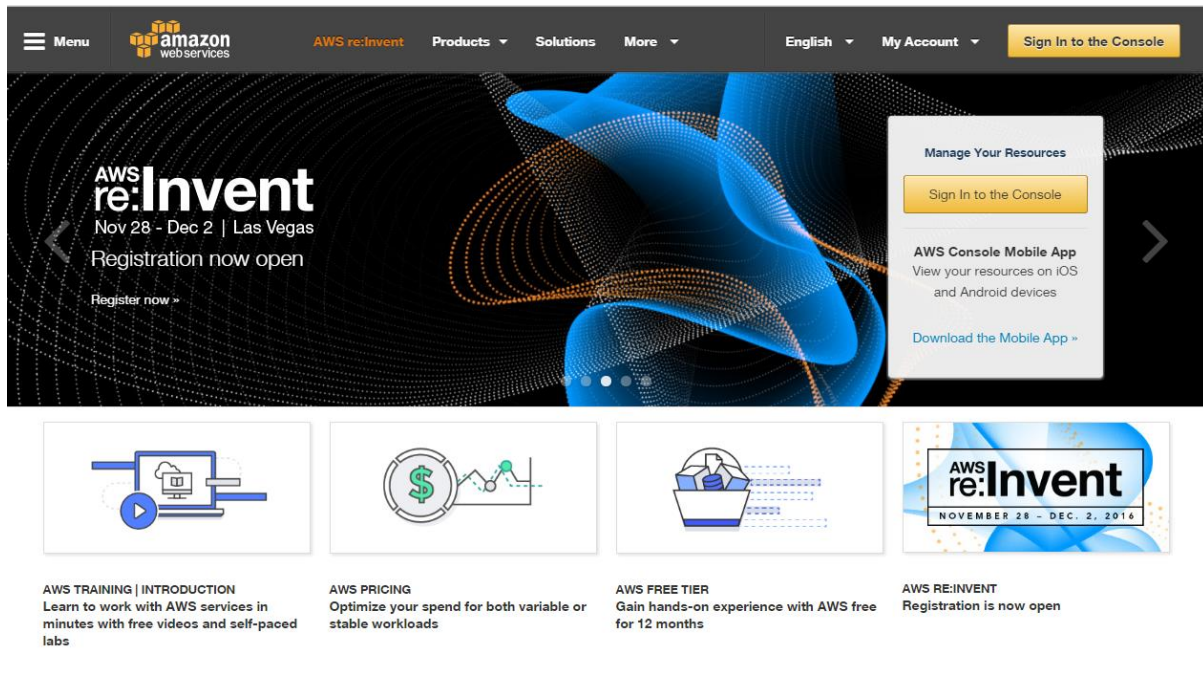


Create Windows 2012 instance in AWS

- Logging in to AWS console using this link <https://aws.amazon.com/>



- When we logged we can see the console of AWS

AWS

Services

Edit

Anusha Chaturanga

Oregon

Support

Amazon Web Services

Compute

EC2

Virtual Servers in the Cloud

EC2 Container Service

Run and Manage Docker Containers

Elastic Beanstalk

Run and Manage Web Apps

Lambda

Run Code in Response to Events

Storage & Content Delivery

S3

Scalable Storage in the Cloud

CloudFront

Global Content Delivery Network

Elastic File System

Fully Managed File System for EC2

Glacier

Archive Storage in the Cloud

Snowball

Large Scale Data Transport

Storage Gateway

Hybrid Storage Integration

Database

RDS

Managed Relational Database Service

DynamoDB

Managed NoSQL Database

ElastiCache

In-Memory Cache

Redshift

Fast, Simple, Cost-Effective Data Warehousing

DMS

Managed Database Migration Service

Networking

VPC

Isolated Cloud Resources

Direct Connect

Dedicated Network Connection to AWS

Route 53

Scalable DNS and Domain Name Registration

Developer Tools

CodeCommit

Store Code in Private Git Repositories

CodeDeploy

Automate Code Deployments

CodePipeline

Release Software using Continuous Delivery

Management Tools

CloudWatch

Monitor Resources and Applications

CloudFormation

Create and Manage Resources with Templates

CloudTrail

Track User Activity and API Usage

Config

Track Resource Inventory and Changes

OpsWorks

Automate Operations with Chef

Service Catalog

Create and Use Standardized Products

Trusted Advisor

Optimize Performance and Security

Security & Identity

Identity & Access Management

Manage User Access and Encryption Keys

Directory Service

Host and Manage Active Directory

Inspector

Analyze Application Security

WAF

Filter Malicious Web Traffic

Certificate Manager

Provision, Manage, and Deploy SSL/TLS Certificates

Analytics

EMR

Managed Hadoop Framework

Data Pipeline

Orchestration for Data-Driven Workflows

Elasticsearch Service

Run and Scale Elasticsearch Clusters

Kinesis

Internet of Things

AWS IoT

Connect Devices to the Cloud

Game Development

Gamelift

Deploy and Scale Session-based Multiplayer Games

Mobile Services

Mobile Hub

Build, Test, and Monitor Mobile Apps

Cognito

User Identity and App Data Synchronization

Device Farm

Test Android, iOS, and Web Apps on Real Devices in the Cloud

Mobile Analytics

Collect, View and Export App Analytics

SNS

Push Notification Service

Application Services

API Gateway

Build, Deploy and Manage APIs

AppStream

Low Latency Application Streaming

CloudSearch

Managed Search Service

Elastic Transcoder

Easy-to-Use Scalable Media Transcoding

SES

Email Sending and Receiving Service

SQS

Message Queue Service

SWF

Workflow Service for Coordinating Application Components

Enterprise Applications

WorkSpaces

Desktops in the Cloud

WorkDocs

Secure Enterprise Storage and Sharing Service

WorkMail

Secure Email and Collaboration Service

Resource Groups

Learn more

A resource group is a collection of resources that share one or more tags. Create a group for each project, application, or environment in your account.

Create a Group

Tag Editor

Additional Resources

Getting Started

Read our documentation or view our training to learn more about AWS.

AWS Console Mobile App

View your resources on the go with our AWS Console mobile app, available from Amazon Appstore, Google Play, or iTunes.

AWS Marketplace

Find and buy software, launch with 1-Click and pay by the hour.

AWS re:Invent Announcements

Explore the next generation of AWS cloud capabilities. See what's new

Service Health

Unable to retrieve service health updates.

Service Health Dashboard

- You already have instance on AWS you can see all details of EC2 resources, so create new instance click on Launch Instance button

Resources

You are using the following Amazon EC2 resources in the US West (Oregon) region:

1 Running Instances	0 Elastic IPs
0 Dedicated Hosts	0 Snapshots
2 Volumes	0 Load Balancers
1 Key Pairs	7 Security Groups
0 Placement Groups	

Build and run distributed, fault-tolerant applications in the cloud with [Amazon Simple Workflow Service](#).

Create Instance

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

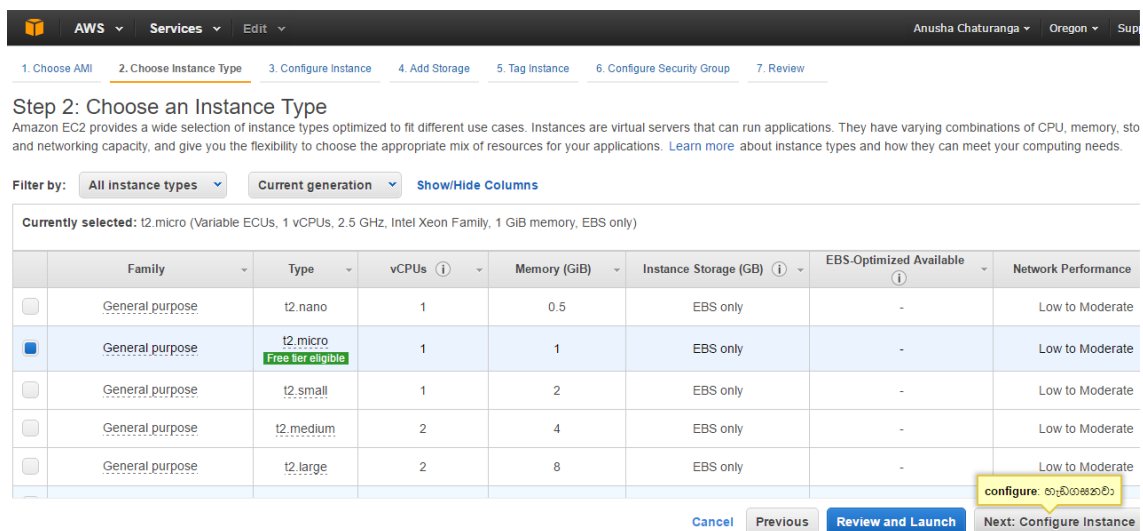
[Launch Instance](#)

Note: Your instances will launch in the US West (Oregon) region

- Now you can see several Operating Systems and details of each then select Microsoft Windows Server 2012 R2 Base Free tier eligible



- Select t2 micro(Free tier eligible) and click Review and Launch(default configuration)



- Now you can see Review instance page that page contain all configuration what we have configured so far hit Launch button to launch instance

AWS Services Edit Anusha Chaturanga Oregon Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

⚠ Improve your instances' security. Your security group, launch-wizard-3, 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](#)

AMI Details [Edit AMI](#)

Microsoft Windows Server 2012 R2 Base - ami-26e72546

Free tier eligible Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English]
 Root Device Type: ebs Virtualization type: hvm

If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the [License Mobility Form](#). [Don't show me this again](#)

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

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

- Then pop-up come and ask for a key pair if you currently have key pair select “Choose an existing pair” if not Create new key pair I already have key pair and I used that key pair for my instance so launch instance you must put tic on bottom(Red Colour circle)

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

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

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

Choose an existing key pair ▼

Select a key pair

annnnnuza ▼

☒ I acknowledge that I have access to the selected private key file (annnnnuza.pem), and that without this file, I won't be able to log into my instance.

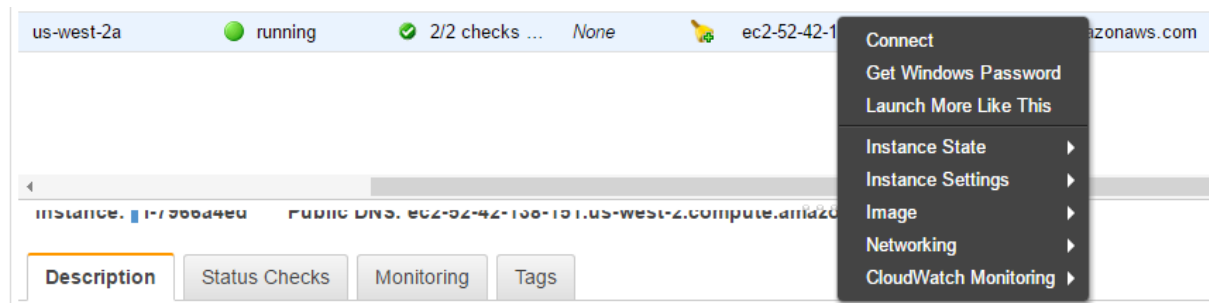
[Cancel](#) [Launch Instances](#)

- Now you can see running instance on EC2 Console

Filter by tags and attributes or search by keyword									
	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS	Publ
<input checked="" type="checkbox"/>		i-1b53908f	t2.micro	us-west-2a	running	2/2 checks ...	None	ec2-52-42-252-98.us-we...	52.42
<input type="checkbox"/>		i-4f63d5e0	t2.micro	us-west-2b	stopped		None		

Connect to AWS Windows instance

- Right Click on instance and select connect



- Now pop-up came and asked to select you key pair then locate key file on computer or you can paste key file contained then click Decrypt Password

Retrieve Default Windows Administrator Password

To access this instance remotely (e.g. Remote Desktop Connection), you will need your Windows Administrator password. A default password was created when the instance was launched and is available encrypted in the system log.

To decrypt your password, you will need your key pair for this instance. Browse to your key pair, or copy and paste the contents of your private key file into the text area below, then click Decrypt Password.

The following Key Pair was associated with this instance when it was created.

Key Namekey2

In order to retrieve your password you will need to specify the path of this Key Pair on your local machine:

Key Pair Path No file chosen

Or you can copy and paste the contents of the Key Pair below:

Paste contents of private key file here

Cancel

Decrypt Password

- Now you can see your Windows instance Username and Password

Retrieve Default Windows Administrator Password

Password Encryption Successful

The password for instance i-7966a4ed was successfully decrypted.

Password change recommended

We recommend that you change your default password. Note: If a default password is changed, it cannot be retrieved through this tool. It's important that you change your password to one that you will remember.

You can connect remotely using this information:

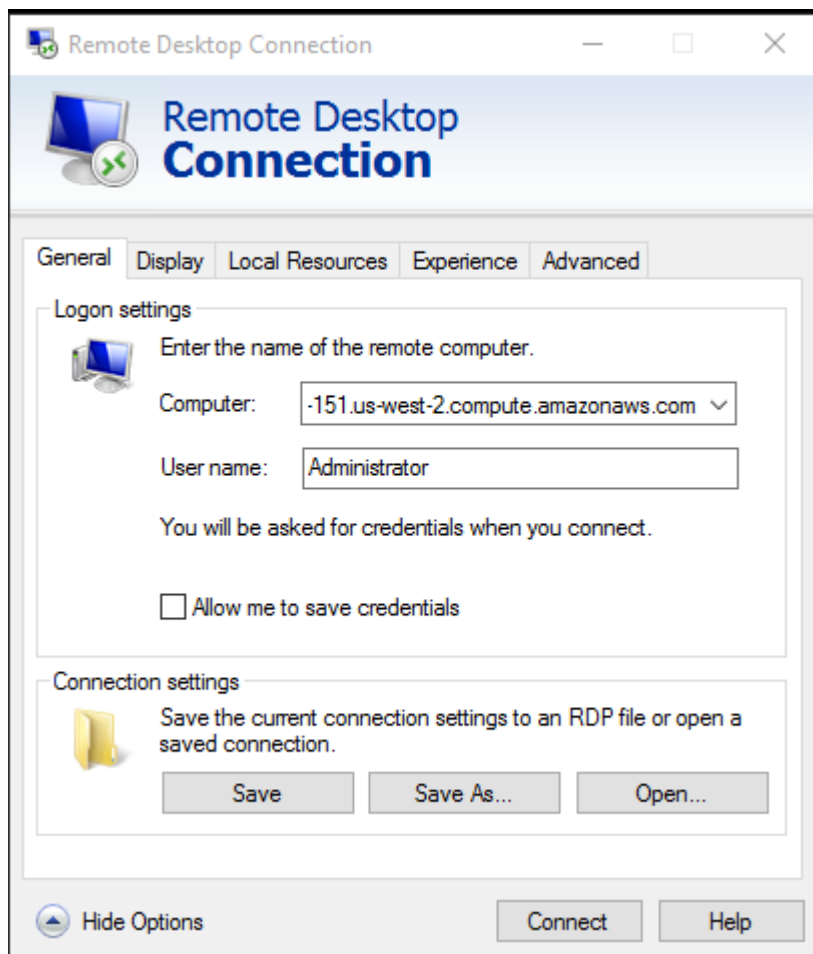
Public DNS ec2-52-42-138-151.us-west-2.compute.amazonaws.com

User name Administrator

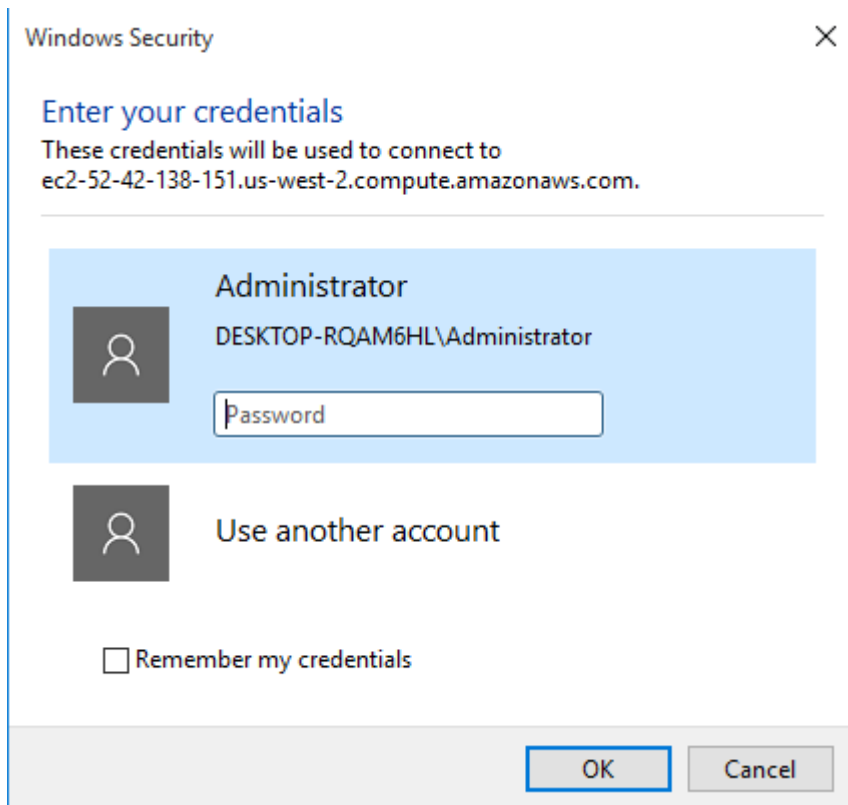
Password

Close

- Copy your Public DNS and start Windows Remote Desktop Connection so when it started paste DNS to first textbox and also type user name as Administrator all steps were done next click Connect button



- Now you can see new window appear and ask password of Administrator account copy the password before we get and paste it and click ok



- Finally, new window opens and asked security certificates click yes



- Connection was done

