Report
Cloud computing project

By

6388113	Poomrapee	Wareeboutr
6388133	Pitchaya	Teerawongpairoj
6388196	Sasima	Srijanya

Present to

Dr. Ittipon Rassameeroj

A Report Submitted in Partial Fulfillment of
the Requirements for

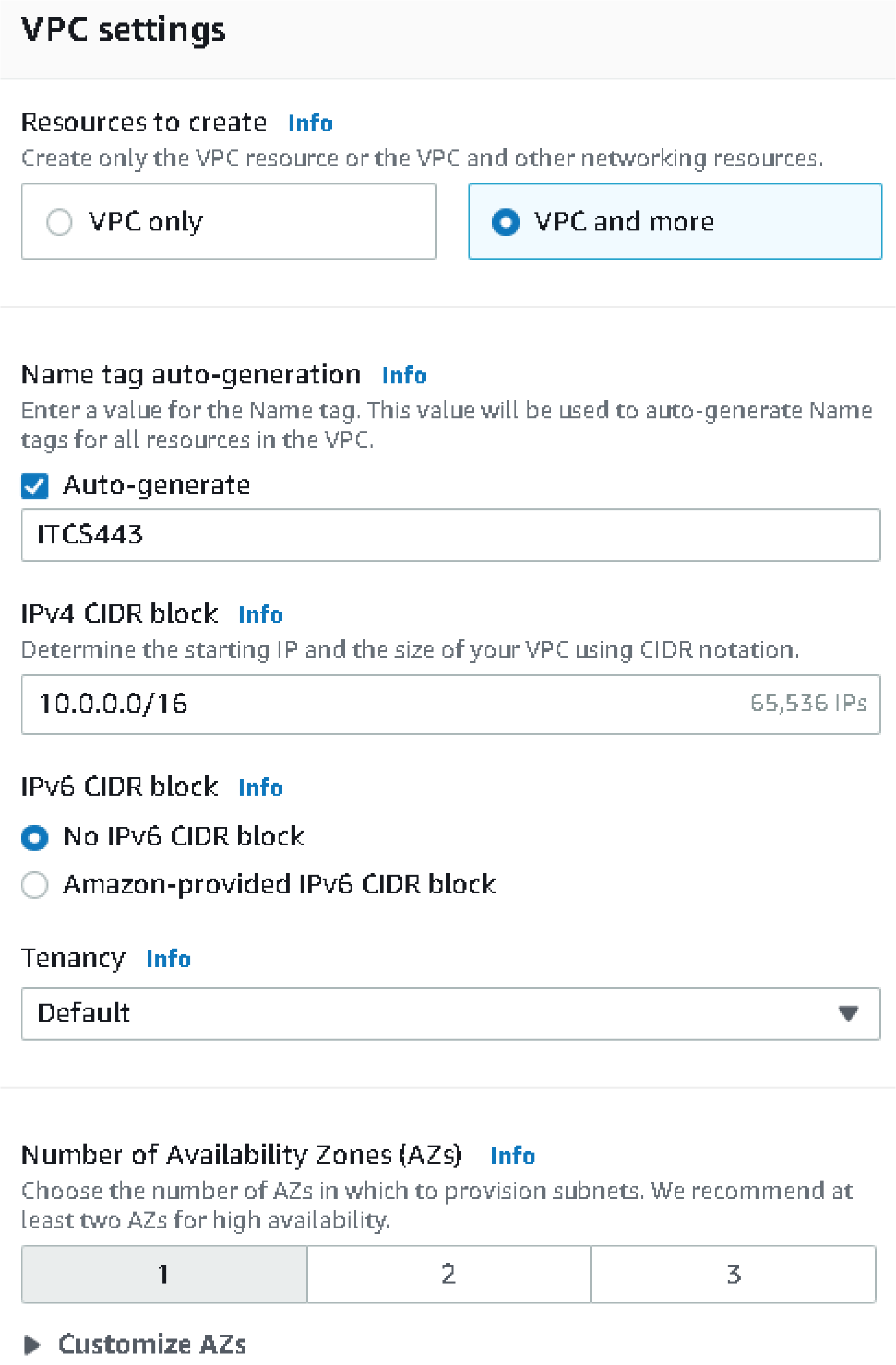
ITCS443 Parallel and Distributed Systems
Faculty of Information and Communication Technology
Mahidol University
Semester 1/2022

Table of Contents

Network

VPC (Virtual Private Cloud)

VPC allow us to launch AWS (Amazon Web Service) resources into the virtual network.



VPC settings

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

○ VPC only ● VPC and more

Name tag auto-generation Info

Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☑ Auto-generate

ITCS443

IPv4 CIDR block Info

Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16 65,536 IPs

IPv6 CIDR block Info

● No IPv6 CIDR block

○ Amazon-provided IPv6 CIDR block

Tenancy Info

Default ▼

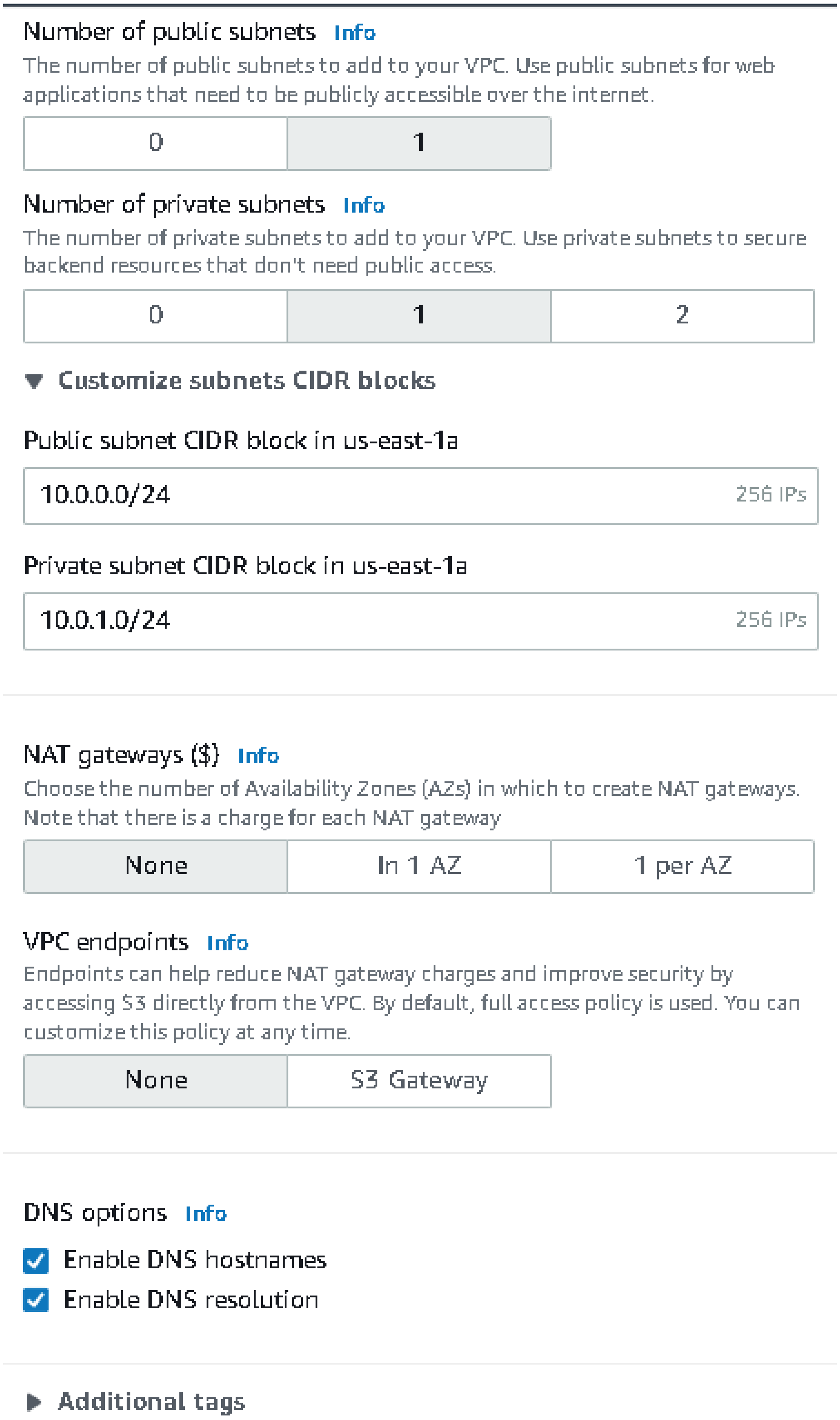
Number of Availability Zones (AZs) Info

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

[✓ 1] 2 3

▶ Customize AZs

Figure 1 VPC Setting



Number of public subnets Info

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0 [✓ 1]

Number of private subnets Info

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0 [✓ 1] 2

▼ Customize subnets CIDR blocks

Public subnet CIDR block in us-east-1a

10.0.0.0/24 256 IPs

Private subnet CIDR block in us-east-1a

10.0.1.0/24 256 IPs

NAT gateways ($) Info

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

[✓ None] In 1 AZ 1 per AZ

VPC endpoints Info

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

[✓ None] S3 Gateway

DNS options Info

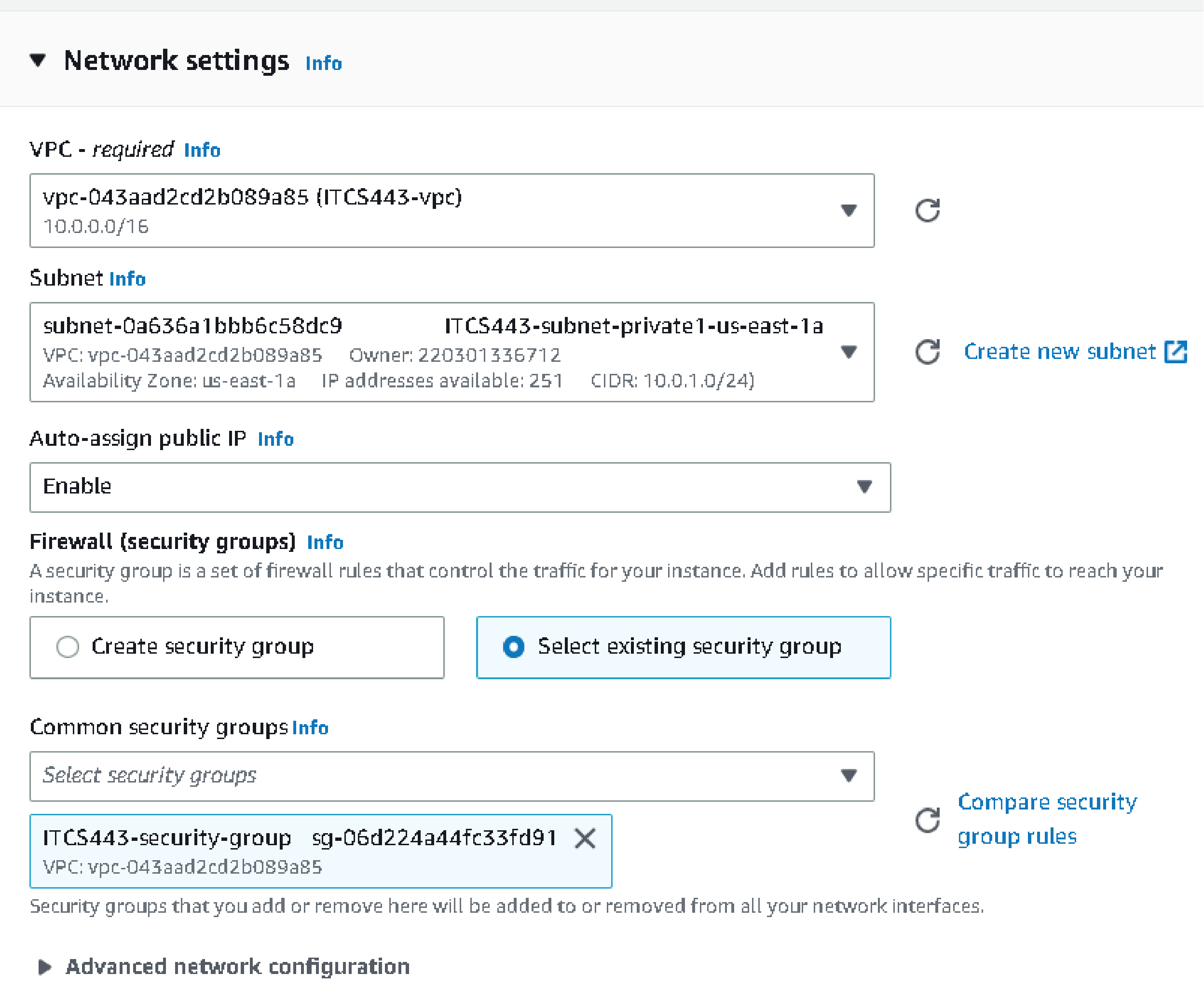
☑ Enable DNS hostnames

☑ Enable DNS resolution

▶ Additional tags

Figure 2 VPC Setting

Figures 1 and 2 are the VPC setting which we configure the VPC detail.



▼ Network settings Info

VPC - *required* Info

vpc-043aad2cd2b089a85 (ITCS443-vpc) ▼
10.0.0.0/16

Subnet Info

subnet-0a636a1bbb6c58dc9 ITCS443-subnet-private1-us-east-1a ▼
VPC: vpc-043aad2cd2b089a85 Owner: 220301336712
Availability Zone: us-east-1a IP addresses available: 251 CIDR: 10.0.1.0/24)

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 ▼

ITCS443-security-group sg-06d224a44fc33fd91 ✕
VPC: vpc-043aad2cd2b089a85

Compare security group rules

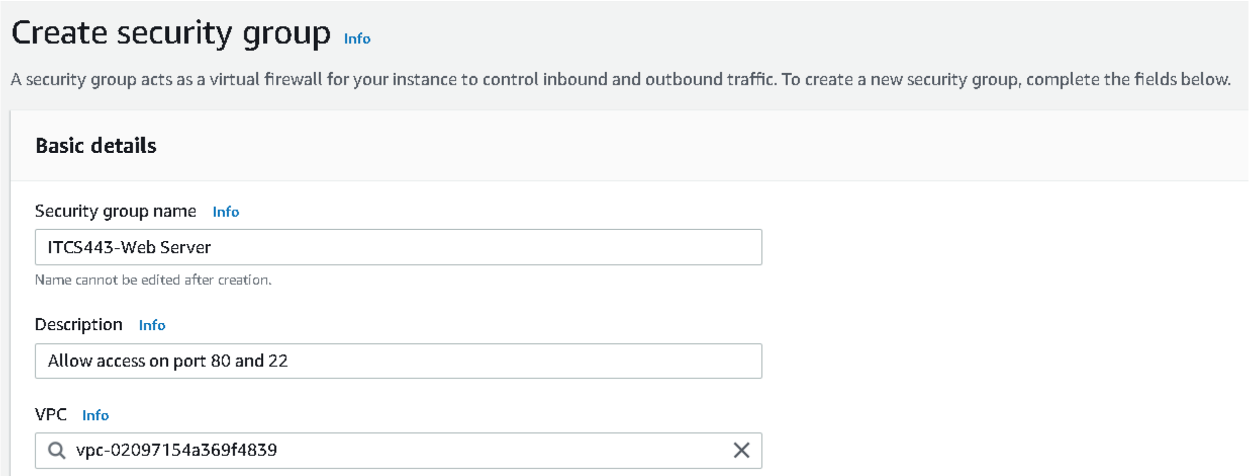
Security groups that you add or remove here will be added to or removed from all your network interfaces.

▶ **Advanced network configuration**

Figure 3 Network setting

Figure 3, we set the network from what we created including ITCS443-VPC and ITCS443-security-group.

Security



Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

ITCS443-Web Server

Name cannot be edited after creation.

Description Info

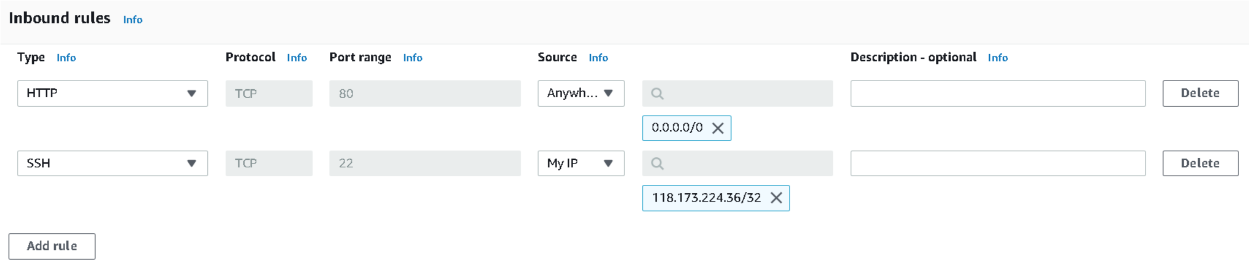
Allow access on port 80 and 22

VPC Info

vpc-02097154a369f4839

Figure 4

Figure 4, we created a security group for access on port 22 and 80 for VPC that we created (VPC: ITCS443).



Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
HTTP ▼	TCP	80	Anywh... ▼	0.0.0.0/0 ✕		Delete
SSH ▼	TCP	22	My IP ▼	118.173.224.36/32 ✕		Delete

Add rule

Figure 5

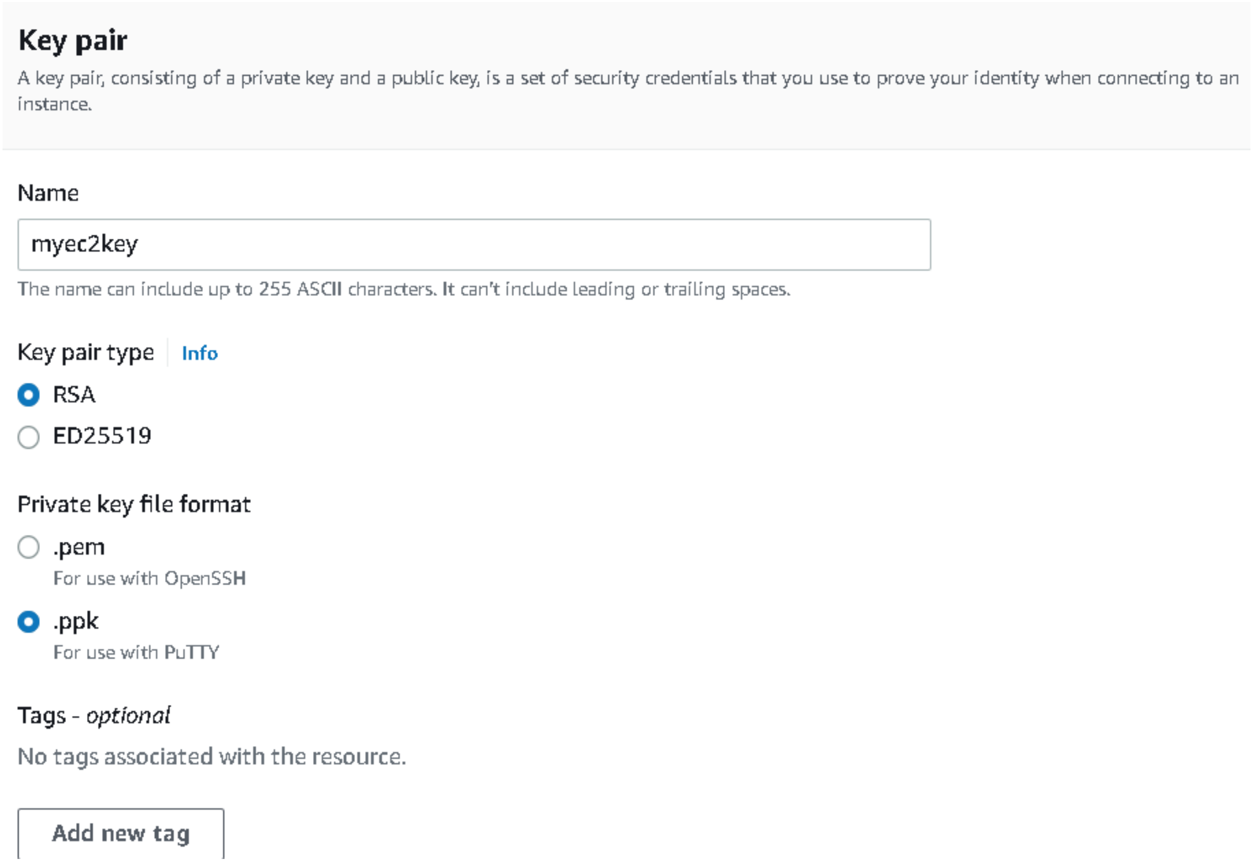
Figure 5, the first rule at inbound rule that we created is for port 80 (HTTP). Opening port 80 will allow users on the internet to access the website (our project). For the sources of the first rule we set as Anywhere IPv4 which allows coming traffic on port 80.

For the second rule that we created is for port 22 (SSH). For the sources of the second rule we set as My IP. When traffic coming on port 22, the traffic will only allow limited IP address that come from this IP address. This port 22 allows ssh into the EC2 instance.

Instance Configuration

Amazon EC2 (AmazonElastic Compute Cloud)

We use EC2 because it can design the cloud to make web-scale cloud computing easier for us which we can also resize the cloud.



Key pair

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

myec2key

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type | Info

● RSA

○ ED25519

Private key file format

○ .pem
For use with OpenSSH

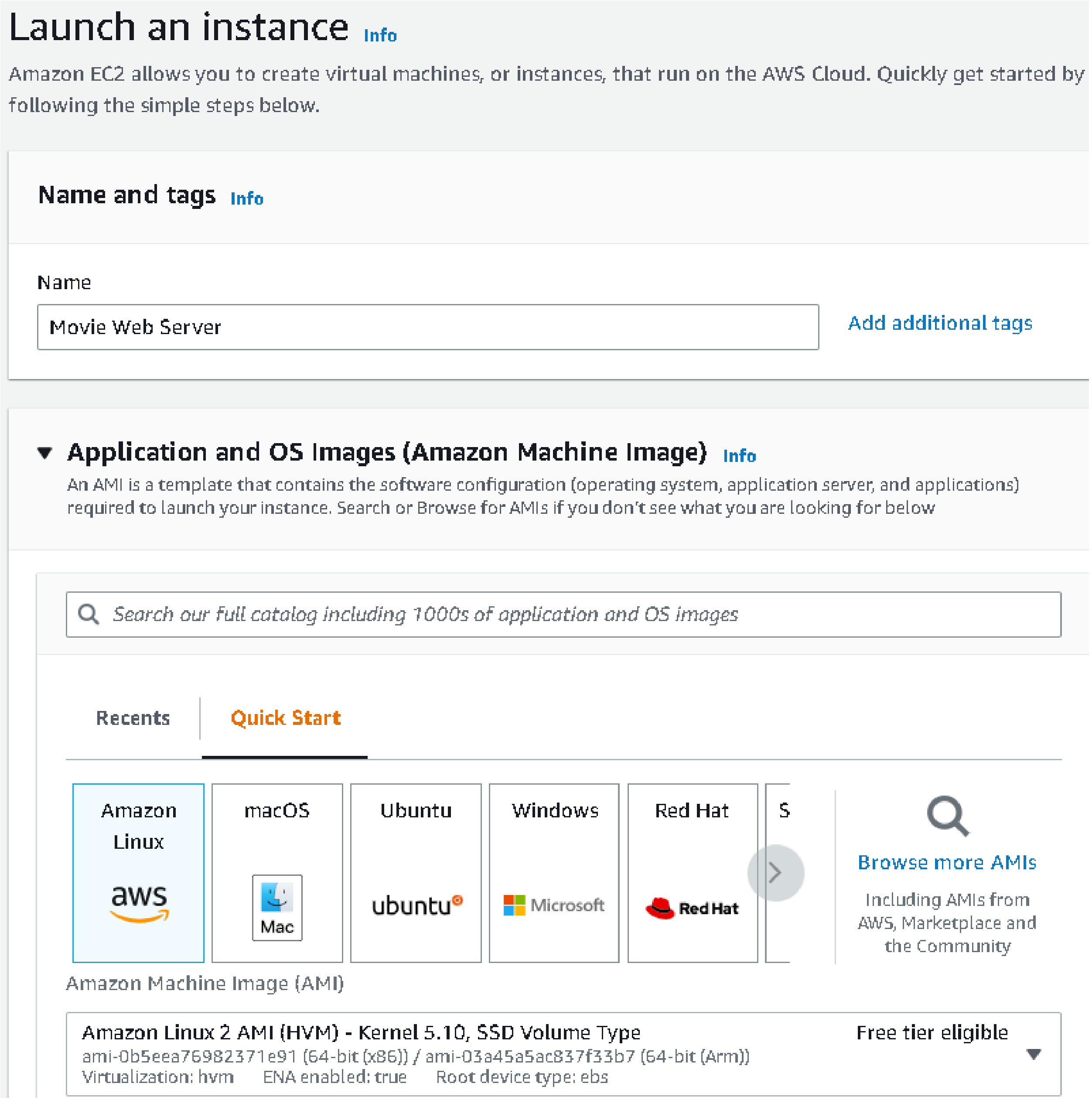
● .ppk
For use with PuTTY

Tags - *optional*

No tags associated with the resource.

Figure 6 EC2 Key pairs

In the figure 6, when connecting to an Amazon EC2 instance with PuTTY, we have implemented a set of security credentials called myec2key that are part of the Amazon EC2 key pairs.



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

Movie Web Server

Add additional tags

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

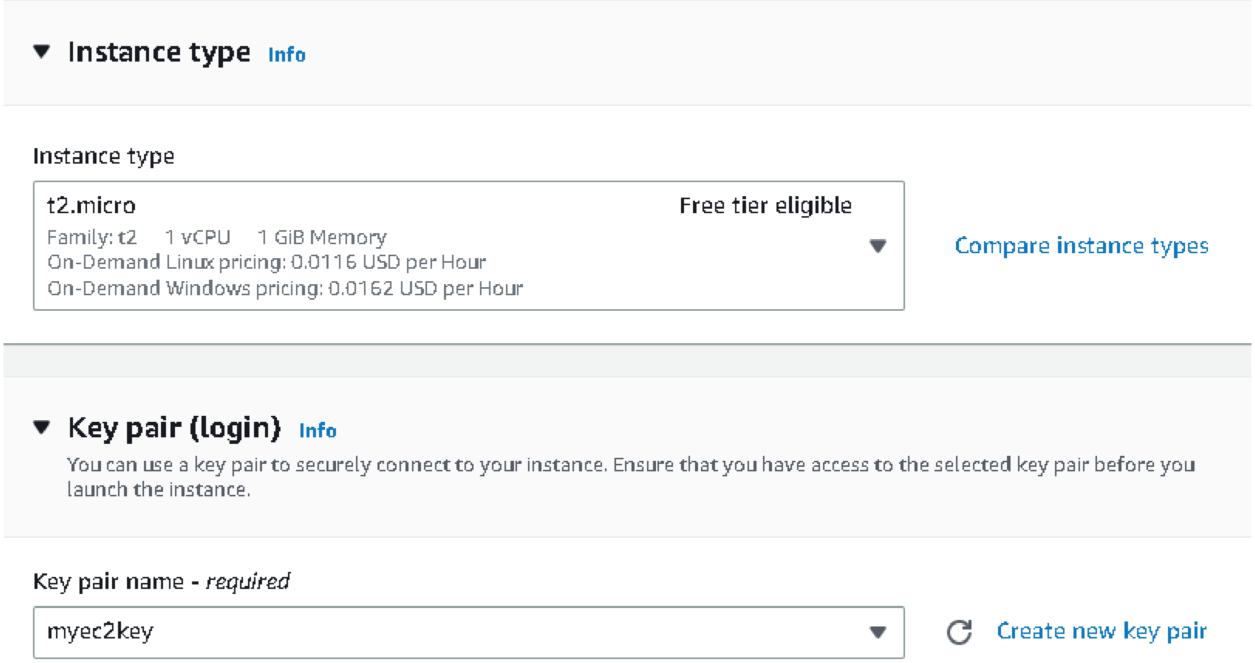
Search our full catalog including 1000s of application and OS images

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type   Free tier eligible
ami-0b5eea76982371e91 (64-bit (x86)) / ami-03a45a5ac837f33b7 (64-bit (Arm))
Virtualization: hvm   ENA enabled: true   Root device type: ebs

Figure 7 EC2 instance

Figure 7, we have launched a new instance in the EC2 named Movie Web Server and configured the instance details.



Instance type

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GiB Memory

On-Demand Linux pricing: 0.0116 USD per Hour

On-Demand Windows pricing: 0.0162 USD per Hour

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*

myec2key

Figure 8 EC2 instance

Figure 8, we set instance type as t2.micro and myec2key that we created.

System Diagram

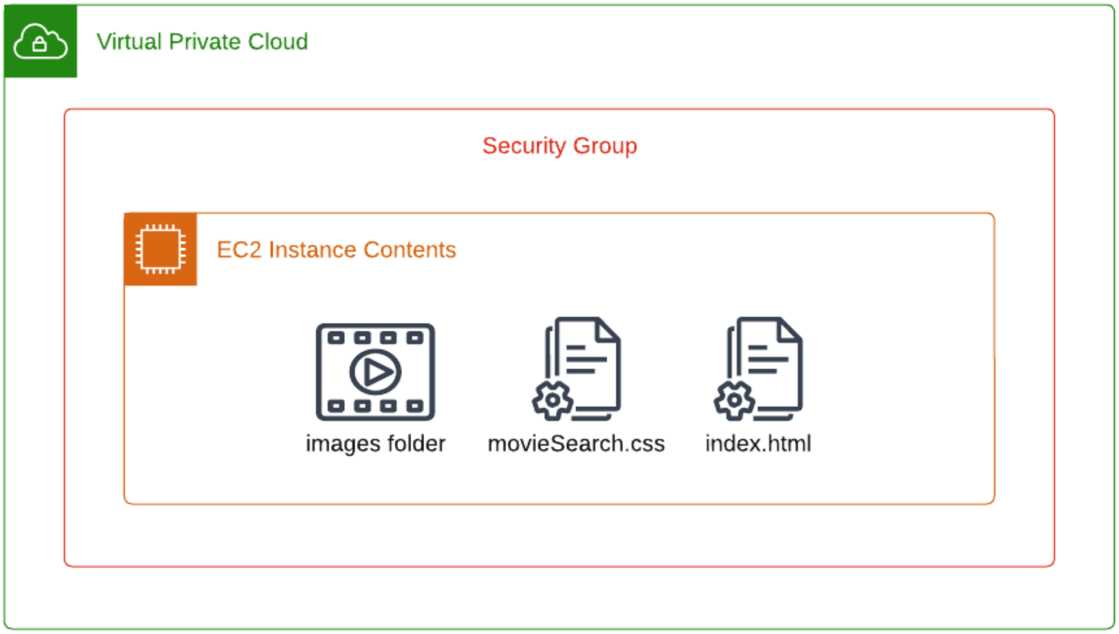


Figure 9 AWS architecture of the project

The diagram above shows an overview of the AWS architecture that we use to design for deploying the website as well as the content within the EC2 instance.

Setup Diagram

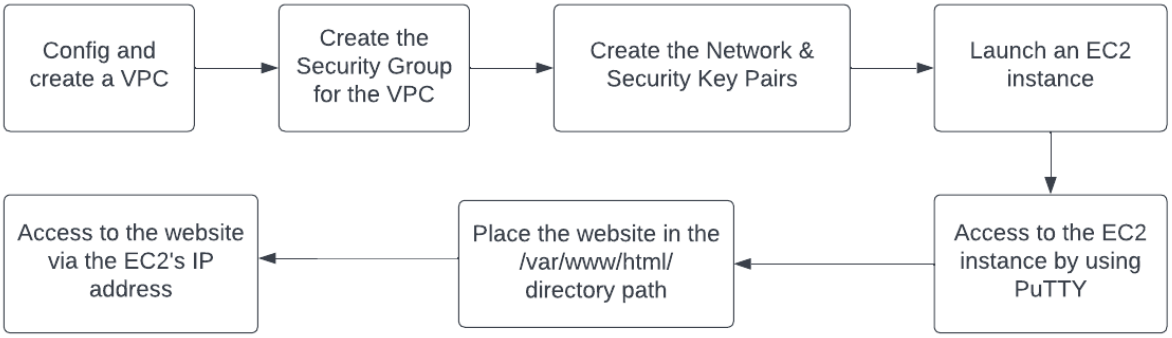

Config and create a VPC
Create the Security Group for the VPC
Create the Network & Security Key Pairs
Launch an EC2 instance
Access to the EC2 instance by using PuTTY
Place the website in the /var/www/html/ directory path
Access to the website via the EC2's IP address

Figure 10 Steps to deploy the website on AWS cloud

The setup diagram explains how we came up with and deployed the website live on the AWS cloud. Also, it is even an actual step we do in this project.

Video’s link

Link to the video of deployed project:

https://www.loom.com/share/ef9871fbe97949188ad7323ac5317f4a