

## **Assisted Practice: 3.6 Launch and Connect to an EC2 Linux Instance**

This section will guide you to:

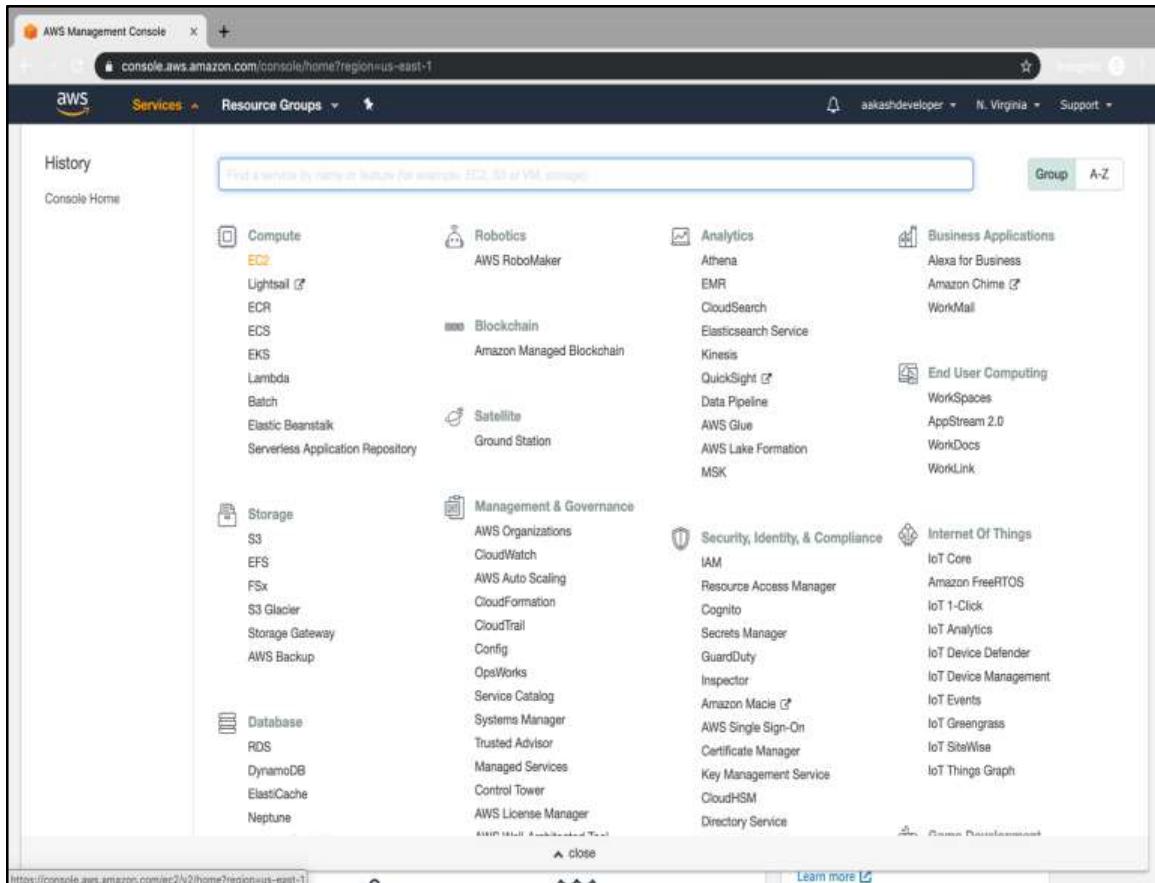
- Launch and connect to an EC2 instance

This lab has three subsections, namely:

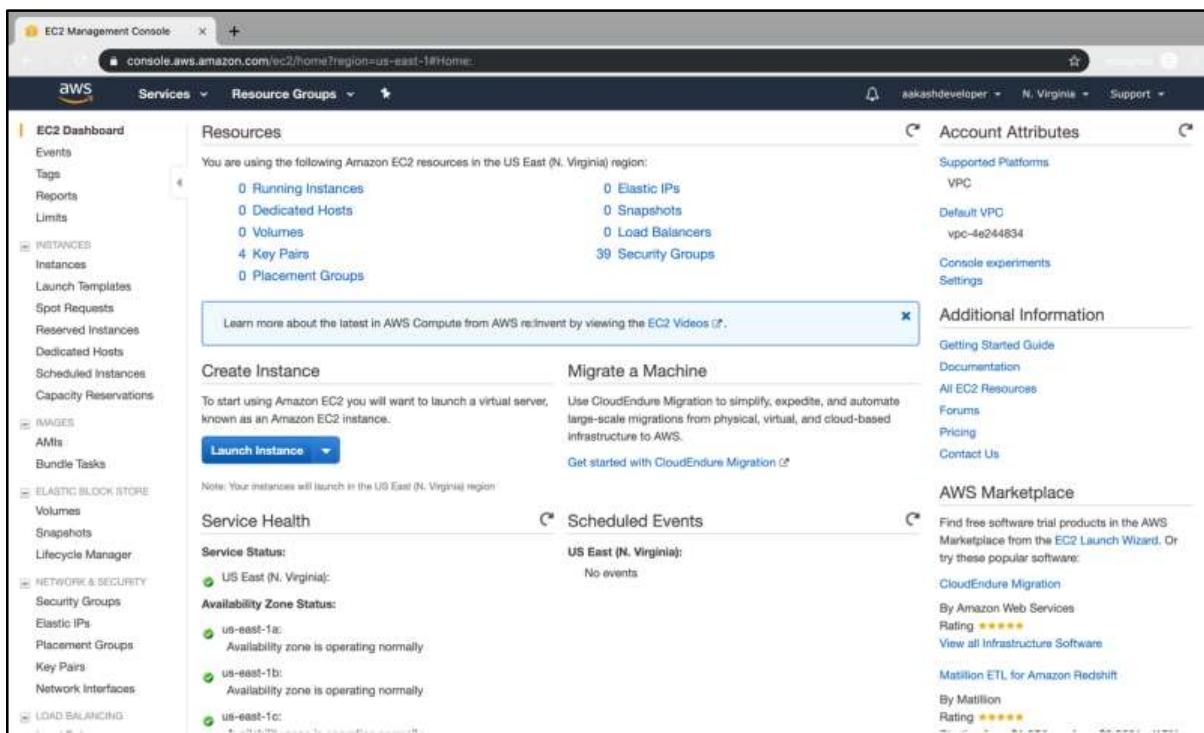
- 3.1.1 Launching an EC2 instance
- 3.1.2 Connecting to the EC2 instance
- 3.1.3 Pushing the files to GitHub repositories

**Step 3.1.1:** Launching an EC2 instance

- Go to Amazon dashboard
- Select EC2



- Click on *launch instance* to run any instance



- Select the AMI

**Step 1: Choose an Amazon Machine Image (AMI)**

Search for an AMI by entering a search term e.g. "Windows"

Image	Name	Description	Select
Amazon Linux	Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0b69ea66#7391e80 (64-bit x86) / ami-09c61c4850b7465cb (64-bit Arm)	Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.	<input checked="" type="button"/> Select 64-bit (x86) 64-bit (Arm)
Amazon Linux	Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-00eb20669e0990cb4	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.	<input checked="" type="button"/> Select 64-bit (x86)
Red Hat	Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-0c322300a1dd5dc79 (64-bit x86) / ami-03587fa4048e9eb92 (64-bit Arm)	Red Hat Enterprise Linux version 8 (HVM), EBS General Purpose (SSD) Volume Type	<input checked="" type="button"/> Select 64-bit (x86) 64-bit (Arm)
SUSE Linux	SUSE Linux Enterprise Server 15 SP1 (HVM), SSD Volume Type - ami-0b5372ab3202bd20b (64-bit x86) / ami-0072af0151fbe67b9 (64-bit Arm)	SUSE Linux Enterprise Server 15 Service Pack 1 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.	<input checked="" type="button"/> Select 64-bit (x86) 64-bit (Arm)

Feedback English (US) © 2006 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

- 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 (GB)	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) © 2006 - 2018, 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

**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](#)

- 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

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more about storage options in Amazon EC2.](#)

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

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

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

Add another tag (Up to 50 tags maximum)

Review and Launch

**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

Security group name: launch-wizard-25  
Description: launch-wizard-25 created 2019-09-21T06:50:43.598+01:00

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom <input type="text" value="0.0.0.0/0"/>	e.g. SSH for Admin Desktop <input type="button" value="X"/>
HTTP	TCP	80	Custom <input type="text" value="0.0.0.0/0,::/0"/>	e.g. SSH for Admin Desktop <input type="button" value="X"/>

[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

**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

**Security Groups**

Security group name: launch-wizard-25  
Description: launch-wizard-25 created 2019-09-21T06:50:43.598+01:00

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	

**Instance Details**

**Storage**

**Tags**

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

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

The screenshot shows the AWS Launch Instance wizard at Step 7: Review Instance Launch. The main page displays instance configuration details such as AMI, instance type (t2.micro), security groups, and network settings. A modal window titled "Select an existing key pair or create a new key pair" is open, showing options for creating a new key pair (selected) or choosing an existing one. It also includes a checkbox for acknowledging access to the private key file.

**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.

**Instance Type**

Instance Type	ECUs	vCPUs
t2.micro	Variable	1

**Security Groups**

Type	Protocol
SSH	TCP
HTTP	TCP
HTTP	TCP

**Select an existing key pair or create a new key pair**

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.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair  
 Create a new key pair  
 Proceed without a key pair

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.

**Launch Instances**

- The instance is ready to use

The screenshot shows the AWS EC2 Instances dashboard. On the left, there's a sidebar with navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, AMIs, and Elastic Block Store. The main content area displays a table of instances. A single row is selected, showing details for an instance named 'i-0ccb6d6e60f077cbc' which is a 't2.micro' type running in 'us-east-1b'. The Public DNS is listed as 'ec2-52-91-199-186.compute-1.amazonaws.com' and the IP address as '52.91.199.186'. Below the table, a detailed view for the selected instance is shown with tabs for Description, Status Checks, Monitoring, and Tags. The 'Description' tab is active, displaying the same information as the table.

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

The screenshot shows a terminal window with the following text:  
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
  _\   _/ ) Amazon Linux AMI
  _\ \_\_|
https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
3 package(s) needed for security, out of 7 available
Run "sudo yum update" to apply all updates.
-bash: warning: setlocale: LC_CTYPE: cannot change locale (UTF-8): No such file or directory
[ec2-user@ip-172-31-91-59 ~]$
```

### Step 3.1.2: 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
amzn-updates
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          1/5
  Installing : apr-util-1.5.4-6.18.amzn1.x86_64      2/5
  Installing : httpd-tools-2.2.34-1.16.amzn1.x86_64  3/5
  Installing : apr-util-ldap-1.5.4-6.18.amzn1.x86_64  4/5
  Installing : httpd-2.2.34-1.16.amzn1.x86_64       5/5
  Verifying   : httpd-tools-2.2.34-1.16.amzn1.x86_64  1/5
  Verifying   : apr-util-1.5.4-6.18.amzn1.x86_64      2/5
  Verifying   : httpd-2.2.34-1.16.amzn1.x86_64       3/5
  Verifying   : apr-1.5.2-5.13.amzn1.x86_64          4/5
  Verifying   : apr-util-ldap-1.5.4-6.18.amzn1.x86_64  5/5

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

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

```

- Enter / 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 ]
[root@ip-172-31-91-59 html]#
```



### **Step 3.1.3:** Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

**cd <folder path>**

- Initialize your repository using the following command:

**git init**

- Add all the files to your git repository using the following command:

**git add .**

- Commit the changes using the following command:

**git commit . -m "Changes have been committed."**

- Push the files to the folder you initially created using the following command:

**git push -u origin master**

## **Assisted Practice: 3.7 Change the Volume Size of an Instance**

This section will guide you to:

- Change the volume size of an instance

This lab has seven subsections, namely:

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

3.2.2 Validating the Availability zone of the EC2 instance with which you want to add volume

3.2.3 Providing type, size, availability zone, and snapshot name on the **create volume** tab

3.2.4 Selecting newly created volume and clicking on the action to attach the volume to the instance

3.2.5 Selecting the instance of the same availability zone and attaching the volume in pop

3.2.6 Verifying the instance by adding one more device to the block device

3.2.7 Pushing the code to GitHub repositories

**Note:** By default, when we create a new instance, we need to attach the minimum volume to the instance depending on the OS or AMI. But we can also add or remove the volume.

**Step 3.2.1:** 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 the EC2 service. The top navigation bar includes tabs for 'Your Repositories', 'React-AWS/Server.js', 'Reminder:React JS E...', 'GoToWebinar...', 'Demos\_from\_SME - G...', 'AWS\_Certified\_Dev...', and 'Volumes (EC2 Manager)'. The AWS logo is on the left, followed by 'Services' and 'Resource Groups' dropdown menus. A user profile for 'akashdeveloper' is shown on the right.

The main content area is titled 'Create Volume' and displays a table of volumes. The table has columns for Name, Volume ID, Size, Volume Type, IOPS, Snapshot, Created, Availability Zone, State, and Alarm Status. One volume is listed:

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone	State	Alarm Status
vol-0a786e19d090c3099	vol-0a786e19d090c3099	8 GB	gp2	100	snap-05a19c3...	September 21, 2019	us-east-1c	in-use	None

Below the table, a detailed view of the selected volume (vol-0a786e19d090c3099) is shown. The 'Volumes' tab is selected in the sidebar. The volume details are as follows:

Description	Status Checks	Monitoring	Tags
Volume ID: vol-0a786e19d090c3099	Size: 8 GB	Created: September 21, 2019 at 9:30:28 AM UTC+1	State: in-use
			Attachment information: i-07f602857b811d56a /dev/xvda (attached)
			Alarm status: None
			Snapshot: snap-05a19c3561bd794a
			Availability Zone: us-east-1c
			Encryption: Not Encrypted
			KMS Key ID: KMS Key ID

At the bottom, there are links for 'Feedback', 'English (US)', and legal notices: '© 2006 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.' and 'Privacy Policy | Terms of Use'.

**Step 3.2.2:** Validating the Availability zone of the EC2 instance with which you want to add volume

The screenshot shows the AWS EC2 Management console. The left sidebar is collapsed, and the main area displays a table of instances. One instance is listed:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
	i-071602837b831d86a	t2.micro	us-east-1c	running	2/2 checks ...	None	ec2-54-227-70-128.co...	54.227.70.128

Below the table, a detailed view for the selected instance (i-071602837b831d86a) is shown. The 'Description' tab is selected, displaying the following details:

Instance ID	Public DNS (IPv4)
i-071602837b831d86a	ec2-54-227-70-128.compute-1.amazonaws.com

Other tabs available in the description view include 'Status Checks', 'Monitoring', and 'Tags'. At the bottom of the page, there are links for 'Feedback', 'English (US)', and legal notices.

**Step 3.2.3:** Providing type, size, availability zone, and snapshot name on the **create volume** tab

Create Volume

Volume Type: General Purpose SSD (gp3) ?

Size (GB):  (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) ?

Availability Zone\*: us-east-1c ?

Throughput [MB/s]: Not applicable ?

Snapshot ID: Select a snapshot ?

Encryption:  Encrypt this volume

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)	<input type="button" value="Cancel"/>	<input type="button" value="Create Volume"/>

\* Required

Feedback English (US) © 2006 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

**Step 3.2.4:** 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' section selected. A context menu is open over a volume entry, with 'Attach Volume' highlighted. The main table lists two volumes: one available and one in-use.

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

**Actions** menu options shown in the context menu:

- Modify Volume
- Create Snapshot
- Delete Volume
- Attach Volume**
- Detach Volume
- Force Detach Volume
- Change Auto-Enable I/O Setting
- Add/Edit Tags

**Step 3.2.5:** Selecting the instance of the same availability zone and attaching the volume in pop

Screenshot of the AWS EC2 Management Console showing the Attach Volume dialog.

The left sidebar shows the navigation menu with the "Volumes" option selected under "Elastic Block Store".

The main content area displays a table of volumes:

Name	Volume ID	Size	Type	IOPS	Snapshot	Created	Availability Zone	Status	Alarm Status
vol-08837d7...	vol-08837d74e970201a4	2 GB	gp2	100		September 21, 201...	us-east-1c	available	None
vol-0a786ef...	vol-0a786ef05a19c3...	8 GB	gp2	100	anap-05a19c3...	September 21, 201...	us-east-1c	in-use	None

The "Attach Volume" dialog is open, showing the following fields:

- Volume: vol-08837d74e970201a4 in us-east-1c
- Instance: i-071602537c831c86a in us-east-1c
- Device: /dev/sdf

A note in the dialog states: "Note: Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdz internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp."

At the bottom of the dialog are "Cancel" and "Attach" buttons.

The volume details at the bottom of the page are:

Volume ID	Size	Created	Snapshot	Availability Zone	Encryption	KMS Key ID
vol-08837d74e970201a4	2 GB	September 21, 2019 at 9:44:52 AM UTC+1	-	us-east-1c	Not Encrypted	

**Step 3.2.6:** Verifying the instance by adding one more device to the block device

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with navigation links like Events, Tags, Reports, Limits, Instances (selected), Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, Images (AMIs), and Elastic Block Store (Volumes, Snapshots, Lifecycle Manager). The main content area has tabs for Launch Instance, Connect, and Actions. A search bar at the top right says "Filter by tags and attributes or search by keyword". Below it is a table with one row, showing details for an instance named i-07602337b631d86a. The instance is an i2.micro type, running in the us-east-1c availability zone, with a Public DNS of ec2-54-227-70-128.compute-1.amazonaws.com 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, there's a detailed view of the instance configuration, including fields like Platform, IAM role, Key pair name, Owner, Launch time, Termination protection, Lifecycle, Monitoring, Alarm status, Kernel ID, RAM disk ID, Placement group, Partition number, Virtualization, VPC ID, Subnet ID, Network interfaces, Source/dest. check, T2/T3 Unlimited, EBS-optimized, Root device type, Root device, Block devices, Basic Graphics ID, Basic Inference accelerator ID, Capacity Reservation, and Capacity Reservation Settings.

### Step 3.2.7: Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

**cd <folder path>**

- Initialize your repository using the following command:

**git init**

- Add all the files to your git repository using the following command:

**git add .**

- Commit the changes using the following command:

**git commit . -m "Changes have been committed."**

- Push the files to the folder you initially created using the following command:

**git push -u origin master**

# 3.9 Launch an Instance in a Placement Group

---

This section will guide you to:

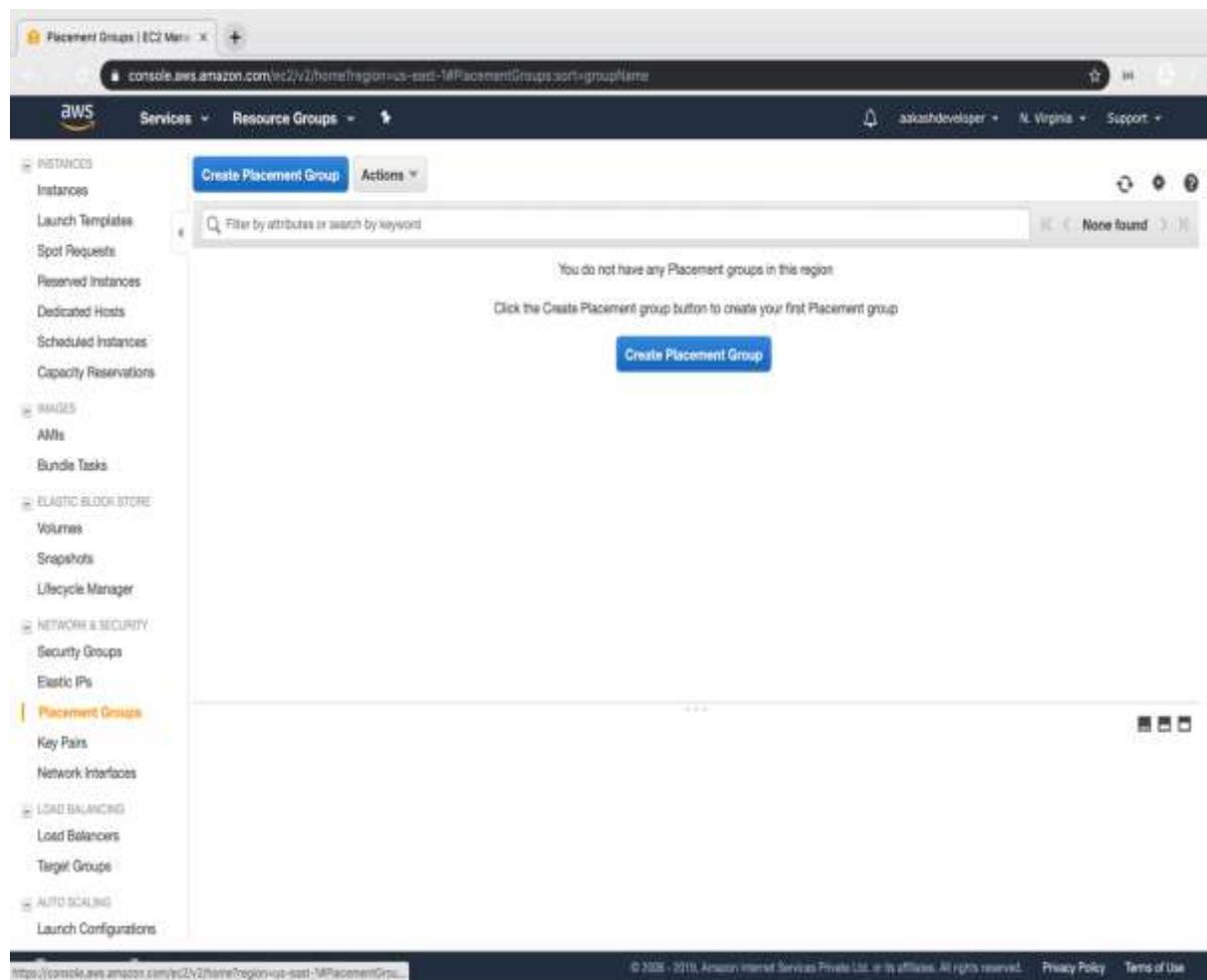
- Launch an instance in a placement group

This lab has two subsections, namely:

- 4.3.1 Creating a placement group
- 4.3.2 Launching an instance in the placement group

## Step 4.3.1: Creating a placement group

- Click on *Create Placement Group*



- Provide a name and strategy

Create Placement Group

Name: simpleamplifyApp

Strategy: Cluster

AWS Command Line Interface command:

- Cluster
- Spread
- Partition

\* Required: Cluster

Create

### Step 4.3.2: Launching an instance in the placement group

- Launch the new EC2 instance

EC2 Management Console

Services - Resource Groups -

Feedback English (US)

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) region:

- 0 Running Instances
- 0 Dedicated Hosts
- 0 Volumes
- 4 Key Pairs
- 1 Placement Groups

Learn more about the latest in AWS Compute from AWS re:invent by viewing the [EC2 Videos](#).

**Create Instance**

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

**Launch Instance**

**Migrate a Machine**

Use CloudEndure Migration to simplify, expedite, and automate large-scale migrations from physical, virtual, and cloud-based infrastructure to AWS.

[Get started with CloudEndure Migration](#)

**Service Health**

**Service Status:** US East (N. Virginia)

**Availability Zone Status:**

- us-east-1a: Availability zone is operating normally
- us-east-1c: Availability zone is operating normally
- us-east-1d: Availability zone is operating normally

**Scheduled Events**

US East (N. Virginia): No events

**AWS Marketplace**

Find free software trial products in the AWS Marketplace from the EC2 Launch Wizard. Or try these popular software:

- CloudEndure Migration
- By Amazon Web Services
- Rating: ★★★★
- [View all Infrastructure Software](#)
- Amazon ETL for Amazon Redshift
- By Matillion
- Rating: ★★★★

Feedback English (US)

© 2006 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

- Select the placement group

**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	<input type="radio"/> Request Spot instances	
Network	vpc-4e244834 (default)	<input type="radio"/> Create new VPC
Subnet	No preference (default subnet in any Availability Zone)	<input type="radio"/> Create new subnet
Auto-assign Public IP	Use subnet setting (Enabled)	
Placement group	<input checked="" type="radio"/> Add instance to placement group:  <input checked="" type="radio"/> Add to existing placement group:  <input type="radio"/> Add to a new placement group:	
Placement group name	simple spread	
Capacity Reservation	<input type="radio"/> Create new Capacity Reservation	
IAM role	None	
Shutdown behavior	Stop	

Choose placement group:  
 Filter by attributes  

Name	Strategy
simple	spread

Cancel Previous Review and Launch Next: Add Storage

Feedback English (US) © 2018 - 2019 Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

**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	<input type="radio"/> Request Spot instances	
Network	vpc-4e244834 (default)	<input type="radio"/> Create new VPC
Subnet	No preference (default subnet in any Availability Zone)	<input type="radio"/> Create new subnet
Auto-assign Public IP	Use subnet setting (Enabled)	
Placement group	<input checked="" type="radio"/> Add instance to placement group:  <input checked="" type="radio"/> Add to existing placement group:  <input type="radio"/> Add to a new placement group:	
Placement group name	simple spread	
Capacity Reservation	<input type="radio"/> Open	
IAM role	None	
Shutdown behavior	Stop	

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

Choose placement group:  
 Filter by attributes  

Name	Strategy
simple	simple

Cancel Previous Review and Launch Next: Add Storage

Feedback English (US) © 2018 - 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/v2/home?region=us-east-1&stackId=905-1004&rootId=905

Services: Resource Groups

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:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
	i-04259c2a3ee710f	t2.micro	us-east-1a	terminated		None		
<b>Instance</b>	i-07cdcc06e6412bdf	t2.micro	us-east-1c	running	2/2 checks ...	None	ec2-34-207-220-254.co...	34.207.220.254
	i-079602637b621d99e	t2.micro	us-east-1c	terminated		None		

Termination protection: False

Root device: /dev/xvda

Block devices: /dev/xvdb

Elastic Graphics ID: -

Elastic Inference accelerator ID: -

Capacity Reservation: -

Capacity Reservation Settings: Open

Lifecycle: normal

Monitoring: basic

Alarm status: None

Kernel ID: -

RAM disk ID: -

Placement group: **Amazon** (0)

Partition number: -

Virtualization: hvm

Reservation: H2R8H3t4u98U70T84

AMI launch index: 0

Priority: default

Host ID: -

Affinity: -

State transition reason: -

State transition reason message: -

Stop - Hibernation behavior: Disabled

Number of vCPUs: 1

Feedback English (US) © 2006 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

## **Assisted Practice: 3.13 Create an EBS Volume**

This section will guide you to:

- Change the volume size of an instance

This lab has six subsections, namely:

3.4.1 Selecting the **volume** tab in the EC2 dashboard

3.4.2 Creating a new volume by clicking on **Create**

3.4.3>Selecting the volume type according to the project requirement

3.4.4 Creating a new volume by specifying the size and defining the zone

3.4.5 Verifying the new volume created on the volume console and its availability

3.4.6 Pushing the code to GitHub repositories

**Step 3.4.1:** Selecting the **volume** tab in the EC2 dashboard

The screenshot shows the AWS EC2 Management Console interface. The left sidebar contains navigation links for various EC2 services. The main content area displays a summary of resources in the US East (N. Virginia) region. A 'Create Instance' button is present. The right side features account attributes, additional information links, and an AWS Marketplace section.

### Step 3.4.2: Creating a new volume by clicking on **Create**

The screenshot shows the AWS EC2 Management Console with the 'Volumes' page selected. The left sidebar includes links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, Images, AMIs, Bundle Tasks, Elastic Block Store (with Volumes selected), Snapshots, Lifecycle Manager, Network & Security (with Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), and Load Balancing.

The main content area displays a table of volumes. The table has columns for Name, Volume ID, Size, Volume Type, IOPS, Snapshot, Created, Availability Zone, State, and Alarm Status. One volume is listed:

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone	State	Alarm Status
vol-037de514fb90f1baf	vol-037de514fb90f1baf	8 GB	gp2	100	snap-05e19c3551abd794a	September 21, 2019 at 6:35:06 PM UTC+1	us-east-1c	In-use	None

Below the table, there is a detailed view for the selected volume (vol-037de514fb90f1baf). It shows the following information:

Description	Status Checks	Monitoring	Tags
Volume ID: vol-037de514fb90f1baf	Size: 8 GB	Created: September 21, 2019 at 6:35:06 PM UTC+1	State: In-use
			Attachment information: i-07ccb006eb412b0f/dev/xvda (attached)
			Volume ID: vol-037de514fb90f1baf
			Size: 8 GB
			Created: September 21, 2019 at 6:35:06 PM UTC+1
			State: In-use
			Attachment information: i-07ccb006eb412b0f/dev/xvda (attached)
			Volume ID: vol-037de514fb90f1baf
			Size: 8 GB
			Created: September 21, 2019 at 6:35:06 PM UTC+1
			State: In-use
			Attachment information: i-07ccb006eb412b0f/dev/xvda (attached)
			Volume ID: vol-037de514fb90f1baf
			Size: 8 GB
			Created: September 21, 2019 at 6:35:06 PM UTC+1
			State: In-use
			Attachment information: i-07ccb006eb412b0f/dev/xvda (attached)

At the bottom of the page, there are links for Feedback, English (US), and a footer with copyright information: © 2006 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use.

### Step 3.4.3: Selecting the volume type according to the project requirement

The screenshot shows the AWS EC2 Manager interface for creating a new EBS volume. The top navigation bar includes tabs for 'Create Volume' and 'Creating an Amazon EBS Volume'. The main title is 'Create Volume'. The 'Volume Type' dropdown is set to 'General Purpose SSD (gp2)'. A dropdown menu is open, showing options: 'General Purpose SSD (gp2)' (selected), 'Provisioned IOPS SSD (io1)', 'Cold HDD (sc1)', 'Throughput Optimized HDD (st1)', and 'Magnetic (standard)'. Other fields include 'Size (GiB)' (Max: 16384 GiB), 'IOPS' (3 IOPS per GiB with a 100 IOPS, burstable to 1000), 'Availability Zone' (us-east-1a), 'Throughput (MB/s)' (Not applicable), 'Snapshot ID' (Select a snapshot), 'Encryption' (Encrypt this volume checked), and a section for adding tags with 'Key' and 'Value' fields. At the bottom, there are links for 'Feedback', 'English (US)', and legal notices.

#### Step 3.4.4: 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](https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateVolume). The top right corner shows the user 'akosnDeveloper', the region 'N. Virginia', and a 'Support' link.

The main form is titled 'Create Volume' and contains the following fields:

- Volume Type:** General Purpose SSD (gp2) (dropdown)
- Size (GiB):** 1 (input field, 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 (dropdown)
- Throughput (MB/s):** Not applicable (info icon)
- Snapshot ID:** Select a snapshot (dropdown)
- Encryption:**  Encrypt this volume

Below the form, there is a section for tags:

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

The message 'This resource currently has no tags.' is displayed, followed by 'Choose the Add tag button or [click to add a Name tag](#)'.

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

**Step 3.4.5:** Verifying the new volume created on the volume console and its availability

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone	State	Alarm Status
	vol-01beb43...	1 GB	gp2	100		September 21, 201...	us-east-1a	available	None
	vol-037de51...	8 GB	gp2	100	snap-05a19c3...	September 21, 201...	us-east-1c	in-use	None

### Step 3.4.6: Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

**cd <folder path>**

- Initialize your repository using the following command:

**git init**

- Add all the files to your git repository using the following command:

**git add .**

- Commit the changes using the following command:

**git commit . -m "Changes have been committed."**

- Push the files to the folder you initially created using the following command:

**git push -u origin master**

# **Assisted Practice: 3.15 Format and Mount an EBS Volume**

This section will guide you to:

- Format and mount an EBS volume

This lab has four subsections, namely:

- 3.5.1 Attaching an existing EBS volume
- 3.5.2 Mounting the EBS volume
- 3.5.3 Unmounting the EBS volume
- 3.5.4 Pushing the files to GitHub repositories

## **Step 3.5.1: Attaching an existing EBS volume**

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

**Attach Volume**

Volume	<input type="text"/> vol-3113afe8 in ap-northeast-2a
Instance	<input type="text"/> i-5f2b41f8 in ap-northeast-2a
Device	<input type="text"/> /dev/sdf Linux Devices: /dev/sdf through /dev/sdp

Note: Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdp internally, even when the device name is still /dev/sdf.

## **Step 3.5.2: 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 3.5.3:** Unmounting the EBS volume

- Use the following command to unmount the volume:

*umount /dev/xvdf*

#### **Step 3.5.4:** Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

**cd <folder path>**

- Initialize your repository using the following command:

**git init**

- Add all the files to your git repository using the following command:

**git add .**

- Commit the changes using the following command:

**git commit . -m "Changes have been committed."**

- Push the files to the folder you initially created using the following command:

**git push -u origin master**

# Assisted Practice: 3.16 Detach an EBS Volume

This section will guide you to:

- Detach an EBS volume from an instance

This lab has three subsections, namely:

- 3.6.1 Selecting the EBS volume you want to detach
- 3.6.2 Detaching the volume
- 3.6.3 Pushing the files to GitHub repositories

## **Step 3.6.1: Selecting the EBS volume you want to detach**

- Choose the bucket

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone	State	Alarm Status
vol-09671dfb8dcde0f2	vol-09671dfb8dcde0f2	1 GB	gp2	100	snap-0xa19c3...	September 21, 2019	us-east-1c	In-use	None
vol-037ae61...	vol-037ae61...	8 GB	gp2	100	snap-0xa19c3...	September 21, 2019	us-east-1c	In-use	None

- Select *Detach Volume* option

The screenshot shows the AWS EC2 Management Console. On the left, there's a navigation sidebar with links like EC2 Dashboard, Events, Reports, Limits, Instances, Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, AMIs, and Lifecycle Manager. The main area has a title bar with the URL <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#VOLUMEID:sort=CREATIONTIME>. Below the title bar, there are tabs for Actions, Filter by tag, and Name. A dropdown menu is open under Actions, showing options: Modify Volume, Create Snapshot, Detach Volume, Attach Volume, Delete Volume, Force Detach Volume, Change Auto-Enable I/O Setting, and Add/Edit Tags. The 'Delete Volume' option is highlighted with a yellow background. The main table lists two volumes: gp2 (Volume ID: vol-0967dfdeb6d0e0f2, Size: 1 GiB, Created: September 21, 2019 at 6:54:29 PM UTC+1, Availability Zone: us-east-1c, State: in-use, Alarm Status: None) and gp2 (Volume ID: vol-0967dfdeb6d0e0f2, Size: 1 GiB, Created: September 21, 2019 at 6:54:29 PM UTC+1, Availability Zone: us-east-1c, State: in-use, Alarm Status: None). At the bottom of the table, there are buttons for 1 to 2 of 2, Next, and Previous. Below the table, there's a detailed view for the first volume: Volume ID: vol-0967dfdeb6d0e0f2, Size: 1 GiB, Created: September 21, 2019 at 6:54:29 PM UTC+1, State: In-use, Attachment Information: i-0967dfdeb6d0e0f2/dev/sdf (attached), and other details like Snapshot ID, Availability Zone, Encryption, and KMS Key ID.

### Step 3.6.2: Detaching the volume

- Select Yes once the confirmation pop-up appears

The screenshot shows the AWS EC2 Management console with the 'Volumes' section selected. On the left, there's a sidebar with various navigation options like 'Create Volume', 'Actions', 'Filters', 'Tags', 'Metrics', 'Launch', 'Instances', 'Launch Templates', 'Spot Requests', 'Amazone Instances', 'Dedicated Hosts', 'Scheduled Instances', 'Capacity Reservations', 'AWS Lambda', 'Amazon VPC', 'Amazon S3', 'Amazon SNS', 'Amazon S3', 'Amazon CloudWatch Metrics', and 'Metrics'. The main area displays a table of volumes with columns: Name, Volume ID, Size, Volume Type, IOPS, Snapshot, Created, Availability Zone, State, and Alarm Status. Two volumes are listed: 'vol-0007d902a2e2' (1 GiB, gp2, 100, September 21, 2018, us-east-1, available) and 'vol-0007d902a2e3' (0 GiB, gp2, 100, snap-0007d902, September 21, 2018, us-east-1, available). Below the table, a modal dialog box titled 'Detach Volume' contains the message 'Are you sure you want to detach this volume?' followed by the volume ID 'vol-0007d902a2e2'. It has 'Cancel' and 'Yes, Detach' buttons, with 'Yes, Detach' being the active one. At the bottom of the page, there are links for 'Feedback', 'English (US)', and 'AWS Support'.

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

The screenshot shows the AWS EC2 Volumes Management interface. 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, Images, AMIs, and Bundle Tasks. The main area has tabs for Create Volume and Actions. A search bar at the top says "Filter by tags and attributes or search by keyword". Below it is a table with columns: Name, Volume ID, Size, Volume Type, IOPS, Snapshot, Created, Availability Zone, State, and Alarm Status. Two volumes are listed:

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone	State	Alarm Status
vol-09671dfe...	1 GB	gp2	100		September 21, 201...	us-east-1c	available	None	Yellow
vol-037de51...	8 GB	gp2	100	snap-05a19c3...	September 21, 201...	us-east-1c	in-use	None	Yellow

On the right, there's a detailed view for the first volume (vol-09671dfe8dcde0f2). It shows the following details:

Description	Value	Description	Value
Volume ID	vol-09671dfe8dcde0f2	Alarm status	None
Size	1 GB	Snapshot	-
Created	September 21, 2019 at 6:54:29 PM UTC+1	Availability Zone	us-east-1c
State	available	Encryption	Not Encrypted
Attachment information		KMS Key ID	

At the bottom, there are links for Feedback, English (US), and footer links for Privacy Policy and Terms of Use.

### Step 3.6.3: Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

**cd <folder path>**

- Initialize your repository using the following command:

**git init**

- Add all the files to your git repository using the following command:

**git add .**

- Commit the changes using the following command:

**git commit . -m "Changes have been committed."**

- Push the files to the folder you initially created using the following command:

**git push -u origin master**

## **Assisted Practice: 3.17 Delete an EBS Volume**

This section will guide you to:

- Delete an EBS volume

This lab has three subsections, namely:

3.7.1 Selecting the EBS volume you want to delete

3.7.2 Deleting the volume

3.7.3 Pushing the file to GitHub repositories

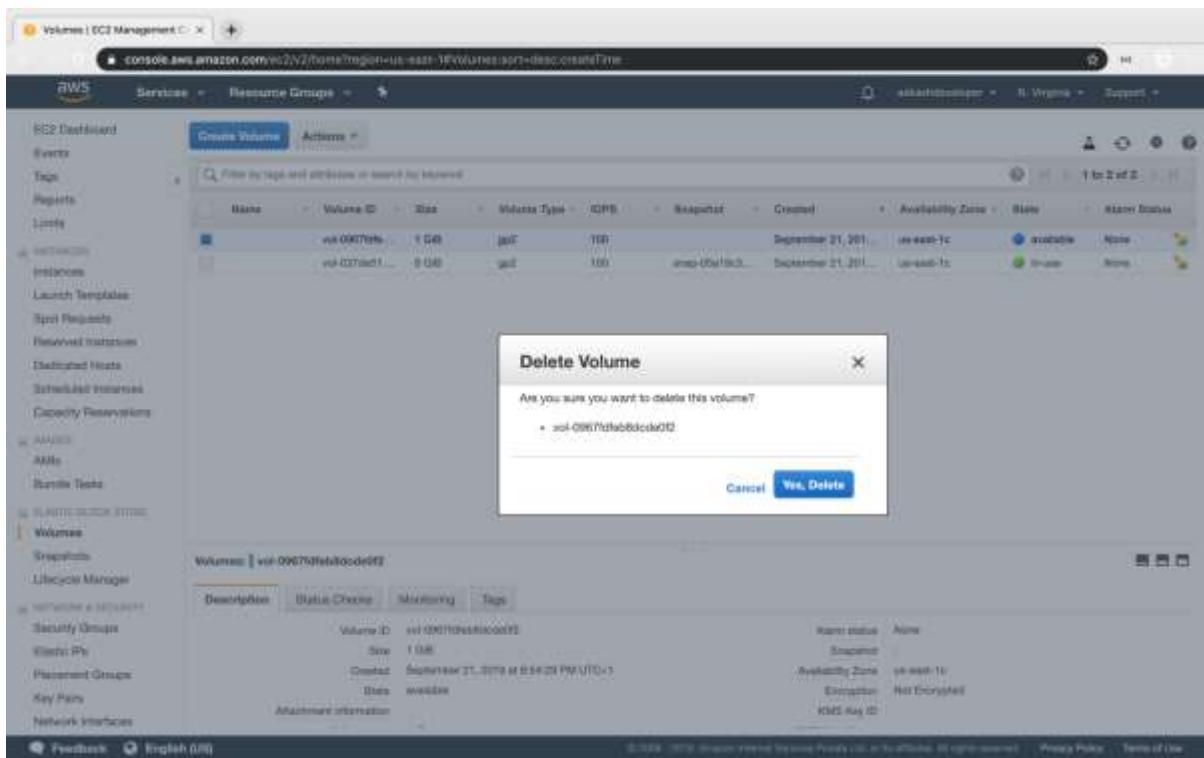
**Step 3.7.1:** Selecting the EBS volume you want to delete

The screenshot shows the AWS EC2 Management Console with the 'Volumes' section selected. On the left, there's a sidebar with various navigation options like EC2 Dashboard, Instances, AMIs, and Network & Security. The main area displays a table of volumes. A context menu is open over one of the rows, with 'Delete Volume' highlighted. The table shows two entries:

Name	Volume Type	IOPS	Snapshot	Created	Availability Zone	State	Alarm Status
gp2	gp2	100		September 21, 2019	us-east-1c	available	None
gp2	gp2	100	snap-06a19c3...	September 21, 2019	us-east-1c	in-use	None

Below the table, there are tabs for Description, Status Checks, Monitoring, and Tags. The 'Description' tab is active, showing details for the selected volume (Volume ID: vol-09671d1eb8dcde02, Size: 1 GB, Created: September 21, 2019 at 6:54:29 PM UTC+1, State: available). The 'Tags' tab is also visible.

### Step 3.7.2: Deleting the volume



### Step 3.7.3: Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

**cd <folder path>**

- Initialize your repository using the following command:

**git init**

- Add all the files to your git repository using the following command:

**git add .**

- Commit the changes using the following command:

```
git commit . -m "Changes have been committed."
```

- Push the files to the folder you initially created using the following command:

```
git push -u origin master
```

## **Assisted Practice: 3.20 Create an EBS Snapshot**

This section will guide you to:

- Create an EBS snapshot

This lab has two subsection, namely:

3.8.1 Creating an EBS snapshot

3.8.2 Pushing the file to GitHub repositories

**Step 3.8.1:** Creating an EBS snapshot

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

The screenshot shows the AWS EC2 Management Console with the 'Volumes' section selected. A context menu is open over a specific volume entry, listing options such as 'Modify Volume', 'Create Snapshot' (which is highlighted in yellow), 'Delete Volume', 'Attach Volume', 'Detach Volume', 'Force Detach Volume', 'Change Auto-Enable I/O Setting', and 'Add/Edit Tags'. The main table displays one volume entry:

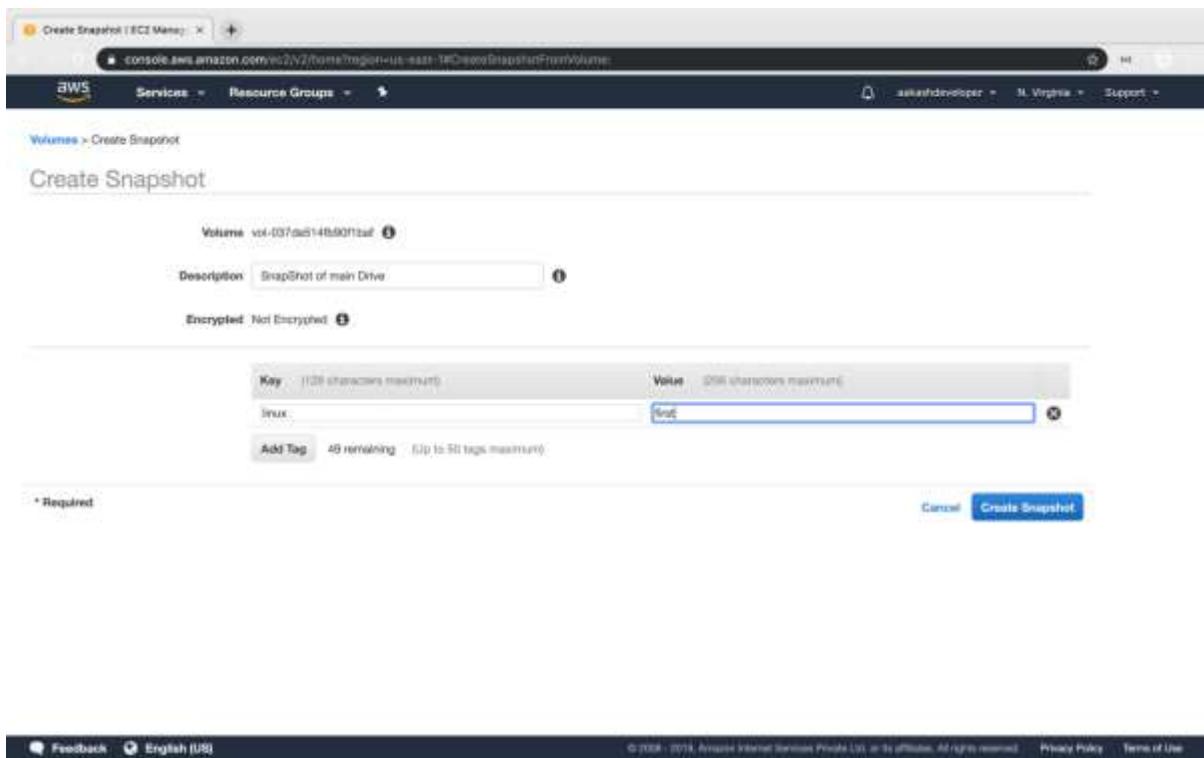
Volume Type	IOPS	Snapshot	Created	Availability Zone	State	Alarm Status
gp2	100	snap-05a19c3...	September 21, 201...	us-east-1c	In-use	None

Below the table, there are tabs for 'Description', 'Status Checks', 'Monitoring', and 'Tags'. The 'Description' tab is active, showing detailed information about the volume:

Volume ID	Size	Created	State	Attachment Information	Alarm status	Snapshot	Availability Zone	Encryption	KMS Key ID
vol-037de514fb901ba	8 GB	September 21, 2019 at 6:39:06 PM UTC+1	In-use	i-07ccba096eb412b0 /dev/xvda (attached)	None	tmp-05a19c3561sted794e	us-east-1c	Not Encrypted	

At the bottom of the page, there are links for 'Feedback', 'English (US)', and legal notices.

- Add snapshot name, key, and value



### Step 3.8.2: Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

**cd <folder path>**

- Initialize your repository using the following command:

**git init**

- Add all the files to your git repository using the following command:

**git add .**

- Commit the changes using the following command:

```
git commit . -m "Changes have been committed."
```

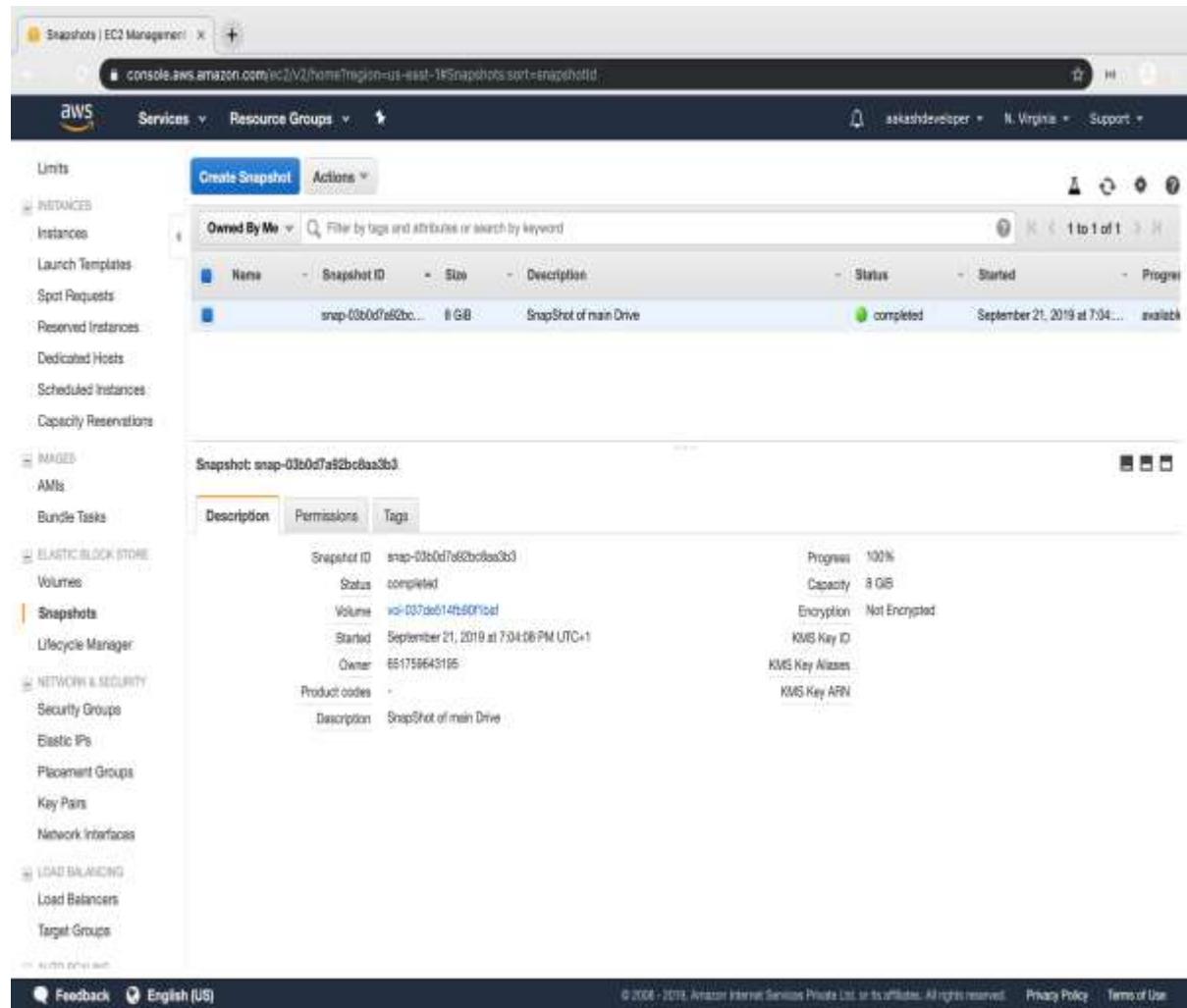
- Push the files to the folder you initially created using the following command:

```
git push -u origin master
```

## Assisted Practice: 3.21 View snapshot

This section will guide you to view a snapshot in your AWS account.

**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 Snapshots dashboard. On the left sidebar, under the 'SNAPS' section, the 'Schemas' option is selected. The main content area displays a table of snapshots. One row is highlighted, showing the following details:

Name	Snapshot ID	Size	Description	Status	Started	Progress
snap-03b0d7a82bc8aa3b3	snap-03b0d7a82bc8aa3b3	8 GiB	SnapShot of main Drive	completed	September 21, 2019 at 7:04:06 UTC+0	available

Below the table, there is a detailed view for the selected snapshot:

Snapshot: snap-03b0d7a82bc8aa3b3		
Description	Permissions	Tags
Snapshot ID: snap-03b0d7a82bc8aa3b3 Status: completed Volume: vol-037de514fb60f1cd Started: September 21, 2019 at 7:04:06 UTC+0 Owner: 651736643165 Product codes: Description: SnapShot of main Drive	Progress: 100% Capacity: 8 GiB Encryption: Not Encrypted KMS Key ID: KMS Key Aliases: KMS Key ARN:	

At the bottom of the page, there are links for 'Feedback', 'English (US)', and copyright information: '© 2006 - 2019 Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use'.

**Step 2:** Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

**cd <folder path>**

- Initialize your repository using the following command:

**git init**

- Add all the files to your git repository using the following command:

**git add .**

- Commit the changes using the following command:

**git commit . -m "Changes have been committed."**

- Push the files to the folder you initially created using the following command:

**git push -u origin master**

## **Assisted Practice: 3.22 Initialize a Volume Restored from a Snapshot on Linux**

This section will guide you to:

- Initialize a volume restored from a snapshot

This lab has three subsections, namely:

- 3.10.1 Selecting the snapshot
- 3.10.2 Restoring volume from the snapshot
- 3.10.3 Pushing the files to GitHub repositories

**Step 3.10.1:** Selecting the snapshot

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

Snapshots | EC2 Management

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

Services ▾ Resource Groups ▾

sakashdeveloper N. Virginia Support

Limits

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

AMIS AMIs Bundle Tasks

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

Amazon VPC

Create Snapshot Actions ▾

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

Name	Snapshot ID	Size	Description	Status	Started	Progress
	snap-03b0d7a92bc8aa3b3	8 GiB	SnapShot of main Drive	completed	September 21, 2019 at 7:04:58 PM UTC+1	available

1 to 1 of 1

Snapshot: snap-03b0d7a92bc8aa3b3

Description Permissions Tags

Snapshot ID: snap-03b0d7a92bc8aa3b3	Progress: 100%
Status: completed	Capacity: 8 GiB
Volume: vdi-037de614fb90ff1bf	Encryption: Not Encrypted
Started: September 21, 2019 at 7:04:58 PM UTC+1	KMS Key ID:
Owner: 661799643195	KMS Key Aliases:

© 2006–2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

### Step 3.10.2: Restoring volume from the snapshot

- Select the snapshot and click on *Action*

The screenshot shows the AWS EC2 Snapshots page. On the left, there's a navigation sidebar with sections like Instances, Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, AMIs, and Snapshots. The 'Snapshots' section is currently selected. In the main content area, a table lists a single snapshot: 'Snapshot: snap-03b0d7a02bcbaa3b3'. A context menu is open over this snapshot, with 'Create Volume' highlighted. Other options in the menu include Delete, Create Image, Copy, Modify Permissions, and Add/Edit Tags.

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

The screenshot shows the 'Create Volume' page. At the top, it says 'Create Volume' and has a 'Snapshot ID' field containing 'snap-03b0d7a02bcbaa3b3'. Below that, 'Volume Type' is set to 'General Purpose SSD (gp2)'. The 'Size (GB)' is set to '8' (Min: 1 GB, Max: 16384 GB). Under 'Performance', 'IOPS' is set to '100 / 3000' (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS). The 'Availability Zone' is 'us-east-1a'. The 'Throughput (MB/s)' is 'Not applicable'. Under 'Encryption', there's an option to 'Encrypt this volume'. At the bottom, there's a 'Tags' section where a new tag is being added: 'Key' is 'backup' and 'Value' is 'snapshot restore'. There's also a note saying 'Add Tag' and '49 remaining (Up to 50 tags maximum)'. At the very bottom right is a 'Create Volume' button.

- Restore the volume from the snapshot

The screenshot shows the AWS Management Console for EC2 Snapshots. On the left, there's a navigation pane with various EC2-related options like Instances, Launch Templates, and Snapshots. The main area is titled 'Create Snapshot' and shows a table of existing snapshots. One snapshot is highlighted: 'snap-03b007a62bc...' with a size of 8 GiB and a description 'Snapshot of main Drive'. The status is 'completed' with a timestamp of 'September 21, 2019 at 7:04:...'. Below this, there's a detailed view of the selected snapshot, showing its ID, status (completed), volume (vol-037de614f60016af), owner (661798643196), product code (Loading...), and description ('Snapshot of main Drive').

### Step 3.10.3: Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

**cd <folder path>**

- Initialize your repository using the following command:

**git init**

- Add all the files to your git repository using the following command:

**git add .**

- Commit the changes using the following command:

```
git commit . -m "Changes have been committed."
```

- Push the files to the folder you initially created using the following command:

```
git push -u origin master
```

## **Assisted Practice: 3.25 Create a Bucket**

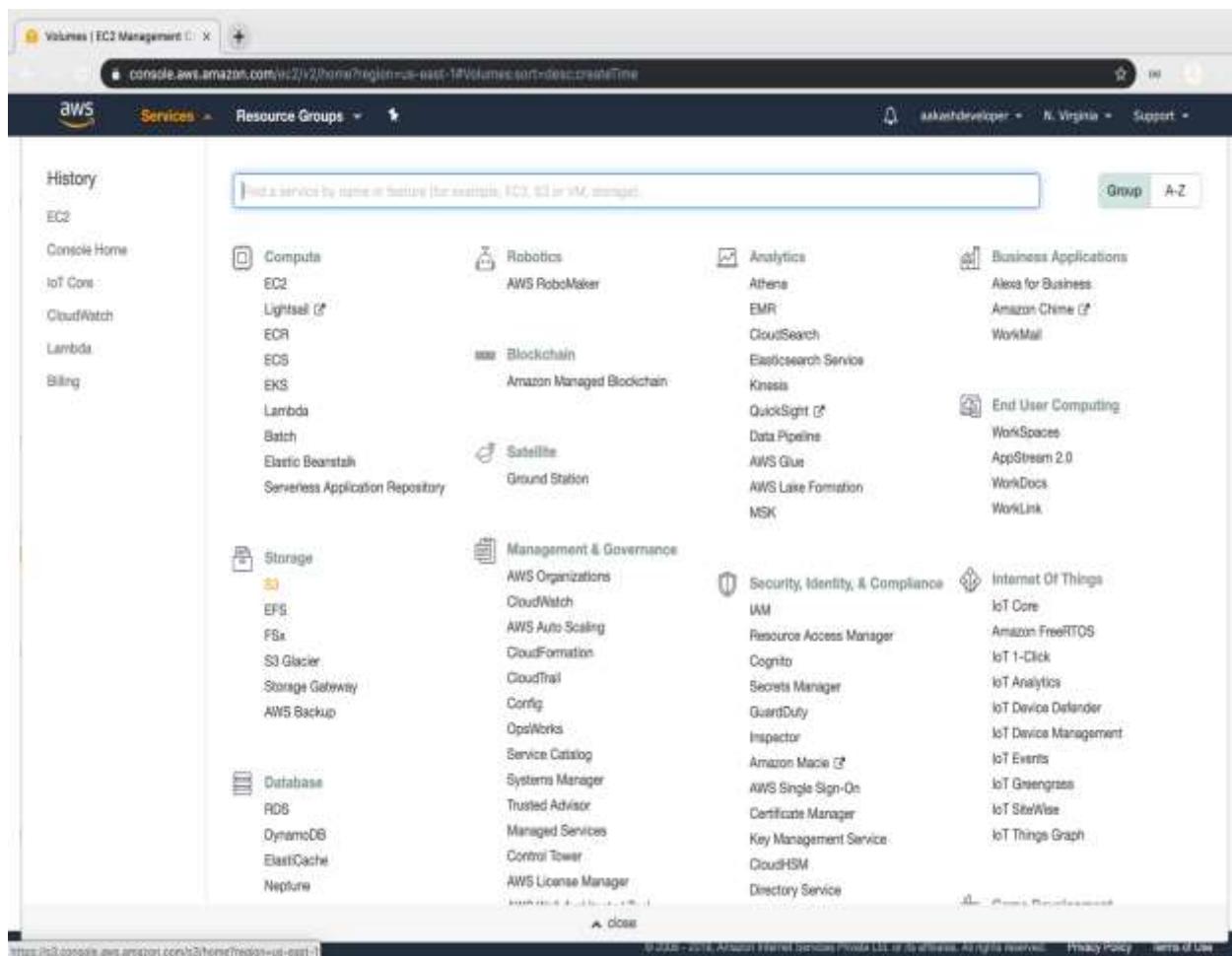
This section will guide you to:

- Create a bucket

This lab has eight subsections, namely:

- 3.11.1 Selecting S3 from the storage of the AWS service panel
- 3.11.2 Verifying the button to create a bucket
- 3.11.3 Providing a bucket name and region
- 3.11.4 Entering key and value for identification and tracking the bucket
- 3.11.5 Blocking all the public access
- 3.11.6 Reviewing all parameters and creating the bucket
- 3.11.7 Verifying the newly created bucket on the panel of S3
- 3.11.8 Pushing the files to GitHub repositories

**Step 3.11.1:** Selecting S3 from the storage of the AWS service panel



### Step 3.11..2: Verifying the button to create a bucket

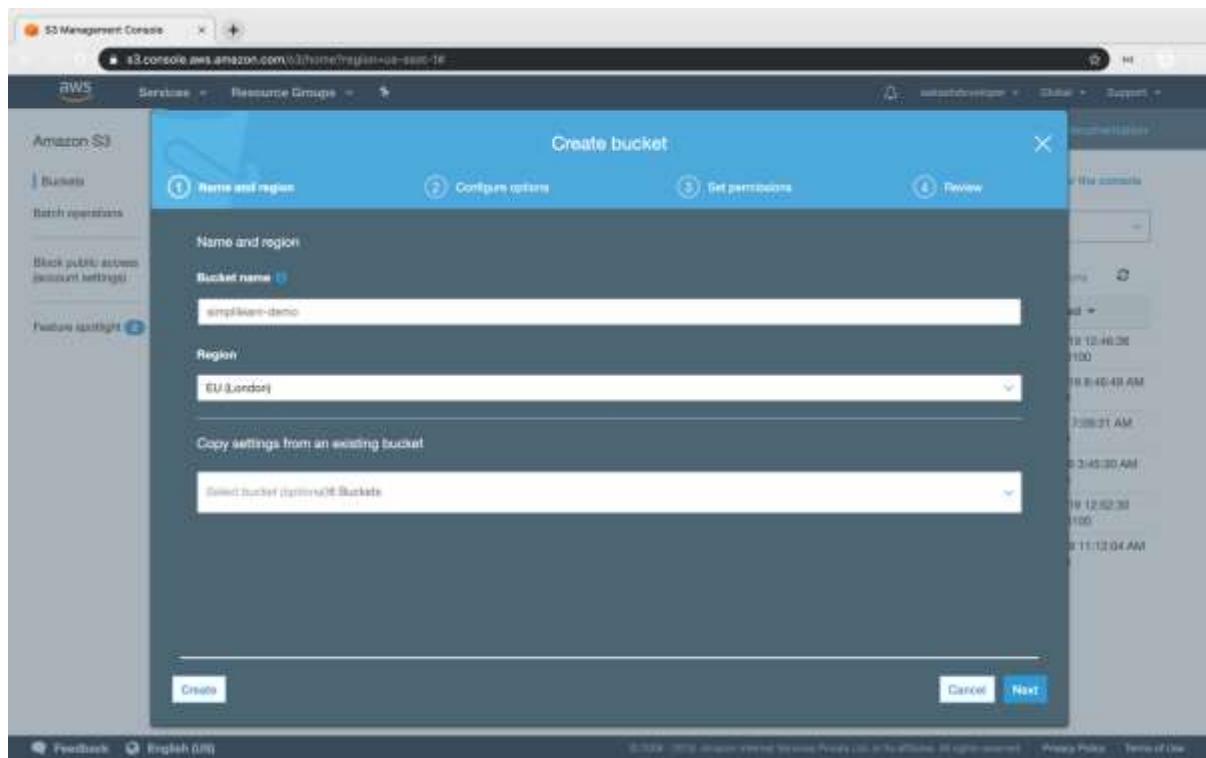
The screenshot shows the AWS S3 Management Console interface. The top navigation bar includes the AWS logo, services dropdown, resource groups dropdown, user information (zakashdev), global region (Global), and support links. Below the navigation is a banner about Amazon S3 Block Public Access. The main area is titled "S3 buckets" and contains a search bar, a "Create bucket" button, and filters for "All access types". A table lists six buckets, each with a checkbox, bucket name, access level, region, and creation date. The buckets listed are:

	Bucket name	Access	Region	Date created
<input type="checkbox"/>	cl-tempstatus-d8bjthujn9-us-east-1	Objects can be public	US East (N. Virginia)	Aug 12, 2019 12:46:38 PM GMT+0100
<input type="checkbox"/>	codepipeline-us-east-1-631614116465	Objects can be public	US East (N. Virginia)	Aug 12, 2019 8:48:49 AM GMT+0100
<input type="checkbox"/>	elasticbeansatik-us-east-1-691759643195	Objects can be public	US East (N. Virginia)	Jul 6, 2019 7:09:31 AM GMT+0100
<input type="checkbox"/>	projectsubmissions3	Objects can be public	US East (N. Virginia)	Aug 4, 2019 3:45:30 AM GMT+0100
<input type="checkbox"/>	s3edurekacf-edurekacf-1m6vocw1sj0f	Objects can be public	US East (N. Virginia)	Aug 12, 2019 12:52:30 PM GMT+0100
<input type="checkbox"/>	amongameedunika	Objects can be public	US East (N. Virginia)	Jul 22, 2019 11:12:04 AM GMT+0100

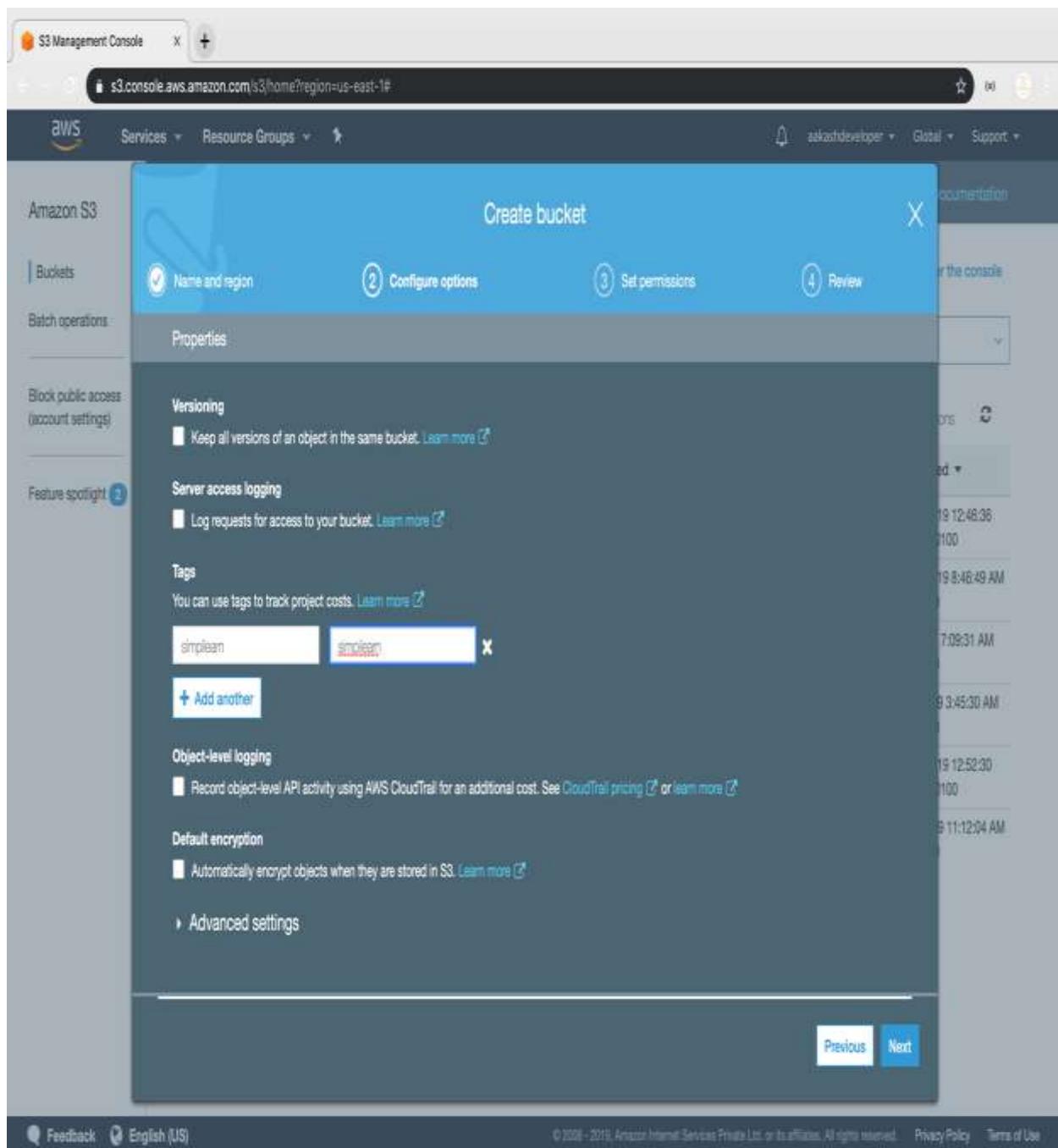
At the bottom of the page are links for Feedback, English (US), and legal notices.

### Step 3.11.3: Providing a bucket name and region

- Make sure that the bucket name is unique



**Step 4.11.4:** Entering key and value for identification and tracking the bucket



### Step 3.11.5: Blocking all the public access

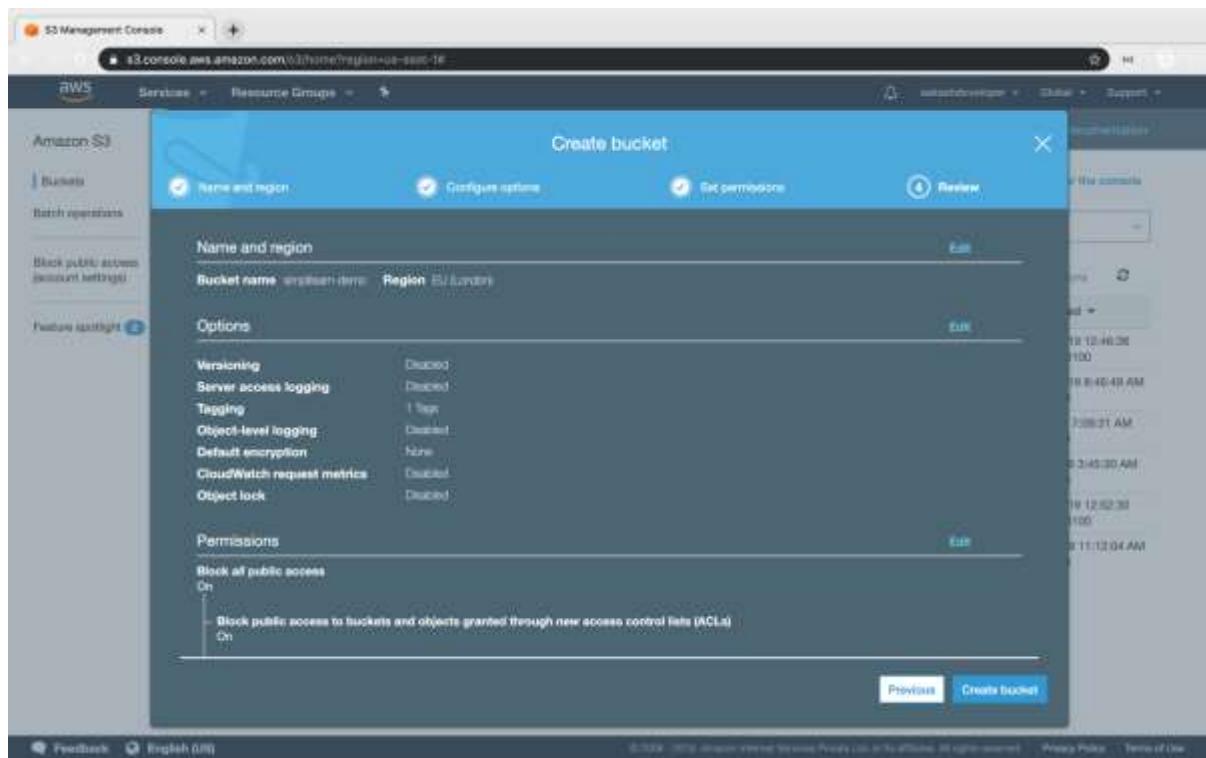
- If required, you can configure it later

The screenshot shows the AWS S3 Management Console interface for creating a new bucket. The main title is "Create bucket". The current step is "3 Set permissions". Below this, there is a note: "Note: You can grant access to specific users after you create the bucket." A section titled "Block public access (bucket settings)" is expanded, showing four checkboxes under "Block all public access":

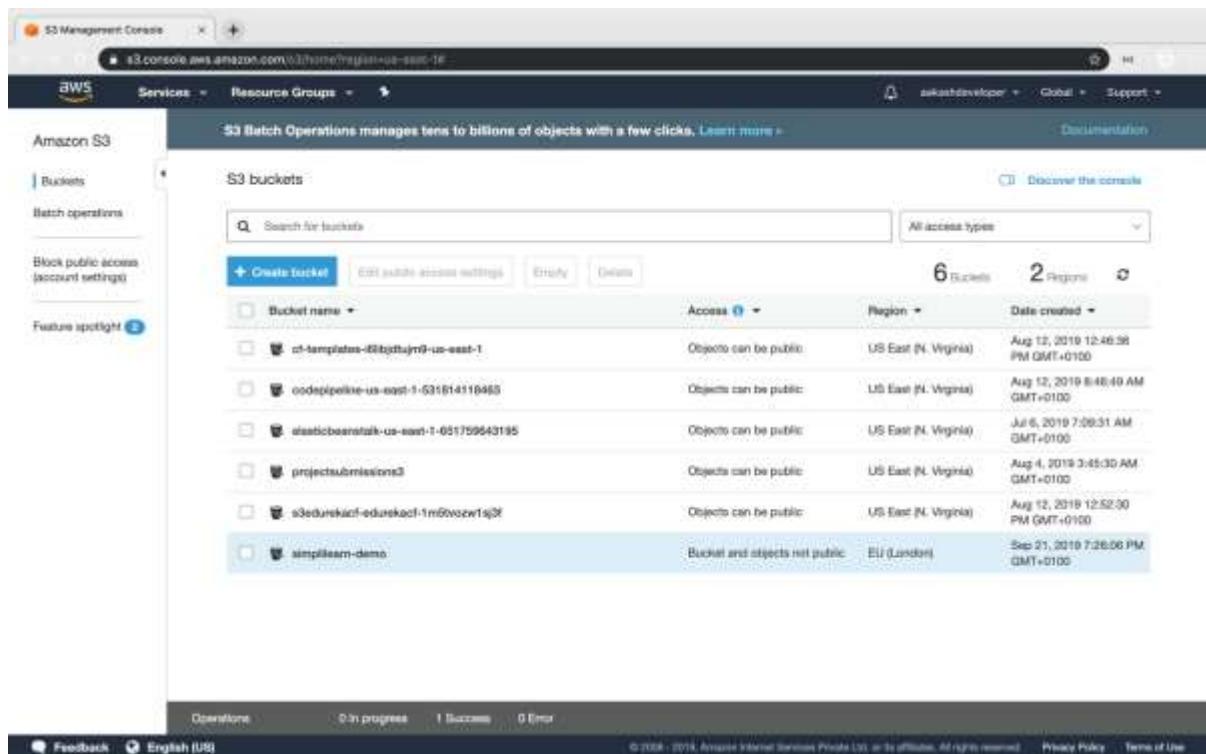
- Block public access to buckets and objects granted through new access control lists (ACLs)
- Block public access to buckets and objects granted through any access control lists (ACLs)
- Block public access to buckets and objects granted through new public bucket policies
- Block public and cross-account access to buckets and objects through any public bucket policies

At the bottom right of the wizard, there are "Previous" and "Next" buttons.

### Step 3.11.6: Reviewing all parameters and creating the bucket



### Step 3.11.7: Verifying the newly created bucket on the panel of S3



### **Step 3.11.8:** Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

**cd <folder path>**

- Initialize your repository using the following command:

**git init**

- Add all the files to your git repository using the following command:

**git add .**

- Commit the changes using the following command:

**git commit . -m "Changes have been committed."**

- Push the files to the folder you initially created using the following command:

**git push -u origin master**

## Assisted Practice: 3.28 Delete an S3 Bucket

This section will guide you to:

- Delete an S3 bucket

This lab has three subsections, namely:

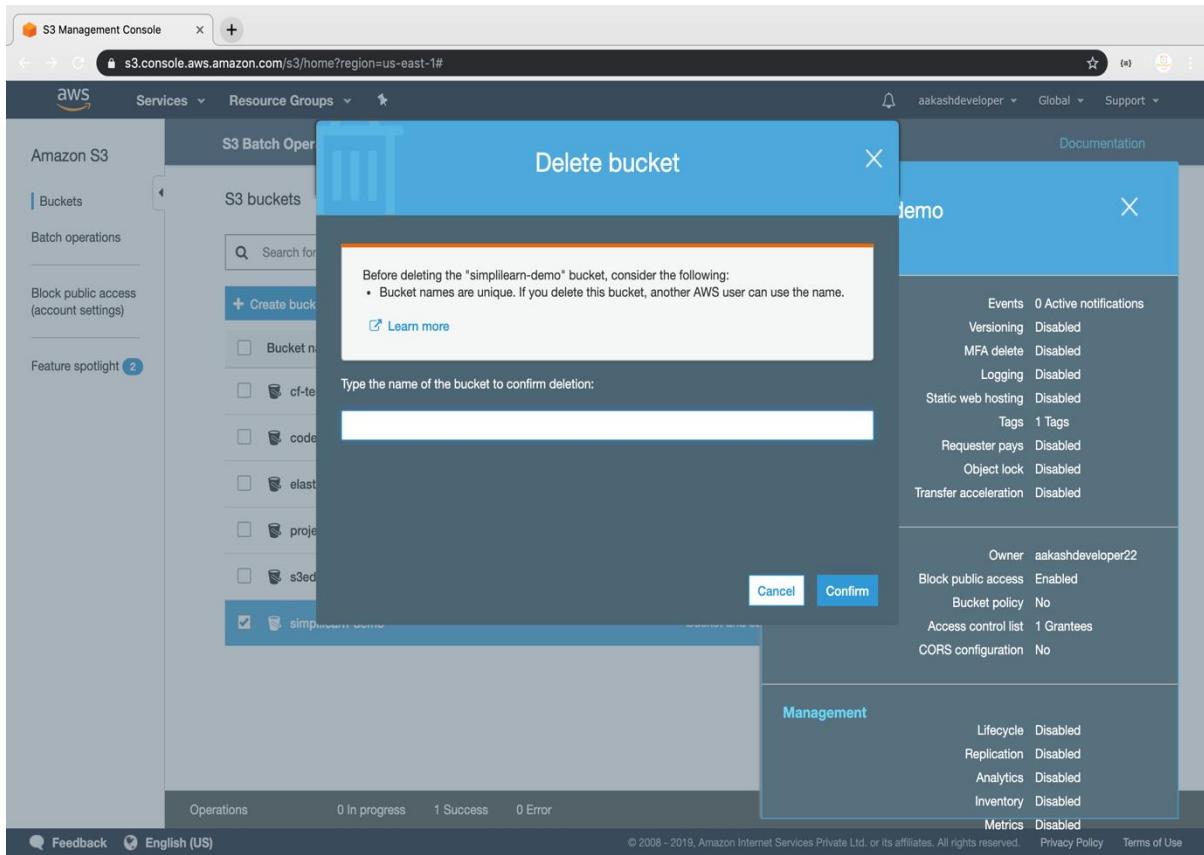
- 3.12.1 Selecting the S3 bucket you want to delete
- 3.12.2 Deleting the bucket
- 3.12.3 Pushing the files to GitHub repositories

### **Step 3.12.1: 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' and 'Batch operations'. The main area displays a list of S3 buckets. One bucket, 'simplilearn-demo', is selected and highlighted with a blue background. A detailed modal window for this bucket is open, showing its properties, permissions, and management settings. The properties include: Events (0), Active notifications (Disabled), Versioning (Disabled), MFA delete (Disabled), Logging (Disabled), Static web hosting (Disabled), Tags (1 Tag), Requester pays (Disabled), Object lock (Disabled), and Transfer acceleration (Disabled). The permissions section shows the owner as 'akashdeveloper22', block public access as 'Enabled', and a bucket policy of 'No'. The management section shows lifecycle, replication, analytics, inventory, and metrics all set to 'Disabled'.

### Step 3.12.2: Deleting the bucket



### Step 3.12.3: Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

```
cd <folder path>
```

- Initialize your repository using the following command:

```
git init
```

- Add all the files to your git repository using the following command:

**git add .**

- Commit the changes using the following command:

**git commit . -m "Changes have been committed."**

- Push the files to the folder you initially created using the following command:

**git push -u origin master**

## Assisted Practice: 3.28 Delete an S3 Bucket

This section will guide you to:

- Delete an S3 bucket

This lab has three subsections, namely:

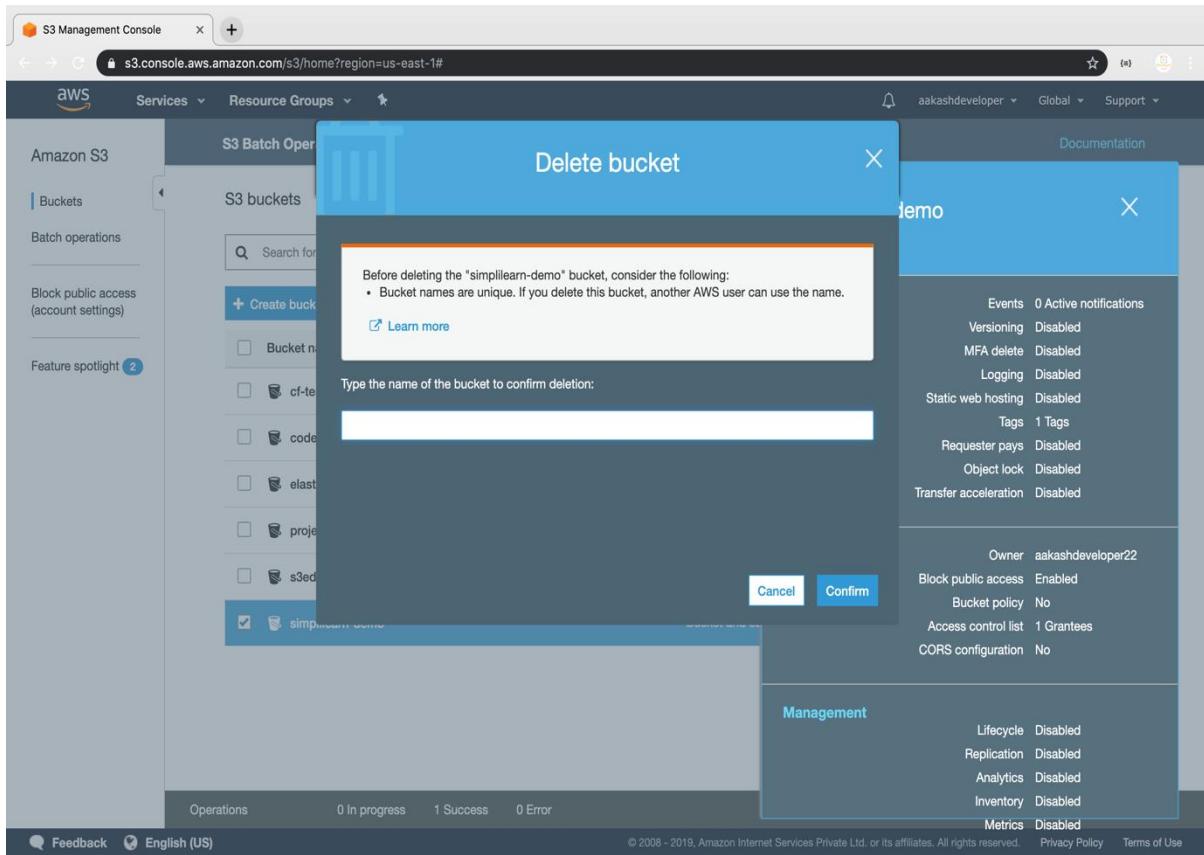
- 3.12.1 Selecting the S3 bucket you want to delete
- 3.12.2 Deleting the bucket
- 3.12.3 Pushing the files to GitHub repositories

### **Step 3.12.1: 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' and 'Batch operations'. The main area displays a list of S3 buckets. One bucket, 'simplilearn-demo', is selected and highlighted with a blue background. A detailed modal window for this bucket is open, showing its properties, permissions, and management settings. The properties include: Events (0), Active notifications (Disabled), Versioning (Disabled), MFA delete (Disabled), Logging (Disabled), Static web hosting (Disabled), Tags (1 Tag), Requester pays (Disabled), Object lock (Disabled), and Transfer acceleration (Disabled). The permissions section shows the owner as 'akashdeveloper22', block public access as 'Enabled', and a bucket policy of 'No'. The management section shows lifecycle, replication, analytics, inventory, and metrics all set to 'Disabled'. At the bottom of the modal, there are buttons for 'Delete' and 'Cancel'.

### Step 3.12.2: Deleting the bucket



### Step 3.12.3: Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

```
cd <folder path>
```

- Initialize your repository using the following command:

```
git init
```

- Add all the files to your git repository using the following command:

**git add .**

- Commit the changes using the following command:

**git commit . -m "Changes have been committed."**

- Push the files to the folder you initially created using the following command:

**git push -u origin master**

# Assisted Practice: 3.32 Set the Storage Class of an Object

This section will guide you to:

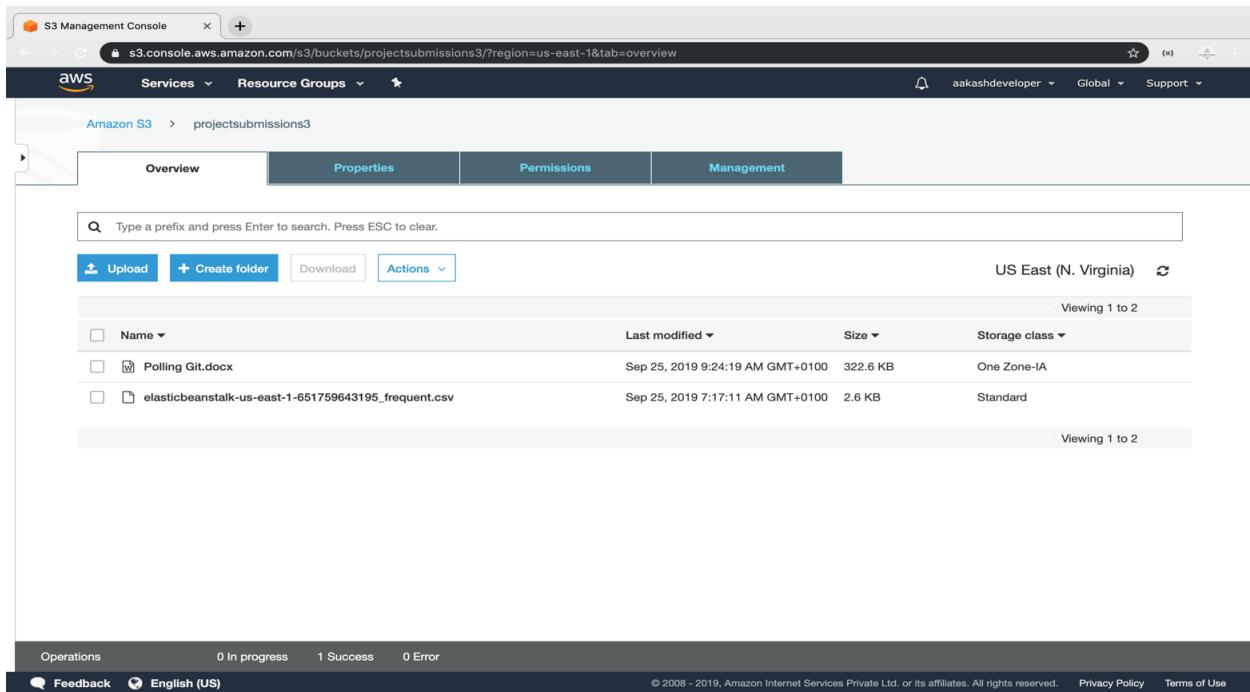
- Set the storage class of an object

This lab has three subsections, namely:

- 3.14.1 Selecting the bucket
- 3.14.2 Setting the storage class of an object
- 3.14.3 Pushing the files to GitHub repositories

## **Step 3.14.1: Selecting the bucket**

- Select the bucket and open the list of items



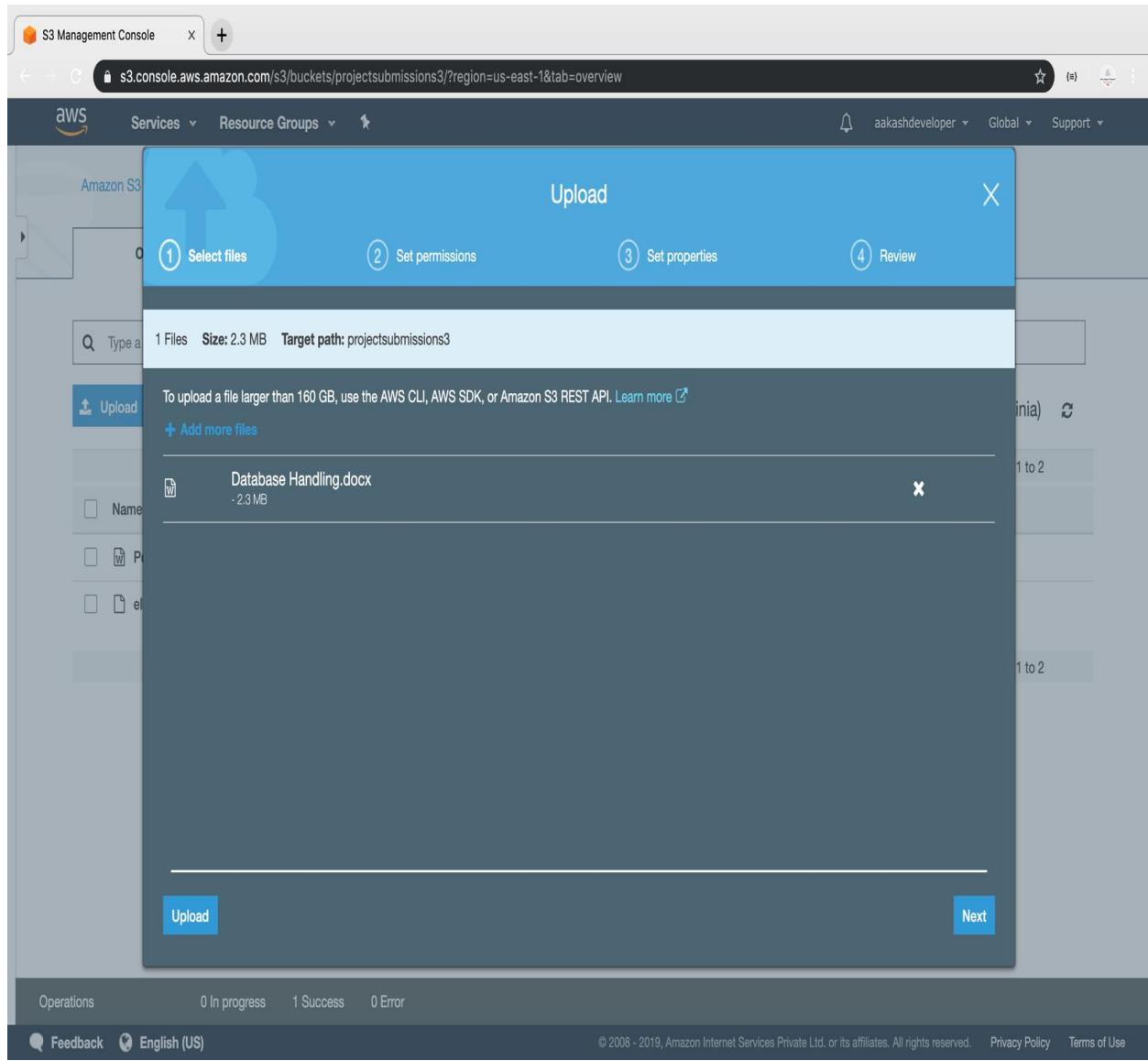
The screenshot shows the AWS S3 Management Console interface. The URL in the browser is [s3.console.aws.amazon.com/s3/buckets/projectsubmissions3/?region=us-east-1&tab=overview](https://s3.console.aws.amazon.com/s3/buckets/projectsubmissions3/?region=us-east-1&tab=overview). The page displays two files in the 'projectsubmissions3' bucket:

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 of the console, there are links for Operations (0 In progress, 1 Success, 0 Error), Feedback, English (US), and footer links for Privacy Policy and Terms of Use.

## **Step 3.14.2: Setting the storage class of an object**

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



- Select the class and click *Next*

S3 Management Console

s3.console.aws.amazon.com/s3/buckets/projectsubmissions3?region=us-east-1&tab=overview

aws Services Resource Groups

Amazon S3

Upload

Select files Set permissions Set properties Review

1 Files Size: 2.3 MB Target path: projectsubmissions3

Storage class

Choose a storage class based on your use case and access requirements. [Learn more](#) or see [Amazon S3 pricing](#)

Storage class	Designed for	Availability Zones	Min storage duration	Min billable object size	Monitoring and automation fees	Retrieval fees
<input checked="" type="radio"/> Standard	Frequently accessed data	≥ 3	-	-	-	-
<input type="radio"/> Intelligent-Tiering	Long-lived data with changing or unknown access patterns	≥ 3	30 days	-	Per-object fees apply	-
<input type="radio"/> Standard-IA	Long-lived, infrequently accessed data	≥ 3	30 days	128KB	-	Per-GB fees apply
<input type="radio"/> One Zone-IA	Long-lived, infrequently accessed, non-critical data	≥ 1	30 days	128KB	-	Per-GB fees apply
<input type="radio"/> Glacier	Archive data with retrieval times ranging from minutes to hours	≥ 3	90 days	40KB	-	Per-GB fees apply
<input type="radio"/> Glacier Deep Archive	Archive data that rarely, if ever, needs ≥ 3	180 days	40KB	-	Per-GB fees apply	-

Upload Previous Next

Operations 0 In progress 1 Success 0 Error

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

Storage class	Designed for	Availability Zones	Min storage duration	Min billable object size	Monitoring and automation fees	Retrieval fees
<input checked="" type="radio"/> Standard	Frequently accessed data	≥ 3	-	-	-	-
<input type="radio"/> Intelligent-Tiering	Long-lived data with changing or unknown access patterns	≥ 3	30 days	-	Per-object fees apply	-
<input type="radio"/> Standard-IA	Long-lived, infrequently accessed data	≥ 3	30 days	128KB	-	Per-GB fees apply
<input type="radio"/> One Zone-IA	Long-lived, infrequently accessed, non-critical data	≥ 1	30 days	128KB	-	Per-GB fees apply
<input type="radio"/> Glacier	Archive data with retrieval times ranging from minutes to hours	≥ 3	90 days	40KB	-	Per-GB fees apply
<input type="radio"/> Glacier Deep Archive	Archive data that rarely, if ever, needs ≥ 3	180 days	40KB	-	Per-GB fees apply	-

- The class will get assigned to the uploaded object

Name	Last modified	Size	Storage class
Database Handling.docx	Sep 25, 2019 9:28:46 AM GMT+0100	2.3 MB	Intelligent-Tiering
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

### Step 3.14.3: Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

```
cd <folder path>
```

- Initialize your repository using the following command:

```
git init
```

- Add all the files to your git repository using the following command:

```
git add .
```

- Commit the changes using the following command:

```
git commit . -m "Changes have been committed."
```

- Push the files to the folder you initially created using the following command:

```
git push -u origin master
```

## **Assisted Practice: 3.36 Create an IAM User**

This section will guide you to:

- Create an IAM user
- Validate the newly created IAM user

This lab has five subsections, namely:

3.15.1 Selecting the IAM from the AWS Console

3.15.2 Navigating to the user creation page

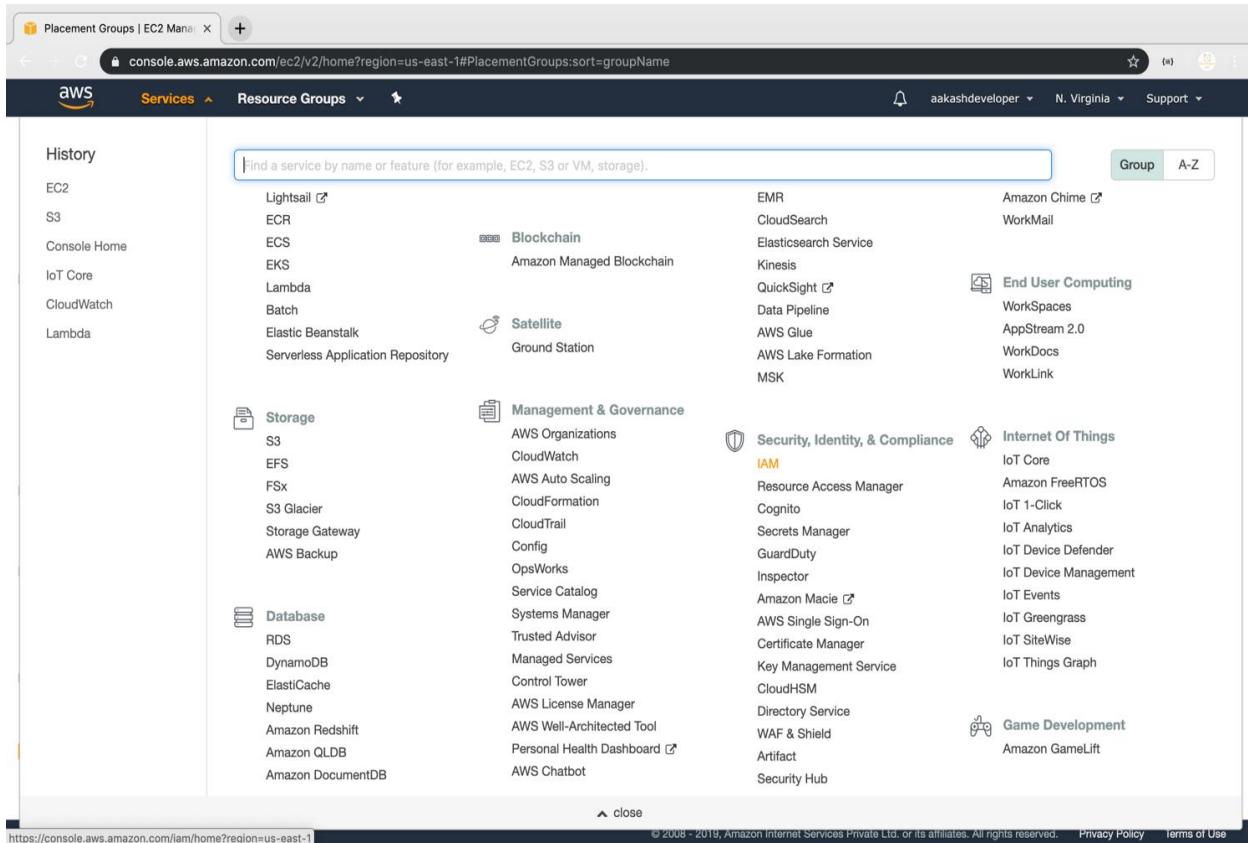
3.15.3 Changing access permissions

3.15.4 Adding an identifier

3.15.5 Pushing the files to GitHub repositories

**Step 3.15.1:** Selecting the IAM from the AWS console

- Login to your AWS console and search for IAM



### Step 3.15.2: 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. On the left, there's a sidebar with options like 'Identity and Access Management (IAM)', 'AWS Account (651759643195)', 'Dashboard', 'Groups', 'Users' (which is selected and highlighted in orange), 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Credential report'. Below that is a search bar labeled 'Search IAM'. Under 'AWS Organizations', there are links for 'Organization activity' and 'Service control policies (SCPs)'. The main area is titled 'Add user' and 'Delete user'. It contains a search bar 'Find users by username or access key' and a table with columns 'User name', 'Groups', 'Access key age', 'Password age', 'Last activity', and 'MFA'. One row is shown for 'John'. At the bottom, there are links for 'Feedback', 'English (US)', and copyright information.

### Step 3.15.3: 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 'Add user' wizard, step 1: Set user details. It has five steps numbered 1 to 5 at the top right. Step 1 is highlighted. The form has a section 'Set user details' with a note: 'You can add multiple users at once with the same access type and permissions.' It includes a 'User name\*' field with 'SimplilearnUser' entered, a link to 'Add another user', and a 'Select AWS access type' section. Under 'Access type\*', there are two options: 'Programmatic access' (unchecked) and 'AWS Management Console access' (checked). Below that is a 'Console password\*' section with 'Autogenerated password' and 'Custom password' radio buttons, and a password input field. At the bottom, there's a 'Require password reset' checkbox checked, with a note about users creating new passwords. At the very bottom are 'Cancel' and 'Next: Permissions' buttons.

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

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

**Add user to group**

[Create group](#) [Refresh](#)

Search		Showing 1 result
Group	Attached policies	
<input type="checkbox"/> devs	AmazonEC2FullAccess and 1 more	

[Cancel](#) [Previous](#) [Next: Tags](#)

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

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

**Set permissions boundary**

[Cancel](#) [Previous](#) [Next: Tags](#)

[https://console.aws.amazon.com/iam/home?region=us-east-1#/policies/arn%3aws%3lam%3aaws%3Apolicy%2FAmazonEC2ContainerRegistryFullAccess](#) | Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

### Step 3.15.4: Adding an identifier

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

The screenshot shows the AWS IAM Management Console with the URL [console.aws.amazon.com/iam/home?region=us-east-1#/users\\$new?step=tags&login&userNames=SimplilearnUser&passwordType=manual&permissionType=policies...](https://console.aws.amazon.com/iam/home?region=us-east-1#/users$new?step=tags&login&userNames=SimplilearnUser&passwordType=manual&permissionType=policies...). The page is titled 'Add User' and is on step 3 of 5. It shows a table for adding IAM tags. One tag is present: Key 'Ec2' and Value 'Ec2Admin'. There is also a placeholder 'Add new key'. Below the table, it says 'You can add 49 more tags.' At the bottom, there are buttons for 'Cancel', 'Previous', and 'Next: Review'.

Key	Value (optional)	Remove
Ec2	Ec2Admin	x
Add new key		

You can add 49 more tags.

Cancel Previous Next: Review

- 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

**Buttons:** Cancel, Previous, 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>

**User**

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

**Buttons:** Download .csv, 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

The screenshot shows the AWS IAM Management Console. On the left, there's a navigation sidebar with options like Dashboard, Groups, Users (which is selected), Roles, Policies, Identity providers, Account settings, and Credential report. A search bar for 'Search IAM' is also present. The main content area is titled 'Summary' for the user '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, tabs for Permissions, Groups, Tags (1), Security credentials (which is selected), and Access Advisor are visible. The 'Sign-in credentials' section shows a summary with a link to the console sign-in link. The 'Assigned MFA device' and 'Signing certificates' sections show 'Not assigned' and 'None' respectively. The 'Access keys' section has a 'Create access key' button and a table with columns for Access key ID, Created, Last used, and Status, showing 'No results'. The 'SSH keys for AWS CodeCommit' section is partially visible at the bottom.

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

This screenshot is similar to the previous one, showing the user summary for 'SimplilearnUser'. However, the 'Groups' tab is now selected in the navigation bar. The main content area shows the same summary information: User ARN, Path, and Creation time. The 'Groups' tab is highlighted in orange. Below it, there's a blue 'Add user to groups' button. A table for managing group attachments is shown with columns for 'Group name' and 'Attached permissions', both currently showing 'No results'.

### **Step 3.15.5:** Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

**cd <folder path>**

- Initialize your repository using the following command:

**git init**

- Add all the files to your git repository using the following command:

**git add .**

- Commit the changes using the following command:

**git commit . -m "Changes have been committed."**

- Push the files to the folder you initially created using the following command:

**git push -u origin master**

## **Assisted Practice: 3.37 Create an IAM Role**

This section will guide you to:

- Create an IAM role

This lab has four subsections, namely:

- 3.16.1 Creating an IAM role
- 3.16.2 Adding AWS policy to the role
- 3.16.3 Providing a key and a value for the role
- 3.16.4 Pushing the files to GitHub repositories

**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 with the URL <https://console.aws.amazon.com/iam/home?region=us-east-1#/roles>. The left sidebar has 'Identity and Access Management (IAM)' selected under 'AWS Account (651759643195)'. The main content area displays a list of roles with columns for Role name, Description, and Trusted entities. A search bar at the top right of the list table shows 'Showing 25 results'.

Role name	Description	Trusted entities
admin		AWS service: lambda
aws-elasticbeanstalk-ec2-role		AWS service: ec2
aws-elasticbeanstalk-service-role		AWS service: elasticbeanstalk
AWSCodePipelineServiceRole-...		AWS service: codepipeline
AWSCodePipelineServiceRole-...		AWS service: codepipeline
AWSCodePipelineServiceRole-...		AWS service: codepipeline
AWSServiceRoleForAutoScaling	Default Service-Linked Role enables access to AWS Services and...	AWS service: autoscaling (Service-Linked role)
AWSServiceRoleForCloudWatch...		AWS service: events (Service-Linked role)
AWSServiceRoleForElastiCache	This policy allows ElastiCache to manage AWS resources on your...	AWS service: elasticache (Service-Linked role)
AWSServiceRoleForElasticLoadBalancing	Allows ELB to call AWS services on your behalf.	AWS service: elasticloadbalancing (Service-...
AWSServiceRoleForRDS	Allows Amazon RDS to manage AWS resources on your behalf	AWS service: rds (Service-Linked role)

- Select the service

Create role

Select type of trusted entity

AWS service  
EC2, Lambda and others

Another AWS account  
Belonging to you or 3rd party

Web identity  
Cognito or any OpenID provider

SAML 2.0 federation  
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

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

**Lambda**  
Allows Lambda functions to call AWS services on your behalf.

API Gateway	Comprehend	ElastiCache	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	IQ	Quicksight	Textract

\* Required Cancel Next: Permissions

## Step 3.16.2: Adding AWS policy to the role

Create role

Attach permissions policies

Choose one or more policies to attach to your new role.

Policy name	Used as	Description
AmazonDMSRedshiftS3Role	None	Provides access to manage S3 settings ...
<input checked="" type="checkbox"/> 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...
s3crr_for_julyswssession_to_testwebsites312	Permissions policy (1)	

Showing 5 results

Set permissions boundary

\* Required Cancel Previous Next: Tags

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

- Add a key and a value to the role

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. [Learn more](#)

Key	Value (optional)	Remove
Ec2 access S3	Ec2 access S3	x
Add new key		

You can add 49 more tags.

Cancel Previous Next: Review

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

- Add a role:

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

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

#### Step 3.16.4: Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

**cd <folder path>**

- Initialize your repository using the following command:

**git init**

- Add all the files to your git repository using the following command:

**git add .**

- Commit the changes using the following command:

```
git commit . -m "Changes have been committed."
```

- Push the files to the folder you initially created using the following command:

```
git push -u origin master
```

## **Assisted Practice: 3.38 Create an IAM Group**

This section will guide you to:

- Create an IAM group

This lab has three subsections, namely:

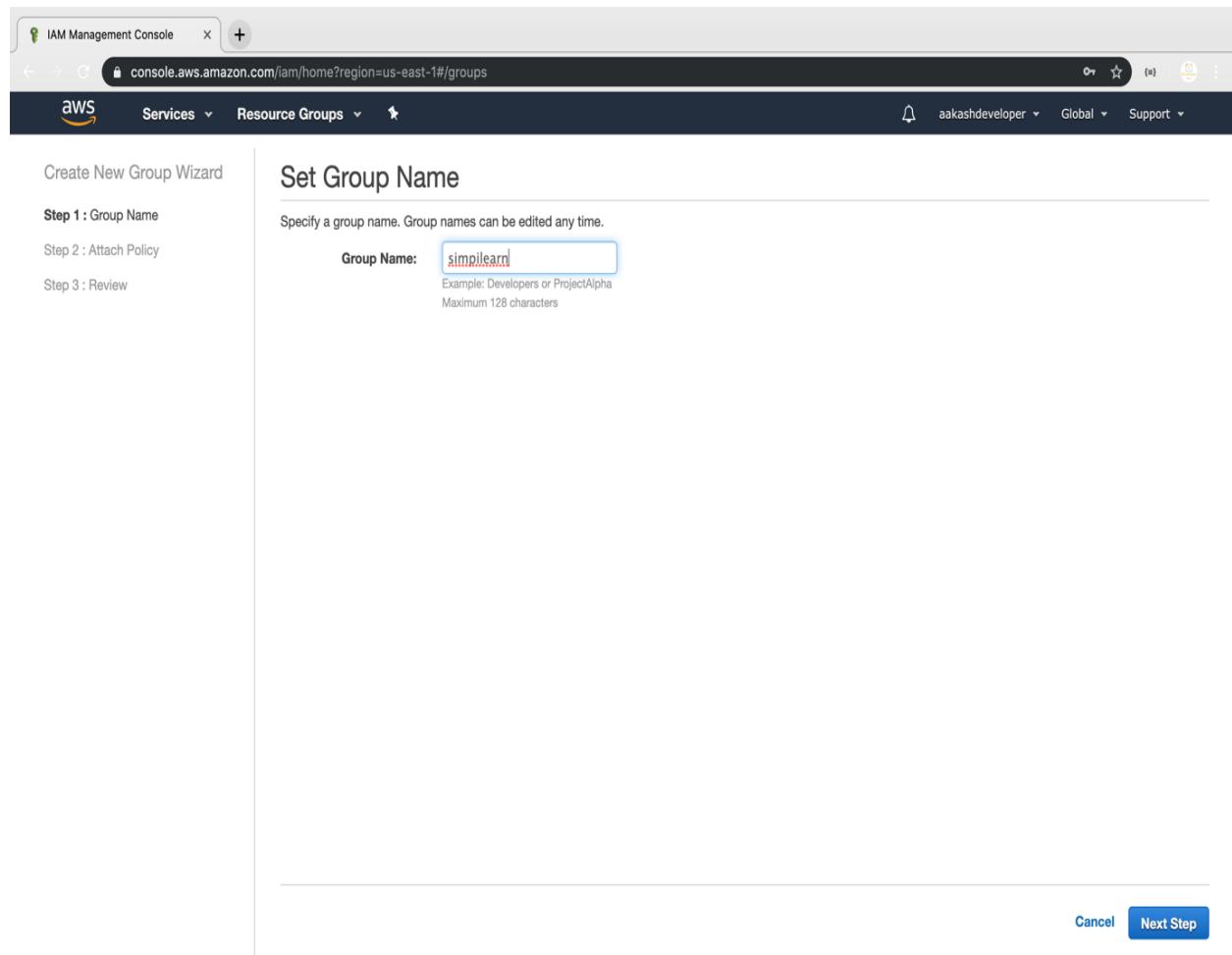
- 3.17.1 Creating an IAM group
- 3.17.2 Assigning the required policy to the group
- 3.17.3 Pushing the files to GitHub repositories

### **Step 3.17.1: 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 interface. The left sidebar navigation bar includes links for Identity and Access Management (IAM), AWS Account, Dashboard, Groups (which is highlighted in orange), Users, Roles, Policies, Identity providers, Account settings, Credential report, and a search bar labeled 'Search IAM'. The main content area is titled 'Create New Group' and displays a table with one result. The table columns are 'Group Name', 'Users', 'Inline Policy', and 'Creation Time'. The single entry is 'devs', which has 0 users and was created on 2019-09-12 10:18 UTC+0100. There are also 'Group Actions' dropdown and filter buttons at the top of the table.

- Enter the group name



### Step 3.17.2: Assigning the required policy to the group

- Assign the policy provided by AWS

IAM Management Console

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

AWS Services Resource 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"/>	AmazonEC2ContainerRegistryFul...	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-u...	1	2019-08-12 08:46 UTC+0100	2019-08-12 08:46 UTC+0100
<input type="checkbox"/>	AWSCodePipelineServiceRole-u...	1	2019-08-12 10:48 UTC+0100	2019-08-12 10:48 UTC+0100
<input type="checkbox"/>	AWSCodePipelineServiceRole-u...	1	2019-08-26 16:10 UTC+0100	2019-08-26 16:10 UTC+0100
<input type="checkbox"/>	AWSElasticBeanstalkEnhancedH...	1	2016-02-08 23:17 UTC+0100	2018-04-09 23:12 UTC+0100
<input type="checkbox"/>	AWSElasticBeanstalkMulticontai...	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

Filter: Policy Type Search

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 has 'Identity and Access Management (IAM)' selected under 'AWS Account (651759643195)'. The main content area shows a table of groups:

Group Name	Users	Inline Policy	Creation Time
devs	0		2019-09-12 10:18 UTC+0100
simplelearn	0		2019-09-21 19:49 UTC+0100

At the bottom, there are links for Feedback, English (US), 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/simplelearn](https://console.aws.amazon.com/iam/home?region=us-east-1#/groups/simplelearn). The left sidebar has 'Identity and Access Management (IAM)' selected under 'AWS Account (651759643195)'. The main content area shows the 'Summary' tab for the 'simplelearn' group:

Group ARN:	arn:aws:iam::651759643195:group/simplelearn
Users (in this group):	0
Path:	/
Creation Time:	2019-09-21 19:49 UTC+0100

Below the summary, there are tabs for 'Users' (selected), 'Permissions', and 'Access Advisor'. A message says '⚠ This group does not contain any users.' with a 'Add Users to Group' button.

At the bottom, there are links for Feedback, English (US), Privacy Policy, and Terms of Use.

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

Select users to add to the group **simplilearn**

<input type="checkbox"/>	User Name	Groups	Password	Password Last Used	Access Keys	Creation Time
<input type="checkbox"/>	John	0	✓	2019-09-12 10:15 UTC+0100	None	2019-09-12 10:13 UT...
<input checked="" type="checkbox"/>	SimplilearnUser	0	✓	Never	None	2019-09-21 19:45 UT...

**Add Users**

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

**IAM > Groups > simplilearn**

Summary

Group ARN: arn:aws:iam::651759643195:group/simplilearn

Users (in this group): 1

Path: /

Creation Time: 2019-09-21 19:49 UTC+0100

**Users** **Permissions** **Access Advisor**

This view shows all users in this group: 1 User

User	Actions
SimplilearnUser	Remove User from Group

### **Step 3.17.3:** Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

**cd <folder path>**

- Initialize your repository using the following command:

**git init**

- Add all the files to your git repository using the following command:

**git add .**

- Commit the changes using the following command:

**git commit . -m "Changes have been committed."**

- Push the files to the folder you initially created using the following command:

**git push -u origin master**

# Assisted Practice: 3.39 Policies and Permissions

This section will guide you to:

- Implement policies and permissions on an S3 bucket

This lab has three subsections, namely:

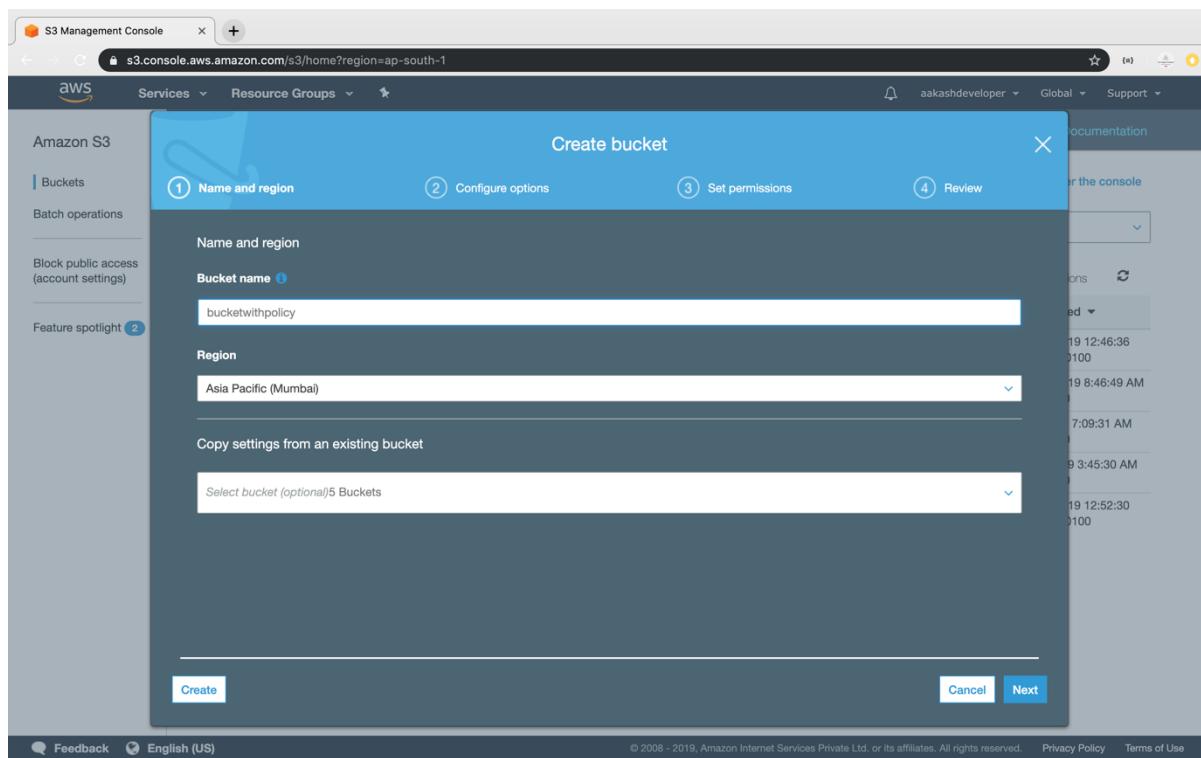
3.18.1 Creating a bucket

3.18.2 Adding policies

3.18.3 Pushing the files to GitHub repositories

## **Step 3.18.1:** Creating a bucket

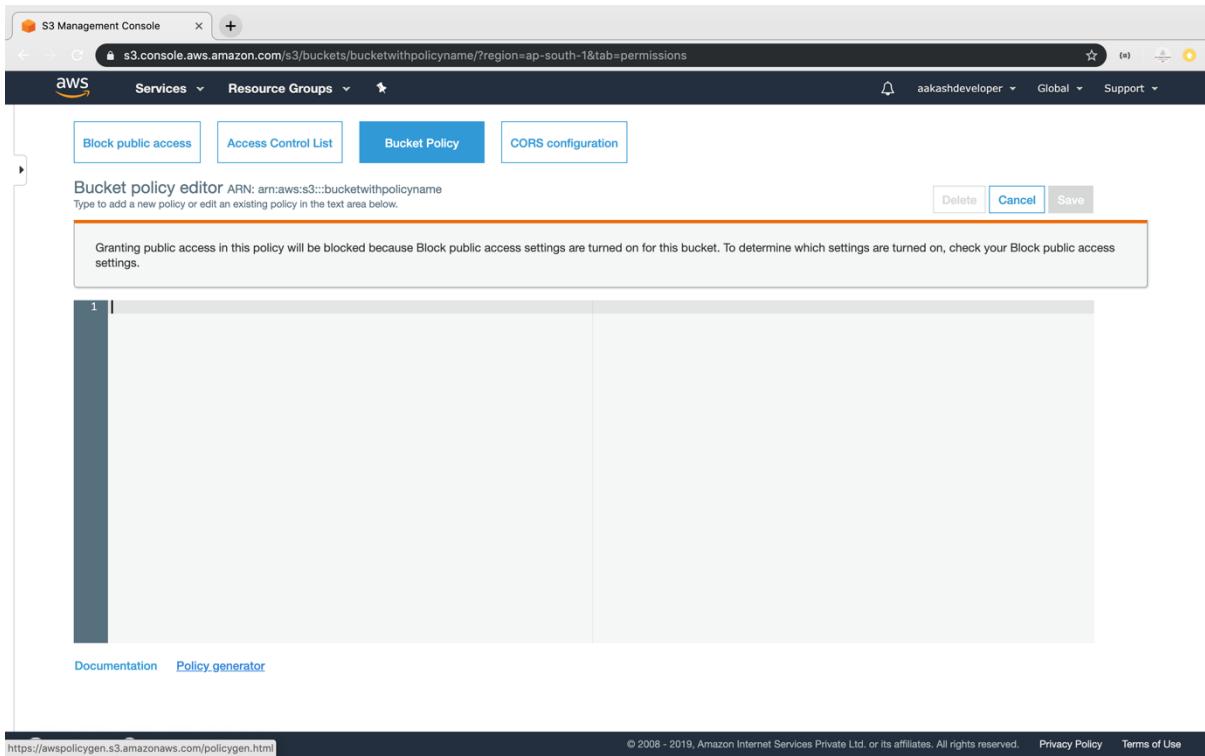
- Create a new bucket in which we want to add policy with all default settings.



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

### Step 3.18.2: Adding policies

- Click on the *Policy Generator*.



- 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 (radio button selected) Deny

Principal: [empty input field]

AWS Service: Amazon S3 (radio button selected) All Services (\*)

Actions: 1 Action(s) Selected (dropdown menu) All Actions (\*)

Amazon Resource Name (ARN): [empty input field]

Actions dropdown menu (selected item: CreateBucket):

- AbortMultipartUpload
- CreateBucket (checkbox checked)
- CreateJob
- DeleteBucket
- DeleteBucketPolicy
- DeleteBucketWebsite
- DeleteObject
- DeleteObjectTagging

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 (radio button selected) Deny

Principal: Allow Creation

AWS Service: Amazon S3 (radio button selected) All Services (\*)

Actions: 1 Action(s) Selected (dropdown menu) All Actions (\*)

Amazon Resource Name (ARN): arn:aws:s3:::bucketwill

Add Conditions (Optional)

Add Statement

Step 3: Generate Policy

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

S3 Management Console    AWS Policy Generator

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

**Effect**  Allow  Deny

**Principal**

Use a comma to separate multiple values.

**AWS Service**  Amazon S3  All Services (\*)

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

**Actions** -- Select Actions --  All Actions (\*)

**Amazon Resource Name (ARN)**

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**

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

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

**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.

**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.

S3 Management Console    AWS Policy Generator

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

**Effect**  Allow  Deny

**Principal**

Use a comma to separate multiple values.

**AWS Service**  Amazon S3  All Services (\*)

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

**Policy JSON Document**

Click below to edit. To save the policy, copy the text below to a text editor.  
Changes made below will not be reflected in the policy generator tool.

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

You added the following statements:

Principal	Effect	Action	Resource	Conditions
+ Allow Creation	Allow	+ s3:CreateBucket	arn:aws:s3:::bucketwithpolicyname	None

**Step 3: Generate Policy**

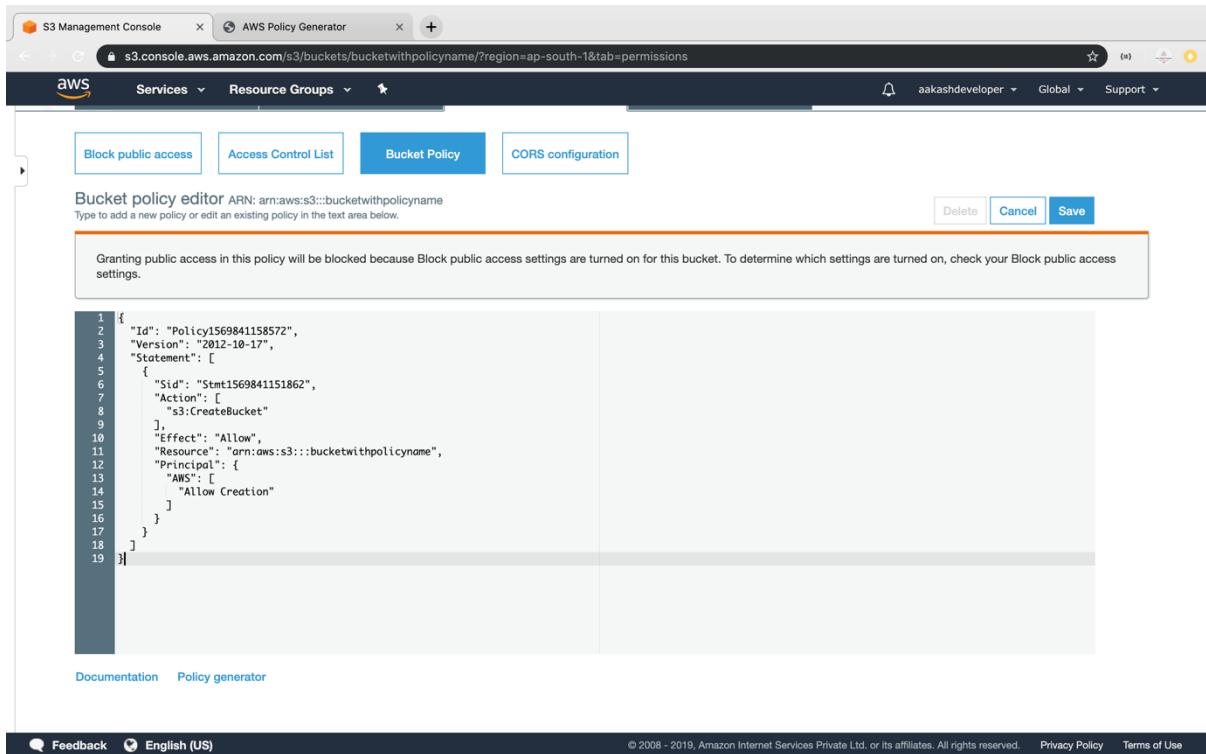
A policy is a document (written in the Access Policy Language) that acts as a container for one or more statements.

**Close**

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

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



```

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 }

```

Documentation Policy generator

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

### Step 3.18.3: Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

**cd <folder path>**

- Initialize your repository using the following command:

**git init**

- Add all the files to your git repository using the following command:

**git add .**

- Commit the changes using the following command:

```
git commit . -m "Changes have been committed."
```

- Push the files to the folder you initially created using the following command:

```
git push -u origin master
```

# Assisted Practice: 3.41 Empty an S3 Bucket

This section will guide you to:

- Empty an S3 bucket

This lab has three subsections, namely:

3.13.1 Selecting the S3 bucket you want to empty

3.13.2 Emptying the bucket

3.13.3 Pushing the files to GitHub repositories

**Step 3.13.1:** Selecting the S3 bucket you want to empty

The screenshot shows the AWS S3 Management Console interface. On the left, there's a sidebar with options like 'Buckets' (which is selected), '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 shown, with 'projectsubmissions3' selected. A modal window for 'projectsubmissions3' is open, displaying its properties, permissions, and management settings. The properties tab shows details like 'Events 0 Active notifications', 'Versioning Disabled', and 'Logging Enabled'. The permissions tab shows the owner as 'akashdeveloper22' and various access controls. The management tab shows lifecycle, replication, analytics, inventory, and metrics settings.

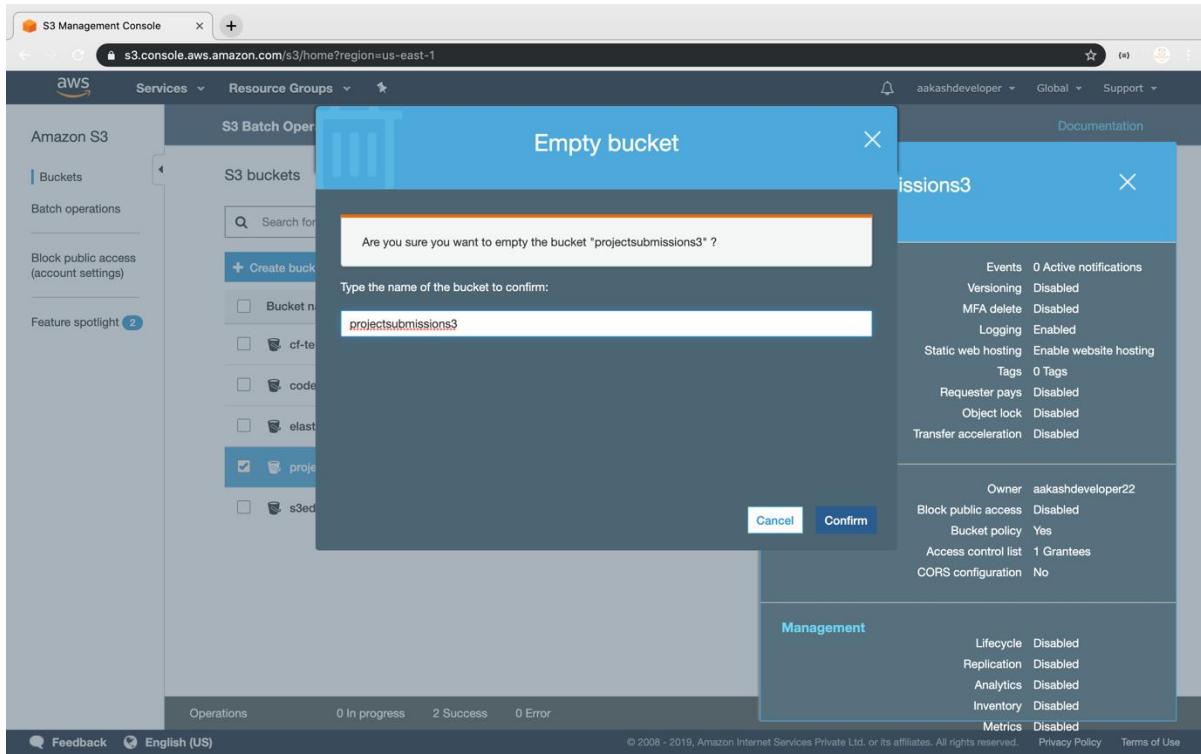
### Step 3.13.2: Emptying the bucket

- Verify the content present in the bucket

The screenshot shows the AWS S3 Management Console interface. The URL in the address bar is [s3.console.aws.amazon.com/s3/buckets/projectsubmissions3?region=us-east-1&tab=overview](https://s3.console.aws.amazon.com/s3/buckets/projectsubmissions3?region=us-east-1&tab=overview). The top navigation bar includes the AWS logo, Services dropdown, Resource Groups dropdown, a user account (akashdeveloper), Global dropdown, and Support dropdown. The main navigation bar shows 'Amazon S3 > projectsubmissions3'. Below this is a tab bar with 'Overview' (selected), 'Properties', 'Permissions', and 'Management'. A search bar contains the placeholder 'Type a prefix and press Enter to search. Press ESC to clear.' Below the search bar are buttons for 'Upload', '+ Create folder', 'Download', and 'Actions'. To the right of these buttons is the region 'US East (N. Virginia)' with a refresh icon. The main content area displays a table of objects. The table has columns: Name, Last modified, Size, and Storage class. One object is listed: 'index.html' was last modified on Aug 4, 2019 at 3:45:59 AM GMT+0100, has a size of 132.0 B, and is stored in the Standard storage class. At the bottom of the page, there is a footer with 'Operations' (0 In progress, 2 Success, 0 Error), a feedback link, language selection ('English (US)'), and legal links ('© 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.', 'Privacy Policy', 'Terms of Use').

Name	Last modified	Size	Storage class
index.html	Aug 4, 2019 3:45:59 AM GMT+0100	132.0 B	Standard

- Empty the bucket



### Step 3.13.3: Pushing the code to your GitHub repositories

- Open your command prompt and navigate to the folder where you have created your files.

**cd <folder path>**

- Initialize your repository using the following command:

**git init**

- Add all the files to your git repository using the following command:

**git add .**

- Commit the changes using the following command:

**git commit . -m "Changes have been committed."**

- Push the files to the folder you initially created using the following command:

```
git push -u origin master
```