

Capstone Project: Deploying Cart Management Application to Cloud

DESCRIPTION

You work for an E-commerce company and as a Cloud Architect you are asked to deploy the Cart Management Application on cloud.

Background of the problem statement:

The company has created a new website for the organization where the user can add and delete products from the cart. The company wants to use a public cloud for the internet facing website of the organization. Once the website was deployed, users started complaining that all the products are not loading fast enough. You realized that the website gets global traffic and the static assets like pages and products are served from a single server. You need to make sure that the traffic coming to the application from different parts of the world is load balanced at the DNS level. Also, internal employees within your organization told that they are facing difficulty in accessing common files of the website, as they need to get it from each other when accessing them from Virtual Machine.

You can use either Azure or AWS platforms to design the solution using IaaS OR PaaS.

You must use the following tools:

- AWS: Route 53, S3 Bucket, CloudFront, EC2
- Azure: Azure App Service, CDN, DNS, Azure VM, Azure Traffic Manager

Following requirements should be met:

1. Suggest an appropriate solution so that your company can make use of cloud while keeping the requirements mentioned above for your company in mind
2. Provide an approach to:
 - a. Govern all the resources being used for development, testing, and production of the company's website.
 - b. Keep a separate track of the billing life cycle and cost management of all the services being used for hosting the company's website on Cloud
3. Upload all static content of your website to cloud
4. Create a CDN endpoint and configure it to serve the static files you have uploaded
5. Use storage service and upload files for your teammates to share
6. Connect Windows or Linux VM to the Storage service

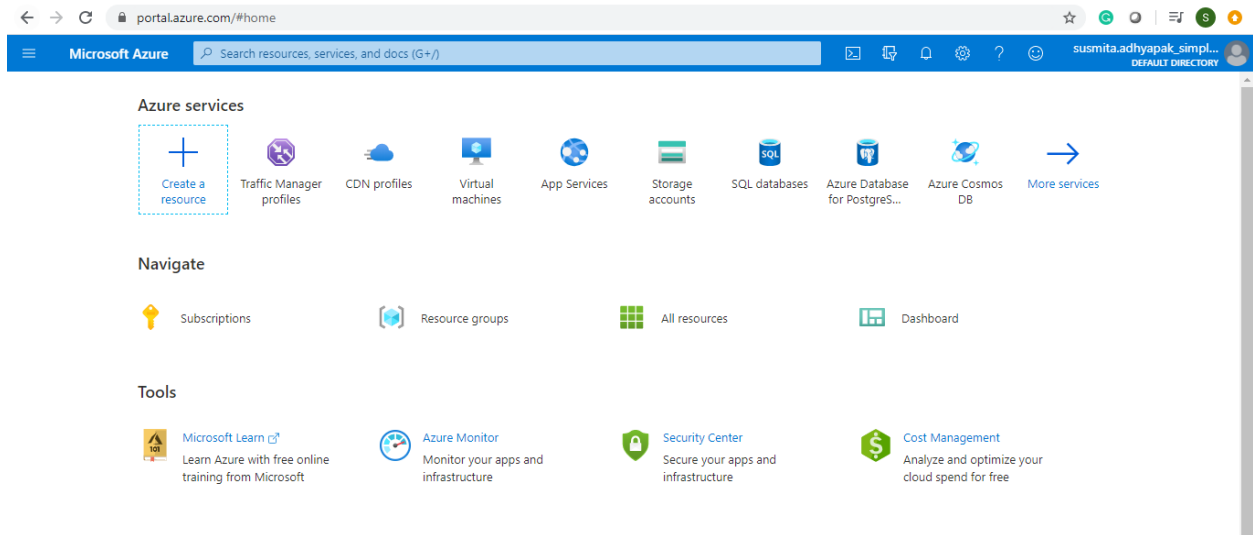
This section will guide you to deploy an application on:

- Azure
- AWS

Azure:

Approach 1:

Step 1: Log into the Azure portal

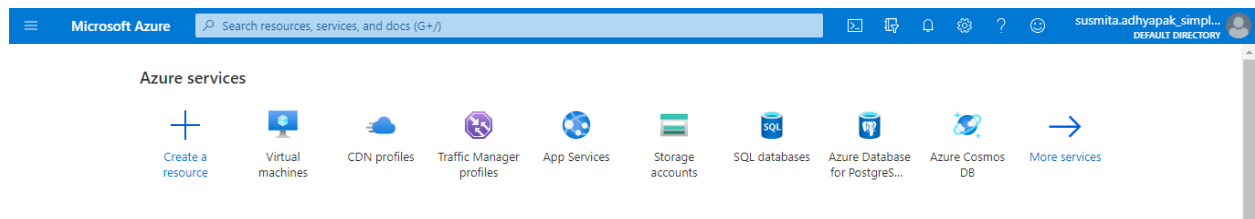


Step 2: Before creating the resources, make sure you apply tags to the resources so that you can keep a track of billing later on

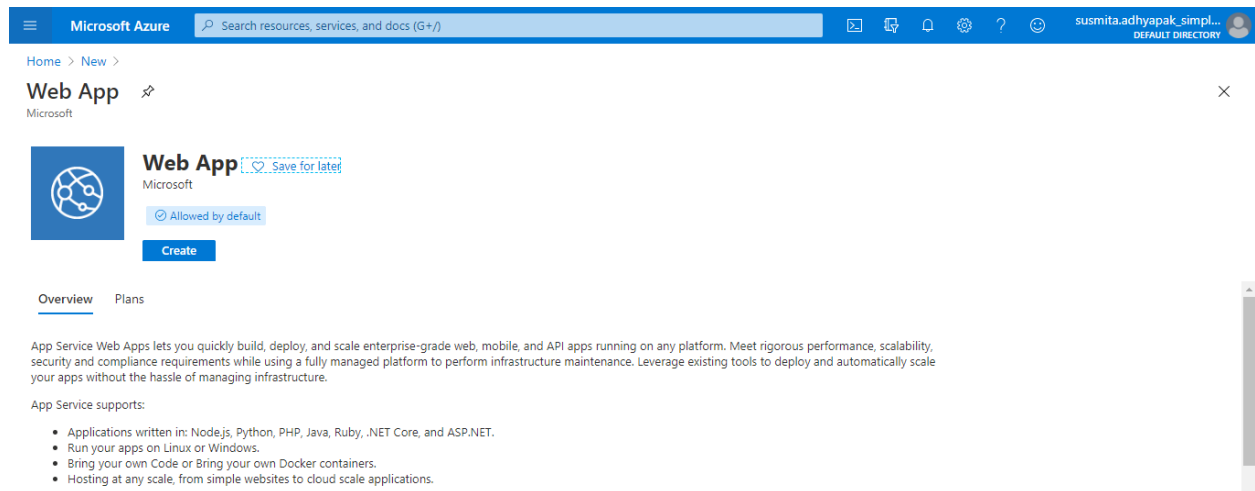
Step 3: To begin, create an Azure App service plan in the standard tier.

Step 4: Create an App Service (Web App) using the App Service Plan that you created in the previous step

Step 4.1: Click on the **Create a resource** tab



Step 4.2: Search for Web App and click on the **Create** tab



Step 4.3: Provide basic information in the application

Microsoft Azure

Search resources, services, and docs (G+)

asmita.ray_simplilearn.n...
DEFAULT DIRECTORY

Home > New > Web App >

Web App

Basics

Monitoring

Tags

Review + create

App Service Web Apps lets you quickly build, deploy, and scale enterprise-grade web, mobile, and API apps running on any platform. Meet rigorous performance, scalability, security and compliance requirements while using a fully managed platform to perform infrastructure maintenance. [Learn more](#)

Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Microsoft Azure Sponsorship - production

Resource Group *

rg-asmita.ray_simplilearn-ykuos

Create new

Instance Details

Name *

cartlapp

.azurewebsites.net

Publish *

☒ Code
 ☐ Docker Container

Review + create

< Previous

Next : Monitoring >

Microsoft Azure

Search resources, services, and docs (G+)

asmita.ray_simplilearn.n...
DEFAULT DIRECTORY

Home > New > Web App >

Web App

Basics

Monitoring

Tags

Review + create

Publish *

☒ Code
 ☐ Docker Container

Runtime stack *

ASP.NET V4.7

Operating System *

☐ Linux
 ☒ Windows

Region *

West US

Not finding your App Service Plan? Try a different region.

App Service Plan

App Service plan pricing tier determines the location, features, cost and compute resources associated with your app. [Learn more](#)

Windows Plan (West US) *

ASP-rgasmitaray_simplilearn-ykuos-a3f9 (S1)

Create new

Sku and size *

Standard S1

100 total ACU, 1.75 GB memory

Review + create

< Previous

Next : Monitoring >

Note: Choose the runtime stack as ASP.NET V4.7 and choose the region as West US or West US 2

Step 4.4: In the monitoring section, select **No** for **Enable Application Insights**

Microsoft Azure

Search resources, services, and docs (G+/I)

asmita.ray_simplilearn.n...

DEFAULT DIRECTORY

Home > New > Web App >

Web App

Basics

Monitoring

Tags

Review + create

Application Insights is a code-less attach to provide detailed observability in to your application. [Learn more](#)

Application Insights

Enable Application Insights *

☒ No
 ☐ Yes


Review + create

< Previous

Next : Tags >

Step 4.5: Click on **Review and Create**

Step 4.6: Click on **Create**


 **Microsoft Azure**

[Home](#) > [New](#) > [Web App](#) >

Web App

[Basics](#) [Monitoring](#) [Tags](#) **Review + create**

Summary

 **Web App**
by Microsoft

Details

Subscription	34f4ae1c-3e38-4e06-ae3-4b37a7d1b483
Resource Group	rg-asmita.ray_simplilearn-br5wl
Name	cart1app
Publish	Code
Runtime stack	ASP.NET V4.7

App Service Plan (New)

Name	ASP-rgasmitaraysimplilearnbr5wl-84fe
Operating System	Windows
Region	West US

Create [< Previous](#) [Next >](#) [Download a template for automation](#)

This will create the Web App on Azure.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information. The main content area displays the 'Overview' page for a deployment named 'Microsoft.Web-WebApp-Portal-61d280be-b507'. A green checkmark indicates that the deployment is complete. Key details include the deployment name, subscription (Microsoft Azure Sponsorship - production), resource group (rg-asmita.ray_simplilearn-ykuos), start time (6/9/2020, 2:21:37 PM), and correlation ID. A 'Go to resource' button is prominently displayed. On the right, there are links to the Security Center, Free Microsoft tutorials, and an option to work with an expert.

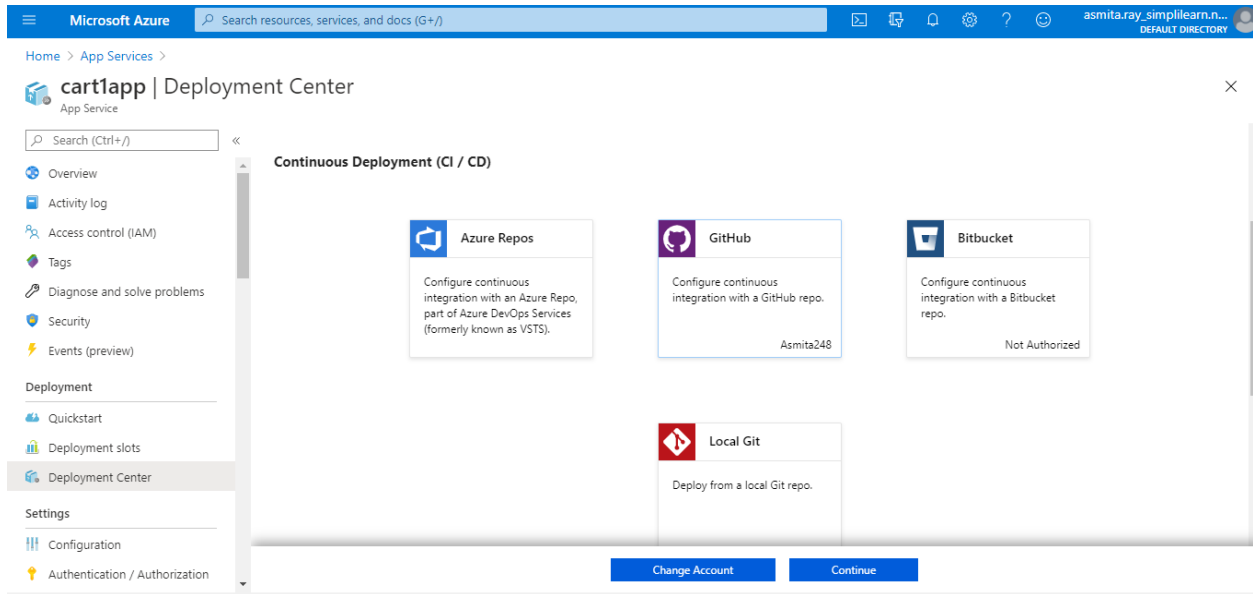
Step 4.7: Click on **Go to resource** to get the overview of the created web app

The screenshot shows the Microsoft Azure portal interface for the 'cart1app' App Service. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Security, Events (preview), Deployment, Quickstart, Deployment slots, Deployment Center, Settings, Configuration, and Authentication / Authorization. The main content area displays the 'Overview' page for the 'cart1app' App Service. A purple banner at the top provides a link to the Quickstart guide. Below this, a table lists key properties: Resource group (rg-asmita.ray_simplilearn-ykuos), URL (https://cart1app.azurewebsites.net), Status (Running), App Service Plan (ASP-rgasmitaray_simplilearn-ykuos-a3f9 (S1: 1)), Location (West US), FTP/deployment username (No FTP/deployment user set), Subscription ID (34f4ae1c-3e38-4e06-ae3-4b37a7d1b483), and Tags (Click here to add tags). At the bottom, there are three tiles for 'Diagnose and solve problems', 'Application Insights', and 'App Service Advisor', along with a 'Http 5xx' status indicator.

Step 5: Deploy your static web app to Azure App Service (web app) using a method of

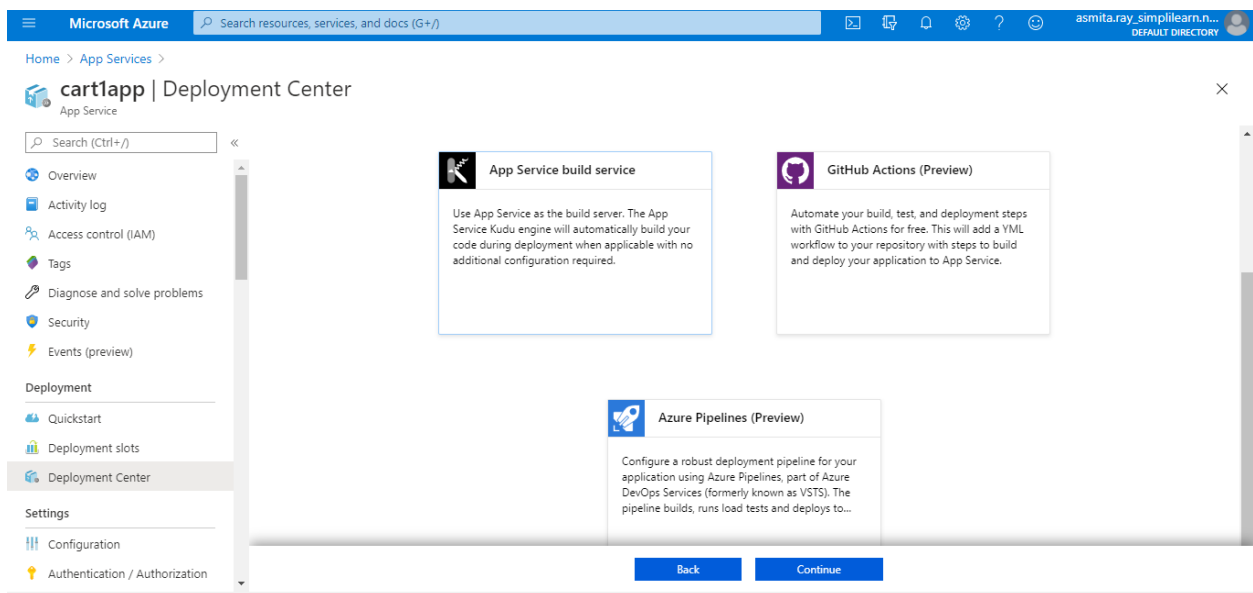
your choice such as Visual Studio Code or GitHub or FTP

Step 5.1: Go to the **Deployment Center**



Step 5.2: Select GitHub

Step 5.3: Authorize your account



Step 5.4: Select the application files uploaded on GitHub and click on **Continue**

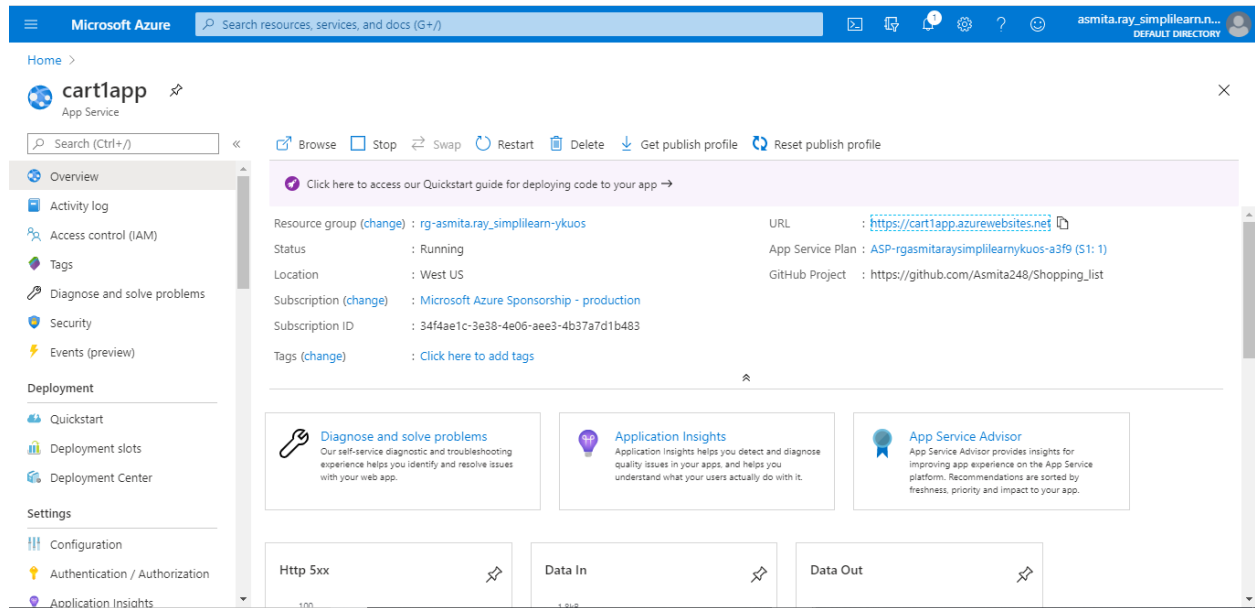
The screenshot shows the Microsoft Azure portal interface for configuring a deployment center. The breadcrumb navigation indicates the path: Home > App Services > Deployment Center. The page title is 'cart1app | Deployment Center'. On the left, there is a sidebar with navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Security, Events (preview), Deployment (with sub-links for Quickstart, Deployment slots, and Deployment Center), and Settings (with sub-links for Configuration and Authentication / Authorization). The main content area shows a progress bar with four steps: SOURCE CONTROL, BUILD PROVIDER, CONFIGURE (active), and SUMMARY. Below the progress bar, there is a 'Code' section with a message: 'If you can't find an organization or repository, you might need to enable additional permissions on GitHub.' Below this message are three dropdown menus: Organization (Asmita248), Repository (Shopping_list), and Branch (master). At the bottom right, there are two buttons: 'Back' and 'Continue'.

Step 5.5: Click on **Finish**

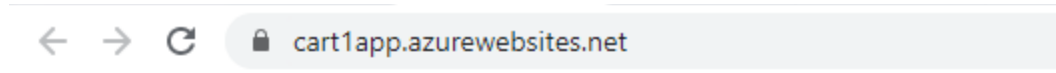
The screenshot shows the Microsoft Azure portal interface for the 'SUMMARY' step of the deployment center configuration. The breadcrumb navigation is the same: Home > App Services > Deployment Center. The page title is 'cart1app | Deployment Center'. The sidebar is identical to the previous screenshot. The progress bar now shows all four steps (SOURCE CONTROL, BUILD PROVIDER, CONFIGURE, and SUMMARY) with green checkmarks, indicating they are all completed. The 'SUMMARY' section displays the configured values: 'SOURCE CONTROL' with Repository 'https://github.com/Asmita248/Shopping_list' and Branch 'master', and 'BUILD PROVIDER' with Provider 'App Service build service'. At the bottom right, there are two buttons: 'Back' and 'Finish'.

Step 6: Hit the web app endpoint to check if the application is online

Step 6.1: Click on Overview of the web app



Step 6.2: Click on the URL and you will get the application running



Shopping List

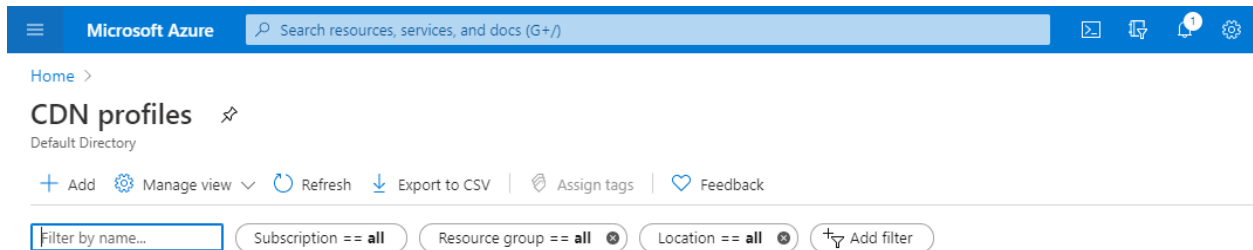
Get it done today

- Notebook ☐ Done
- Jello ☐ Done
- Spinach ☐ Done
- Rice ☐ Done
- Birthday Cake ☐ Done
- Candles ☐ Done

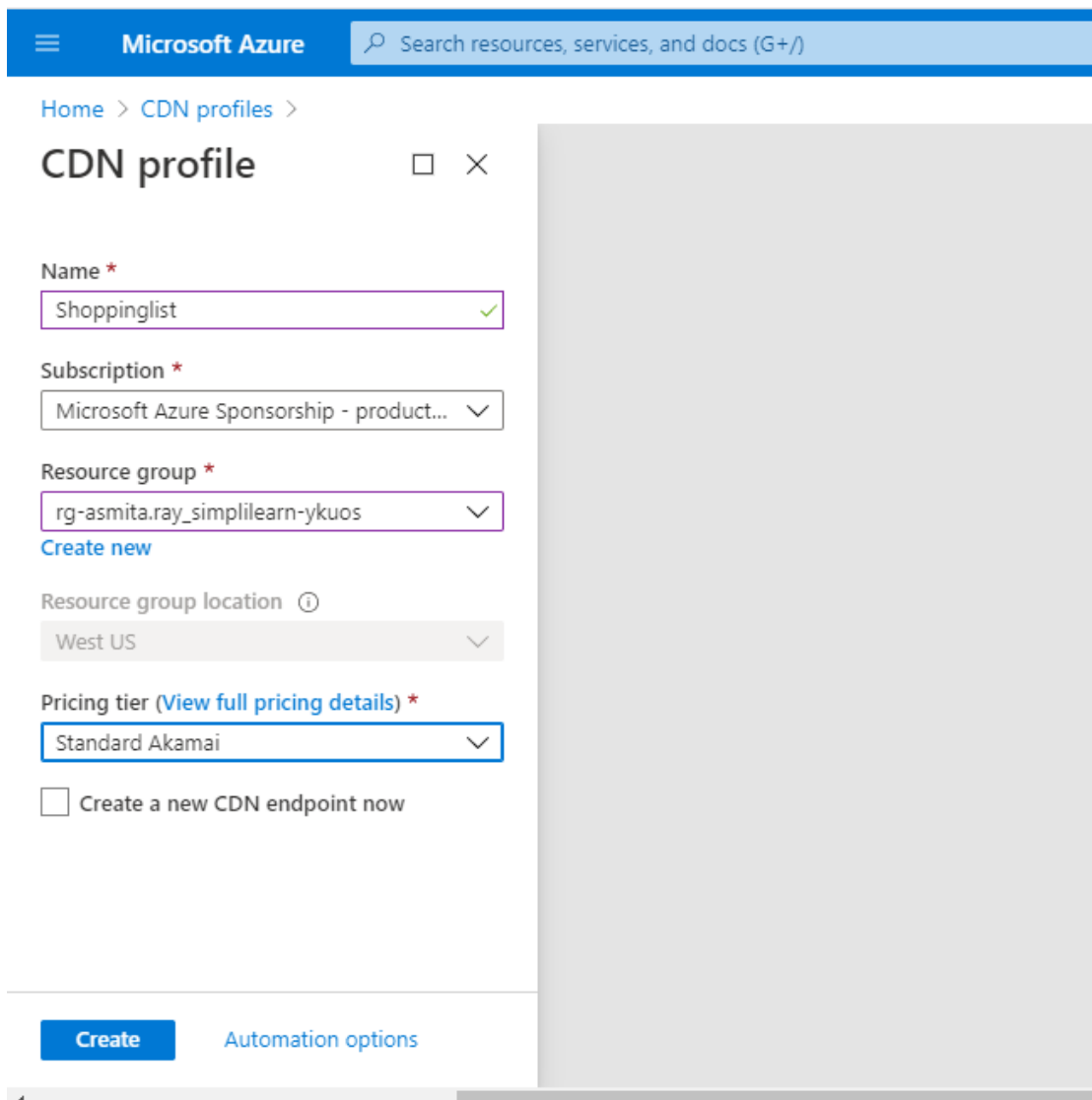
Step 7: Now create a CDN profile

Step 7.1: In the search window, search for CDN profiles

Step 7.2: Click on **Add**



Step 7.3: Provide the information to create the CDN and click on **Create**



Step 8: Use CDN profile to create an endpoint.

Step 8.1: Go to the created CDN

Step 8.2: Click on **Endpoint**

Step 8.3: Provide the basic information about the endpoint and click on **Add**

The screenshot shows the Microsoft Azure portal interface. On the left, the 'CDN profiles' section is visible, with 'Shoppinglist' selected. The main area displays the 'Add an endpoint' dialog. The dialog contains the following fields and options:

- Name:** shop1
- Origin type:** Web App
- Origin hostname:** cart1app.azurewebsites.net
- Origin path:** /Path
- Origin host header:** cart1app.azurewebsites.net
- Protocol:** HTTP (checked), HTTPS (checked)
- Origin port:** 80 (for HTTP), 443 (for HTTPS)
- Optimized for:** General web delivery

The 'Add' button is highlighted at the bottom of the dialog.

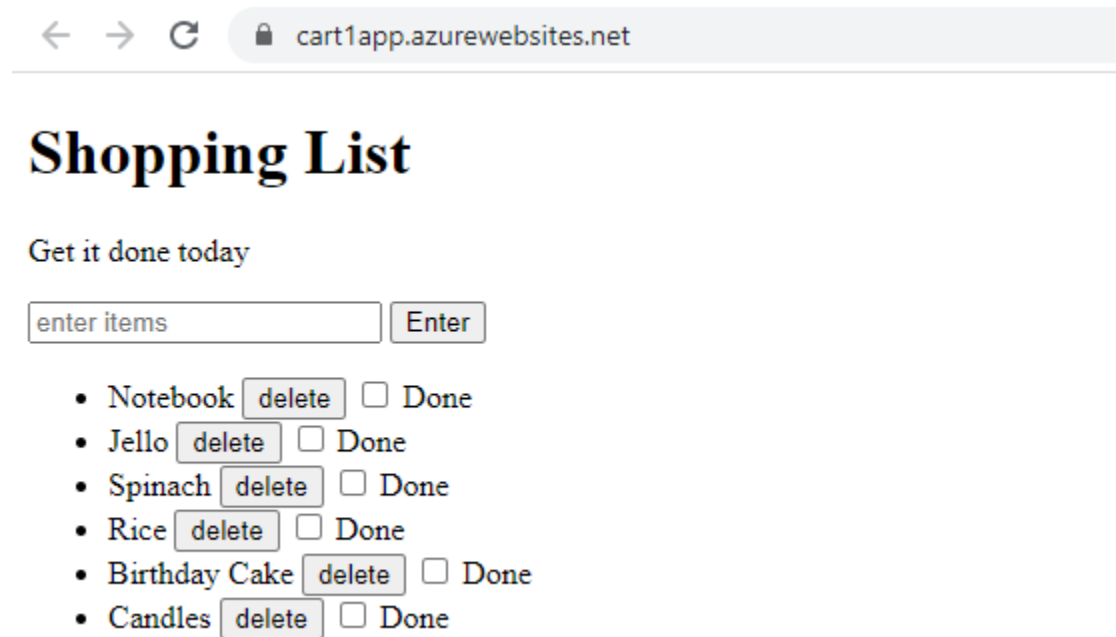
Step 8.4: Go to the created CDN endpoint and click on **Origin hostname**

The screenshot shows the Microsoft Azure portal interface for the 'shop1 (Shoppinglist/shop1)' endpoint. The left sidebar shows the 'Overview' tab selected. The main area displays the endpoint details:

- Resource group (change):** rg-asmita.ray_simplilearn-ykuos
- Status:** Running
- Location:** global
- Subscription (change):** Microsoft Azure Sponsorship - production
- Subscription ID:** 34f4ae1c-3e38-4e06-ae3-4b37a7d1b483
- Endpoint hostname:** https://shop1.azureedge.net
- Origin hostname:** https://cart1app.azurewebsites.net
- Protocols:** HTTP, HTTPS
- Optimization type:** General web delivery

Below the details, there is a section for 'Custom domains' with a table that currently has no entries.

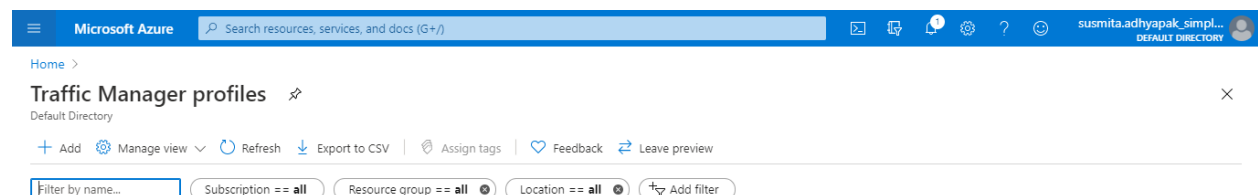
Step 8.5 Your application is running



Step 9: Repeat steps 2 to 7 to create multiple deployments of your application in different regions so that you can meet the global traffic demand.

Step 10: To make sure that traffic coming from different parts of the world is load balanced at DNS level, create a Traffic Manager Profile

Step 10.1: In the search window, search for Traffic Manager Profile and click on **Add** to create a new traffic manager profile

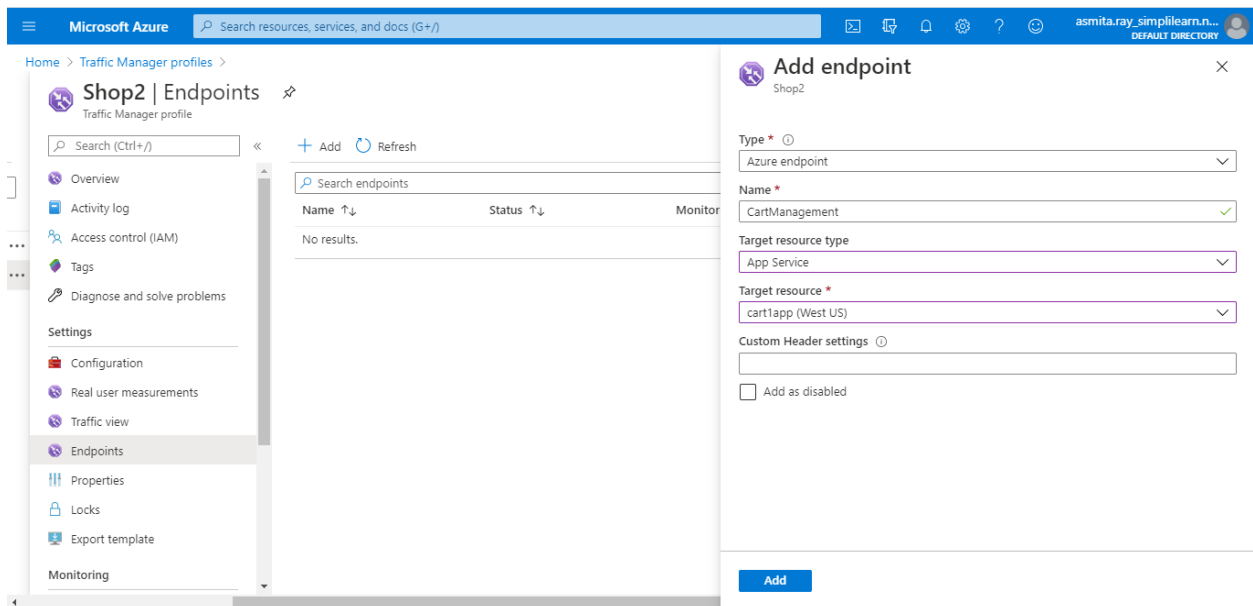


Step 11: Create endpoints in the traffic manager corresponding to each CDN endpoint that you have created

Step 11.1: Go to the created Traffic Manager Profile

Step 11.2: Click on **Endpoints** and click on **Add** to add new endpoints

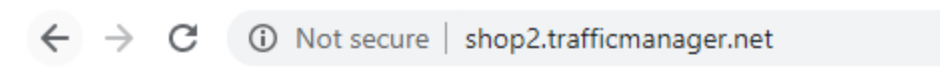
Step 11.3: Provide the required information and click on **Add**



Step 11.4: Once the monitor status is online, copy the link of the DNS name and check whether the application is online

The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar and navigation icons. The main content area displays the 'Shop2' Traffic Manager profile. On the left, a sidebar lists various settings like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Configuration, Real user measurements, Traffic view, Endpoints, Properties, Locks, Export template, and Monitoring. The 'Overview' section is active, showing details such as Resource group (rg-asmita.ray_simplilearn-ykuos), DNS name (http://shop2.trafficmanager.net), Status (Enabled), Subscription (Microsoft Azure Sponsorship - production), Subscription ID (34f4ae1c-3e38-4e06-ae3-4b37a7d1b483), and Tags. Below this, a table lists endpoints with columns for Name, Status, Monitor status, Type, and Location. One endpoint, 'CartManagement', is listed as 'Enabled' with a 'Monitor status' of 'Online' and is an 'Azure endpoint' located in 'West US'.

Your application is running.



Shopping List

Get it done today

- Notebook ☐ Done
- Jello ☐ Done
- Spinach ☐ Done
- Rice ☐ Done
- Birthday Cake ☐ Done
- Candles ☐ Done

Step 12: Optionally, if you want to add the application in your own domain, you can configure the traffic manager to point to a custom domain.

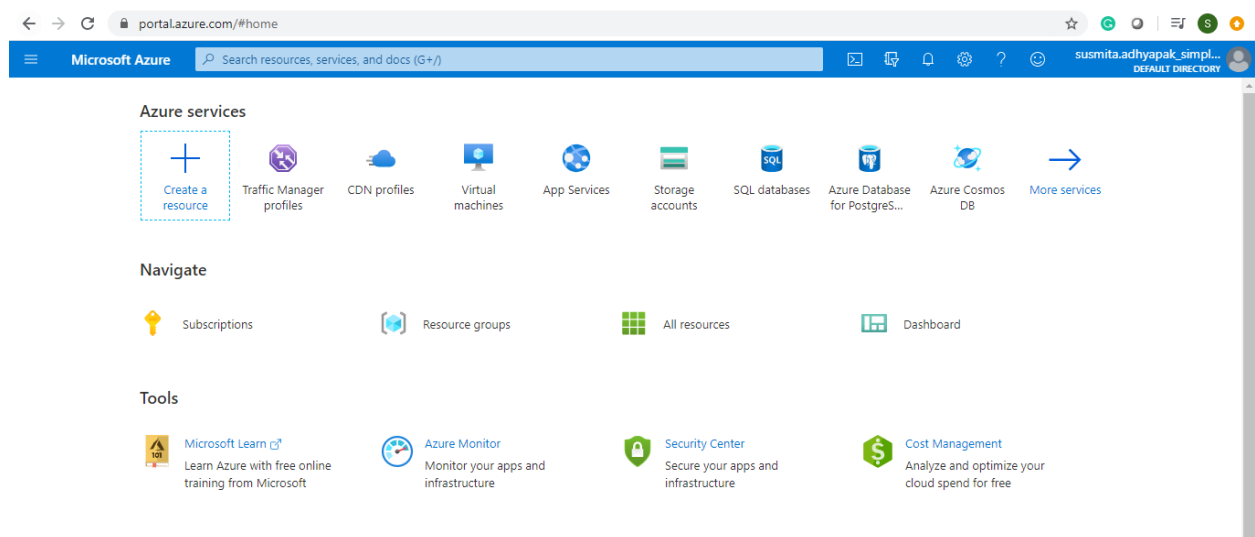
Step 13: As good practice, follow the principle of least privilege so that you only give

access to the services that need to be accessed within the Azure portal.

Azure:

Approach 2:

Step 1: Login to Azure Portal

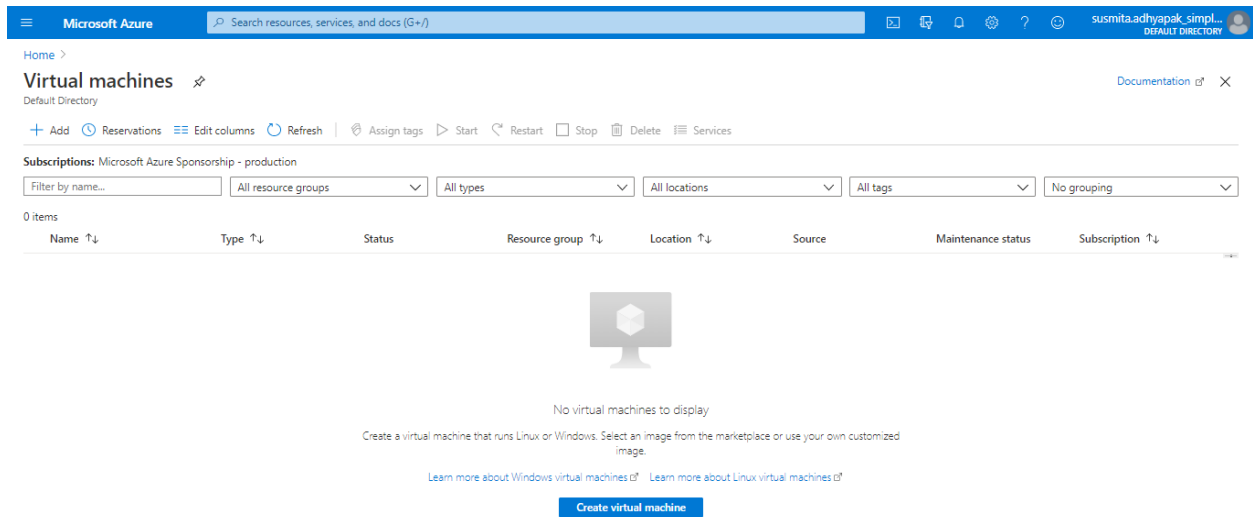


Step 2: Before creating the resources, make sure that you apply tags to resources so

that you can keep a track of billing later on.

Step 3: To begin , create an Azure VM

Step 3.1: Search for Virtual Machines and click on **Add**



Step 3.2: Provide basic information about VM

Microsoft Azure

Search resources, services, and docs (G+)

[Home](#) > [Virtual machines](#) >

Create a virtual machine

[Basics](#)
[Disks](#)
[Networking](#)
[Management](#)
[Advanced](#)
[Tags](#)
[Review + create](#)

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Microsoft Azure Sponsorship - production

Resource group *

rg-susmita.adhyapak_simplilearn-gye3v

[Create new](#)

Instance details

Virtual machine name *

SimpliVM

Region *

(US) West US

Availability options

No infrastructure redundancy required

Image *

Windows Server 2016 Datacenter

Review + create

< Previous

Next : Disks >

Microsoft Azure

Search resources, services, and docs (G+)

[Home](#) > [Virtual machines](#) >

Create a virtual machine

[Basics](#)
[Disks](#)
[Networking](#)
[Management](#)
[Advanced](#)
[Tags](#)
[Review + create](#)

Azure Spot instance

☐ Yes
 ☒ No

Size *

Standard_B2s - 2 vcpus, 4 GiB memory (₹2,779.22/month)

[Select size](#)

Administrator account

Username *

AzureUser

Password *

Confirm password *

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports *

☐ None
 ☒ Allow selected ports

Select inbound ports *

HTTP (80), HTTPS (443), RDP (3389)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Review + create

< Previous

Next : Disks >

Step 3.3: In the Disks section, provide the required information

Microsoft Azure

Search resources, services, and docs (G+)

Home > Virtual machines >

Create a virtual machine

Basics

Disks

Networking

Management

Advanced

Tags

Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

OS disk type *

Standard HDD

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Encryption type *

(Default) Encryption at-rest with a platform-managed key

Enable Ultra Disk compatibility

☐ Yes
 ☒ No

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching
Create and attach a new disk Attach an existing disk				

Review + create

< Previous

Next : Networking >

Step 3.4: In the Management section, turn off the Boot diagnostics

Microsoft Azure

Search resources, services, and docs (G+/)

[Home](#) > [Virtual machines](#) >

Create a virtual machine

[Basics](#)
[Disks](#)
[Networking](#)
[Management](#)
[Advanced](#)
[Tags](#)
[Review + create](#)

Configure monitoring and management options for your VM.

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.
[Learn more](#)

✔ Your subscription is protected by Azure Security Center basic plan.

Monitoring

Boot diagnostics ⓘ ☐ On ☒ Off

OS guest diagnostics ⓘ ☐ On ☒ Off

Identity

System assigned managed identity ⓘ ☐ On ☒ Off

Azure Active Directory

Login with AAD credentials (Preview) ⓘ ☐ On ☒ Off

Review + create

< Previous

Next : Advanced >

Step 3.4: Click on **Review and Create**

Microsoft Azure

Search resources, services, and docs (G+)

Home > Virtual machines >

Create a virtual machine

Basics

Disks

Networking

Management

Advanced

Tags

Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name	Value	Resource
<input type="text"/>	:	<input type="text"/> 11 selected

Review + create

< Previous

Next : Review + create >

Step 3.5: Click on **Create**

Microsoft Azure

Search resources, services, and docs (G+)

Home > Virtual machines >

Create a virtual machine

Validation passed

Basics

Disks

Networking

Management

Advanced

Tags

Review + create

PRODUCT DETAILS

Standard B2s

by Microsoft

[Terms of use](#) | [Privacy policy](#)

Subscription credits apply

3.8071 INR/hr

[Pricing for other VM sizes](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

You have set RDP port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Create

< Previous

Next >

Download a template for automation

Step 3.6: Your VM will get deployed

Microsoft Azure

Search resources, services, and docs (G+)

Home >

CreateVm-MicrosoftWindowsServer.WindowsServer-201-20200612123115 | Overview

Deployment

Search (Ctrl+)

Delete

Cancel

Redeploy

Refresh

Overview

Inputs

Outputs

Template

We'd love your feedback! →

✓

Your deployment is complete

Deployment name: CreateVm-MicrosoftWindowsServer.WindowsS...

Subscription: [Microsoft Azure Sponsorship - production](#)

Resource group: [rg-susmita.adhyapak_simplilearn-gye3v](#)

Start time: 6/12/2020, 12:35:14 PM

Correlation ID: da58f25d-3d73-4073-be26-838ca01f152b

Deployment details

(Download)

Next steps

Setup auto-shutdown

Recommended

Monitor VM health, performance and network dependencies

Recommended

Run a script inside the virtual machine

Recommended

Go to resource

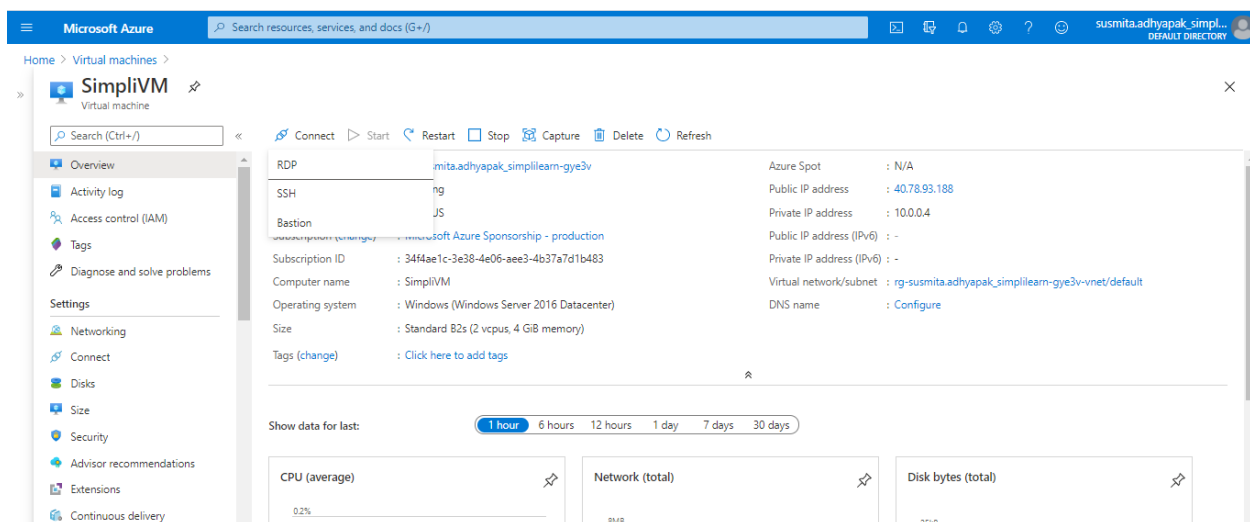
Create another VM

Step 4: Make sure you have inbound traffic on port 80 and port 443 open.

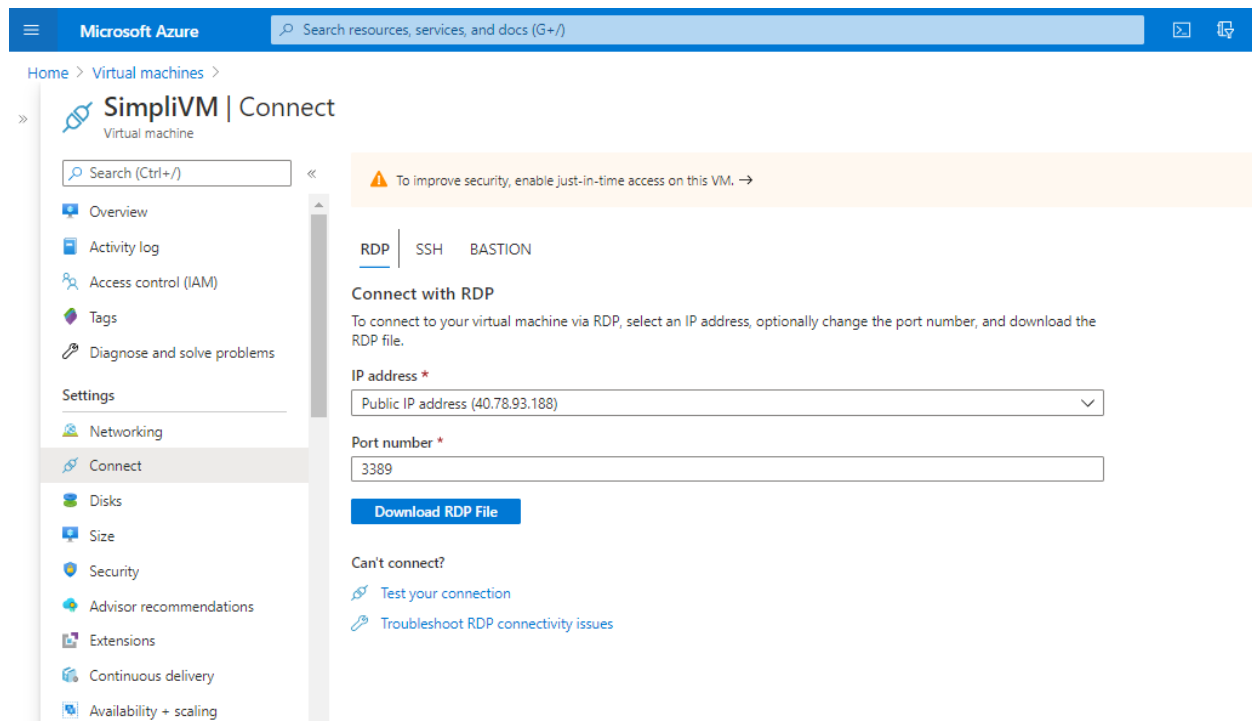
Step 5: Make sure port 445 is opened on your VMs so that teammates can use common file share to access and share files if needed.

Step 6: Login to Azure VM and spin up a web server of your choice on port 80

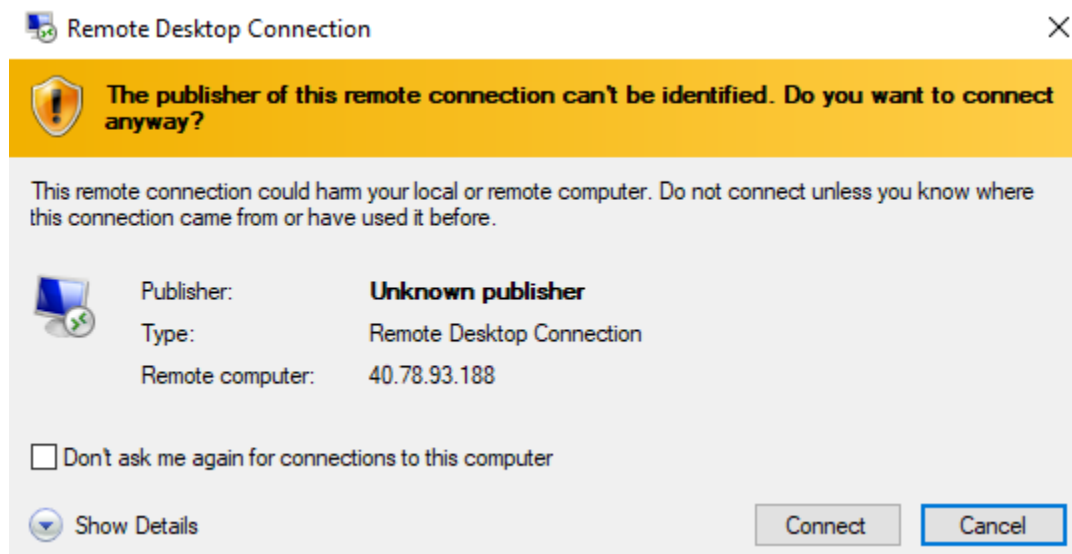
Step 6.1: Click on Connect and select RDP



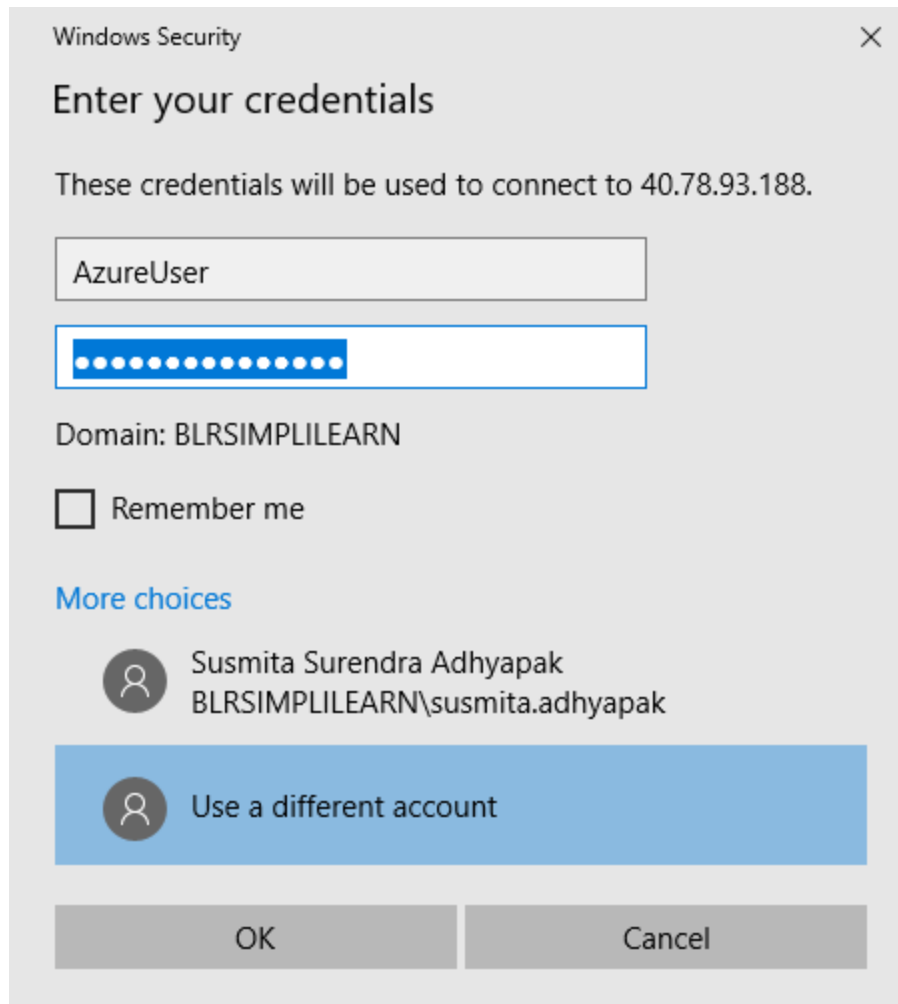
Step 6.2: Click on **Download RDP file**. It will download the created VM in your system.



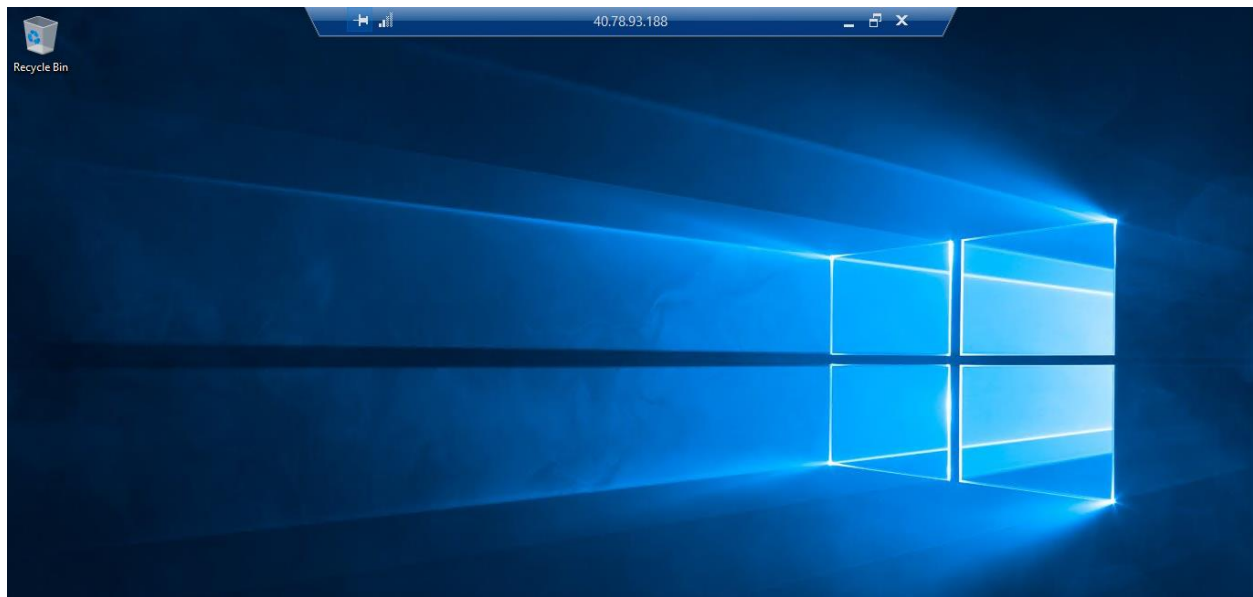
Step 6.3: Open the downloaded VM. Click on **Connect**



Step 6.4: Enter the credentials to login into VM and click on **OK**

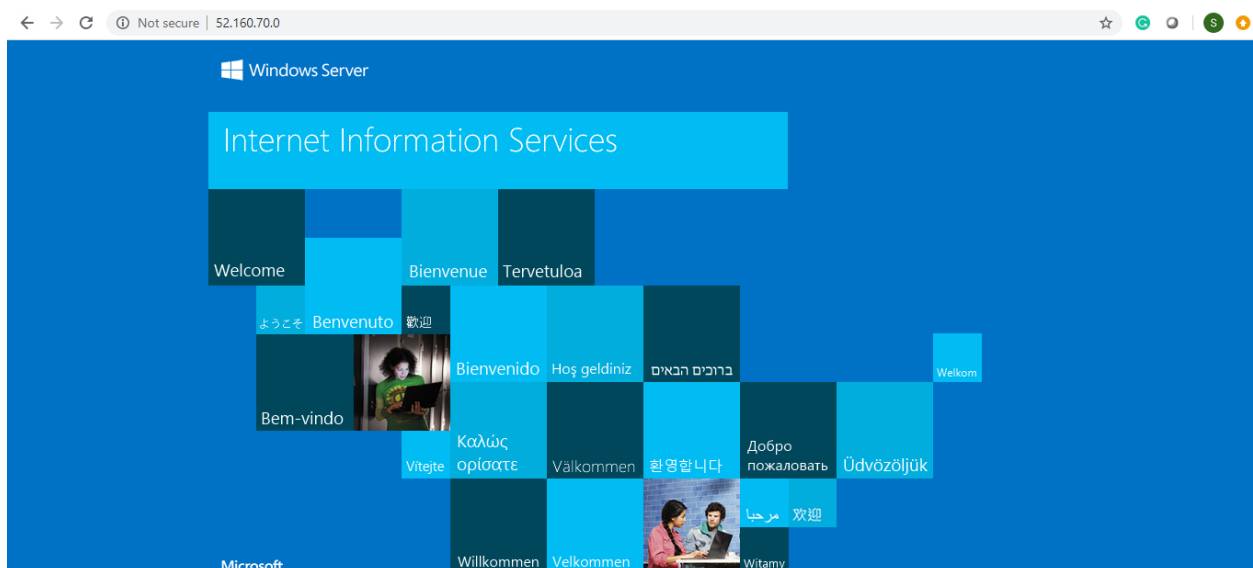


Step 6.5: This will open the VM in your system



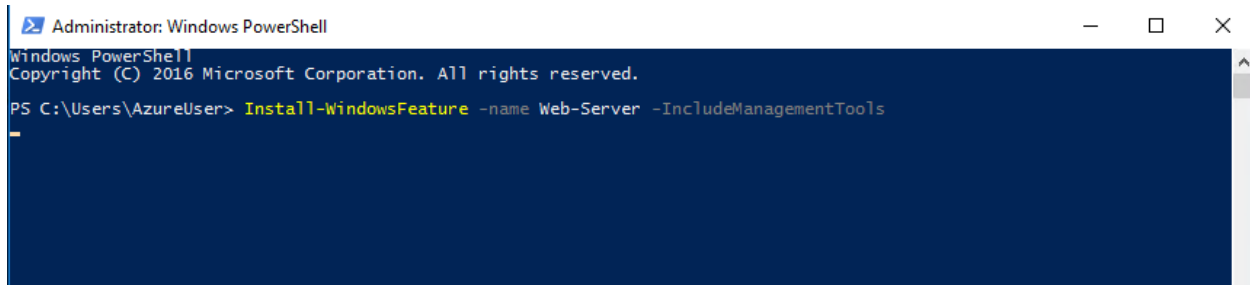
Step 7: Deploy your application on the web server that you have created within the virtual machine

Step 7.1: In the portal, select the VM and in the overview of the VM, use the Click to copy button to the right of the IP address to copy it and paste it into a browser tab. The default IIS welcome page will open, and should look like this:

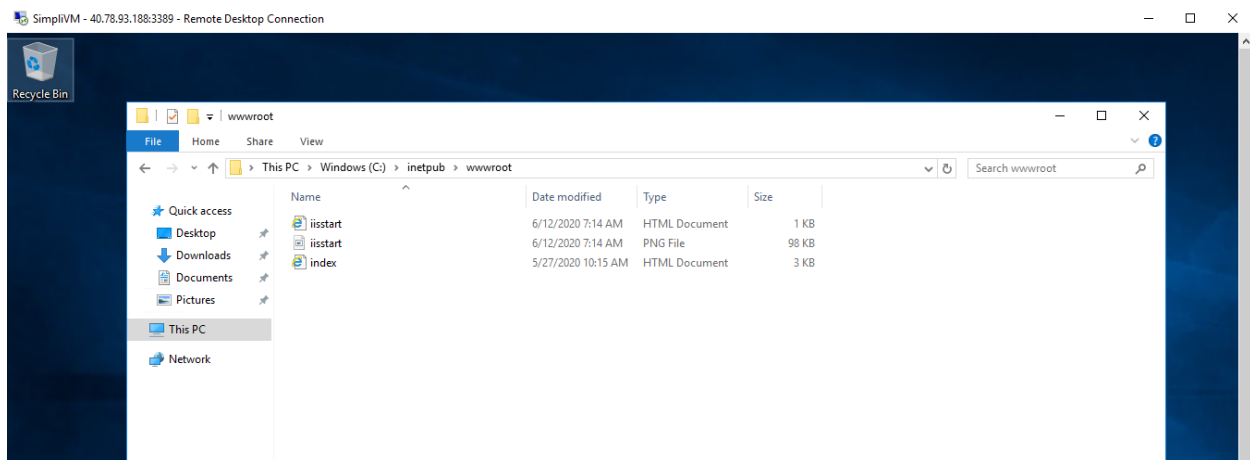


Step 7.2: Open powershell and type the following command

Install-WindowsFeature -name Web-Server -IncludeManagementTools



Step 7.3: The above command will create an inetpub folder in your C drive. Go to C:\inetpub\wwwroot and copy-paste the index.html file of your application which you want to deploy here



Step 7.4: Copy and paste the public IP address of the created VM in the browser and you will get the output

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the 'Microsoft Azure' logo, a search bar, and user information for 'susmita.adhyapak_simpli...'. The main content area displays the details of a virtual machine named 'SimpliVM'. On the left, there is a sidebar with navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, Connect, Disks, Size, Security, Advisor recommendations, and Extensions. The 'Overview' tab is selected, showing various properties of the VM. Below the properties, there is a section for 'Show data for last:' with a dropdown menu set to '1 hour'. Three charts are displayed: 'CPU (average)', 'Network (total)', and 'Disk bytes (total)', each with a star icon for favoriting.

Property	Value
Resource group	rg-susmita.adhyapak_simplilearn-gye3v
Status	Running
Location	West US
Subscription	Microsoft Azure Sponsorship - production
Subscription ID	34f4ae1c-3e38-4e06-ae03-4b37a7d1b483
Computer name	SimpliVM
Operating system	Windows (Windows Server 2016 Datacenter)
Size	Standard B2s (2 vcpus, 4 GiB memory)
Tags	Click here to add tags
Azure Spot	N/A
Public IP address	40.78.93.188
Private IP address	10.0.0.4
Public IP address (IPv6)	-
Private IP address (IPv6)	-
Virtual network/subnet	rg-susmita.adhyapak_simplilearn-gye3v-vnet/default
DNS name	Configure

Shopping List

Get it done today

- Notebook ☐ Done
- Jello ☐ Done
- Spinach ☐ Done
- Rice ☐ Done
- Birthday Cake ☐ Done
- Candles ☐ Done

Step 8: Repeat steps 2 to 6 to create multiple deployments of your application in different regions so that you can meet the global traffic demand.

Step 9: To make sure that traffic coming from different parts of the world is load balanced at DNS level, create a Traffic Manager Profile

Step 9.1: Click on the Public IP address of the created VM

Step 9.2: Enter the DNS name and click on Save

The screenshot shows the 'SimpliVM-ip | Configuration' page in the Microsoft Azure portal. The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Settings (selected), Configuration (selected), Properties, Locks, Export template, Monitoring, Diagnostic settings, Logs, and Support + troubleshooting. The main content area shows the configuration for the Public IP address. The 'Assignment' section has 'Dynamic' selected. The 'IP address' is 40.78.93.188. The 'Idle timeout (minutes)' is set to 4. The 'DNS name label (optional)' is 'onlinemovie'. Below this, there is a note about alias record sets and a link to create an alias record. At the bottom, there is a table with columns: Subscription, DNS zone, Name, Type, and TTL. The table currently shows 'No results'.

Step 9.3: In the search window, search for Traffic Manager Profile. Click on **Add** to create a new traffic manager profile

The screenshot shows the 'Traffic Manager profiles' page in the Microsoft Azure portal. The left sidebar contains navigation options: Home, Traffic Manager profiles (selected), Add, Manage view, Refresh, Export to CSV, Assign tags, Feedback, and Leave preview. The main content area shows a search bar and filter buttons. The search bar contains 'Filter by name...'. The filter buttons are: Subscription == all, Resource group == all, Location == all, and Add filter.

Step 10.2: Provide the required information and click on **Create** to create the Traffic Manager Profile

Microsoft Azure Search resources, services, and docs (G+)

Home > Traffic Manager profiles >

Create Traffic Manager profile

Name *
onlineMovieTrafficManager ✓
.trafficmanager.net

Routing method
Performance

Subscription *
Microsoft Azure Sponsorship - product...

Resource group *
rg-susmita.adhyapak_simplilearn-gye3v
[Create new](#)

Resource group location ⓘ
West US

[Create](#) [Automation options](#)

Step 10: Create endpoints in the traffic manager corresponding to public IP of each virtual machine that you have created.

Step 10.1: Go to the created Traffic Manager Profile

Microsoft Azure Search resources, services, and docs (G+)

Home > Traffic Manager profiles >

onlineMovieTrafficManager

Traffic Manager profile

Search (Ctrl+/)

Enable profile Disable profile Refresh Move Delete profile

Resource group (change) : rg-susmita.adhyapak_simplilearn-gye3v DNS name : http://onlinemovietrafficmanager.trafficmanager.net

Status : Enabled Monitor status : Inactive

Subscription (change) : Microsoft Azure Sponsorship - production

Subscription ID : 34f4ae1c-3e38-4e06-ae3-4b37a7d1b483

Tags (change) : [Click here to add tags](#)

Routing method : Performance

Search endpoints

Name	Status	Monitor status	Type	Location
No results.				

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings
Configuration
Real user measurements
Traffic view
Endpoints
Properties
Locks
Export template

Step 10.2: Click on **Endpoints**. Click on **Add** to add new endpoints

Microsoft Azure | Search resources, services, and docs (G+/I)

Home > Traffic Manager profiles > onlineMovieTrafficManager | Endpoints

Search (Ctrl+/) « + Add Refresh

Search endpoints

Name ↑↓	Status ↑↓	Monitor status ↑↓	Type ↑↓	Location ↑↓
No results.				

Step 10.3: Provide the required information and click on **Add**

Microsoft Azure | Search resources, services, and docs (G+/I)

Home > Traffic Manager profiles > onlineMovieTrafficManager | Endpoints

Search (Ctrl+/) « + Add Refresh

Search endpoints

Name ↑↓	Status ↑↓	Monitor status ↑↓
No results.		

Add endpoint
onlineMovieTrafficManager

Type * Azure endpoint

Name * onlineMovieEndpoint

Target resource type Public IP address

Public IP address * SimpliVM-ip (40.78.93.188)

Custom Header settings

☐ Add as disabled

Step 10.4: Copy-paste the DNS name link in the web browser and you'll get the output

The screenshot shows the Azure portal interface for a Traffic Manager profile named 'onlineMovieTrafficManager'. The profile is in an 'Enabled' state. Key details include:

- Resource group:** rg-susmita.adhyapak_simplilearn-gye3v
- Status:** Enabled
- Subscription:** Microsoft Azure Sponsorship - production
- Subscription ID:** 34f4ae1c-3e38-4e06-ae3-4b37a7d1b483
- DNS name:** http://onlinemovietrafficmanager.trafficmanager.net
- Monitor status:** Unknown
- Routing method:** Performance

Under the 'Endpoints' section, there is a table with the following data:

Name	Status	Monitor status	Type	Location
onlineMovieEndpoint	Enabled	Checking endpoint	Azure endpoint	West US

Shopping List

Get it done today

- Notebook ☐ Done
- Jello ☐ Done
- Spinach ☐ Done
- Rice ☐ Done
- Birthday Cake ☐ Done
- Candles ☐ Done

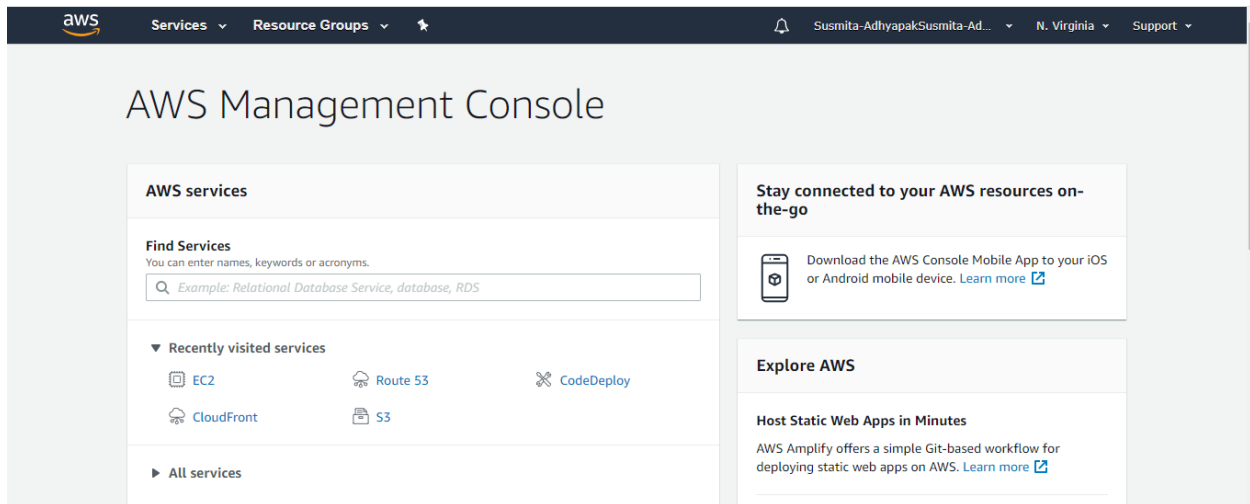
Step 11: Optionally, if you want to add in your own domain, you can configure the traffic manager to point to a custom domain.

Step 12: As good practice, follow the principle of least privilege so that you only give access to the services that need to be accessed within the Azure portal.

AWS:

Approach 1:

Step 1: Log into the AWS console.

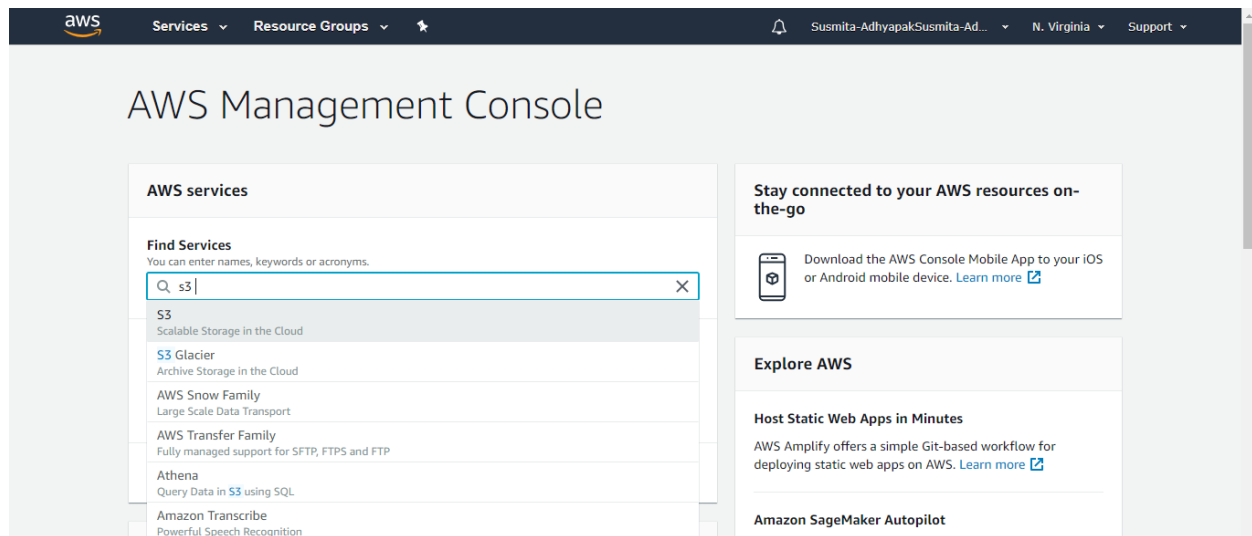


Step 2: Before creating the resources, make sure you apply cost allocation tags to resources so that you can keep a track of billing later on.

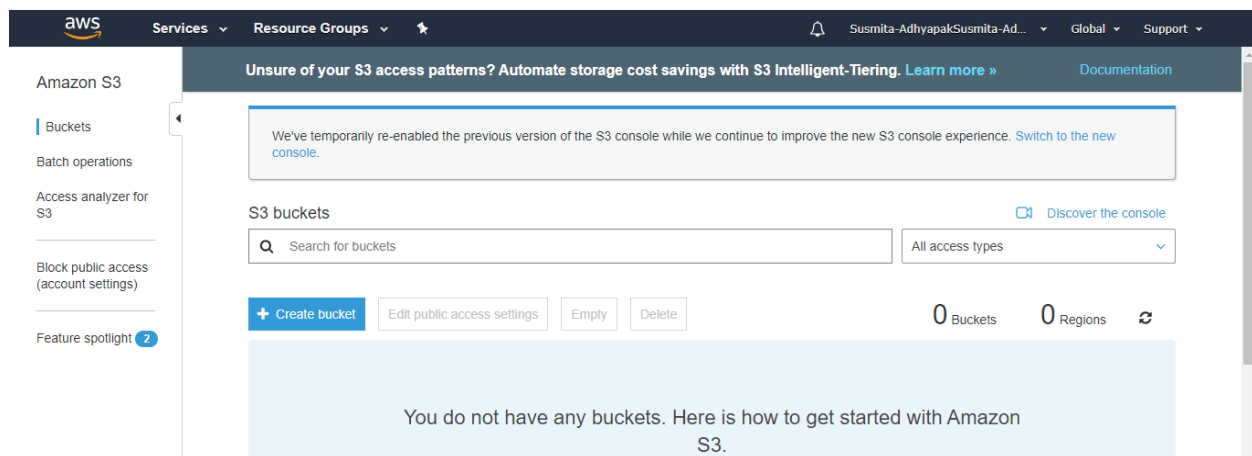
Step 3: To begin with, create Route 53 and add a hosted zone if you have your own domain. This is an optional step to configure a custom domain for your web app.

Step 4: Create an S3 bucket.

Step 4.1: In the search window, search for S3 service



Step 4.2: Click on **Create bucket**



Step 4.3: Provide the bucket name, select the region, and click on **Next**

Create bucket

1 Name and region 2 Configure options 3 Set permissions 4 Review

Name and region

Bucket name ⓘ

cloudcapstone123

Region

US East (N. Virginia) ▾

Copy settings from an existing bucket

You have no buckets0 Buckets ▾

Create Cancel Next

Step 4.4: In the Set permissions section, uncheck the box of Block all public access and acknowledge the terms and click on **Next**

Create bucket

1 Name and region 2 Configure options 3 Set permissions 4 Review

⚠ Disabling Block all public access may result in this bucket and the objects within becoming public
 AWS recommends that you block all public access to your bucket, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings may result in this bucket and the objects within becoming public

Block all public access
 Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**
 S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**
 S3 will ignore all ACLs that grant public access to buckets and objects.
- ☐ **Block public access to buckets and objects granted through new public bucket or access point policies**

Previous Next

Step 4.5: Click on **Create bucket**

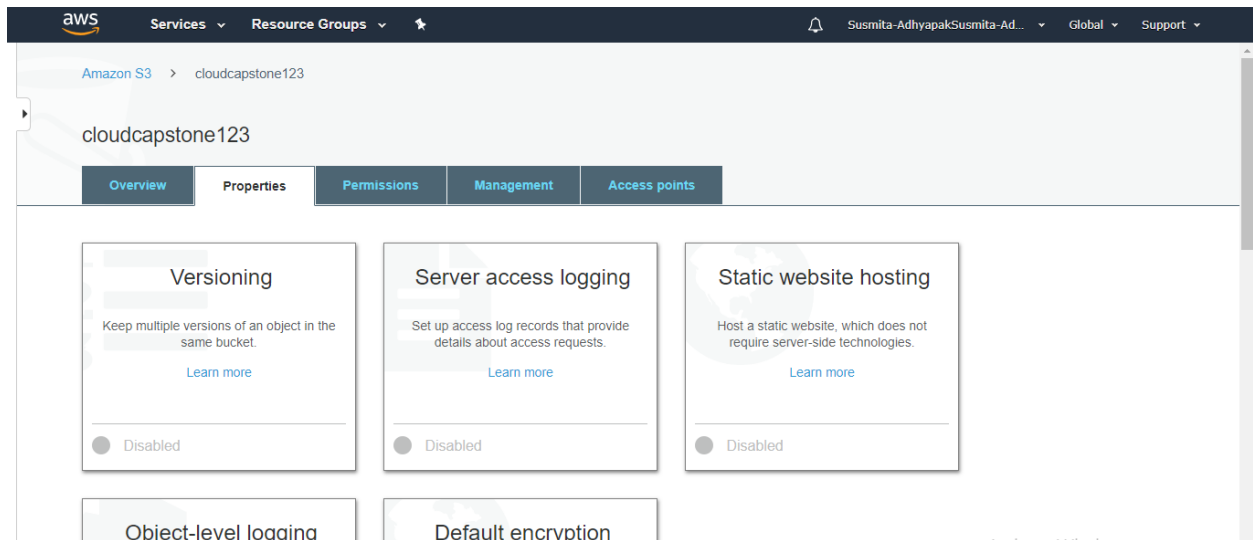
Step 4.6: The created bucket will be visible in the portal

<input type="checkbox"/>	Bucket name	Access	Region	Date created
<input type="checkbox"/>	cloudcapstone123	Objects can be public	US East (N. Virginia)	Jun 15, 2020 12:47:33 PM GMT+0530

Step 5: In the properties of S3 bucket, configure the S3 bucket to enable Static website hosting.

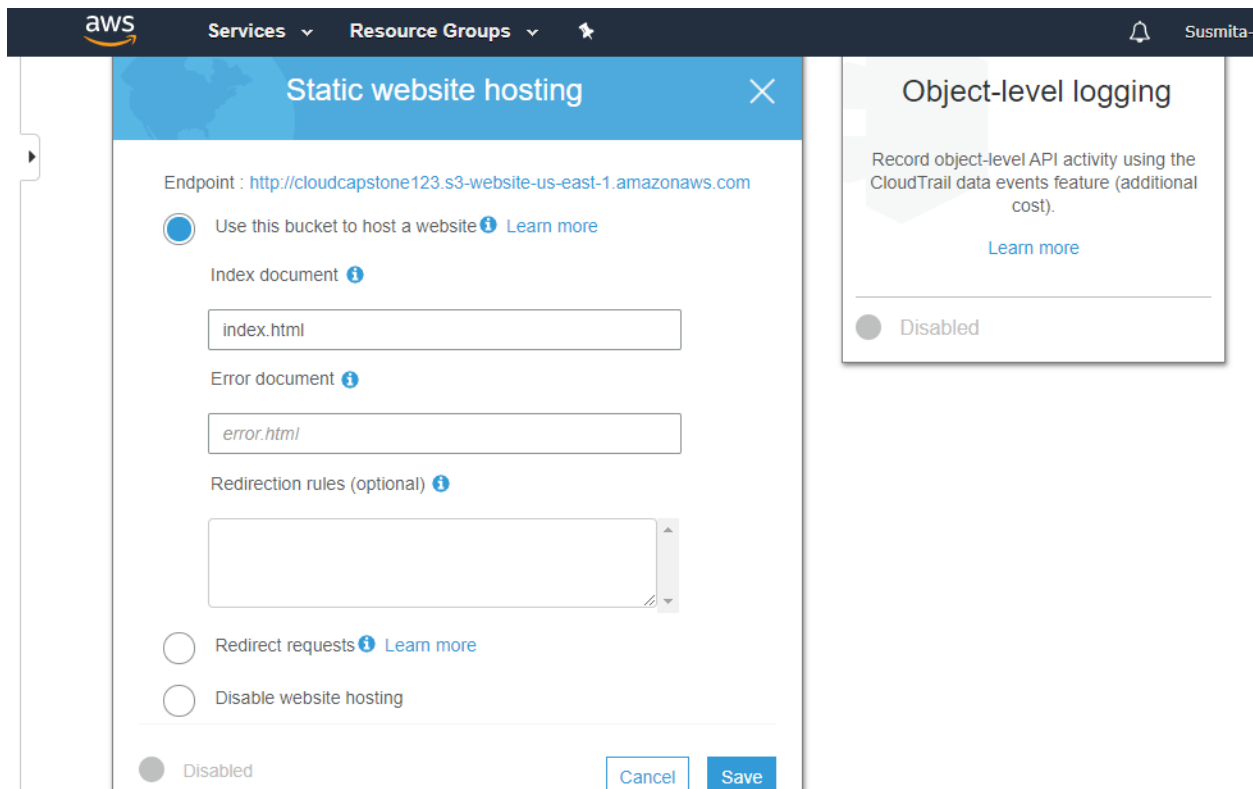
Step 5.1: Click on the created bucket

Step 5.2: Go to **Properties**



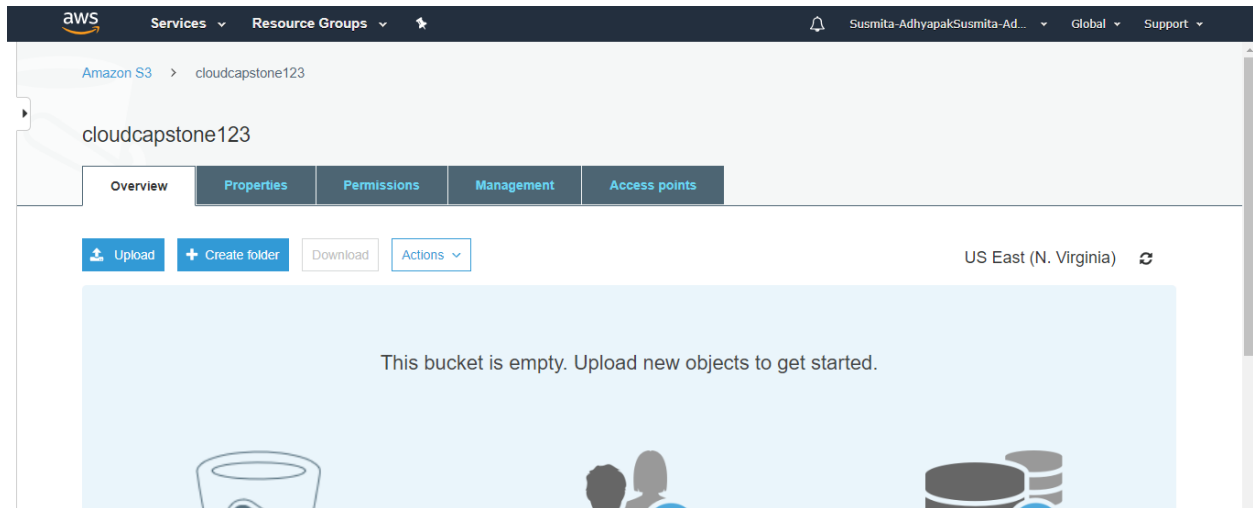
Step 5.3: Select Static web hosting

Step 5.4: Select **Use this bucket to host a website**, provide the required information and click on **Save**

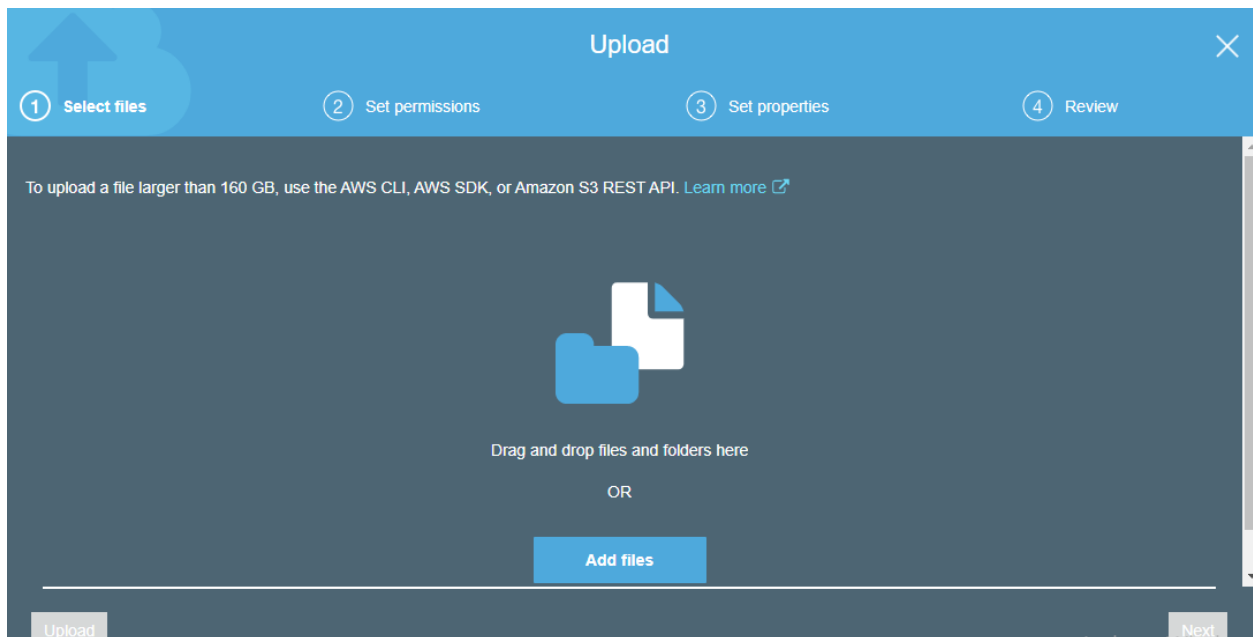


Step 6: Upload your static content (web app files) to the S3 bucket.

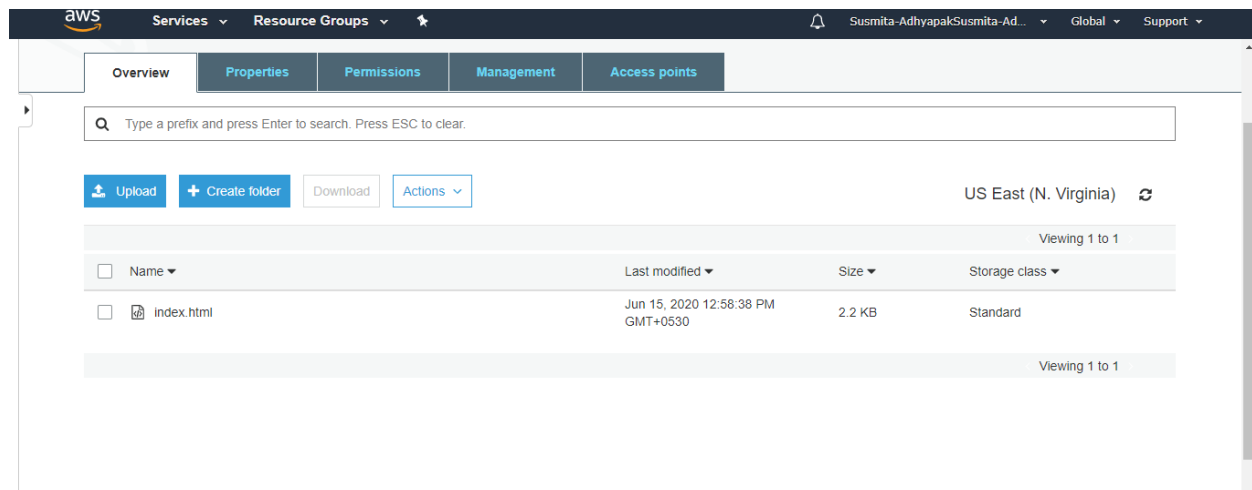
Step 6.1: Go to Overview tab of the created bucket and click on **Upload**



Step 6.2: Select the files of your application which you want to deploy and click on **Next** and click on **Upload**



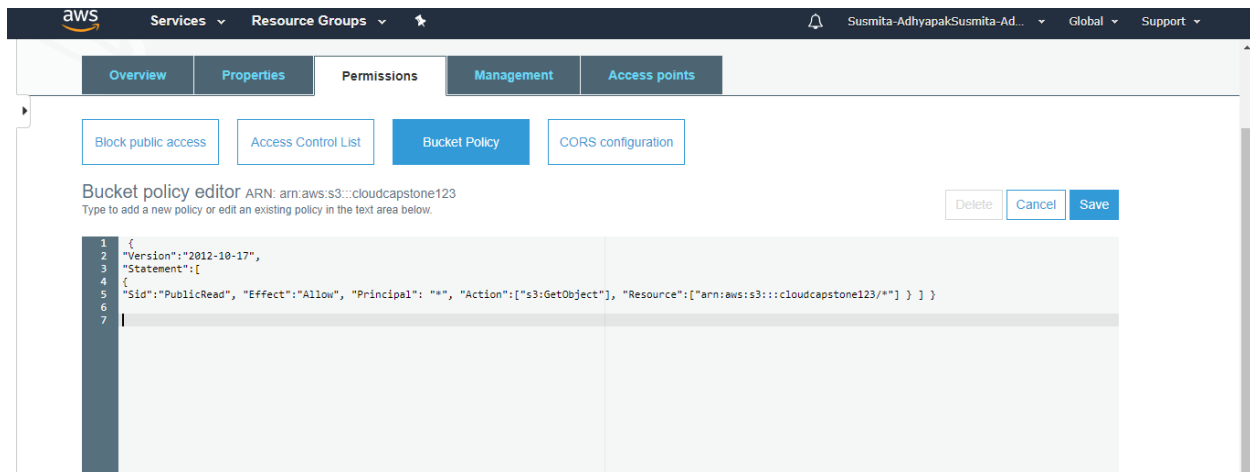
Step 6.3: This will add the files of your application in the S3 bucket



Step 7: Configure permissions in S3 and add below bucket policy to give read only access to the static web app endpoint.

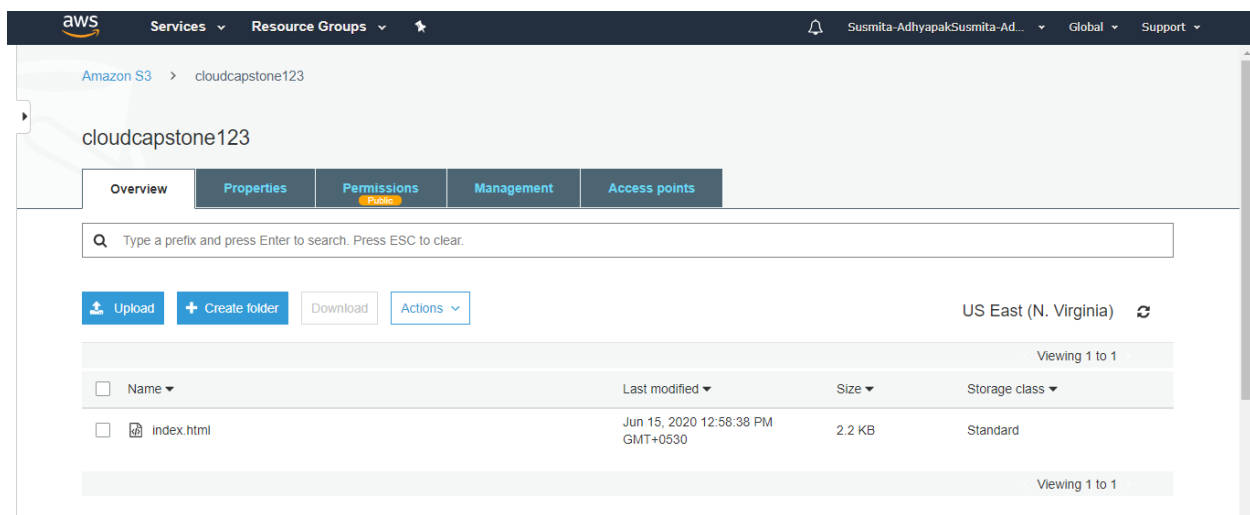
Step 7.1: Go to the **Permissions**, click on **Bucket policy**, add the following code there and click on **Save**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicRead", "Effect": "Allow", "Principal": "*",
      "Action": ["s3:GetObject"],
      "Resource": ["arn:aws:s3:::cloudcapstone123/*"] } ] }
```

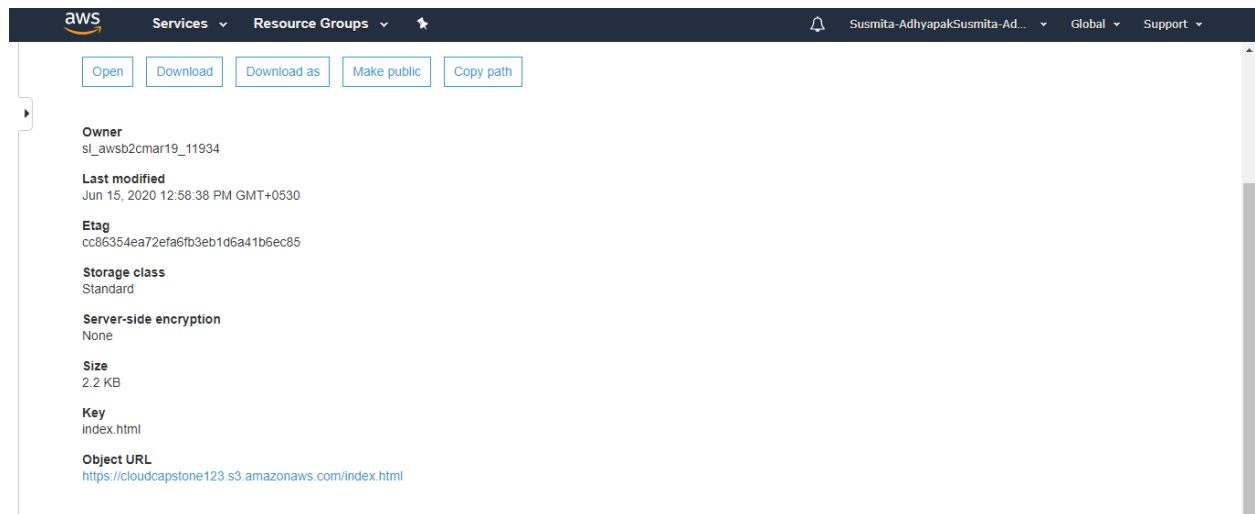



Step 8: Hit the web app endpoint to check if the application is online.

Step 8.1: Click on the Overview tab of the created bucket and click on the uploaded file



Step 8.2: Click on the **Object URL**



Step 8.3: Your application will start running

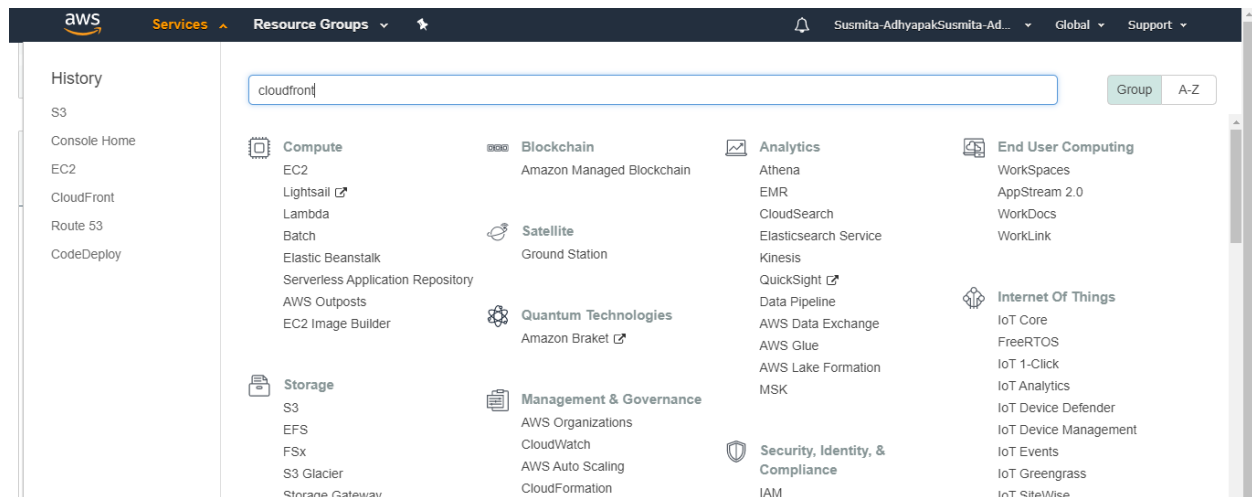
Shopping List

Get it done today

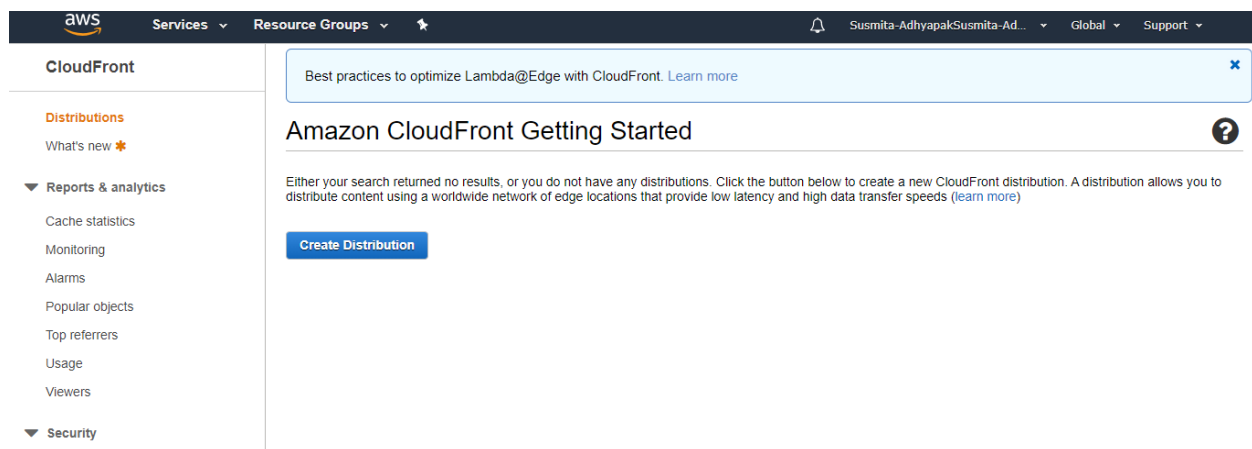
- Notebook ☐ Done
- Jello ☐ Done
- Spinach ☐ Done
- Rice ☐ Done
- Birthday Cake ☐ Done
- Candles ☐ Done

Step 9: Now create a CloudFront distribution corresponding to the static web app endpoint.

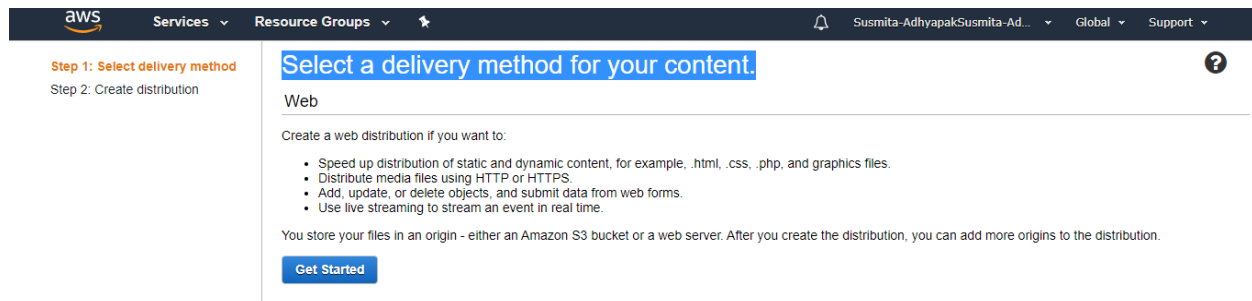
Step 9.1: Go to services and search for CloudFront



Step 9.2: Click on **Create Distribution**



Step 9.3: Select a delivery method for your content as Web and click on Get Started



Step 9.4: Provide the Origin Domain Name and Origin ID

The screenshot shows the 'Create Distribution' page in the AWS console, specifically the 'Origin Settings' section. The page has a dark header with the AWS logo and navigation links. On the left, there are two steps: 'Step 1: Select delivery method' and 'Step 2: Create distribution'. The main content area is titled 'Create Distribution' and 'Origin Settings'. It contains several form fields: 'Origin Domain Name' (cloudcapstone123.s3.amazonaws.com), 'Origin Path' (Amazon S3 Buckets - cloudcapstone123.s3.amazonaws.com), 'Origin ID' (S3-cloudcapstone123), 'Restrict Bucket Access' (radio buttons for Yes and No, with No selected), 'Origin Connection Attempts' (3), 'Origin Connection Timeout' (10), and 'Origin Custom Headers' (a table with 'Header Name' and 'Value' columns). Below these is the 'Default Cache Behavior Settings' section.

Step 9.5: Keep all the values as default and click on **Create Distribution**

The screenshot shows the 'Create Distribution' page in the AWS console, specifically the 'Default Cache Behavior Settings' section. The page has a dark header with the AWS logo and navigation links. On the left, there are two steps: 'Step 1: Select delivery method' and 'Step 2: Create distribution'. The main content area is titled 'Create Distribution' and 'Default Cache Behavior Settings'. It contains several form fields: 'Supported HTTP Versions' (radio buttons for HTTP/2, HTTP/1.1, HTTP/1.0, with HTTP/2 selected), 'Default Root Object' (empty), 'Logging' (radio buttons for On and Off, with Off selected), 'Bucket for Logs' (empty), 'Log Prefix' (empty), 'Cookie Logging' (radio buttons for On and Off, with Off selected), 'Enable IPv6' (checkbox checked), 'Comment' (empty), and 'Distribution State' (radio buttons for Enabled and Disabled, with Enabled selected). At the bottom right, there are three buttons: 'Cancel', 'Back', and 'Create Distribution'.

Step 9.6: These steps will create your CloudFront distribution

The screenshot shows the AWS CloudFront console. At the top, there's a navigation bar with the AWS logo, 'Services', 'Resource Groups', and a user profile. A notification banner at the top says 'Enable new real-time metrics for better visibility of your traffic. Learn more'. The left sidebar shows 'CloudFront' as the selected service, with sub-sections like 'Distributions', 'What's new', 'Reports & analytics', 'Cache statistics', 'Monitoring', 'Alarms', 'Popular objects', 'Top referrers', 'Usage', and 'Viewers'. The main content area is titled 'CloudFront Distributions'. It includes buttons for 'Create Distribution', 'Distribution Settings', 'Delete', 'Enable', and 'Disable'. Below these are filters for 'Viewing: Any Delivery Method' and 'Any State'. A table lists the distributions:

	Delivery Method	ID	Domain Name	Comment	Origin	CNAMEs	Status	State	Last Modified
<input type="checkbox"/>	Web	E28IVNJY4FZDCR	d3r6xle28zocdi.cl	-	cloudcaps	-	In Prog	Enabled	2020-06-15 13:1

At the bottom right of the table, it says 'Viewing 1 to 1 of 1 Items'.

Step 10: Configure the CloudFront distribution to point to your domain by editing the configuration and adding the domain name in Alternate Domain Name field.

Step 10.1: Once the CloudFront service get deployed, create a new file of .html extension in your system and copy the following content in it

```
<html>

  <head>My CloudFront Test</head>

  <body>

    <p>My text content goes here.</p>

    <p><img src=https://d1111111abcdef8.cloudfront.net/.html
alt="my test image"/>

  </body>

</html>
```

Step 10.2: Upload the same file in the created S3 bucket

Amazon S3 > cloudcapstone123

cloudcapstone123

Overview Properties Permissions Management Access points

Search: Type a prefix and press Enter to search. Press ESC to clear.

Upload Create folder Download Actions

US East (N. Virginia)

Name	Last modified	Size	Storage class
demo.html	Jun 15, 2020 1:23:53 PM GMT+0530	203.0 B	Standard
index.html	Jun 15, 2020 12:58:38 PM GMT+0530	2.2 KB	Standard

Step 10.3: Click on the newly uploaded file, and go to the Object URL

Open Download Download as Make public Copy path

Owner
si_awsb2cmar19_11934

Last modified
Jun 15, 2020 1:23:53 PM GMT+0530

Etag
ca1f0da0b8a6784b50a6b33be7840e14

Storage class
Standard

Server-side encryption
None

Size
203.0 B

Key
demo.html

Object URL
<https://cloudcapstone123.s3.amazonaws.com/demo.html>

cloudcapstone123.s3.amazonaws.com/demo.html

My CloudFront Test

My text content goes here.

my test image

Step 11: Repeat Steps 5 to 11 to create multiple deployments of your application in different regions so that you can meet the global traffic demand.

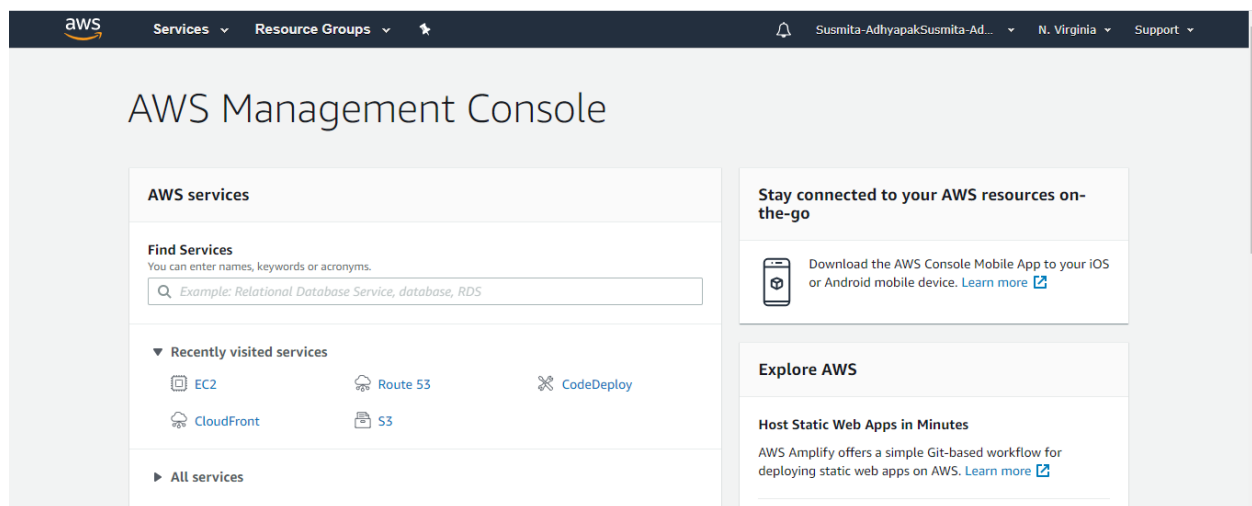
Step 12: Use the traffic flow editor to create traffic policy to route traffic to different endpoints across the globe.

Step 13: As a best practice, follow the principle of least privilege so that you give access to the services that need to be accessed within the AWS console.

AWS:

Approach 2:

Step 1: Log into the AWS console

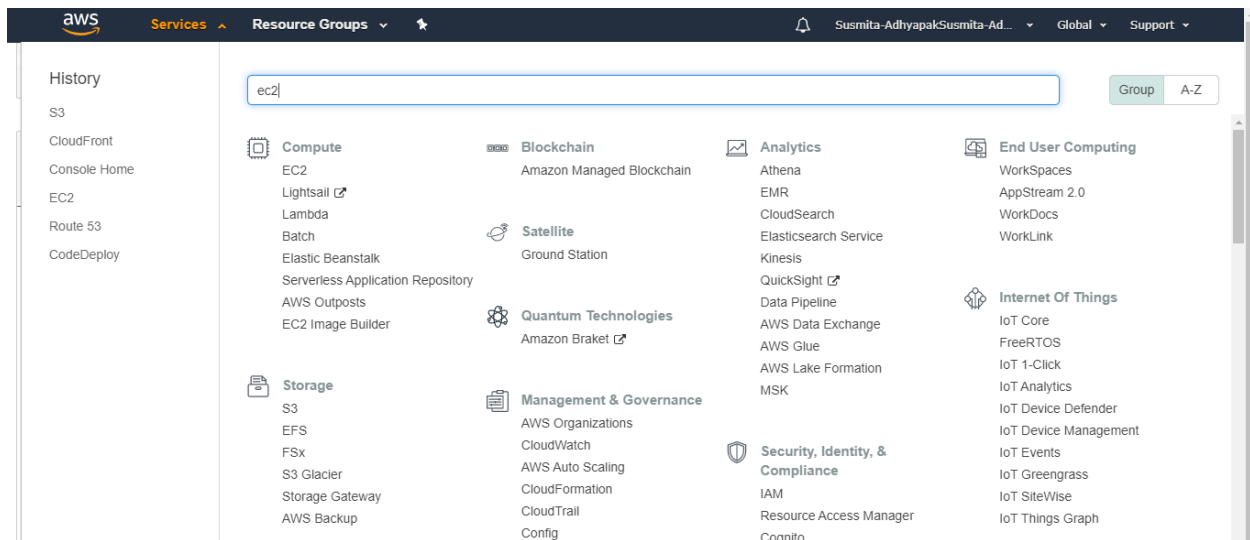


Step 2: Before creating the resources, make sure you apply cost allocation tags to resources so that you can keep a track of billing later on

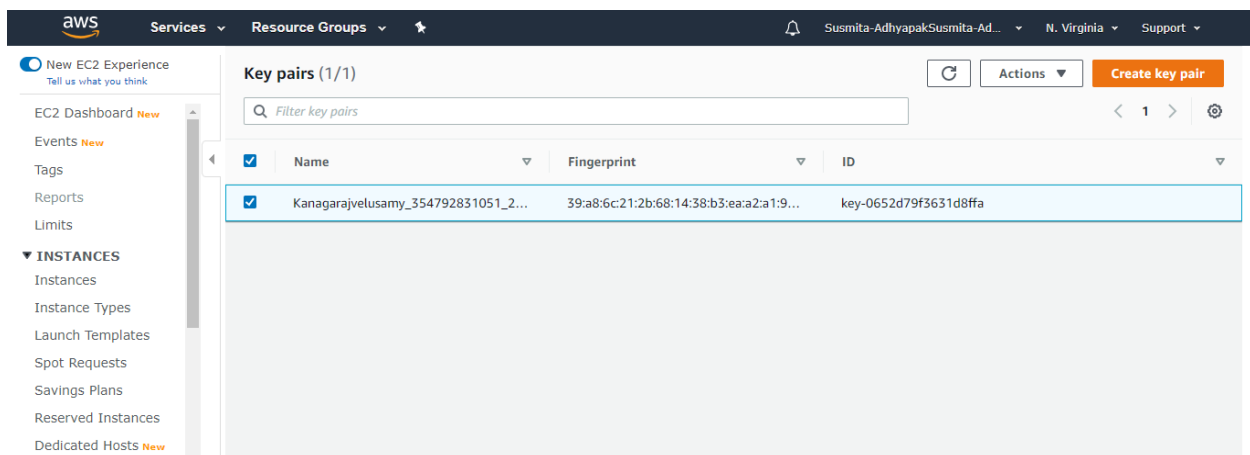
Step 3: To begin, create Route 53 and add a hosted zone if you have your own domain, this is an optional step to configure a custom domain for your web app

Step 4: Create an EC2 instance

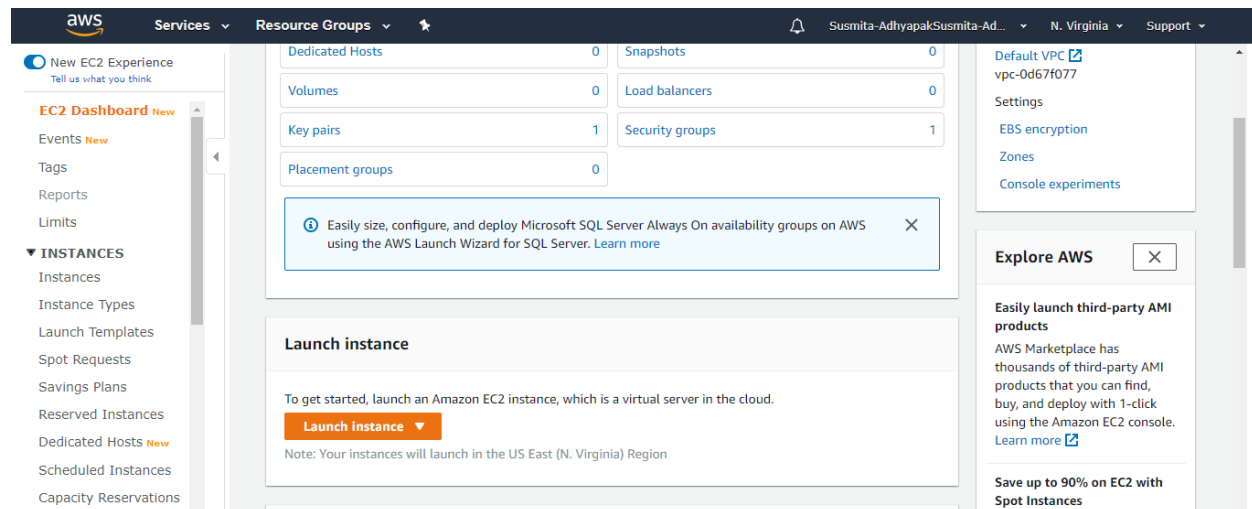
Step 4.1: In the search window, search for EC2



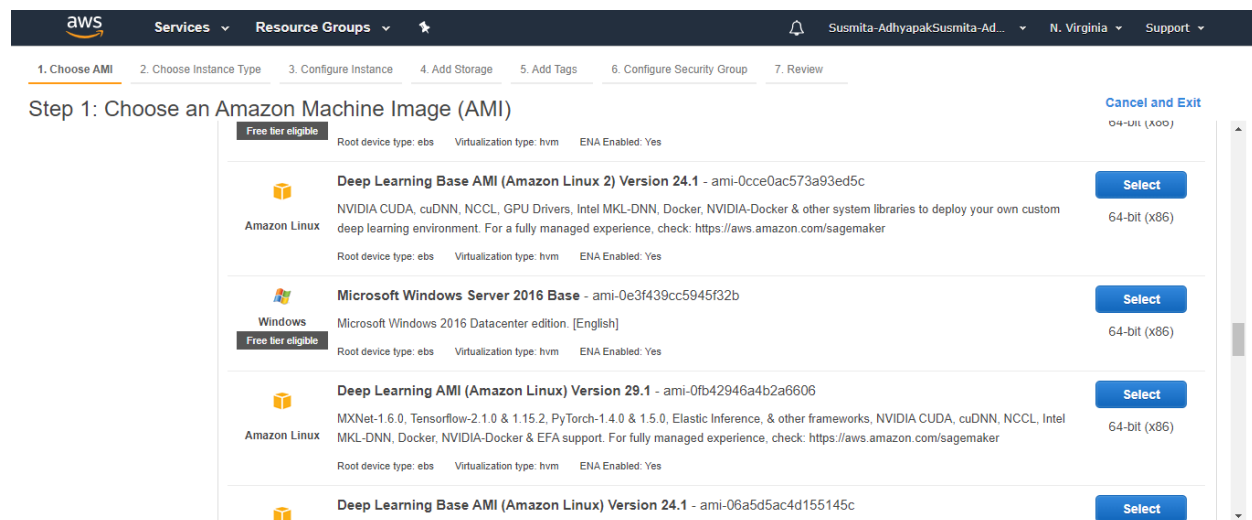
Step 4.2: In the EC2 instance, check whether a key-value pair is created or not. If not then create one



Step 4.3: Click on Launch instance



Step 4.4: Choose an Amazon Machine Image (AMI) (Free tier only) and click on **Select**



Step 4.5: Select a proper instance type (Select t2 micro) and click on **Next: Configure Instance Details**

Services
Resource Groups

Susmita-AdhyapakSusmita-Ad...
N. Virginia
Support

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

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 types Current generation Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

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

Cancel
Previous
Review and Launch
Next: Configure Instance Details

Step 4.6: In the EC2 dashboard, click on **Next: Add Storage**

Services
Resource Groups

Susmita-AdhyapakSusmita-Ad...
N. Virginia
Support

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

Step 3: Configure Instance Details

Auto-assign Public IP Use subnet setting (Enable)

Placement group ☐ Add instance to placement group

Capacity Reservation Open Create new Capacity Reservation

IAM role Simpli@123 Create new IAM role

Shutdown behavior Stop

Stop - Hibernate behavior ☐ Enable hibernation as an additional stop behavior

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

Tenancy Shared - Run a shared hardware instance
[Additional charges may apply when launching Dedicated instances.](#)

Elastic Inference ☐ Add an Elastic Inference accelerator
[Additional charges apply.](#)

Cancel
Previous
Review and Launch
Next: Add Storage

Step 4.7: Click on **Next: Add Tags**

Services
Resource Groups

Susmita-AdhyapakSusmita-Ad...
N. Virginia
Support

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

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/sda1	snap-0726b711cf1c5ad43	30	General Purpose SSD (gp2) ▾	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypt ▾

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

Step 4.8: Click on **Next: Configure Security Groups**

Services
Resource Groups

Susmita-AdhyapakSusmita-Ad...
N. Virginia
Support

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

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 ⓘ
This resource currently has no tags			

Choose the Add tag button or [click to add a Name tag](#).
Make sure your [IAM policy](#) includes permissions to create tags.

Add Tag (Up to 50 tags maximum)

Cancel
Previous
Review and Launch
Next: Configure Security Group

Step 4.9: Click on **Review and Launch**

Services
Resource Groups

Susmita-AdhyapakSusmita-Ad...
N. Virginia
Support

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

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a **new** security group
☐ Select an **existing** security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

[Add Rule](#)

Warning
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.

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

Step 4.10: Click on **Launch**

Services
Resource Groups

Susmita-AdhyapakSusmita-Ad...
N. Virginia
Support

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
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 2016 Base - ami-0e3f439cc5945f32b

Free tier eligible
Microsoft Windows 2016 Datacenter edition. [English]
Root Device Type: ebs Virtualization type: hvm

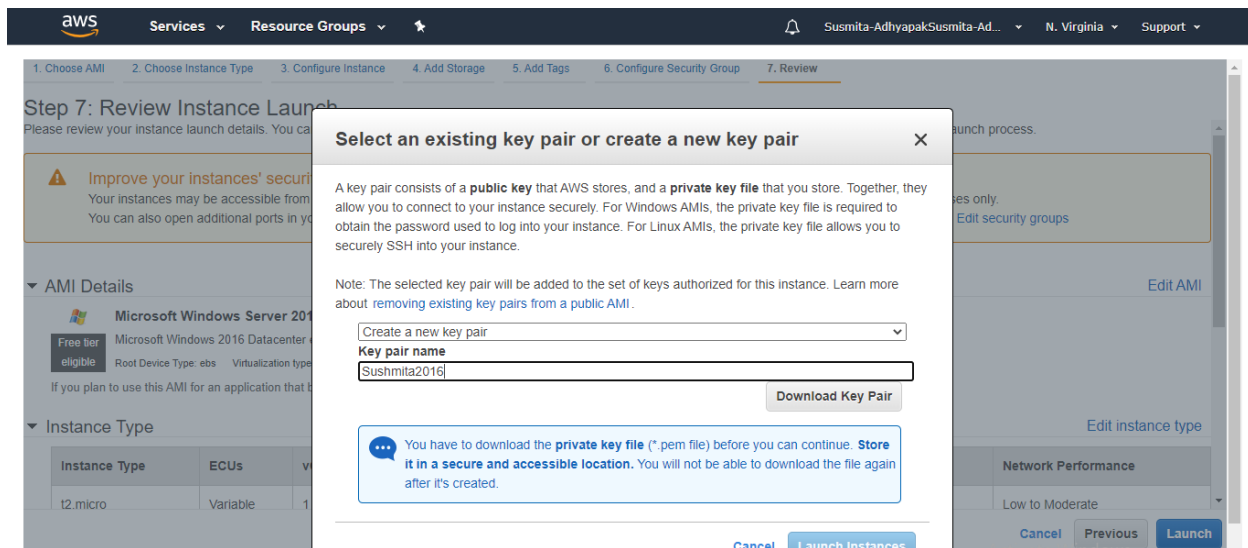
If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the [License Mobility Form](#). Don't show me this again

Instance Type
Edit instance type

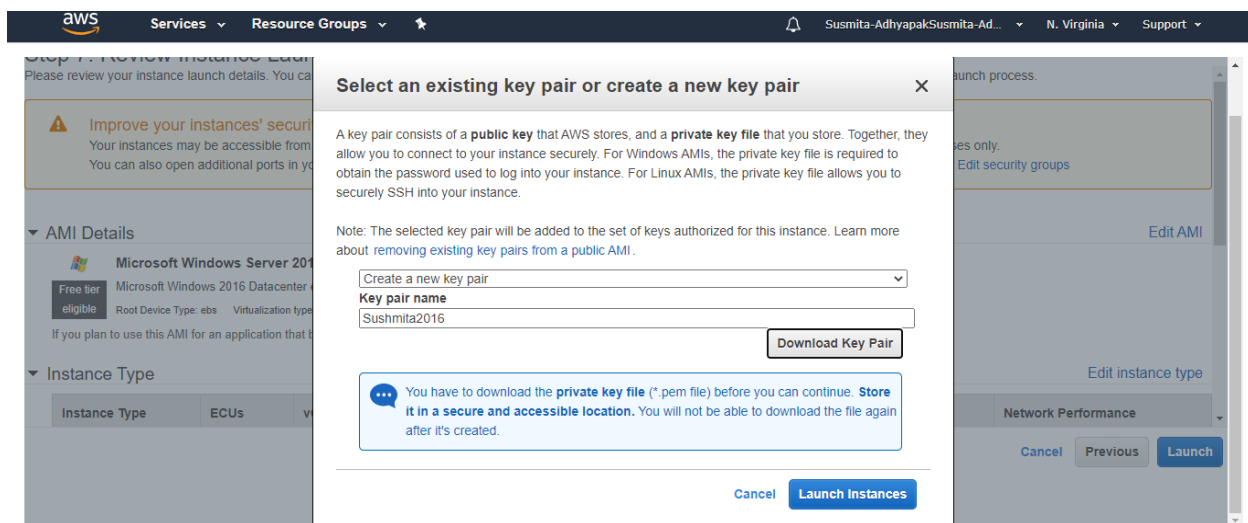
Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

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

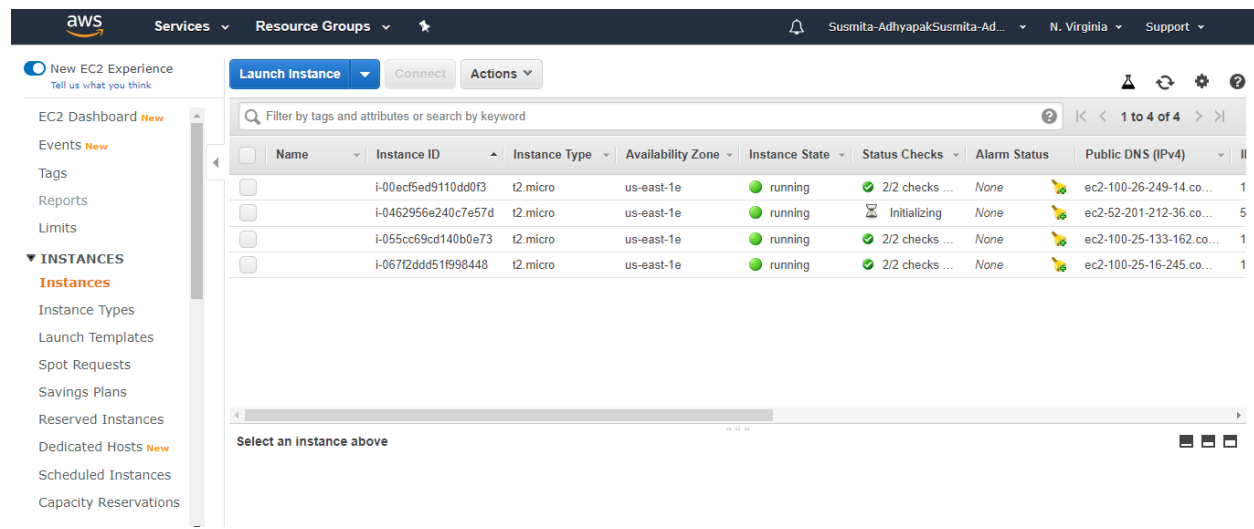
Step 4.11: Create a new key-pair, provide the name of the file and click on **Download Key Pair**



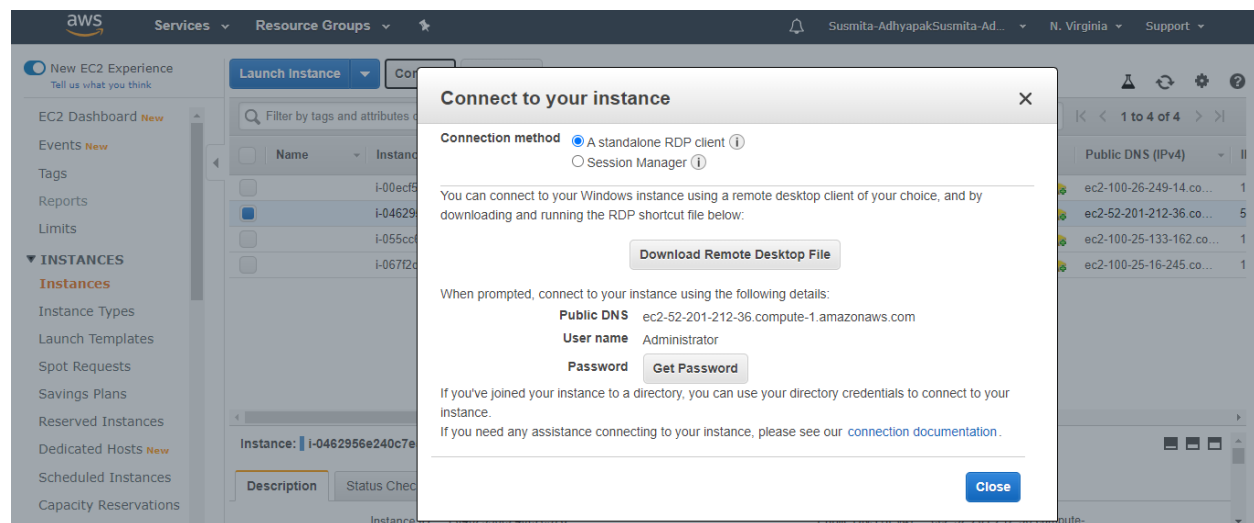
Step 4.12: Click on **Launch Instances**



Step 4.13: Go to the EC2 dashboard, select the created EC2 instance and click on **Connect**

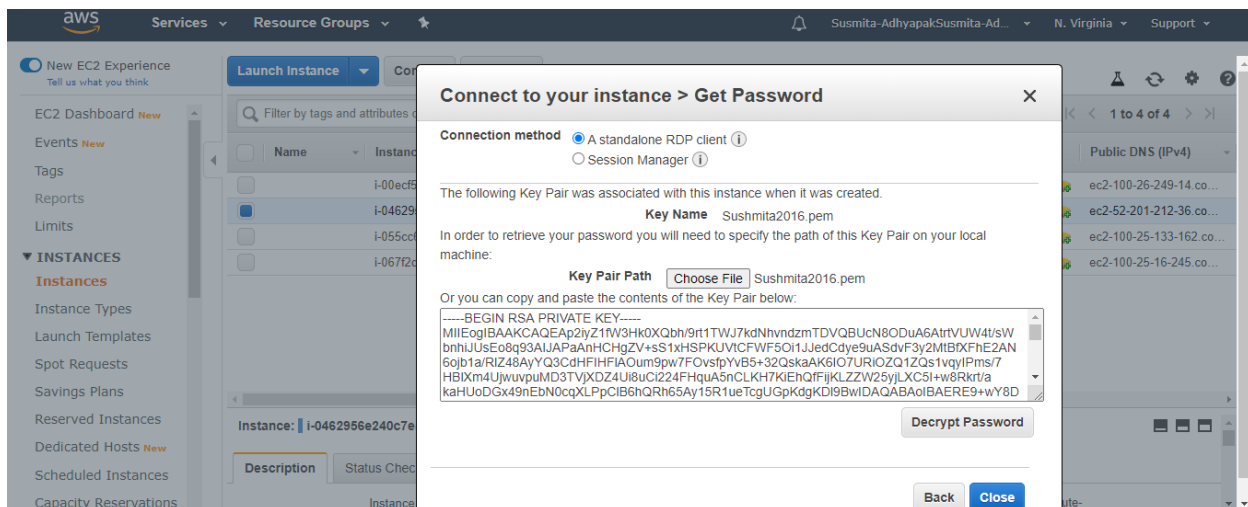


Step 4.14: Click on **Download Remote Desktop File**

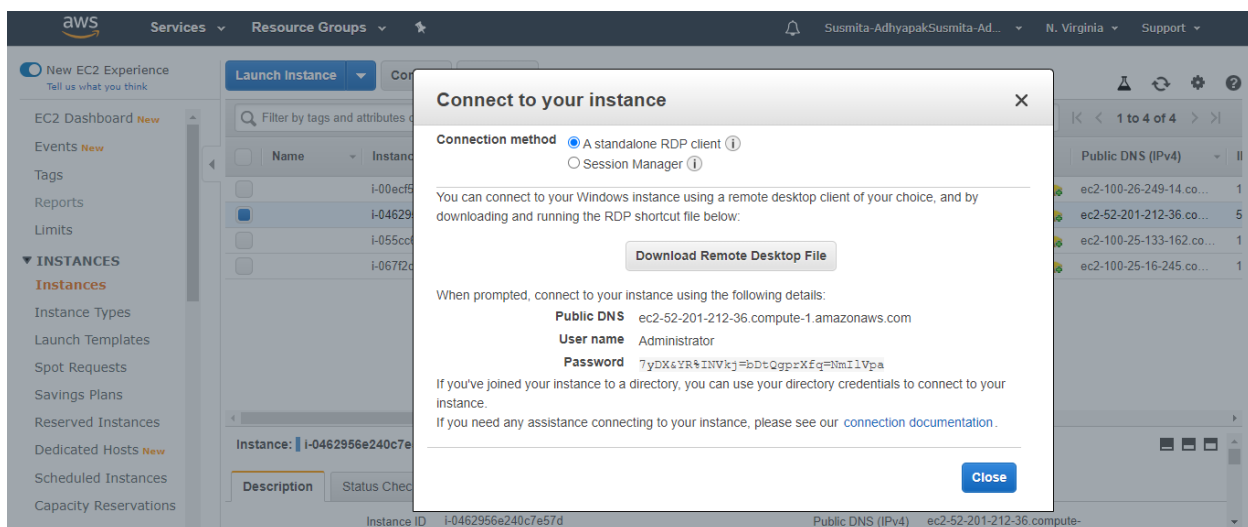


Step 4.15: Click on **Get Password**

Step 4.16: Browse to the Key Pair File you have downloaded using **Choose File** option



Step 4.17: Click on **Decrypt Password**



Step 4.18: Copy the decrypted password

Step 5: Make sure you have inbound traffic on port 80 and port 443 open

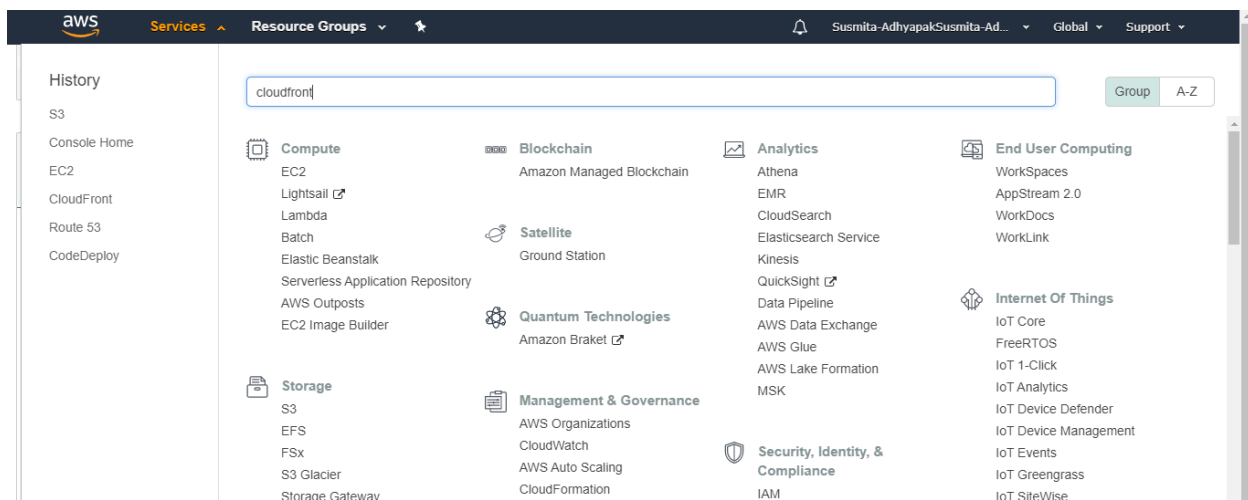
Step 6: Log into EC2 instance and spin up a web server of your choice on port 80

Step 7: Deploy your application on the web server that you have created within the virtual machine

Step 8: Hit the Public IP of EC2 instance (web app endpoint) to check if the application is online

Step 9: Now create a CloudFront distribution corresponding to the static web app endpoint.

Step 9.1: Go to services and search for CloudFront



Step 9.2: Click on **Create Distribution**

CloudFront

Distributions

What's new

▼ **Reports & analytics**

- Cache statistics
- Monitoring
- Alarms
- Popular objects
- Top referrers
- Usage
- Viewers

▼ **Security**

Best practices to optimize Lambda@Edge with CloudFront. [Learn more](#)

Amazon CloudFront Getting Started

Either your search returned no results, or you do not have any distributions. Click the button below to create a new CloudFront distribution. A distribution allows you to distribute content using a worldwide network of edge locations that provide low latency and high data transfer speeds ([learn more](#))

[Create Distribution](#)

Step 9.3: Select a delivery method for your content as Web and click on Get Started

Step 1: Select delivery method

Step 2: Create distribution

Select a delivery method for your content.

Web

Create a web distribution if you want to:

- Speed up distribution of static and dynamic content, for example, .html, .css, .php, and graphics files.
- Distribute media files using HTTP or HTTPS.
- Add, update, or delete objects, and submit data from web forms.
- Use live streaming to stream an event in real time.

You store your files in an origin - either an Amazon S3 bucket or a web server. After you create the distribution, you can add more origins to the distribution.

[Get Started](#)

Step 9.4: Provide the Origin Domain Name (DNS name of the3 created EC2 instance) and Origin ID

Step 1: Select delivery method

Step 2: Create distribution

Create Distribution

Origin Settings

Origin Domain Name:

Origin Path:

Origin ID:

Restrict Bucket Access: ☐ Yes ☒ No

Origin Connection Attempts:

Origin Connection Timeout:

Origin Custom Headers: Header Name Value

Default Cache Behavior Settings

Step 9.5: Keep all the values as default and click on **Create Distribution**

Step 1: Select delivery method
Step 2: Create distribution

Supported HTTP Versions ☒ HTTP/2, HTTP/1.1, HTTP/1.0
☐ HTTP/1.1, HTTP/1.0

Default Root Object

Logging ☐ On
☒ Off

Bucket for Logs

Log Prefix

Cookie Logging ☐ On
☒ Off

Enable IPv6 ☒ [Learn more](#)

Comment

Distribution State ☒ Enabled
☐ Disabled

[Cancel](#) [Back](#) [Create Distribution](#)

Step 9.6: These steps will create your CloudFront distribution.

CloudFront Distributions

[Create Distribution](#) [Distribution Settings](#) [Delete](#) [Enable](#) [Disable](#)

Viewing: Any Delivery Method Any State

	Delivery Method	ID	Domain Name	Comment	Origin	CNAMEs	Status	State	Last Modified
<input type="checkbox"/>	Web	E28IVNJY4FZDCR	d3r6xle28zocdi.cl	-	cloudcaps	-	In Prog	Enabled	2020-06-15 13:1

Step 10: Configure the CloudFront distribution to point to your domain by editing the configuration and adding the domain name in Alternate Domain Name field

Step 11: Repeat steps 4 to 10 to create multiple deployments of your application in

different regions so that you can meet the global traffic demand

Step 12: Use the traffic flow editor to create traffic policy to route traffic to different endpoints across the globe

Step 13: As good practice, follow the principle of least privilege so that you give access to the services that need to be accessed within the AWS console