

## Exp - 4                      Implementing IaaS - Compute through EC2

29/07/24

### Aim:

To implement IaaS by compute through EC2.

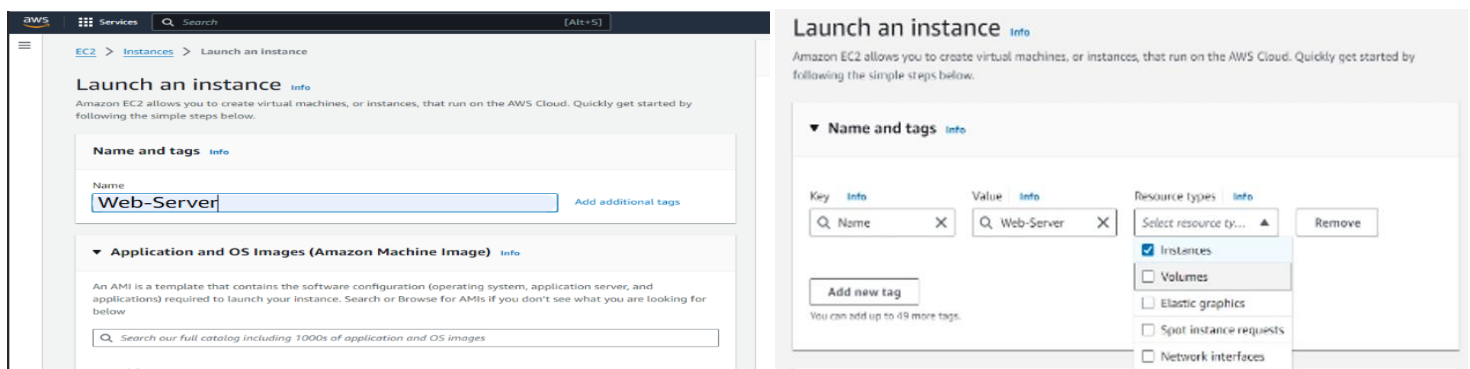
### Procedure:

#### Task 1: Launching your EC2 instance

In the AWS Management Console in the Search, enter EC2 and choose Enter. From the search results, choose EC2. In the Launch instance section, choose Launch instance.

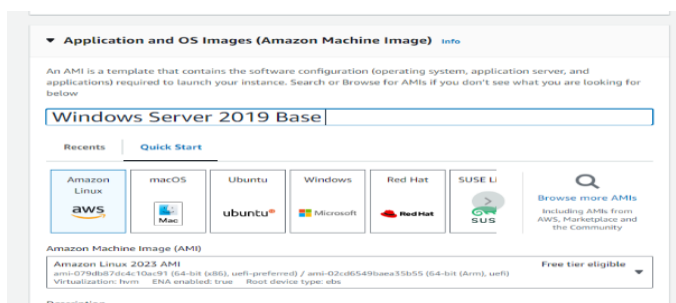
From the Resource types dropdown list, Instances is selected by default. Leave Instances selected and select Volumes.

#### STEP 1: NAME YOUR EC2 INSTANCE



#### STEP 2: CHOOSE AN AMI

Locate the Application and OS Images (Amazon Machine Image) section. It's below the Name and tags section. In the search box, enter Windows Server 2019 Base and choose Enter. Next to Microsoft Windows Server 2019 Base, choose Select.



### STEP 3: CHOOSE AN INSTANCE TYPE

**Instance type**

**t2.micro**  
 Family: t2 1 vCPU 1 GiB Memory Current generation: true  
 On-Demand Windows base pricing: 0.0162 USD per Hour  
 On-Demand SUSE base pricing: 0.0116 USD per Hour  
 On-Demand RHEL base pricing: 0.0716 USD per Hour  
 On-Demand Linux base pricing: 0.0116 USD per Hour

Free tier eligible

☐ All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

### STEP 4: CONFIGURE A KEY PAIR

**▼ Key pair (login) Info**

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

Key pair name - required

Select  
 Q  
 Proceed without a key pair (Not recommended) Default value

Create new key pair  
 decrypted password to connect to

### STEP 5: CONFIGURE THE NETWORK SETTINGS

**▼ Network settings Info**

**VPC - required Info**

vpc-0b0e6a462c748cf47 (Lab VPC)  
10.0.0.0/16

↻

**Subnet Info**

subnet-0f93350e8897039bb  
 VPC: vpc-0b0e6a462c748cf47 Owner: 449413273277 Availability Zone: us-east-1a  
 IP addresses available: 250 CIDR: 10.0.1.0/24

Public Subnet 1

↻ 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  
 Q |

Compare security group rules  
 interfaces.

<input type="checkbox"/> default	sg-02d523264d0e38ed9
VPC: vpc-0b0e6a462c748cf47	
<input type="checkbox"/> Web Server security group	sg-0908c88bda0a7a16e
VPC: vpc-0b0e6a462c748cf47	

## STEP 6: ADD STORAGE

▼ Configure storage [Info](#)

Advanced

1x  GiB  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

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

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](#)

## STEP 7: CONFIGURE ADVANCED DETAILS:

Expand the Advanced details section. For IAM instance profile, choose the role that begins with LabStack in the name and make the termination protection enabled. choose the User data text box. Then, choose Paste.

▼ Advanced details [Info](#)

Domain join directory [Info](#)

Select

Create new directory

IAM instance profile [Info](#)

Select

Q

Select

LabStack-a5c32332-95b2-4017-a5ba-d693ed28febf-p34gwX3bB6DPk9aSwY7Z5-0-LabInstanceProfile-XzhZa6GzQRP6  
arn:aws:iam:449413273277:instance-profile/LabStack-a5c32332-95b2-4017-a5ba-d693ed28febf-p34gwX3bB6DPk9aSwY7Z5-0-LabInstanceProfile-XzhZa6GzQRP6

Create new IAM profile

Termination protection [Info](#)

Select

Select

Enable

Disable

User data - optional [Info](#)

Upload a file with your user data or enter it in the field.

Choose file

```

C:\Users\Administrator\Downloads\code.zip
# Unzipping website code
Add-Type -AssemblyName System.IO.Compression.FileSystem
function Unzip
{
    param([string]$zipfile, [string]$outpath)
    [System.IO.Compression.ZipFile]::ExtractToDirectory($zipfile, $outpath)
}
Unzip "C:\Users\Administrator\Downloads\code.zip" "C:\inetpub\"
# Setting Administrator password
$Secure_String_Pwd = ConvertTo-SecureString "P@ssW0rd!" -AsPlainText -Force
$UserAccount = Get-LocalUser -Name "Administrator"
$UserAccount | Set-LocalUser -Password $Secure_String_Pwd
</powershell>

```

☐ User data has already been base64 encoded

## STEP 8: LAUNCH AN EC2 INSTANCE

In the Summary section, choose Launch instance. Your instance should display the following:

- Instance State: Running • Status Checks: 2/2 checks passed



Instances (1/1) [Info](#)

Find Instance by attribute or tag (case-sensitive)

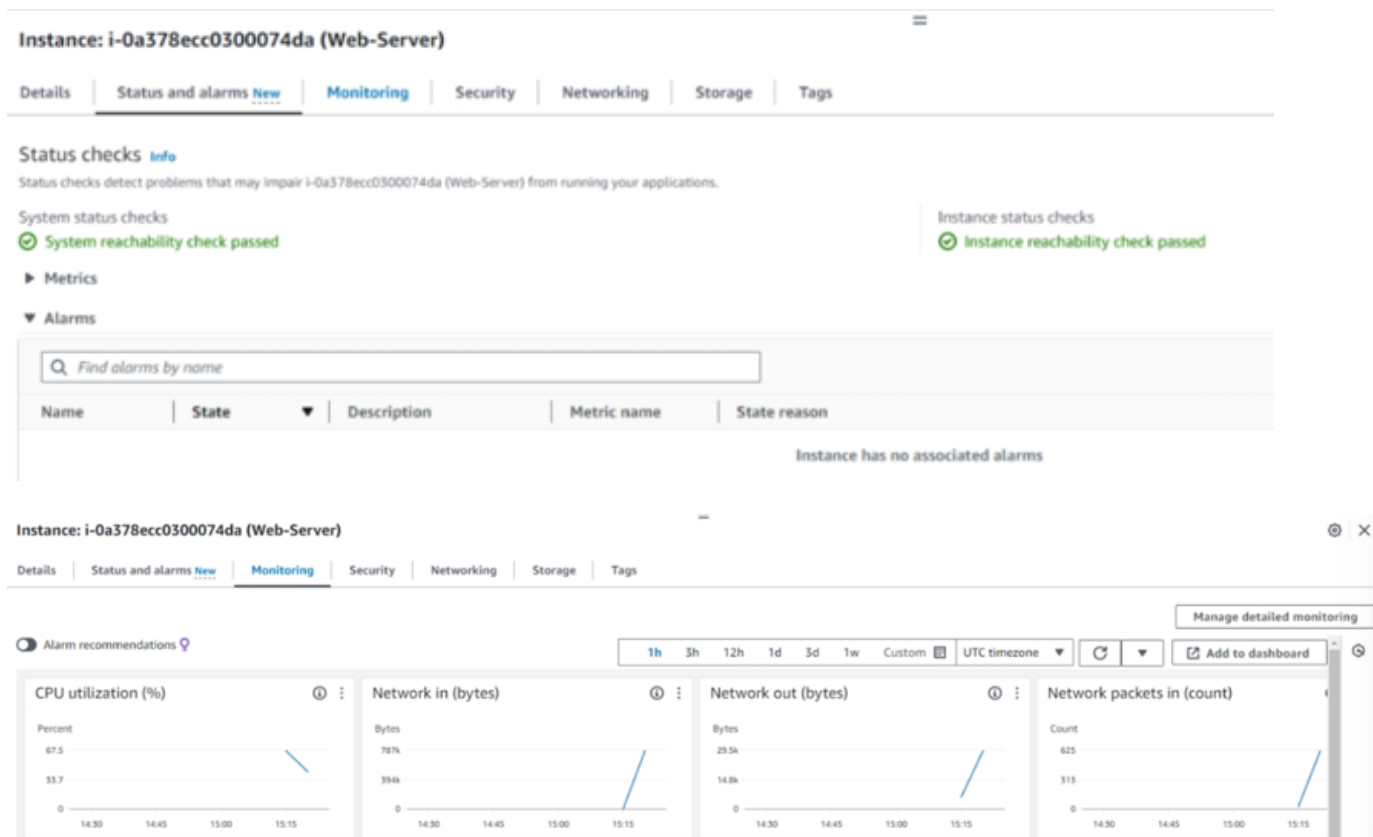
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
Web-Server	i-0a378ecc0300074da	Running	t2.micro	2/2 checks passed	<a href="#">View alarms</a>	us-east-1a	ec2-54-89-233-131.co...	54.89.233.131	-

Instance: i-0a378ecc0300074da (Web-Server)

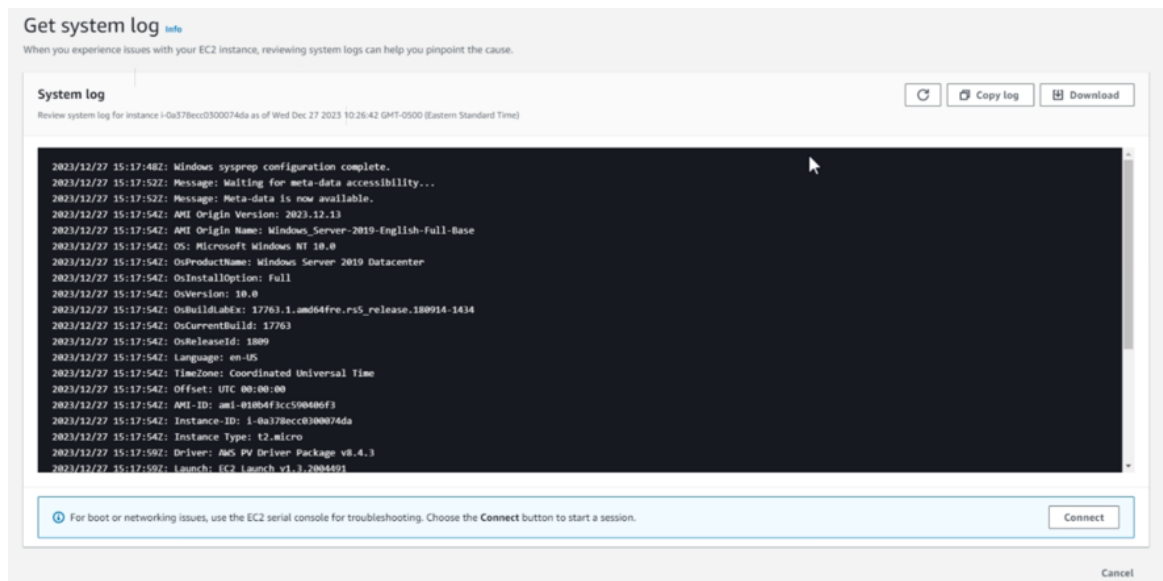
[Details](#) [Status and alarms \*\*New\*\*](#) [Monitoring](#) [Security](#) [Networking](#) [Storage](#) [Tags](#)

## Task 2: Monitor your instance

Choose the Status and alarms tab. Review the information that's available to you. Choose the Monitoring tab.

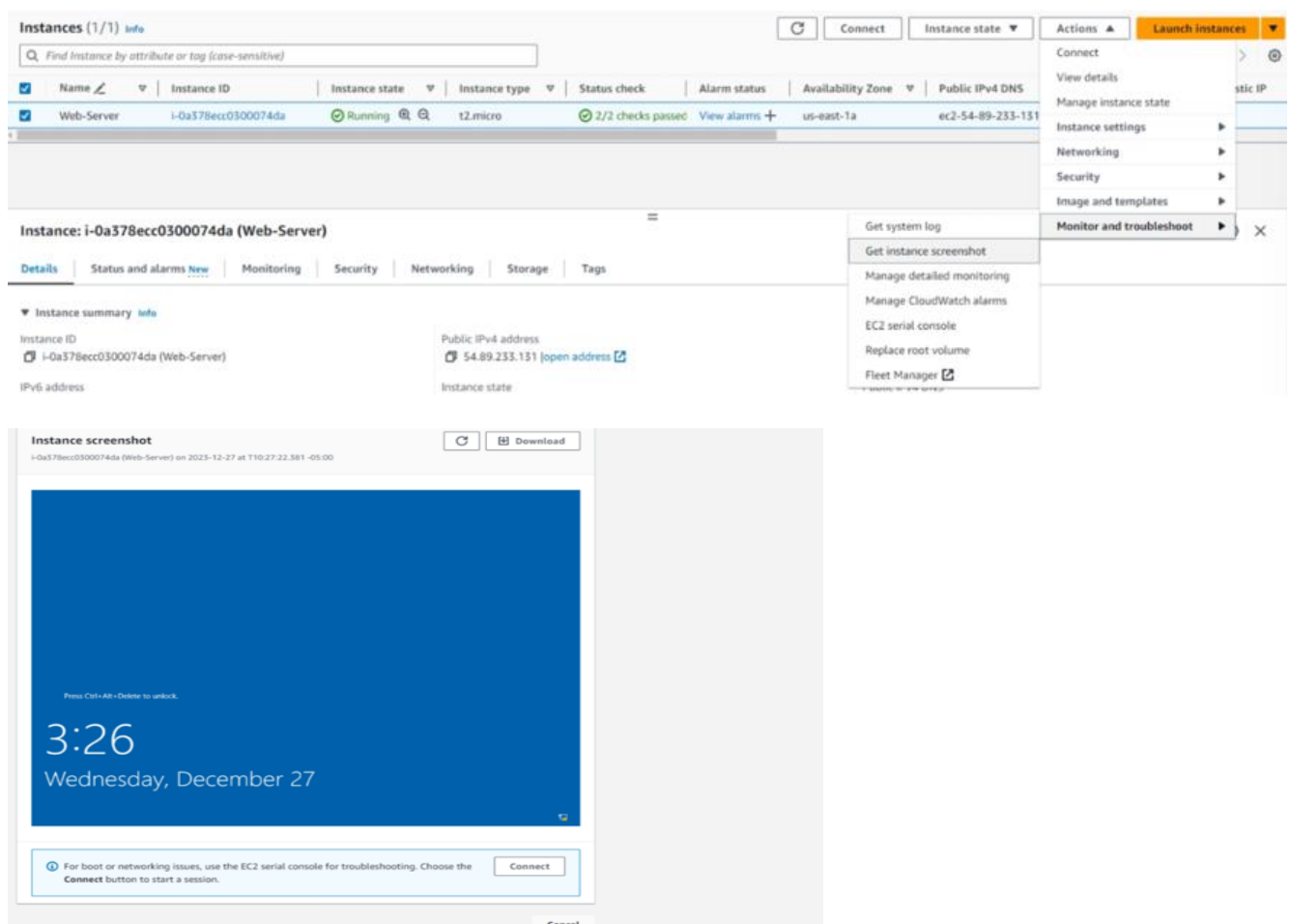


At the top of the page, choose the Actions dropdown list. Choose Monitor and troubleshoot Get system log.



To return to the Amazon EC2 dashboard, choose Cancel.

With your Web-Server selected, choose the Actions dropdown list, and choose Monitor and troubleshoot Get instance screenshot.



### Task 3: Updating your security group and accessing the web server

In the left navigation pane, choose Security Groups. Next to Web Server security group, select the check box. Choose the Inbound rules tab.

The screenshot shows the AWS Management Console interface. At the top, there's a search bar and buttons for 'Actions', 'Export security groups to CSV', and 'Create security group'. Below this is a table of security groups:

Name	Security group ID	Security group name	VPC ID	Description	Owner
-	sg-0e79a7889e0095c53	default	vpc-0cedae4b2556a74f3	default VPC security group	929932431040
<input checked="" type="checkbox"/>	sg-0732c055047233cb0	Web Server security group	vpc-0cedae4b2556a74f3	Security group for the web server	929932431040
-	sg-0416a76dccc7c3620	default	vpc-0b9aac07b48093f	default VPC security group	929932431040

Below the table, the 'sg-0732c055047233cb0 - Web Server security group' is selected. The 'Inbound rules' tab is active, showing a search bar and a table with columns: Name, Security group rule..., IP version, Type, Protocol, Port range, Source, and Description. The message 'No security group rules found' is displayed.

Choose Edit inbound rules, and then choose Add rule, and configure the following options  
 Type: Choose HTTP. • Source: Choose Anywhere-IPv4.

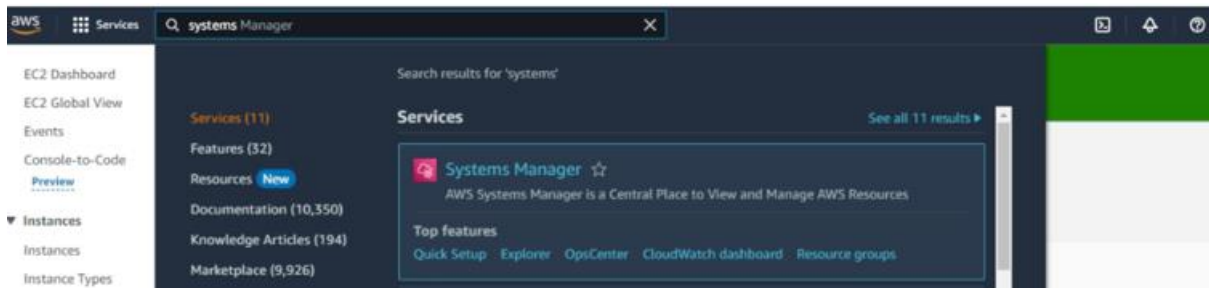
The screenshot shows the 'Edit inbound rules' page for the 'Web Server security group'. It includes a search bar and a table with columns: Security group rule ID, Type, Protocol, Port range, Source, and Description - optional. The 'Add rule' button is visible. A warning message at the bottom states: '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.'

The screenshot shows the 'Web Server security group' details page. A green banner at the top indicates 'Inbound security group rules successfully modified on security group sg-0732c055047233cb0 (Web Server security group)'. The 'Details' section shows the security group name, ID, description, VPC ID, owner, and inbound rules count (1 Permission entry). The 'Inbound rules' tab is active, showing a table with columns: Name, Security group rule..., IP version, Type, Protocol, Port range, Source, and Description. The table contains one rule:

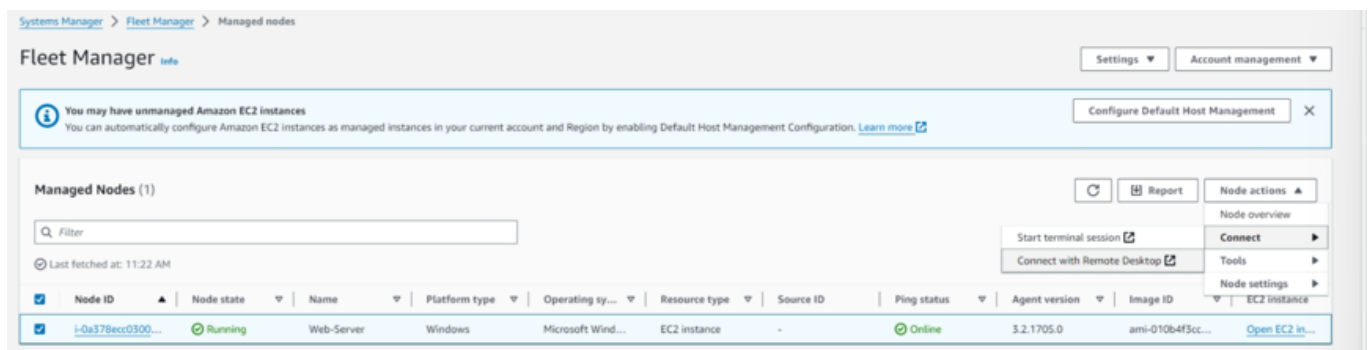
Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sg-0de078fca80b080b	IPv4	HTTP	TCP	80	0.0.0.0/0	-

## Task 4: Connecting to your instance using AWS Systems Manager Fleet Manager

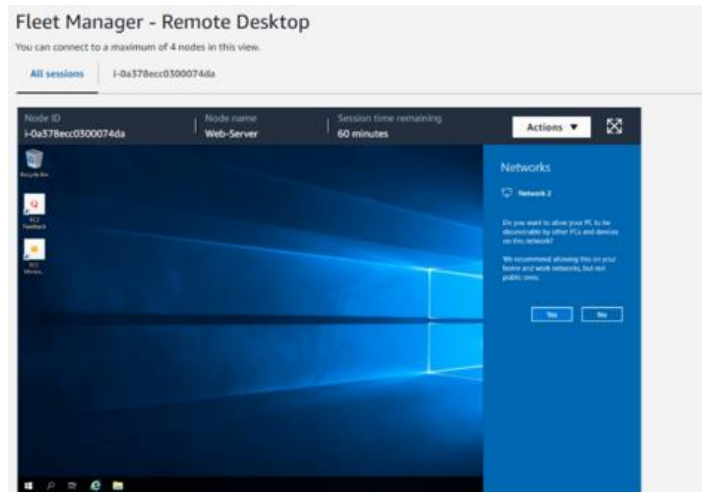
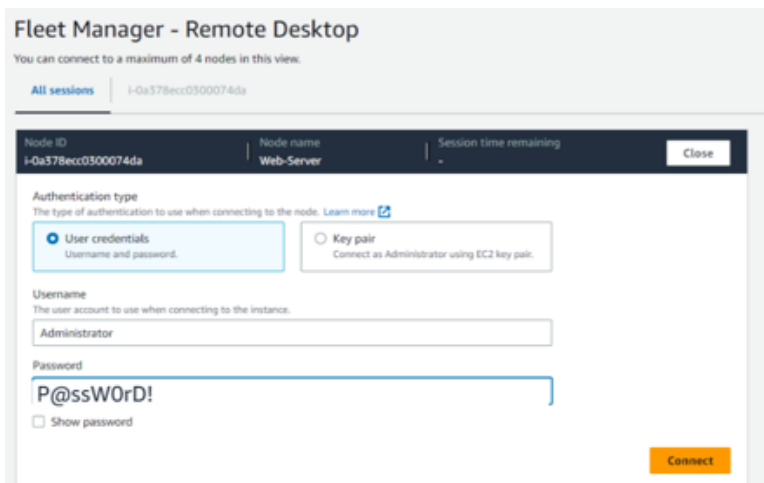
Search for Systems Manager and choose Enter. Choose Systems Manager.



In left navigation pane, choose Fleet Manager. Under Managed nodes, select your Web-Server EC2 instance. From the Node actions dropdown list, choose Connect, then Connect with Remote Desktop.



Enter the Username: Administrator. Enter the Password: P@ssW0rD! 43. Choose Connect.

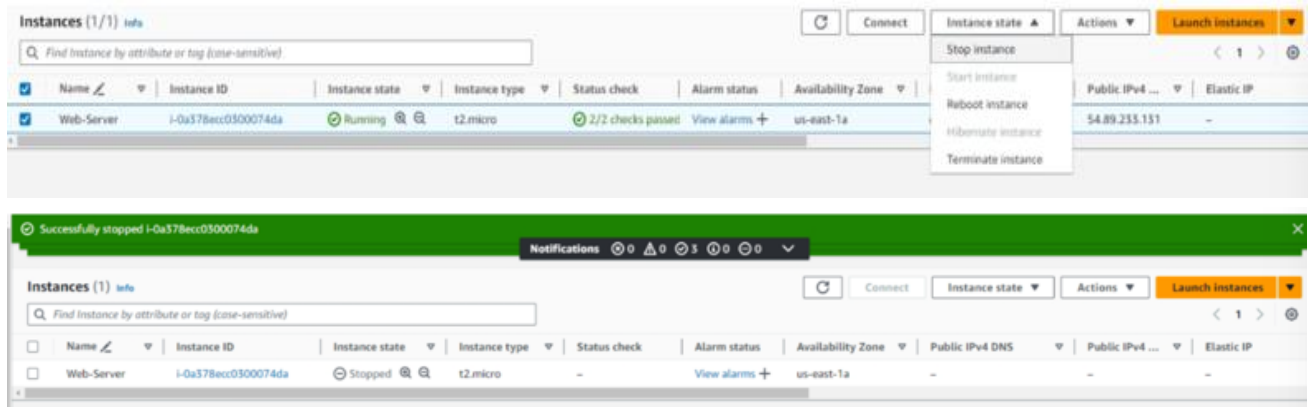


To disconnect from your Web-Server instance, choose Action and then choose End session.



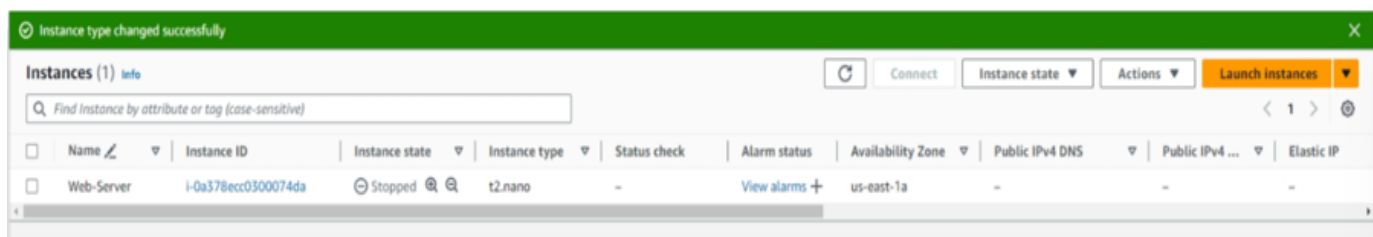
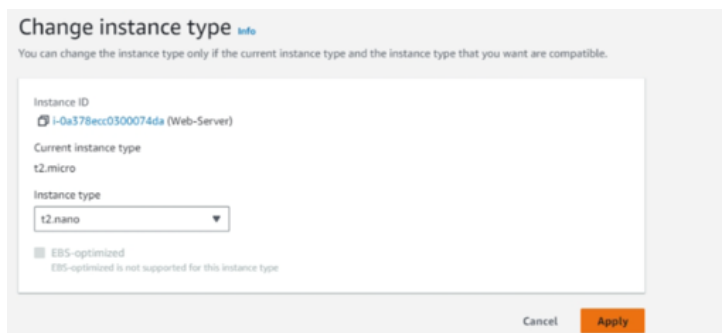
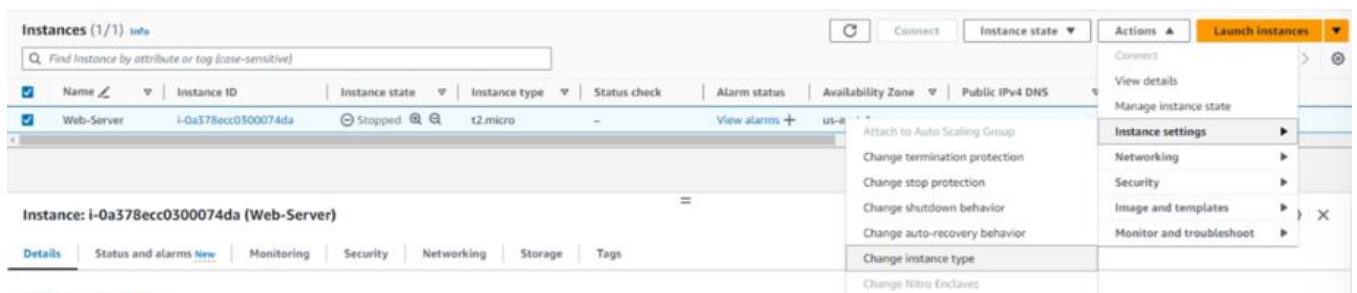
## Task 5: Resizing your instance

In the AWS Management Console, search for EC2 and choose Enter. Then, choose EC2. On the EC2 Management Console, left navigation pane, choose Instances. Select the check box next to your Web-Server instance. At the top of the page, choose the Instance state dropdown list, choose Stop instance.



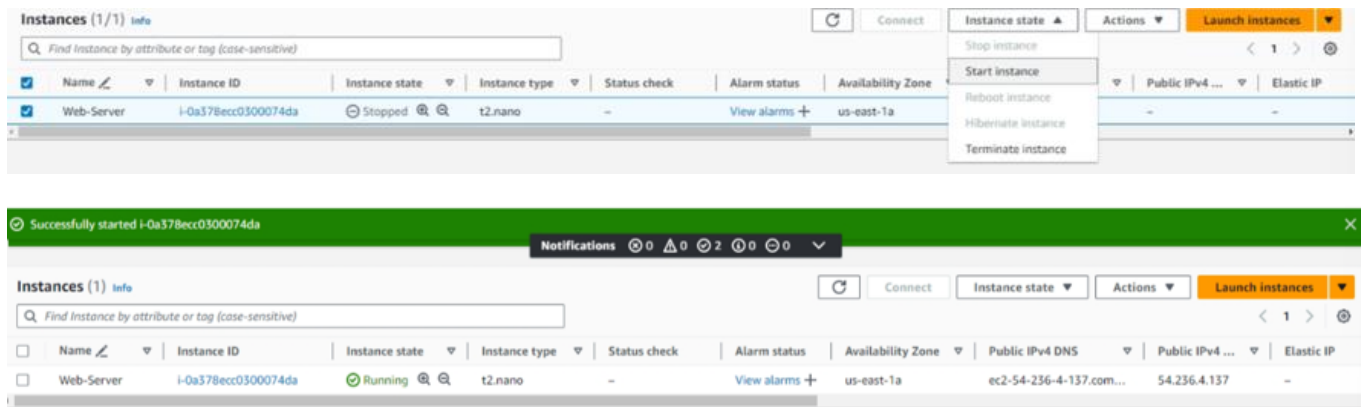
Select the check box next to your Web-Server. From the Actions dropdown list, select Instance settings Change instance type, and then configure the following option:

Instance type: Select t2.nano. And select Apply.





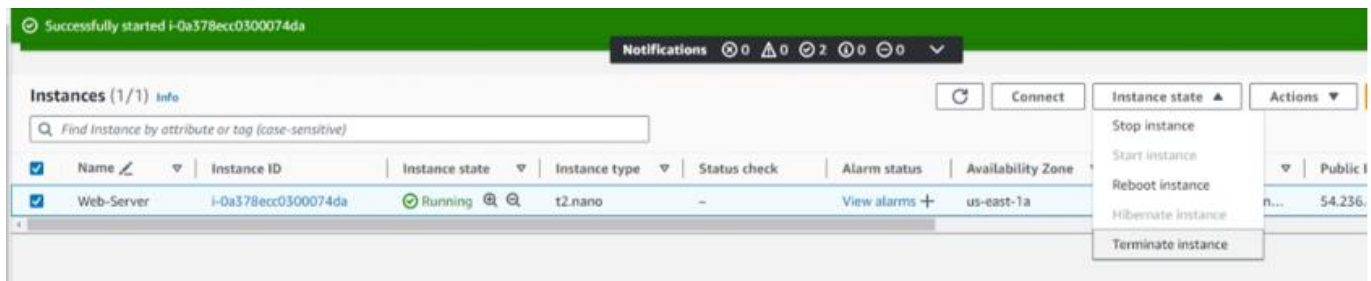
Now, again start the instance.



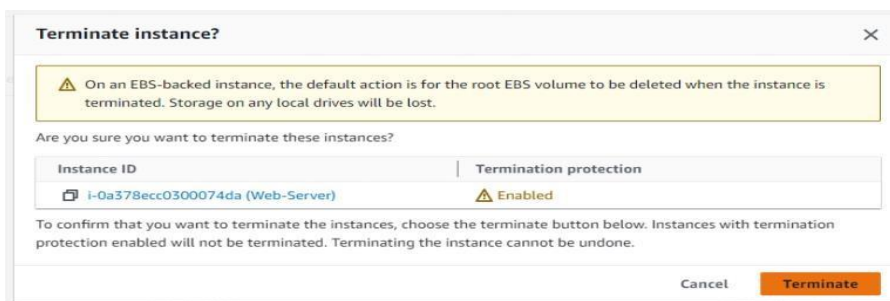
The screenshot shows the AWS Management Console 'Instances' page. The instance 'Web-Server' (ID: i-Oa378ecc0300074da) is in a 'Stopped' state. The 'Instance state' dropdown menu is open, showing options: Stop instance, Start instance, Reboot instance, Hibernate instance, and Terminate instance. The 'Start instance' option is selected.

## Task 6: Testing termination protection

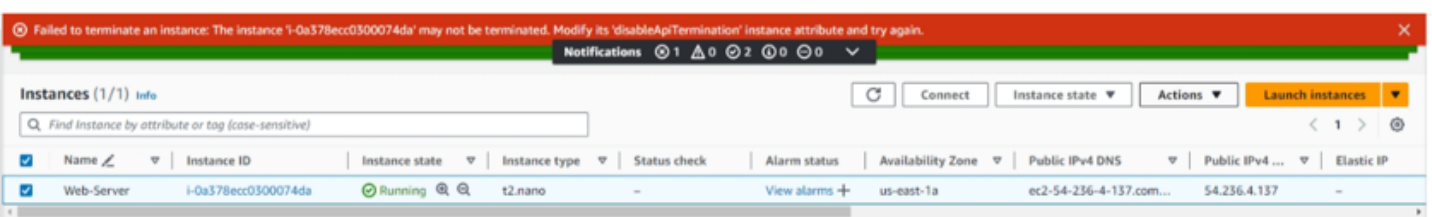
Select the check box next to your Web-Server instance. From the Instance state dropdown list, choose Terminate instance.



The screenshot shows the AWS Management Console 'Instances' page. The instance 'Web-Server' (ID: i-Oa378ecc0300074da) is in a 'Running' state. The 'Instance state' dropdown menu is open, showing options: Stop instance, Start instance, Reboot instance, Hibernate instance, and Terminate instance. The 'Terminate instance' option is selected.



The screenshot shows the 'Terminate instance?' dialog box. It contains a warning message: "On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost." Below this, it asks "Are you sure you want to terminate these instances?". The 'Instance ID' is 'i-Oa378ecc0300074da (Web-Server)' and 'Termination protection' is 'Enabled'. At the bottom, there are 'Cancel' and 'Terminate' buttons.



The screenshot shows the AWS Management Console 'Instances' page. A red error banner at the top reads: "Failed to terminate an instance: The instance 'i-Oa378ecc0300074da' may not be terminated. Modify its 'DisableApiTermination' instance attribute and try again." The 'Web-Server' instance (ID: i-Oa378ecc0300074da) is in a 'Running' state.

Notice that Termination protection is enabled. This is a safeguard to prevent the accidental termination of an instance.

If you really want to terminate the instance, you need to turn off termination protection.

Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Web-Server	i-0a378ecc0300074da	Running	t2.nano	-	View alarms +		

Instance: i-0a378ecc0300074da (Web-Server)

Details | Status and alarms **New** | Monitoring | Security | Networking | Storage | Tags

Actions

- Connect
- View details
- Manage instance state
- Attach to Auto Scaling Group
- Change termination protection
- Change stop protection
- Change shutdown behavior
- Change auto-recovery behavior
- Change instance type

Instance settings

- Networking
- Security
- Image and templates
- Monitor and troubleshoot

### Change termination protection

To prevent your instance from being accidentally terminated, you can enable termination protection for the instance. [Learn more](#)

Instance ID  
i-0a378ecc0300074da (Web-Server)

Termination protection  
☐ Enable

**Termination protection disabled.**  
The instance is no longer protected against accidental termination. If the instance is terminated, data stored on ephemeral storage is lost.

Cancel Save

Successfully removed termination protection for instance i-0a378ecc0300074da. The instance can be terminated.

Notifications 1 0 3 0 0 0

Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Elastic IP
Web-Server	i-0a378ecc0300074da	Running	t2.nano	-	View alarms +	us-east-1a	ec2-54-236-4-137.com...	54.236.4.137

Actions

- Stop instance
- Start instance
- Reboot instance
- Hibernate instance
- Terminate instance

Termination protection is disabled. Now, you can terminate the instance.

### Terminate instance?

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

Are you sure you want to terminate these instances?

Instance ID	Termination protection
i-0a378ecc0300074da (Web-Server)	Disabled

To confirm that you want to terminate the instances, choose the terminate button below. Instances with termination protection enabled will not be terminated. Terminating the instance cannot be undone.

Cancel Terminate

Successfully terminated i-0a378ecc0300074da

Notifications 1 0 4 0 0 0

EC2 Dashboard | EC2 Global View | Events | Console | Previous

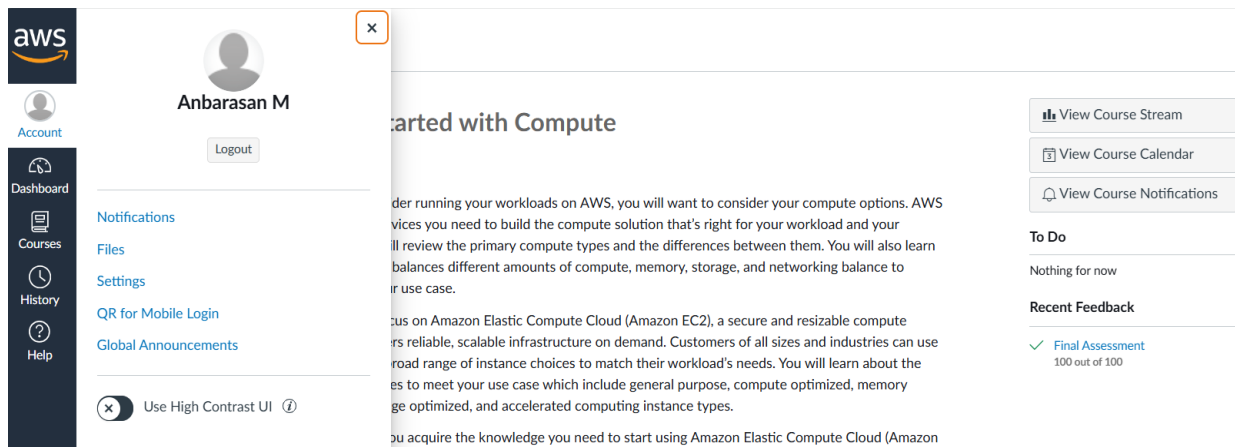
Instances

Instance Types

The instance has now successfully terminated.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
Web-Server	i-0a378ecc0300074da	Shutting-d...	t2.nano	-	View alarms +	us-east-1a	ec2-54-236-4-137.com...	54.236.4.137	-

## Screenshot of AWS login:



## **Result:**

Thus the implementation of Iaas through computing amazon EC2 have been successfully completed.