**Academic Year: 2021-2022** **Semester: VIII**
**Subject: Cloud Computing Lab** **Class / Branch / Division: BE/CMPN A**
**Name: Nithin Menezes** **Roll Number: 56**

**Experiment No: 2**

**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 distribution model in which a cloud provider hosts applications and makes them available to end-users over the internet. In this model, an independent software vendor (ISV) may contract a third-party cloud provider to host the application. Or, with larger companies, such as Microsoft, the cloud provider might also be the software vendor. SaaS is one of three main categories of cloud computing, alongside infrastructure as a service (IaaS) and platform as a service (PaaS). A range of IT professionals, business users, and personal users use SaaS applications. Products range from personal entertainment, such as Netflix, to advanced IT tools. Unlike IaaS and PaaS, SaaS products are frequently marketed to both B2B and B2C users.

**2. How does software as a service work?**
SaaS works through the cloud delivery model. A software provider will either host the application and related data using its servers, databases, networking, and computing resources, or it may be an ISV that contracts a cloud provider to host the application in the provider's data center. The application will be accessible to any device with a network connection. SaaS applications are typically accessed via web browsers. As a result, companies using SaaS applications are not tasked with the setup and maintenance of the software. Users simply pay a subscription fee to gain access to the software, which is a ready-made solution. SaaS is closely related to the application service provider (ASP) and on-demand computing software delivery models where the provider hosts the customer's software and delivers it to approved end-users over the internet. In the software-on-demand SaaS model, the provider gives customers network-based access to a single copy of an application that the provider created specifically for SaaS distribution. The application's source code is the same for all customers, and when new features or functionalities are released, they are rolled out to all customers. Depending on the service level agreement (SLA), the customer's data for each model may be stored locally, in the cloud, or both locally and in the cloud. Organizations can integrate SaaS applications with other software using application programming interfaces (APIs). For example, a business can write its software tools and use the SaaS provider's APIs to integrate those tools with the SaaS offering.

**3. SaaS architecture**
SaaS applications and services typically use a multi-tenant approach, which means a single instance of the SaaS application will be running on the host servers, and that single instance will serve each subscribing customer or cloud tenant. The application will run on a single version and configuration across all customers or tenants. Though different subscribing customers will run on the same cloud instance with a common infrastructure and platform, the data from different customers will still be segregated.
The typical multi-tenant architecture of SaaS applications means the cloud service provider can manage maintenance, updates, and bug fixes faster, easier, and more efficiently. Rather than having to implement changes in multiple instances, engineers can make necessary changes for all customers by maintaining one, shared instance.
Furthermore, multi-tenancy allows a greater pool of resources to be available to a larger group of people, without compromising important cloud functions such as security, speed, and privacy.

**4. Advantages and Limitations of SaaS**
SaaS advantages
SaaS removes the need for organizations to install and run applications on their computers or in their data centers. This eliminates the expense of hardware acquisition, provisioning, and maintenance, as well as software licensing, installation, and support. Other benefits of the SaaS model include:
a) Flexible payments. Rather than purchasing software to install, or additional hardware to support it, customers subscribe to a SaaS offering. Transitioning costs to a recurring operating expense allows many businesses to exercise better and more predictable budgeting. Users can also terminate SaaS offerings at any time to stop those recurring costs.

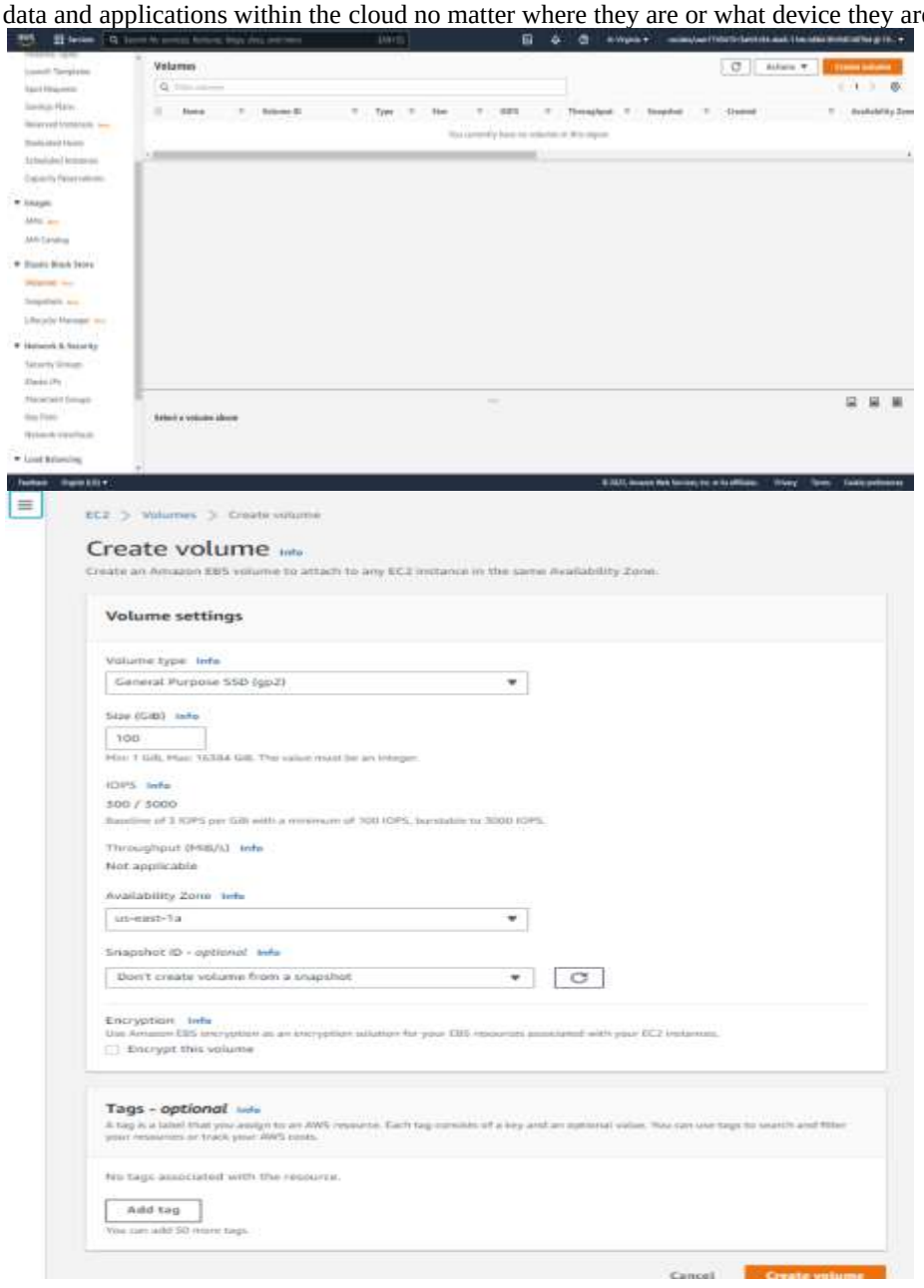
b) Scalable usage. Cloud services like SaaS offer high Vertical scalability, which gives customers the option to access more or fewer services or features on-demand. c) Automatic updates. Rather than purchasing new software, customers can rely on a SaaS provider to automatically perform updates and patch management. This further reduces the burden on in-house IT staff.
d) Accessibility and persistence. Since SaaS vendors deliver applications over the internet, users can access them from any internet-enabled device and location. e) Customization. SaaS applications are often customizable and can be integrated with other business applications, especially across applications from a common software provider.

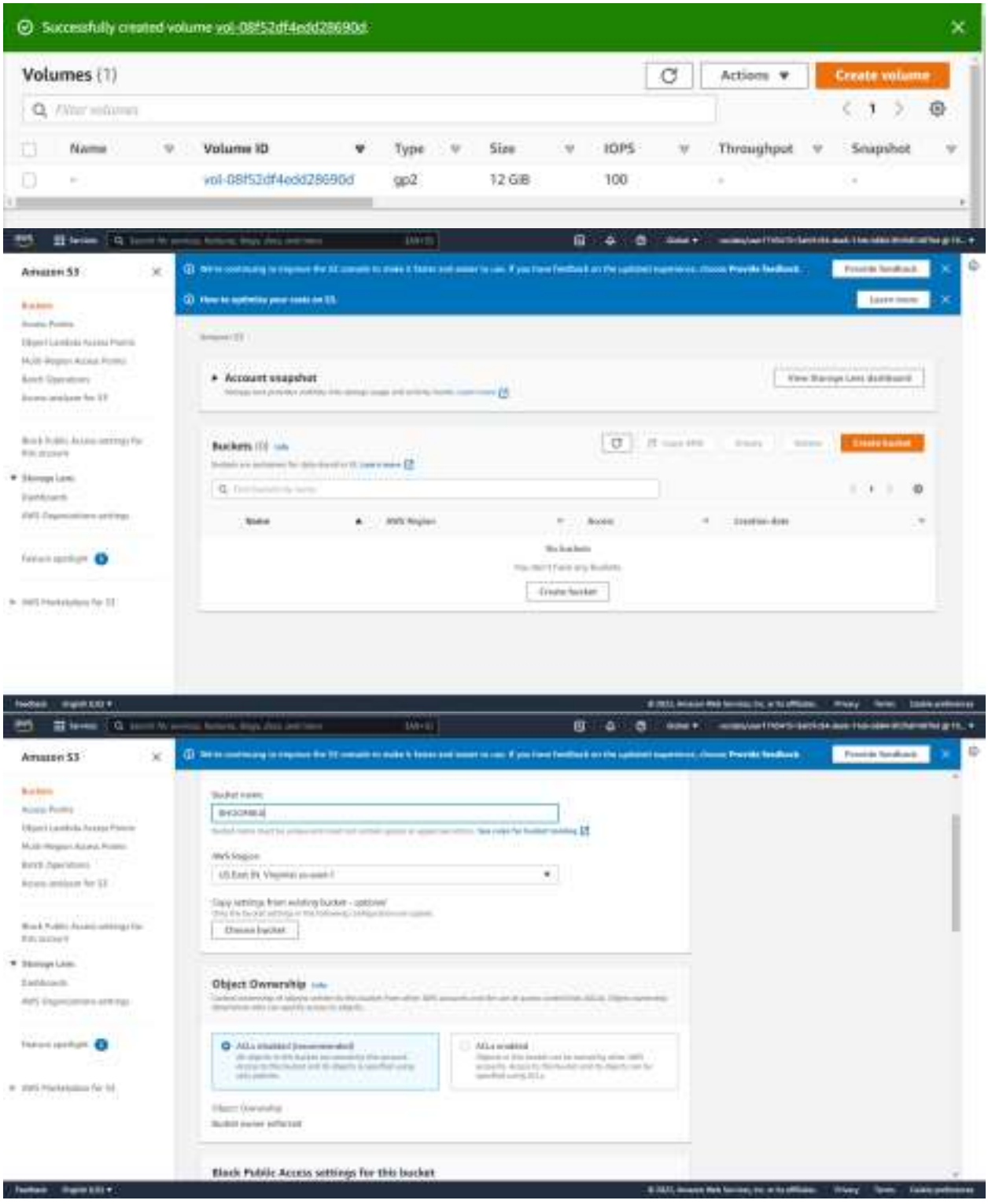
SaaS Limitations:
SaaS also poses some potential risks and challenges, as businesses must rely on outside vendors to provide the software, keep that software up and running, track and report accurate billing and facilitate a secure environment for the business's data.
a) Issues beyond customer control. Issues can arise when providers experience service disruptions, impose unwanted changes to service offerings or experience a security breach -- all of which can have a profound effect on the customers' ability to use the SaaS offering. To proactively mitigate these issues, customers should understand their SaaS provider's SLA and make sure it is enforced.
b) Customers lose control over versioning. If the provider adopts a new version of an application, it will roll out to all of its customers, regardless of whether or not the customer wants the newer version. This may require the organization to provide extra time and resources for training.
c) Difficulty switching vendors. As with using any cloud service provider, switching vendors can be difficult. To switch vendors, customers must migrate very large amounts of data. Furthermore, some vendors use proprietary technologies and data types, which can further complicate customer data transfer between different cloud providers. Vendor lock-in is when a customer cannot easily transition between service providers due to these conditions.
d) Security. Cloud security is often cited as a significant challenge for SaaS applications.

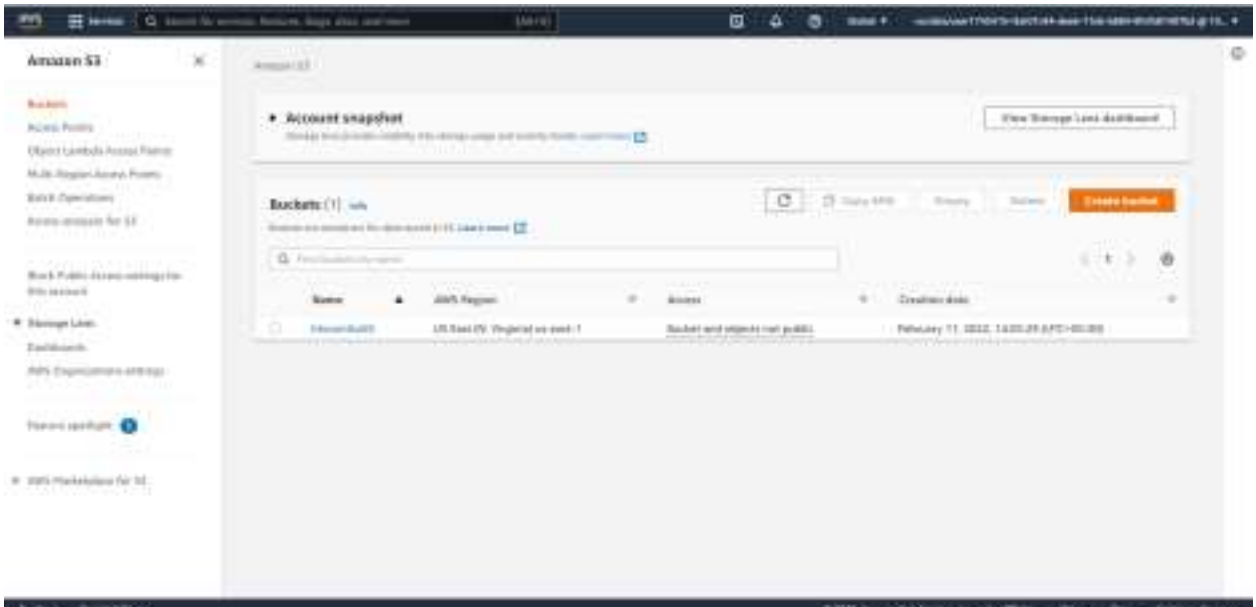
**5. Study security issues in cloud computing**
Some of the most common Security Risks of Cloud Computing
a) Data Loss
Data loss is the most common cloud security risk of cloud computing. It is also known as data leakage. Data loss is the process in which data is being deleted, corrupted, and unreadable by a user, software, or application. In a cloud computing environment, data loss occurs when our sensitive data is in somebody else's hands, one or more data elements cannot be utilized by the data owner, the hard disk is not working properly, and the software is not updated.
b) Hacked Interfaces and Insecure APIs
As we all know, cloud computing is completely depending on Internet, so it is compulsory to protect interfaces and APIs that are used by external users. APIs are the easiest way to communicate with most cloud services. In cloud computing, few services are available in the public domain. These services can be accessed by third parties, so there may be a chance that these services are easily harmed and hacked by hackers.
c) Data Breach
Data Breach is the process in which confidential data is viewed, accessed, or stolen by a third party without any authorization, so an organization's data is hacked by the hackers.
d) Vendor lock-in
Vendor lock-in is the of the biggest security risks in cloud computing. Organizations may face problems when transferring their services from one vendor to another. As different vendors provide different platforms, that can cause difficulty moving one cloud to another.
e) Increased complexity strains IT, staff
Migrating, integrating, and operating cloud services is complex for the IT staff. IT staff must require the extra capability and skills to manage, integrate, and maintain the data in the cloud.
f) Spectre & Meltdown
Spectre & Meltdown allows programs to view and steal data that is currently processed on the computer. It can run on personal computers, mobile devices, and the cloud. It can store the password, your personal information such as images, emails, and business documents in the memory of other running programs.
g) Denial of Service (DoS) attacks
Denial of service (DoS) attacks occur when the system receives too much traffic to buffer the server. Mostly, DoS attackers target web servers of large organizations such as banking sectors, media companies, and government organizations. To recover the lost data, DoS attackers charge a great deal of time and money to handle the data.
h) Account hijacking
Account hijacking is a serious security risk in cloud computing. It is the process in which an individual user's or organization's cloud account (bank account, e-mail account, and social media account) is stolen by hackers. The hackers use the stolen account to perform unauthorized activities.

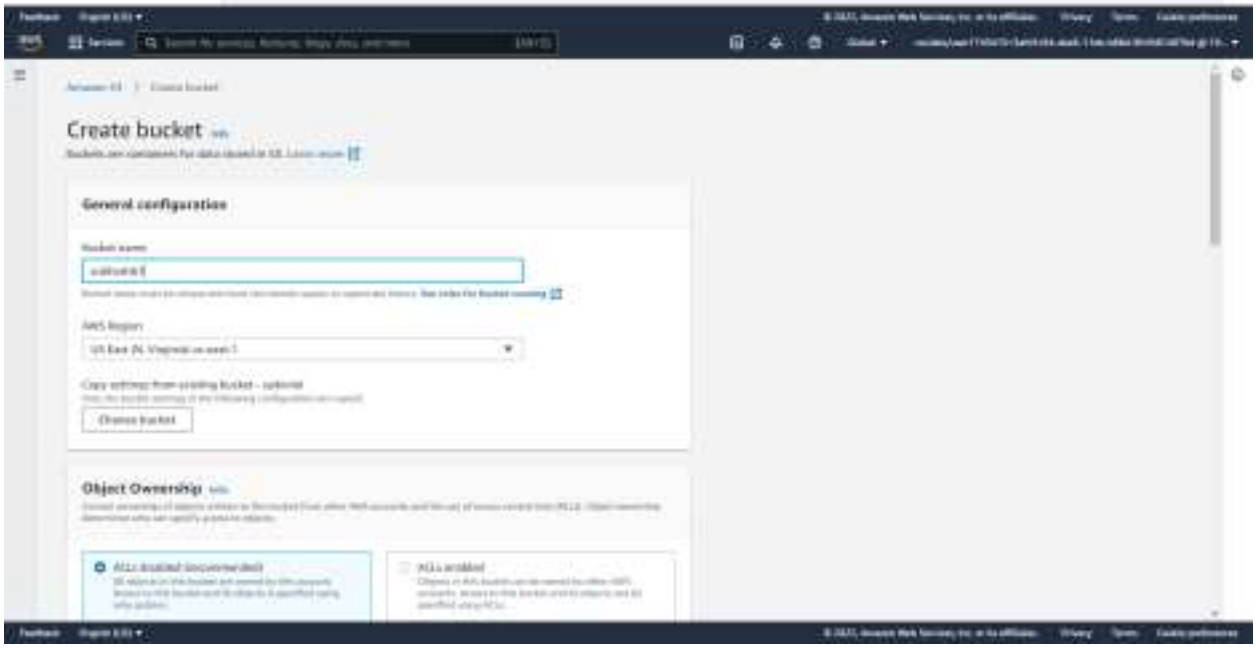
**6. Explain Server and Data Security is cloud computing**
Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures, and technologies that work together to protect cloud-based systems, data, and infrastructure. These security measures are configured to protect cloud data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business. And because

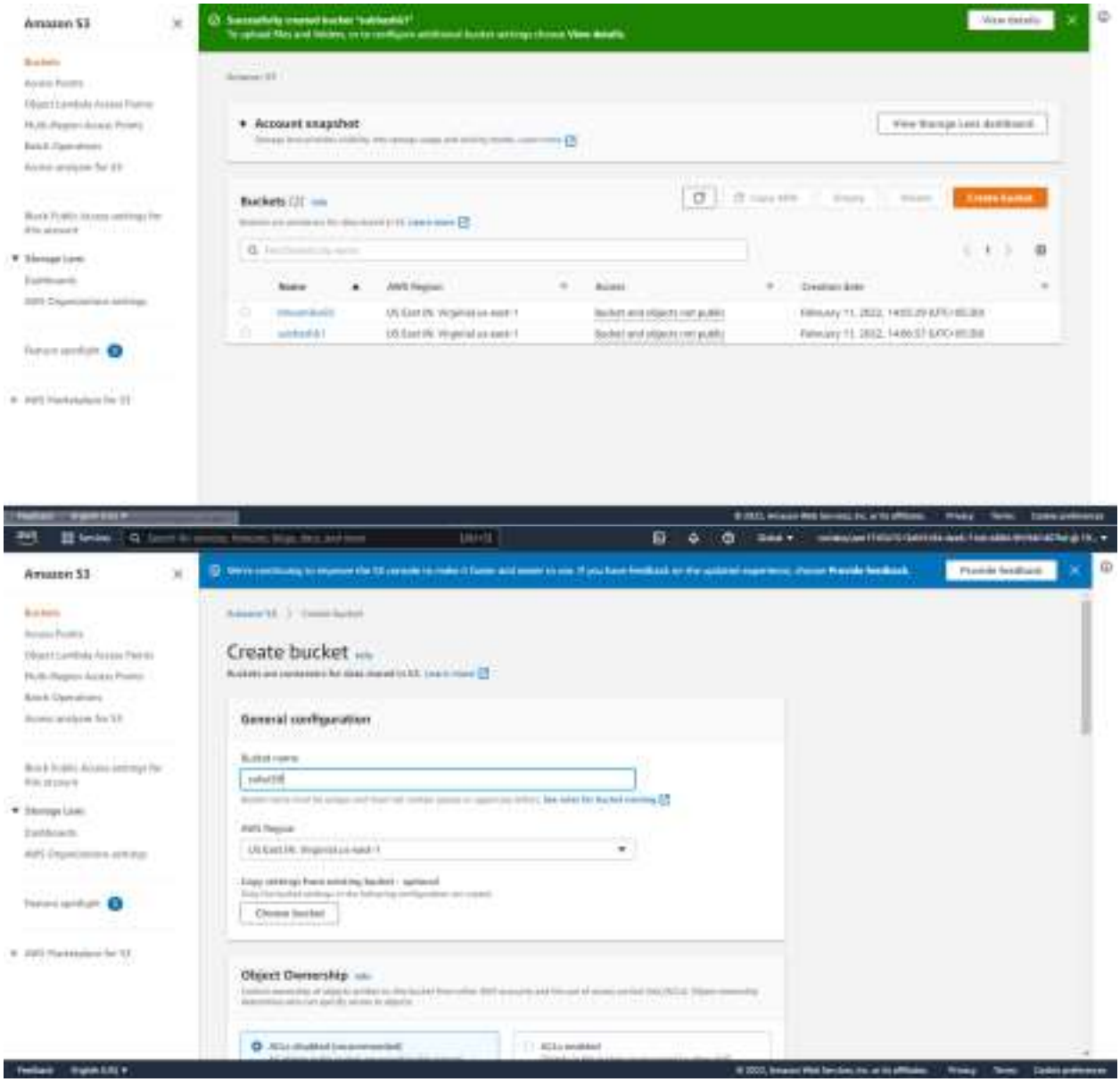
these rules can be configured and managed in one place, administration overheads are reduced and IT teams are empowered to focus on other areas of the business.
The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions in place. However, the implementation of cloud security processes should be a joint responsibility between the business owner and the solution provider.
Cloud security offers many benefits, including:
• Centralized security: Just as cloud computing centralizes applications and data, cloud security centralizes protection. Cloud-based business networks consist of numerous devices and endpoints that can be difficult to manage when dealing with shadow IT or BYOD. Managing these entities centrally enhances traffic analysis and web filtering, streamlines the monitoring of network events, and results in fewer software and policy updates. Disaster recovery plans can also be implemented and actioned easily when they are managed in one place.
• Reduced costs: One of the benefits of utilizing cloud storage and security is that it eliminates the need to invest in dedicated hardware. Not only does this reduce capital expenditure, but it also reduces administrative overheads. Where once IT teams were firefighting security issues reactively, cloud security delivers proactive security features that offer protection 24/7 with little or no human intervention.
• Reduced Administration: When you choose a reputable cloud services provider or cloud security platform, you can kiss goodbye to manual security configurations and almost constant security updates. These tasks can have a massive drain on resources, but when you move them to the cloud, all security administration happens in one place and is fully managed on your behalf.
• Reliability: Cloud computing services offer the ultimate in dependability. With the right cloud security measures in place, users can safely access data and applications within the cloud no matter where they are or what device they are using.

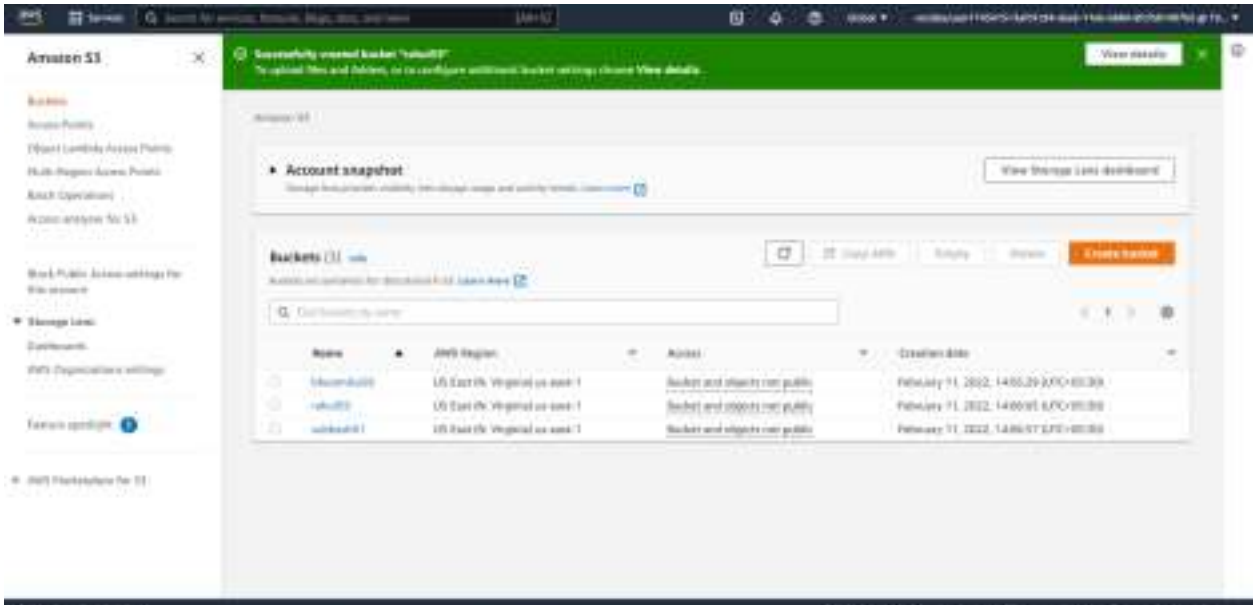


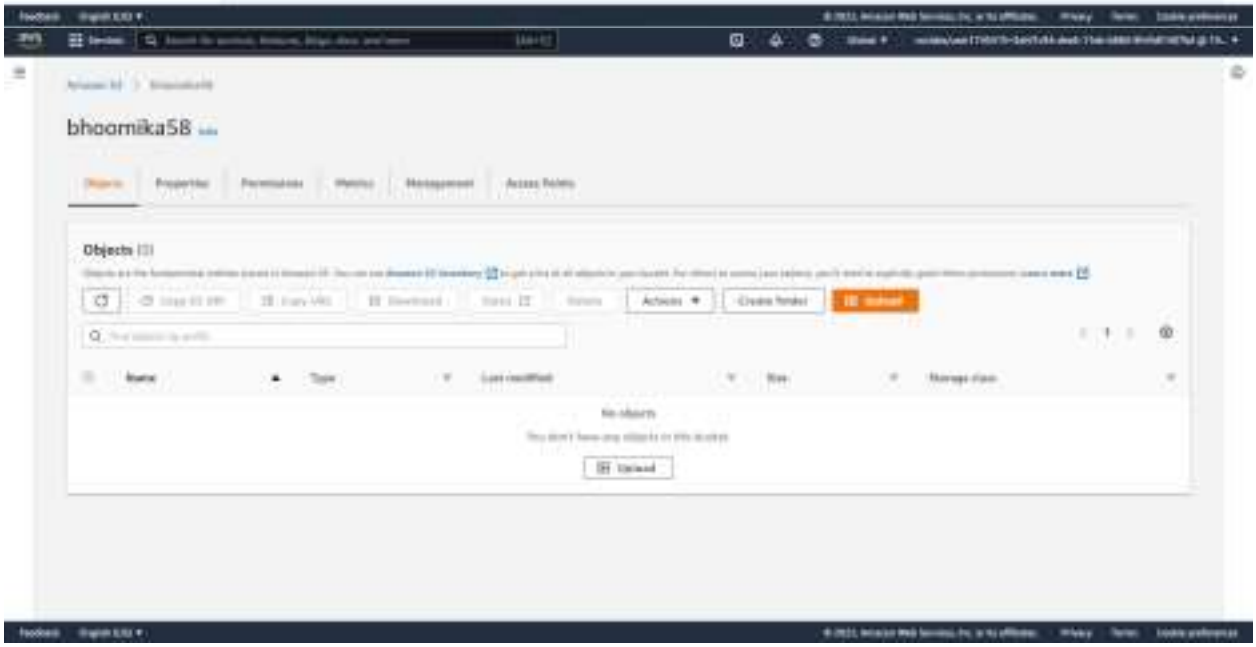

Successfully created volume vol-08f52df4edd28690d
Volumes (1)
Actions
Create volume
Name
Volume ID
Type
Size
IOPS
Throughput
Snapshot
vol-08f52df4edd28690d
gp2
12 GiB
100
Amazon S3
Account snapshot
Buckets
Create bucket
Object Ownership
Block Public Access settings for this bucket


Amazon S3
Account snapshot
Buckets (1)


Create bucket
General configuration
Object Ownership


Amazon S3
Account snapshot
Buckets
Create bucket




**Conclusion:**

1. **Why is SaaS required?**

5 reasons why you should be considering the SaaS business model for your business applications. a) Flexibility and scalability
If you aim to be successful, you will have to be flexible. If you are a business owner, you will have to be able to adjust to changes in your business and also from other external factors.
SaaS applications enable you to choose the delivery model and easily change it when your business requirement changes. It is way easier to get new users, integrate with other systems, and turn on an additional set of components.
You will be able to experiment in a less risky environment by trying on a new project, acquisition, or user base. Since your provider manages the back-end with the cloud, you do not have to be concerned about the infrastructure.
Thanks to the flexible subscription-based licensing, SaaS applications scale easily. A scale is required to manage huge amounts of data from various sources.
b) Ease of use and Speed factor
The selection and deployment of a business application have never been an easy task. Factors such as time and effort stack up, even after the implementation is successful. Cloud applications deploy faster, therefore bringing down the installation and administration efforts.
Having the ability to develop and deploy quickly will let one have a competitive edge and also the ability to speed up the business benefits.
SaaS creates value for its users much faster and also offers companies the flexibility that is needed to bring in change when they need it.
c) Great and updated features

Having the best features for your business apps can make work more interesting and can bring in high productivity among employees. Your team can use new features instantly to make informed business decisions.
Businesses with traditional applications have to spend heavily on upgrades. With SaaS, businesses are benefitted as these upgrades will be managed by the providers, letting businesses focus on or use new capabilities as and when it is available. The security and functionality are improved as it is done in the background.
d) Minimizing Application Costs
Bringing down the cost of business applications can benefit everyone, from the CXO to the individual business units, which also include the IT staff. Businesses are increasingly using a system of chargebacks, wherein the IT charges many business units for the IT services that they consume.
Given the lower infrastructure as well as maintenance costs, SaaS business applications can considerably bring down the percentage of your business unit's budget that is devoted to IT spending, which also means that you can invest in other areas while still using the latest, fully functional and highly secure business applications.
The subscription-based model not only offers great flexibility in terms of licensing, but its feature-rich apps are also quite easy to use and are custom-made for the kind of business role a user has.
In case you want to extend the capabilities of SaaS applications, your IT team can easily do so with the help of some development tools that they are already familiar with, also offered in the subscription model.
This mainly saves time, cost and brings down the investment risk. These additional extensions or features will have automatic upgrades, which means, these applications will continue to function smoothly when the underlying platform or the app is upgraded.
e) Performance and Time Management
The cloud solution deployment time is way less when compared with the on-premise systems. You can deploy a cloud-based system across many regions, thereby avoiding the cost associated with those rollouts.
No additional hardware is required, which also means that you will not be wasting time in procuring and setting up IT infrastructure and VPN access across numerous sites. You can add more users as your business expands without thinking about improving the hardware.

**2. Why cloud computing security is important.**

Cloud security, also known as cloud computing security, is a collection of security measures designed to protect cloud-based infrastructure, applications, and data. These measures ensure the authentication of users and devices, access control for data and resources, and protection of data privacy. They also support regulatory compliance.
Cloud security is critical since most organizations are already using cloud computing in one form or another. Gartner's recently reported that the worldwide market for public cloud services grew 17% in 2020, with software as a service (SaaS) remaining the largest market segment. But as companies move more data and applications to the cloud, IT professionals remain concerned about security, governance, and compliance issues when their electronic data is stored in the cloud. They worry that highly sensitive business information and intellectual property may be exposed through accidental leaks or due to increasingly sophisticated cyber threats.
Maintaining a solid cloud security posture helps organizations achieve the now widely recognized benefits of cloud computing:
a) Lower upfront costs
b) Reduced ongoing operational and administrative expenses
c) Ease of scaling
d) Increased reliability and availability
e) A whole new way of working

**References:**

https://www.techtarget.com/searchcloudcomputing/definition/Software-as-a-Service https://www.javatpoint.com/security-risks-of-cloud-computing
https://www.forcepoint.com/cyber-edu/cloud-security
https://medium.com/swlh/5-reasons-to-consider-saas-for-your-business-applications 352366564ea3
https://www.harbortg.com/blog/importance-of-cloud
security