AWS Hand On

(ON CONSOLE)

Q 01.

1. Create Security Group:
- Create one security group for the web server.
- Configure inbound rules for the web server security group to allow HTTP traffic (port 80) and SSH traffic (port 22) from any source.

2. Launch EC2 Instance:
- Launch an EC2 instance for the web server using Amazon Linux 2 AMI.
- Associate the web server security group created earlier with this instance.
- Use an appropriate instance type for a web server.
- Ensure the instance has a public IP address.

3. SSH Access:
- Generate an SSH key pair for secure access to the instances.
- Configure the web server instance to accept SSH connections using the generated key pair.
- Attempt to SSH into the web server instance to verify successful access.

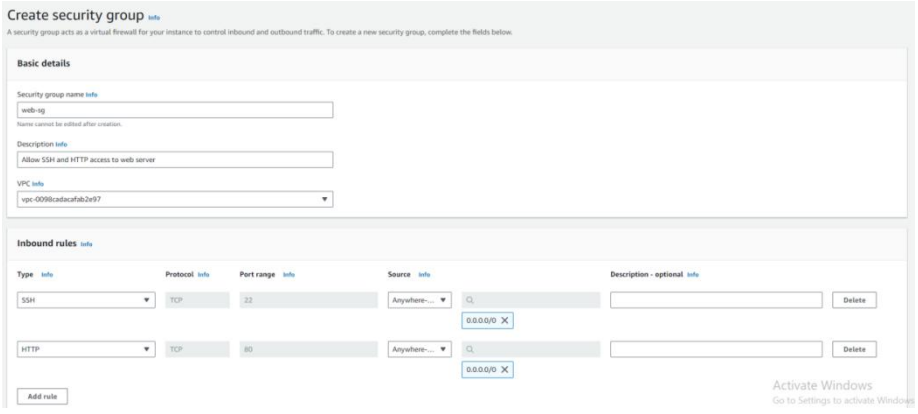
SOLUTION:-

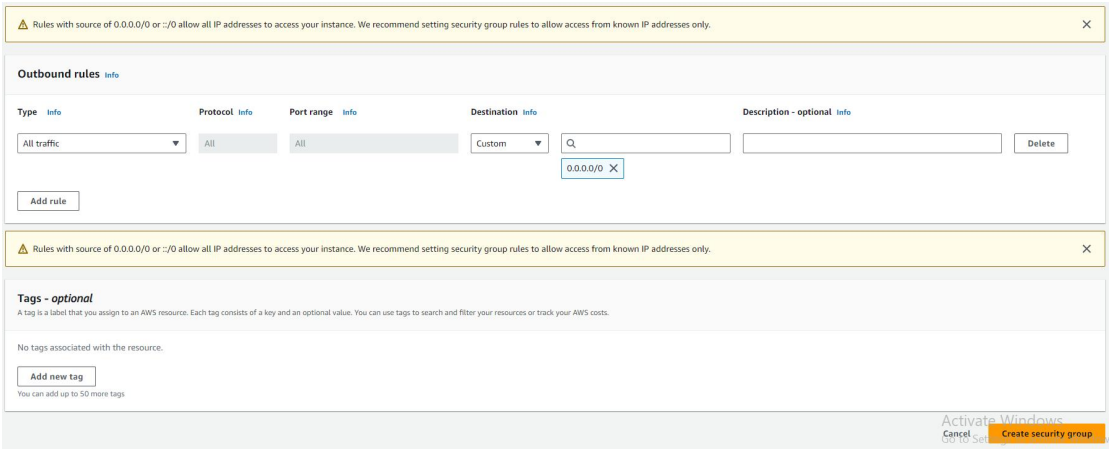
4. Web Application Setup:
- Install a web server (e.g., Apache or Nginx) on the web server instance.
- Create a simple HTML page to confirm the web server is working.
- Test accessing the web server's public IP address in a web browser.

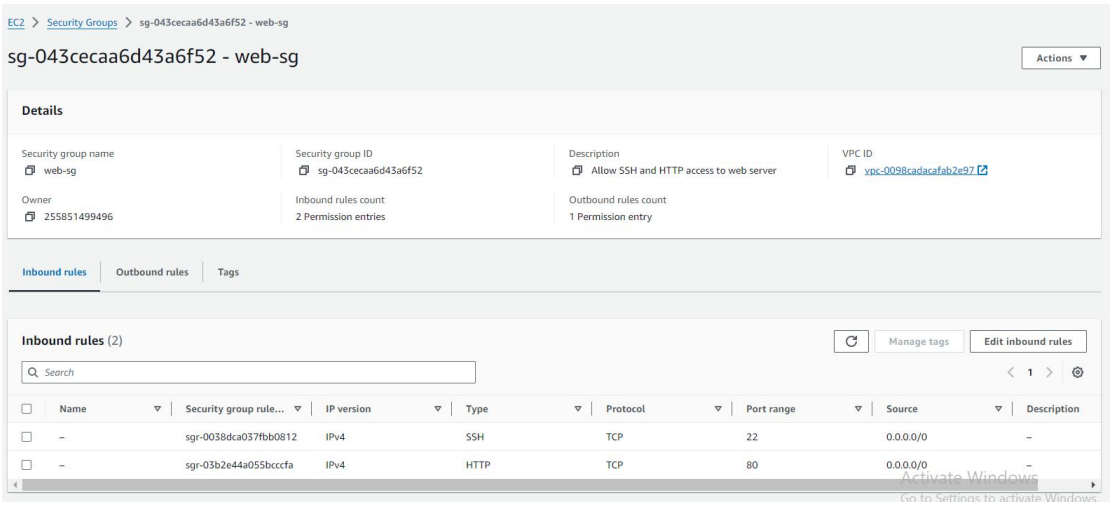
5. Documentation:
- Provide clear documentation outlining the steps you took to complete each task.
- Include relevant screenshots or command outputs to demonstrate the successful implementation of security groups, instance launches, and SSH access.

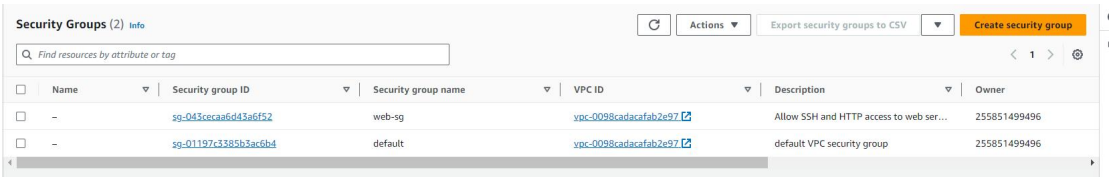
SOLUTION:-

Q1:- 1

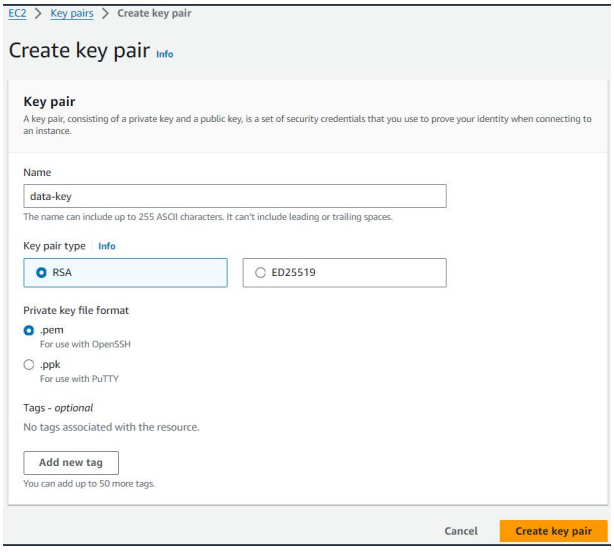


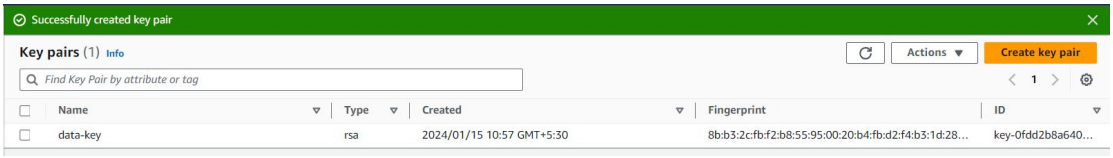

Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Outbound rules Info
Type Info
Protocol Info
Port range Info
Destination Info
Description - optional Info
All traffic
All
All
Custom
0.0.0.0/0
Delete
Add rule
Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags
Activate Windows
Cancel
Create security group

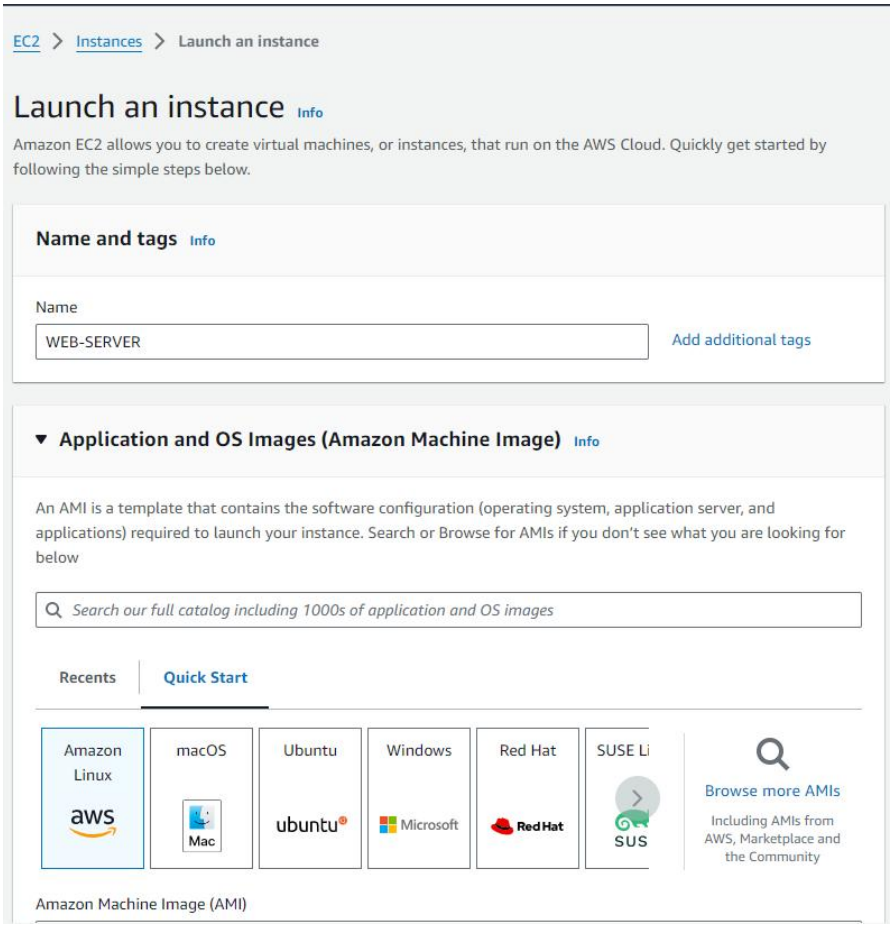

EC2 > Security Groups > sg-043cecaa6d43a6f52 - web-sg
sg-043cecaa6d43a6f52 - web-sg
Actions
Details
Security group name
web-sg
Security group ID
sg-043cecaa6d43a6f52
Description
Allow SSH and HTTP access to web server
VPC ID
vpc-0098cadacafab2e97
Owner
255851499496
Inbound rules count
2 Permission entries
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Tags
Inbound rules (2)
Manage tags
Edit inbound rules
Search
Name
Security group rule...
IP version
Type
Protocol
Port range
Source
Description
sgr-0038dca037fbb0812
IPv4
SSH
TCP
22
0.0.0.0/0
sgr-03b2e44a055bcccfa
IPv4
HTTP
TCP
80
0.0.0.0/0
Activate Windows

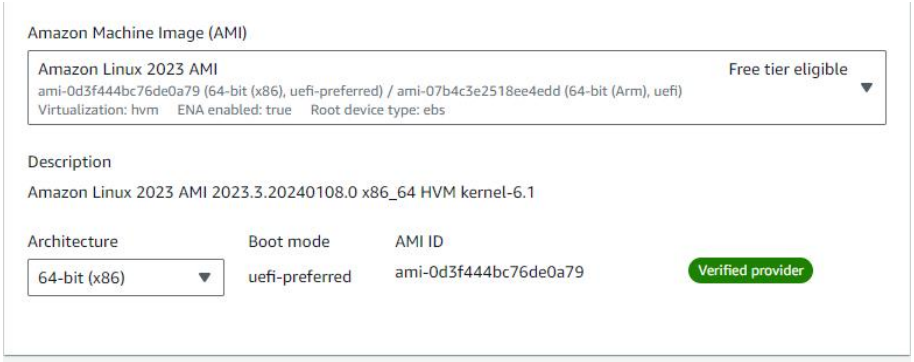

Security Groups (2) Info
Actions
Export security groups to CSV
Create security group
Find resources by attribute or tag
Name
Security group ID
Security group name
VPC ID
Description
Owner
sg-043cecaa6d43a6f52
web-sg
vpc-0098cadacafab2e97
Allow SSH and HTTP access to web ser...
255851499496
sg-01197c3385b3ac6b4
default
vpc-0098cadacafab2e97
default VPC security group
255851499496

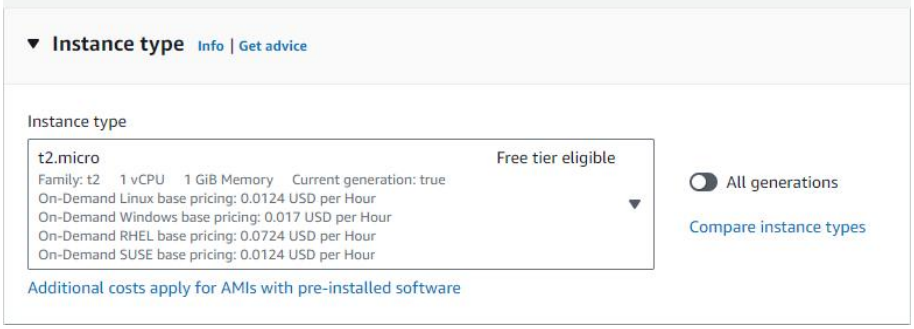
Q1:- 2


EC2 > Key pairs > Create key pair
Create key pair Info
Key pair
A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.
Name
data-key
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.
Key pair type Info
RSA
ED25519
Private key file format
.pem
For use with OpenSSH
.ppk
For use with PuTTY
Tags - optional
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Create key pair


Successfully created key pair
Key pairs (1) Info
Actions
Create key pair
Find Key Pair by attribute or tag
Name
Type
Created
Fingerprint
ID
data-key
rsa
2024/01/15 10:57 GMT+5:30
8b:b3:2c:fb:f2:b8:55:95:00:20:b4:fb:d2:f4:b3:1d:28...
key-0fdd2b8a640...


EC2 > Instances > Launch an instance
Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
WEB-SERVER
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below
Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Li
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)


Amazon Machine Image (AMI)
Amazon Linux 2023 AMI
Free tier eligible
ami-0d3f444bc76de0a79 (64-bit (x86), uefi-preferred) / ami-07b4c3e2518ee4edd (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs
Description
Amazon Linux 2023 AMI 2023.3.20240108.0 x86_64 HVM kernel-6.1
Architecture
Boot mode
AMI ID
64-bit (x86)
uefi-preferred
ami-0d3f444bc76de0a79
Verified provider


Instance type Info | Get advice
Instance type
t2.micro
Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0724 USD per Hour
On-Demand SUSE base pricing: 0.0124 USD per Hour
All generations
Compare instance types
Additional costs apply for AMIs with pre-installed software

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

data-key

Create new key pair

Network settings Info

VPC - *required* Info

vpc-0098cadacafab2e97 (default)
172.31.0.0/16

Subnet Info

subnet-0709cc7ad6133f2a5 my-subnet
VPC: vpc-0098cadacafab2e97 Owner: 255851499496
Availability Zone: ap-south-1a IP addresses available: 4091 CIDR: 172.31.0.0/20)

Create new subnet

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

○ Create security group

● Select existing security group

Common security groups Info

Select security groups

web-sg sg-043cecaa6d43a6f52
VPC: vpc-0098cadacafab2e97

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

▶ Advanced network configuration

Configure storage Info

Advanced

1x 8 GiB gp3 Root volume (Not encrypted)

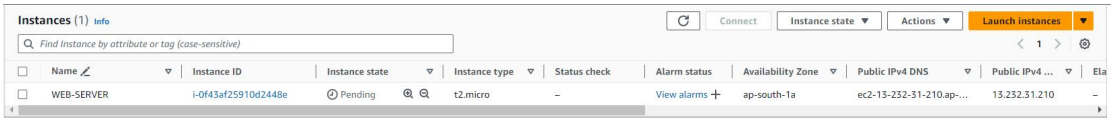
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems Edit

Advanced details Info



Q1:- 3

```
root@DESKTOP-VIDGD8F:Desktop# ssh -i "data-key.pem" ec2-user@ec2-13-201-124-168.ap-south-1.compute.amazonaws.com
The authenticity of host 'ec2-13-201-124-168.ap-south-1.compute.amazonaws.com (13.201.124.168)' can't be established.
ED25519 key fingerprint is SHA256:UoJ5yrraPtgciUi70jl1RWvraGRd4eCOxkN4unu3ek0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-201-124-168.ap-south-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Mon Jan 15 06:59:46 2024 from 13.233.177.5
[ec2-user@ip-172-31-15-228 ~]$
```

Q1:- 4

```
[ec2-user@ip-172-31-15-228 ~]$ sudo su -
[root@ip-172-31-15-228 ~]# yum install httpd -y
Last metadata expiration check: 0:01:55 ago on Mon Jan 15 06:59:52 2024.
Dependencies resolved.
================================================================================================================================================
 Package                                Architecture            Version                                  Repository                      Size
================================================================================================================================================
Installing:
 httpd                                  x86_64                  2.4.58-1.amzn2023                        amazonlinux                     47 k
Installing dependencies:
 apr                                    x86_64                  1.7.2-2.amzn2023.0.2                     amazonlinux                    129 k
 apr-util                               x86_64                  1.6.3-1.amzn2023.0.1                     amazonlinux                     98 k
 generic-logos-httpd                    noarch                  18.0.0-12.amzn2023.0.3                   amazonlinux                     19 k
 httpd-core                             x86_64                  2.4.58-1.amzn2023                        amazonlinux                    1.4 M
 httpd-filesystem                       noarch                  2.4.58-1.amzn2023                        amazonlinux                     14 k
 httpd-tools                            x86_64                  2.4.58-1.amzn2023                        amazonlinux                     81 k
 libbrotli                              x86_64                  1.0.9-4.amzn2023.0.2                     amazonlinux                    315 k
 mailcap                                noarch                  2.1.49-3.amzn2023.0.3                    amazonlinux                     33 k
Installing weak dependencies:
 apr-util-openssl                       x86_64                  1.6.3-1.amzn2023.0.1                     amazonlinux                     17 k
 mod_http2                              x86_64                  2.0.11-2.amzn2023                        amazonlinux                    150 k
 mod_lua                                x86_64                  2.4.58-1.amzn2023                        amazonlinux                     61 k

Transaction Summary
================================================================================================================================================
Install  12 Packages

Total download size: 2.3 M
Installed size: 6.9 M
Downloading Packages:
(1/12): mod_lua-2.4.58-1.amzn2023.x86_64.rpm                                    969 kB/s |  61 kB     00:00
(2/12): apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64.rpm                        256 kB/s |  17 kB     00:00
(3/12): httpd-tools-2.4.58-1.amzn2023.x86_64.rpm                                1.1 MB/s |  81 kB     00:00
(4/12): httpd-2.4.58-1.amzn2023.x86_64.rpm                                      3.7 MB/s | 1.7 MB     00:00
(5/12): apr-util-1.6.3-1.amzn2023.0.1.x86_64.rpm                                6.9 MB/s |  98 kB     00:00
```



```
[root@ip-172-31-15-228 ~]# cd /var/www/html/
[root@ip-172-31-15-228 html]# ll
total 0
[root@ip-172-31-15-228 html]# echo "WELCOME TO WEB SERVER" >index.html
[root@ip-172-31-15-228 html]#
```

(ON CLI)

Q 02.

1. Create Security Group for Web Server Using AWS CLI:
- Use the AWS CLI to create a security group for the web server.
- Configure inbound rules to allow HTTP traffic (port 80) and SSH traffic (port 22) from any source.

2. Launch EC2 Instance for Web Server Using AWS CLI:
- Use the AWS CLI to launch an EC2 instance for the web server using Amazon Linux 2 AMI.
- Associate the security group created earlier with this instance.
- Use an appropriate instance type for a web server.
- Ensure the instance has a public IP address.

3. SSH Access Using AWS CLI:
- Use the AWS CLI to generate an SSH key pair for secure access to the web server instance.
- Configure the web server instance to accept SSH connections using the generated key pair.
- Use the AWS CLI to attempt to SSH into the web server instance to verify successful access.

4. Web Application Setup Using AWS CLI:
- Use the AWS CLI to install a web server (e.g., Apache or Nginx) on the web server instance.
- Create a simple HTML page using the AWS CLI to confirm the web server is working.
- Use the AWS CLI to test accessing the web server's public IP address in a web browser.

5. Documentation:
- Provide clear documentation in a text file outlining the AWS CLI commands used for each task along with their outputs.
- Include any relevant information such as IP addresses, instance IDs, etc.

SOLUTION:-

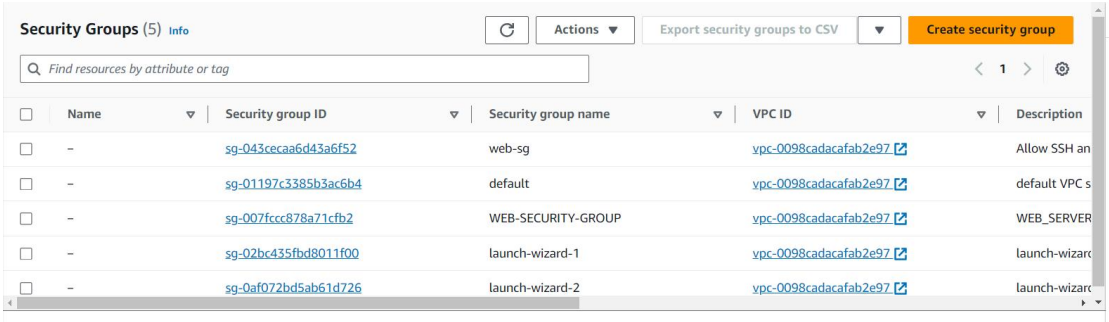
Q1:- 1
create a security group for the web server

```
root@DESKTOP-VIDGD8F:AWS# aws ec2 create-security-group --description
WEB_SERVER_SECURITY_GROUP --group-name WEB-SECURITY-GROUP
{
   "GroupId": "sg-007fccc878a71cfb2"
}
root@DESKTOP-VIDGD8F:AWS#
```

Configure inbound rules to allow HTTP traffic (port 80) and SSH traffic (port 22) from any source.

```
root@DESKTOP-VIDGD8F:AWS# aws ec2 authorize-security-group-ingress --
group-id sg-007fccc878a71cfb2 --ip-permissions IpProtocol=tcp,FromPort=80,T
oPort=80,UserIdGroupPairs='[{GroupId=sg-007fccc878a71cfb2}]'
{
    "Return": true,
    "SecurityGroupRules": [
        {
            "SecurityGroupRuleId": "sgr-06701676745fb026f",
            "GroupId": "sg-007fccc878a71cfb2",
            "GroupOwnerId": "255851499496",
            "IsEgress": false,
            "IpProtocol": "tcp",
            "FromPort": 80,
            "ToPort": 80,
            "ReferencedGroupInfo": {
                "GroupId": "sg-007fccc878a71cfb2",
                "UserId": "255851499496"
            }
        }
    ]
}

root@DESKTOP-VIDGD8F:AWS# aws ec2 authorize-security-group-ingress --
group-id sg-007fccc878a71cfb2 --ip-permissions IpProtocol=tcp,FromPort=22,T
oPort=22,UserIdGroupPairs='[{GroupId=sg-007fccc878a71cfb2}]'
{
    "Return": true,
    "SecurityGroupRules": [
        {
            "SecurityGroupRuleId": "sgr-0d53e58311c0e97fb",
            "GroupId": "sg-007fccc878a71cfb2",
            "GroupOwnerId": "255851499496",
            "IsEgress": false,
            "IpProtocol": "tcp",
            "FromPort": 22,
            "ToPort": 22,
            "ReferencedGroupInfo": {
                "GroupId": "sg-007fccc878a71cfb2",
                "UserId": "255851499496"
            }
        }
    ]
}
```



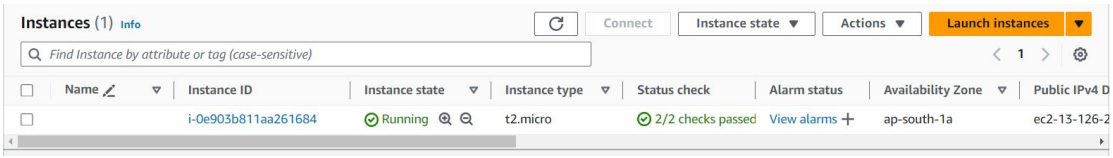
Q1:- 2

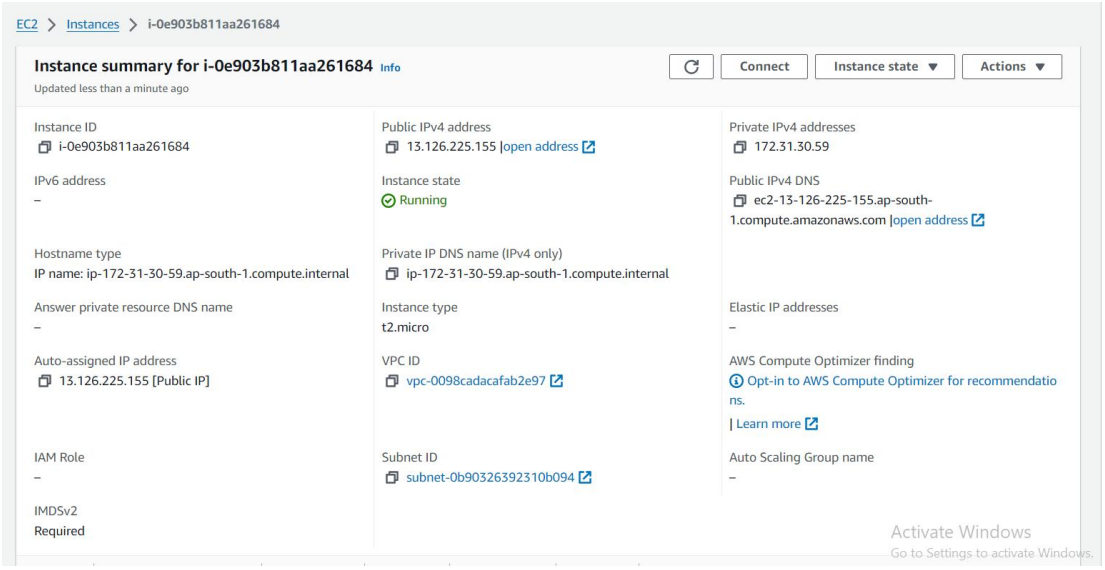
root@DESKTOP-VIDGD8F:AWS# aws ec2 run-instances --image-id ami-0d3f444bc76de0a79 --instance-type t2.micro --key-name data-key --security-group-ids sg-007fccc878a71cfb2 --associate-public-ip-address


```
{
    "Groups": [],
    "Instances": [
        {
            "AmiLaunchIndex": 0,
            "ImageId": "ami-0d3f444bc76de0a79",
            "InstanceId": "i-0e903b811aa261684",
            "InstanceType": "t2.micro",
            "KeyName": "data-key",
            "LaunchTime": "2024-01-19T05:54:22.000Z",
            "Monitoring": {
                "State": "disabled"
            },
            "Placement": {
                "AvailabilityZone": "ap-south-1a",
                "GroupName": "",
                "Tenancy": "default"
            },
            "PrivateDnsName": "ip-172-31-30-59.ap-south-1.compute.internal",
            "PrivateIpAddress": "172.31.30.59",
            "ProductCodes": [],
            "PublicDnsName": "",
            "State": {
                "Code": 0,
                "Name": "pending"
            },
            "StateTransitionReason": "",
            "SubnetId": "subnet-0b90326392310b094",
            "VpcId": "vpc-0098cadacafab2e97",
            "Architecture": "x86_64",
            "BlockDeviceMappings": [],
            "ClientToken": "f1cc4b77-6000-493c-bb62-4219f75debf9",
            "EbsOptimized": false,
            "EnaSupport": true,
            "Hypervisor": "xen",
            "NetworkInterfaces": [
```

```
    {
      "Attachment": {
        "AttachTime": "2024-01-19T05:54:22.000Z",
        "AttachmentId": "eni-attach-03b7fabd92f4888fd",
        "DeleteOnTermination": true,
        "DeviceIndex": 0,
        "Status": "attaching",
        "NetworkCardIndex": 0
      },
      "Description": "",
      "Groups": [
        {
          "GroupName": "WEB-SECURITY-GROUP",
          "GroupId": "sg-007fccc878a71cfb2"
        }
      ],
      "Ipv6Addresses": [],
      "MacAddress": "02:9d:a2:7e:fa:d3",
      "NetworkInterfaceId": "eni-00d9e74a67456beea",
      "OwnerId": "255851499496",
      "PrivateDnsName": "ip-172-31-30-59.ap-south-1.compute.internal",
      "PrivateIpAddress": "172.31.30.59",
      "PrivateIpAddresses": [
        {
          "Primary": true,
          "PrivateDnsName": "ip-172-31-30-59.ap-south-1.compute.internal",
          "PrivateIpAddress": "172.31.30.59"
        }
      ],
      "SourceDestCheck": true,
      "Status": "in-use",
      "SubnetId": "subnet-0b90326392310b094",
      "VpcId": "vpc-0098cadacafab2e97",
      "InterfaceType": "interface"
    }
  ],
  "RootDeviceName": "/dev/xvda",
  "RootDeviceType": "ebs",
  "SecurityGroups": [
    {
      "GroupName": "WEB-SECURITY-GROUP",
      "GroupId": "sg-007fccc878a71cfb2"
    }
  ],
  "SourceDestCheck": true,
  "StateReason": {
    "Code": "pending",
    "Message": "pending"
  },
  "VirtualizationType": "hvm",
```

```
            "CpuOptions": {
                "CoreCount": 1,
                "ThreadsPerCore": 1
            },
            "CapacityReservationSpecification": {
                "CapacityReservationPreference": "open"
            },
            "MetadataOptions": {
                "State": "pending",
                "HttpTokens": "required",
                "HttpPutResponseHopLimit": 2,
                "HttpEndpoint": "enabled",
                "HttpProtocolIpv6": "disabled",
                "InstanceMetadataTags": "disabled"
            },
            "EnclaveOptions": {
                "Enabled": false
            },
            "BootMode": "uefi-preferred",
            "PrivateDnsNameOptions": {
                "HostnameType": "ip-name",
                "EnableResourceNameDnsARecord": false,
                "EnableResourceNameDnsAAAARecord": false
            }
        }
    ],
    "OwnerId": "255851499496",
    "ReservationId": "r-09f66a502f58df098"
}
root@DESKTOP-VIDGD8F:AWS#
```



Q1:- 3

root@DESKTOP-VIDGD8F:AWS# aws ec2 create-key-pair --key-name data-key

{
"KeyFingerprint": "e0:a8:b4:2c:4f:5c:9f:70:10:04:52:eb:d3:e8:ec:f3:ad:3b:a5:30",
"KeyMaterial": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEogIBAAKCAQEAylp0XQm9WwoNZC6Vp8xx4/mBBxQF4MkX/GGn3UNT
Dk5Dn44+\nmqqlg20VdeEsFwRLmhJUaBLCfVTvxRCzWm5roYtZajqURcPUNwh
mS11L6rmMA8IK\nGNFJMCRAdYWFOyeOBO5h6fIPAAl31KK7l0Tgf/j/7PZteO8
Hto5nj37WNh9tEOWh\n1lBy+c3b1QgJKqTpCH3nuU0ElGmAmeoMHRZArqukf6/
bElP8aRztIPkrduJkYL3f\nuMh2yhOv5khXiDfH+4npUL+DE8JZLXo52SjVw6/Rcq
LrzQWuGmtqMciFywfYv+Fm\nmPv1qEb+7WlIcG9fRVVlVfTD2sQInQSayUvxw
QIDAQABAoIBAFBOT6nwyJZNyfy9\nRCVgzL418c/2UVLhW8SMmQsFwfuGce3
rjMri+GbNLtwmbdIAoWRW6+qVr1wADlv+\nAb/c3Jgy7lxrPRbm3dytV7OHJi7UT
k3bfxhUTqBtcqtxPuu4CfPJC1DGAM/58fWQ\nU7R34ETJc//92HpLGpuHrm/TXX4
CjBns0iLaSbCVLQ81maSaCHrzZ+7vQITNFFwX\ngXUerGvtIgbmDQ5rM62XDPij
5JdqzS91VaRb2cnQE9wBumbYfhLS8dsnmuuoFIfx\n1m5GUardboWruGfmicC8lgJ
NSdO4tPgCzZxeF5/fw7IQjuZORt3j0ivlHdxspJTJ\na7rT78ECgYEA6M4Az5EXAm
b8msc72b3dcz98tkduyLhQ3bEV68FadOf+9YX6rVO+\nSJehNw+hbyzWCcv7vXu0
Z5YZMPXjMHl2dt79hwsdJmwKCZOsePL/JvG4hOV7uELL\n2WQ1kGE0twFPfYZ
QG7VAbpMk+dgHkwJBDqjKDDMrZ6i1Jm9JuUEZW2kCgYEA3oO/\nmvecMk8/jj
KSzbG9mMvFhw28a2ZSZuB7uSkri5Nl8bL3lpCqczFfu4sZTPl9yRpM\nsu4TW+45a
facJlpoVFEv7Jxfsj6/P4wKOUFMnYjVW4Bie8KJbDpxvxfB101F5el1\nrXF9nesFlB
wzQFUjpMZyroE8Fu/ILtlyUK8H0JkCgYBc0v7JxG0rPQsNX9FCYYzx\nzeeY+mR
2zd8YdepqpR6/LF2hYflwsMpXQXY7cRUKMhNptpa6l594CgYjWndqtZOB\nlCn8
dXb7AesCpIoJc8I+sfTDsIijEKcdF/KvjcKqEXCzeSFp2txE+pCsufFTMXvl\nL3HYa
XKuEzufhpIbtpQ4uQKBgEx258wgFMvxEb0SwgHvd2DffXSIktwxYFW8BKg/\nbp
hbQagKQSy7b+d/6w7uoPYjskb+Q6clSv/HYHF6bnR7kuiOsbJUlkoRZ/U1cXn1\nZ5
enIvJ7rtwqoMDRYK8zQchz5HY6gNbmbi1rSxJ3kmEkIMiJ7XTsMjMLmTYIQVFa
\npIvZAoGAQxMiMqpYZDUxaCB2jw7BIR8KhkUKQd1xScPsF2niLQnTR+JRC/N
wsePG\nuG48ugmXACy9YnxjMMEuiw1THCuWS7et3vyw6VY0QqbIsmdkhbB4u

wHfCOgOjX1W\nCB7ybWDo5Qzbsvgku6BRs4fMCyixVM4q++IW+rzRuPA8fm1s
gJw=\n-----END RSA PRIVATE KEY-----",
"KeyName": "data-key",
"KeyPairId": "key-02024028e29472180"
}

```
root@DESKTOP-VIDGD8F:AWS# ssh -i "data-key.pem" ec2-user@ec2-15-206-171-131.ap-south-1.compute.amazonaws.com
The authenticity of host 'ec2-15-206-171-131.ap-south-1.compute.amazonaws.com (15.206.171.131)' can't be established.
ED25519 key fingerprint is SHA256:J4xI5+hPLqrnqc+ndyGQECDoEcb+QgL/ikBpQxARIK0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-15-206-171-131.ap-south-1.compute.amazonaws.com' (ED25519) to the list of known hosts.

A newer release of "Amazon Linux" is available.
  Version 2023.3.20240117:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-172-31-26-75 ~]$
```

Q1:- 4

root@DESKTOP-VIDGD8F:AWS# aws ec2 run-instances --image-id ami-0d3f444bc76de0a79 --key-name data-key --instance-type t2.micro --security-group-ids sg-007fccc878a71cfb2 --associate-public-ip-address --tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=Ec2_Instance}]' --user-data file://saniya.sh


```
{
   "Groups": [],
   "Instances": [
      {
         "AmiLaunchIndex": 0,
         "ImageId": "ami-0d3f444bc76de0a79",
         "InstanceId": "i-02c7ab0243ddf7960",
         "InstanceType": "t2.micro",
         "KeyName": "data-key",
         "LaunchTime": "2024-01-19T11:04:53.000Z",
         "Monitoring": {
            "State": "disabled"
         },
         "Placement": {
            "AvailabilityZone": "ap-south-1a",
            "GroupName": "",
            "Tenancy": "default"
         },
         "PrivateDnsName": "ip-172-31-19-117.ap-south-1.compute.internal",
         "PrivateIpAddress": "172.31.19.117",
         "ProductCodes": [],
         "PublicDnsName": "",
         "State": {
            "Code": 0,
            "Name": "pending"
```

```
        },
        "StateTransitionReason": "",
        "SubnetId": "subnet-0b90326392310b094",
        "VpcId": "vpc-0098cadacafab2e97",
        "Architecture": "x86_64",
        "BlockDeviceMappings": [],
        "ClientToken": "3fc70102-64d6-4569-8f1a-fe0b5bcc28c5",
        "EbsOptimized": false,
        "EnaSupport": true,
        "Hypervisor": "xen",
        "NetworkInterfaces": [
          {
            "Attachment": {
              "AttachTime": "2024-01-19T11:04:53.000Z",
              "AttachmentId": "eni-attach-0fce9525ed98ca14f",
              "DeleteOnTermination": true,
              "DeviceIndex": 0,
              "Status": "attaching",
              "NetworkCardIndex": 0
            },
            "Description": "",
            "Groups": [
              {
                "GroupName": "WEB-SECURITY-GROUP",
                "GroupId": "sg-007fccc878a71cfb2"
              }
            ],
            "Ipv6Addresses": [],
            "MacAddress": "02:b6:52:83:7a:11",
            "NetworkInterfaceId": "eni-01d54e4a4e974c518",
            "OwnerId": "255851499496",
            "PrivateDnsName": "ip-172-31-19-117.ap-south-1.compute.internal",
            "PrivateIpAddress": "172.31.19.117",
            "PrivateIpAddresses": [
              {
                "Primary": true,
                "PrivateDnsName": "ip-172-31-19-117.ap-south-
1.compute.internal",
                "PrivateIpAddress": "172.31.19.117"
              }
            ],
            "SourceDestCheck": true,
            "Status": "in-use",
            "SubnetId": "subnet-0b90326392310b094",
            "VpcId": "vpc-0098cadacafab2e97",
            "InterfaceType": "interface"
          }
        ],
        "RootDeviceName": "/dev/xvda",
        "RootDeviceType": "ebs",
```

```
            "SecurityGroups": [
                {
                    "GroupName": "WEB-SECURITY-GROUP",
                    "GroupId": "sg-007fccc878a71cfb2"
                }
            ],
            "SourceDestCheck": true,
            "StateReason": {
                "Code": "pending",
                "Message": "pending"
            },
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Ec2_Instance"
                }
            ],
            "VirtualizationType": "hvm",
            "CpuOptions": {
                "CoreCount": 1,
                "ThreadsPerCore": 1
            },
            "CapacityReservationSpecification": {
                "CapacityReservationPreference": "open"
            },
            "MetadataOptions": {
                "State": "pending",
                "HttpTokens": "required",
                "HttpPutResponseHopLimit": 2,
                "HttpEndpoint": "enabled",
                "HttpProtocolIpv6": "disabled",
                "InstanceMetadataTags": "disabled"
            },
            "EnclaveOptions": {
                "Enabled": false
            },
            "BootMode": "uefi-preferred",
            "PrivateDnsNameOptions": {
                "HostnameType": "ip-name",
                "EnableResourceNameDnsARecord": false,
                "EnableResourceNameDnsAAAARecord": false
            }
        }
    ],
    "OwnerId": "255851499496",
    "ReservationId": "r-053999eeb97b9b271"
}
root@DESKTOP-VIDGD8F:AWS#
```

```
root@DESKTOP-VIDGD8F:AWS# ssh -i "data-key.pem" ec2-user@ec2-13-201-47-231.ap-south-1.compute.amazonaws.com

A newer release of "Amazon Linux" is available.
  Version 2023.3.20240117:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Jan 19 11:05:48 2024 from 137.59.68.246
[ec2-user@ip-172-31-19-117 ~]$ sudo su
[root@ip-172-31-19-117 ec2-user]# cat /var/www/html/index.html
HELLO HTTPD PAGE
[root@ip-172-31-19-117 ec2-user]#
```