Instances Capacity Reservations

IMAGES AMIs Bundle Tasks

ELASTIC BLOCK STORE Volumes Snapshots Lifecycle Manager

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

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword 1 to 3 of 3

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
i-042fb99c2e3ee710f	i2.micro	us-east-1a	terminated					-
<b>i-07ccbc006eb412b0f</b>	i2.micro	us-east-1c	running	2/2 checks ...	None		ec2-34-207-220-254.co...	34.207.220.254
i-07f602837b831d86a	i2.micro	us-east-1c	terminated					-

Termination protection: False Root device: /dev/xvda

Lifecycle: normal Block devices: /dev/xvda

Monitoring: basic Elastic Graphics ID: -

Alarm status: None Elastic Inference accelerator ID: -

Kernel ID: - Capacity Reservation: -

RAM disk ID: - Capacity Reservation Settings: Open

Placement group: simplilearn

Partition number: -

Virtualization: hvm

Reservation: r-02803c51a5807016a

AMI launch index: 0

Tenancy: default

Host ID: -

Affinity: -

State transition reason: -

State transition reason message: -

Stop - Hibernation behavior: Disabled

Number of vCPUs: 1

Feedback English (US) © 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

# 4. Create an EBS Volume.

## Step 1: Selecting the volume tab in the EC2 dashboard

The screenshot shows the AWS EC2 Management Console dashboard. The left sidebar has 'ELASTIC BLOCK STORE' expanded, with 'Volumes' selected. The main content area displays various EC2 resources: 1 Running Instances, 0 Dedicated Hosts, 1 Volumes, 4 Key Pairs, and 1 Placement Groups. On the right, there are sections for 'Account Attributes' (Supported Platforms: VPC; Default VPC: vpc-f4e244834) and 'Additional Information' (Getting Started Guide, Documentation, All EC2 Resources, Forums, Pricing, Contact Us). Below these are sections for 'Service Health' (Status: US East (N. Virginia) is operating normally) and 'Scheduled Events' (US East (N. Virginia): No events). A 'Create Instance' section includes a 'Launch Instance' button. A note at the bottom says 'Note: Your instances will launch in the US East (N. Virginia) region'. The URL in the address bar is <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Volumes>.

## Step 2: Creating a new volume by clicking on Create

The screenshot shows the 'Volumes' page in the AWS EC2 Management Console. The left sidebar has 'ELASTIC BLOCK STORE' expanded, with 'Volumes' selected. The main content area features a 'Create Volume' button and a table displaying existing volumes. The table columns include Name, Volume ID, Size, Volume Type, IOPS, Snapshot, Created, Availability Zone, State, and Alarm Status. One volume is listed: vol-037de51... (8 GiB, gp2, 100 IOPS, snap-05a19c3..., September 21, 201..., us-east-1c, in-use, None). A 'Actions' dropdown menu is open above the table. A search bar at the top allows filtering by tags and attributes or searching by keyword. The URL in the address bar is <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Volumes:sort=desc:createTime>.

## Step 3: Selecting the volume type according to the project requirement

The screenshot shows the 'Create Volume' page in the AWS Management Console. The 'Volume Type' dropdown is open, displaying the following options:

- General Purpose SSD (gp2) (selected)
- Provisioned IOPS SSD (io1)
- Cold HDD (sc1)
- Throughput Optimized HDD (st1)
- Magnetic (standard)

The 'Size (GiB)' field is set to 'Filter by attributes' with a maximum value of 16384 GiB. The 'IOPS' section indicates 3 IOPS per GiB with a maximum of 100 IOPS burstable. The 'Availability Zone\*' dropdown is set to 'us-east-1'. The 'Throughput (MB/s)' field is marked as 'Not applicable'. The 'Snapshot ID' dropdown is set to 'Select a snapshot'. The 'Encryption' checkbox is unchecked. Below the form, there are fields for 'Key' and 'Value' with placeholder text: 'This resource currently has no tags' and 'Choose the Add tag button or click to add a Name tag'. At the bottom, there is an 'Add Tag' button and a note about remaining tags: '50 remaining (Up to 50 tags maximum)'. The footer includes links for Feedback, English (US), Privacy Policy, and Terms of Use.

## Step 4: Creating a new volume by specifying the size and defining the zone

The screenshot shows the 'Create Volume' page in the AWS EC2 Manager. The top navigation bar includes tabs for 'Create Volume | EC2 Manager' and 'Creating an Amazon EBS Volume'. The URL in the address bar is 'console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateVolume'. The top right corner shows user information: 'akashdeveloper' with a bell icon, 'N. Virginia', and 'Support'.

The main form fields are:

- Volume Type:** General Purpose SSD (gp2)
- Size (GiB):** 1 (Min: 1 GiB, Max: 16384 GiB)
- IOPS:** 100 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)
- Availability Zone:** us-east-1a
- Throughput (MB/s):** Not applicable
- Snapshot ID:** Select a snapshot
- Encryption:**  Encrypt this volume

Below the form, there is a section for tags:

Key (128 characters maximum)      Value (256 characters maximum)

This resource currently has no tags

Choose the Add tag button or click to add a Name tag

Add Tag 50 remaining (Up to 50 tags maximum)

At the bottom of the page, there are links for Feedback, English (US), and footer text: © 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

**Step 5:** Verifying the new volume created on the volume console and its availability

Volumes | EC2 Management Consoles | Creating an Amazon EBS Volume | +

console.aws.amazon.com/ec2/v2/home?region=us-east-1#Volumes:sort=desc:createTime

aakashdeveloper N. Virginia Support

EC2 Dashboard Create Volume Actions

Events Tags Reports Limits

INSTANCES Instances Launch Templates Spot Requests Reserved Instances Dedicated Hosts Scheduled Instances Capacity Reservations

IMAGES AMIs Bundle Tasks

ELASTIC BLOCK STORE Volumes Snapshots Lifecycle Manager

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

LOAD BALANCING

Feedback English (US)

Creating an Amazon EBS Volume

Filter by tags and attributes or search by keyword

1 to 2 of 2

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone	State	Alarm Status
	vol-01bab43...	1 GiB	gp2	100		September 21, 2019 at 6:35:06 PM UTC+1	us-east-1a	available	None
	vol-037de51...	8 GiB	gp2	100	snap-05a19c3...	September 21, 2019 at 6:35:06 PM UTC+1	us-east-1c	in-use	None

Volumes: vol-037de514fb90f1baf

Description Status Checks Monitoring Tags

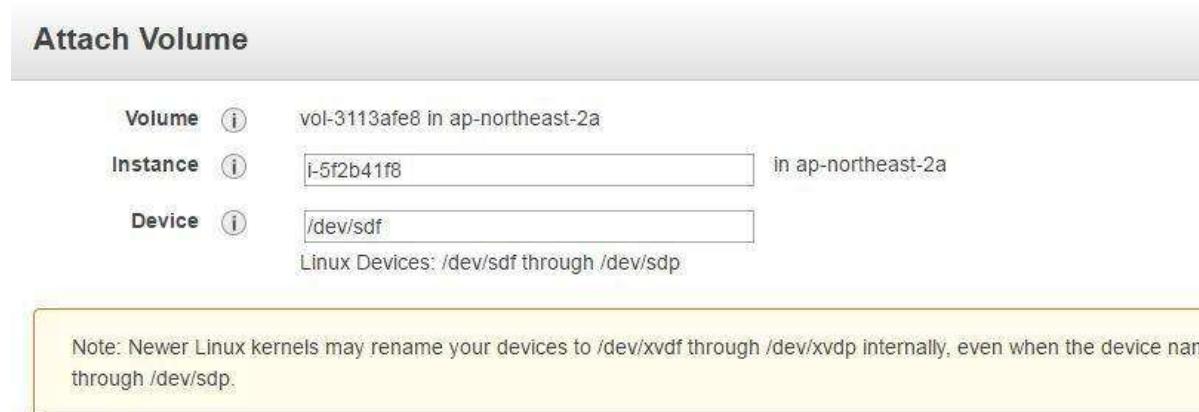
Volume ID	vol-037de514fb90f1baf	Alarm status	None
Size	8 GiB	Snapshot	snap-05a19c3561abd794a
Created	September 21, 2019 at 6:35:06 PM UTC+1	Availability Zone	us-east-1c
State	in-use	Encryption	Not Encrypted
Attachment information	i-07ccbc006eb412b0f/dev/xvda (attached)	KMS Key ID	

© 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

# 5. Format and Mount an EBS Volume.

## Step 1: Attaching an existing EBS volume

- Select an existing volume and click on *Attach Volume*
- Select the instance



## Step 2: Mounting the EBS volume

- Login to your EC2 instance and list the available disks using the following command:

```
lblk
```

- Use the following command to check if the volume has any data:

```
sudo file -s /dev/xvdf
```

- Use the following command to format the volume to ext4 filesystem:

```
sudo mkfs -t ext4 /dev/xvdf
```

- Use the following command to create a directory to mount the volume:

```
sudo mkdir /newvolume
```

- Use the following command to mount the volume:

```
sudo mount /dev/xvdf /newvolume/
```

- Check the disk space using the following command:

```
cd /newvolume
```

*df -h .*

**Step 3:** Unmounting the EBS volume

- Use the following command to unmount the volume:

*umount /dev/xvdf*

# 6. Detach an EBS Volume.

## Step 1: Selecting the EBS volume you want to detach

- Choose the bucket

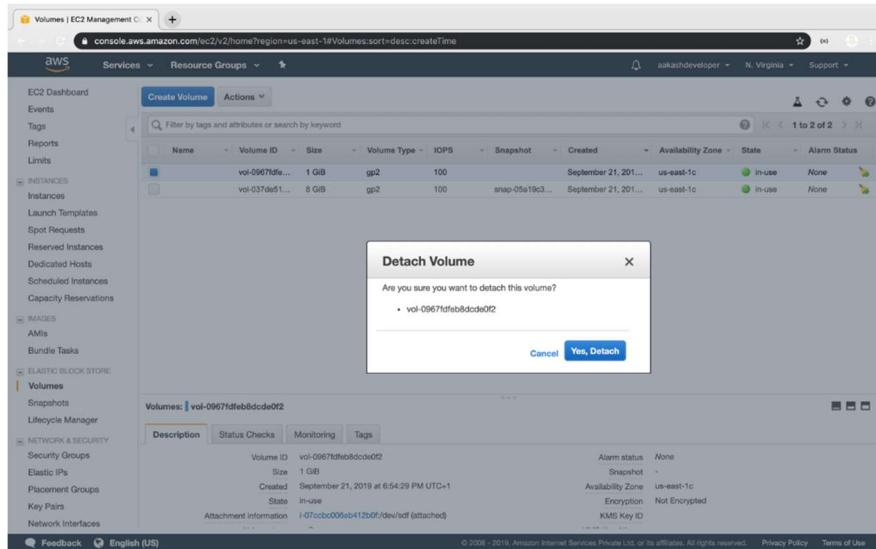
Name	Volume ID	Size	Type	IOPS	Snapshot	Created	Availability Zone	State	Alarm Status
vol-0967df...	vol-0967df...	1 GiB	gp2	100		September 21, 201...	us-east-1c	in-use	None
vol-037de5...	vol-037de5...	8 GiB	gp2	100	snap-05a19c3...	September 21, 201...	us-east-1c	in-use	None

- Select *Detach Volume* option

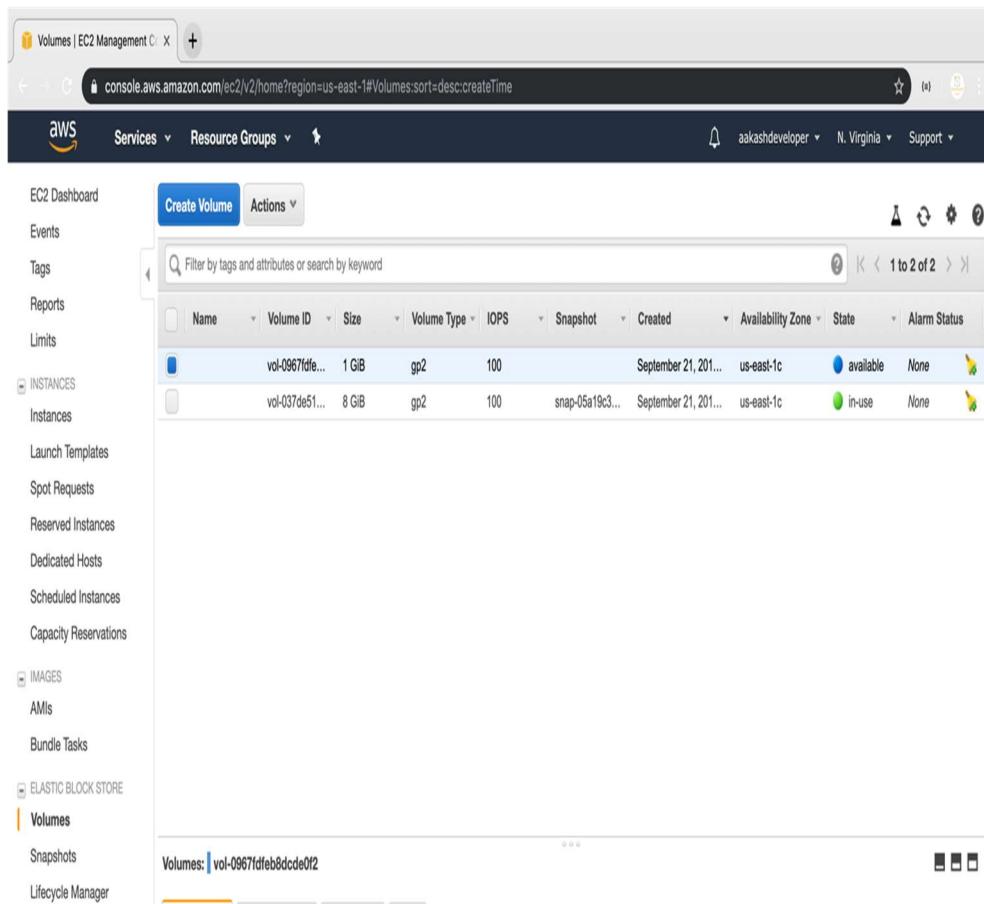
- Actions ▾
- Modify Volume
- Create Snapshot
- Delete Volume
- Attach Volume
- Detach Volume**
- Force Detach Volume
- Change Auto-Enable IO Setting
- Add/Edit Tags

## Step 2: Detaching the volume

- Select Yes once the confirmation pop-up appears

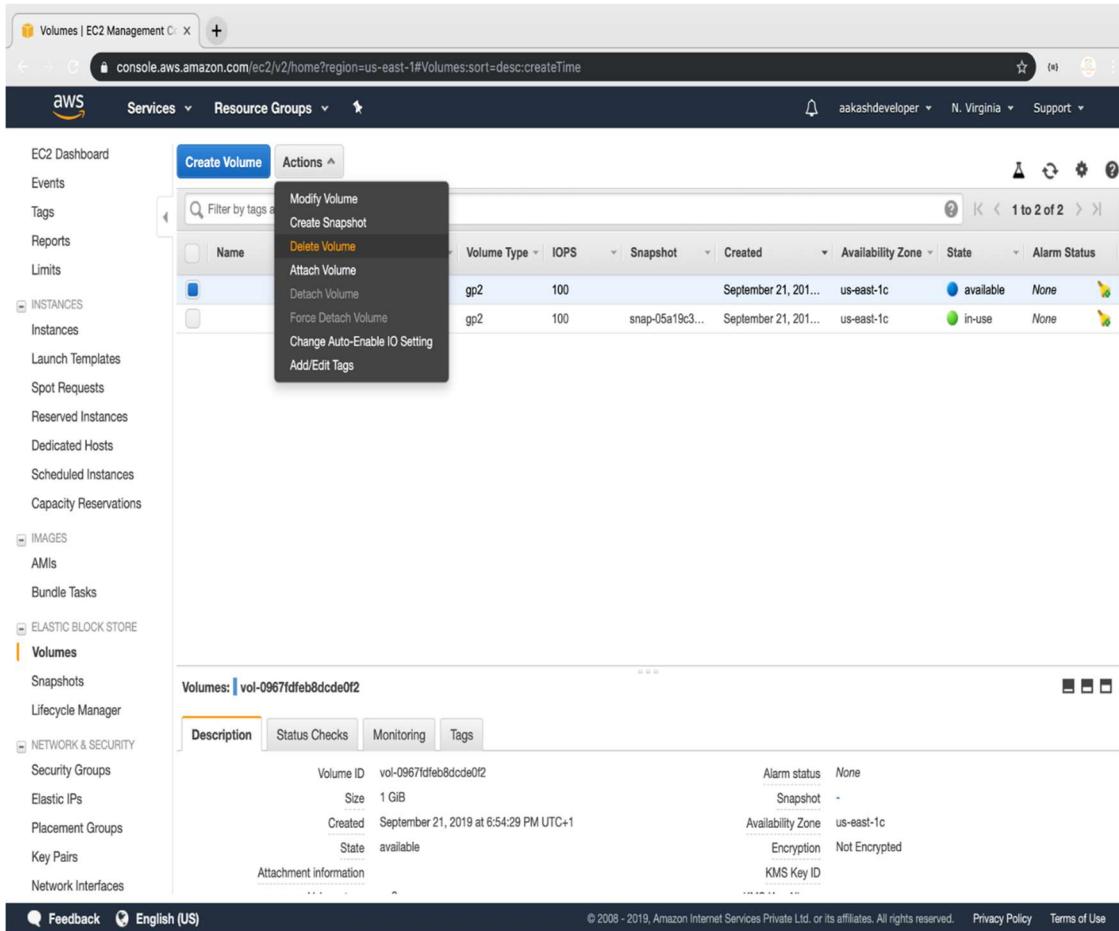


- Once detached, the volume will be labeled as *Available*



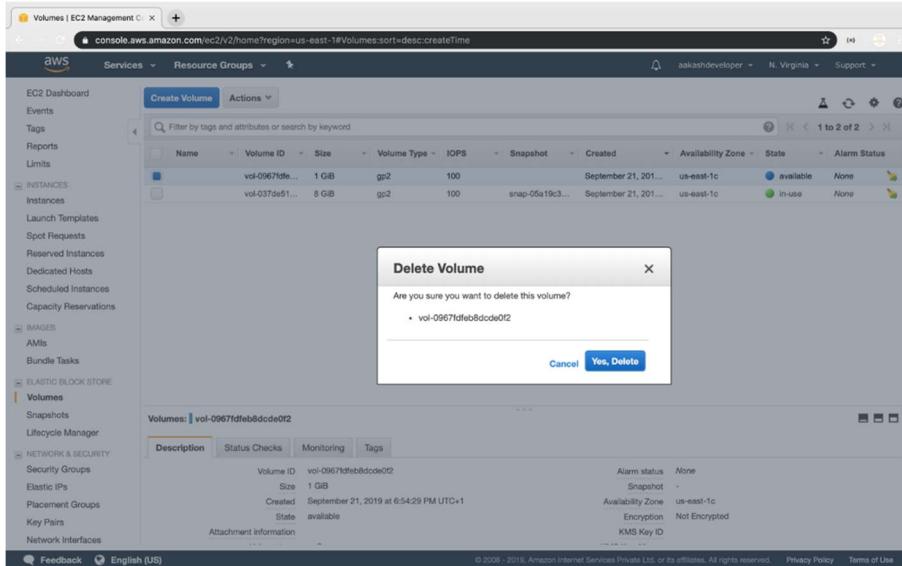
# 7. Delete an EBS Volume.

## Step 1: Selecting the EBS volume you want to delete



The screenshot shows the AWS EC2 Management Console with the 'Volumes' section selected. A context menu is open over a specific volume, listing options like 'Modify Volume', 'Create Snapshot', 'Delete Volume', 'Attach Volume', 'Detach Volume', 'Force Detach Volume', 'Change Auto-Enable IO Setting', and 'Add/Edit Tags'. The 'Delete Volume' option is highlighted. The main table lists two volumes: one gp2 volume of 100 IOPS created on September 21, 2019, and another gp2 volume of 100 IOPS created on September 21, 2019, which is currently in-use.

## Step 2: Deleting the volume



The screenshot shows the 'Delete Volume' confirmation dialog box. It asks 'Are you sure you want to delete this volume?' and lists the volume ID as 'vol-0967fdfb8dcde0f2'. At the bottom of the dialog are 'Cancel' and 'Yes, Delete' buttons. The background shows the same Volumes page as the previous screenshot, with the volume selection still visible.

# 8. Create an EBS Snapshot.

## Step 1: Creating an EBS snapshot

- Select *Volume* in EC2 dashboard
- Click on *Action -> Create Snapshot*

The screenshot shows the AWS EC2 Volumes Management interface. On the left, there's a sidebar with navigation links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, AMIs, and ELASTIC BLOCK STORE. Under EBS, 'Volumes' is selected, and its sub-links are Snapshots and Lifecycle Manager. The main content area shows a table of volumes. A context menu is open over a specific volume row, with 'Create Snapshot' highlighted. The table details a single volume entry:

Name	Volume Type	IOPS	Snapshot	Created	Availability Zone	State	Alarm Status
vol-037de514fb90fbaf	gp2	100	snap-05a19c3...	September 21, 201...	us-east-1c	in-use	None

At the bottom, there are links for Feedback, English (US), and footer links for 2008-2019 Amazon Internet Services Private Ltd. or its affiliates. All rights reserved., Privacy Policy, and Terms of Use.

- Add snapshot name, key, and value

Create Snapshot | EC2 Manager

console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateSnapshotFromVolume:

AWS Services Resource Groups

aakashdeveloper N. Virginia Support

Volumes > Create Snapshot

## Create Snapshot

Volume vol-037de514fb90f1baf ⓘ

Description SnapShot of main Drive ⓘ

Encrypted Not Encrypted ⓘ

Key (128 characters maximum) Value (256 characters maximum)

linux first ⌂

Add Tag 49 remaining (Up to 50 tags maximum)

\* Required Cancel Create Snapshot

Feedback English (US)

© 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

# 9. View snapshot.

**Step 1:** To view snapshots, you need to navigate to the EC2 **dashboard** available on the panel on the left. Click on **snapshot** to view all available snapshots.

The screenshot shows the AWS EC2 Management console with the following details:

**Snapshots | EC2 Management**

**Services** ▾ **Resource Groups** ▾

**Create Snapshot** **Actions** ▾

**Owned By Me** ▾ **Filter by tags and attributes or search by keyword**

**Snapshot Details:**

Name	Snapshot ID	Size	Description	Status	Started	Progress
snap-03b0d7a92bc...	8 GiB	SnapShot of main Drive	completed	September 21, 2019 at 7:04:...	available	100%

**Snapshot: snap-03b0d7a92bc8aa3b3**

**Description** **Permissions** **Tags**

Snapshot ID	Snapshot ID: snap-03b0d7a92bc8aa3b3	Progress	100%
Status	Status: completed	Capacity	8 GiB
Volume	Volume: vol-037de514fb90f1baf	Encryption	Not Encrypted
Started	Started: September 21, 2019 at 7:04:08 PM UTC+1	KMS Key ID	
Owner	Owner: 651759643195	KMS Key Aliases	
Product codes	-	KMS Key ARN	
Description	Description: SnapShot of main Drive		

**Feedback** **English (US)**

© 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

# 10. Initialize a Volume Restored from a Snapshot on Linux.

## Step 1: Selecting the snapshot

- Go to EC2 dashboard in EBS and click on *Snapshot*

The screenshot shows the AWS EC2 Management console with the 'Schemas | EC2 Management' tab selected. The URL in the address bar is <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Schemas:sort=snapshotId>. The navigation bar includes 'Services', 'Resource Groups', and account information for 'akashdeveloper' in 'N. Virginia'. On the left, a sidebar lists various services: Instances, Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, AMIs, Volumes, Snapshots (which is selected and highlighted in orange), Lifecycle Manager, Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces, Load Balancers, Target Groups, and Auto Scaling. The main content area displays a table titled 'Owned By Me' with columns: Name, Snapshot ID, Size, Description, Status, Started, and Progress. A single row is shown: 'snap-03b0d7a92bc...', '8 GiB', 'SnapShot of main Drive', 'completed', 'September 21, 2019 at 7:04...', and 'available'. Below the table, a detailed view for 'Snapshot: snap-03b0d7a92bc8aa3b3' is shown with tabs for Description, Permissions, and Tags. The 'Description' tab displays the following details:

Snapshot ID	vol-037de514fb90f1baf	Progress	100%
Status	completed	Capacity	8 GiB
Volume	vol-037de514fb90f1baf	Encryption	Not Encrypted
Started	September 21, 2019 at 7:04:08 PM UTC+1	KMS Key ID	
Owner	651759643195	KMS Key Aliases	

## Step 2: Restoring volume from the snapshot

- Select the snapshot and click on *Action*

Snapshots | EC2 Management

Create Snapshot Actions

Owned By Me

Delete  
Create Volume  
Create Image  
Copy  
Modify Permissions  
Add/Edit Tags

Name	Size	Description	Status	Started	Progress
snap-03b0d7a92bc8aa3b3	8 GiB	SnapShot of main Drive	completed	September 21, 2019 at 7:04:...	available

Snapshot: snap-03b0d7a92bc8aa3b3

Description Permissions Tags

Snapshot ID: snap-03b0d7a92bc8aa3b3 Status: completed Progress: 100% Capacity: 8 GiB  
Volume: vol-037de514fb90f1ba Status: completed Encryption: Not Encrypted  
Started: September 21, 2019 at 7:04:08 PM UTC+0 Owner: 651759643195 KMS Key ID: KMS Key Aliases: KMS Key ARN: Product codes: - Description: SnapShot of main Drive

Feedback English (US) © 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

- You can specify the key and value to identify the volume

Create Volume | EC2 Manager

Snapshots > Create Volume

Snapshot ID: snap-03b0d7a92bc8aa3b3

Volume Type: General Purpose SSD (gp2)

Size (GiB): 8 (Min: 1 GiB, Max: 16384 GiB)

IOPS: 100 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)

Availability Zone\*: us-east-1a

Throughput (MB/s): Not applicable

Encryption:  Encrypt this volume

Add Tag: Key (128 characters maximum) Value (256 characters maximum)  
Key: backup Value: snapshot restore

\* Required Cancel Create Volume

Feedback English (US) © 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

- Restore the volume from the snapshot

Snapshots | EC2 Management

console.aws.amazon.com/ec2/v2/home?region=us-east-1#Snapshots:sort=snapshotId

aakashdeveloper N. Virginia Support

**Create Snapshot** Actions

Owned By Me Filter by tags and attributes or search by keyword

Name	Snapshot ID	Size	Description	Status	Started	Progress
snap-03b0d7a92bc8aa3b...	8 GiB	SnapShot of main Drive	completed	September 21, 2019 at 7:04:...	available	

**Snapshot: snap-03b0d7a92bc8aa3b3**

Description Permissions Tags

Snapshot ID	snap-03b0d7a92bc8aa3b3	Progress	100%
Status	completed	Capacity	8 GiB
Volume	vol-037de514fb90f1baf	Encryption	Not Encrypted
Started	September 21, 2019 at 7:04:08 PM UTC+1	KMS Key ID	
Owner	651759643195	KMS Key Aliases	
Product codes	Loading...	KMS Key ARN	
Description	SnapShot of main Drive		

Feedback English (US) © 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

# 11. Create a Bucket.

Step 1: Selecting S3 from the storage of the AWS service panel

The screenshot shows the AWS Service Catalog interface. On the left, there's a sidebar with links like History, EC2, Console Home, IoT Core, CloudWatch, Lambda, and Billing. The main area is titled "Find a service by name or feature (for example, EC2, S3 or VM, storage)." It's organized into four columns: Compute (EC2, Lightsail, ECR, ECS, EKS, Lambda, Batch, Elastic Beanstalk, Serverless Application Repository), Robotics (AWS RoboMaker), Analytics (Athena, EMR, CloudSearch, Elasticsearch Service, Kinesis, QuickSight, Data Pipeline, AWS Glue, AWS Lake Formation, MSK), Business Applications (Alexa for Business, Amazon Chime, WorkMail), Storage (S3, EFS), Management & Governance (AWS Organizations, CloudWatch, AWS Auto Scaling), Security, Identity, & Compliance (IAM), and End User Computing (WorkSpaces, AppStream 2.0, WorkDocs, WorkLink). The S3 icon is highlighted in orange.

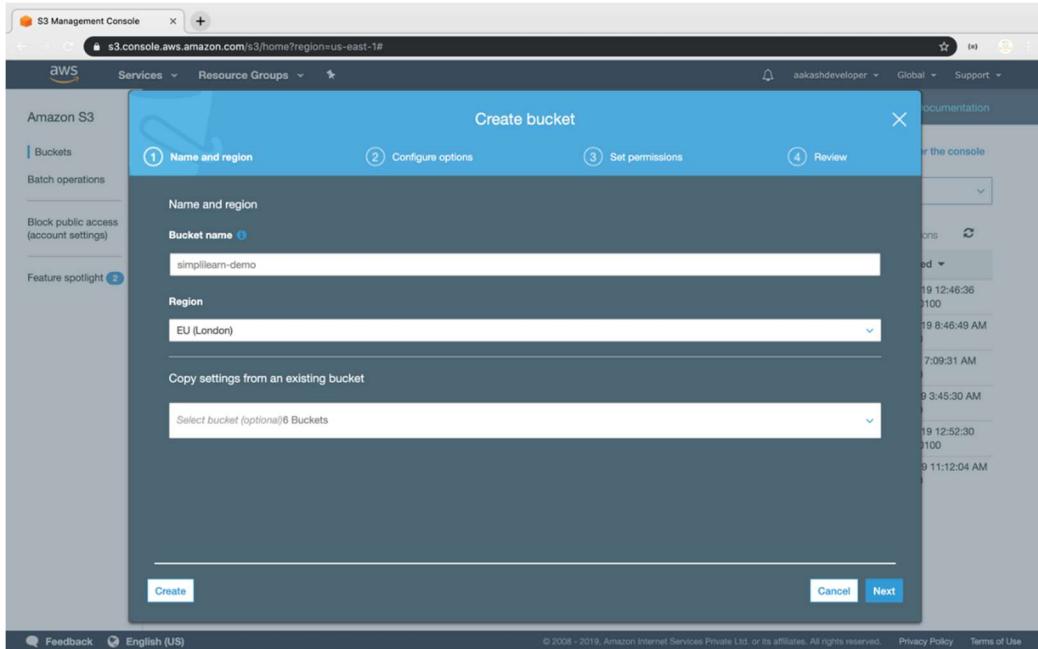
Step 2: Verifying the button to create a bucket

The screenshot shows the AWS S3 Management Console. The left sidebar has links for Amazon S3 (Buckets, Batch operations, Block public access (account settings)), Feature spotlight (2), and a Feedback link. The main area is titled "Amazon S3 Block Public Access lets you to enforce a no public access policy for your accounts & buckets. Learn more »". It features a "Discover the console" button. Below is a search bar and a dropdown for "All access types". A table lists 6 Buckets across 1 Region. The table includes columns for Bucket name, Access, Region, and Date created. The "Create bucket" button is located at the top left of the table area. The table data is as follows:

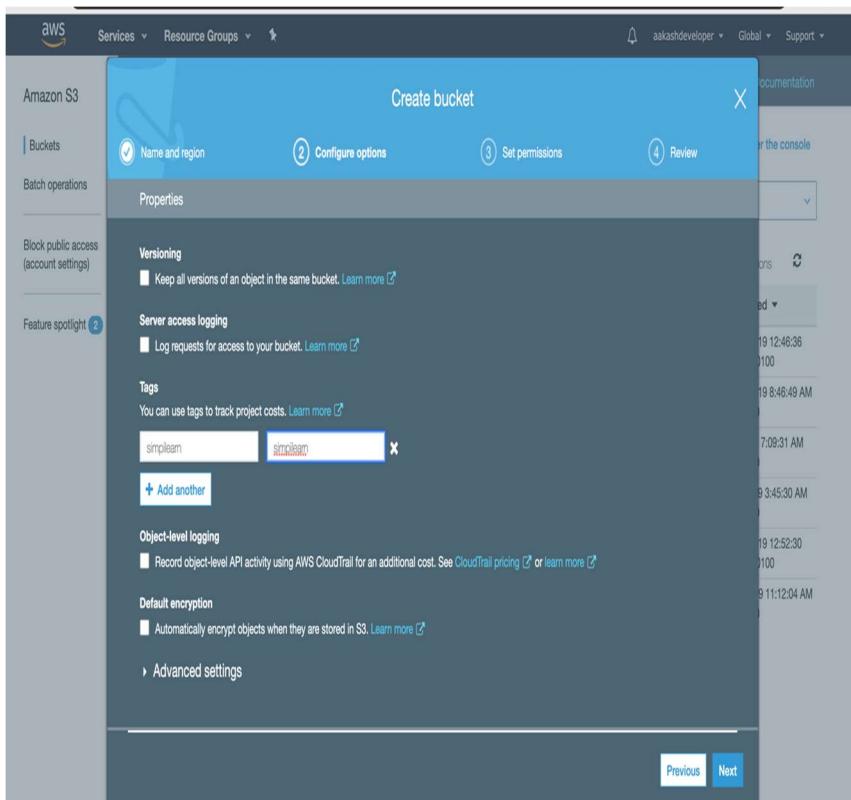
Bucket name	Access	Region	Date created
cf-templates-i6libjdtujm9-us-east-1	Objects can be public	US East (N. Virginia)	Aug 12, 2019 12:46:36 PM GMT+0100
codepipeline-us-east-1-531814118463	Objects can be public	US East (N. Virginia)	Aug 12, 2019 8:46:49 AM GMT+0100
elasticbeanstalk-us-east-1-651759643195	Objects can be public	US East (N. Virginia)	Jul 6, 2019 7:09:31 AM GMT+0100
projectsubmissions3	Objects can be public	US East (N. Virginia)	Aug 4, 2019 3:45:30 AM GMT+0100
s3edurekacf-edurekacf-1m5tvozw1sj3f	Objects can be public	US East (N. Virginia)	Aug 12, 2019 12:52:30 PM GMT+0100
simongameedureka	Objects can be public	US East (N. Virginia)	Jul 22, 2019 11:12:04 AM GMT+0100

### Step 3: Providing a bucket name and region

- Make sure that the bucket name is unique



### Step 4: Entering key and value for identification and tracking the bucket



### Step 5: Blocking all the public access

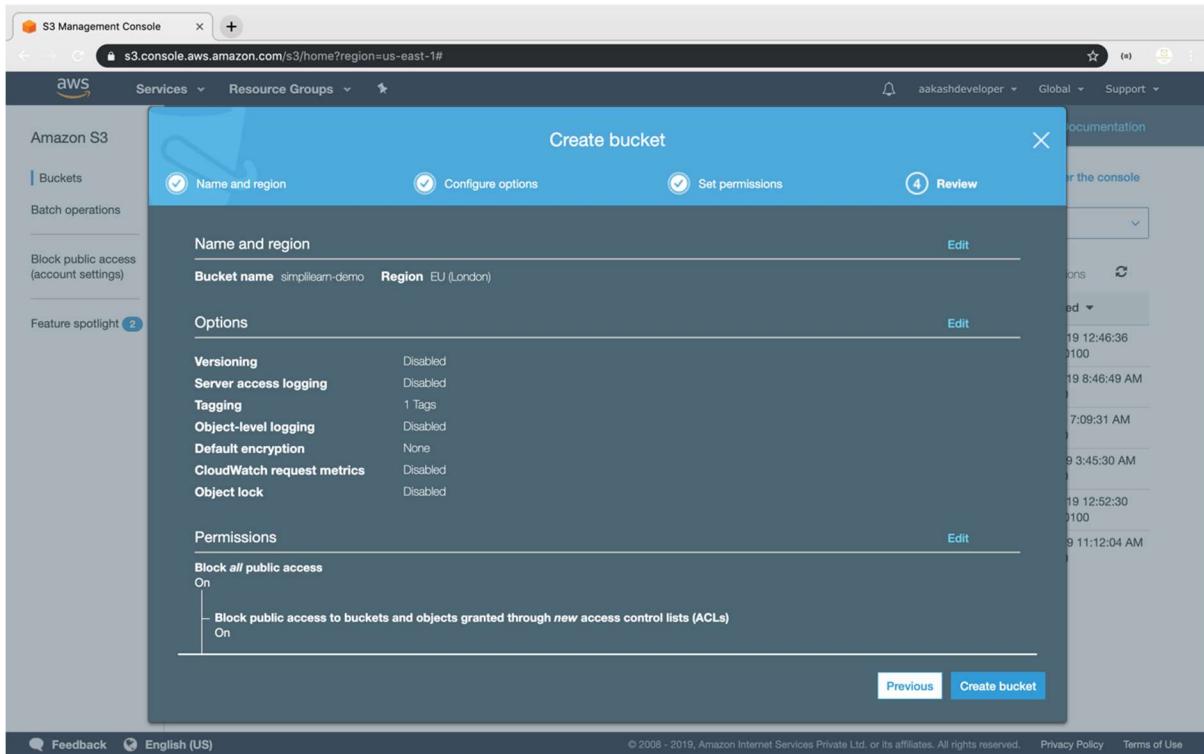
- If required, you can configure it later

The screenshot shows the AWS S3 Management Console interface for creating a new bucket. The top navigation bar includes the AWS logo, services dropdown, resource groups, user profile (akashdeveloper), global settings, and support links. The main title is "Create bucket". The current step is "3 Set permissions". A note at the top says: "Note: You can grant access to specific users after you create the bucket." Below this, the "Block public access (bucket settings)" section is active, indicated by a blue background. It contains four checkboxes:
 

- Block all public access: Description: 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): Description: 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): Description: 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 policies: Description: S3 will block new bucket 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 policies: Description: S3 will ignore public and cross-account access for buckets with policies that grant public access to buckets and objects.

 At the bottom right of the wizard, there are "Previous" and "Next" buttons. The "Next" button is highlighted in blue, indicating the next step in the process.

### Step 6: Reviewing all parameters and creating the bucket



## Step 7: Verifying the newly created bucket on the panel of S3

Screenshot of the AWS S3 Management Console showing the 'S3 buckets' list. Buckets: cf-templates-i6libjdtujm9-us-east-1, codepipeline-us-east-1-531814118463, elasticbeanstalk-us-east-1-65195643195, projectsubmissions3, s3edurekacf-edurekacf-1m5tvozw1sj3f, simplilearn-demo. Simplilearn-demo is highlighted.

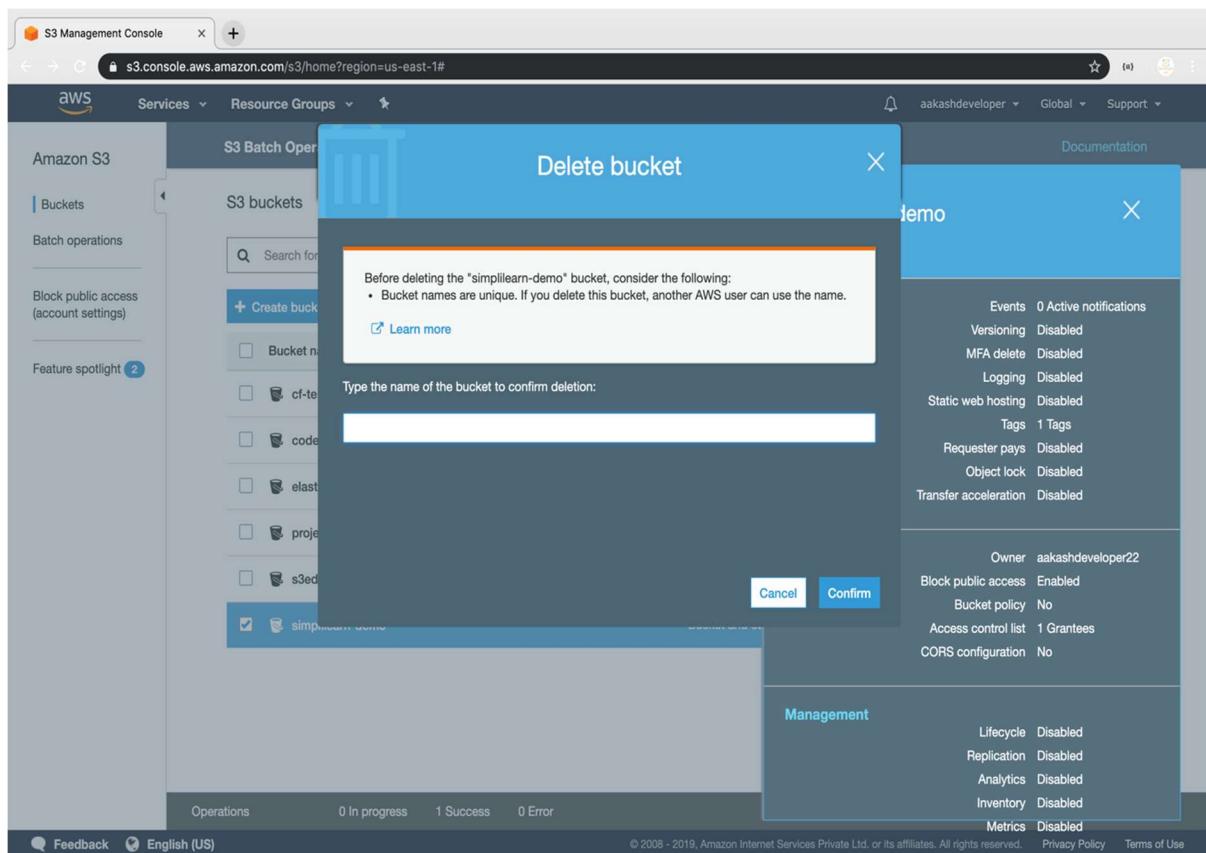
# 12. Delete an S3 Bucket.

Step 1: Selecting the S3 bucket you want to delete

- Choose the bucket

The screenshot shows the AWS S3 Management Console interface. On the left, there's a sidebar with options like 'Buckets', 'Batch operations', 'Block public access (account settings)', and 'Feature spotlight'. The main area is titled 'S3 buckets' and contains a search bar and buttons for '+ Create bucket', 'Edit public access settings', 'Empty', and 'Delete'. A list of buckets is displayed, with 'simplilearn-demo' selected, indicated by a blue background. To the right, a detailed view of the selected bucket is shown in a modal window. The modal has tabs for 'Properties', 'Permissions', and 'Management'. Under 'Properties', it shows details like 'Events 0 Active notifications', 'Versioning Disabled', etc. Under 'Permissions', it shows 'Owner aakashdeveloper22', 'Block public access Enabled', etc. Under 'Management', it shows 'Lifecycle Disabled', 'Replication Disabled', etc. At the bottom of the modal, there's a 'Copy Bucket ARN' button. The footer of the page includes links for 'Feedback', 'English (US)', and copyright information: '© 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use'.

Step 2: Deleting the bucket



# 13. Set the Storage Class of an Object.

## Step 1: Selecting the bucket

- Select the bucket and open the list of items

The screenshot shows the AWS S3 Management Console interface. At the top, the URL is s3.console.aws.amazon.com/s3/buckets/projectsubmissions3?region=us-east-1&tab=overview. The navigation bar includes 'Services', 'Resource Groups', and 'Global'. The user 'akashdeveloper' is logged in. The main area shows the 'Overview' tab selected. A search bar at the top says 'Type a prefix and press Enter to search. Press ESC to clear.' Below it are buttons for 'Upload', 'Creates folder', 'Download', and 'Actions'. The storage region is set to 'US East (N. Virginia)'. The table lists two objects:

Name	Last modified	Size	Storage class
Polling Git.docx	Sep 25, 2019 9:24:19 AM GMT+0100	322.6 KB	One Zone-IA
elasticbeanstalk-us-east-1-651759643195_frequent.csv	Sep 25, 2019 7:17:11 AM GMT+0100	2.6 KB	Standard

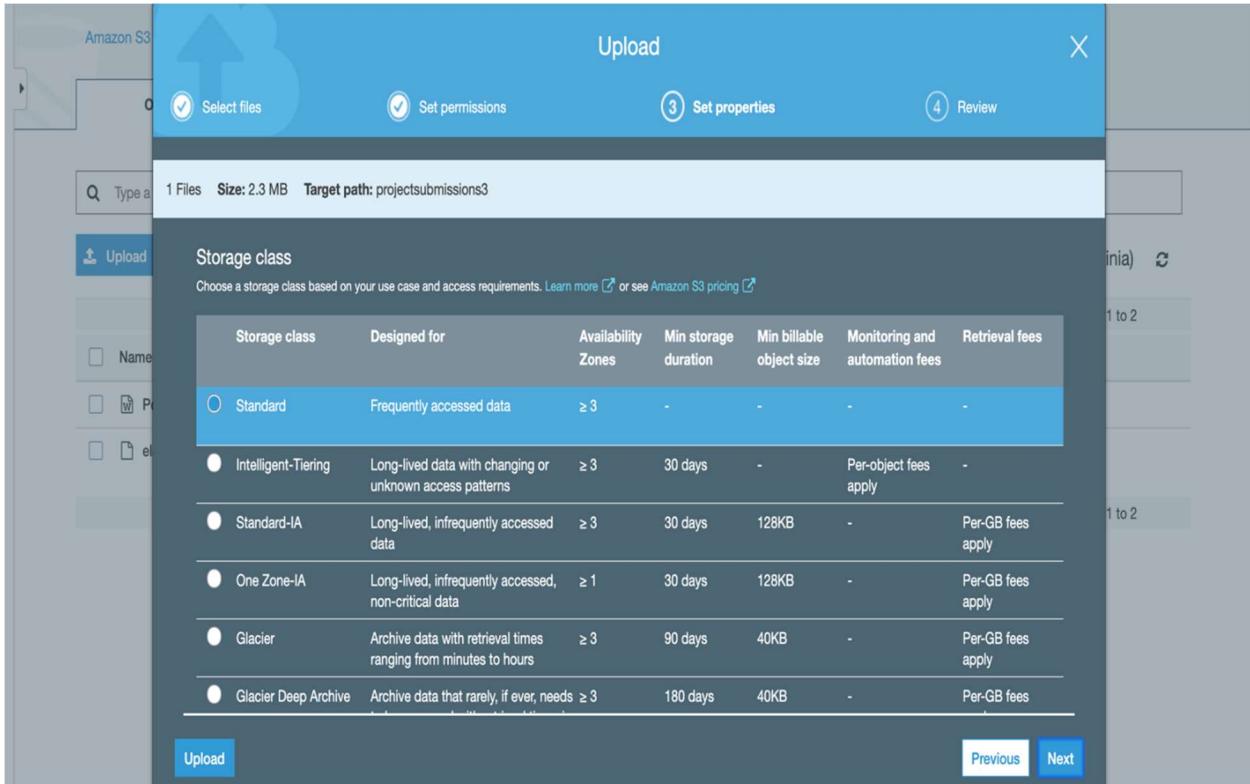
At the bottom, there's an 'Operations' summary: 0 In progress, 1 Success, 0 Error. The footer includes links for 'Feedback', 'English (US)', and copyright information: © 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use.

## Step 2: Setting the storage class of an object

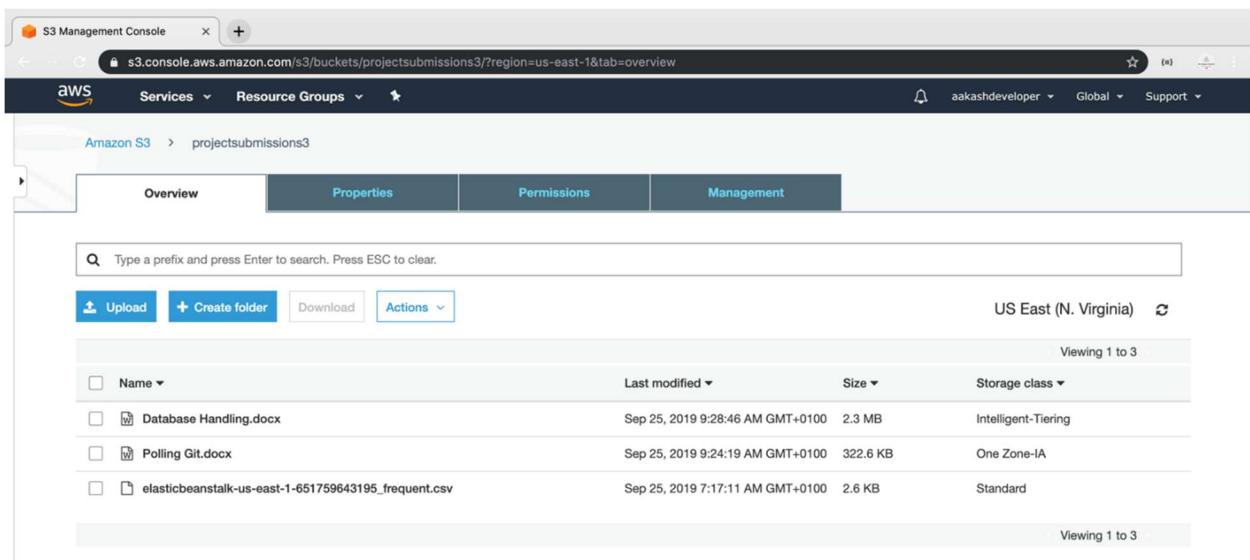
- Click on *Upload* and select the file and click *Next*

The screenshot shows the 'Upload' dialog box over the S3 Management Console. The dialog has four steps: 1. Select files, 2. Set permissions, 3. Set properties, 4. Review. Step 1 is active, showing '1 Files Size: 2.3 MB Target path: projectsubmissions3'. A file named 'Database Handling.docx' (2.3 MB) is selected. Step 2, 'Set permissions', is shown below with a note: 'To upload a file larger than 160 GB, use the AWS CLI, AWS SDK, or Amazon S3 REST API. Learn more' and a link '+ Add more files'. The background shows the S3 bucket list with the same two objects as before.

- Select the class and click *Next*



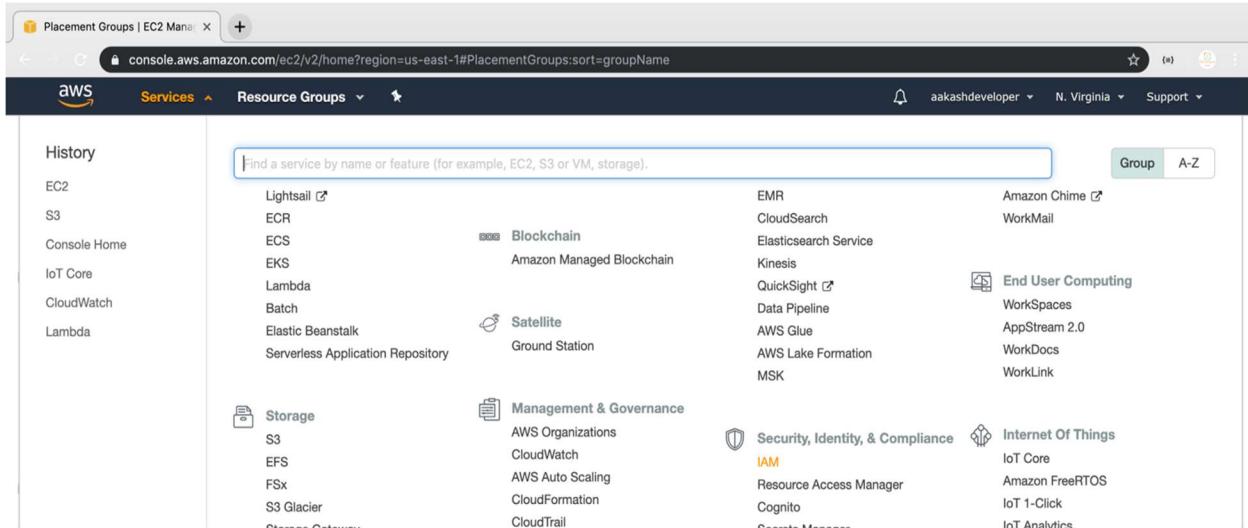
- The class will get assigned to the uploaded object



# 14.Create an IAM User.

## Step 1: Selecting the IAM from the AWS console

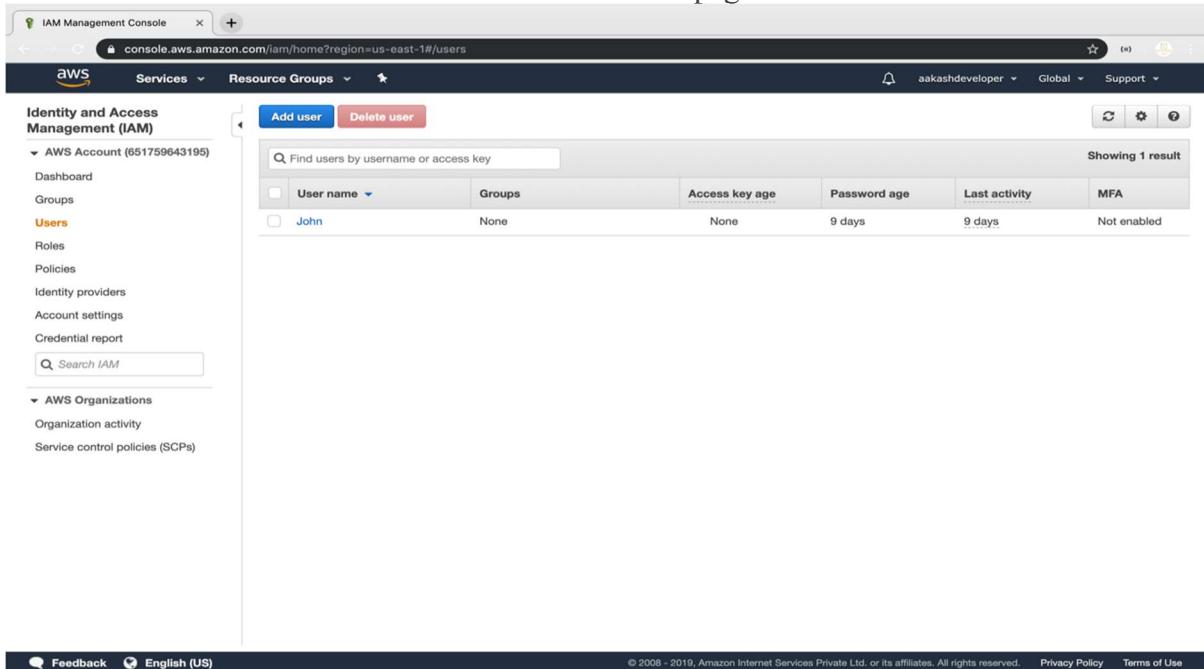
- Login to your AWS console and search for IAM



The screenshot shows the AWS EC2 Management Console. At the top, there's a search bar with placeholder text "Find a service by name or feature (for example, EC2, S3 or VM, storage)." Below the search bar, there's a navigation bar with tabs for "Services" and "Resource Groups". On the left, there's a sidebar with links to various services like EC2, S3, and Lambda. The main area displays a grid of service icons and names. Some services have additional details or links below them. A "Group" button and an "A-Z" link are visible in the top right corner of the main content area.

## Step 2: Navigate to the user creation page

- Click on Users to redirect to the user creation page to create IAM users



The screenshot shows the AWS IAM Management Console. At the top, there's a search bar with placeholder text "Find users by username or access key". Below the search bar, there's a navigation bar with tabs for "Add user" and "Delete user". On the left, there's a sidebar with links to "Identity and Access Management (IAM)" (which is expanded to show "AWS Account (651759643195)", "Dashboard", "Groups", "Users" which is selected and highlighted in orange, "Roles", "Policies", "Identity providers", "Account settings", and "Credential report"), "AWS Organizations" (which is expanded to show "Organization activity" and "Service control policies (SCPs)"), and a search bar labeled "Search IAM". The main area displays a table titled "Showing 1 result" with one row containing a user named "John". The columns in the table are "User name", "Groups", "Access key age", "Password age", "Last activity", and "MFA". The "User name" column shows "John", "Groups" shows "None", "Access key age" shows "None", "Password age" shows "9 days", "Last activity" shows "9 days", and "MFA" shows "Not enabled".

### Step 3: Changing access permissions

- Add username in the **User name\*** section. Select **AWS Management Console access** and select one of the ways to configure **console password**

The screenshot shows the 'Set user details' step of the IAM user creation wizard. The 'User name\*' field contains 'SimplilearnUser'. Under 'Select AWS access type', the 'AWS Management Console access' option is selected. In the 'Console password\*' section, 'Custom password' is chosen, and a password is entered. The 'Require password reset' checkbox is checked. At the bottom, there are 'Cancel' and 'Next: Permissions' buttons.

- Either we can add user to the created group or we can add policy as shown below:

The screenshot shows the 'Set permissions' step of the IAM user creation wizard. Under 'Add user to group', the 'devs' group is selected. In the 'Attached policies' table, 'AmazonEC2FullAccess' is listed. At the bottom, there are 'Cancel', 'Previous', and 'Next: Tags' buttons.

- In case a user needs to add a policy first, then he or she needs to search and then add policy to the user

The screenshot shows the 'Add user' wizard in the IAM Management Console. Step 2 is 'Set permissions'. The 'Attach existing policies directly' button is highlighted. A search bar filters results for 'Ec2'. A table lists policies, with one row for 'AmazonEC2ContainerRegistryFullAccess' selected. Step 3, 'Set permissions boundary', is visible below.

#### Step 4: Adding an identifier

- Add an identifier by adding key and value to tag each user as shown below:

The screenshot shows the 'Add tags (optional)' step of the 'Add user' wizard. A table lists a single tag: 'Ec2' with 'Ec2Admin' as its value. A note at the bottom indicates you can add up to 49 more tags.

- Finally, it will create a user with a group or an added policy

**Review**

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

**User details**

User name	SimplilearnUser
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

**Permissions summary**

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AmazonEC2ContainerRegistryFullAccess

**Tags**

The new user will receive the following tag

Key	Value
Ec2	Ec2Admin

**Create user**

- On successful user creation, a URL will be created with which a user can login as an IAM user

**Success**

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://651759643195.signin.aws.amazon.com/console>

**Download .csv**

User	Email login instructions
SimplilearnUser	<a href="#">Send email</a>

**Close**

- The newly created user will be available on the dashboard as shown below:

User name	Groups	Access key age	Password age	Last activity	MFA
John	None	None	9 days	9 days	Not enabled
SimplilearnUser	None	None	Today	None	Not enabled

- By clicking on each user, you can see the key sign in the URL

**Summary**

User ARN: arn:aws:iam::651759643195:user/SimplilearnUser

Path: /

Creation time: 2019-09-21 19:45 UTC+0100

**Security credentials**

Console sign-in link: <https://651759643195.signin.aws.amazon.com/console>

Console password: Enabled (never signed in) | Manage

Assigned MFA device: Not assigned | Manage

Signing certificates: None

**Access keys**

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. [Learn more](#)

**Create access key**

Access key ID	Created	Last used	Status
No results			

**SSH keys for AWS CodeCommit**

- By selecting a user, you can add that user to a particular group

The screenshot shows the AWS IAM Management Console interface. On the left, there's a navigation sidebar with options like Dashboard, Groups, Users (which is selected), Roles, Policies, Identity providers, Account settings, Credential report, and a search bar. The main content area is titled 'Summary' for a user named 'SimplilearnUser'. It displays the User ARN (arn:aws:iam::651759643195:user/SimplilearnUser), Path (/), and Creation time (2019-09-21 19:45 UTC+0100). Below this, there are tabs for Permissions, Groups (which is active), Tags (!), Security credentials, and Access Advisor. A prominent blue button labeled 'Add user to groups' is visible. Under the 'Groups' tab, there's a table with two columns: 'Group name' and 'Attached permissions'. The table shows 'No results'. At the bottom of the page, the URL https://console.aws.amazon.com/iam/home?region=us-east-1#/users/SimplilearnUser\$addToGroups?section=groups is displayed along with copyright information and links to Privacy Policy and Terms of Use.

# 15. Create an IAM Role.

## Step 3.16.1: Creating an IAM role

- In the IAM panel, click on *Roles* -> *Create role*

The screenshot shows the AWS IAM Management Console. On the left, there's a sidebar with navigation links: Identity and Access Management (IAM), AWS Account (651759643195), Dashboard, Groups, Users, Roles (which is selected and highlighted in orange), Policies, Identity providers, Account settings, and Credential report. Below these is a search bar labeled "Search IAM". Under "AWS Organizations", there are links for Organization activity and Service control policies (SCPs). The main content area has a heading "Additional resources:" with links to IAM Roles FAQ, Documentation, and a tutorial. Below this is a table titled "Create role" with a "Delete role" button. The table has columns for "Role name", "Description", and "Trusted entities". It lists 25 results, including "admin", "aws-elasticbeanstalk-ec2-role", "aws-elasticbeanstalk-service-role", and various AWS service roles like "lambda", "ec2", "elasticbeanstalk", "codepipeline", "autoscaling", "events", "elasticache", "elasticloadbalancing", and "rds". At the bottom of the table, there's a note: "Allows Amazon RDS to manage AWS resources on your behalf." The URL in the address bar is <https://console.aws.amazon.com/iam/home?region=us-east-1#/roles>.

- Select the service

The screenshot shows the "Create role" wizard, step 1: "Select the service". The top navigation bar includes "Services", "Resource Groups", and "Create role" (highlighted in blue). Below the navigation are four tabs: "AWS service" (selected), "Another AWS account", "Web identity", and "SAML 2.0 federation". A note below the tabs says "Allows AWS services to perform actions on your behalf. [Learn more](#)". The next section, "Choose the service that will use this role", shows two options: "EC2" and "Lambda". "EC2" is selected and described as "Allows EC2 instances to call AWS services on your behalf.". "Lambda" is described as "Allows Lambda functions to call AWS services on your behalf.". Below these are tables of services:

API Gateway	Comprehend	ElasticCache	Lambda	S3
AWS Backup	Config	Elastic Beanstalk	Lex	SMS
AWS Support	Connect	Elastic Container Service	License Manager	SNS
Amplify	DMS	Elastic Transcoder	Machine Learning	SWF
AppSync	Data Lifecycle Manager	Elastic Load Balancing	Macie	SageMaker
Application Auto Scaling	Data Pipeline	Forecast	MediaConvert	Security Hub
Application Discovery Service	DataSync	Global Accelerator	Migration Hub	Service Catalog
Batch	DeepLens	Glue	OpsWorks	Step Functions
CloudFormation	Directory Service	Greengrass	Personalize	Storage Gateway
DynamoDB	GuardDuty	IQOR	Textract	

At the bottom, there are buttons for "\* Required", "Cancel", and "Next: Permissions".

### Step 3.16.2: Adding AWS policy to the role

The screenshot shows the 'Create role' wizard in the IAM Management Console. Step 2, 'Attach permissions policies', is active. A search bar at the top right is set to 'Q: S3'. Below it is a table titled 'Showing 5 results' with columns 'Policy name', 'Used as', and 'Description'. The 'AmazonS3FullAccess' policy is selected, indicated by a blue checkmark next to its checkbox.

Policy name	Used as	Description
AmazonDMSRedshiftS3Role	None	Provides access to manage S3 settings ...
AmazonS3FullAccess	Permissions policy (3)	Provides full access to all buckets via th...
AmazonS3ReadOnlyAccess	None	Provides read only access to all buckets ...
QuickSightAccessForS3StorageManagement...	None	Policy used by QuickSight team to acce...
s3cr_for_julyswssession_to_testwebsites312	Permissions policy (1)	

### Step 3.16.3: Providing a key and a value for the role

- Add a key and a value to the role

The screenshot shows the 'Create role' wizard in the IAM Management Console. Step 3, 'Add tags (optional)', is active. A table titled 'Add tags (optional)' shows one tag entry: 'Key' is 'Ec2 access S3' and 'Value (optional)' is 'Ec2 access S3'. A note at the bottom states 'You can add 49 more tags.'

Key	Value (optional)	Remove
Ec2 access S3	Ec2 access S3	x

- Add a role:

Create role

Review

Provide the required information below and review this role before you create it.

Role name*	Ec2access3
Use alphanumeric and '+=_,@-_.' characters. Maximum 64 characters.	
Role description	Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and '+=_,@-_.' characters.	
Trusted entities	AWS service: ec2.amazonaws.com
Policies	AmazonS3FullAccess
Permissions boundary	Permissions boundary is not set
The new role will receive the following tag	
Key	Value
Ec2 access S3	Ec2 access S3

\* Required

Cancel Previous Create role

Feedback English (US) © 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

- Once the role is created, you can find it in the IAM panel

Identity and Access Management (IAM)

AWS Account (651759643195)

Role name	Description	Trusted entities
aws-elasticbeanstalk-ec2-role	AWS service: ec2	
Ec2access3	Allows EC2 instances to call AWS services on your behalf.	AWS service: ec2
ec2accessS3	Allows EC2 instances to call AWS services on your behalf.	AWS service: ec2

Showing 3 results

Search IAM

Feedback English (US) © 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

# 16. Create an IAM Group.

## Step 1: Creating an IAM group

- In the IAM panel, click on *Groups*, and you will land on the *Create New Group* page

The screenshot shows the AWS IAM Management Console. The left sidebar has 'Identity and Access Management (IAM)' selected. Under 'AWS Account (651759643195)', 'Groups' is highlighted. The main area shows a table with one result: 'devs' under 'Group Name', '0' under 'Users', and '2019-09-12 10:18 UTC+0100' under 'Creation Time'. A 'Create New Group' button is at the top left of the main area.

- Enter the group name

The screenshot shows the 'Create New Group Wizard' with 'Step 1 : Group Name' selected. The title is 'Set Group Name'. It says 'Specify a group name. Group names can be edited any time.' Below is a 'Group Name:' field containing 'simplearn'. A note says 'Example: Developers or ProjectAlpha' and 'Maximum 128 characters'. At the bottom are 'Cancel' and 'Next Step' buttons.

## **Step 2:** Assigning the required policy to the group

- Assign the policy provided by AWS

IAM Management Console

console.aws.amazon.com/iam/home?region=us-east-1#groups

aakashdeveloper Global Support

## Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

### Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

	Policy Name	Attached Entities	Creation Time	Edited Time
<input checked="" type="checkbox"/>	AmazonS3FullAccess	3	2015-02-06 18:40 UTC+0100	2015-02-06 18:40 UTC+0100
<input type="checkbox"/>	AmazonDMSVPCManagementRole	1	2015-11-18 16:33 UTC+0100	2016-05-23 17:29 UTC+0100
<input type="checkbox"/>	AmazonEC2ContainerRegistryFullAccess	1	2015-12-21 17:06 UTC+0100	2017-11-10 17:54 UTC+0100
<input checked="" type="checkbox"/>	AmazonEC2FullAccess	1	2015-02-06 18:40 UTC+0100	2018-11-27 02:16 UTC+0100
<input type="checkbox"/>	AWSCodePipelineServiceRole-unique-1	1	2019-08-12 08:46 UTC+0100	2019-08-12 08:46 UTC+0100
<input type="checkbox"/>	AWSCodePipelineServiceRole-unique-2	1	2019-08-12 10:48 UTC+0100	2019-08-12 10:48 UTC+0100
<input type="checkbox"/>	AWSCodePipelineServiceRole-unique-3	1	2019-08-26 16:10 UTC+0100	2019-08-26 16:10 UTC+0100
<input type="checkbox"/>	AWSElasticBeanstalkEnhancedHealthCheckPolicy	1	2016-02-08 23:17 UTC+0100	2018-04-09 23:12 UTC+0100
<input type="checkbox"/>	AWSElasticBeanstalkMulticontainerHealthCheckPolicy	1	2016-02-08 23:15 UTC+0100	2016-06-07 00:45 UTC+0100
<input type="checkbox"/>	AWSElasticBeanstalkService	1	2016-04-11 21:27 UTC+0100	2019-06-15 00:18 UTC+0100
<input type="checkbox"/>	AWSElasticBeanstalkWebTier	1	2016-02-08 23:08 UTC+0100	2019-03-01 00:04 UTC+0100
<input type="checkbox"/>	AWSElasticBeanstalkWorkerTier	1	2016-02-08 23:12 UTC+0100	2019-03-01 00:07 UTC+0100
<input type="checkbox"/>	AWSLambdaBasicExecutionRole	1	2019-08-27 10:39 UTC+0100	2019-08-27 10:39 UTC+0100
<input type="checkbox"/>	AWSLambdaBasicExecutionRole	1	2019-08-04 05:47 UTC+0100	2019-08-04 05:47 UTC+0100

Showing 481 results

[Cancel](#) [Previous](#) [Next Step](#)

- Once the group is created, you can see the new group in the console

The screenshot shows the AWS IAM Management Console with the URL [console.aws.amazon.com/iam/home?region=us-east-1#/groups](https://console.aws.amazon.com/iam/home?region=us-east-1#/groups). The left sidebar navigation includes 'Identity and Access Management (IAM)', 'AWS Account (651759643195)', 'Groups' (selected), 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Credential report', and a search bar. The main content area displays a table titled 'Showing 2 results' with columns: Group Name, Users, Inline Policy, and Creation Time. Two groups are listed: 'devs' (Creation Time: 2019-09-12 10:18 UTC+0100) and 'simplearn' (Creation Time: 2019-09-21 19:49 UTC+0100). The bottom of the screen shows standard AWS footer links: Feedback, English (US), © 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved., Privacy Policy, and Terms of Use.

- You can add a user or a policy to the group any time

The screenshot shows the AWS IAM Management Console with the URL [console.aws.amazon.com/iam/home?region=us-east-1#/groups/simplearn](https://console.aws.amazon.com/iam/home?region=us-east-1#/groups/simplearn). The left sidebar navigation is identical to the previous screenshot. The main content area shows the 'Summary' section for the 'simplearn' group. It displays the Group ARN: `arn:aws:iam::651759643195:group/simplearn`, Users (in this group): 0, Path: /, and Creation Time: 2019-09-21 19:49 UTC+0100. Below this, there are tabs for 'Users' (selected), 'Permissions', and 'Access Advisor'. A message states: '⚠ This group does not contain any users.' followed by a blue 'Add Users to Group' button. The bottom of the screen shows the standard AWS footer links.

- You can see the user list by clicking on *Add User*

User Name	Groups	Password	Password Last Used	Access Keys	Creation Time
John	0	✓	2019-09-12 10:15 UTC+0100	None	2019-09-12 10:13 UT...
SimplilearnUser	0	✓	Never	None	2019-09-21 19:45 UT...

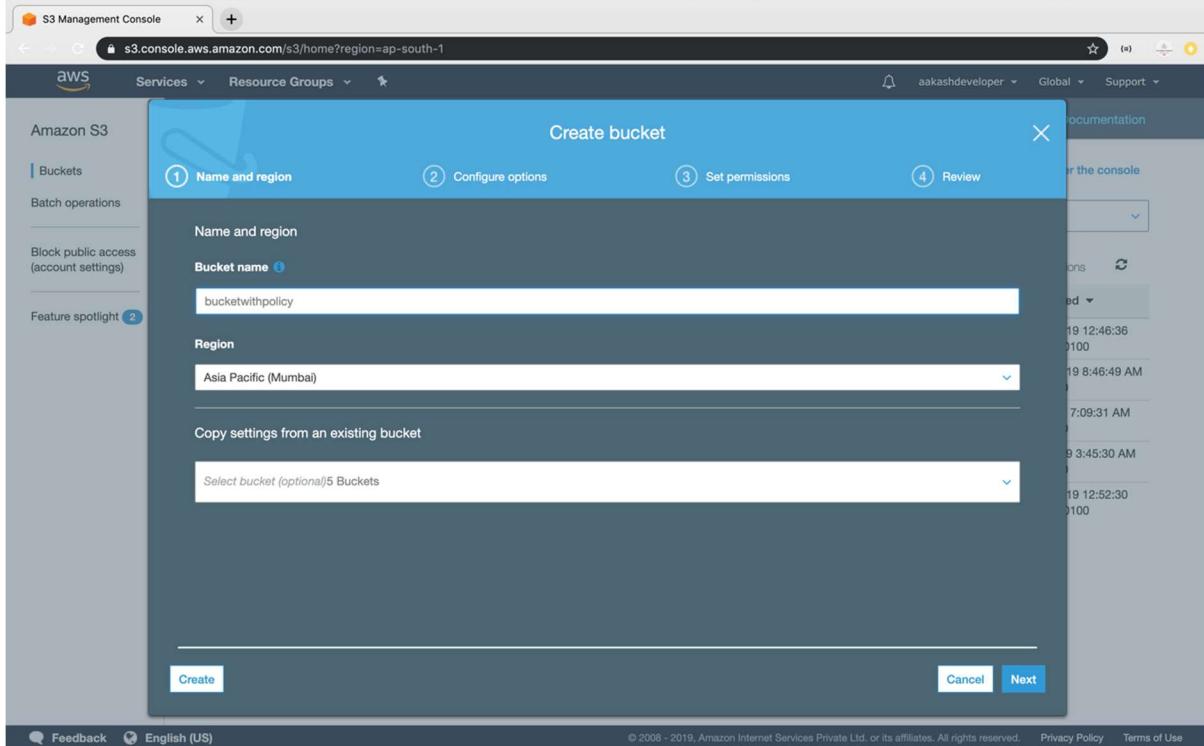
- You can also find all the policies added to the group

User	Actions
SimplilearnUser	<a href="#">Remove User from Group</a>

# 17. Policies and Permissions.

## Step 1: Creating a bucket

- Create a new bucket in which we want to add policy with all default settings.



- Click on the *Permission* section.
- Go to *Bucket Policy*.
- It will open the console where you can add policy.

## Step 2: Adding policies

- Click on the *Policy Generator*.

Bucket policy editor ARN: arn:aws:s3:::bucketwithpolicyname

Type to add a new policy or edit an existing policy in the text area below.

Granting public access in this policy will be blocked because Block public access settings are turned on for this bucket. To determine which settings are turned on, check your Block public access settings.

1

Delete Cancel Save

Documentation Policy generator

<https://awspolicygen.s3.amazonaws.com/policygen.html>

© 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

- Select the type of policy and services required.

AWS Policy Generator

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

**Step 1: Select Policy Type**

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

Select Type of Policy S3 Bucket Policy

**Step 2: Add Statement(s)**

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

Effect  Allow  Deny

Principal

Use a comma to separate multiple values.

AWS Service  Amazon S3  All Services (\*)

Actions 1 Action(s) Selected  AbortMultipartUpload  All Actions (\*)

Amazon Resource Name (ARN)

CreateBucket  CreateJob  DeleteBucket  DeleteBucketPolicy  DeleteBucketWebsite  DeleteObject  DeleteObjectTagging

:<bucket\_name>/<key\_name>, [more Principals](#).

**Step 3: Generate Policy**

- Add ARN for S3 to add the policy.

**AWS Policy Generator**

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

**Step 1: Select Policy Type**  
A Policy is a container for permissions. The different types of policies you can create are an **IAM Policy**, an **S3 Bucket Policy**, an **SNS Topic Policy**, a **VPC Endpoint Policy**, and an **SQS Queue Policy**.

**Select Type of Policy**: S3 Bucket Policy

**Step 2: Add Statement(s)**  
A statement is the formal description of a single permission. See a [description of elements](#) that you can use in statements.

**Effect**:  Allow    Deny

**Principal**: Allow Creation  
Use a comma to separate multiple values.

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

**Actions**: 1 Action(s) Selected    All Actions ('\*')

**Amazon Resource Name (ARN)**: arn:aws:s3:::bucketwithpolicyname  
ARN should follow the following format: arn:aws:s3:::<bucket\_name>/<key\_name>. Use a comma to separate multiple values.

**Add Conditions (Optional)**

**Add Statement**

**Step 3: Generate Policy**

- Click on policy generator to create the JSON of the policy.

**Step 3: Generate Policy**  
A **policy** is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

Principal(s)	Effect	Action	Resource	Conditions
Allow Creation	Allow	s3:CreateBucket	arn:aws:s3:::bucketwithpolicyname	None

You added the following statements. Click the button below to Generate a policy.

**Generate Policy**   **Start Over**

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided **as is** without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.  
An [amazon.com](#) company

- Copy the generated JSON.

The screenshot shows the AWS Policy Generator interface. At the top, there are fields for 'Effect' (Allow selected), 'Principal' (empty), and 'AWS Service' (Amazon S3 selected). Below these, a modal window titled 'Policy JSON Document' displays the following JSON code:

```
{
  "Id": "Policy1569841158572",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1569841151862",
      "Action": [
        "s3:CreateBucket"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucketwithpolicyname",
      "Principal": {
        "AWS": [
          "Allow Creation"
        ]
      }
    }
  ]
}
```

Below the modal, a note says 'Step 3: A policy is a JSON document'. At the bottom right of the modal is a 'Close' button. The footer of the page includes a copyright notice for 2010, Amazon Web Services LLC or its affiliates, and a statement that the generator is provided 'as is' without warranty.

- Paste the JSON in the policy console of bucket and click on *Save*.

The screenshot shows the AWS S3 Bucket Policy editor. The top navigation bar includes 'Services', 'Resource Groups', and the user 'akashdeveloper'. The tabs at the top are 'Block public access', 'Access Control List', 'Bucket Policy' (selected), and 'CORS configuration'. The main area contains the following text:

Bucket policy editor ARN: arn:aws:s3:::bucketwithpolicyname  
Type to add a new policy or edit an existing policy in the text area below.

Granting public access in this policy will be blocked because Block public access settings are turned on for this bucket. To determine which settings are turned on, check your Block public access settings.

```

1  {
2    "Id": "Policy1569841158572",
3    "Version": "2012-10-17",
4    "Statement": [
5      {
6        "Sid": "Stmt1569841151862",
7        "Action": [
8          "s3:CreateBucket"
9        ],
10       "Effect": "Allow",
11       "Resource": "arn:aws:s3:::bucketwithpolicyname",
12       "Principal": {
13         "AWS": [
14           "Allow Creation"
15         ]
16       }
17     }
18   }
19 }
```

At the bottom right are 'Delete', 'Cancel', and 'Save' buttons. At the very bottom of the page are links for 'Documentation' and 'Policy generator'.

# 18. Empty an S3 Bucket.

Step 3.13.1: Selecting the S3 bucket you want to empty

The screenshot shows the AWS S3 Management Console. On the left, there's a sidebar with 'Amazon S3' and options like 'Buckets', 'Batch operations', 'Block public access (account settings)', and 'Feature spotlight'. The main area is titled 'S3 buckets' with a search bar. It lists several buckets: 'cf-templates-i6libjdtujm9-us-east-1', 'codepipeline-us-east-1-531814118463', 'elasticbeanstalk-us-east-1-651759643195', and 'projectsubmissions3'. The 'projectsubmissions3' bucket has a checked checkbox next to it. Below the list are buttons for '+ Create bucket', 'Edit public access settings', 'Empty', and 'Delete'. A modal window for 'projectsubmissions3' is open, showing its properties. The 'Properties' tab includes fields like 'Events' (0 Active notifications), 'Versioning' (Disabled), 'MFA delete' (Disabled), 'Logging' (Enabled), 'Static web hosting' (Enable website hosting), 'Tags' (0 Tags), 'Requester pays' (Disabled), 'Object lock' (Disabled), and 'Transfer acceleration' (Disabled). The 'Permissions' tab shows the owner as 'akashdeveloper22', and the 'Management' tab shows lifecycle, replication, analytics, inventory, and metrics settings. At the bottom, there are tabs for 'Operations' (0 In progress, 2 Success, 0 Error) and links for 'Feedback', 'English (US)', and copyright information.

Step 3.13.2: Emptying the bucket

- Verify the content present in the bucket

The screenshot shows the AWS S3 Management Console with the 'projectsubmissions3' bucket selected. The top navigation bar includes 'Services', 'Resource Groups', and 'Management'. The main area has tabs for 'Overview', 'Properties', 'Permissions', and 'Management'. The 'Overview' tab is active. It features a search bar, 'Upload', 'Create folder', 'Download', and 'Actions' buttons. The content area shows a table with one item: 'index.html'. The table has columns for 'Name', 'Last modified', 'Size', and 'Storage class'. The 'index.html' file was last modified on Aug 4, 2019, at 3:45:59 AM GMT+0100, is 132.0 B in size, and is stored in the 'Standard' storage class. There are also 'Viewing 1 to 1' and 'Viewing 1 to 1' status indicators at the bottom.

- Empty the bucket

