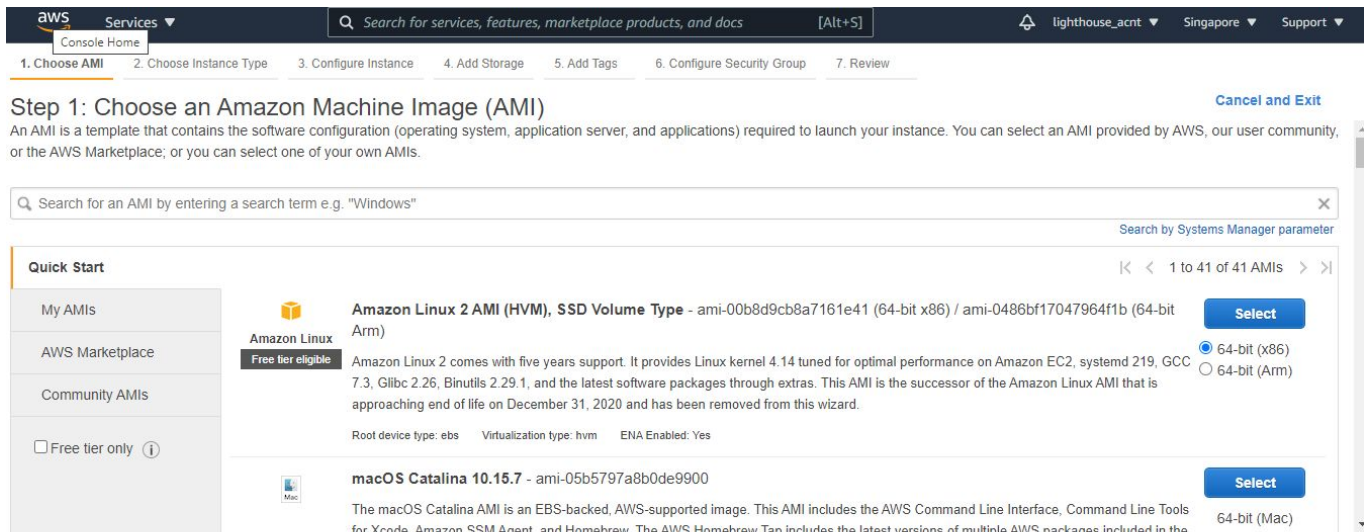


Week 1 Lab

Launch EC2 - make it web server

Step 1: Go to the Launch page in the console after selecting the region. Select Ubuntu AMI



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Search for an AMI by entering a search term e.g. "Windows"

Search by Systems Manager parameter

Quick Start

My AMIs

AWS Marketplace

Community AMIs

☐ Free tier only ⓘ

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-00b8d9cb8a7161e41 (64-bit x86) / ami-0486bf17047964f1b (64-bit Arm)

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.

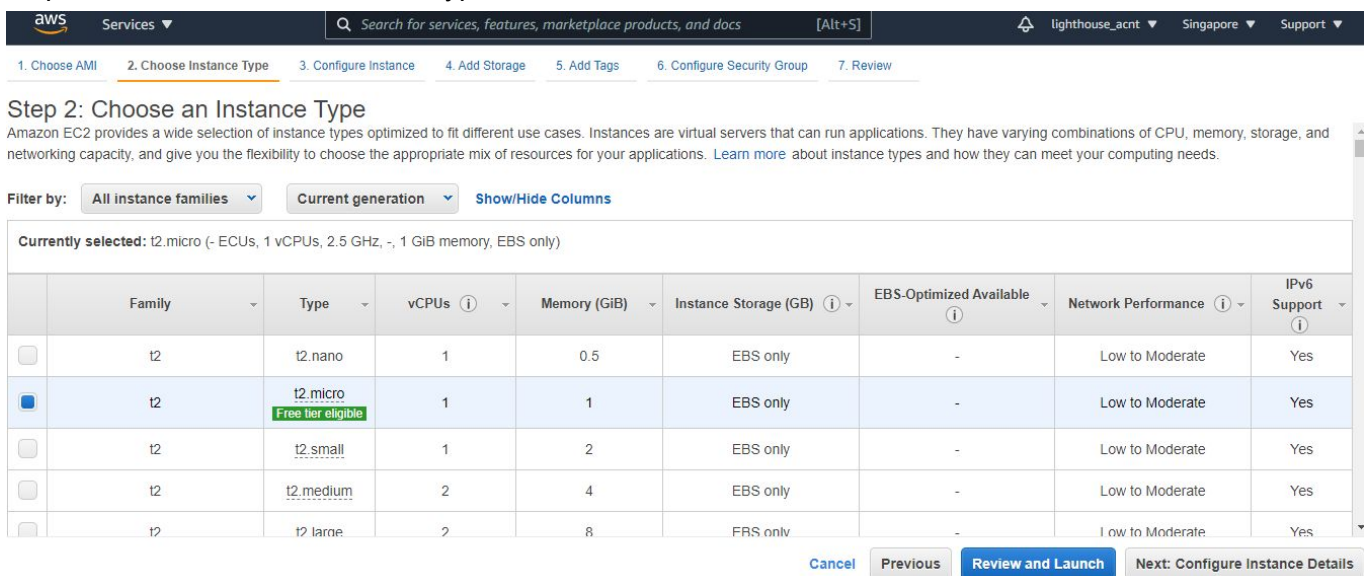
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

macOS Catalina 10.15.7 - ami-05b5797a8b0de9900

The macOS Catalina AMI is an EBS-backed, AWS-supported image. This AMI includes the AWS Command Line Interface, Command Line Tools for Xcode, Amazon SSM Agent, and Homebrew. The AWS Homebrew Tap includes the latest versions of multiple AWS packages included in the

64-bit (x86) ☒ 64-bit (Arm) ☐ 64-bit (Mac) ☐

Step 2: Use the free tier instance type



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 families Current generation Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

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

Cancel Previous **Review and Launch** Next: Configure Instance Details

Step 3: Use the default VPC and change the subnet to **1a**. Remaining can be left as default.

Step 3: Configure Instance Details

Purchasing option ⓘ ☐ Request Spot instances

Network ⓘ vpc-8bb953ed (default) Create new VPC

Subnet ⓘ subnet-fa17c89c | Default in ap-southeast-1a Create new subnet
4091 IP Addresses available

Auto-assign Public IP ⓘ Use subnet setting (Enable)

Placement group ⓘ ☐ Add instance to placement group

Capacity Reservation ⓘ Open

Domain join directory ⓘ No directory Create new directory

IAM role ⓘ None Create new IAM role

CPU options ⓘ ☐ Specify CPU options

Cancel Previous **Review and Launch** Next: Add Storage

Step 4: Default EBS volume of 8GiB is sufficient.

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-0e99f1c66c03daf7c	8	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 5: Add the name tag for server identification

aws Services Search for services, features, marketplace products, and docs [Alt+S] lighthouse_acnt Singapore 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
Name	Web server 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

Step 6: By default a security group is created with port 22 open to the public.

aws Services Search for services, features, marketplace products, and docs [Alt+S] lighthouse_acnt Singapore 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: launch-wizard-1

Description: launch-wizard-1 created 2021-01-08T15:38:38.742+05:30

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

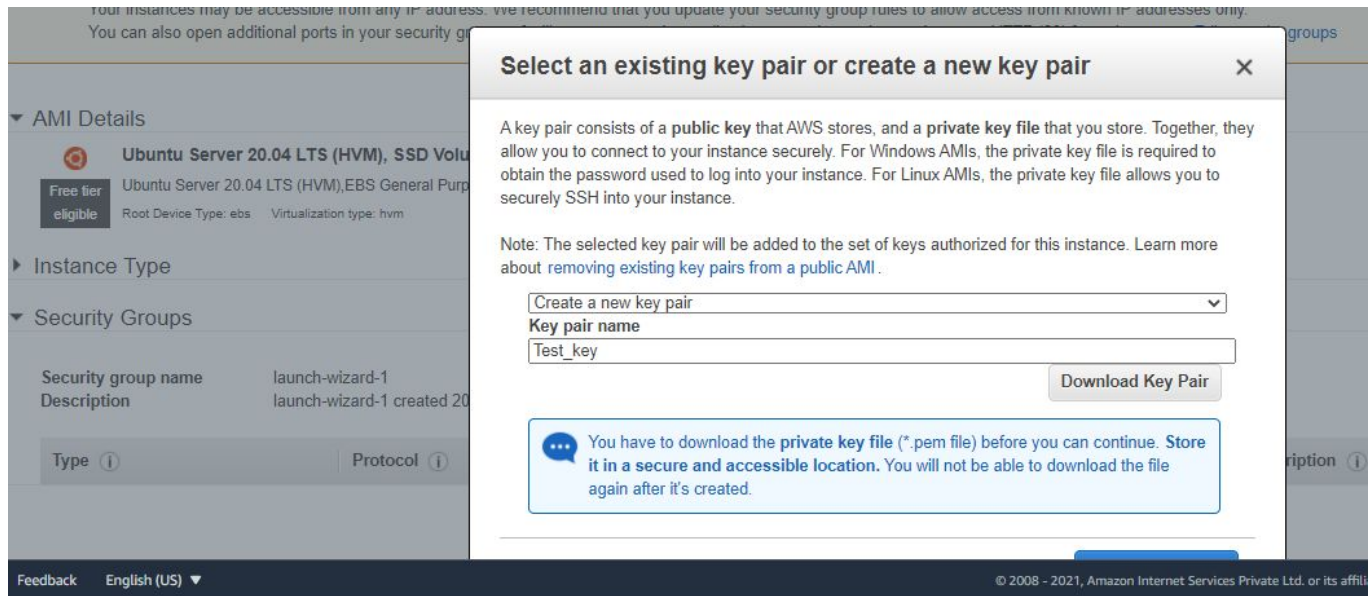
[Add Rule](#)

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](#)

PG Program in Cloud Computing

Step 7: Review the configuration - Click Launch->Create a new key-pair and download it before launching the instance.



Test_key.pem

From windows system, if no other SSH client is present use the chrome extension



chrome web store



[Redacted]

Home > Apps > Secure Shell App



Secure Shell App

Launch app

Offered by: Google Secure Shell Developers

★★★★★ 3,139 | Extensions | 800,000+ users

By Google | Runs offline

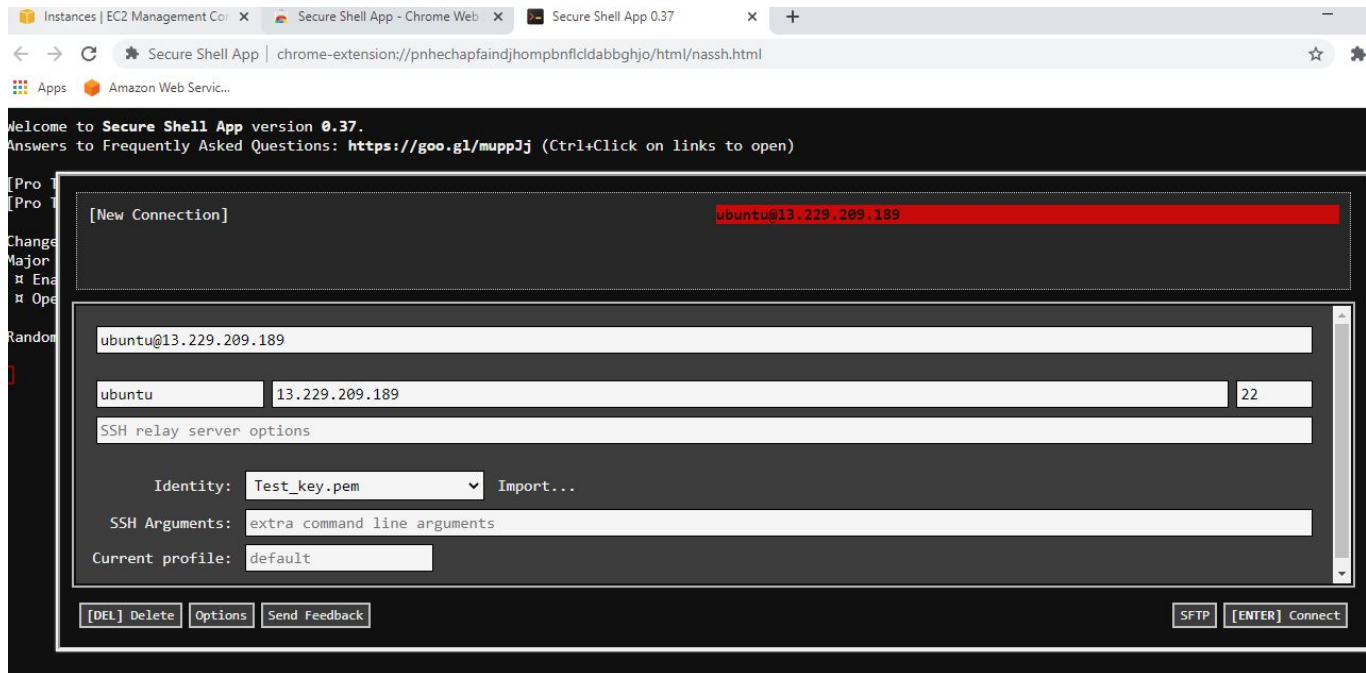
Overview

Reviews

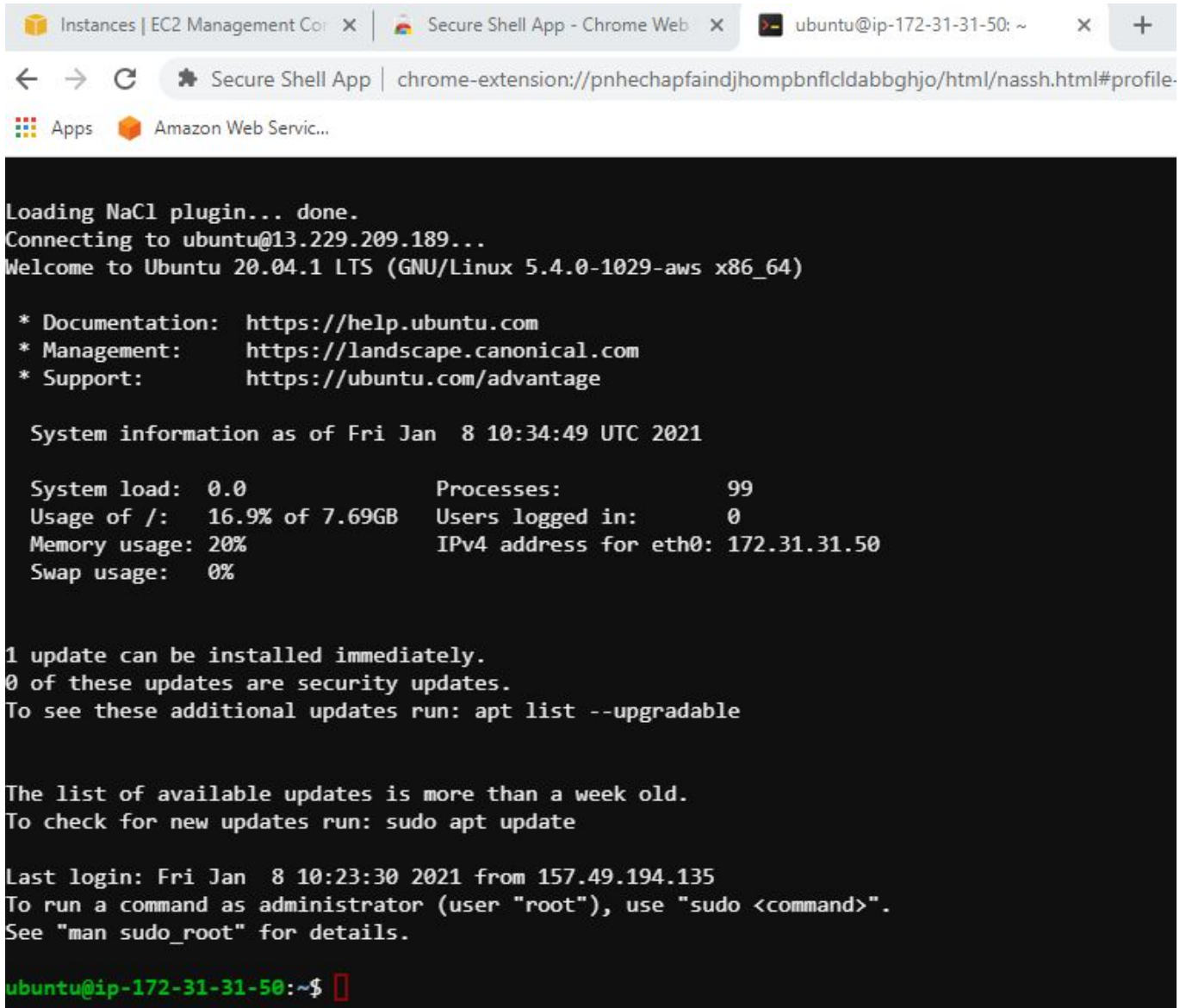
Support

Related

Input the launched EC2 server IP, username as 'ubuntu'(Default username for ubuntu AMIs)
Amazon AMI's have 'ec2-user' as a username.
In identity, map the downloaded .pem file. Connect



PG Program in Cloud Computing



```

Loading NaCl plugin... done.
Connecting to ubuntu@13.229.209.189...
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-1029-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri Jan  8 10:34:49 UTC 2021

System load:  0.0           Processes:            99
Usage of /:   16.9% of 7.69GB Users logged in:       0
Memory usage: 20%          IPv4 address for eth0: 172.31.31.50
Swap usage:   0%

1 update can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Jan  8 10:23:30 2021 from 157.49.194.135
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-31-50:~$

```

Once connected install httpd(apache2) by using the following commands

sudo apt update

sudo apt-get install apache2

Check the status with -> **sudo service apache2 status**

PG Program in Cloud Computing

```
ubuntu@ip-172-31-31-50:~$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-01-08 10:46:24 UTC; 1min 35s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2943 (apache2)
    Tasks: 55 (limit: 1164)
   Memory: 5.3M
   CGroup: /system.slice/apache2.service
           └─2943 /usr/sbin/apache2 -k start
             └─2945 /usr/sbin/apache2 -k start
               └─2946 /usr/sbin/apache2 -k start

Jan 08 10:46:24 ip-172-31-31-50 systemd[1]: Starting The Apache HTTP Server...
Jan 08 10:46:24 ip-172-31-31-50 systemd[1]: Started The Apache HTTP Server.
ubuntu@ip-172-31-31-50:~$
```

Go to the Security groups menu in the Network tab on the left pane in the console.
Create a new security group with ports 22 for SSH and port 80 for http.

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](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
SSH	TCP	22	Custom <input type="text" value="0.0.0.0/0"/>	<input type="text"/>	Delete
HTTP	TCP	80	Custom <input type="text" value="0.0.0.0/0"/>	<input type="text"/>	Delete

Now from EC2 console page go to Actions->Security->Change Security group
Remove the old one and add the newly created group

The screenshot shows the AWS Management Console interface for the 'Change security groups' page of an EC2 instance. The breadcrumb trail at the top reads: EC2 > Instances > i-0ae1f9c1bdd84d2fb > Change security groups. The page title is 'Change security groups' with an 'Info' link. A descriptive paragraph states: 'Amazon EC2 evaluates all the rules of the selected security groups to control inbound and outbound traffic to and from your instance. You can use this window to add and remove security groups.'

Instance details

Instance ID i-0ae1f9c1bdd84d2fb (Web server 1)	Network interface ID eni-00e1e93d46d72e1e5
---	---

Associated security groups
Add one or more security groups to the network interface. You can also remove security groups.

Search bar:

Security groups associated with the network interface (eni-00e1e93d46d72e1e5)

Security group name	Security group ID	
webserver-test-group	sg-04d89ce460a2eaa9c	<input type="button" value="Remove"/>

At the bottom right, there are 'Cancel' and 'Save' buttons.

After enabling ec2 with a new security group, use the ec2 public IP on the browser tab to view the apache's default page.

Instances | EC2 Management Console | Secure Shell App - Chrome Web... | root@ip-172-31-31-50: /home/u... | Apache2 Ubuntu Default Page: It works! | +

← → ↻ ⚠ Not secure | 13.229.209.189

Apps Amazon Web Service...

Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

.Execute the command to change your default html page by running the following command:
`sudo echo "Web server 1" > /var/www/html/index.html`

Instances | x | Secure Shell | x | root@ip-17 | x | 13.229.209 | x

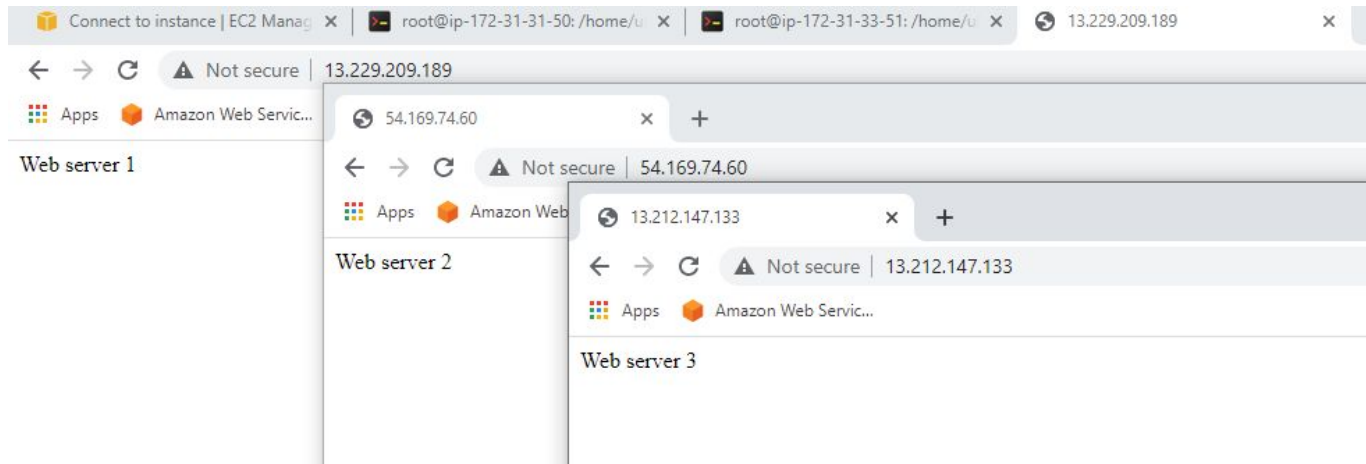
← → ↻ ⚠ Not secure | 13.229.209.189

Apps Amazon Web Service...

Web server 1

PG Program in Cloud Computing

Launch web server 2,3 and setup /health.html

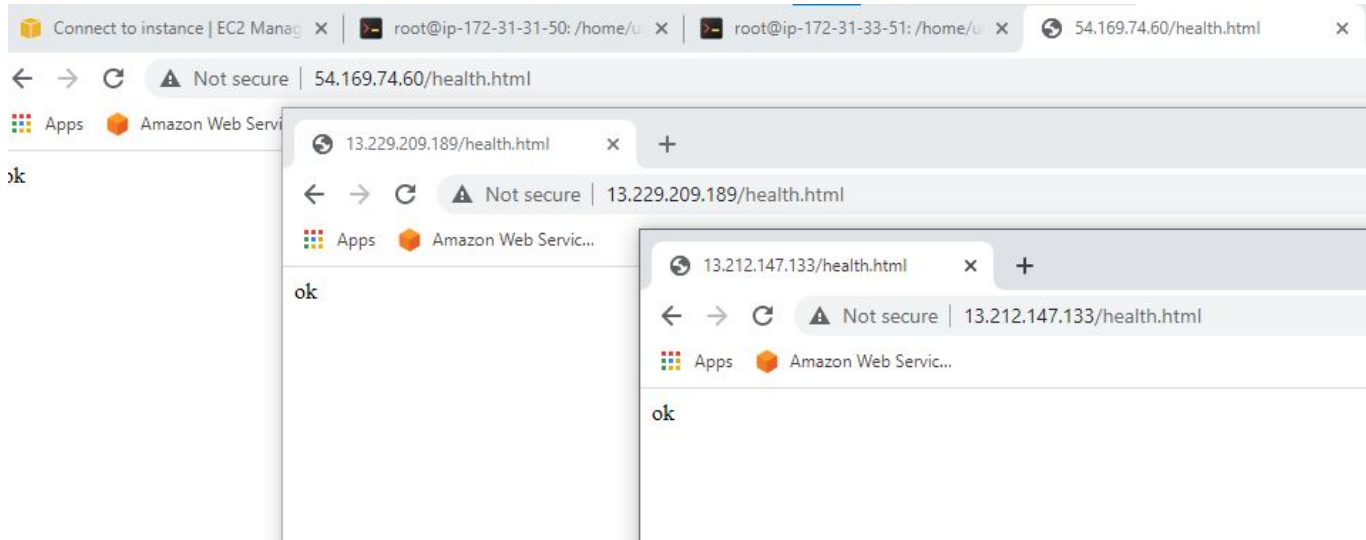


Along with index.html

create another page health.html in all the server.

echo "ok" > /var/www/html/health.html

use 'sudo su' before creating html files



PG Program in Cloud Computing

Load Balancer creation:

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 1: Configure Load Balancer

Add listener

Availability Zones

Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify the availability of your load balancer.

VPC	<input type="checkbox"/>	vpc-8bb953ed (172.31.0.0/16) (default)
Availability Zones	<input checked="" type="checkbox"/>	ap-southeast-1a
		subnet-fa17c89c
		IPv4 address Assigned by AWS
	<input checked="" type="checkbox"/>	ap-southeast-1b
		subnet-c6ca058e
		IPv4 address Assigned by AWS
	<input checked="" type="checkbox"/>	ap-southeast-1c
		subnet-f39a10aa
		IPv4 address Assigned by AWS

Add-on services

Additional AWS services can be integrated with this load balancer at launch when you enable them below. You can also add these and other services at any time.

☐ AWS Global Accelerator ☐ Create an accelerator to get static IP addresses and improve the performance and availability of your applications.

Configure a new security group with only 80 port open.

Configure health.html to health check parameter:

Services ▾

Search for services, features, marketplace products, and docs [Alt+S]

1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
5. Register Targets
6. Review

Step 4: Configure Routing

Protocol version ⓘ

☒ HTTP1

Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

☐ HTTP2

Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.

☐ gRPC

Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Health checks

Protocol ⓘ

HTTP

Path ⓘ

/health.html

Advanced health check settings

Port ⓘ

☒ traffic port

☐ override

Healthy threshold ⓘ

5

Unhealthy threshold ⓘ

2

Timeout ⓘ

5 seconds

Interval ⓘ

30 seconds

Success codes ⓘ

200

Register all the targets:

Services ▾

Search for services, features, marketplace products, and docs [Alt+S]

lighthouse_acnt

1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
5. Register Targets
6. Review

Step 5: Register Targets

Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health check.

Registered targets

To deregister instances, select one or more registered instances and then click Remove.

Remove

<input type="checkbox"/>	Instance ▾	Name ▾	Port ▾	State ▾	Security groups ▾	Zone ▾
<input type="checkbox"/>	i-0ae1f9c1bdd84d2fb	Web server 1	80	running	webserver-test-group	ap-southeast-1a
<input type="checkbox"/>	i-09592ad40548c8ce8	Web server 2	80	running	webserver-test-group	ap-southeast-1b
<input type="checkbox"/>	i-089dc356bb352ce5a	Web server 3	80	running	webserver-test-group	ap-southeast-1c

Instances

To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

Add to registered
 on port 80

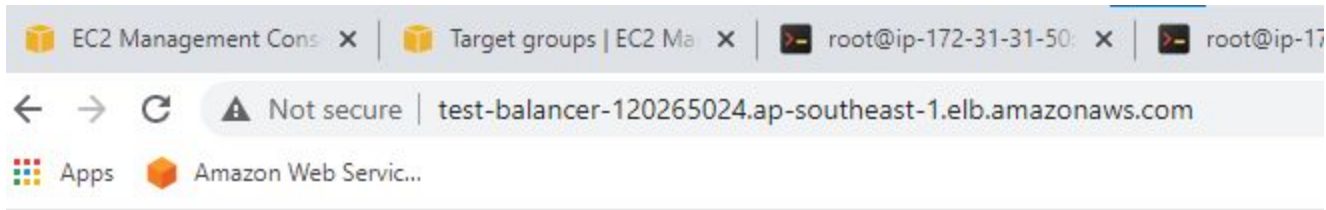
Search Instances X

<input type="checkbox"/>	Instance ▾	Name ▾	State ▾	Security groups ▾	Zone ▾	Subnet ID ▾	Subnet CIDR ▾
<input type="checkbox"/>	i-0ae1f9c1bdd84d2fb	Web server 1	running	webserver-test-group	ap-southeast-1a	subnet-fa17c89c	172.31.16.0/20
<input type="checkbox"/>	i-09592ad40548c8ce8	Web server 2	running	webserver-test-group	ap-southeast-1b	subnet-c8ca058e	172.31.32.0/20
<input type="checkbox"/>	i-089dc356bb352ce5a	Web server 3	running	webserver-test-group	ap-southeast-1c	subnet-f39a10aa	172.31.0.0/20

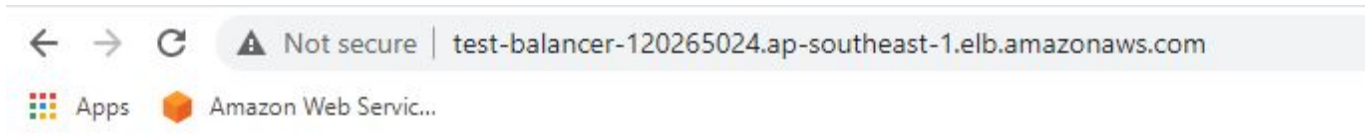
Cancel

PG Program in Cloud Computing

Use the DNS name of the load balancer and refresh the page. We should be able to see all 3 web servers in rotation.

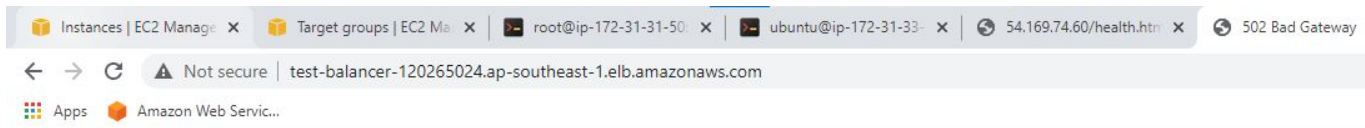


Web server 2



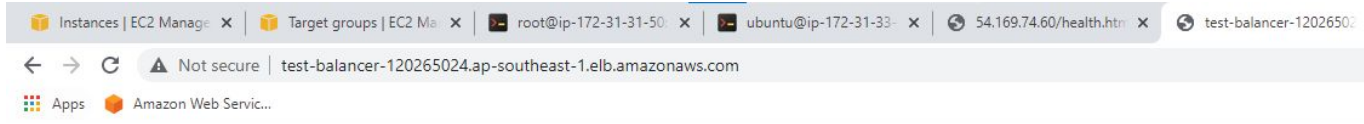
Web server 3

Now take down one server and try to refresh. In between times when ELB is checking the health status of the failed server it still redirects to the failed server. Showing us a bad gateway error.



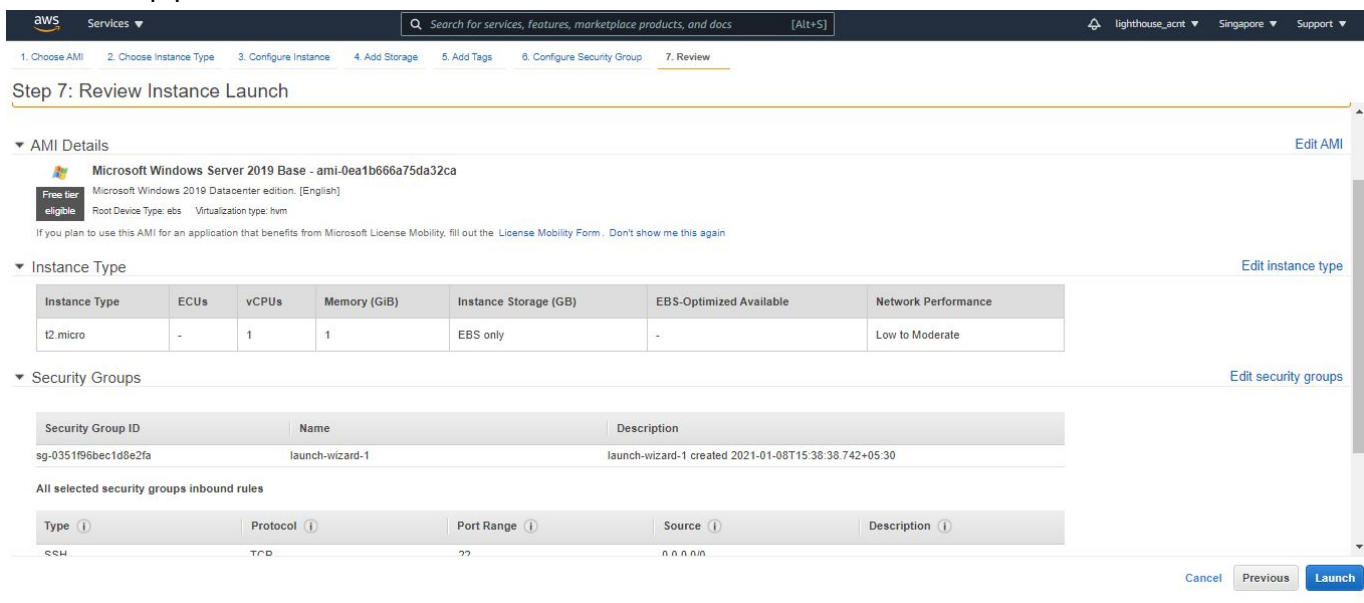
502 Bad Gateway

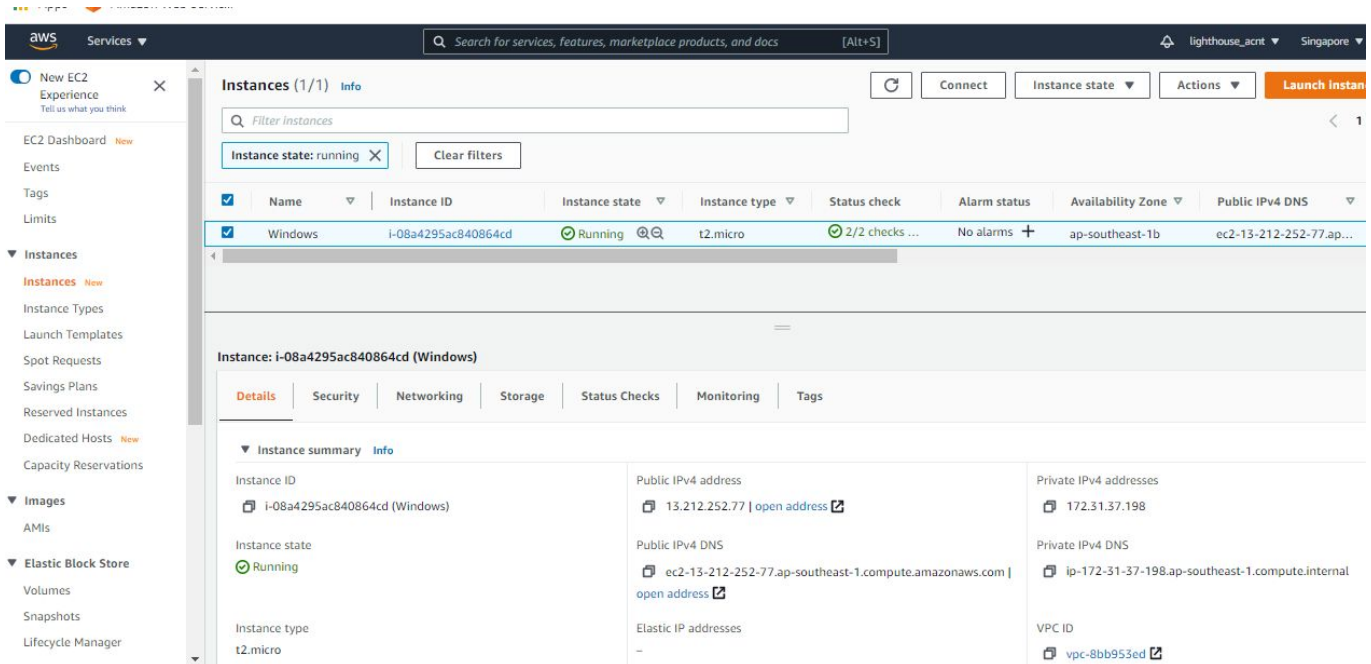
When ELD discovers the health status of one server is bad, then it redirecting to only the working instances



Launching a Windows instance and logging in with RDP

Same 7 step process with Windows AMI





The screenshot shows the AWS Management Console 'Instances' page. The instance 'i-08a4295ac840864cd' is in the 'Running' state. The 'Details' tab is selected, showing instance summary information.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Windows	i-08a4295ac840864cd	Running	t2.micro	2/2 checks ...	No alarms	ap-southeast-1b	ec2-13-212-252-77.ap...

Instance: i-08a4295ac840864cd (Windows)

Details | Security | Networking | Storage | Status Checks | Monitoring | Tags

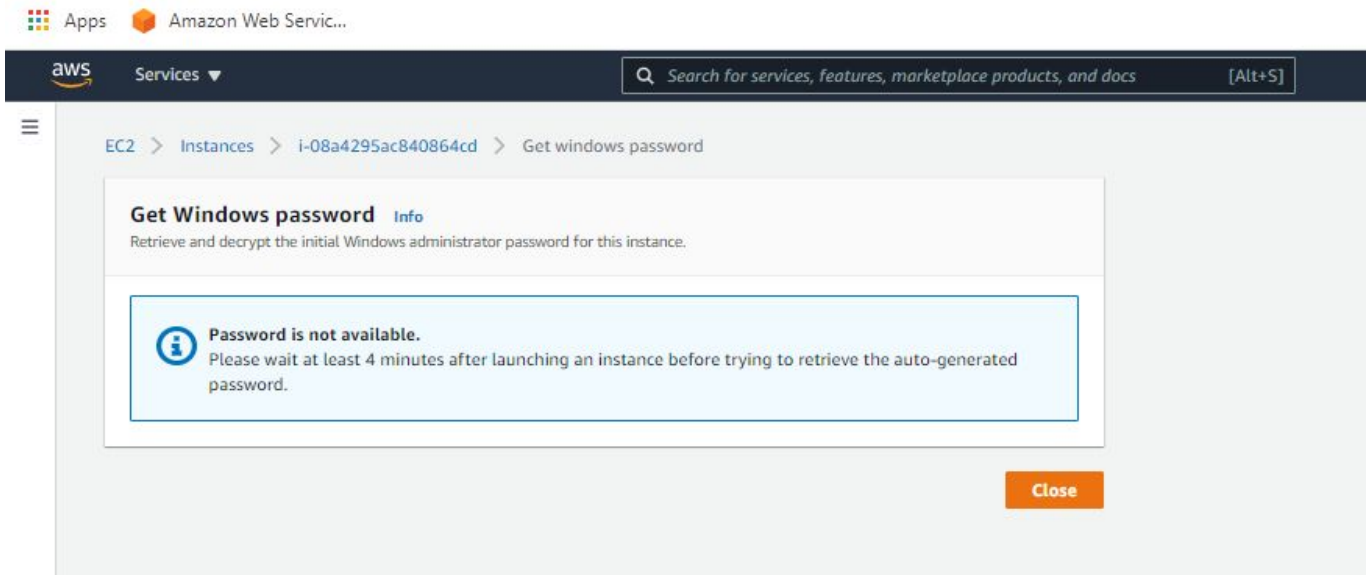
Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-08a4295ac840864cd (Windows)	13.212.252.77 open address	172.31.37.198

Instance state	Public IPv4 DNS	Private IPv4 DNS
Running	ec2-13-212-252-77.ap-southeast-1.compute.amazonaws.com open address	ip-172-31-37-198.ap-southeast-1.compute.internal

Instance type	Elastic IP addresses	VPC ID
t2.micro	-	vpc-8bb953ed

Need to wait for 4 mins after launching to get the password



The screenshot shows the AWS Management Console 'Get Windows password' page. A message states: 'Password is not available. Please wait at least 4 minutes after launching an instance before trying to retrieve the auto-generated password.'

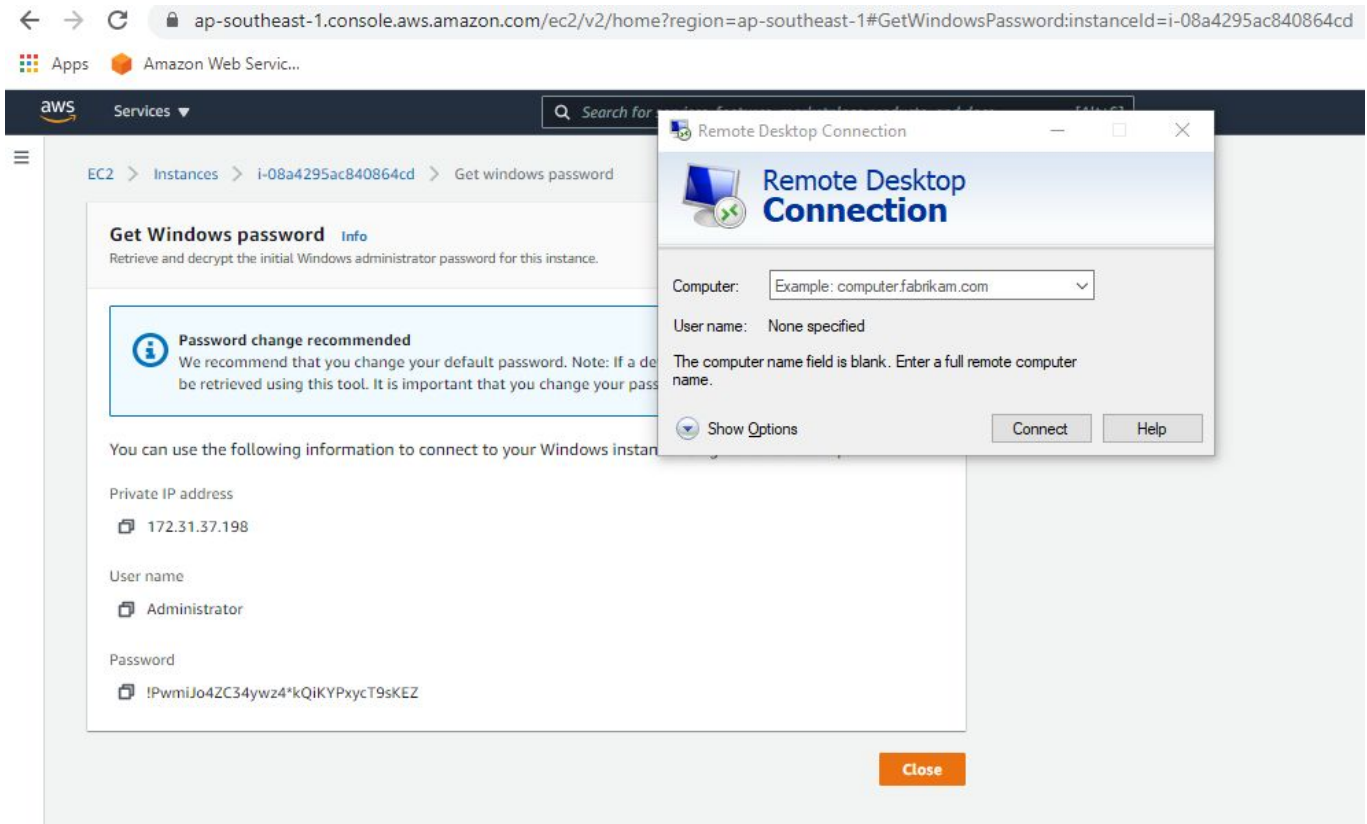
Get Windows password Info

Retrieve and decrypt the initial Windows administrator password for this instance.

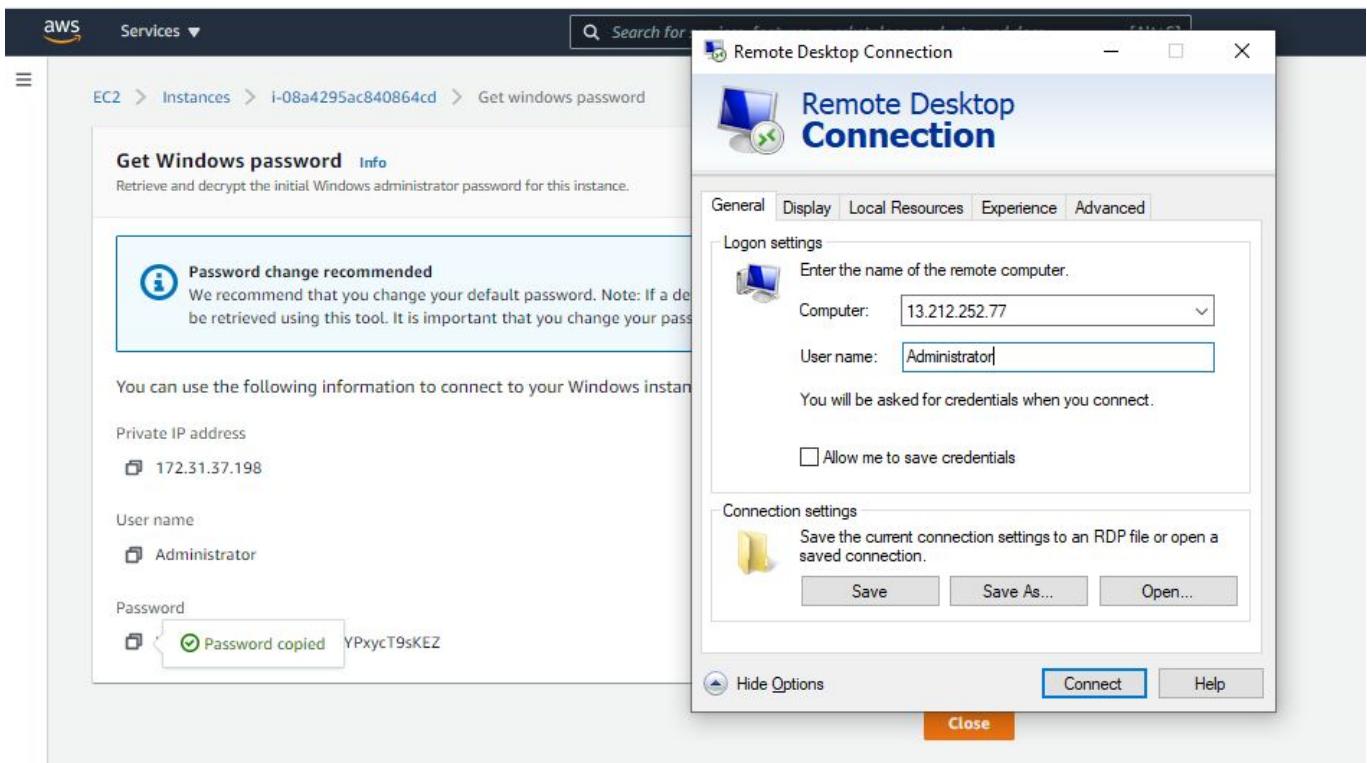
Password is not available.
Please wait at least 4 minutes after launching an instance before trying to retrieve the auto-generated password.

[Close](#)

Get the password from the console with the help of the pem file.
Actions->Security->Get Windows Password
Open the "Remote desktop connection" application of windows.

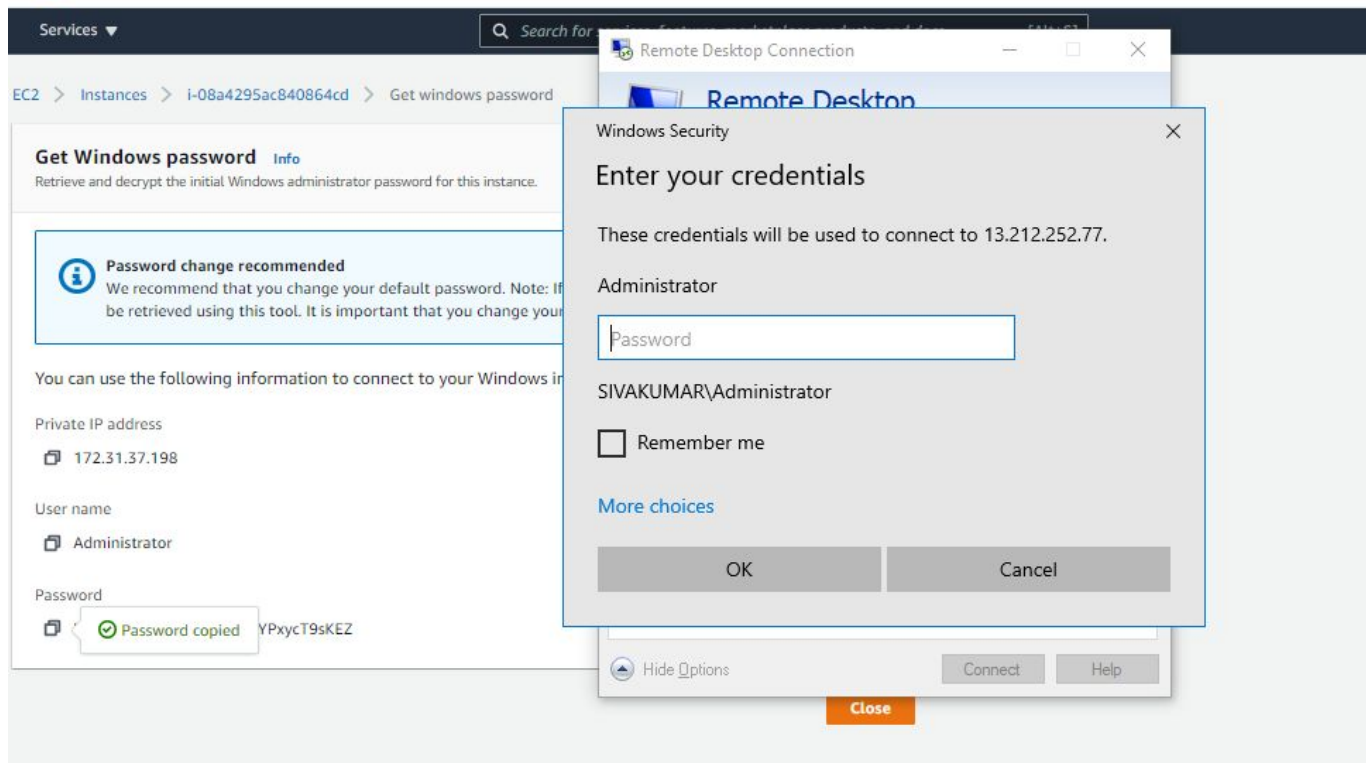


Use the public IP of the server not the private IP.

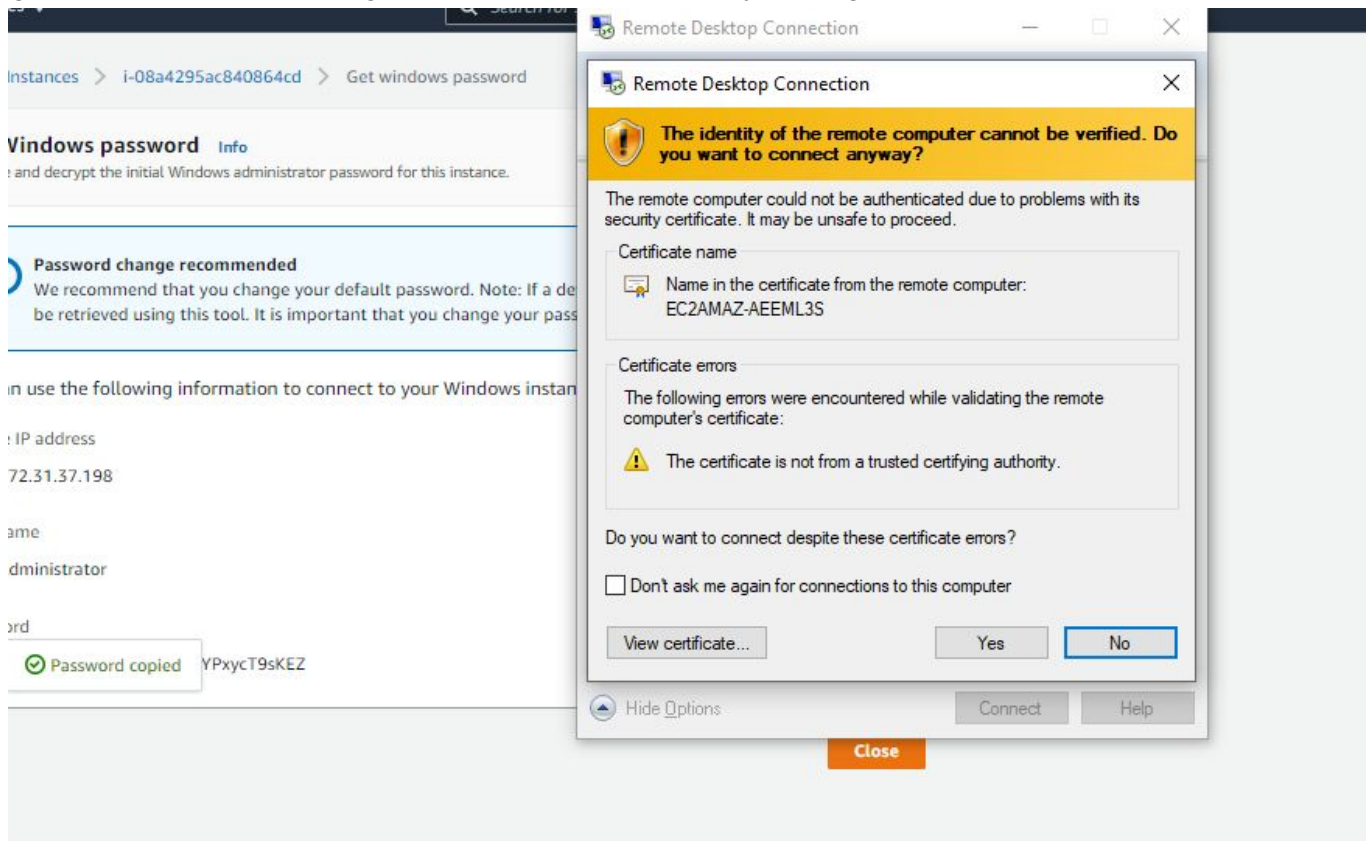


PG Program in Cloud Computing

Once the server is discovered it asks for the password.



Ignore the certificate warning and connect to the server by clicking 'Yes'



After connecting to the remote Windows server.

