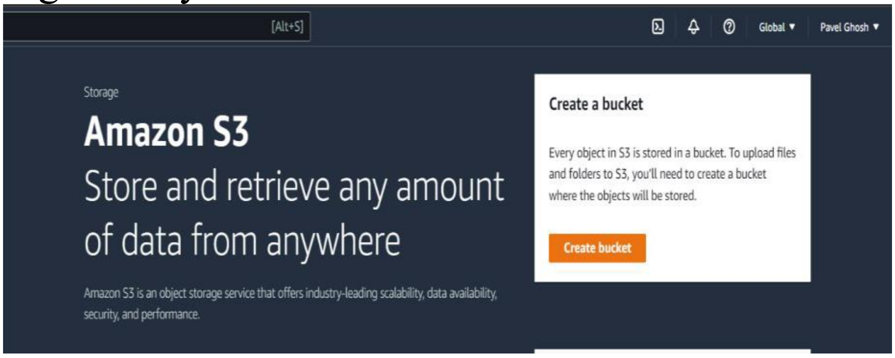
Assignment 7

Problem Statement: Host a website on EC2 service of AWS.
Procedure:

1. Sign in to your **AWS account** as root user.



Storage

Amazon S3

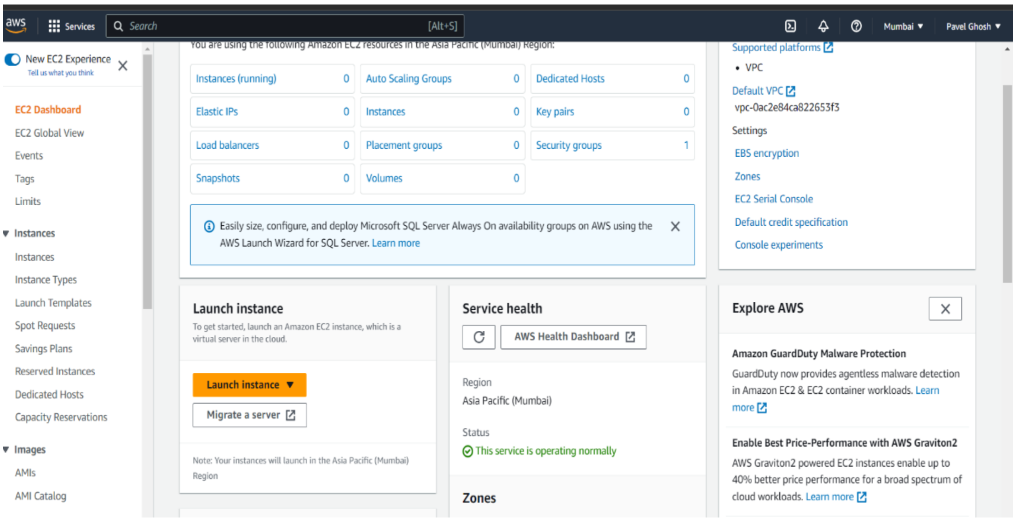
Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

2. Search for EC2 then click on the Launch Instance button. A dropdown appears, from which select Launch Instance.



You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:

Instances (running)	0	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0	Key pairs	0
Load balancers	0	Placement groups	0	Security groups	1
Snapshots	0	Volumes	0		

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more

Supported platforms
- VPC

Default VPC
vpc-0ac2e84ca822653f3

Settings
EBS encryption
Zones
EC2 Serial Console
Default credit specification
Console experiments

Launch instance
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the Asia Pacific (Mumbai) Region

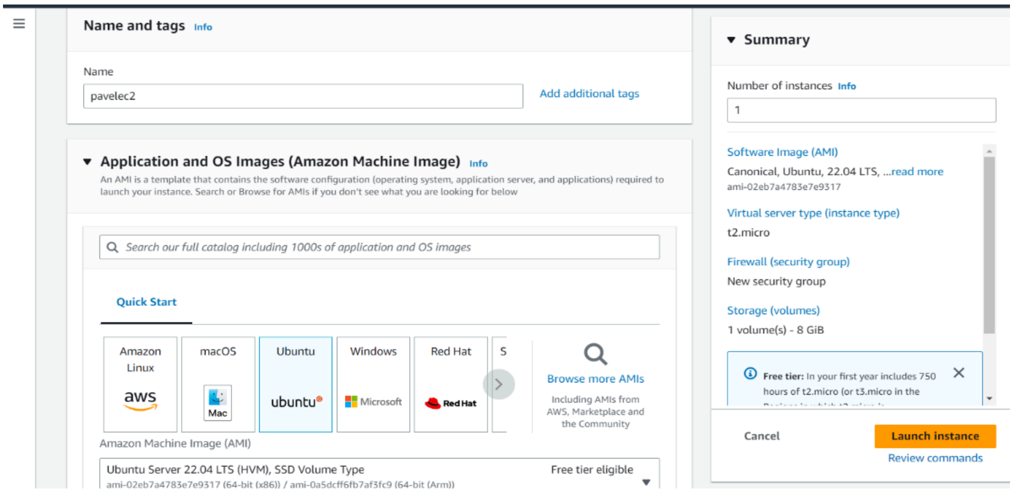
Service health
Region
Asia Pacific (Mumbai)
Status
This service is operating normally

Zones

Amazon GuardDuty Malware Protection
GuardDuty now provides agentless malware detection in Amazon EC2 & EC2 container workloads. Learn more

Enable Best Price-Performance with AWS Graviton2
AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads. Learn more

3. On the new window that opens, set a name for the instance, and select the Ubuntu platform.



Name and tags

Name: pavelec2

Application and OS Images (Amazon Machine Image)

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

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)
Ubuntu Server 22.04 LTS (HVM), SSD Volume Type — Free tier eligible
ami-02eb7a4783e7e9317 (64-bit (x86)) / ami-0a5dcff6fb7af3fc9 (64-bit (Arm))

Summary

Number of instances: 1

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-02eb7a4783e7e9317

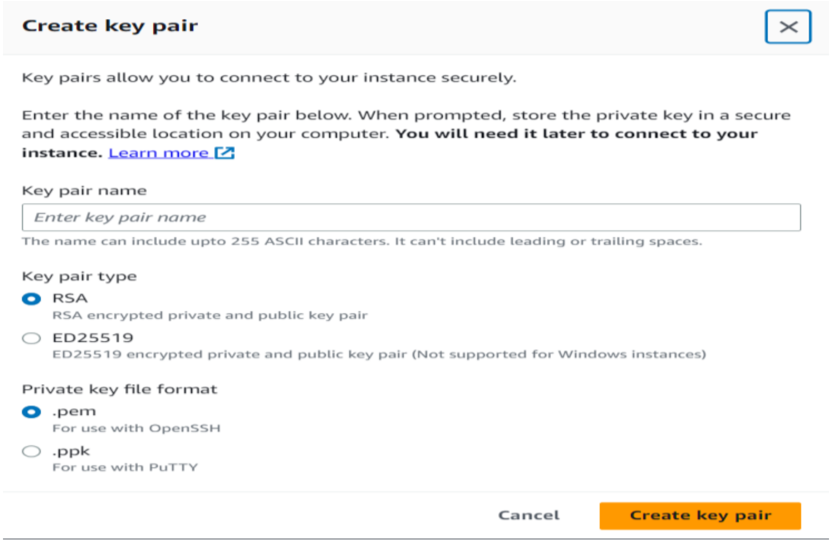
Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the

4. Create a new key pair, if does not exist already. For this click on Create new key pair.



Create key pair

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** Learn more

Key pair name

Enter key pair name

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

Key pair type

● RSA
RSA encrypted private and public key pair

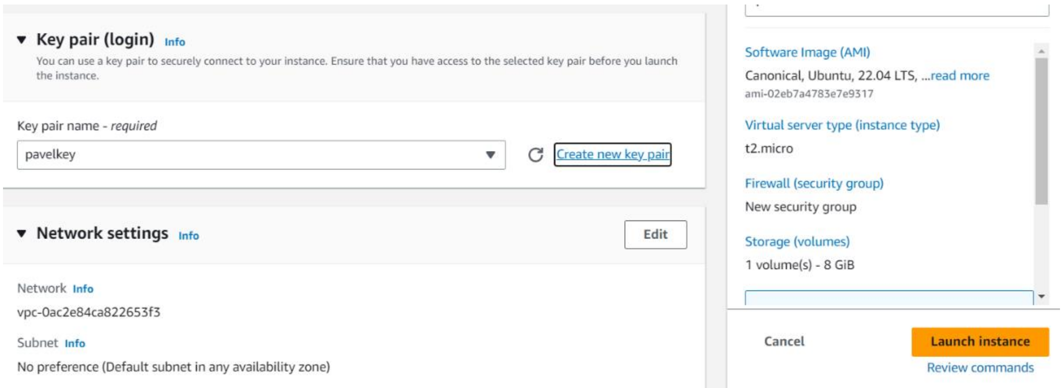
○ ED25519
ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

● .pem
For use with OpenSSH

○ .ppk
For use with PuTTY

5. The new popup appears, where we enter the name of the key pair, and leave all other options default (RSA security option, and the '.pem' extension).Then click on the Create key pair button. Save the file in some directory on your computer.



Key pair (login) Info

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*

pavelkey

Network settings Info

Network Info
vpc-0ac2e84ca822653f3

Subnet Info
No preference (Default subnet in any availability zone)

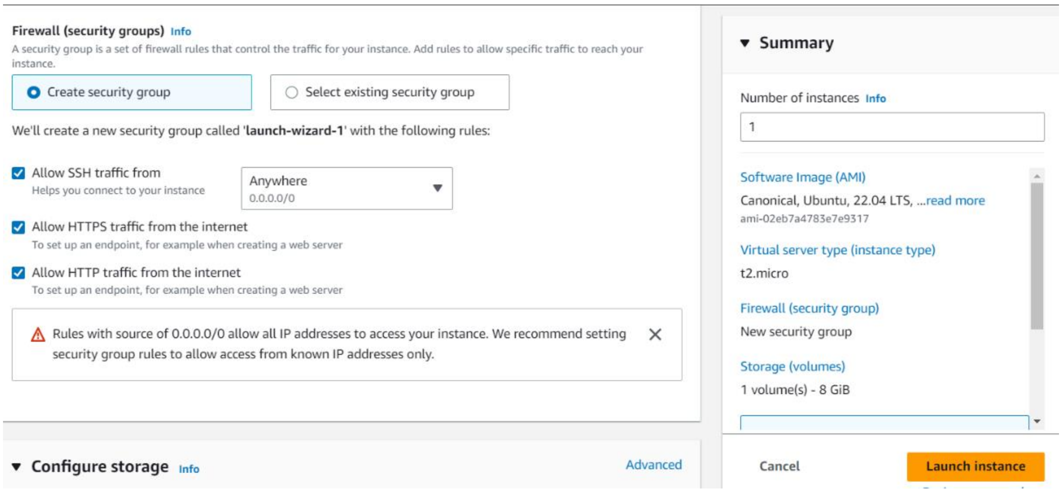
Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-02eb7a4783e7e9317

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

6. Then check all the checkboxes, in the firewall settings.



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

We'll create a new security group called **'launch-wizard-1'** with the following rules:

☑ Allow SSH traffic from
Helps you connect to your instance

Anywhere
0.0.0.0/0

☑ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☑ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

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.

Configure storage Info

Summary

Number of instances Info

1

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-02eb7a4783e7e9317

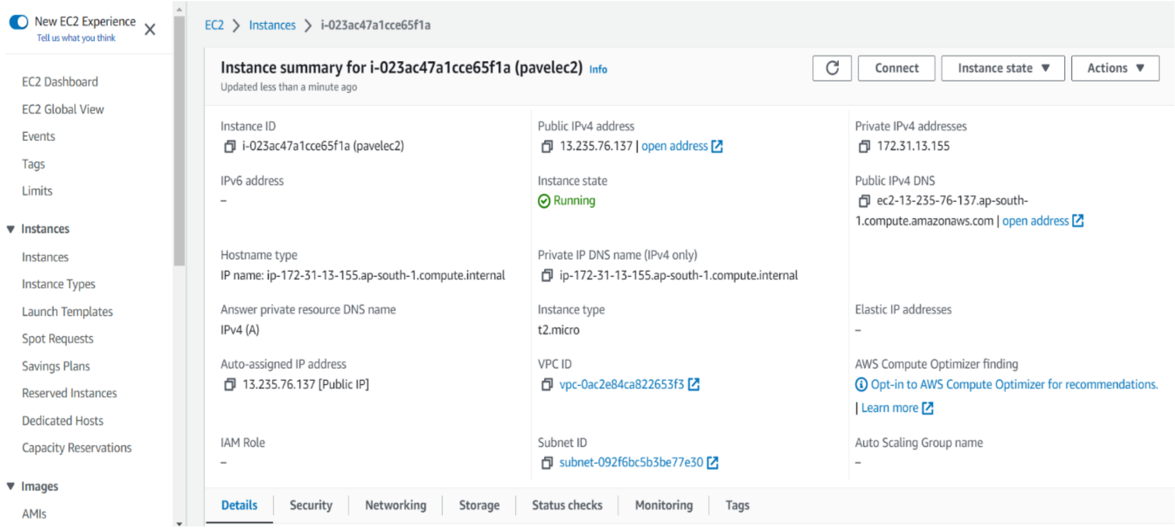
Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

7. Then click on Launch instance. A success message is shown on a new window. Click on View all instances. After this, a window showing all instances is open.

8. Now click on the Instance ID (hidden in the image, but it is actually visible on the website). Copy the public IPv4 address as visible from the new interface that opens.



Instance summary for i-023ac47a1cce65f1a (pavelec2)
Updated less than a minute ago

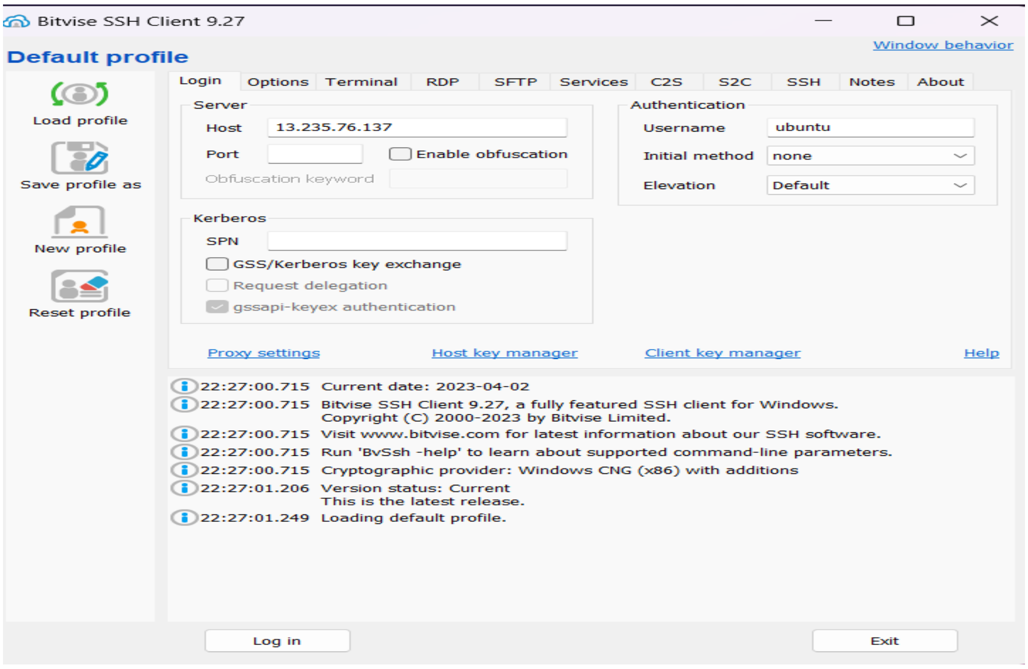
Instance ID: i-023ac47a1cce65f1a (pavelec2)
Public IPv4 address: 13.235.76.137 | open address
Private IPv4 addresses: 172.31.13.155
IPv6 address: –
Instance state: Running
Public IPv4 DNS: ec2-13-235-76-137.ap-south-1.compute.amazonaws.com | open address
Hostname type: IP name: ip-172-31-13-155.ap-south-1.compute.internal
Private IP DNS name (IPv4 only): ip-172-31-13-155.ap-south-1.compute.internal
Answer private resource DNS name: IPv4 (A)
Instance type: t2.micro
Elastic IP addresses: –
Auto-assigned IP address: 13.235.76.137 [Public IP]
VPC ID: vpc-0ac2e84ca822653f3
AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more
IAM Role: –
Subnet ID: subnet-092f6bc5b3be77e30
Auto Scaling Group name: –

9. Now, our ec2 service is ready to work with.

<u>Using the Bitvise SSH client</u>

<u>Steps:</u>

1. If not installed, then go to the website https://www.bitvise.com/ssh-client-download, download the installer, run the installer when downloaded. Now the bitvise client is ready. It is useful for connecting to the server of the ec2 service and install necessary tools to proceed with (however that can also be done directly from the ec2 service website). Moreover, the Bitvise client provides an SFTP client, through which we can transfer files from the local machine to the remote machine, just by simple drag and drop. **Using the Bitvise SSH client.**
2. Open the Bitvise client, and paste the public IPv4 address copied from the EC2 website in the 'Host' field.



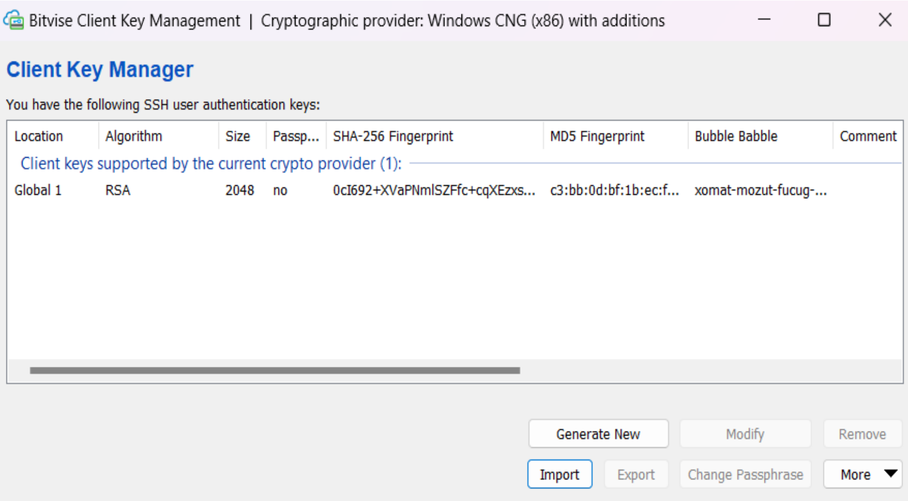
Server
Host: 13.235.76.137
Port:
□ Enable obfuscation
Obfuscation keyword

Authentication
Username: ubuntu
Initial method: none
Elevation: Default

Kerberos
SPN:
□ GSS/Kerberos key exchange
□ Request delegation
☑ gssapi-keyex authentication

```
22:27:00.715 Current date: 2023-04-02
22:27:00.715 Bitvise SSH Client 9.27, a fully featured SSH client for Windows.
             Copyright (C) 2000-2023 by Bitvise Limited.
22:27:00.715 Visit www.bitvise.com for latest information about our SSH software.
22:27:00.715 Run 'BvSsh -help' to learn about supported command-line parameters.
22:27:00.715 Cryptographic provider: Windows CNG (x86) with additions
22:27:01.206 Version status: Current
             This is the latest release.
22:27:01.249 Loading default profile.
```

3. Then click on the Client key manager. A new window gets opened. Click on the Import button, and using the file picker, select the downloaded .pem file(key pair file). Then leaving all settings default click on Import.



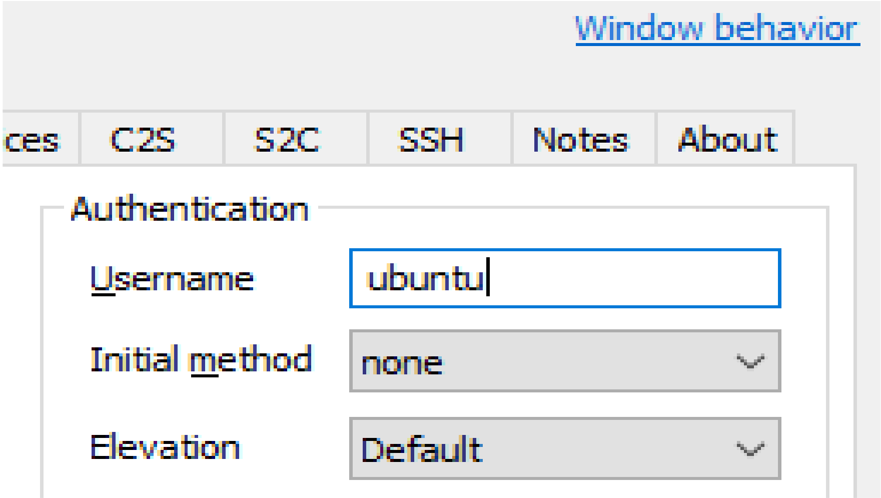
Bitvise Client Key Management | Cryptographic provider: Windows CNG (x86) with additions

Client Key Manager

You have the following SSH user authentication keys:

Location	Algorithm	Size	Passp...	SHA-256 Fingerprint	MD5 Fingerprint	Bubble Babble	Comment
Client keys supported by the current crypto provider (1):							
Global 1	RSA	2048	no	0cI692+XVaPNmlSZFfc+cqXEzxs...	c3:bb:0d:bf:1b:ec:f...	xomat-mozut-fucug-...	

4. Then set username as ubuntu. Now click on the Log in button.



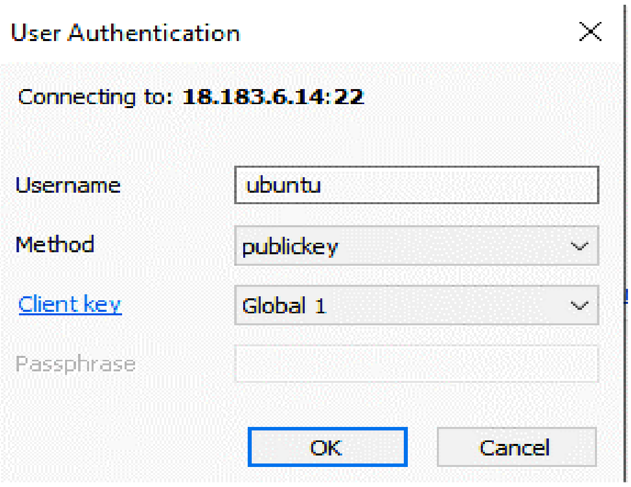
Authentication

Username: ubuntu

Initial method: none

Elevation: Default

5. Then, on the new popup, select Client key as Global 1, and click OK.



User Authentication

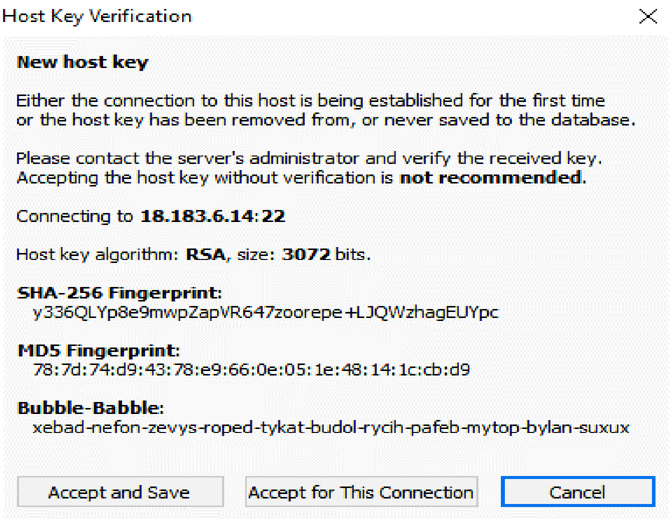
Connecting to: **18.183.6.14:22**

Username: ubuntu

Method: publickey

Client key: Global 1

Passphrase:



Host Key Verification

New host key

Either the connection to this host is being established for the first time or the host key has been removed from, or never saved to the database.

Please contact the server's administrator and verify the received key. Accepting the host key without verification is **not recommended.**

Connecting to **18.183.6.14:22**

Host key algorithm: **RSA**, size: **3072** bits.

SHA-256 Fingerprint:
y336QLYp8e9mwpZapVR647zoorepe+LJQWzhagEUYpc

MD5 Fingerprint:
78:7d:74:d9:43:78:e9:66:0e:05:1e:48:14:1c:cb:d9

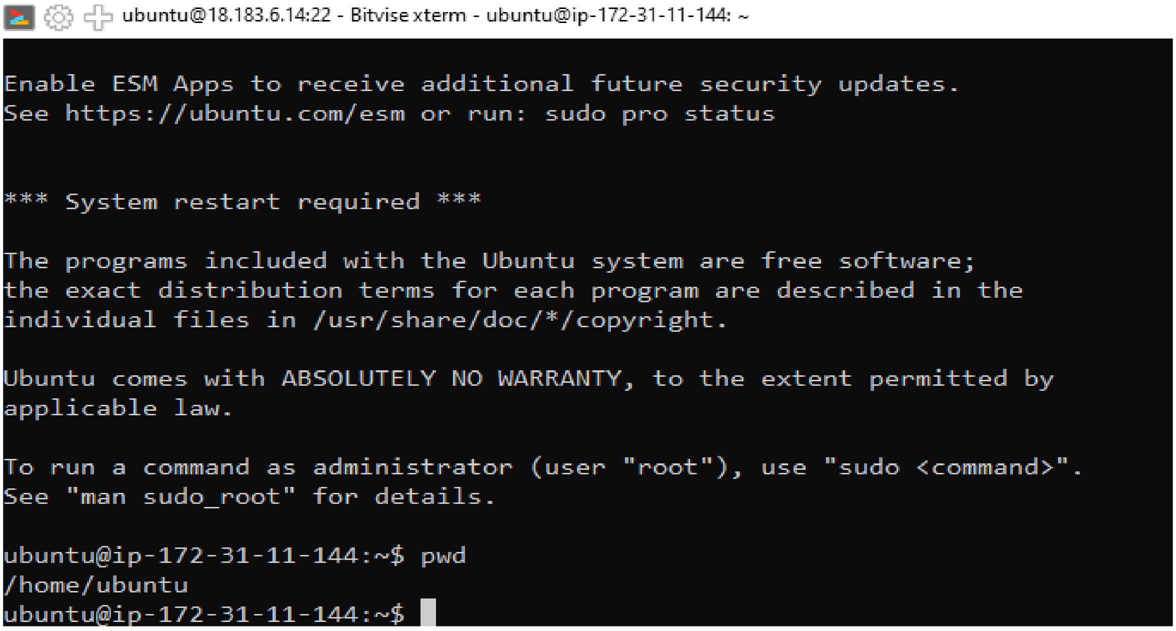
Bubble-Babble:
xebad-nefon-zevys-roped-tykat-budol-rycih-pafeb-mytop-bylan-suxux

6. This makes the connection to the server. Now, two new options open in the Bitvise Client; **New terminal Console** and **New SFTP window.**

Installing the nginx server and transferring website files to the remote server

Steps:

1. In the Bitvise Client (where we just logged in), open the New terminal console. We can see the current working directory using the pwd command. It shows /home/ubuntu. This confirms the connection with the server, and we have open the terminal in the home directory of the server.


ubuntu@18.183.6.14:22 - Bitvise xterm - ubuntu@ip-172-31-11-144: ~

```
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-11-144:~$ pwd
/home/ubuntu
ubuntu@ip-172-31-11-144:~$
```

2. These commands are to be run on this terminal.
sudo apt-get update
sudo apt-get upgrade (-> Press y when asked, and then in the window that opens, select OK and Press 'Enter'.)
sudo apt-get install nginx (-> Press y when asked, and then in the window that opens, select OK and Press 'Enter'.)
These will update and upgrade the ubuntu server, and install nginx server on the remote ubuntu machine.

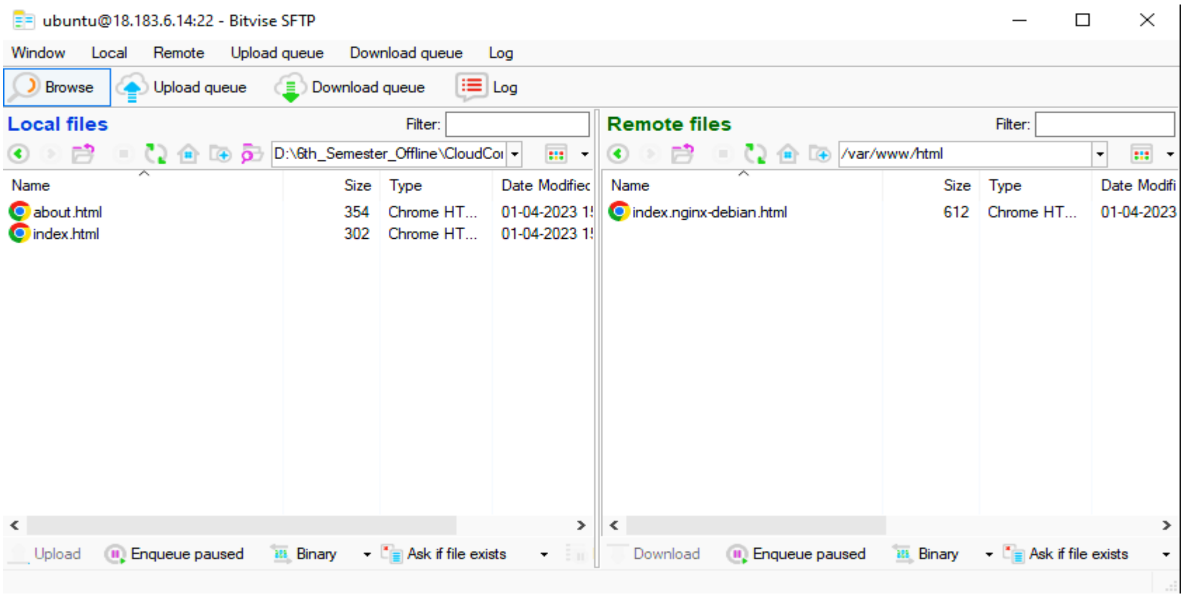
3. Now open the public IPv4 address in any browser. It shows 'Welcome to nginx!', which confirms the successful installation of nginx on the ec2 remote machine.

4. Open New SFTP window. In the Local files section, open the folder where the static website resides in our computer. (Local files means the files existing on our client machine).

5. Go to the root directory in the Remote files section. (Remote files means the files existing in the remote server directory.

6. Then open ‘var’ directory. Then inside it, open the ‘www’ directory. Then inside it, open the ‘html’ directory. This is the directory where we shall keep the html files of our static website, for hosting.

We see that the html directory is denying the uploading of files, because it does not have the appropriate permissions.



D:\6th_Semester_Offline\CloudCo

Name	Size	Type	Date Modifiec
about.html	354	Chrome HT...	01-04-2023 1!
index.html	302	Chrome HT...	01-04-2023 1!

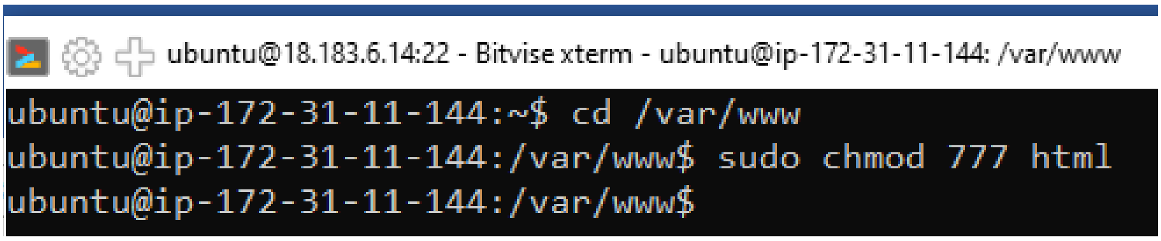
/var/www/html

Name	Size	Type	Date Modifi
index.nginx-debian.html	612	Chrome HT...	01-04-2023

7. To add the permissions, run the following commands in the terminal console (the one that was used for installation of the nginx).

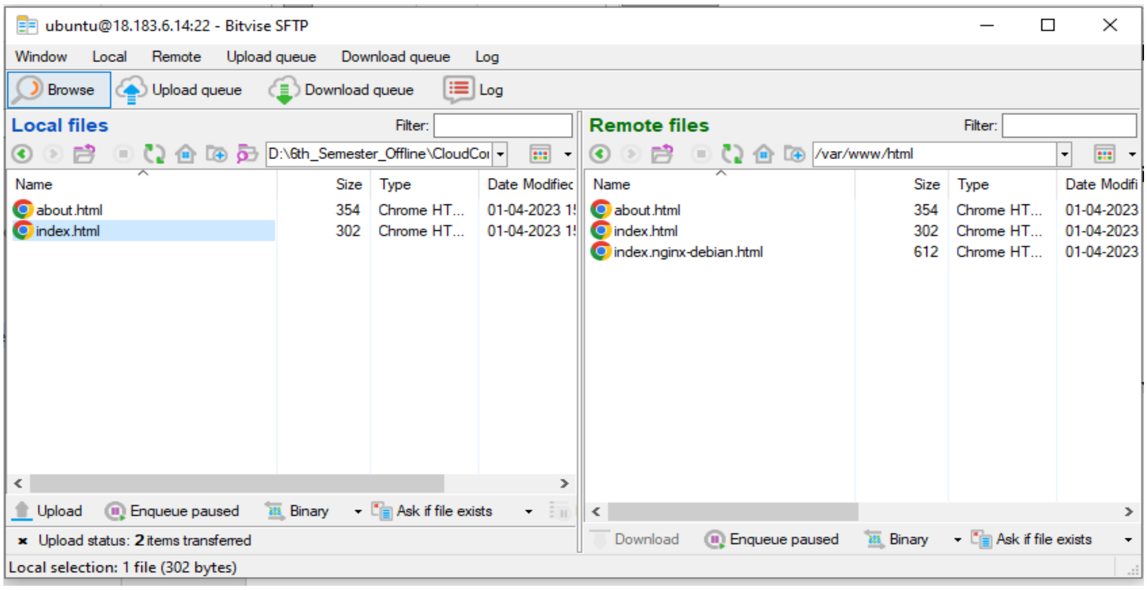
cd /var/www (-> This changes the directory to /var/www.)

sudo chmod 777 html (-> This gives read, write, and execute permissions for all users, to the html directory.)


ubuntu@18.183.6.14:22 - Bitvise xterm - ubuntu@ip-172-31-11-144: /var/www

```
ubuntu@ip-172-31-11-144:~$ cd /var/www
ubuntu@ip-172-31-11-144:/var/www$ sudo chmod 777 html
ubuntu@ip-172-31-11-144:/var/www$
```

8. Now maximize the SFTP window, and drag and drop the files from the Local files to the Remote files section.



D:\6th_Semester_Offline\CloudCo

Name	Size	Type	Date Modifiec
about.html	354	Chrome HT...	01-04-2023 1!
index.html	302	Chrome HT...	01-04-2023 1!

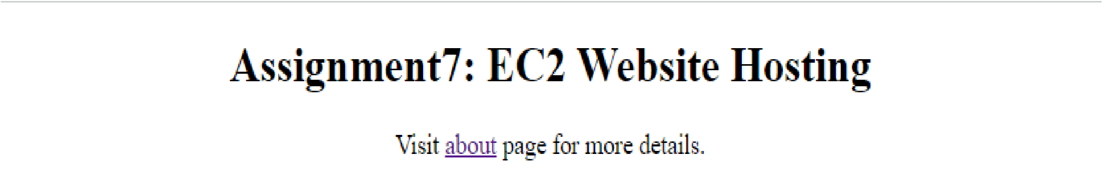
/var/www/html

Name	Size	Type	Date Modifi
about.html	354	Chrome HT...	01-04-2023
index.html	302	Chrome HT...	01-04-2023
index.nginx-debian.html	612	Chrome HT...	01-04-2023

Upload status: 2 items transferred

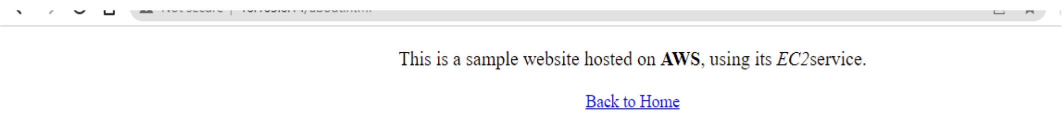
Local selection: 1 file (302 bytes)

9. Open the public IPv4 address (from the ec2 instance), again, on any web browser. Now our website is visible, through this IP. So, finally our website is hosted on the EC2 service.



Assignment7: EC2 Website Hosting

Visit about page for more details.



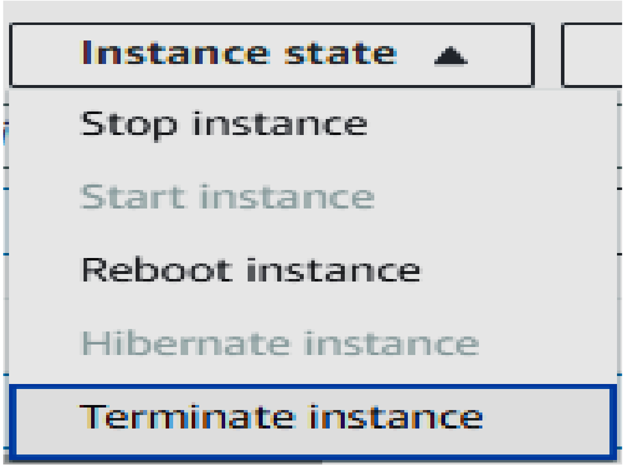
This is a sample website hosted on **AWS**, using its *EC2*service.

Back to Home

10. Now close the SFTP window, and the terminal console.

11. Go to AWS console
Search for ec2; Select the Instances (running).

The new window that opens, shows all the running instances. Select the instance that you created, and then click on Instance state (dropdown).



12. Click on Terminate instance. On the popup window that opens, click on the Terminate button. After few moments, we see that the it does not show Running anymore. And, after some hours, the instance gets deleted automatically.