**EXPERIMENT 04**

CLASS: BE CMPN A 2 ROLL NO. : 18

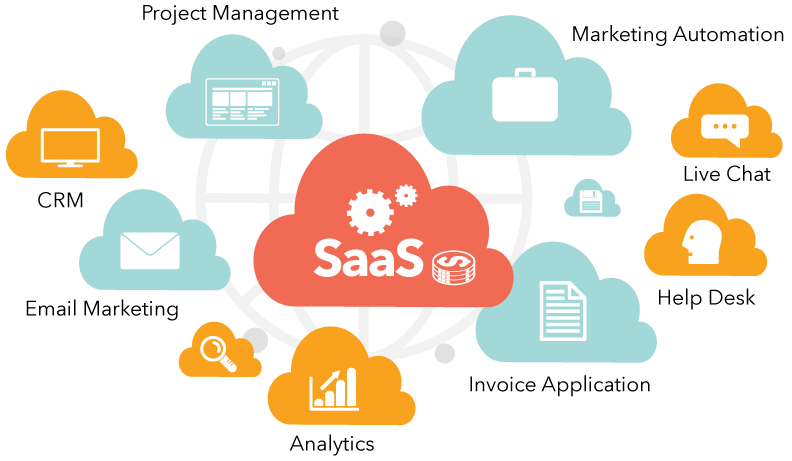
NAME: REBECCA DIAS PID: 182027

**Aim**: Study Software as a Service and Cloud Security

**Theory:**

1. Prepare a detailed study of Software as a Service

Software-as-a-Service (SaaS) is a software model in which access to the software is provided on a subscription basis, with the software being located on external servers rather than on servers located in-house.



SaaS is also known as "On-Demand Software". It is a software distribution model in which services are hosted by a cloud service provider. These services are available to end-users over the internet so, the end-users do not need to install any software on their devices to access these services.

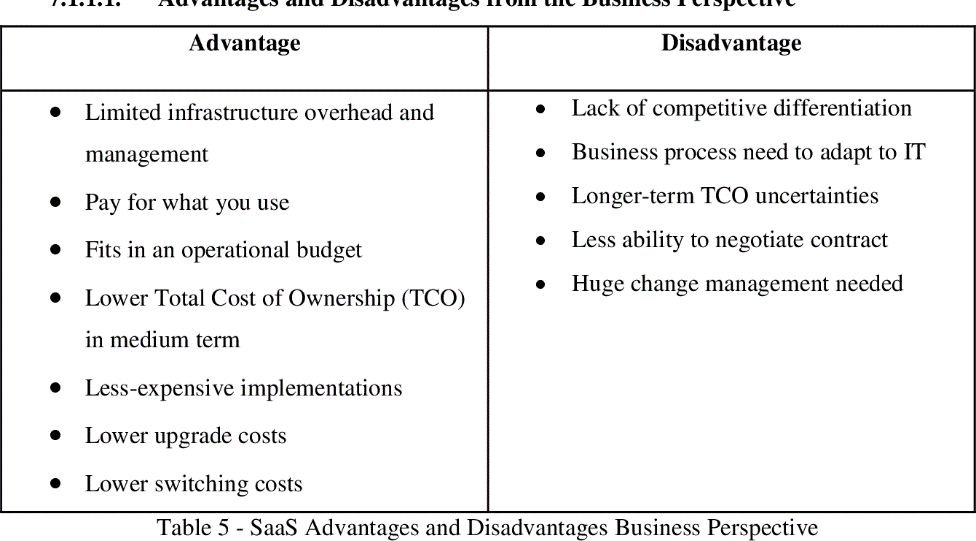
There are the following services provided by SaaS providers -

* Business Services - SaaS Provider provides various business services to start-up the business. The SaaS business services include ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), billing, and sales.
* Document Management - SaaS document management is a software application offered by a third party (SaaS providers) to create, manage, and track electronic documents.Example: Slack, Samepage, Box, and Zoho Forms.
* Social Networks - As we all know, social networking sites are used by the general public, so social networking service providers use SaaS for their convenience and handle the general public's information.
* Mail Services - To handle the unpredictable number of users and load on e-mail services, many e-mail providers offering their services using SaaS.

1. Advantages and Limitation of SaaS

*Advantages*

* Easily Deployable- The ease of access and implementation of SaaS is one of the things that fascinate decision-makers. SaaS solutions are pre-existing, the deployment time is extremely low. In addition, they are generally very flexible and therefore make it possible to stick as closely as possible to user needs and to implement solutions on demand.
* Cost Reduction- The use of a SaaS allows the reduction of costs with servers, which in addition to the cost still requires hours of maintenance and care by your IT staff.The exchange of the physical infrastructure required to maintain a product for a cloud service, whether public or private, saves physical space in addition to financial savings.
* High Scalability- SaaS allows you to multiply access according to the needs of the business rather than investing in software licenses and server capacities internally.The pay-as-you-go model allows organizations to transfer costs to an ongoing operating expense to facilitate budget management.
* Access Anytime and Anywhere- One of the basic principles of SaaS is that it is accessible anytime and anywhere. Through a browser and an internet connection, its users have easy access at any time, making this an important differential that allows more mobility, agility, and practicality for all employees inside and outside the business environment.



*Disadvantages*

* Confidentiality- The data related to the client company is generally kept on the provider’s servers, which can, therefore, generate confidentiality concerns.The risk of having your data exposed to a public network is one of the key disadvantages, especially when dealing with more traditional corporations.To prevent this, it is necessary to know the accounts that cloud technology provides and make a prior agreement with the service provider listing everything that could happen in the event of disasters.
* Stability- SaaS is an online service that inevitably requires a good internet connection. Hence connectivity is a con as you always need to have a stable internet connection for the system to work in a complete way.Network problems can cause very annoying download delays, which can lead to loss of productivity.

1. Study security issues in cloud computing



* Responsibility ambiguity- Cloud service users consume delivered resources through service models. The customer-built IT system thus relies on the services. The lack of a clear definition of responsibility among cloud service users and Providers may evoke conceptual conflicts. Moreover, any contractual inconsistency of provided services could induce anomaly, or incidents. However the problem of which entity is the data controller which on is the data processor stays open at an international scale (even if the international aspect is reduced to a minimal third party outside of the specific region like EU).
* Loss of Governance- For an enterprise, migrating a part of its own IT system to a cloud infrastructure implies to partially give control to the cloud service providers. This loss of governance depends on the cloud service models. For instance, IaaS only delegates hardware and network management to the provider, while SaaS also delegates OS, application, and service integration in order to provide a turnkey service to the cloud service user.
* Loss of Trust- It is sometime difficult for a cloud service user to recognize his providers trust level due to the black-box feature of the cloud service. There is no measure how to get and share the providers security level in formalized manner. Furthermore, the cloud service users have no abilities to evaluate security implementation level achieved by the provider. Such a lack of sharing security level in view of cloud service provider will become a serious security threat in use of cloud services for cloud service users.
* Service Provider Lock-in- A consequence of the loss of governance could be a lack of freedom regarding how to replace a cloud provider by another. This could be the case if a cloud provider relies on non-standard hypervisors or virtual machine image format and does not provide tools to convert virtual machines to a standardized format.
* Unsecure Cloud Service User Access- As most of the resource deliveries are through remote connection, non -protected APIs, (mostly management APIs and PaaS services is one of the easiest attack vector). Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.
* Lack of Information/Asset Management- When applying to use Cloud Computing Services, the cloud service user will have serious concerns on lack of information/asset management by cloud service providers such as location of sensitive asset/information, lack of physical control for data storage, reliability of data backup (data retention issues), countermeasures for BCP and Disaster Recovery and so on. Furthermore, the cloud service users also have important concerns on exposure of data to foreign government and on compliance with privacy law such as EU data protection directive.

1. Explain Server and Data Security is cloud computing

* Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. It’s a concept that encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies and procedures.
* **Types of data security**

1. **Encryption**

Using an algorithm to transform normal text characters into an unreadable format, encryption keys scramble data so that only authorized users can read it. File and database encryption solutions serve as a final line of defense for sensitive volumes by obscuring their contents through encryption or tokenization. Most solutions also include security key management capabilities.

1. **Data Erasure**

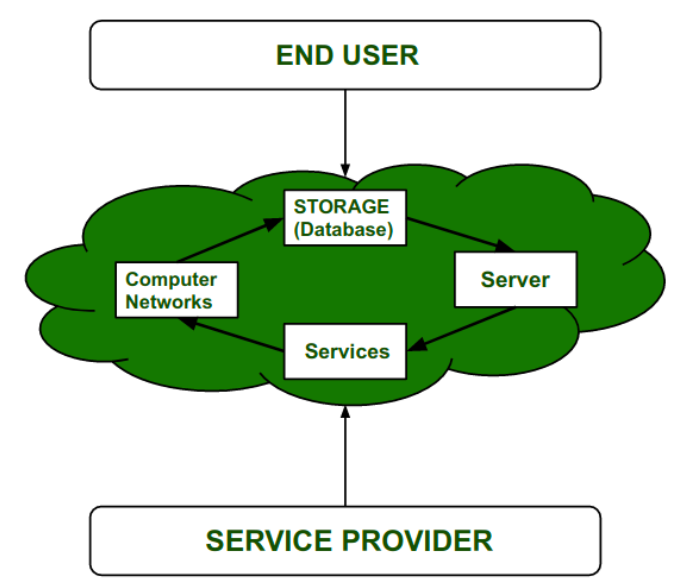
More secure than standard data wiping, data erasure uses software to completely overwrite data on any storage device. It verifies that the data is unrecoverable.

1. **Data Masking**

By masking data, organizations can allow teams to develop applications or train people using real data. It masks personally identifiable information (PII) where necessary so that development can occur in environments that are compliant.

1. **Data Resiliency**

Resiliency is determined by how well an organization endures or recovers from any type of failure – from hardware problems to power shortages and other events that affect data availability (PDF, 256 KB). Speed of recovery is critical to minimize impact.

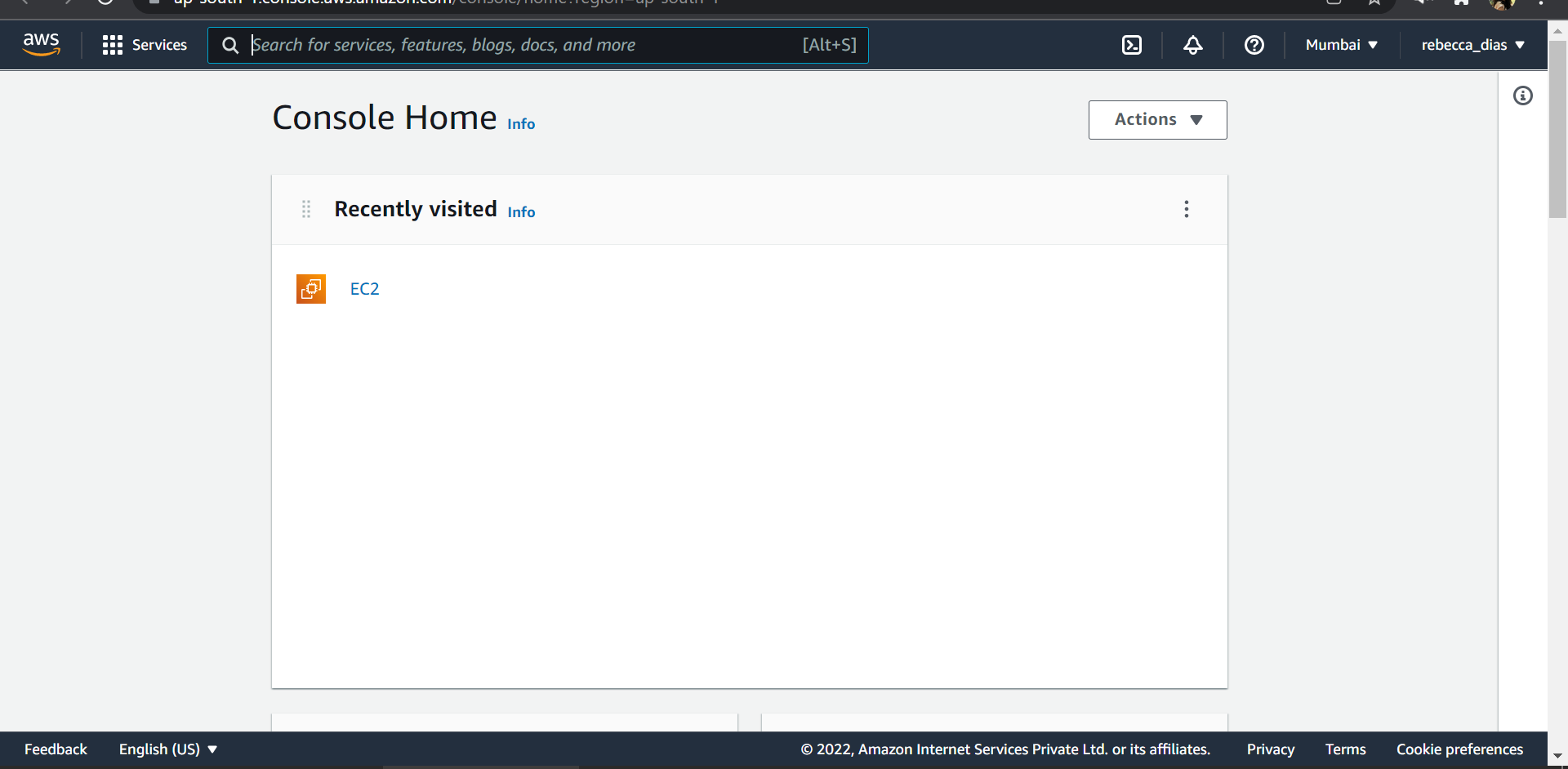


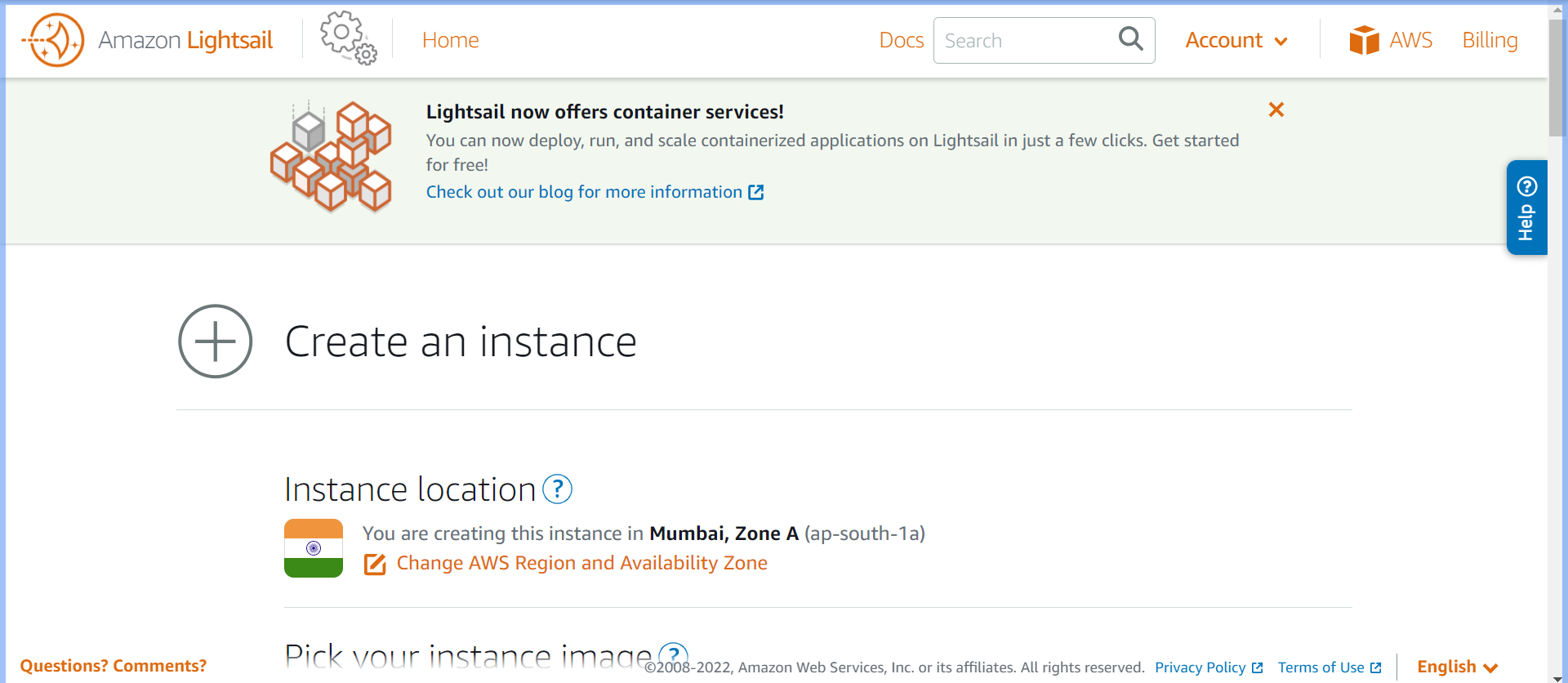
* When properly implemented, robust data security strategies will protect an organization’s information assets against cybercriminal activities, but they also guard against insider threats and human error, which remains among the leading causes of data breaches today. Data security involves deploying tools and technologies that enhance the organization’s visibility into where its critical data resides and how it is used. Ideally, these tools should be able to apply protections like encryption, data masking, and redaction of sensitive files, and should automate reporting to streamline audits and adhering to regulatory requirements.
* Server security is a discipline of cyber security dedicated to securing cloud computing systems. This includes keeping data private and safe across online-based infrastructure, applications, and platforms. Securing these systems involves the efforts of cloud providers and the clients that use them, whether an individual, small to medium business, or enterprise uses.
* Cloud providers host services on their servers through always-on internet connections. Since their business relies on customer trust, cloud security methods are used to keep client data private and safely stored.

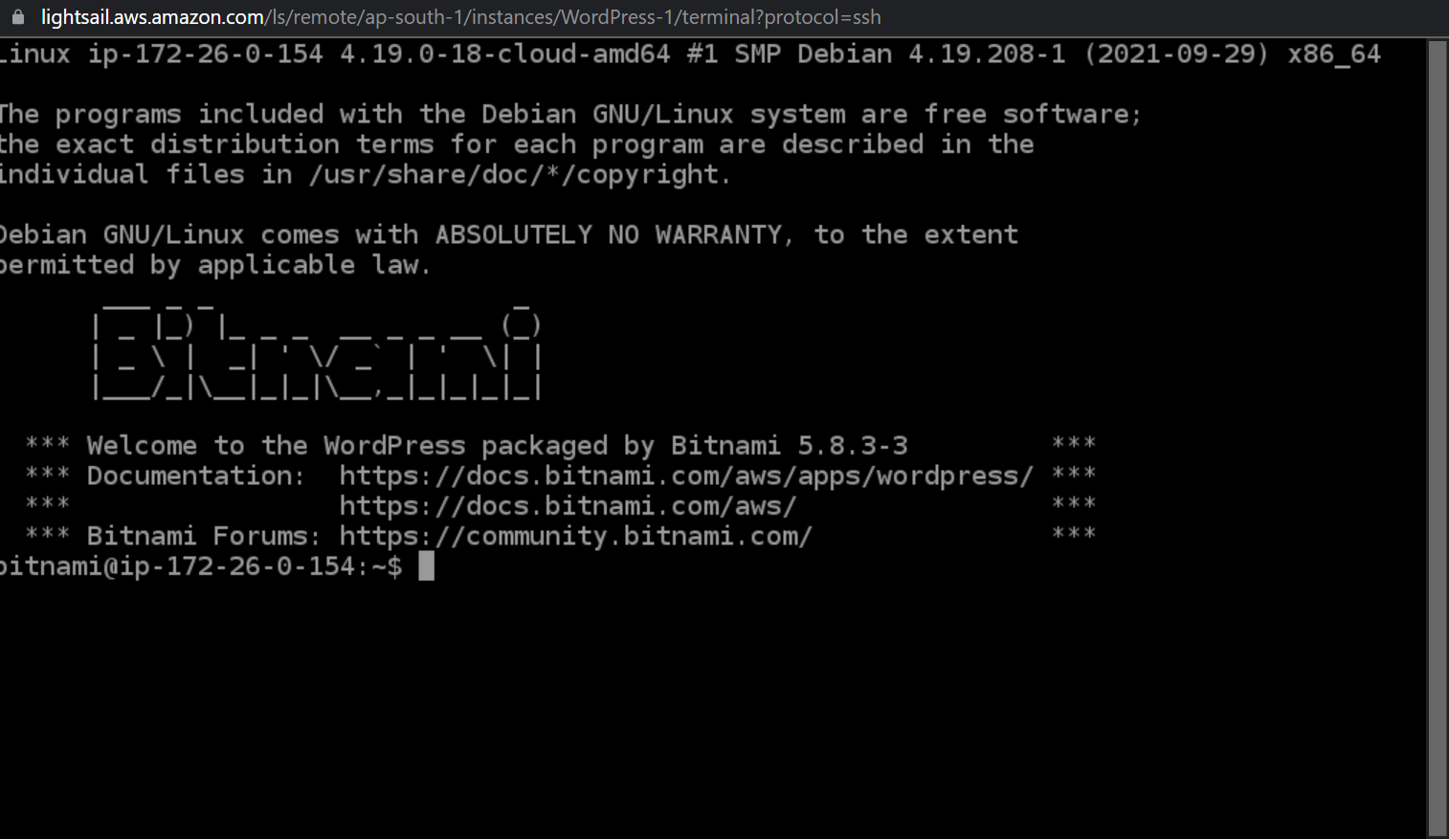
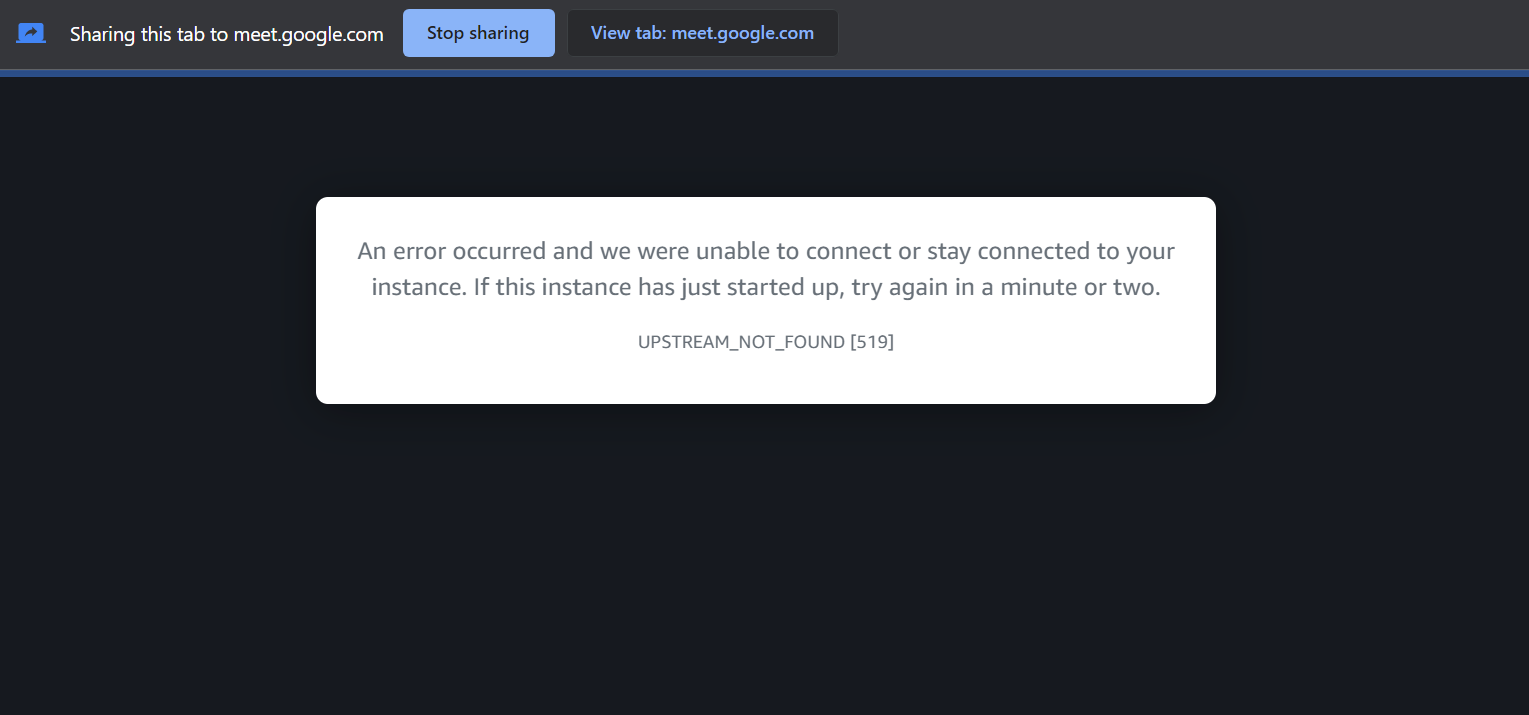
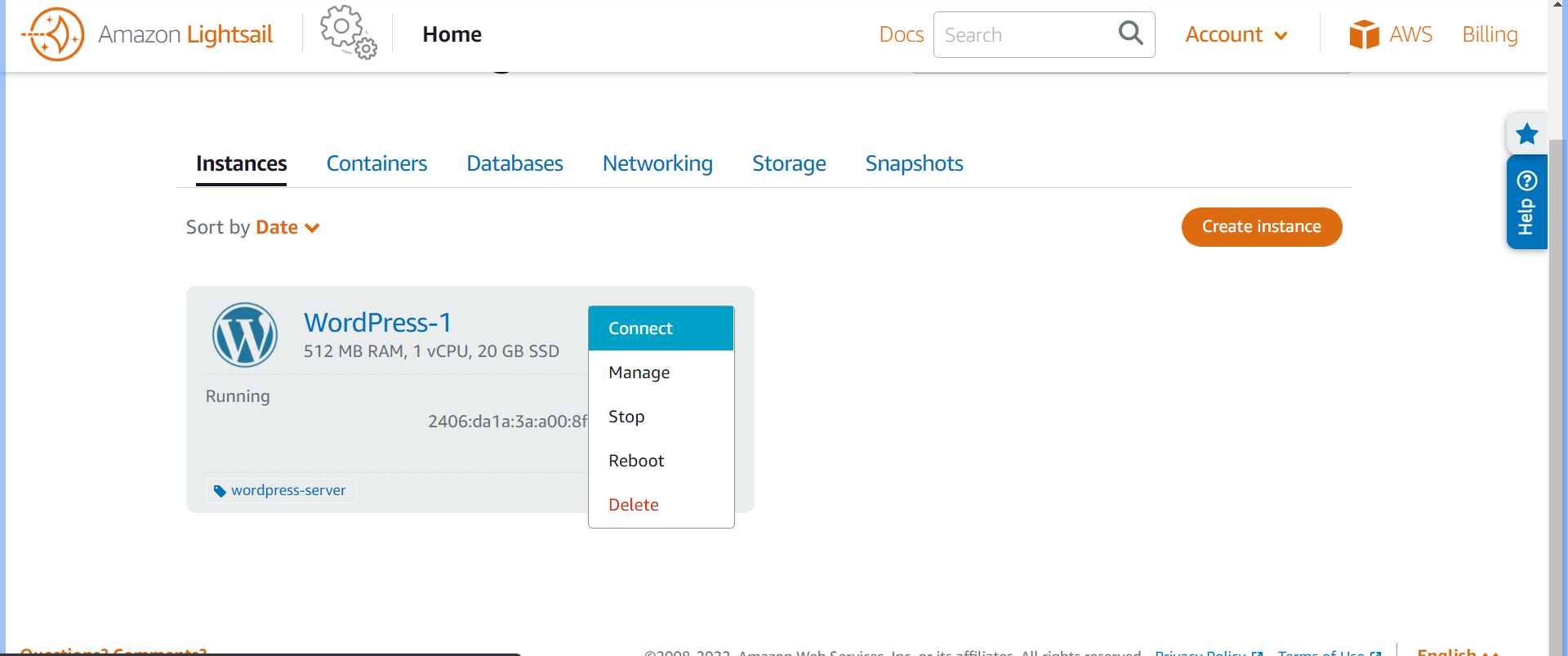
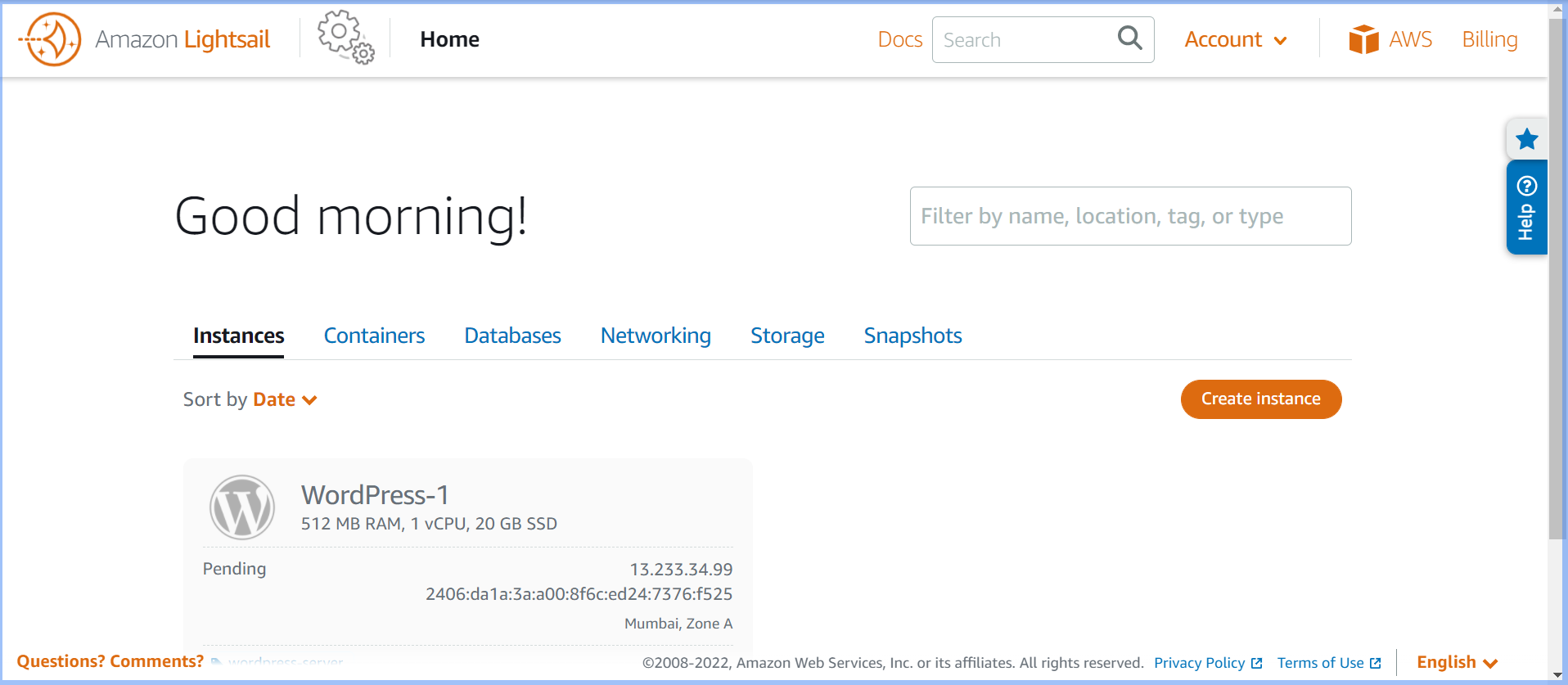
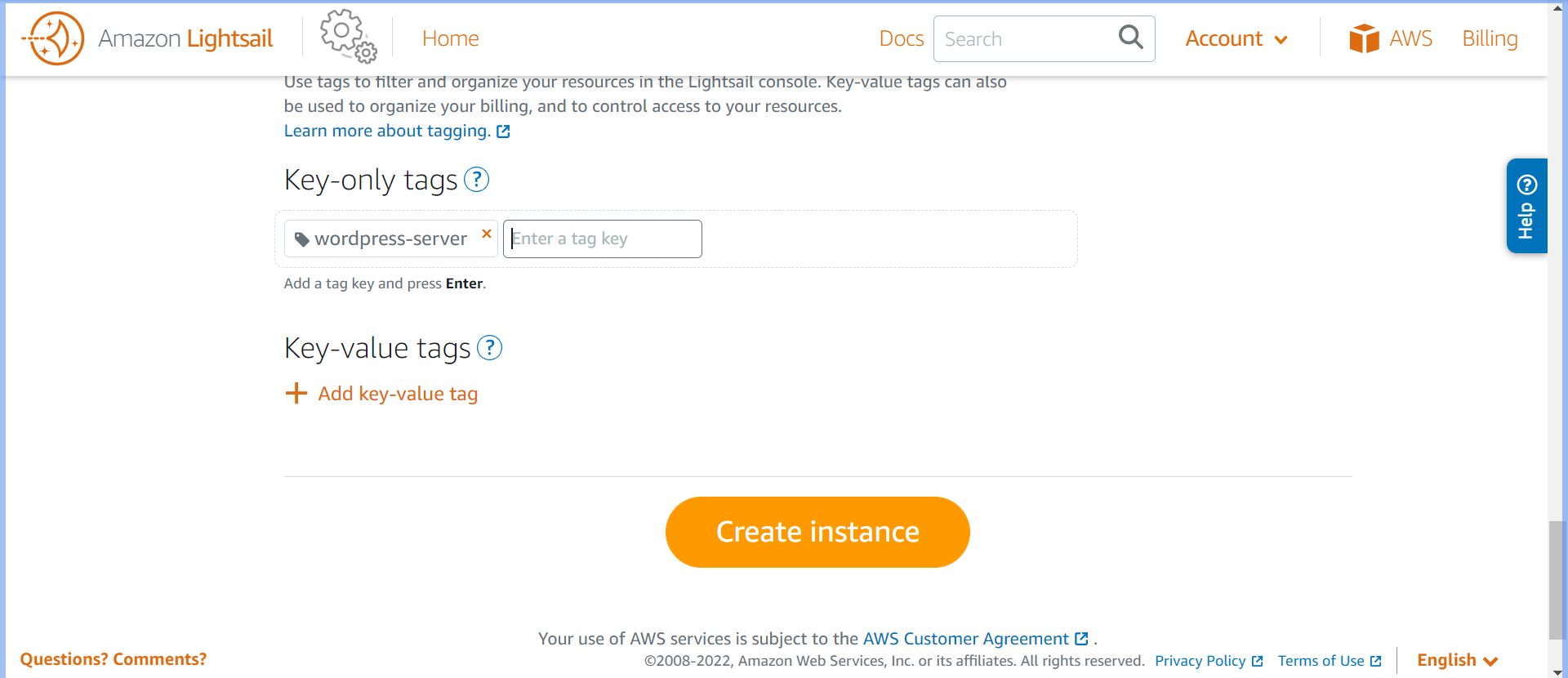
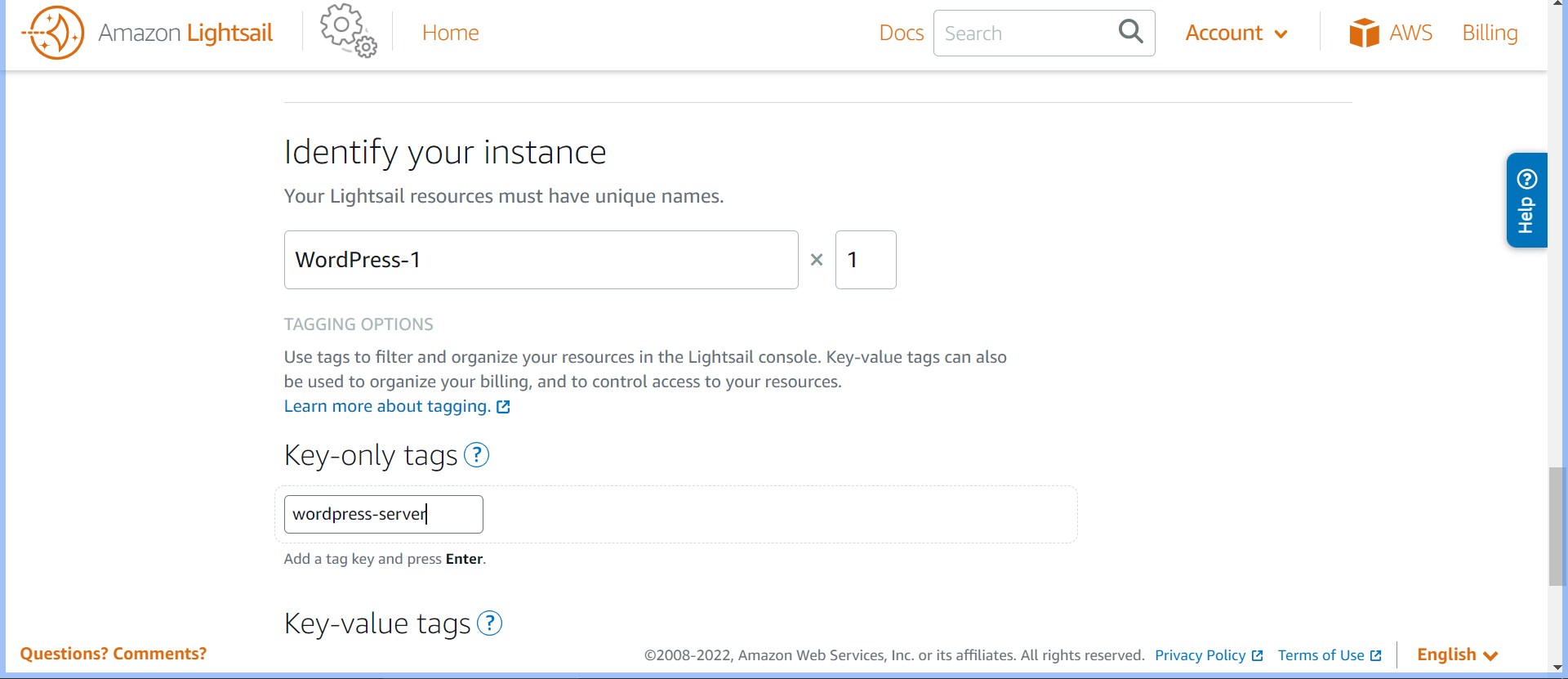
**Activity:**

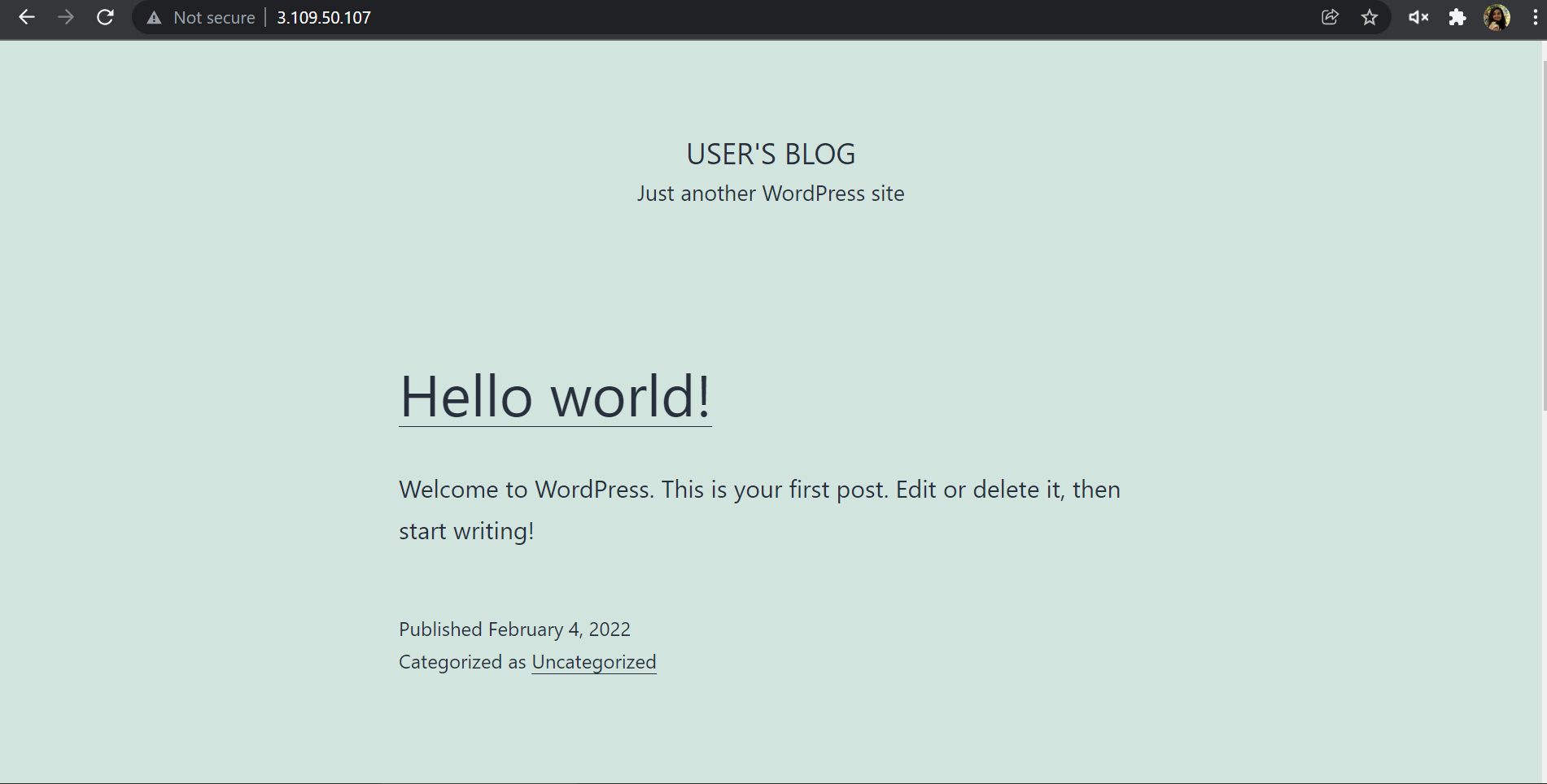
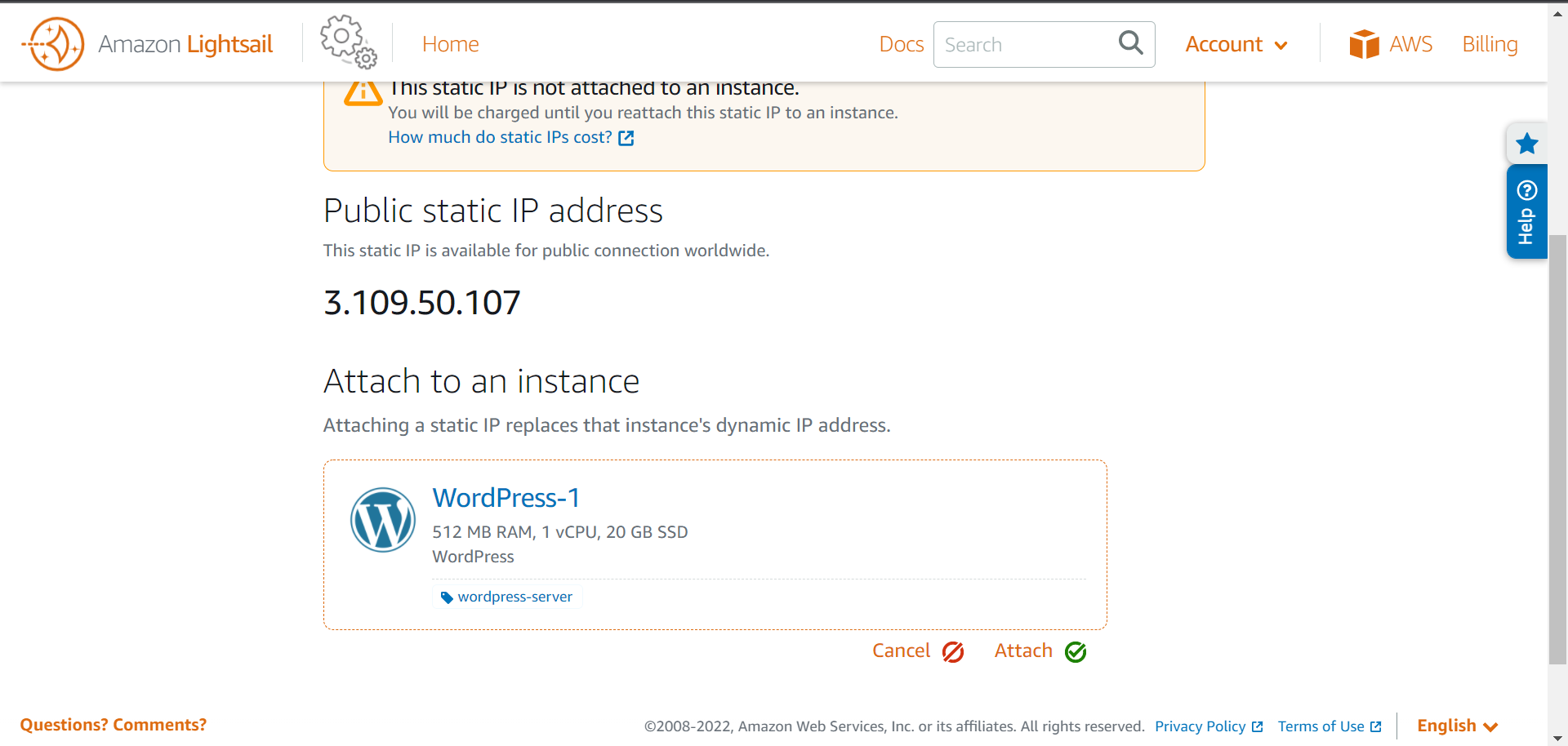
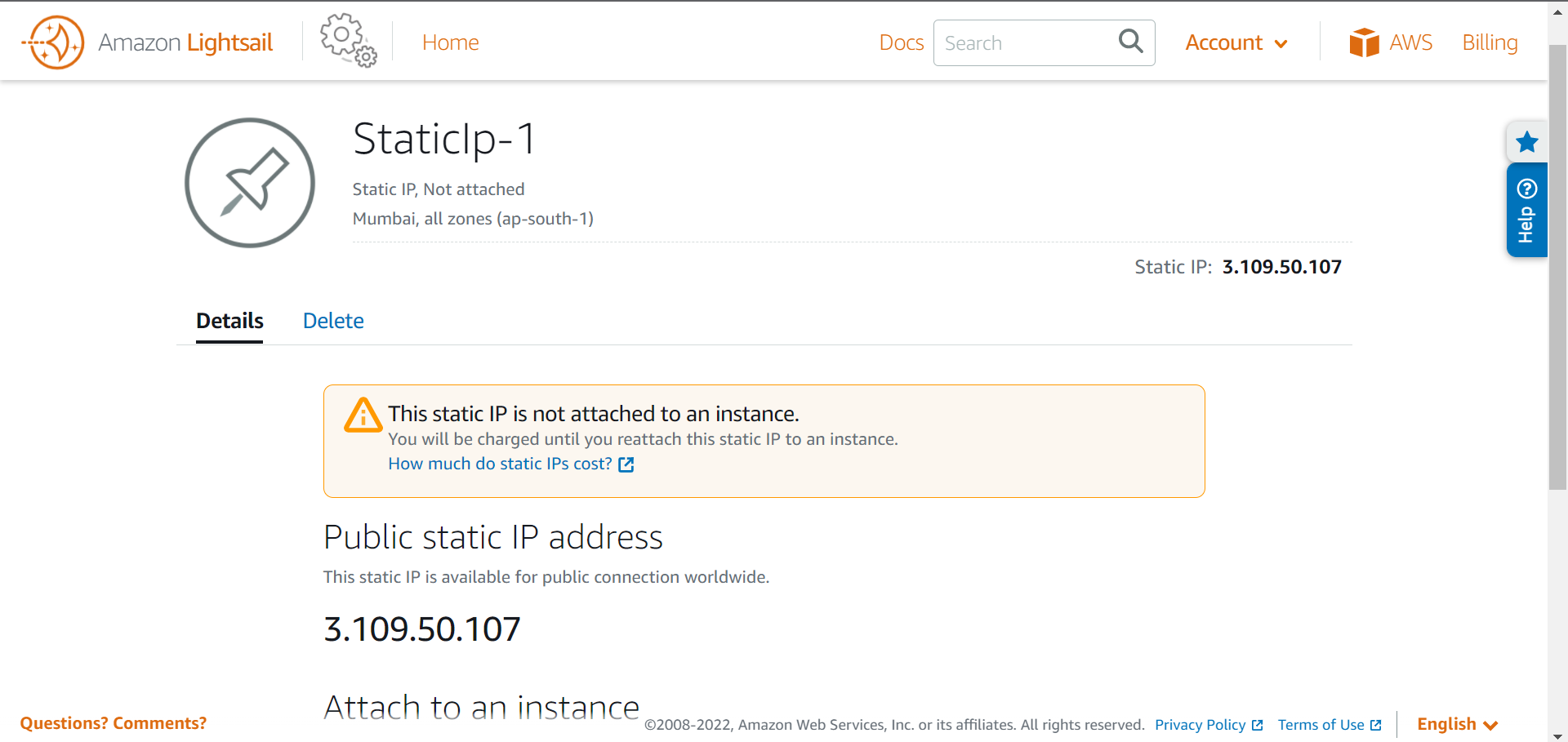
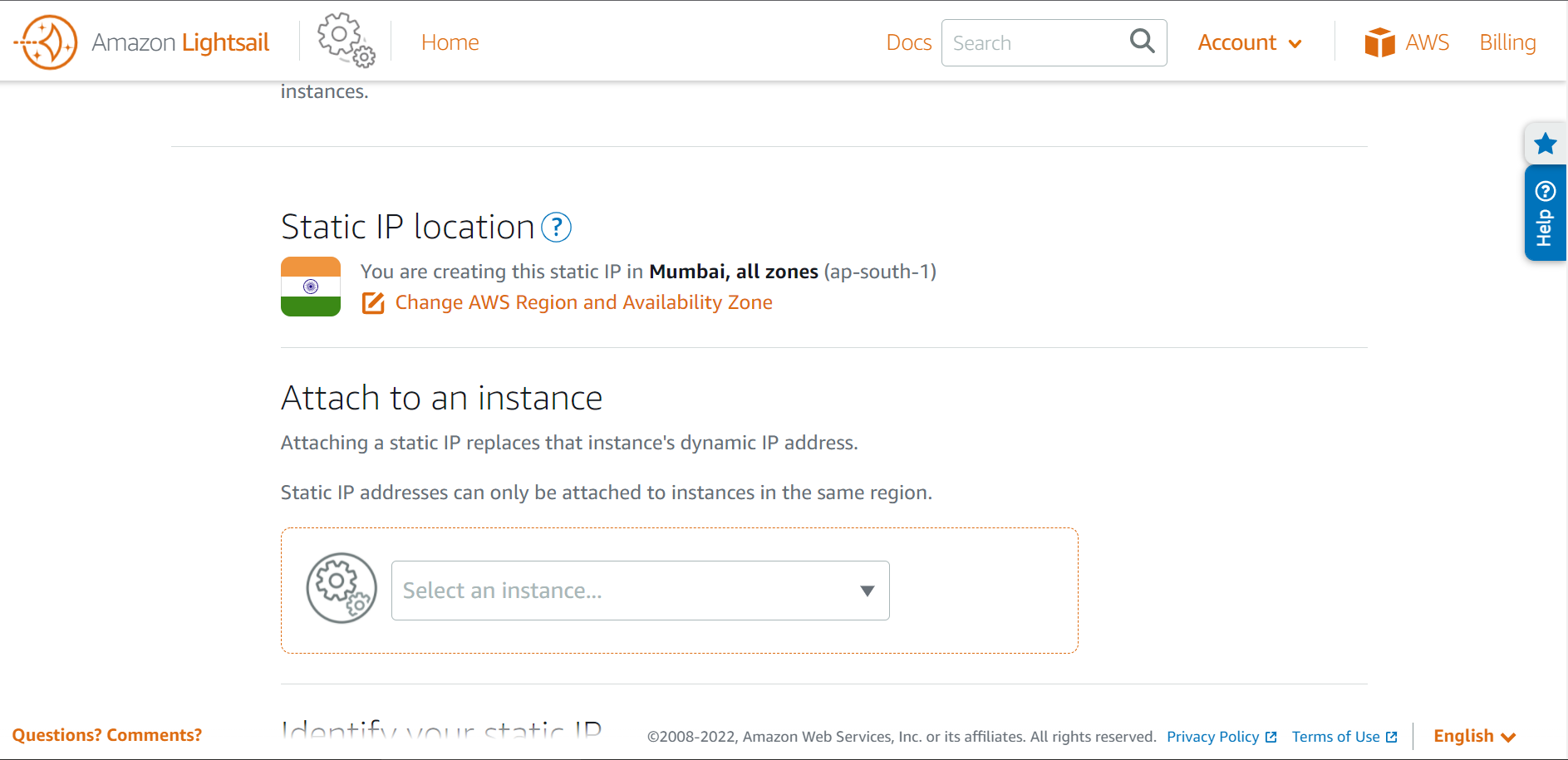
## With the help of any suitable cloud service explain SaaS

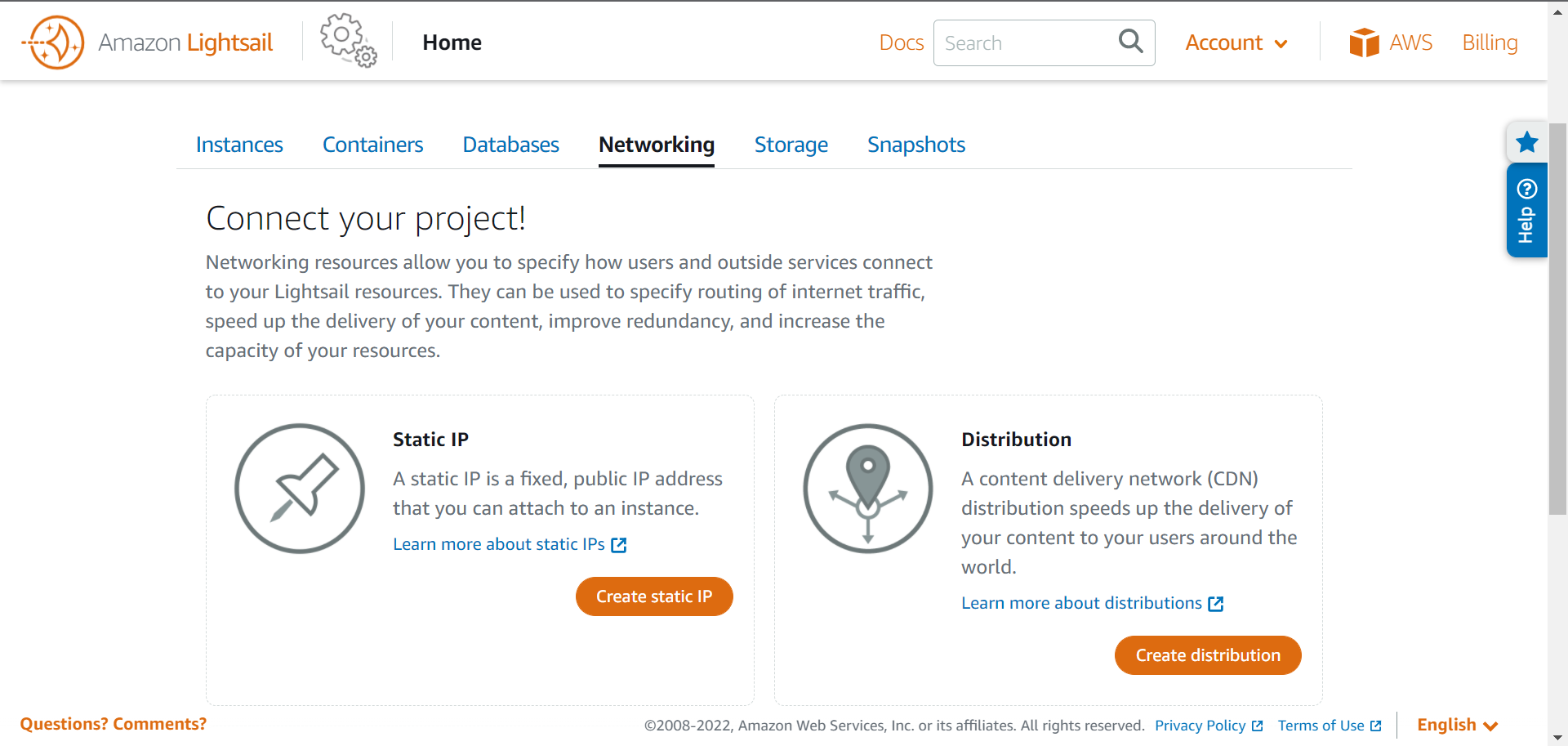
## Use your own cloud to explain the security of the webserver and data directory.



****

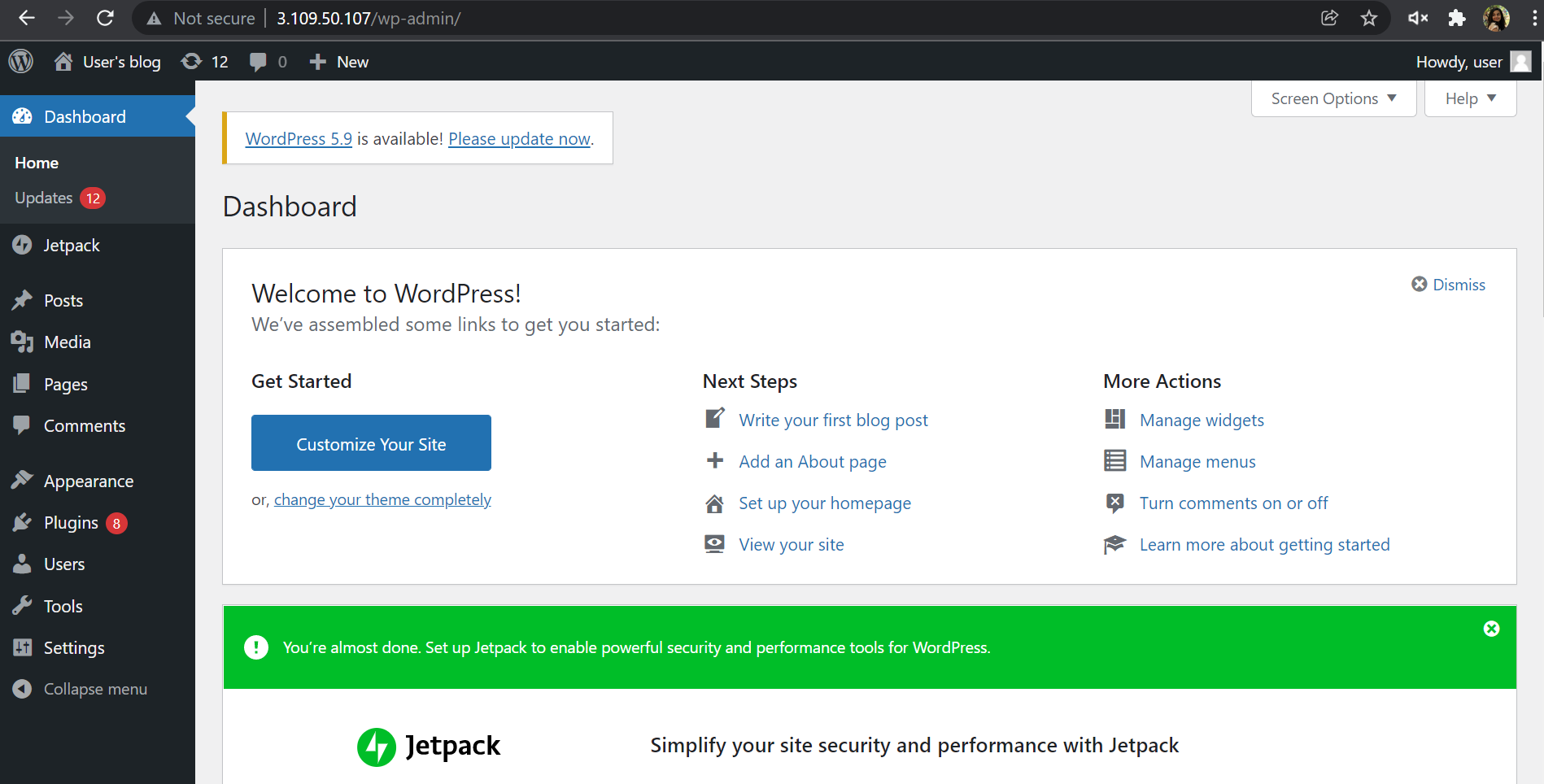
****

****

****

Username: user

Password:DYSDWUxP6uIm

****

**Conclusion:**

## **Why is SaaS required?**

1. Cost

SaaS can provide notable savings for several different reasons. Foremost, it eliminates the upfront cost of purchase/installation, as well on-going costs like maintenance and upgrades. Instead of spending large amounts of money on hardware installations, SaaS applications can be easily downloaded and maintained.

2. Time

Many people say “time is money” and thankfully, SaaS can save both. For many SaaS applications, installation is as simple as having an internet connection and acquiring a log-in. Furthermore, maintenance responsibilities are shifted from your IT department to the vendor itself. This eliminates extra work hours and downtime that might have been necessary to upgrade conventional software.

3. Scalability & Accessibility

Another great feature of SaaS is that the pay-as-you-go model provides fantastic flexibility and options. Because the software is hosted externally by a vendor, changing your usage plan is easy and can be done without advance notice. Additionally, web-based use allows subscribers to access the software easily from any location with internet capabilities.

4. Compatibility

With the conventional software installation method, updates can require enormous amounts of time and money. Even worse, version discrepancies between members of your workforce can lead to compatibility issues and wasted time. With SaaS however, subscribers can simply log-on to already upgraded services.

**Why cloud computing security is important?**

Security in cloud computing is crucial to any company looking to keep its applications and data protected from bad actors. Maintaining a strong cloud security posture helps organizations achieve the now widely recognized benefits of cloud computing.

1. Lower upfront costs

One of the biggest advantages of using cloud computing is that you don't need to pay for dedicated hardware. Not having to invest in dedicated hardware helps you initially save a significant amount of money and can also help you upgrade your security. This helps you save on costs and reduce the risks associated with having to hire an internal security team to safeguard dedicated hardware.

2. Reduced ongoing operational and administrative expenses

Cloud security can also lower your ongoing administrative and operational expenses. A CSP will handle all your security needs for you, removing the need to pay for staff to provide manual security updates and configurations. You can also enjoy greater security, as the CSP will have expert staff able to handle any of your security issues for you.

3. Increased reliability and availability

You need a secure way to immediately access your data. Cloud security ensures your data and applications are readily available to authorized users. There will always be a reliable method to access your cloud applications and information, helping you quickly take action on any potential security issues.

4. Centralized security

Cloud computing gives a centralized location for data and applications, with many endpoints and devices requiring security. Security for cloud computing centrally manages all the applications, devices, and data to ensure everything is protected. The centralized location allows cloud security companies to more easily perform tasks, such as implementing disaster recovery plans, streamlining network event monitoring, and enhancing web filtering.

5. Greater ease of scaling

Cloud computing allows us to scale with new demands, providing more applications and data storage whenever needed. Cloud security easily scales with cloud computing services. When one needs change, the centralized nature of cloud security allows you to easily integrate new applications and other features without sacrificing your data's safety. Cloud security can also scale during high traffic periods, providing more security.

6. Improved DDoS protection

Distributed Denial of Service (DDoS) attacks are some of the biggest threats to cloud computing. These attacks aim a lot of traffic at servers at once to cause harm. Cloud security protects your servers from these attacks by monitoring and dispersing them.

**References:**

[Software-as-a-Service (SaaS)](https://www.investopedia.com/terms/s/software-as-a-service-saas.asp)

[Software as a Service | SAAS - javatpoint](https://www.javatpoint.com/software-as-a-service)

[What are the Advantages and Disadvantages of SaaS?](https://wisdomplexus.com/blogs/advantages-disadvantages-saas/)

<https://www.ijert.org/an-empirical-study-on-security-issues-in-cloud-computing-environments>