


Practical: Creating an EC2 Instance

Table of Contents

- [Section Overview](#)
- [References](#)
- [Settings quick summary](#)
- [Prerequisites](#)
- [Step 1. Login to AWS.](#)
- [Step 2. EC2 launch instance page](#)
- [Step 3. Instance name and tags](#)
- [Step 4. OS settings](#)
- [Step 5. Instance type](#)
- [Step 6. Key pair for remote login](#)
- [Step 7. Edit network settings](#)
- [Step 8. Storage](#)
- [Step 9. Roles and shutdown settings](#)
- [Step 10. Review settings and launch](#)
- [Step 11. View EC2 instances](#)
- [Step 12. Terminating the instance](#)
- [Additional reading](#)
 - [Subnets](#)
 - [Bastion Host](#)
 - [Security Groups](#)
 - [Common errors](#)
 - [Lights-out policy](#)

Section Overview

This guide will show you how to create an EC2 instance in AWS via the user portal (AWS Console). EC2 instance will be the Virtual Machines (VM's) we will be using throughout the course.

QUT have followed the [AWS Well-Architected](https://aws.amazon.com/architecture/well-architected/)  (<https://aws.amazon.com/architecture/well-architected/>) framework to configure your workspace so there are a few things we have to work with.

References

- [AWS What is an EC2 \(VM\)](https://aws.amazon.com/ec2/)  (<https://aws.amazon.com/ec2/>)

- [AWS Guide on building an EC2](https://aws.amazon.com/getting-started/launch-a-virtual-machine-B-0/)  [\(https://aws.amazon.com/getting-started/launch-a-virtual-machine-B-0/\)](https://aws.amazon.com/getting-started/launch-a-virtual-machine-B-0/)
- [AWS Well-Architected framework](https://aws.amazon.com/architecture/well-architected/)  [\(https://aws.amazon.com/architecture/well-architected/\)](https://aws.amazon.com/architecture/well-architected/)

Settings quick summary

This is a summary of the settings that need to be changed and is intended as a reference only. Please see the complete instructions below if you are not already familiar with the process.

- **Name and tags:** add the `purpose` tag. The `qut-username` tag will be automatically created.
- **Application and OS Images:** Ubuntu 24.04
- **Instance type:** t3.micro
- **Key pair:** select your keypair identifier
- **Network settings:**
 - select a public subnet to be accessible from the internet
 - select existing security group: `CAB432SG`
- **Advanced details:**
 - IAM instance profile: `CAB432-Instance-Role`
 - Shutdown behaviour: Terminate

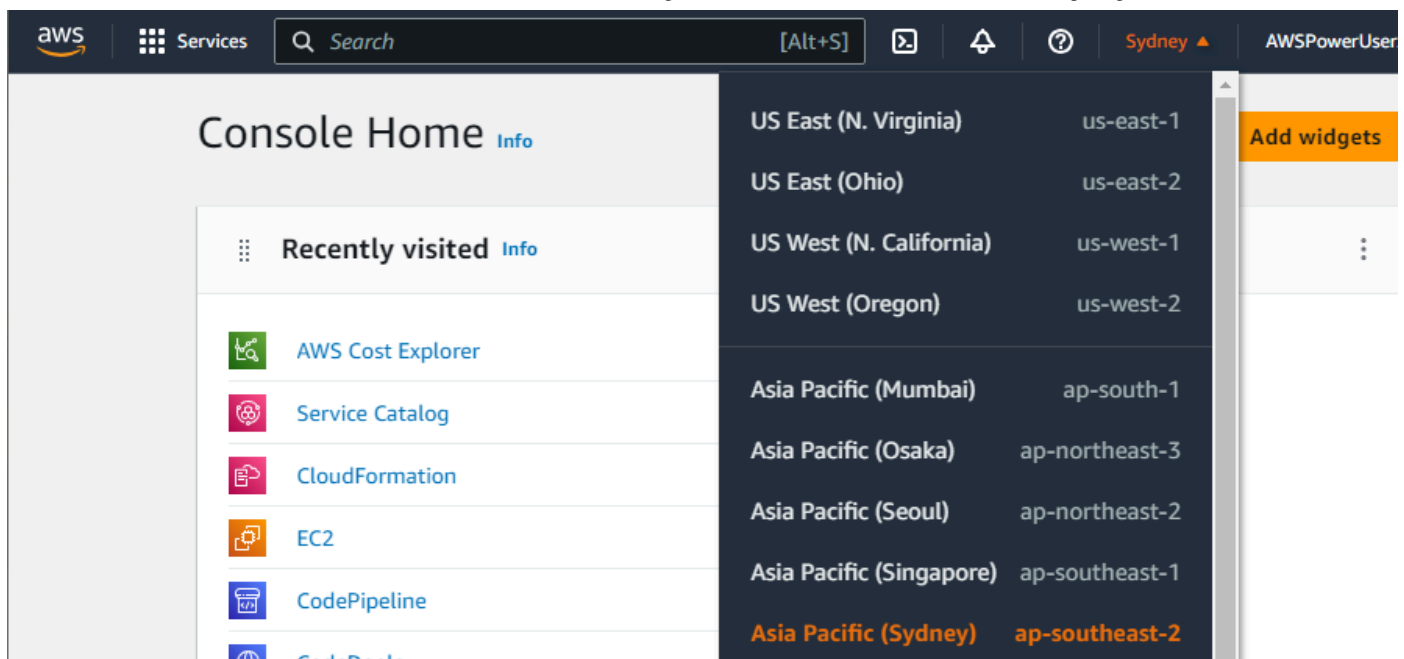
Prerequisites

- [Accessing the CAB432 cloud console](https://canvas.qut.edu.au/courses/20367/pages/practical-logging-on-to-qut-aws-cloud)
(<https://canvas.qut.edu.au/courses/20367/pages/practical-logging-on-to-qut-aws-cloud>)

Step 1. Login to AWS.

Follow the [Accessing the CAB432 cloud console](https://canvas.qut.edu.au/courses/20367/pages/practical-logging-on-to-qut-aws-cloud) (<https://canvas.qut.edu.au/courses/20367/pages/practical-logging-on-to-qut-aws-cloud>) to log in to the CAB432 AWS account.

Ensure your AWS Region is set to Sydney (`ap-southeast-2`). You can do this by clicking on the region in the top right hand corner of the AWS Console. If you are not in the Sydney region, please change to Sydney.

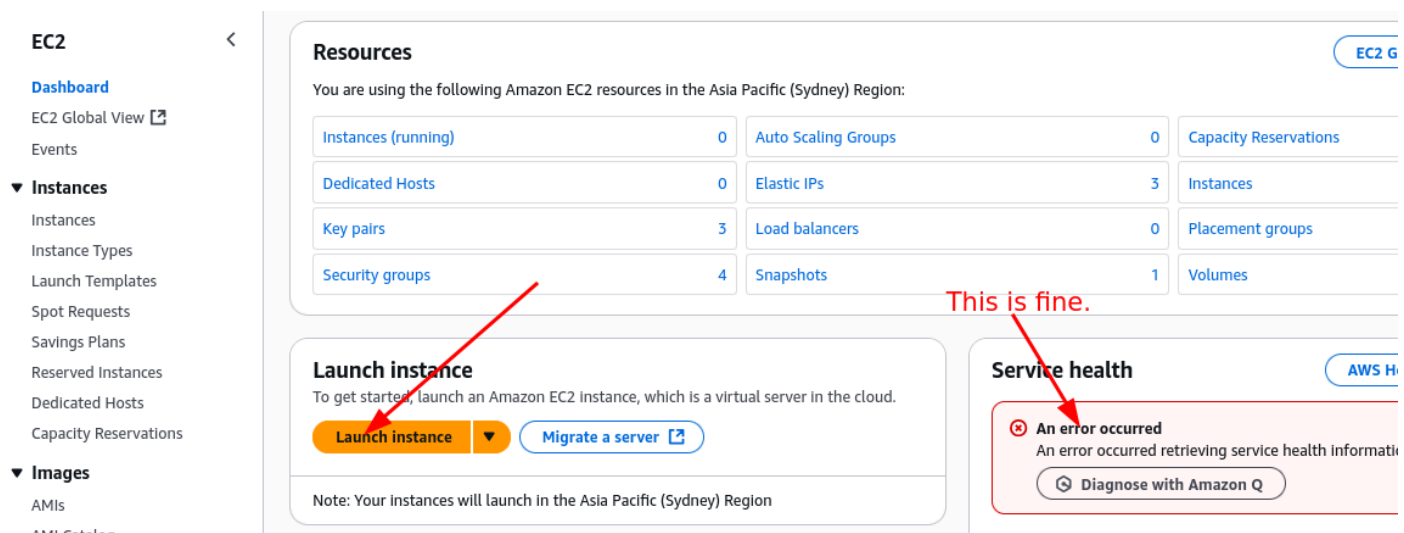


Step 2. EC2 launch instance page

On the search bar (Shortcut via Alt + S), type in EC2 and select the EC2 service.

The EC2 Dashboard will provide you with a list of resources. Take notice of the number of EC2 resources in the CAB432 account. For instance, the number of running instances.

The dashboard has an orange button that says "Launch instance". Please click it.



Step 3. Instance name and tags

In this page, we will be defining our parameters and configuration for our EC2 instance. Please use the following configurations

- You can **name** your EC2 instance whatever you like. Some common conventions include `ec2-RegionCode-EnvironmentCode-ApplicationCode`.

We also want to specify additional tags. Click on "Add additional tags", to the right of the Name input field.

- A tag with key **qut-username** will be automatically created. Without this tag you will not be able to access your EC2 instance, so do not modify it.
- Add a tag with key **purpose**. In this case, enter **practical** as the value. We use these tags when determining whether resources are safe to delete, so please set it correctly.

▼

Name and tags

Info

Key

Info

Value

Info

Resource types

Info

Q

Name

×

Q

Enter value

Select resource ty...

▼

Remove

Instances

×

Key

Info

Value

Info

Resource types

Info

Q

qut-username

×

Q

n1234567@qut.

×

Select resource ty...

▼

Remove

Instances

×

Key

Info

Value

Info

Resource types

Info

Q

purpose

×

Q

practical

×

Select resource ty...

▼

Remove

Instances

×

Add new tag

You can add up to 47 more tags.

Step 4. OS settings

- **[OS]** We will be using the Ubuntu 24.04 LTS AMI (Amazon Machine Image) for this course. Other images are fine but at your own risk.
- **[OS]** 64-bit (x86) Architecture is fine.

▼ 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

My AMIs


Quick Start




Amazon Linux




macOS



Ubuntu




Windows



Red Hat



SUSE Linux



[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type

Free tier eligible ▼

ami-03f0544597f43a91d (64-bit (x86)) / ami-003e57d854eb96910 (64-bit (Arm))

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

Description

Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Architecture

64-bit (x86) ▼

AMI ID

ami-03f0544597f43a91d

Verified provider

Step 5. Instance type

- Accept the default **t3.micro** instance type. This defines the spec (number of CPU cores, amount of RAM, etc.) of your VM.

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t3.micro

Family: t3 2 vCPU 1 GiB Memory Current generation: true

On-Demand Ubuntu Pro base pricing: 0.0167 USD per Hour On-Demand RHEL base pricing: 0.042 USD per Hour ▼

On-Demand Windows base pricing: 0.0224 USD per Hour On-Demand SUSE base pricing: 0.0132 USD per Hour

On-Demand Linux base pricing: 0.0132 USD per Hour

Additional costs apply for AMIs with pre-installed software

Step 6. Key pair for remote login

You probably do not yet have a [key pair](#) ➞

(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html>) in the CAB432 AWS account. Create one now and re-use it for the entire semester (unless it becomes compromised).

A key pair, consisting of a public key and a private key, is a set of security credentials that you use to prove your identity when connecting to an Amazon EC2 instance. For Linux instances, the private key allows you to securely SSH into your instance. For Windows instances, the private key is required to decrypt the administrator password, which you then use to connect to your instance.

Because Amazon EC2 doesn't keep a copy of your private key, there is no way to recover a private key if you lose it.

Source: [AWS Documentation](#) ➞ (<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html>)

Click **Create new key pair**.

Important: your key pair's name must identify you by name or ID! If we do not know who owns a key pair, we will delete it without notice!

Enter a name, accept the defaults and click **Create new key pair**. This will trigger a download for your private key file. You will need this to connect to your EC2 instance, so save it somewhere where you can access it again later. If you lose this then you will likely need to create a new EC2 instance.

Step 7. Edit network settings

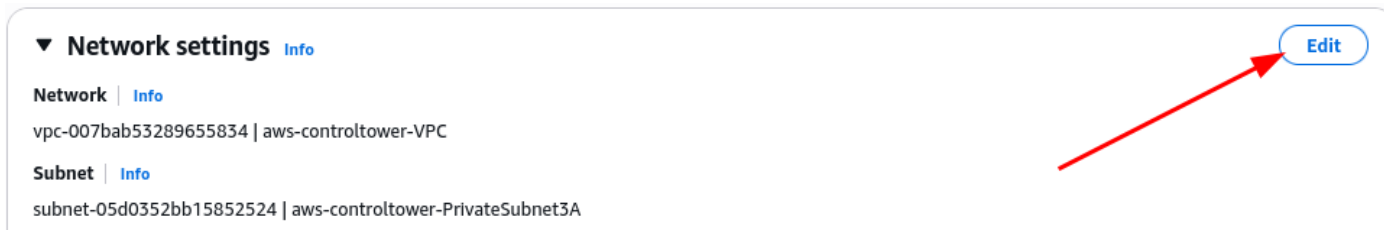
Our virtual machine will be launched in a **virtual private cloud** (VPC).

With Amazon Virtual Private Cloud (Amazon VPC), you can launch AWS resources in a logically isolated virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

Source: [Amazon Documentation](#) ➞ (<https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html>)

The default settings may not be appropriate for what we want to do. In the next prac, we will create a web server that needs to connect to the internet so we need to create our VM in any of the **public** subnets.

Click **Edit**



▼ **Network settings** [Info](#)

Network | [Info](#)

vpc-007bab53289655834 | aws-controltower-VPC

Subnet | [Info](#)

subnet-05d0352bb15852524 | aws-controltower-PrivateSubnet3A

[Edit](#)

Subnet

In the subnet drop-down, select any of the **public** subnets, named `aws-controltower-PublicSubnetN` where `N` is 1, 2 or 3.

At this point, you may realise that naming of cloud resources is critical, and often full of jargon (e.g., `aws-controltower-PublicSubnet2`). The console also makes some bold assumptions, like you knowing the basics of networking. Consider in this panel that it indicates the CIDR of this subnet. Do you recall what a **CIDR** (https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing) is from your time studying networks?

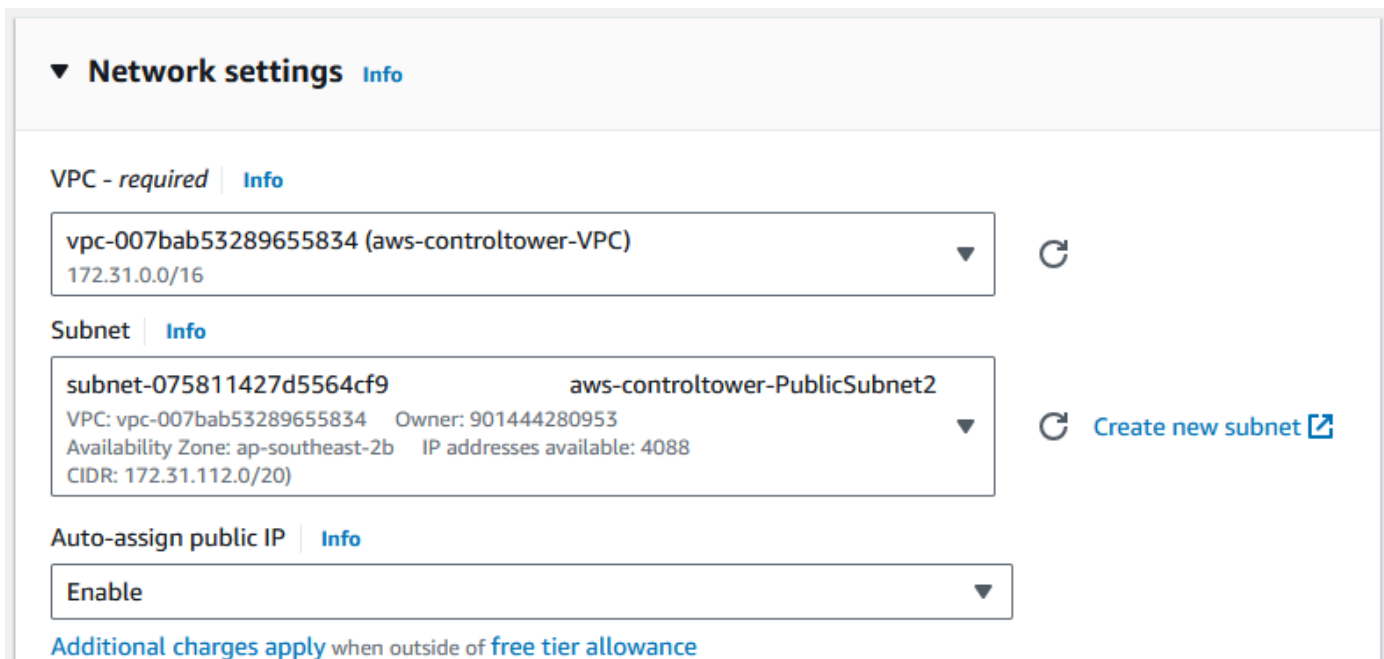
Auto-assign public IP

Leave this enabled. AWS does provide the facility to attach an instance to an IP address that you can lease for a long term (that does come with a cost, but its small). See [Elastic IP addresses](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html) (<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html>):

An Elastic IP address is a static IPv4 address designed for dynamic cloud computing. An Elastic IP address is allocated to your AWS account, and is yours until you release it. By using an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account. Alternatively, you can specify the Elastic IP address in a DNS record for your domain, so that your domain points to your instance.

Source: [AWS Documentation](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html)

(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html>)



▼ **Network settings** [Info](#)

VPC - required | [Info](#)

vpc-007bab53289655834 (aws-controltower-VPC) [↻](#)
172.31.0.0/16

Subnet | [Info](#)

subnet-075811427d5564cf9 **aws-controltower-PublicSubnet2** [↻](#)
VPC: vpc-007bab53289655834 Owner: 901444280953
Availability Zone: ap-southeast-2b IP addresses available: 4088
CIDR: 172.31.112.0/20 [Create new subnet](#)

Auto-assign public IP | [Info](#)

Enable

Additional charges apply when outside of **free tier allowance**

Security group

We must assign an existing security group that was configured by QUT.

- Click the "select existing security group" radio button & then select the **CAB432SG**.

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 y

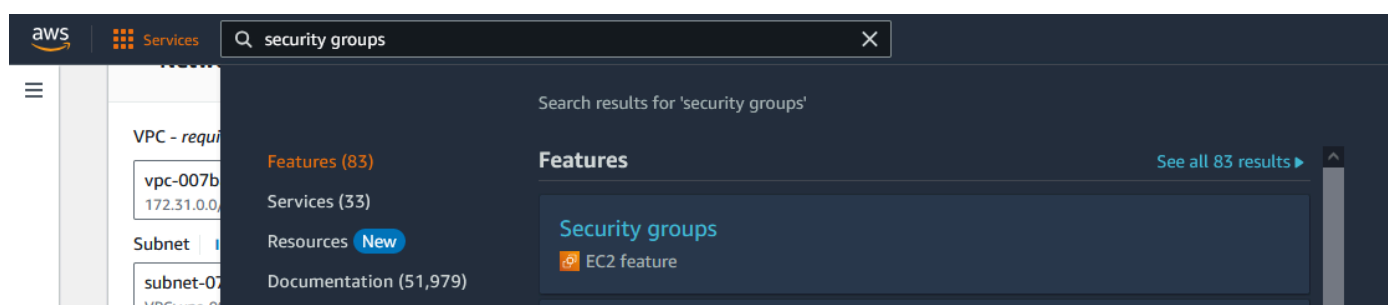
☐ Create security group ☒ Select existing security group

Common security groups | Info

Select security groups

CAB432SG sg-032bd1ff8cf77dbb9 X
VPC: vpc-007bab53289655834

While this panel of the EC2 does not show the rules of the security groups we have chosen, there are others areas that can reveal that information. A quick way to get there is by searching "security groups" in the search bar. Just make sure you open the link in a new tab otherwise you will have to start creating your EC2 instance all over again.



After finding the security groups feature of EC2, search for the SG by its name then investigate the tabs for "Inbound rules" and "Outbound rules".

CAB432SG adds rules that allow most of the traffic that we'll need for the unit:

- SSH and RDP access from the QUT network, including QUT VPN access
- Public internet access to several TCP ports for web traffic (80, 443, 8080, 5000, 3000-3010)
- ICMP (ping) from the QUT network, including QUT VPN access
- All outbound traffic

Step 8. Storage

For this section we will accept the defaults, but read further to understand what these settings are for.

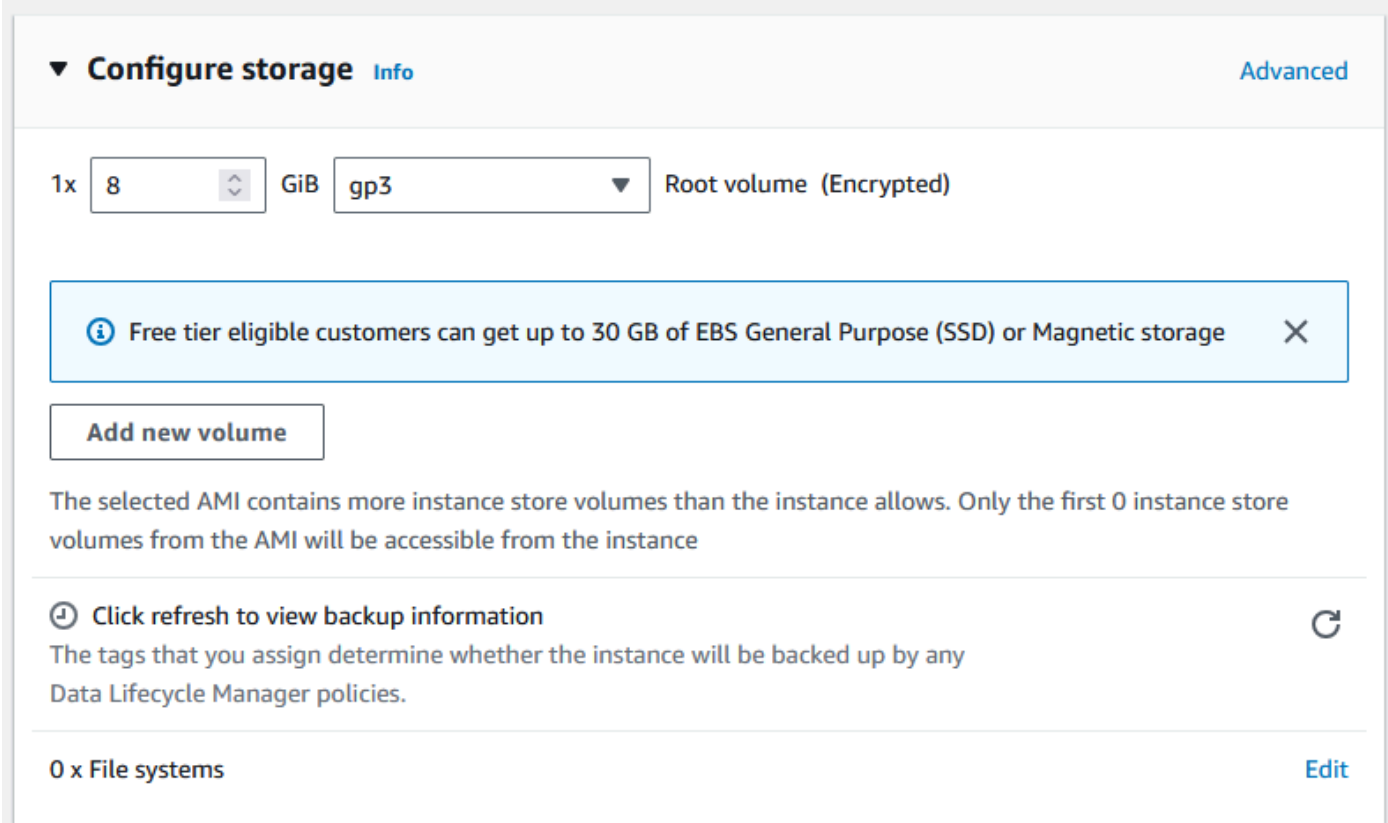
Just as a physical machine, a virtual machine needs secondary storage for persisting data nearby to it.

We will use [AWS Elastic Block Store \(EBS\)](https://aws.amazon.com/ebs/features/). EBS effectively provides virtual storage devices. You can configure the volume size and performance.

Amazon EBS allows you to create storage volumes and attach them to Amazon EC2 instances. Once attached, you can create a file system on top of these volumes, run a database, or use them in any other way you would use block storage.

Source: [AWS Documentation](https://aws.amazon.com/ebs/features/)  (<https://aws.amazon.com/ebs/features/>)

Eight gigabytes would be enough, even if it seems tiny. That would be adequate for this exercise. We do not require a massive data store in many cases, especially if our work is largely about the processing of streaming data or simple content provision. Still, EBS should be seen as a local disk drive rather than as repository, and it will die with the machine later.



The screenshot shows the 'Configure storage' section of the AWS console. At the top, there is a dropdown menu set to '1x' with a value of '8' and a unit of 'GiB'. Next to it is a dropdown menu set to 'gp3'. To the right of these is the text 'Root volume (Encrypted)'. Below this is a light blue informational banner that reads: 'Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage'. Below the banner is a button labeled 'Add new volume'. Further down, there is a message: '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'. Below this message is a section with a refresh icon and the text 'Click refresh to view backup information'. Underneath this is another message: 'The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.' At the bottom of the section, there is a summary row showing '0 x File systems' and an 'Edit' link.

Step 9. Roles and shutdown settings

IAM role

We now must add an IAM role. IAM is [AWS Identity and Access Management](https://aws.amazon.com/iam/getting-started/?nc=sn&loc=3)  (<https://aws.amazon.com/iam/getting-started/?nc=sn&loc=3>).

With IAM, you define who can access what by specifying fine-grained permissions. IAM then enforces those permissions for every request. Access is denied by default and access is granted only when permissions specify an "Allow."

Source: [AWS Documentation](https://aws.amazon.com/iam/getting-started/?nc=sn&loc=3)  (<https://aws.amazon.com/iam/getting-started/?nc=sn&loc=3>)

You will learn more about IAM later in the semester. For now, know that we will use an IAM role that allows the VM to connect to the AWS Systems Manager (SSM) service.

- Click the triangle beside **Advanced details**
- Under **IAM instance profile** choose **CAB432-Instance-Role**

Shutdown settings

An EC2 can exist in the states:

- Pending
- Running
- Stopping
- Shutting-down
- Stopped
- Terminated

You should read about the lifecycle of an EC2 here: [Instance lifecycle](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html) ↗

(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html>)

- Change **Shutdown behaviour** to **terminate**, rather than **stop**.

A terminated instance will be permanently deleted. A stopped instance can be booted again.

▼ **Advanced details** [Info](#)

Domain join directory | [Info](#)

Select ▼

IAM instance profile | [Info](#)

CAB432-Instance-Role
arn:aws:iam::901444280953:instance-profile/CAB432-Instance-Role ▼

Hostname type | [Info](#)

IP name ▼

DNS Hostname | [Info](#)

☒ Enable IP name IPv4 (A record) DNS requests

☐ Enable resource-based IPv4 (A record) DNS requests

☐ Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery | [Info](#)

Select ▼

Shutdown behavior | [Info](#)

Terminate ▼

Step 10. Review settings and launch

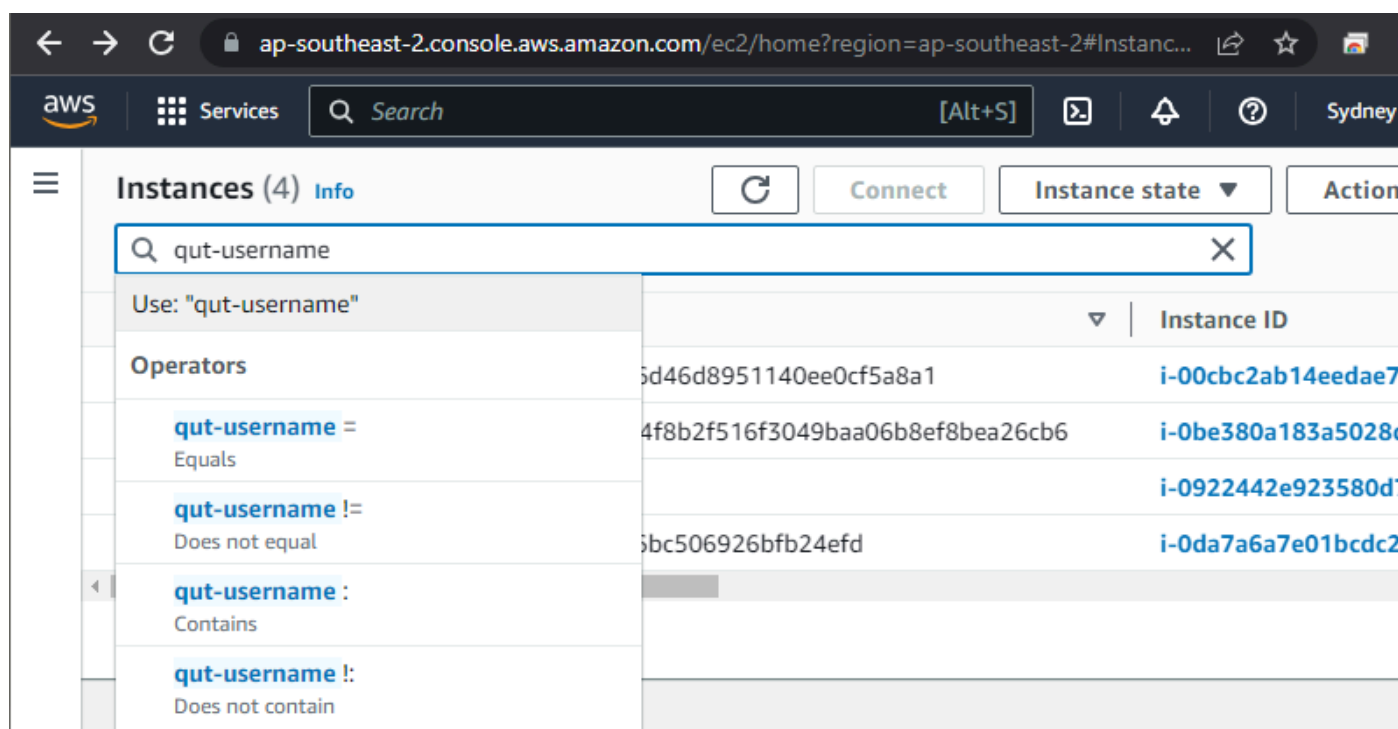
Double check your settings.

In the panel on the right, click the orange button "Launch instance".

Step 11. View EC2 instances

After launching the instance, click "Instances" in the EC2 console navigation bar (left).

You will probably see a long list of instances listed. Filter the list by using your tags. Click on the cog in the top right hand corner, tick the qut-username box on the left & close. Now you can look for your username in the second column.



If you click on the Instance ID for your instance then you will see a lot of information, in particular note:

- **Public DNS** is the DNS address for your EC2 instance that can be used to access it from the public internet. You'll need this to connect to your instance over SSH.

Step 12. Terminating the instance

Even stopped instances continue to incur AWS charges, so when you complete the exercise, terminate the instance. If you are continuing with [Practical: Remotely connecting to an EC2 instance \(https://canvas.qut.edu.au/courses/20367/pages/practical-remotely-connecting-to-an-ec2-instance\)](https://canvas.qut.edu.au/courses/20367/pages/practical-remotely-connecting-to-an-ec2-instance) then you can skip this step for now.

1. Use the Terminate option on the Instance state menu to delete the VM.

While it is possible to keep an instance around for experimenting and development, you should get used to the idea of terminating instance when you are done and creating a new instance when starting something new. This workflow has several advantages, such as always starting with your instance in a known state and reducing costs associated with storing stopped instances. In a later practical we'll see how to use templates to make it easy to create a new instance.

Additional reading

Subnets

We are using public subnets in the three availability zones to provide network address translation, and load balancing services.

What is an Public Subnet?

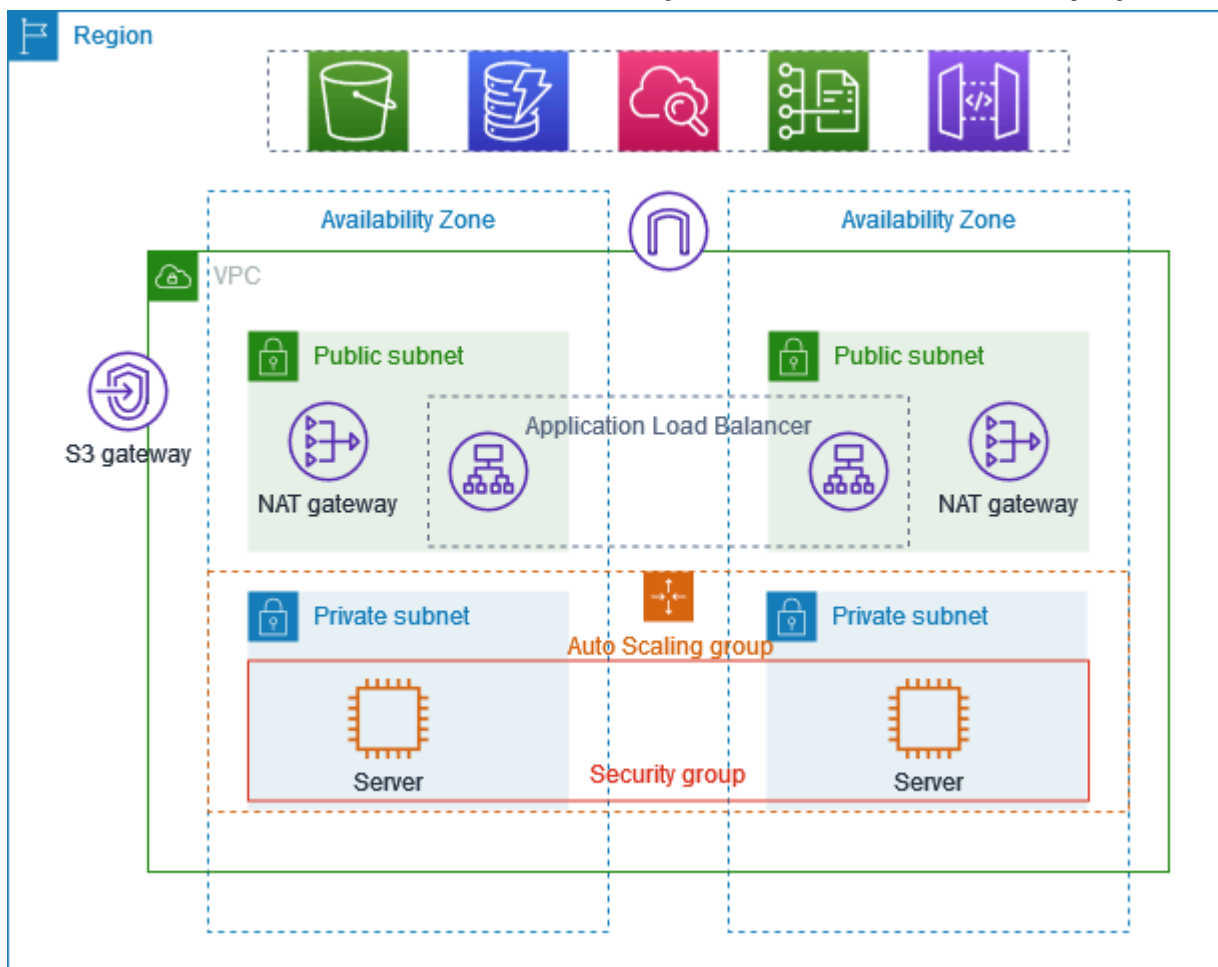
A segment IP addresses within a virtual private cloud that are associated with a route table that can have a direct route to an Internet gateway. This connects the VPC to the Internet and to other AWS services. Things like web servers, where access from users via internet is required will be placed in the public subnet.

In a later prac we will be enabling a simple HTTP web server on this VM so we will need a public IP created for us. Select enable in the drop down.

What is an Private Subnet?

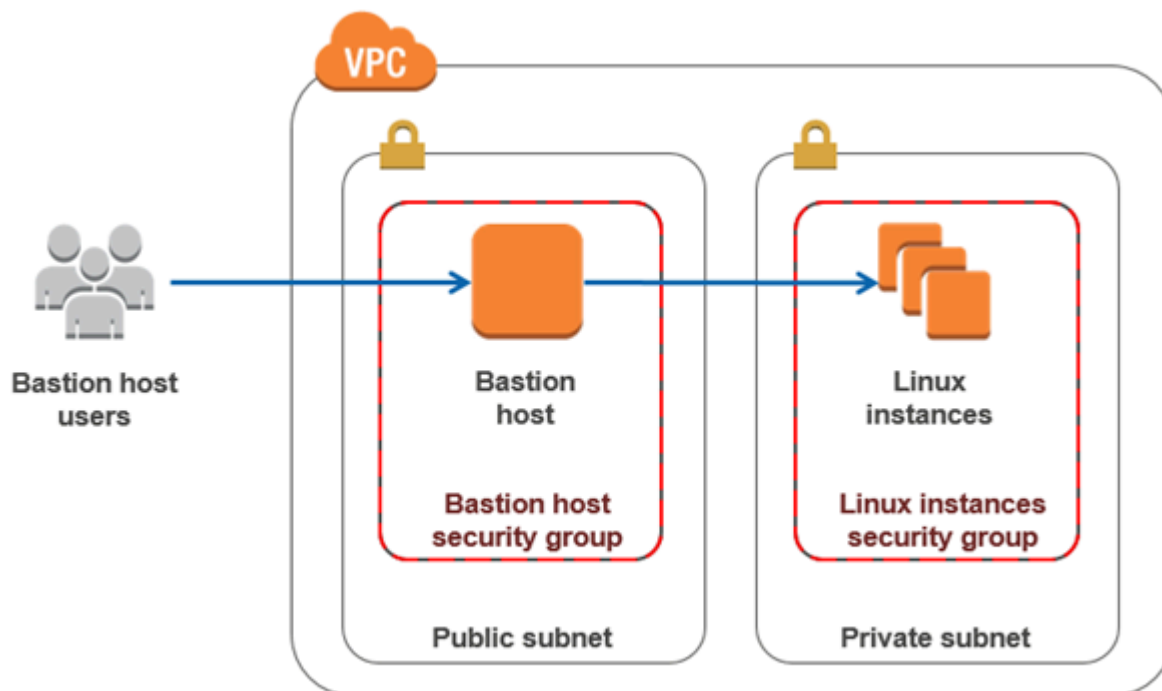
A private subnet is a subnet that is associated with a route table that does not have a route to an internet gateway. Instances in the private subnet are backend servers they do not accept the traffic from the internet. EC2 instances, web apps, databases and other compute environments may exist within private subnets. They cannot send outbound traffic directly to the Internet. That can only be done via a Network Address Translation (NAT) Gateway in the public subnet.

The following diagram provides an overview between how private and public subnets are used together. The VPC has public subnets and private subnets in two Availability Zones. Each public subnet contains a NAT gateway and a load balancer node. The servers run in the private subnets, are launched and terminated by using an Auto Scaling group, and receive traffic from the load balancer. The servers can connect to the internet by using the NAT gateway. The servers can connect to Amazon S3 by using a gateway VPC endpoint.



Bastion Host

If we need to access private resources from the internet, we can deploy bastion hosts to provide temporary and/or limited access to these resources within a Virtual Private Cloud (VPC). Bastion hosts, typically positioned in public subnets, are fortified with robust security controls. They act as "jump" boxes, facilitating secure access to the private resources without exposing them directly to the internet.



Security Groups

For most of what we're doing in CAB432 we'll be using :

- **CAB432SG**

These provide a default list of ports for EC2 instances to provide connectivity to the EC2 instance via Systems Manager / Sessions Manager.

What is a Security Group?

A security group acts as a virtual firewall for your EC2 instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC can be assigned to a different set of security groups.

If you launch an instance, it is automatically assigned to the default security group for the VPC. If you launch an instance using the Amazon EC2 console, you have an option to create a new security group for the instance or utilise a defined security group for the workload.

For each security group, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.

Common errors

Error 1: Cannot find instance post deployment/access.

- Please ensure you have South East Asia (Sydney) selected as your region. If you are still having issues please contact your instructor.

Error 2: Deployments are failing

- Please ensure you have South East Asia (Sydney) selected as your region. If you are still having issues please contact your instructor.
- Ensure you pick t3 micro instance size. Only certain sizes of VM's are allowed.
- Subnet - You must choose one of the public subnets
- IAM role issue - You must choose the IAM role **CAB432-Instance-Role**

Lights-out policy

The CAB432 AWS account has a lights-out policy for EC2 instances. All EC2 instance will be stopped (not terminated) at 3am every day. If you are no longer using an instance please terminate it, even if it is stopped, as there is still a charge for stopped EC2 instances.

TEQSA PRV12079 | CRICOS 00213J | ABN 83 791 724 622