

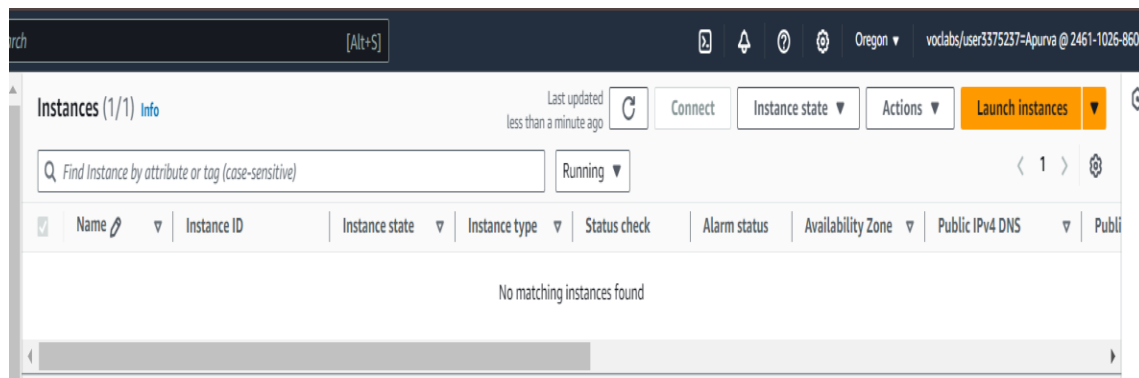
ASSIGNMENT-I

Working and Implementation of Infrastructure as a service Launch EC2 Instance(Windows)- AWS Platform. Prepare Screenshots file. Write down the steps to launch EC2 instance (Windows) Make single Word or PDF file .

Step 1: Log in to AWS Management Console and Navigate to EC2 Dashboard

1. Log in to the AWS Management Console at <https://aws.amazon.com/>.
2. In the search bar at the top, type EC2 and select it from the dropdown.
3. This will take you to the EC2 Dashboard.

Step 2: Launch Instance



On the EC2 Dashboard, click on Launch instance.

2. In the "Name and tags" section, provide a name for your instance, for example: MyWindowsInstance.

Services

Q Search

[Alt+S]

[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

MyWindowsInstance

Add additional tags

Step 3: Choose an Amazon Machine Image (AMI)

1. In the "Application and OS Images (Amazon Machine Image)" section, scroll down and select a Windows Server AMI, such as Microsoft Windows Server 2022 Base.

▼ 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

Q Search our full catalog including 1000s of application and OS images

Recents

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Li

SUS

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Microsoft Windows Server 2022 Base

Free tier eligible

ami-0845068028e672a07 (64-bit (x86))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Microsoft Windows 2022 Datacenter edition. [English]

Architecture

AMI ID

Username

64-bit (x86)

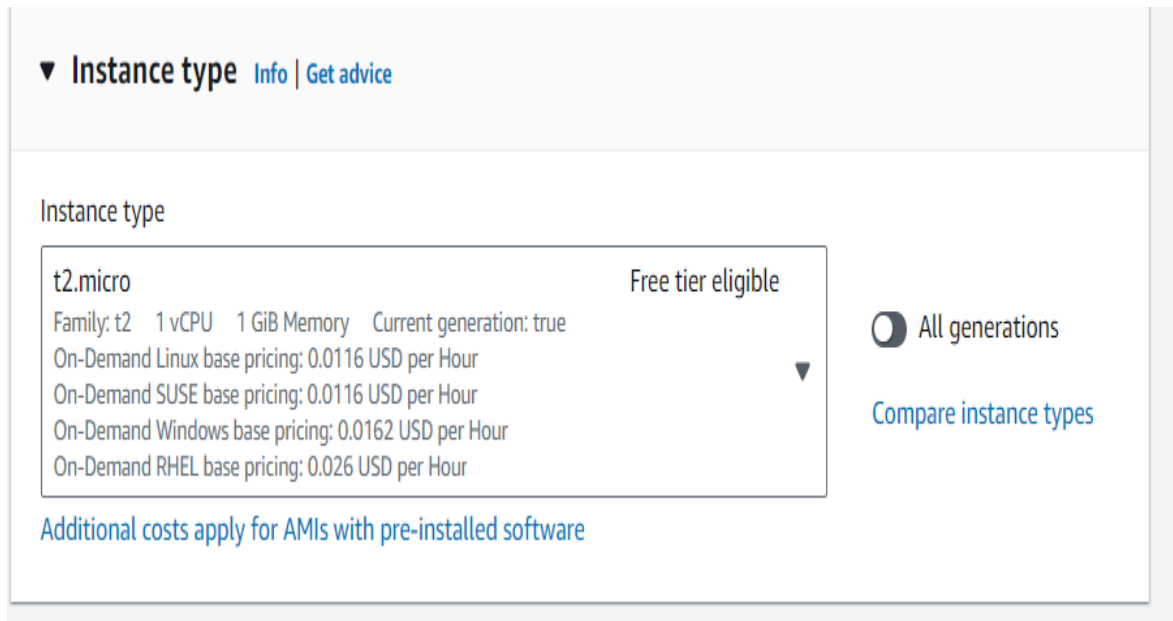
ami-0845068028e672a07

root

Verified provider

Step 4: Choose an Instance Type

1. Select an instance type such as t2.micro (free tier eligible).



2. Click Next: Configure Instance Details.

Step 5: Configure Instance Details

1. Leave the default settings or modify according to your needs.

2. Click Next: Add Storage.

Step 6: Add Storage

1. The default storage size is sufficient for basic use. Modify it if needed.

▼ **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: Add Key Pair

1. When prompted, Create a new key pair or select an existing one.
2. Name your key pair (e.g., Window) and download the private key file (`.pem`).

▼ **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*

▼

Create new key pair

For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.

3. Store this key file securely on your system.

Step 8: Configure Security Group

1. Create a new security group or use an existing one.
2. Make sure to allow RDP access by enabling inbound traffic on port 3389.
3. Also allow HTTP traffic for web services by enabling port 80.

▼ Network settings [Info](#)

Edit

Network [Info](#)

vpc-0a895b9422fd3af22

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

Additional charges apply when outside of free tier allowance

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

We'll create a new security group called 'launch-wizard-10' with the following rules:

☒ Allow RDP traffic from

Helps you connect to your instance

Anywhere
0.0.0.0/0

☐ Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

☒ Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

⚠ 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.

×

4. Click Review and Launch.

Step 9: Review and Launch

1. Review your instance details.

2. Click Launch and confirm by clicking Launch Instances.

The screenshot shows the 'Review and Launch' step in the AWS Management Console. The interface is divided into two main sections: configuration details on the left and a summary on the right.

Configuration Details (Left):

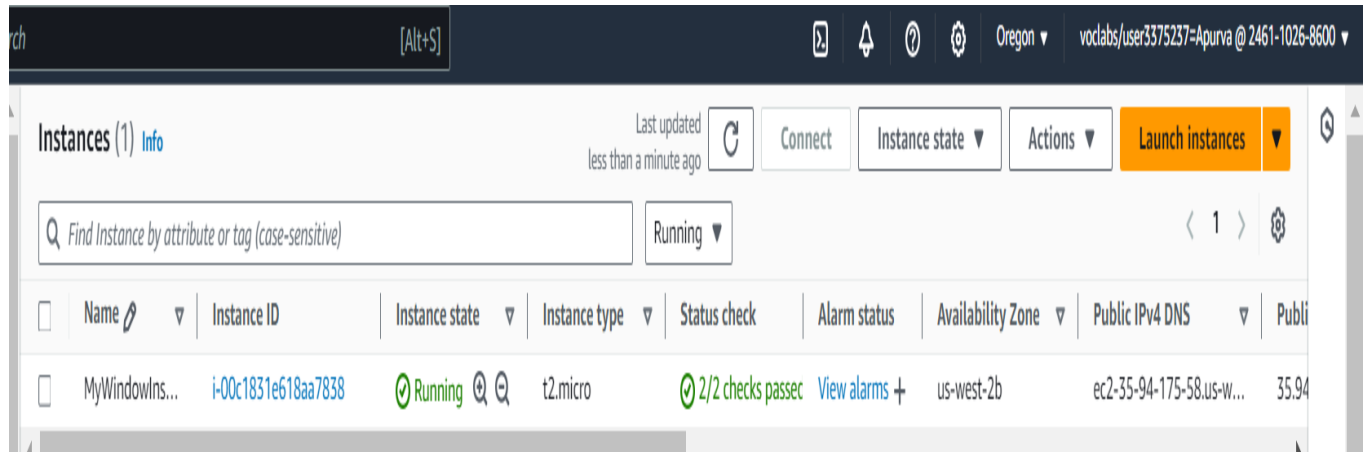
- Internet Access:** A checkbox labeled 'Allow HTTP traffic from the internet' is checked. Below it, a yellow warning box states: 'Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.'
- Configure storage:** A section with an 'Advanced' link. It shows '1x 30 GiB gp2' for the 'Root volume (Not encrypted)'. Below this, a blue information box states: 'Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage'. An 'Add new volume' button is present. A note below reads: '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.'
- Backup Information:** A section with a refresh icon and text: '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.'
- File Systems:** Shows '0 x File systems' with an 'Edit' link.
- Advanced details:** A link at the bottom left of the configuration section.

Summary (Right):

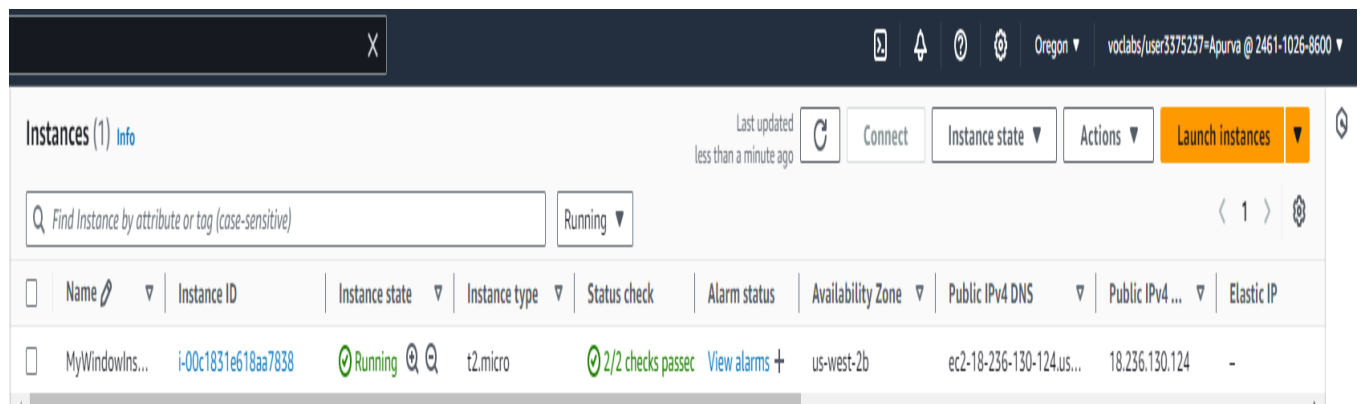
- Number of instances:** A dropdown menu set to '1'.
- Software Image (AMI):** 'Microsoft Windows Server 2022 ...read more' with the ID 'ami-0845068028e672a07'.
- Virtual server type (instance type):** 't2.micro'.
- Firewall (security group):** 'New security group'.
- Storage (volumes):** '1 volume(s) - 30 GiB'.
- Free tier:** A blue information box states: 'Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100'.
- Buttons:** 'Cancel' and 'Launch instance' (orange button). A 'Review commands' link is at the bottom.

Step 10: View Instance

1. Click on View Instances to check the status of your instance.
2. Wait for the instance's status to change to Running



Step 11: Choose the Instance and then connect it.



Step 12: then click on RDP client and download the remote desktop file.

Step 13: then click on Get Password and add their private key and then decrypt password and copy it.

Connect to instance [Info](#)

Connect to your instance i-00c1831e618aa7838 (MyWindowInstance) using any of these options

[Session Manager](#)[RDP client](#)[EC2 serial console](#)

Instance ID

i-00c1831e618aa7838 (MyWindowInstance)

Connection Type

☒ Connect using RDP client

Download a file to use with your RDP client and retrieve your password.

☐ Connect using Fleet Manager

To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#)

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[Download remote desktop file](#)

When prompted, connect to your instance using the following username and password:

Public DNS



ec2-18-236-130-124.us-west-
2.compute.amazonaws.com

Username [Info](#)



Administrator ▼

Password [Get password](#)

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

Cancel

Step13: then click on Get Password and add their private key and then decrypt password and copy it.

EC2 > Instances > i-00c1831e618aa7838 > Get Windows password

Get Windows password [Info](#)

Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.

Instance ID
i-00c1831e618aa7838 (MyWindowInstance)

Key pair associated with this instance
Windows

Private key
Either upload your private key file or copy and paste its contents into the field below.

[Upload private key file](#)

Windows.pem
1.678KB

Private key contents - optional

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAnosKCCkb39GH2MoLqiv5LkzJBzMfJgngclYIF/vENbscu1Li
vZAosKhIEjNR7nd0FuYv3qJYbDRScRjQWkk0m1OQTEbMf7pPfjLckYoKFj8DT1Na
Ij+rcfoDdLErNzcjJWz0saDIXq7cZRirJo8M05Pc/JjAazWUeGljahNEyy9ONc6e
ZYapV0OBmn1E+1LtLV5Y4oC3n7/ZTbYyIV+3i2TbRoWVFsedliQ0MGWM5Ja903gC
C1m/MduCrBb8OdRixM6ccIAfs4s9Ee1NzsltdvsnElQqtxfatc5wgDXI2vtUwqp3
yVpY2Tv4OIIPBoZbhHuhjiNpBGg64M/bKL5blwIDAQABAoIBADQSBkCaB4lympCs
g7pHqRb450nzE3b15X8IHK5r5ZzUMPkhNZEvSP4EwPWCX5WYLEvdHLndznd8Nfup
-----
```

[Cancel](#) [Decrypt](#)

Services [ec2](#)

Connect to instance [Info](#)

Connect to your instance i-00c1831e618aa7838 (MyWindowInstance) using any of these options

Session Manager | **RDP client** | EC2 serial console

Instance ID
i-00c1831e618aa7838 (MyWindowInstance)

Connection Type

Connect using RDP client
Download a file to use with your RDP client and retrieve your password.

Connect using Fleet Manager
To connect to the instance using Fleet Manager Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#)

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading the RDP shortcut file below:

[Download remote desktop file](#)

When prompted, connect to your instance using the following username and password:

Public DNS
ec2-18-236-130-124.us-west-2.amazonaws.com

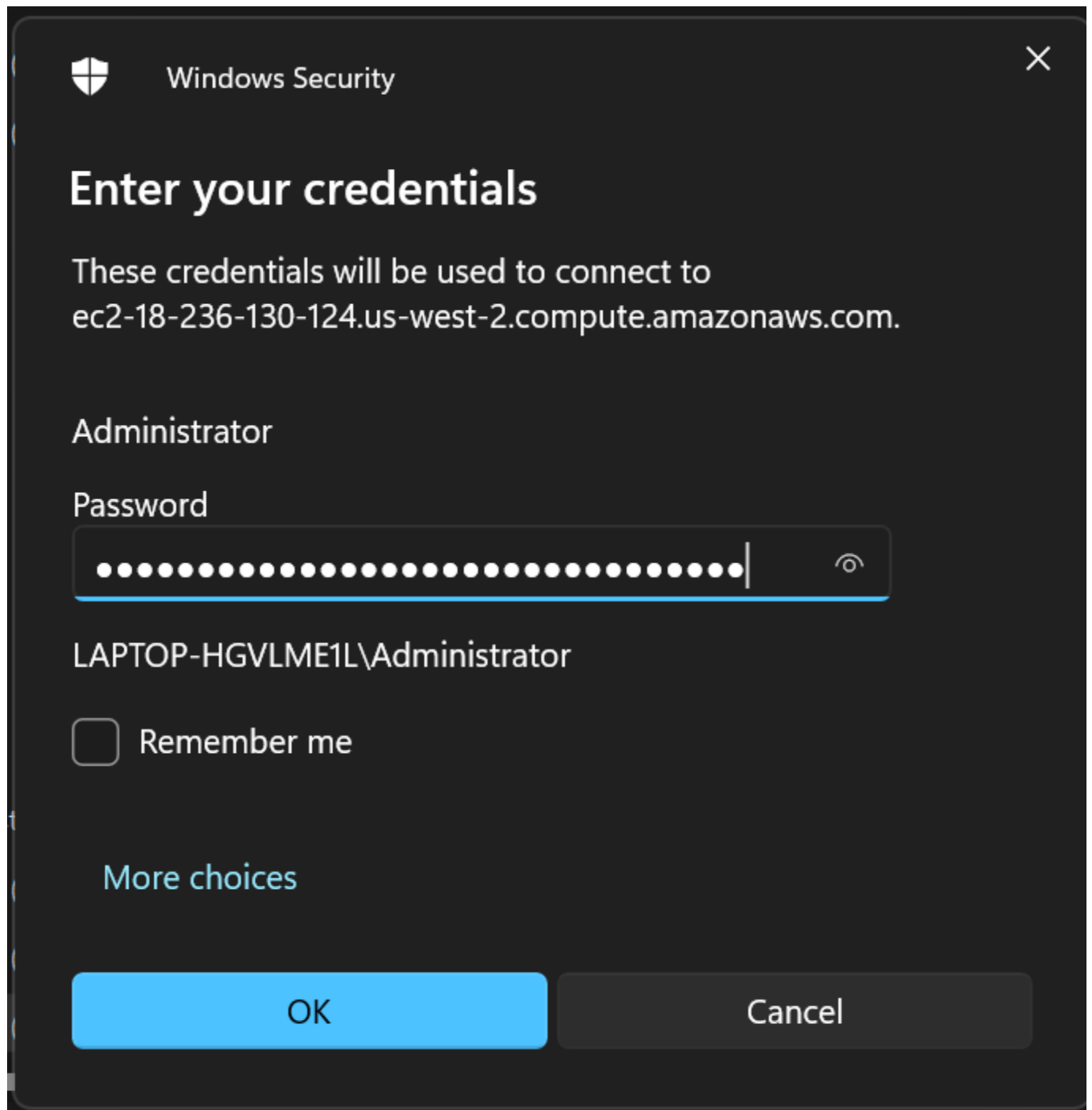
Username [Info](#)
Administrator

Password
ElsS=7TPK-8%M)oZOQna&lZcppDLc\$M

[Password copied](#)

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

Step 14: then open the downloaded file and paste copied password.



Step 15: then click on Ok and we can see the Windows Page.



Recycle Bin



EC2
Feedback



EC2
Microso...



Microsoft
Edge

Hostname: EC2AMAZ-DC8J6B6
Instance ID: i-00c1831e618aa7838
Private IPv4 address: 172.31.17.152
Public IPv4 address: 18.236.130.124
Instance size: t2.micro
Availability Zone: us-west-2b
Architecture: AMD64
Total memory: 1024
Network: Low to Moderate



Type here to search



ENG 10:01 AM
IN 9/30/2024