

Lab Assignment-1

ECSE373L: Cloud Infrastructure and Services

Name: Tanvi Penumudy
Enroll no: E18CSE187
Batch: EB02

Lab Activities:

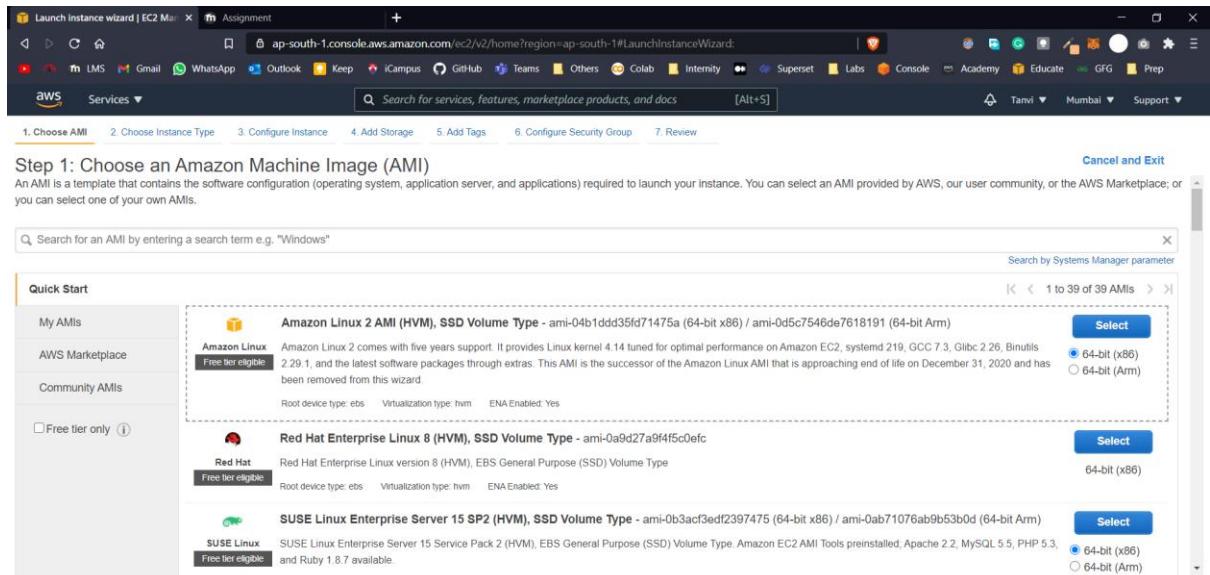
Lab Activity 1: Launch the AWS Linux instance and connect it using PuTTY.

Lab Activity 2: Explore the AWS IAM Service @ Lab Module 4 of AWS Academy Cloud Foundation Course.

Implementation Screenshots (Step-by-Step):

Lab Activity 1

Choose AMI:



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

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

Quick Start

Category	AMI Name	Description	Select
My AMIs	Amazon Linux	Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-04b1ddd35d71475a (64-bit x86) / ami-0d5c7546de7618191 (64-bit Arm)	<input checked="" type="radio"/> 64-bit (x86) <input type="radio"/> 64-bit (Arm)
AWS Marketplace	Red Hat	Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-0a8d27a9ff5c0efc	<input type="radio"/> 64-bit (x86) <input checked="" type="radio"/> 64-bit (Arm)
Community AMIs	SUSE Linux	SUSE Linux Enterprise Server 15 SP2 (HVM), SSD Volume Type - ami-0b3acf3edf2397475 (64-bit x86) / ami-0ab71076ab9b53b0d (64-bit Arm)	<input type="radio"/> 64-bit (x86) <input checked="" type="radio"/> 64-bit (Arm)



Choose 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 families Current generation ShowHide Columns

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

Configure Instance:

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-f586699e (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

Domain join directory: No directory Create new directory

IAM role: None Create new IAM role

CPU options: Specify CPU options

Shutdown behavior: Stop

Cancel Previous Review and Launch Next: Add Storage

Add Storage:

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-06f54b142aaa48c61	20	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

Add Tags:

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	(128 characters maximum)	Value	(256 characters maximum)	Instances	Volumes
Name		Linuxwebserver		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

Configure Security Group:

A screenshot of the AWS Launch Instance Wizard Step 6: Configure Security Group. The page title is "Configure Security Group". Below it, a sub-section title "Step 6: Configure Security Group" is shown. A paragraph explains that a security group is a set of firewall rules that control the traffic for your instance. It mentions that you can add rules to allow specific traffic to reach your instance, such as setting up a web server and allowing Internet traffic. It also notes that you can create a new security group or select an existing one. A "Warning" box at the bottom states: "Rules with source of 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." The main content area contains a table with columns: Type, Protocol, Port Range, Source, and Description. There are three rows of rules: 1. SSH (Protocol TCP, Port Range 22, Source Custom 0.0.0.0/0, Description e.g. SSH for Admin Desktop). 2. HTTP (Protocol TCP, Port Range 80, Source Anywhere 0.0.0.0/0, Description e.g. SSH for Admin Desktop). 3. HTTPS (Protocol TCP, Port Range 443, Source Anywhere 0.0.0.0/0, Description e.g. SSH for Admin Desktop). An "Add Rule" button is located below the table.

Review Instance Launch:

A screenshot of the AWS Launch Instance Wizard Step 7: Review Instance Launch. The page title is "Review Instance Launch". Below it, a sub-section title "Step 7: Review Instance Launch" is shown. A paragraph asks the user to review their instance launch details and provides a link to edit changes. A "Warning" box at the top right of the content area says: "⚠ Improve your instances' security. Your security group, ECSE187Lab1, is open to the world. Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups". The main content area has three sections: 1. "AMI Details": Shows the selected AMI as "Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-04b1ddd35fd71475a". It includes a note about five years support and a table showing Root Device Type: ebs and Virtualization type: hvm. 2. "Instance Type": Shows the selected instance type as "t2.micro" with 1 ECUs, 1 vCPUs, 1 GiB Memory, EBS only storage, and Low to Moderate Network Performance. 3. "Security Groups": Shows the selected security group as "ECSE187Lab1". There is a link "Edit security groups" next to it. At the bottom, there are "Cancel", "Previous", and "Launch" buttons.

Creating New Key-Pair:

The screenshot shows the AWS Launch Instance Wizard at Step 7: Review Instance Launch. A modal window titled "Select an existing key pair or create a new key pair" is displayed, asking for a key pair name (E18CSE187Lab1CIS) and providing a download link. The main wizard page includes sections for AMI Details, Instance Type (t2.micro), and Security Groups.

Launch Status:

The screenshot shows the AWS Launch Instance wizard at the Launch Status page. It displays a green box with a checkmark indicating "Your instances are now launching" and a blue box with a reminder to "Get notified of estimated charges". Below these are sections for "How to connect to your instances" and "Here are some helpful resources to get you started".

The screenshot shows the AWS EC2 Management Console interface. The left sidebar is collapsed, and the main area displays the 'Instances' page. A search bar at the top right contains the placeholder 'Search for services, features, marketplace products, and docs'. Below it, a button labeled '[Alt+S]' is visible.

The 'Instances' table lists two instances:

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
<input checked="" type="checkbox"/>	Linuxwebserver	i-0e6206b5b01110bb0	Running	t2.micro	2/2 checks ...	No alarms	+ ap-south-1a	ec2-52-66-198-1
<input type="checkbox"/>	E18CSE187L...	i-058b5b48370f41ab9	Termina...	t2.micro	-	No alarms	+ ap-south-1b	-

Below the table, a modal window is open for the instance **i-0e6206b5b01110bb0 (Linuxwebserver)**. The modal has tabs for Details, Security, Networking, Storage, Status Checks, Monitoring, and Tags. The Details tab is selected, showing the following information:

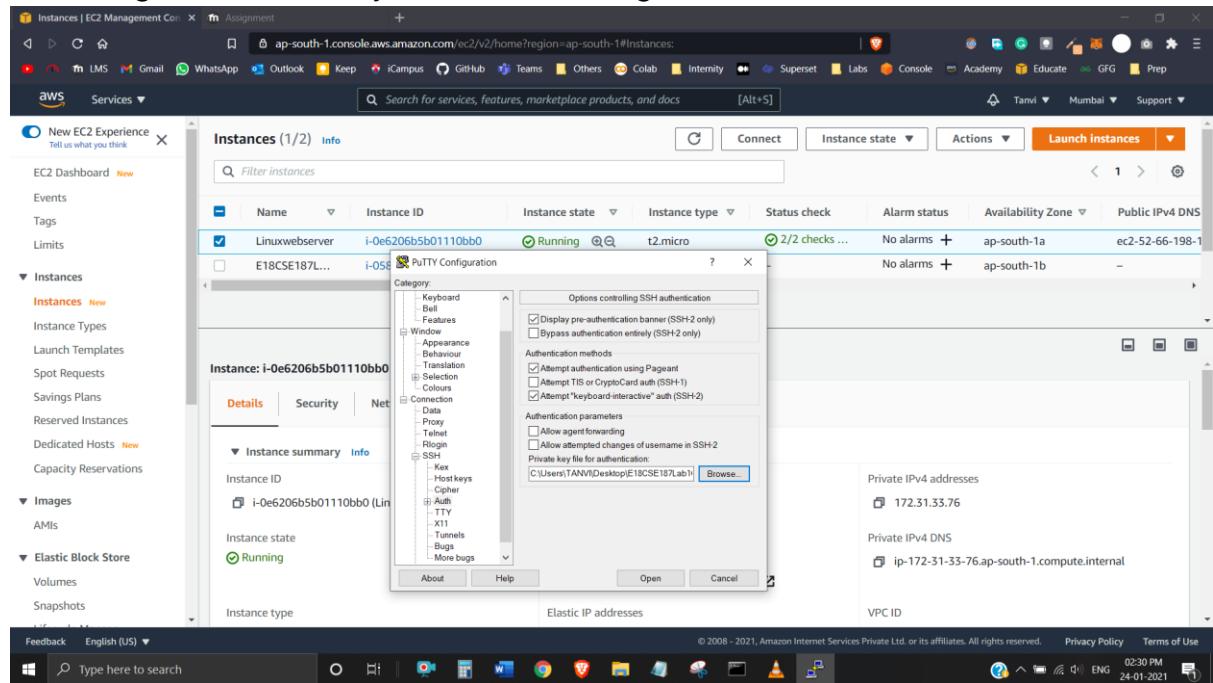
Instance summary	
Instance ID	i-0e6206b5b01110bb0 (Linuxwebserver)
Instance state	Running
Instance type	
Public IPv4 address	52.66.198.194 open address
Public IPv4 DNS	ec2-52-66-198-194.ap-south-1.compute.amazonaws.com open address
Elastic IP addresses	
VPC ID	

Loading .PEM File and Saving Private Key using PuTTYgen:

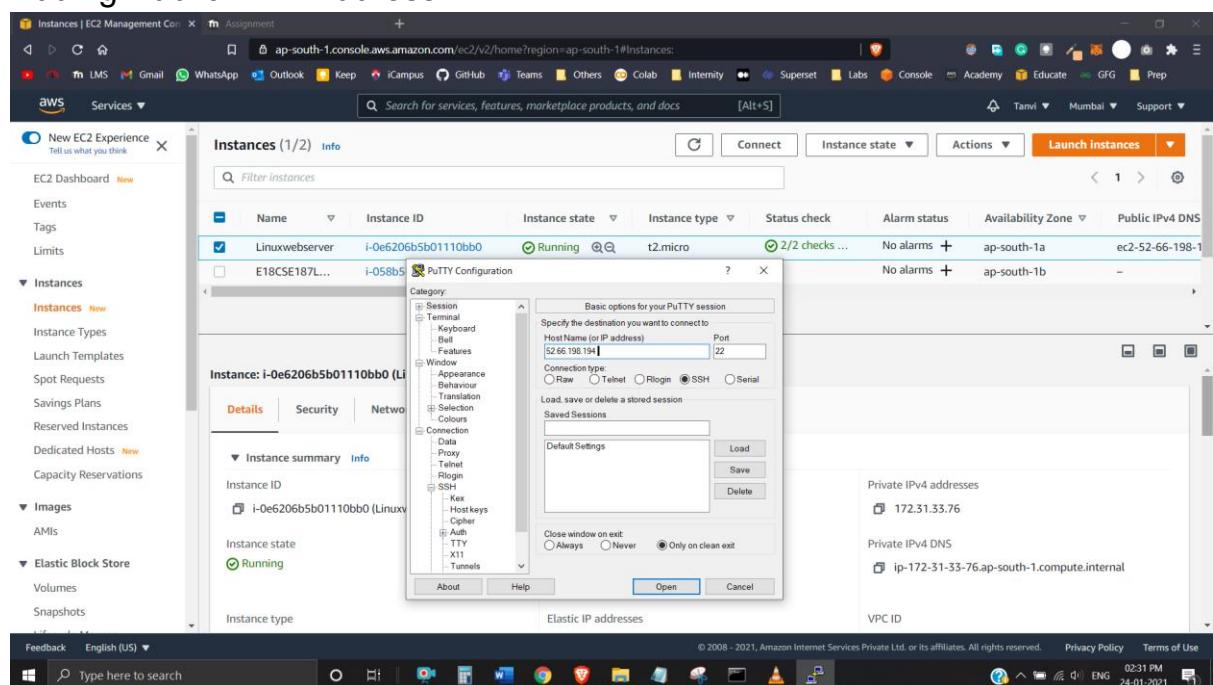
The screenshot shows the AWS EC2 Management Console with the following details:

- Instances (1/2) Info**: Shows two instances: **Linuxwebserver** (i-0e6206b5b01110bb0) and **E18CSE187...** (i-058b5b4d).
- Actions**: Buttons for **Launch instances**, **Instance state**, and **Actions**.
- Putty Key Generator** dialog box is open for the selected instance (i-0e6206b5b01110bb0). It displays:
 - Key**: Public key for pasting into OpenSSH authorized_keys file.
 - Key fingerprint**: ssh-rsa 2048 07:57:76:40:37:79:98:ce:45:87:1b:1a:6c:43:c2
 - Key comment**: imported-openkey
 - Key passphrase**: (empty)
 - Actions**: Buttons for **Generate**, **Load**, **Save public key**, and **Save private key**.
- Details** tab for the instance shows:
 - Instance summary**: Instance ID i-0e6206b5b01110bb0 (Linux web server).
 - Instance state**: Running.
 - Instance type**: Not explicitly listed in the screenshot.
- Network interfaces**: Shows interface ec2-52-66-198-194.ap-south-1.compute.internal with Private IPv4 address 172.31.33.76 and Private IPv4 DNS ip-172-31-33-76.ap-south-1.compute.internal.
- VPC ID**: VPC ID is listed as VPC ID.
- Feedback**: English (US) dropdown.
- Footer**: © 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use.

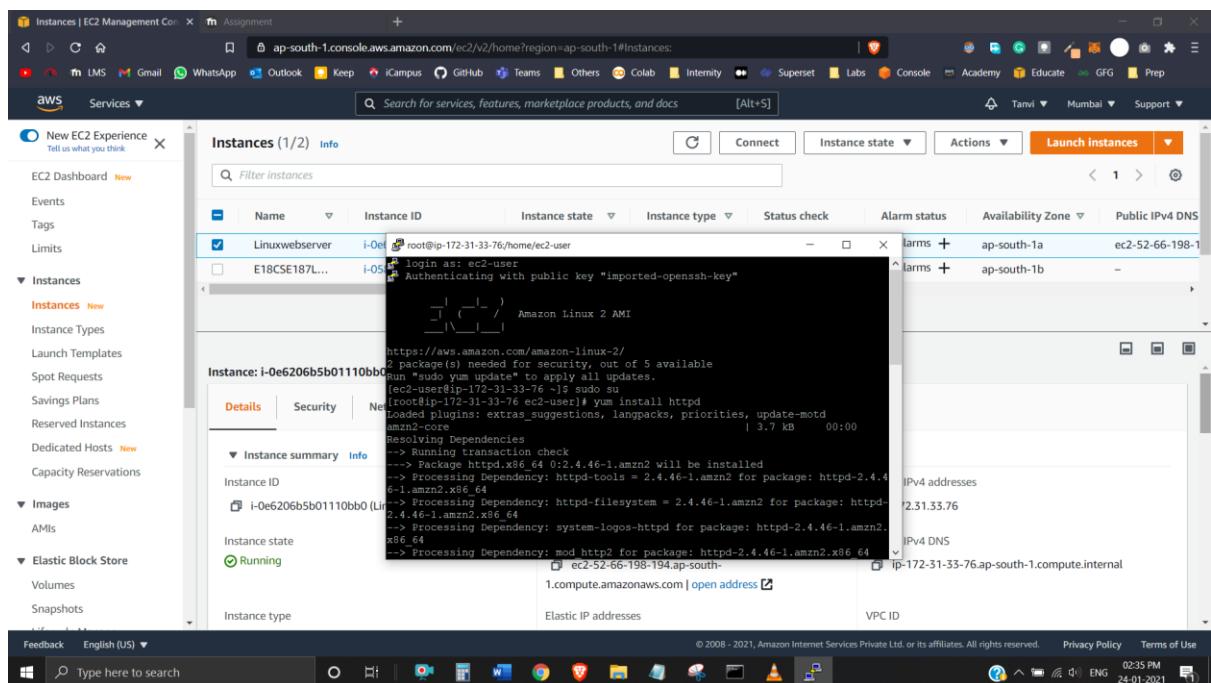
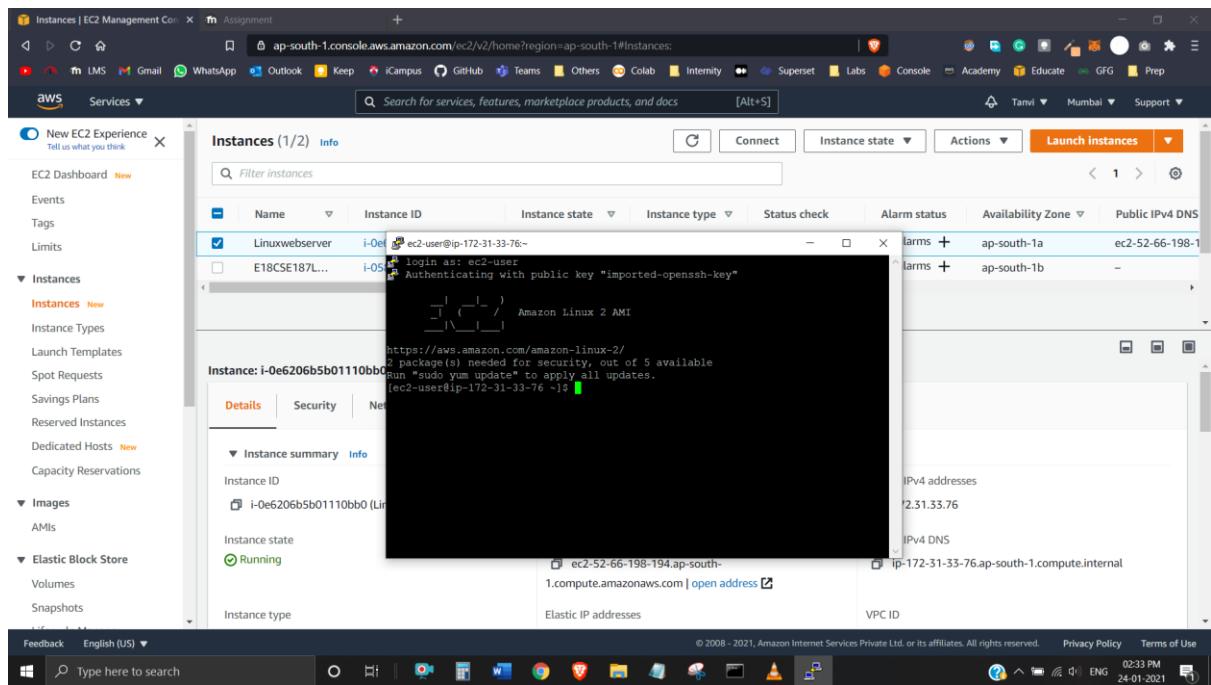
Browsing for Private Key in PuTTY Configure:



Adding Public IPv4 Address:



Connected:



Screenshot of the AWS EC2 Management Console showing the Instances page. The instance 'Linuxwebserver' (i-0e6206b5b01110bb0) is selected. The instance summary shows it is running. The terminal pane shows the command 'service httpd start' being run.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Linuxwebserver	i-0e6206b5b01110bb0	Running	t2.micro	Passing	OK	ap-south-1a	ec2-52-66-198-1
E18CSE187L...	i-05...	Verifying	t2.micro	Passing	OK	ap-south-1b	-

```
[root@ip-172-31-33-76 ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@ip-172-31-33-76 ~]#
```

Screenshot of the AWS EC2 Management Console showing the Instances page. The instance 'Linuxwebserver' (i-0e6206b5b01110bb0) is selected. The instance summary shows it is running. The terminal pane shows the command 'service httpd start' being run.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Linuxwebserver	i-0e6206b5b01110bb0	Running	t2.micro	Passing	OK	ap-south-1a	ec2-52-66-198-1
E18CSE187L...	i-05...	Verifying	t2.micro	Passing	OK	ap-south-1b	-

```
[root@ip-172-31-33-76 ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@ip-172-31-33-76 ~]#
```

Checking Status:

Instances (1/2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
<input checked="" type="checkbox"/> Linuxwebserver	i-0e6206b5b01110bb0	Running	t2.micro	Active: active (running)	-	ap-south-1a	ec2-52-66-198-1
E18CSE187...	i-058b5b48370f41ab9	Terminated	-	-	-	ap-south-1b	-

Instance: i-0e6206b5b01110bb0 (Linuxwebserver)

Details **Security** **Networking**

Instance summary Info

Instance ID: i-0e6206b5b01110bb0 (Linuxwebserver)

Instance state: Running

Instance type: t2.micro

Elastic IP addresses: 52.66.198.194 | open address

VPC ID: ec2-52-66-198-1

Running on <http://52.66.198.194>:

Test Page for the Apache HTTP Server

Test Page

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

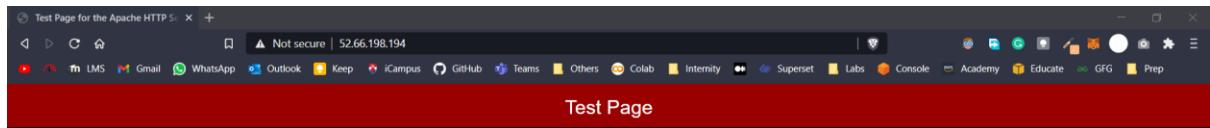
If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you are the website administrator:

You may now add content to the directory /var/www/html/. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the underlined instructions.

```
[root@ip-172-31-33-76 ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@ip-172-31-33-76 ~]# systemctl status httpd.service
● httpd.service - The Apache HTTP Server
    Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
    Active: active (running) since Sun 2021-01-24 09:07:02 UTC; 29s ago
      Docs: man:httpd.service(8)
   Main PID: 3465 (httpd)
      Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec: 0 B/sec"
         CGroup: /system.slice/httpd.service
                 ├─3485 /usr/sbin/httpd -DFOREGROUND
                 ├─3486 /usr/sbin/httpd -DFOREGROUND
                 ├─3487 /usr/sbin/httpd -DFOREGROUND
                 ├─3488 /usr/sbin/httpd -DFOREGROUND
                 ├─3489 /usr/sbin/httpd -DFOREGROUND
                 └─3490 /usr/sbin/httpd -DFOREGROUND
[root@ip-172-31-33-76 ~]#
```



This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

```
[root@ip-172-31-33-76 ec2-user]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@ip-172-31-33-76 ec2-user]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor prese
t: disabled)
     Active: active (running) since Sun 2021-01-24 09:07:02 UTC; 17min ago
       Docs: man:httpd.service(8)
      Main PID: 3485 (httpd)
        Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes se
rved/sec: 0 B/sec"
         CPU: 0.000 CPU(s) since start
          Tasks: 1 (limit: 4634)
          Group: /system.slice/httpd.service
              └─3485 /usr/sbin/httpd -DFOREGROUND
                  ├─3486 /usr/sbin/httpd -DFOREGROUND
                  ├─3487 /usr/sbin/httpd -DFOREGROUND
                  ├─3488 /usr/sbin/httpd -DFOREGROUND
                  ├─3489 /usr/sbin/httpd -DFOREGROUND
                  ├─3490 /usr/sbin/httpd -DFOREGROUND

Jan 24 09:07:02 ip-172-31-33-76.ap-south-1.compute.internal systemd[1]: Start...
Jan 24 09:07:02 ip-172-31-33-76.ap-south-1.compute.internal systemd[1]: Start...
Hint: Some lines were ellipsized, use -l to show in full.
[root@ip-172-31-33-76 ec2-user]#
```

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the image below on web sites powered by the Apache HTTP Server:



Stopping:

Instance ID	Name	Image	InstanceState	Public IPv4 DNS	Private IPv4 DNS	IPv4 Addresses
i-0e6206b5b01110bb0	Linuxwebserver		Running	52.66.198.194 open address	172.31.33.76	
i-05...	E18CSE18L...		Stopped	ec2-52-66-198-1.ap-south-1.compute.internal	ip-172-31-33-76.ap-south-1.compute.internal	

Lab Activity 2 (On AWS Academy)

Task 1: Explore the Users and Groups

Exploring Users:

The screenshot shows the IAM Management Console in a web browser. The left sidebar is titled 'Identity and Access Management (IAM)' and includes sections for Dashboard, Access management (Groups, Users, Roles, Policies), Access reports (Archive rules, Analyzers, Settings), Credential report, Organization activity, and Service control policies (SCPs). The main content area is titled 'Add user' and 'Delete user'. A search bar at the top says 'Find users by username or access key'. Below it is a table with the following data:

User name	Groups	Access key age	Password age	Last activity	MFA
awsstudent		None	None		
user-1	None	None	Today	None	Not enabled
user-2	None	None	Today	None	Not enabled
user-3	None	None	Today	None	Not enabled

Exploring Groups:

The screenshot shows the IAM Management Console in a web browser. The left sidebar is identical to the previous screenshot. The main content area is titled 'Create New Group' and 'Group Actions'. A search bar at the top says 'Search'. Below it is a table with the following data:

Group Name	Users	Inline Policy	Creation Time
EC2-Admin	0	✓	2021-01-24 12:13 UTC+0530
EC2-Support	0		2021-01-24 12:13 UTC+0530
S3-Support	0		2021-01-24 12:13 UTC+0530

Each user is assigned a Console Password:

The screenshot shows the AWS IAM Management Console for a user named 'user-1'. The 'Security credentials' tab is selected. It displays the following details:

- User ARN: arn:aws:iam::123456789012:user/sp166/user-1
- Path: /sp166/
- Creation time: 2021-01-24 12:13 UTC+0530
- Sign-in credentials:
 - Console password: Enabled (never signed in) | Manage
 - Assigned MFA device: Not assigned | Manage
 - Signing certificates: None
- Access keys:
 - Create access key
 - Access key ID: sp166user-1
 - Created: 2021-01-24
 - Last used: N/A
 - Status: Active

EC2-Admin Group – Has Inline Policy:

The screenshot shows the AWS IAM Management Console for a group named 'EC2-Admin'. The 'Permissions' tab is selected. A modal window titled 'Show Policy' displays the following inline policy:

```
{ "Version": "2012-10-17", "Statement": [ { "Action": [ "ec2:Describe*", "ec2:StartInstances", "ec2:StopInstances" ], "Resource": [ "*" ], "Effect": "Allow" } ] }
```

The policy is named 'EC2-Admin-Policy'.

EC2-Support Group – Has Managed Policy (AmazonEC2ReadOnlyAccess):

The screenshot shows the AWS IAM Management Console with the EC2-Support group selected. The 'Permissions' tab is active, showing the attached managed policy 'AmazonEC2ReadOnlyAccess'. The policy document is displayed in a modal window:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:Describe",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:ListMetrics",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:Describe"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "autoscaling:Describe",
            "Resource": "*"
        }
    ]
}
```

S3-Support group – Has Managed Policy (AmazonS3ReadOnlyAccess):

The screenshot shows the AWS IAM Management Console with the S3-Support group selected. The 'Permissions' tab is active, showing the attached managed policy 'AmazonS3ReadOnlyAccess'. The policy document is displayed in a modal window:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get",
                "s3>List"
            ],
            "Resource": "*"
        }
    ]
}
```

Task 2: Add Users to Groups

Added user-1 to S3-Support Group:

The screenshot shows the AWS IAM Management Console with the URL <https://console.aws.amazon.com/iam/home?region=us-east-1#/groups/S3-Support>. The left sidebar is open, showing the 'Groups' section under 'Access management'. The main panel displays the 'Summary' for the 'S3-Support' group. The group ARN is arn:aws:iam::14294228477:group/spi66/S3-Support. It contains 1 user, with a path of /spi66/. The creation time is 2021-01-24 12:13 UTC+0530. Below the summary, there are tabs for 'Users', 'Permissions', and 'Access Advisor'. The 'Users' tab shows a table with one row for 'user-1', with a 'Remove User from Group' button next to it. The status bar at the bottom indicates the date as 24-01-2021.

Added user-2 to EC2-Support Group:

The screenshot shows the AWS IAM Management Console with the URL <https://console.aws.amazon.com/iam/home?region=us-east-1#/groups/EC2-Support>. The left sidebar is open, showing the 'Groups' section under 'Access management'. The main panel displays the 'Summary' for the 'EC2-Support' group. The group ARN is arn:aws:iam::14294228477:group/spi66/EC2-Support. It contains 1 user, with a path of /spi66/. The creation time is 2021-01-24 12:13 UTC+0530. Below the summary, there are tabs for 'Users', 'Permissions', and 'Access Advisor'. The 'Users' tab shows a table with one row for 'user-2', with a 'Remove User from Group' button next to it. The status bar at the bottom indicates the date as 24-01-2021.

Added user-3 to EC2-Admin Group:

The screenshot shows the AWS IAM Management Console with the URL <https://console.aws.amazon.com/iam/home?region=us-east-1#/groups/EC2-Admin>. The left sidebar is expanded to show the 'Groups' section. The main content area displays the 'Summary' tab for the 'EC2-Admin' group. Key details shown include:

- Group ARN: arn:aws:iam::142942228477:group/spi66/EC2-Admin
- Users (in this group): 1
- Path: /spi66/
- Creation Time: 2021-01-24 12:13 UTC+0530

The 'Users' tab is selected, showing a table with one user entry:

User	Actions
user-3	Remove User from Group

At the bottom right of the main content area, there are two buttons: 'Remove Users from Group' and 'Add Users to Group'.

The screenshot shows the AWS IAM Management Console with the URL <https://console.aws.amazon.com/iam/home?region=us-east-1#/groups>. The left sidebar is expanded to show the 'Groups' section. The main content area displays a table of existing groups:

Group Name	Users	Inline Policy	Creation Time
EC2-Admin	1	✓	2021-01-24 12:13 UTC+0530
EC2-Support	1		2021-01-24 12:13 UTC+0530
S3-Support	1		2021-01-24 12:13 UTC+0530

At the top of the main content area, there are buttons for 'Create New Group' and 'Group Actions'. A search bar is also present at the top of the table.

Task 3: Sign-In and Test Users

User-1 can view list of Amazon S3 buckets and their contents:

The screenshot shows the AWS S3 Management Console interface. On the left, there is a sidebar with various options like Buckets, Storage Lens, and Feature spotlight. The main area displays a table titled 'Buckets (1)'. The table has columns for Name, Region, Access, and Creation date. One row is shown with the following details:

Name	Region	Access	Creation date
c24791a312491u1199245t1w14294228477-s3bucket-1loxhr01tpx2	US East (N. Virginia) us-east-1	Objects can be public	January 24, 2021, 12:13:08 (UTC+05:30)

User-1 has not been assigned any permissions to use Amazon EC2:

The screenshot shows the AWS EC2 Management Console interface. On the left, there is a sidebar with options like New EC2 Experience, Instances, Images, and Elastic Block Store. The main area displays a table titled 'Instances'. The table has columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. A message at the top states 'You do not have any instances in this region'. At the bottom, there is a note 'Select an instance above'.

User-2 can view Amazon EC2 Instances since he/she has Read Only Permissions:

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with options like EC2 Dashboard, Instances, Images, and Elastic Block Store. The main area displays a table titled 'Instances (1) info' with one row. The row contains the following information:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
-	i-08aa90b12f26f8fa6	Running	t2.micro	2/2 checks ...	1 alarm...	us-east-1a	ec2-3-93-246-226.i...

Below the table, a message says 'Select an instance above'. At the bottom of the page, there's a footer with links for Feedback, English (US), Privacy Policy, and Terms of Use.

User-2 cannot stop Instance as policy only allows user to view information:

The screenshot shows the same AWS EC2 Management Console interface as the previous one. However, there is an error message displayed prominently at the top of the main content area:

Failed to stop the instance i-08aa90b12f26f8fa6

You are not authorized to perform this operation. Encoded authorization failure message: ObjqquXbfyT14ZnQNQnp43gt3CxBngJsBjdVcDOUs-1BZhocgfUf098Kz215b12cd7cg5G5fXI42G6gRb0ApP27xiQDdnz7Xfhk2lP8dInBtmWns91Wbrydy2yJ5QheL2sGBWOsSy3v1E6GBKxZQZ3Mlpnr0B15s-HjffKG8HFF8IP31De-YtE1xdE3enfeirg5bYO8a3fIE-44gUR1R2RJu6q6CDHe9J6JiIhy8jjpn_zxEa8plk2swr97pbm_pOUldsrdf2B7wa7f1WQKas53JIK-glmQTYWY1DI_HHDtMnojJz5Buhc_vPP8TQS4rN0mGnzapUVDWWS7DXVmLvOp1p1Wdg531S1V2E5v2NGggk-sla7U3g42ww1b6c6k3KTD2N0Srnb9l000Utgw8BzloXv5NiOrOnzXyPlwrR5ja077DmxGmgkmOonenasfunet7eYqlUI4FtcFTNPXykJ9suxu2cbnMtshCrzNFZA8c7tWkjPLePtos6yKDE5Inpa0uvlskyh_EMZG5dndx6NTIKF5SCCTE_q6w5CHba19U-2w-h0b88nrvfB1g2l1mQ2wsXABlnAyjk5YkbRju4a2zExgXfC8yangGntpXfh1er-ZXMb56eQPQg_MSTW-83CWYU3-i9z9GTByTdk44flIrryKz504zVztVkoqC8tMg-2yprDfPnhahBhvJlnL8w0Hjjob48dL41n3fWswdYfCn8eu2Va-puLdk1unCxBA6E4ydzaxr6NFMB0QdkYsGYbSMB3LUixwxV4GFB397DuSvf-n2EA

Below the error message, the 'Instances (1/1) info' table is visible, showing the same instance details as before. At the bottom of the page, there's a footer with links for Feedback, English (US), Privacy Policy, and Terms of Use.

User-2 does not have permission to use Amazon S3:

The screenshot shows the AWS S3 Management Console. The left sidebar has sections for Buckets, Storage Lens, and AWS Marketplace for S3. The main area is titled 'Amazon S3' and shows 'Buckets (0)'. A message box states: 'You don't have permissions to list buckets. After you or your AWS administrator have updated your permissions to allow the s3>ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3.' The status bar at the bottom indicates the user is 'User-2 @ 1429-4222-8477'.

User-3 can view Amazon EC2 Instances:

The screenshot shows the AWS EC2 Management Console. The left sidebar has sections for New EC2 Experience, Instances, Images, and Elastic Block Store. The main area is titled 'Instances (1)' and shows a table with one row: Name: -, Instance ID: i-08aa90b12f26f8fa6, Instance state: Running, Instance type: t2.micro, Status check: 2/2 checks ..., Alarm status: User: ar..., Availability Zone: us-east-1a, Public IPv4 DNS: ec2-3-93-246-226.i. The status bar at the bottom indicates the user is 'user-3 @ 1429-4222-8477'.

User-3 can stop Amazon EC2 Instances:

The screenshot shows the AWS EC2 Management Console. A success message at the top says "Successfully stopped i-08aa90b12f26f8fa6". The main table lists one instance: Name: -, Instance ID: i-08aa90b12f26f8fa6, Instance state: Stopping, Instance type: t2.micro, Status check: 2/2 checks ..., Alarm status: User: ar..., Availability Zone: us-east-1a, Public IPv4 DNS: ec2-3-93-246-226.e. The instance row has a red circle with a slash over the checkbox, indicating it is selected. The status column shows a red circle with a slash over the "Stopping" text.

The screenshot shows the AWS EC2 Management Console. A success message at the top says "Successfully stopped i-08aa90b12f26f8fa6". The main table lists one instance: Name: -, Instance ID: i-08aa90b12f26f8fa6, Instance state: Stopped, Instance type: t2.micro, Status check: -, Alarm status: User: ar..., Availability Zone: us-east-1a, Public IPv4 DNS: -. The instance row has a red circle with a slash over the checkbox, indicating it is selected. The status column shows a red circle with a slash over the "Stopped" text.