**INTERNATIONAL SCHOOL OF   
MANAGEMENT AND TECHNOLOGY**



**FACULTY OF COMPUTING**

**ASSIGNMENT COVER SHEET**

*This form is to be completed by students submitting assignments of level 4 and level 5. Students are required to complete all sections and attach to your assignment.*

|  |  |
| --- | --- |
| STUDENT DETAILS | |
| STUDENT NAME | BISHAL THAPA |
| STUDENT ID | 2023CA05 |

|  |  |  |  |
| --- | --- | --- | --- |
| UNIT AND ASSIGNMENT DETAILS | | | |
| UNIT TITLE | Cloud Computing | | |
| UNIT NUMBER | K/618/7442 - Unit 28 | | |
| ASSIGNMENT TITLE |  | | |
| ISSUE DATE | 24/01/2024 | DUE DATE | 13/03/2024 |
| ASSESSOR NAME | Alish Gurung | | |
| ESTIMATED WORD LENGTH | 8000 | | |

|  |  |
| --- | --- |
| SUBMISSION | |
| HAND IN DATE | 13/03/2024 |

**DECLERATION AND ACKNOWLEDGEMENT**

***When submitting assignments, each student must sign a declaration confirming that the work is their own.***

*Plagiarism and Collusion*

**Plagiarism:** to use or pass off as one’s own, the writings or ideas of another without acknowledging or crediting the source from which the ideas are taken.

**Collusion:** submitting an assignment, project or report completed by another person and passing it off as one’s.

In accordance with the*Academic Integrity and Plagiarism Policy*:

1. **I declare that:**
2. this assignment is entirely my own work, except where I have included fully-documented references to the work of others,
3. the material contained in this assignment has not previously been submitted for any other subject at the University or any other educational institution, except as otherwise permitted,
4. no part of this assignment or product has been submitted by me in another (previous or current) assessment, except where appropriately referenced, and with prior permission from the Lecturer / Tutor / Unit Coordinator for this unit.
5. **I acknowledge that:**
6. if required to do so, I will provide an electronic copy of this assignment to the assessor;
7. the assessor of this assignment may, for the purpose of assessing this assignment:
8. reproduce this assignment and provide a copy to another member of academic staff;
9. communicate a copy of this assignment to a plagiarism checking service such as Plagiarism Check (which may then retain a copy of this assignment on its database for the purpose of future plagiarism checking).

|  |  |  |  |
| --- | --- | --- | --- |
| I am aware of and understand that any breaches to the Academic Code of Conduct will be investigated and sanctioned in accordance with the College Policy. | | | |
| SIGNATURE | BISHAL THAPA | DATE | 13/03/2024 |

Table of Contents

[Executive Summary 1](#_Toc159601597)

[Introduction 1](#_Toc159601598)

[Cloud Computing 1](#_Toc159601599)

[Types of Cloud Computing 2](#_Toc159601600)

[1. Infrastructure as a Service (IaaS) 2](#_Toc159601601)

[2. Platform as a Service (PaaS) 2](#_Toc159601602)

[3. Software as a Service (SaaS) 3](#_Toc159601603)

[Evolution of Cloud Computing 3](#_Toc159601604)

[Fundamental Concepts of Cloud Computing 4](#_Toc159601605)

[Architectural framework 4](#_Toc159601606)

[Design of architectural framework for cloud Computing according to requirement of The London College 5](#_Toc159601607)

[Deployment Model 6](#_Toc159601608)

[1. Public Cloud Deployment Model 6](#_Toc159601609)

[2. Hybrid Deployment Model 7](#_Toc159601610)

[3. Private Cloud Deployment Model 7](#_Toc159601611)

[Deployment model for The London College's cloud migration 7](#_Toc159601612)

[Select an appropriate model for The London College 8](#_Toc159601613)

[Company should migrate to a cloud computing solution 9](#_Toc159601614)

[1. Cost Efficiency 9](#_Toc159601615)

[2. Scalability and Flexibility 9](#_Toc159601616)

[3. Agility and Speed to Market 10](#_Toc159601617)

[4. Global Accessibility and Collaboration 10](#_Toc159601618)

[5. Enhanced Security and Compliance 10](#_Toc159601619)

[6. Disaster Recovery and Business Continuity 10](#_Toc159601620)

[7. Innovation and Access to Advanced Technologies 10](#_Toc159601621)

[8. Environmental Sustainability 10](#_Toc159601622)

[Demonstrate deployment models with Real World Example 11](#_Toc159601623)

[Justification for the tools chosen to convince concerned people for a cloud computing solution 12](#_Toc159601624)

[1. Amazon S3 (Simple Storage Service) 13](#_Toc159601625)

[2. Amazon SNS (Simple Notification Service) 13](#_Toc159601626)

[3. Amazon QuickSight 13](#_Toc159601627)

[4. Amazon WorkDocs 14](#_Toc159601628)

[5. AWS Lambda 14](#_Toc159601629)

[6. AWS CloudTrail 14](#_Toc159601630)

[7. VPC (Virtual Private Cloud) 15](#_Toc159601631)

[8. Load Balancer 15](#_Toc159601632)

[9. EC2 Instance 15](#_Toc159601633)

[10. Autoscaling Group 16](#_Toc159601634)

[11. Nat Gateway (Network Address Translation) 16](#_Toc159601635)

[12. Internet Gateway 16](#_Toc159601636)

[13. Route Table 16](#_Toc159601637)

[14. Security Group 17](#_Toc159601638)

[15. Database 17](#_Toc159601639)

[Conclusion 19](#_Toc159601640)

[Introduction 19](#_Toc159601641)

[Configure a Cloud Computing Platform with AWS Framework 19](#_Toc159601642)

[Implement a Cloud Computing Platform using Open-Source Tools 34](#_Toc159601643)

[1. OpenStack for Private Cloud Management 35](#_Toc159601644)

[1. Kubernetes for Container Orchestration 35](#_Toc159601645)

[2. Docker for Containerization 35](#_Toc159601646)

[3. Ansible for Configuration Management 35](#_Toc159601647)

[4. Prometheus and Grafana for Monitoring and Metrics 36](#_Toc159601648)

[Potential issues and constraints that may arise during the development process of the cloud computing solutions 36](#_Toc159601649)

[The issues and contractions faced during the development process can be overcome 37](#_Toc159601650)

[Conclusion 39](#_Toc159601651)

[Introduction 39](#_Toc159601652)

[Most common problems that arise in a cloud computing platform and discuss appropriate solutions 39](#_Toc159601653)

[Assessment of Common Contemporary Security Issues in the Cloud Environment 41](#_Toc159601654)

[Addressing and Overcoming Common Contemporary Security Issues in Building a Secured Cloud Computing Platform 42](#_Toc159601655)

[London College should protect its data when migrating to the cloud solutio 45](#_Toc159601656)

[Conclusion 46](#_Toc159601657)

[References 47](#_Toc159601658)

# Executive Summary

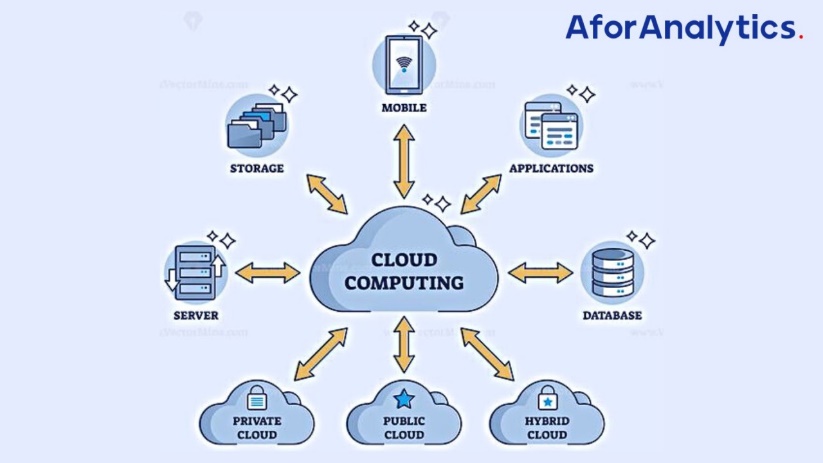
The purpose of this report is to outline the migration process of The London College's on-premises servers to the AWS Cloud. Siddhartha Cloud Computing Pvt. Ltd. has been engaged in facilitating this migration, and I, as the Cloud Administrator, have undertaken various tasks to ensure a seamless transition. The components of this migration are the design of a three-tier AWS Virtual Private Cloud, incorporating an Internet Gateway to establish a secure and controlled pathway for inbound and outbound internet traffic, creating of NAT Gateways for outbound internet connectivity and implementation of security groups for traffic control as well as configuration of auto-scaling groups for EC2 instances, and the setup of an Application Load Balancer for efficient traffic distribution.

# Introduction

In an era where technological advancements shape the landscape of educational institutions, The London College stands at a pivotal moment in its IT infrastructure evolution. The decision to explore cloud computing is not merely a technical pivot but a strategic move towards enhanced scalability, cost-efficiency, and global accessibility. This report serves as a compass, guiding the college through the intricate realms of cloud computing, analyzing its evolution, and delineating a tailored architectural framework. The impending migration is not just about shifting data; it’s about future-proofing the institution’s IT capabilities, fostering innovation, and ensuring a resilient foundation for the years to come.

# Cloud Computing

Cloud Computing is similar, to leasing computer power and storage of possessing and upkeeping your own physical hardware. It provides a means to utilize computing resources such as servers and databases without the necessity of having them on site. Through cloud computing you can execute applications, store and manage data and carry out tasks via the internet. This technology offers adaptability, scalability and cost efficiency as you only pay for the resources utilized. Essentially it's akin to having an, on demand IT infrastructure that you can access whenever required (Amazon, 2023).



# Types of Cloud Computing

# Infrastructure as a Service (IaaS)

Infrastructure, as a Service (IaaS) is similar to having a virtual data center in the cloud. It offers the elements of computing infrastructure without requiring ownership of hardware. With IaaS it's like leasing servers, storage and networking parts, via the internet. This approach provides adaptability and scalability enabling users to adjust resources according to their requirements. It empowers businesses to oversee their applications, operating systems and software components while the cloud service provider takes care of the underlying hardware and infrastructure upkeep. Essentially IaaS lets users concentrate on their applications and data without dealing with the intricacies of managing servers.

# Platform as a Service (PaaS)

PaaS or Platform, as a Service is similar to having a workshop, for developing applications. It simplifies the development process by providing an all platform with tools, middleware and other key components. Developers benefit from a simplified environment, allowing them to focus solely on coding and creating applications without the hassle of managing underlying infrastructure. PaaS accelerates deployment and enhances resource efficiency, providing a robust foundation for innovation in software development. It's like having a supportive environment that handles operational intricacies, empowering developers to concentrate on their core expertise – crafting high-quality software.

# Software as a Service (SaaS)

Using Software as a Service (SaaS) means using software applications of installing them on your device. It's similar, to signing up for a service that offers to use applications whenever you need them. SaaS lets users benefit from using applications, without the hassle of installation, upkeep or upgrades. It's similar to having a software tool that you can access from any device, with an internet connection making tasks smooth and effortless. SaaS is all about simplicity and accessibility, providing a user experience where the software is hosted and maintained by a third party provider (Rajeswari, 2019).

# Evolution of Cloud Computing

The evolution of cloud computing has been a dynamic journey characterized by significant technological milestones and transformative shifts in computing paradigms. In its inception during the late 1990s and early 2000s, the concept emerged with utility computing models and the rise of Application Service Providers (ASPs). Despite laying the groundwork for on-demand computing, this phase faced challenges related to security and standardization. The mid-2000s witnessed a crucial development with the proliferation of virtualization technologies, enabling multiple virtual machines on a single server and setting the stage for scalable cloud architectures. In the 2000s Infrastructure, as a Service (IaaS) began to gain prominence with Amazon Web Services (AWS) unveiling Elastic Compute Cloud (EC2) making scalable computing resources more accessible through a pay as you go model. Over time there was a progression towards Platform as a Service (PaaS) and Software, as a Service (SaaS) making application development and deployment more straightforward. Hybrid and multi-cloud models gained traction in the late 2010s, offering flexibility but introducing challenges of interoperability. The mid-2020s witnessed a focus on edge computing and serverless architectures, addressing latency concerns and further abstracting operational complexities. This multifaceted evolution reflects the continuous adaptation of cloud computing to technological advancements and evolving business requirements, shaping the contemporary landscape of digital infrastructure (Padhy, 2012).

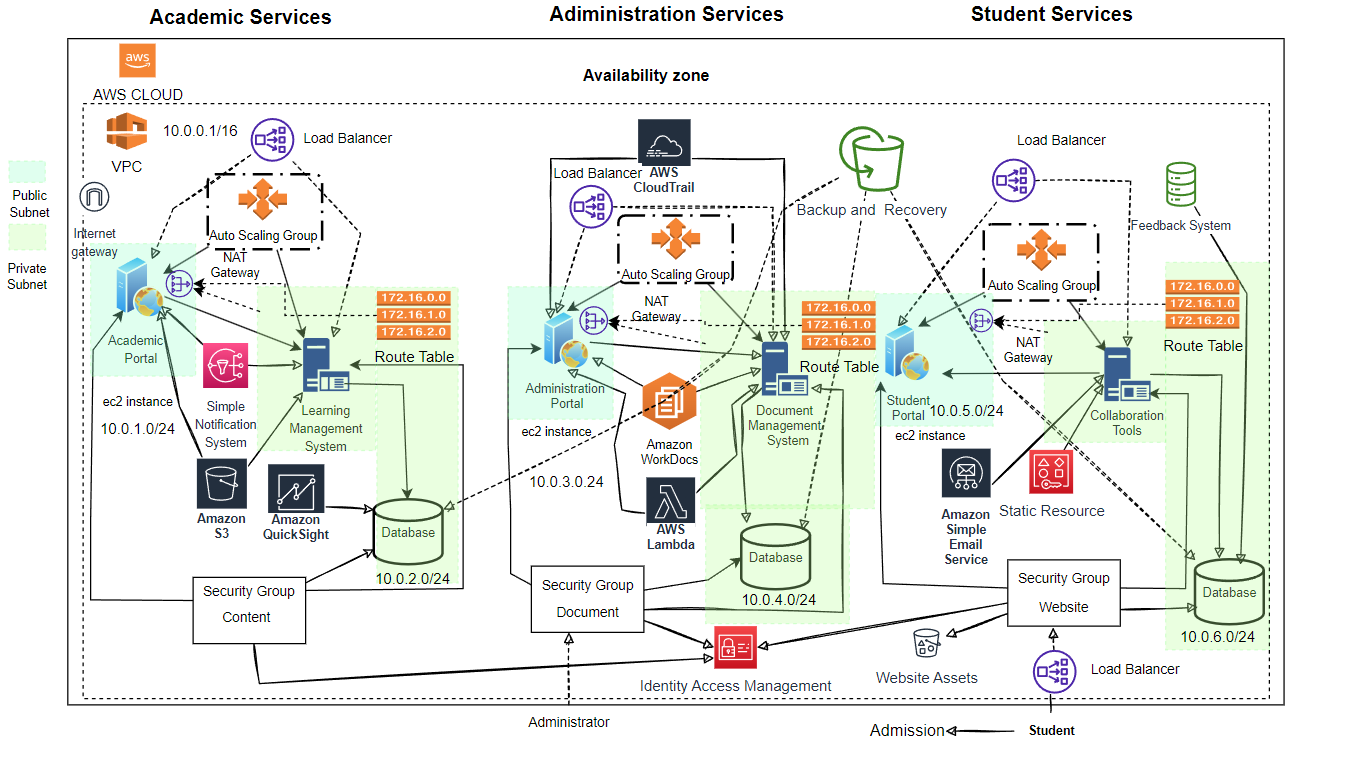
# Fundamental Concepts of Cloud Computing

The fundamental concepts of cloud computing form the cornerstone of its transformative impact on information technology. Virtualization is a key concept, allowing the abstraction of physical hardware into virtual instances, optimizing resource utilization and facilitating the dynamic allocation of computing power. On-demand self-service is another critical concept, enabling users to provision and manage resources autonomously as needed. This self-service aspect promotes agility and efficiency in resource utilization. Resource pooling involves the provider's computing resources being pooled to serve multiple customers, leading to economies of scale and enhanced efficiency. Rapid elasticity allows for automatic scaling of resources to accommodate varying workloads, ensuring optimal performance during peak demands. Moreover, broad network access ensures ubiquitous connectivity to cloud services, facilitating remote access and flexibility. These fundamental concepts reveal a cohesive framework that underpins the adaptability, scalability, and cost-effectiveness inherent in cloud computing. Together, these concepts have revolutionized the IT landscape, offering a paradigm shift in how computing resources are delivered, accessed, and managed (Brandao, 2018).

# Architectural framework

An architectural framework in cloud computing is like the blueprint that guides the design and organization of cloud-based systems. It serves as a structured approach to building and deploying applications in the cloud. Think of it as a set of principles, guidelines, and best practices that provide a clear structure for designing scalable, secure, and efficient cloud solutions. This framework encompasses the overall structure, components, and interactions within a cloud system, addressing key aspects such as data storage, processing, networking, and security. It helps architects and developers make informed decisions about how to structure their applications and leverage cloud services effectively. In essence, the architectural framework acts as a roadmap, ensuring that cloud solutions align with business objectives while optimizing performance, reliability, and security in the cloud environment (Tang, 2019).

# Design of architectural framework for cloud Computing according to requirement of The London College



In designing The London College's cloud computing solution, I've carefully crafted a comprehensive three-tier structure, placing each layer strategically within the Virtual Private Cloud (VPC) to ensure a secure and scalable environment. In the Presentation Layer you'll come across the Academic Portal, Administrative Portal and Student Portal located in subnets (10.0.1.0/24, 10.0.3.0/24 and 10.0.5.0/24 respectively) allowing access, to the internet. On the hand the Application Layer consists of the Learning Management System (LMS) Document Management System (DMS) and Collaboration Tools placed in subnets (10.0.2.0/24, 10.0.4.0/24 and 10.0.6.0/24 respectively) to bolster security and segregation. The Data Layer hosts Academic, Administrative, and Student Databases in private subnets (10.0.2.0/24 and 10.0.4.0/24 and 10.0.6.0/24), ensuring secure data storage and retrieval.

To improve functionality based on needs I've included elements like NAT Gateways, Security Groups ,Auto Scaling Groups and Load Balancers into the system setup. NAT Gateways help with outbound internet connectivity for subnets to ensure interactions, with external services. Meticulously configured Security Groups enforce communication rules between layers, fortifying the VPC's security.

Strategically deploying Auto Scaling Groups and Load Balancers guarantees scalability and high availability across instances. Load Balancers play a crucial role in efficiently distributing traffic between Academic Portal and LMS, Administrative Portal and DMS, as well as Student Portal and Collaboration Tools. These load balancers contribute to fault tolerance, optimized resource utilization, and improved performance, aligning with The London College's specific needs.

In addition, I've incorporated an Internet Gateway and Amazon Route 53 to enhance connectivity and reliability. The Internet Gateway facilitates seamless communication between the VPC and the internet, while Amazon Route 53 ensures efficient domain name system (DNS) management.

Centralized components like Identity Management, Logging and Monitoring, and Backup and Recovery have been thoughtfully integrated across all services to ensure unified identity management, comprehensive observability, and centralized data protection.

In summary, my architectural framework meticulously addresses The London College's specific requirements, establishing a secure, scalable, and interconnected cloud infrastructure. The strategic placement of components and integration of key services contribute to the efficiency, reliability, and performance of the cloud computing solution tailored for the educational institution (Tang, 2019).

# Deployment Model

# Public Cloud Deployment Model

The Public Cloud Deployment Model is like having a shared, virtualized environment accessible to the general public over the internet. It's as if you're renting computing resources and services from third-party providers. In this model, cloud services, such as storage, applications, and virtual machines, are made available to multiple users, fostering scalability and cost-effectiveness. Public clouds are managed and operated by external providers. They handle tasks, like infrastructure maintenance and resource allocation. The pay as you go model available to users allows them to only pay for the resources they actually use. This particular deployment model is great for businesses that value flexibility, quick scalability and cost effectiveness, without the burden of managing their own infrastructure.

# Hybrid Deployment Model

The Hybrid Cloud Deployment Model is similar, to enjoying the benefits of both private clouds offering an approach that combines key features from each. It's as if you're orchestrating a mix of dedicated resources and services from both on-premises infrastructure and external cloud providers. In this model, businesses can enjoy the flexibility and scalability of the public cloud for non-sensitive operations while keeping critical data and applications in a private cloud for enhanced security. The hybrid approach offers a balanced solution, allowing seamless data flow and workload portability between the two environments. This model provides the versatility to scale resources as needed and is well-suited for organizations with dynamic and evolving IT requirements.

# Private Cloud Deployment Model

The Private Cloud Deployment Model is similar, to having a cloud infrastructure tailored for an organization. It's like creating your customizable cloud setup whether it's on site or, through an external service provider. In this model, resources and services are not shared with other organizations, offering greater control, security, and customization options. Private clouds are well-suited for businesses with specific compliance requirements or those handling sensitive data. Organizations maintain direct management over the infrastructure, allowing for tailored configurations to meet their unique needs. While the setup and maintenance demand more resources, the private cloud provides a level of privacy and control that makes it an ideal choice for certain enterprises (B. Patel, 2021).

# Deployment model for The London College's cloud migration

The most suitable deployment model for The London College's cloud migration is a Hybrid Cloud Deployment. This approach seamlessly integrates on-premises infrastructure with cloud-based resources, striking a balance between the advantages of public and private clouds. One compelling reason for choosing a hybrid model is the sensitivity of certain academic, administrative, or student-related data that may be subject to privacy regulations. By keeping sensitive data on-premises, the college can ensure compliance with data protection standards. Additionally, a hybrid model offers scalability and flexibility, allowing the institution to dynamically scale resources based on demand, particularly during peak academic sessions. This approach optimizes costs by leveraging existing on-premises infrastructure for certain workloads while selectively migrating others to the cloud. It accommodates dependencies on legacy systems that might be challenging to migrate entirely to the cloud, enabling the college to modernize gradually. Moreover, a hybrid cloud strategy provides robust disaster recovery and redundancy, ensuring business continuity in the event of on-premises failures. Enhanced collaboration and connectivity between on-premises systems and cloud services are facilitated, enhancing overall organizational efficiency. In summary, a hybrid cloud deployment for The London College offers the flexibility to adapt to changing needs, ensures compliance, optimizes costs, enables modernization, and enhances resilience and collaboration (Patel, 2021).

# Select an appropriate model for The London College

The London College can see improvements by exploring service models, like Infrastructure as a Service (IaaS) Platform as a Service (PaaS) and Software, as a Service (SaaS). Each of these choices comes with its benefits depending on the needs at hand. Each of these options offers advantages based on requirements. IaaS provides the building blocks allowing the college to have control and management over their infrastructure. This includes servers, storage and networking resources. PaaS offers a layer that enables the development and deployment of applications without the complexities of managing the underlying infrastructure. On the hand SaaS delivers ready to use software applications, which means that the college won't have to worry about software development or maintenance. Considering the multifaceted needs of an educational institution like The London College, a Platform as a Service (PaaS) model emerges as a particularly suitable choice. PaaS streamlines application development and deployment, allowing the institution to focus on creating and enhancing its educational applications without concerning itself with the intricacies of infrastructure management. A pertinent real-world example is the adoption of PaaS by educational platforms like Canvas by Instructure. Canvas, a cloud-based learning management system, enables institutions to leverage a pre-built platform for managing and delivering educational content. This aligns with The London College's objectives of enhancing educational services without the burden of extensive infrastructure management.

By adopting a PaaS model, The London College can accelerate application development, reduce time-to-market, and enhance overall agility. This service model empowers educators and administrators to concentrate on creating innovative educational content and applications while relying on a robust and scalable platform. The inherent abstraction of infrastructure complexities in PaaS aligns with the college's goal of efficient resource utilization. Additionally, the PaaS model facilitates collaboration, allowing multiple stakeholders to contribute to the development and improvement of educational applications.

In conclusion, selecting a Platform as a Service (PaaS) model for The London College provides a balance between infrastructure control and application development efficiency. This choice supports the institution's goals of delivering quality educational services while streamlining the development and deployment of applications, as exemplified by successful platforms like Canvas in the education sector (Rajeswari, 2019).

# Company should migrate to a cloud computing solution

Migrating to a cloud computing solution offers companies a plethora of compelling reasons that extend beyond mere technological advancements. The decision to embrace cloud computing is often driven by a combination of strategic, operational, and financial considerations.

## Cost Efficiency

A major reason why businesses opt for cloud migration is the chance to save money. By moving to the cloud companies can cut down on expenses related to maintaining infrastructure, such, as costs, for power and cooling. Cloud service providers provide flexible pricing options where organizations pay based on their usage leading to improved cost effectiveness.

## Scalability and Flexibility

Cloud computing offers scalability enabling businesses to adjust resources according to demand. This flexibility is crucial for businesses with fluctuating workloads, ensuring they can meet peak demands without over-provisioning resources during quieter periods (Sether, 2016).

## Agility and Speed to Market

Cloud services empower companies to deploy applications and services swiftly, reducing time-to-market for new products or features. The agility provided by the cloud fosters innovation, enabling businesses to respond rapidly to market changes and stay ahead of the competition.

## Global Accessibility and Collaboration

Cloud computing enables people from, around the world to access data and software making it possible for employees to work together smoothly no matter where they are located. This is especially important, in todays interconnected business world, where remote work and international teamwork are becoming more prevalent.

## Enhanced Security and Compliance

Leading cloud providers invest heavily in security measures, often surpassing what individual companies can afford. Cloud platforms employ advanced security protocols, encryption, and compliance certifications, providing a robust security framework that helps safeguard sensitive data and ensures regulatory compliance.

## Disaster Recovery and Business Continuity

Cloud-based solutions offer robust disaster recovery capabilities, ensuring data redundancy and backup. This minimizes the risk of data loss and downtime, contributing to a comprehensive business continuity strategy. In contrast, companies relying solely on on-premises infrastructure may face challenges in implementing and maintaining effective disaster recovery plans (Xue, 2016).

## Innovation and Access to Advanced Technologies

Cloud providers regularly update their infrastructure with the latest technologies. By migrating to the cloud, companies gain access to cutting-edge tools, machine learning, artificial intelligence, and other innovative solutions without the burden of managing the underlying technology stack.

## Environmental Sustainability

Cloud computing can contribute to a company's sustainability goals by optimizing resource utilization. Cloud providers typically operate in energy-efficient data centers, and the ability to scale resources based on demand can lead to lower overall energy consumption compared to maintaining on-premises data centers.

While the benefits of cloud migration are substantial, companies may face challenges during the transition, including data migration complexities, integration issues with existing systems, and potential resistance to change from employees. Failure to migrate to a cloud computing solution may result in missed opportunities for innovation, reduced competitiveness, higher operational costs, and a greater exposure to security risks. Therefore, the decision to migrate to the cloud should be a well-considered strategic move, weighing the potential benefits against the challenges and long-term goals of the organization (Moscoso-Zea, 2018).

Hybrid cloud deployment presents a compelling solution for educational institutions like The London College, which must balance the need for stringent data security and compliance with the desire for flexibility, scalability, and cost-effectiveness in their IT infrastructure.

# Demonstrate deployment models with Real World Example

In the case of The London College, a real-world example of why hybrid cloud deployment is chosen can be illustrated by examining its requirements and challenges. As an educational institution, The London College collects and manages sensitive student data, including personal information, academic records, and financial details. Compliance with data protection regulations such as GDPR (General Data Protection Regulation) is paramount to safeguarding student privacy and ensuring legal compliance.

To meet these regulatory requirements and maintain control over sensitive data, The London College may opt for a private cloud infrastructure hosted on-premises or within a dedicated data center. This private cloud environment offers the necessary security measures, access controls, and encryption mechanisms to protect student information from unauthorized access or data breaches.

However, The London College also faces demands for scalability, accessibility, and collaboration in its educational services. For example, the college may need to deploy online learning platforms, collaboration tools, and administrative applications that require dynamic scaling and remote access capabilities to accommodate students, faculty, and staff spread across various locations (B. Patel, 2021).

The college can leverage public cloud services such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP) to augment its private cloud infrastructure. By adopting a hybrid cloud deployment model, The London College can host non-sensitive workloads, such as website hosting, email services, and development environments, on the public cloud. For instance, The London College might utilize AWS for hosting its public-facing website, which can handle fluctuating traffic volumes efficiently and benefit from AWS's global network infrastructure for fast and reliable content delivery. At the same time, critical student data and internal systems remain securely housed within the private cloud environment.

The hybrid cloud architecture enables seamless integration and data exchange between the private and public cloud environments, allowing The London College to leverage the scalability, agility, and cost-effectiveness of public cloud services while maintaining control over sensitive data and ensuring compliance with regulatory requirements. Moreover, by implementing hybrid cloud deployment, The London College gains access to a wide range of cloud-based services and tools for enhancing teaching and learning experiences, supporting research initiatives, and optimizing administrative processes. For example, the college can leverage cloud-based analytics platforms for data-driven decision-making, deploy virtual desktop infrastructure (VDI) solutions for remote learning, and implement collaboration tools for faculty and students (Patel, 2021).

In summary, the adoption of hybrid cloud deployment by educational institutions like The London College reflects a strategic approach to balancing data security, compliance, and innovation in the digital age. By leveraging the strengths of both private and public cloud environments, The London College can effectively meet the diverse needs of its academic community while ensuring the confidentiality, integrity, and availability of sensitive student information.

# Justification for the tools chosen to convince concerned people for a cloud computing solution

During the choosing tools for The London College's cloud computing solution, a careful selection process was undertaken to ensure optimal performance, security, and scalability. The tools selected are AWS-native services, leveraging the robust infrastructure and services provided by Amazon Web Services.

## Amazon S3 (Simple Storage Service)

In addressing the multifaceted challenges of The London College's migration, Amazon S3 stands out as a cornerstone for efficient data storage. The current on-premises servers may encounter limitations in scalability and accessibility, hindering the college's ability to handle growing volumes of academic and administrative data. Amazon S3, a scalable object storage service, not only offers a virtually unlimited capacity but also ensures durability and high availability. Its straightforward and cost-effective model allows The London College to seamlessly manage data, supporting diverse applications and use cases within the academic environment (Jena, 2020).

## Amazon SNS (Simple Notification Service)

Effective communication during the migration process is pivotal to minimize disruptions and maintain transparency. Amazon SNS serves as a strategic choice for The London College to disseminate timely notifications across various communication channels. As the college navigates through different phases of migration, stakeholders need to be informed promptly about updates, potential downtimes, and completed tasks. The versatility of Amazon SNS, supporting email, SMS, and other notification mechanisms, ensures that the relevant parties are kept in the loop. This proactive communication approach minimizes confusion, fosters collaboration, and contributes to an overall smooth migration experience.

## Amazon QuickSight

In the realm of data analytics and visualization, Amazon QuickSight emerges as a powerful tool for The London College. The institution deals with vast datasets encompassing student records, academic performance metrics, and administrative workflows. QuickSight's ability to provide interactive dashboards and business intelligence facilitates insightful data-driven decision-making. The visualizations not only streamline complex data but empower faculty and administrators to gain meaningful insights effortlessly. This tool is not merely about data representation but fundamentally contributes to an institution-wide culture of informed decision-making and continuous improvement (Chafi, 2021).

## Amazon WorkDocs

Collaboration is the heartbeat of any academic institution, and Amazon WorkDocs has been chosen to address the nuances of document management and collaborative work. The London College, like many others, faces the challenge of ensuring secure, version-controlled document sharing among faculty and staff. Amazon WorkDocs, with its robust access controls, real-time collaboration features, and versioning capabilities, becomes a central hub for document sharing. This tool ensures that faculty members and administrative staff can collaborate seamlessly, fostering efficiency and ensuring that the most up-to-date information is readily available.

## AWS Lambda

Automation plays a pivotal role in streamlining tasks and processes, especially during complex migrations. AWS Lambda is strategically selected to bring automation to the forefront of The London College's cloud computing solution. In the dynamic landscape of migration, various manual tasks such as database updates, log management, and system configurations may arise. AWS Lambda's serverless architecture eliminates the need for managing servers, allowing The London College to execute code precisely when needed. This not only enhances operational efficiency but also ensures that routine tasks are automated, reducing the risk of manual errors and enabling a more agile IT environment.

## AWS CloudTrail

Security and compliance are paramount considerations in The London College's migration journey. AWS CloudTrail is meticulously chosen to provide comprehensive visibility into user activity and resource changes within the AWS environment. As the college transitions to the cloud, maintaining governance, compliance, and risk auditing becomes a critical aspect. AWS CloudTrail records API calls, offering detailed insights that are invaluable for detecting unauthorized activities and ensuring a secure and compliant cloud infrastructure. This tool acts as a crucial component in the overall security strategy, aligning with best practices and bolstering The London College's commitment to a secure cloud environment (Kaleem, 2015).

## VPC (Virtual Private Cloud)

A Virtual Private Cloud (VPC) plays a role, in The London Colleges computing setup. It provides a logically isolated section within the AWS Cloud, allowing the institution to securely host its resources. Utilizing a VPC ensures that The London College has control over its network environment, including IP address ranges, subnets, and routing tables. This level of isolation enhances security by enabling the college to define its own virtual network and configure it to meet specific requirements. The VPC acts as a secure foundation for hosting various services, aligning with best practices for network segmentation and resource organization in the cloud.

## Load Balancer

The inclusion of a Load Balancer is a strategic choice in The London College's cloud architecture. A Load Balancer helps distribute incoming network traffic across multiple EC2 instances, ensuring optimal resource utilization and preventing any single server from becoming a bottleneck. This results in improved fault tolerance and availability of applications. The Load Balancer, specifically the Application Load Balancer (ALB) in this scenario, plays a crucial role in enhancing the overall performance and reliability of the college's services. It also facilitates efficient traffic distribution, supporting seamless scalability during peak demands.

## EC2 Instance

The cloud infrastructure of The London College relies heavily on Amazon Elastic Compute Cloud (EC2) instances. These virtual servers offer scalable compute capacity, allowing the institution to run applications and services without the need to invest in physical hardware. EC2 instances provide flexibility in choosing the type of instance based on specific workloads, ensuring optimized performance. The ability to scale instances up or down based on demand aligns with the dynamic nature of the college's computing needs, providing cost-efficiency and responsiveness to changing requirements (Chafi, 2021).

## Autoscaling Group

The implementation of an Autoscaling Group is crucial for ensuring elasticity and responsiveness in The London College's cloud environment. By automatically adjusting the number of EC2 instances based on demand, the Autoscaling Group optimizes resource utilization, providing cost savings during periods of lower activity and scaling up during peak loads. This dynamic scaling ensures that the college's applications can handle varying workloads efficiently. The Autoscaling Group is an integral part of maintaining high availability, reliability, and performance in a cost-effective manner.

## Nat Gateway (Network Address Translation)

A Nat Gateway is a key element in enabling outbound internet connectivity for private subnets within The London College's VPC. It acts as a conduit for instances in private subnets to access the internet while keeping them secure from incoming traffic initiated from the internet. Nat Gateway plays a crucial role in maintaining the security and integrity of the private subnets, allowing them to communicate with external services and resources. This ensures that the college's applications and services can access necessary updates and external data sources while maintaining a robust security posture.

## Internet Gateway

An Internet Gateway is an essential component for The London College's cloud architecture, providing a secure and controlled pathway for internet communication to and from the AWS resources within the VPC. It facilitates outbound and inbound traffic, allowing the college's services to interact with the broader internet while maintaining a secure and controlled network environment. The Internet Gateway is instrumental in supporting web applications, updates, and other internet-dependent functionalities, ensuring a seamless integration of cloud services with external online resources (Patel, 2021).

## Route Table

The utilization of a Route Table is integral to The London College's cloud network architecture. A Route Table defines the rules for routing network traffic within the VPC, ensuring efficient communication between different subnets and controlling traffic flow. By strategically configuring route tables, the college can direct traffic to the appropriate destination, optimizing network performance and security. This granular control over routing enhances the overall flexibility and manageability of the VPC, aligning with best practices for network architecture in a cloud environment.

## Security Group

Security Groups are a critical component in The London College's cloud infrastructure, providing a virtual firewall for controlling inbound and outbound traffic to and from AWS resources. By defining rules within Security Groups, the institution can enforce strict access controls, allowing only necessary communication and blocking unauthorized access. This level of security granularity ensures a robust defense against potential threats, aligning with best practices for securing cloud environments. Security Groups play a pivotal role in maintaining the confidentiality, integrity, and availability of the college's services and data.

## Database

The choice of a reliable database is paramount in The London College's cloud computing solution. Amazon Relational Database Service (RDS) with the MySQL database engine is selected for its robust features, including automated backups, high availability, and scalability. MySQL is a widely-used, open-source relational database management system known for its performance and reliability. RDS eliminates the burden of database management tasks, allowing the college to focus on core academic functions. Its compatibility with the MySQL engine provides flexibility, and the automated updates ensure that the database environment is secure and up-to-date. The use of Amazon RDS with the MySQL edition is justified by MySQL's ability to handle the diverse data needs of the institution efficiently, contributing to a seamless and responsive cloud infrastructure.

In conclusion, the additional tools, including the Virtual Private Cloud (VPC), Load Balancer, EC2 instances, Auto Scaling Group, NAT Gateway, Internet Gateway, Route Table, Security Group, and the selected Amazon RDS with the MySQL edition, enhance the cloud computing solution for The London College. The VPC ensures a secure and isolated network environment, meeting compliance requirements. The Load Balancer optimizes traffic distribution for high availability, while EC2 instances offer flexible and scalable computing resources. The Auto Scaling Group dynamically adjusts instances based on demand, optimizing resource utilization. NAT Gateway provides secure outbound internet connectivity for private subnets, adding an extra layer of security. Internet Gateway establishes a secure pathway for internet communication. The Route Table guides efficient and secure network traffic within the VPC. Security Group enhances overall security by controlling inbound and outbound traffic, providing an extra layer of defense. This set of tools collectively addresses networking, security, scalability, and resource management crucial for a successful cloud migration. The carefully selection of AWS-native services, including Amazon S3, Amazon SNS, Amazon QuickSight, Amazon WorkDocs, AWS Lambda, and AWS CloudTrail, reflects a strategic approach aimed at addressing the institution's unique challenges and ensuring a seamless transition to the cloud. Amazon S3 provides a robust foundation for scalable and efficient data storage, overcoming the limitations of on-premises servers. Amazon SNS facilitates transparent communication, minimizing disruptions during migration and fostering collaboration among stakeholders. Amazon QuickSight empowers the institution with insightful data-driven decision-making, contributing to a culture of continuous improvement. Amazon WorkDocs addresses collaboration challenges, ensuring secure document sharing and version control among faculty and staff. AWS Lambda, with its serverless architecture, brings automation to the forefront, enhancing operational efficiency and reducing the risk of manual errors during complex migrations. Finally, AWS CloudTrail serves as a linchpin for security and compliance, providing detailed visibility into user activity and resource changes. The collective impact of these chosen tools and the database selection ensures that The London College's migration journey is not only technically robust but also aligns with best practices in data management, collaboration, automation, and security. This strategic blend of AWS services, tools, and the selected database lays the groundwork for an agile and future-ready IT environment, enabling the institution to navigate the challenges of the cloud with confidence. As The London College embraces this transformative journey, the selected tools not only meet the immediate needs of the migration but position the institution for sustained success in the dynamic landscape of cloud computing.

# Conclusion

As The London College embarks on the journey to migrate its IT services to the cloud, the envisioned future is one of heightened efficiency, flexibility, and accessibility. The proposed three-tier architectural framework aligns seamlessly with the educational landscape, fostering a digital ecosystem that adapts to evolving demands. The hybrid deployment model strikes a balance between control and scalability, ensuring sensitive data remains secure while harnessing the expansive power of the public cloud. This migration is not merely a technological shift, it’s a strategic leap towards a future where The London College's IT infrastructure becomes an enabler of innovation, collaboration, and educational excellence.

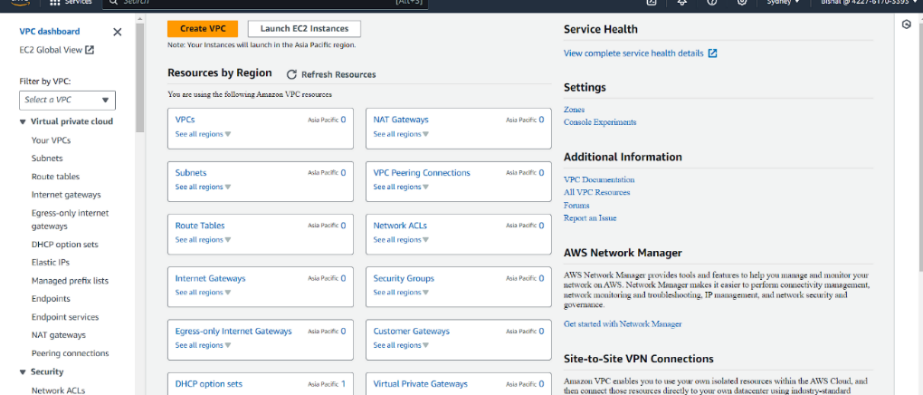
# Introduction

This technical report outlines the process of developing cloud computing solutions for The London College. The tasks involve configuring a cloud computing platform using the AWS framework, implementing a cloud computing platform with open-source tools, identifying potential issues and constraints, and proposing critical solutions to overcome these challenges.

# Configure a Cloud Computing Platform with AWS Framework

To configure a robust cloud computing platform for The London College using AWS services, we begin by constructing a three-tier AWS VPC, carefully partitioning subnets for the presentation, application, and data tiers. Following this, we establish NAT Gateways to enable secure outbound internet access. We then meticulously configure Security Groups tailored to each tier's specific requirements, ensuring optimal network security. Additionally, we deploy Auto Scaling Groups to dynamically manage EC2 instances, optimizing resource allocation and scalability. To efficiently distribute incoming traffic, we implement an Application Load Balancer. Finally, we commit to continuous monitoring and optimization of our infrastructure to guarantee peak performance and cost-effectiveness and by adding IAM The London College can effectively manage access to AWS resources using IAM, ensuring security and compliance with organizational policies and regulations (Huang, 2021).This is Configure for cloud Computing platform of Academic Portal likewise we creating same for Administrative Portal, and Student Portal. We have to create private subnet, public subnet, network interface, Interface gateways, Network ACLs, security group and auto scaling group for them like below:

**Step 1: Go to VPC and Click on Create VPC**



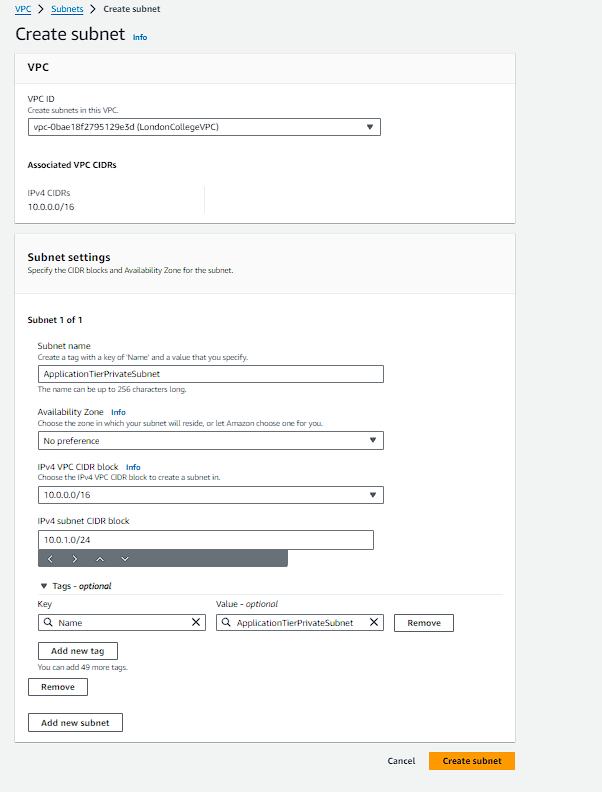
**Step 2: Creating a VPC**

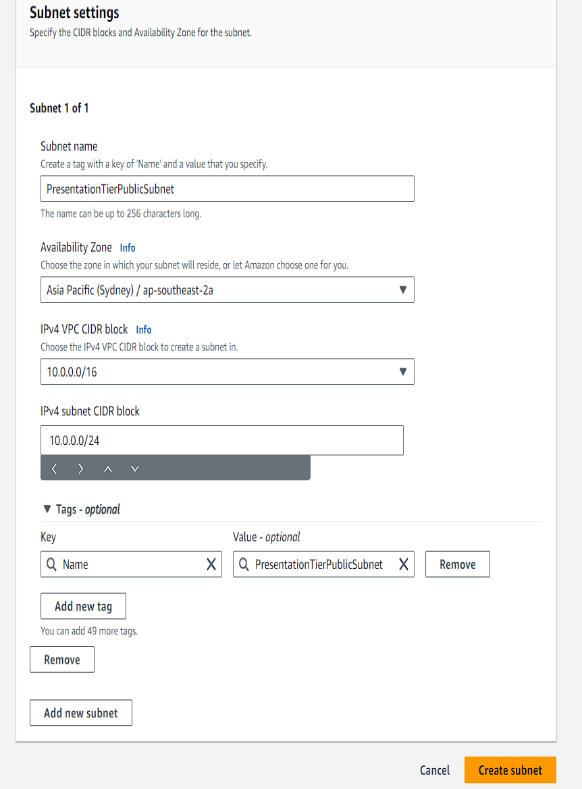




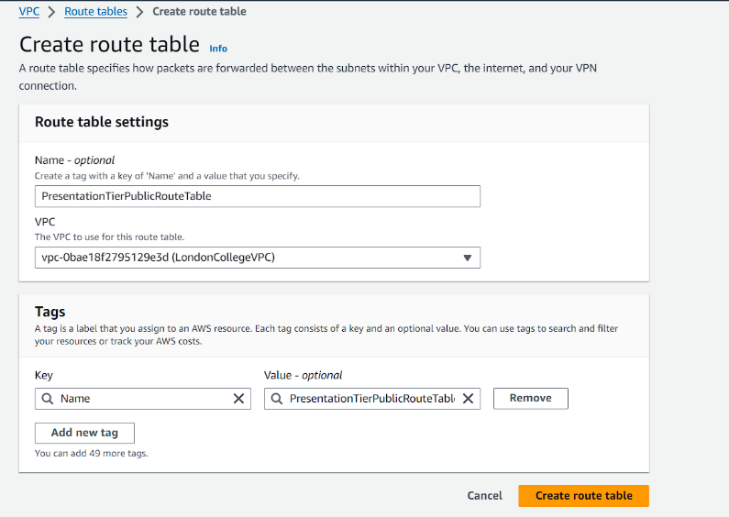
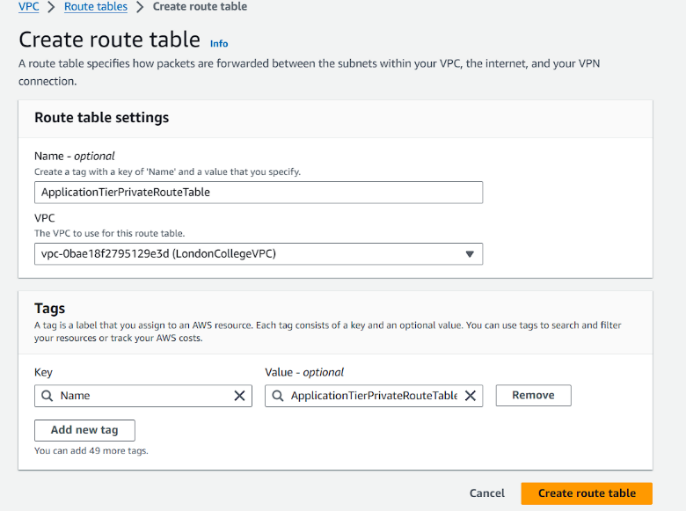
**Step 3: After Creating VPC add and we add three subnet more for Academic likewise also creating three subnets each for Administration portal, Student Portal**

(PresentationTierPublicSubnet,ApplicationTierPrivateSubnet, DataTierPrivateSubnet)



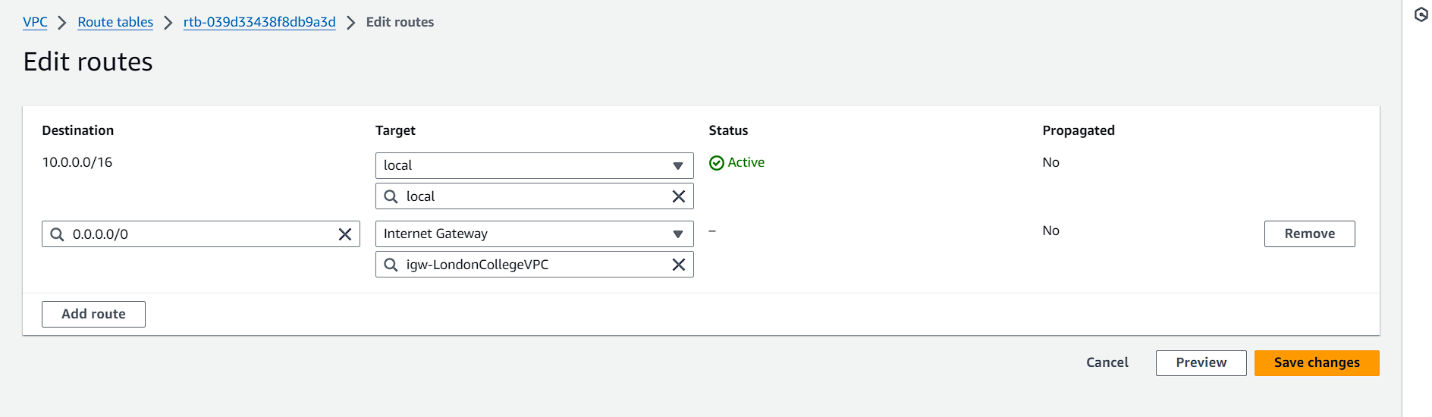


**Step 4: After Creating subnet and Creating Three Route Table for Academic Portal likewise also Creating Three Route each for Administration Portal, Student Portal.**



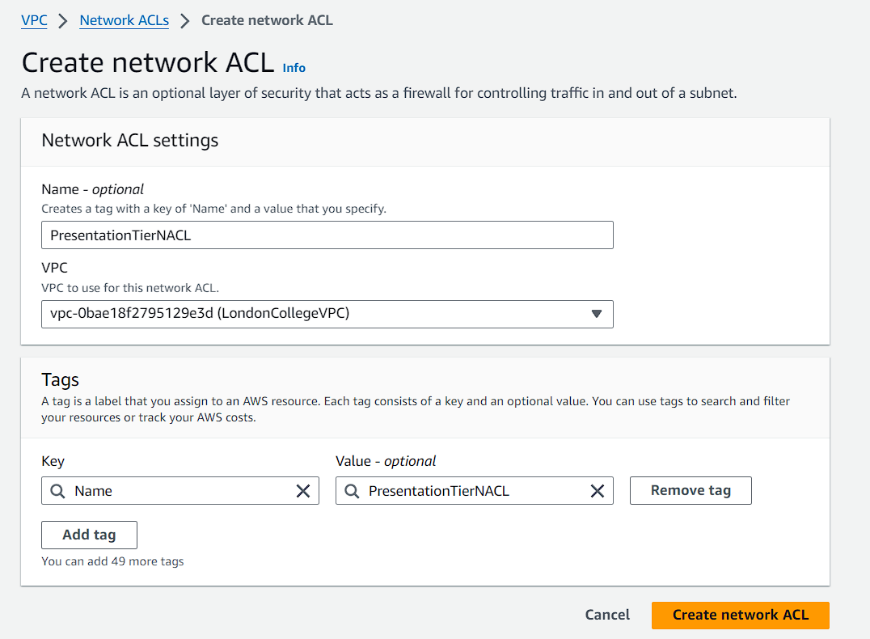


**Step 5: After Creating Route table and now adding Internet Gateway for Academic Portal and also creating Internet Gateway for Administration portal, Student Portal**



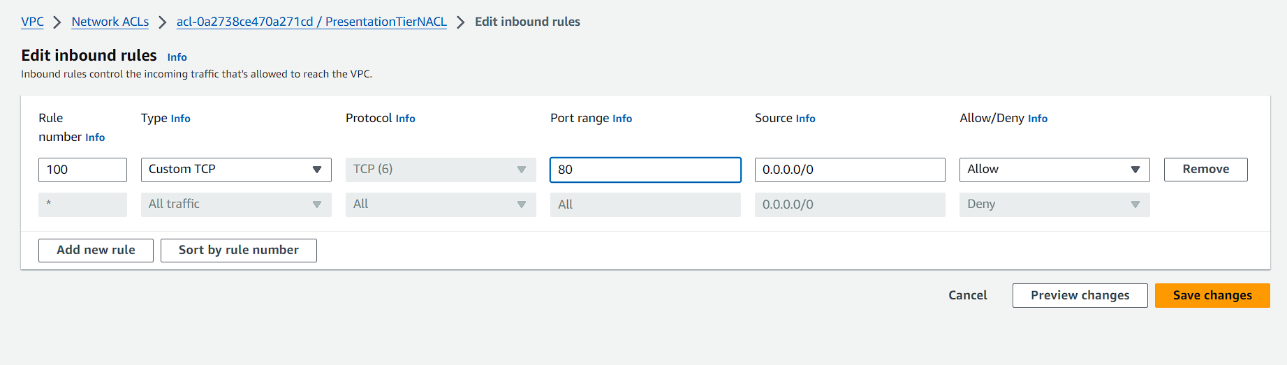
**Step 6: Create Network ACL for Academic Portal for Private and Public Subnet like we creating Network ACL for Private, Public subnet of Administration portal, Academic Portal**

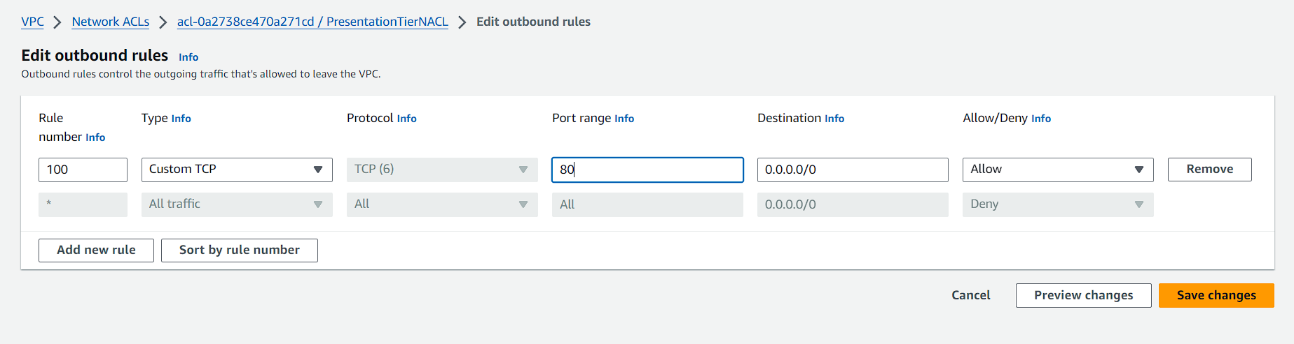
**(PresentationTierNacl, ApplicationTierPrivateSubnetNacl, DataTierPrivateSubnetNacl)**



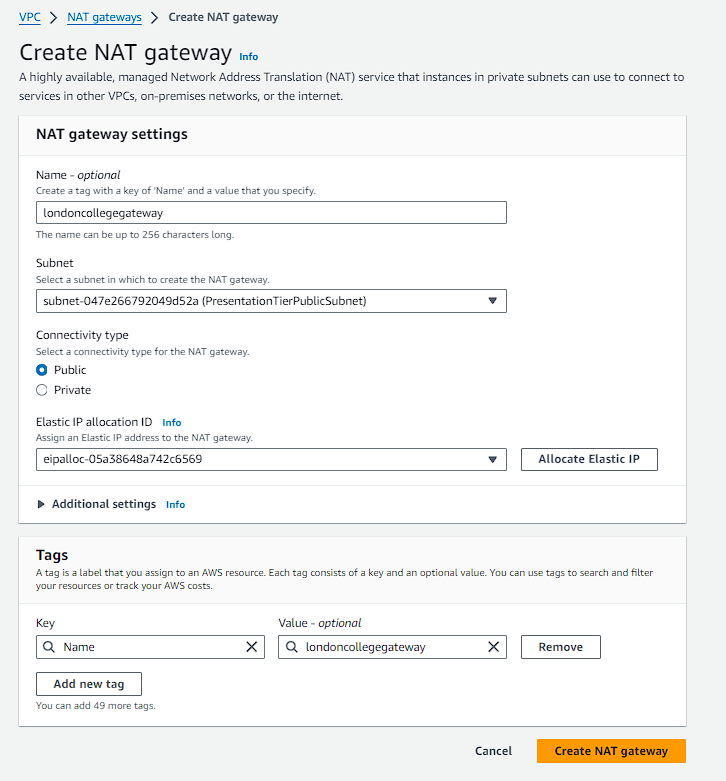


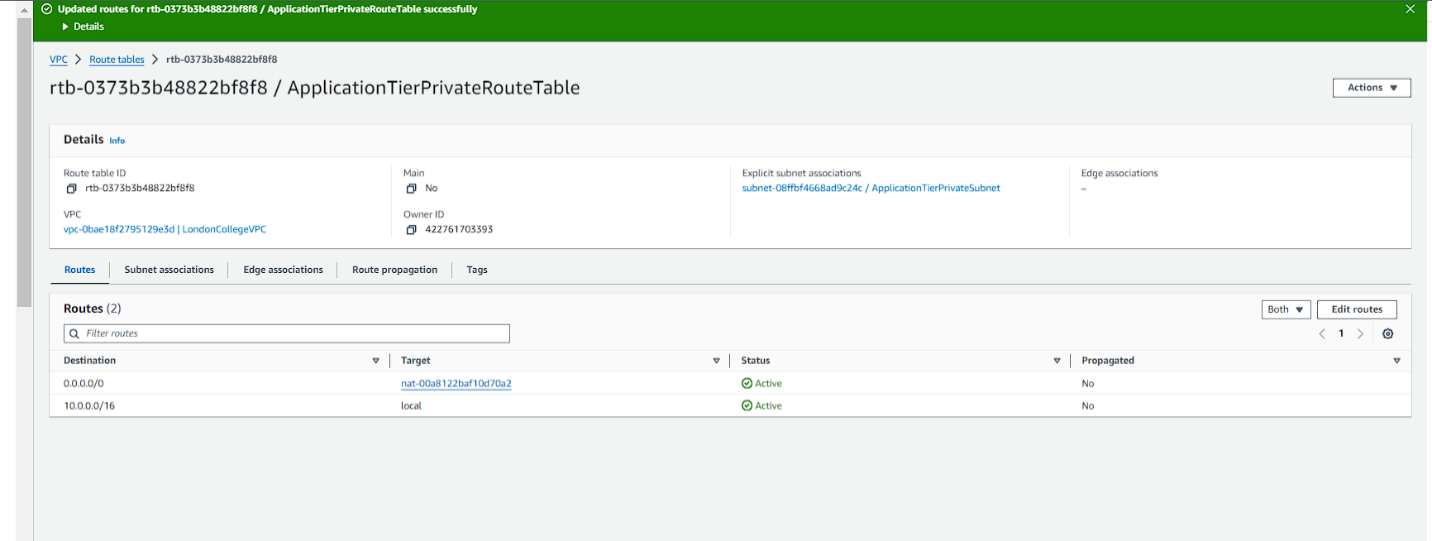
**Step 7: After creating Network ACL Now giving inbound rule and outbound rule for PresentationTierNACL of each Administration portal, Academic Portal.**



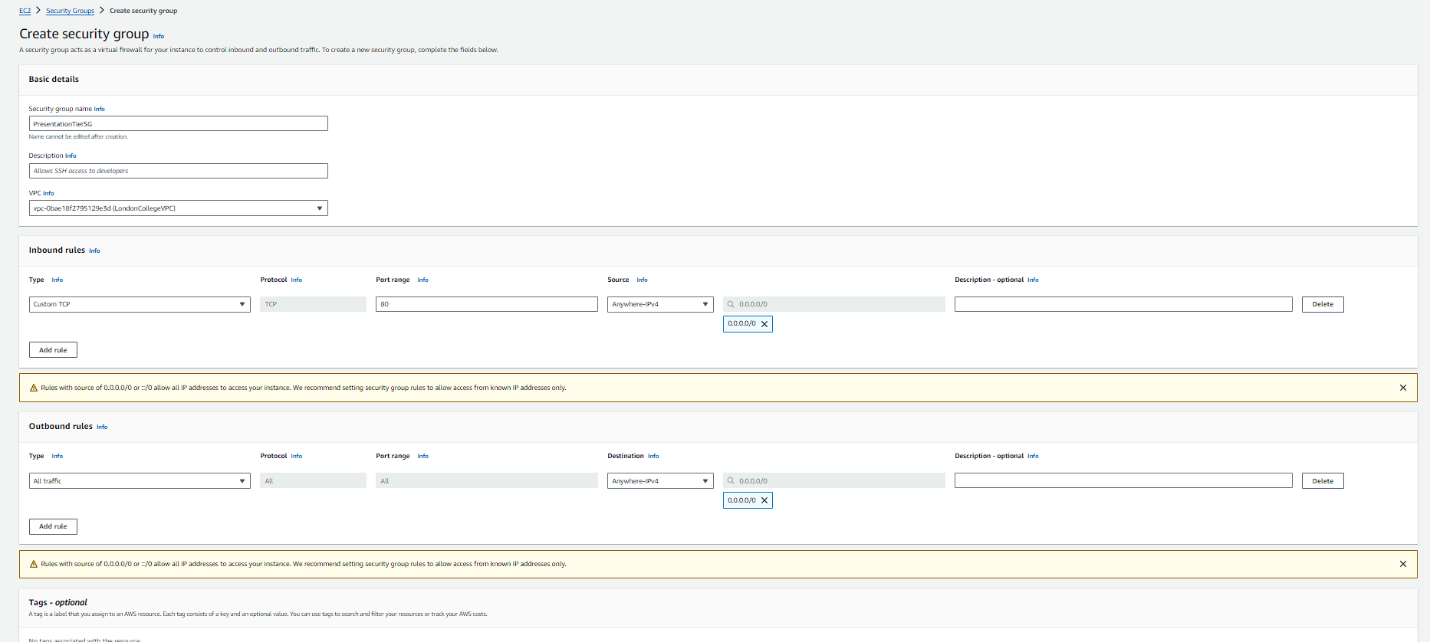


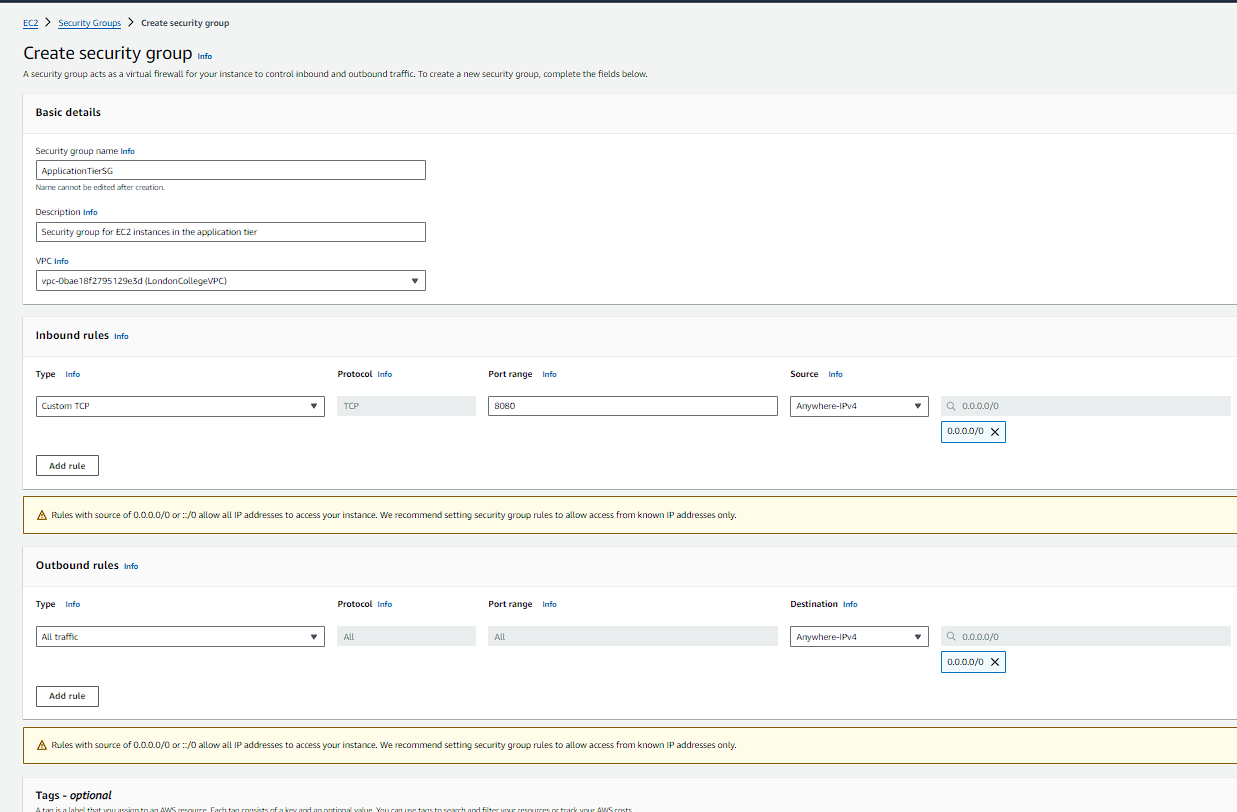
**Step 8: Creating NAT Gateway for Public Subnet of Academic Portal like wise we creating NAT Gateway for public Subnet of Administration Portal and Student Portal.**

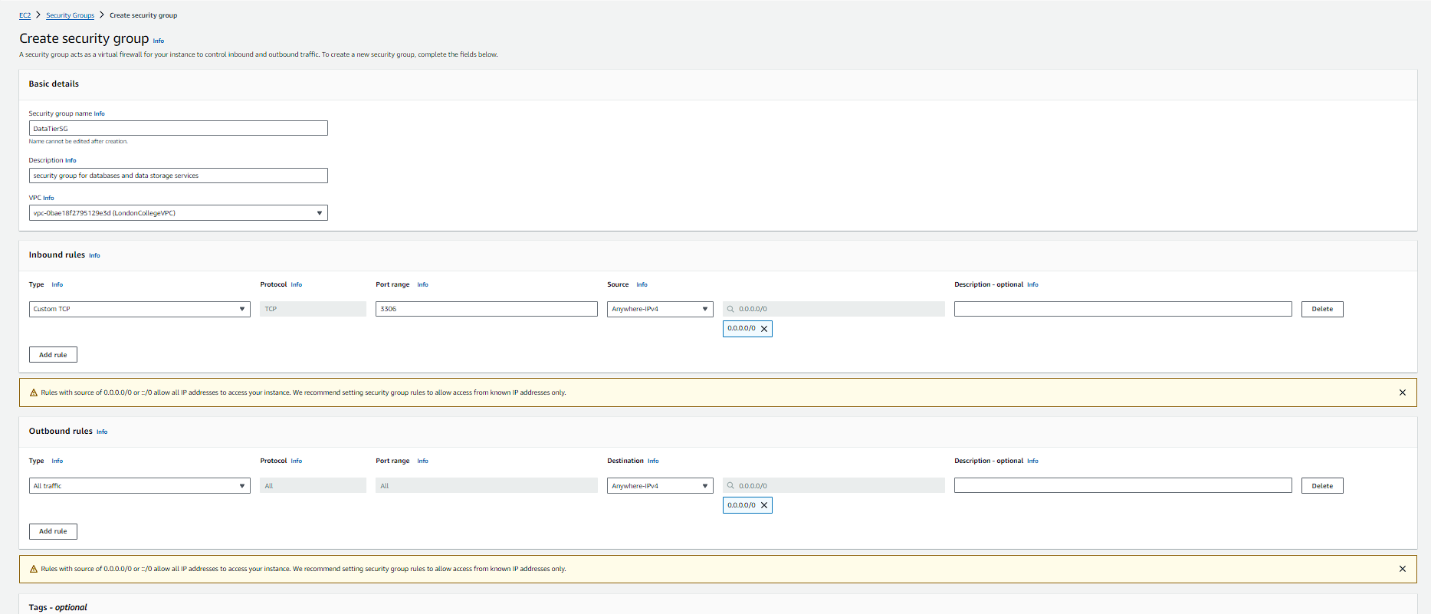


**Step 9: Connecting NAT gateway to Private Subnet for Academic Portal likewise connecting NAT gateway to Private Subnet for Administration Portal, Student Portal.**

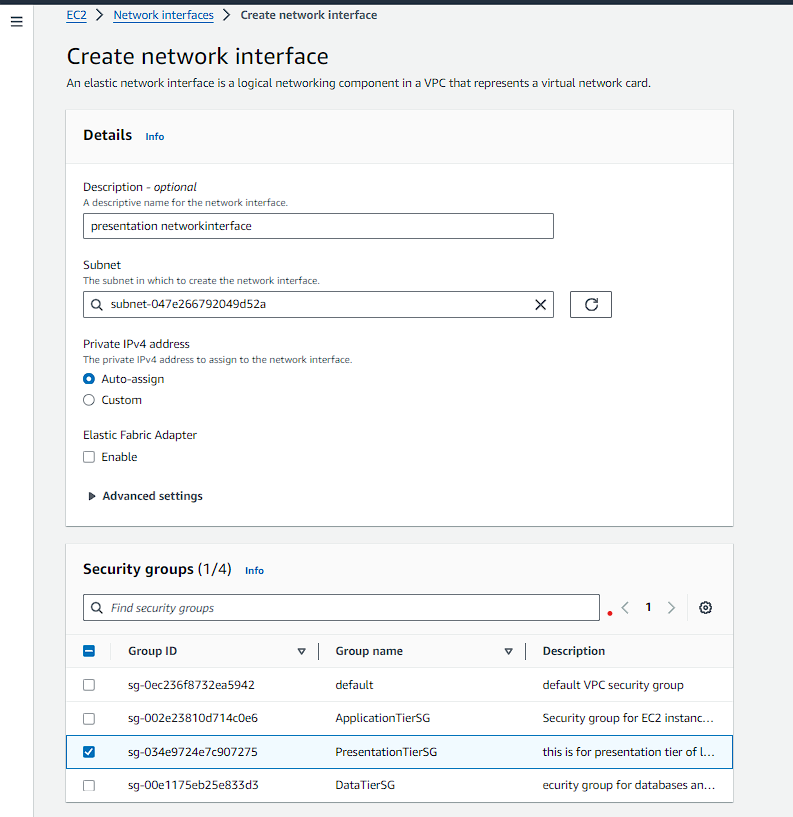
**Step 10: Creating Security group for presentation tier, Application tier, Data Tier for Academic Portal likewise creating for Administration Portal, Student Portal.**

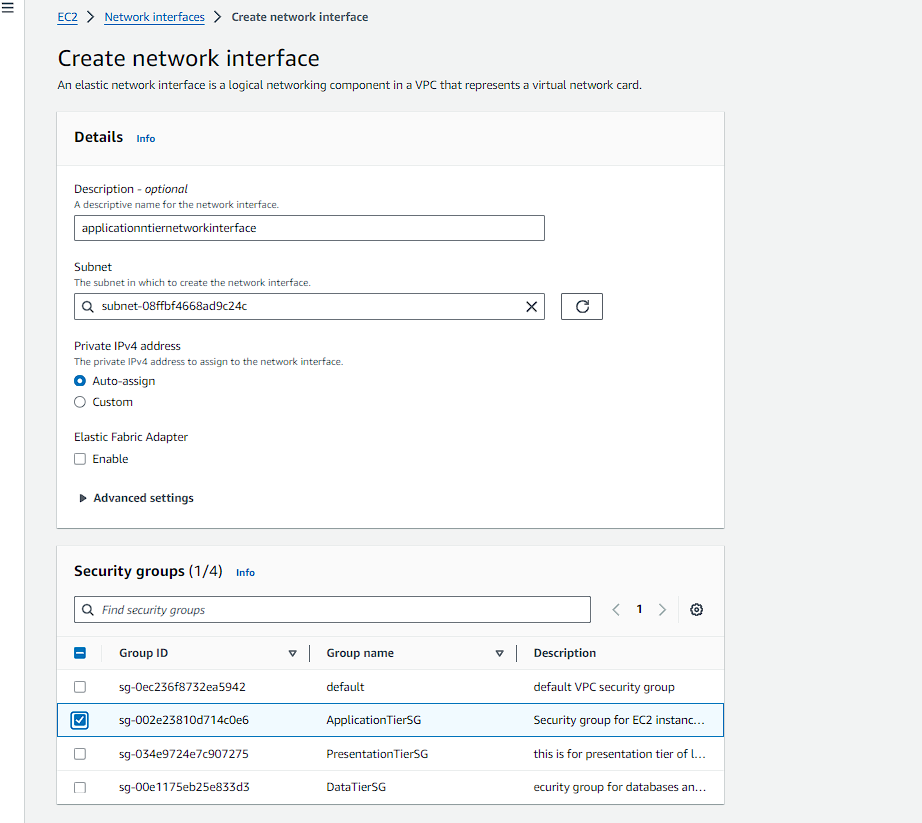






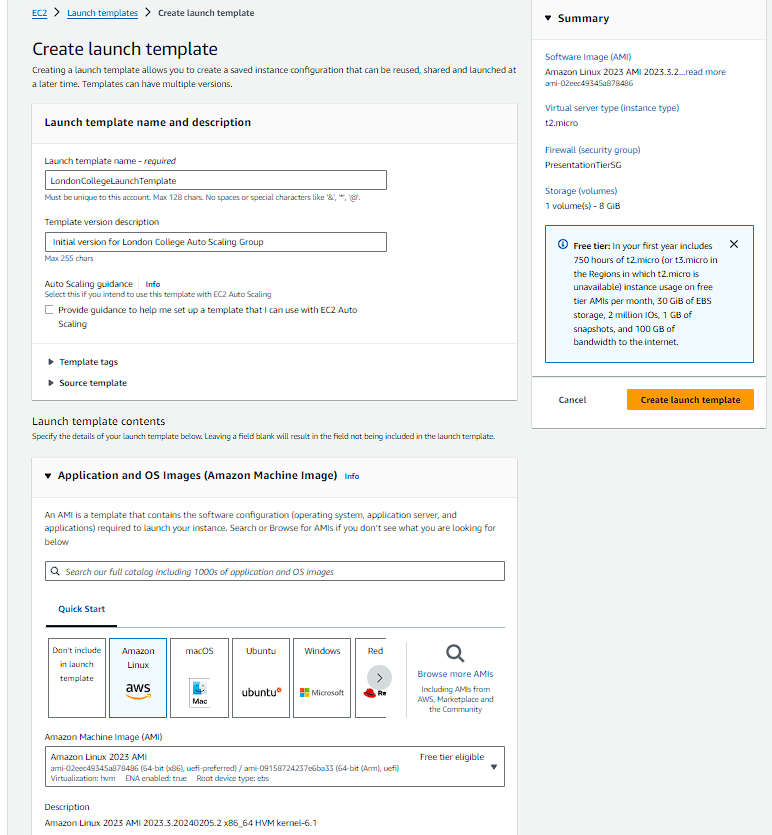
**Step 11: Creating Network Interface in EC2 for Academic Portal likewise we creating network interface in EC2 for Administration Portal and Student Portal.**

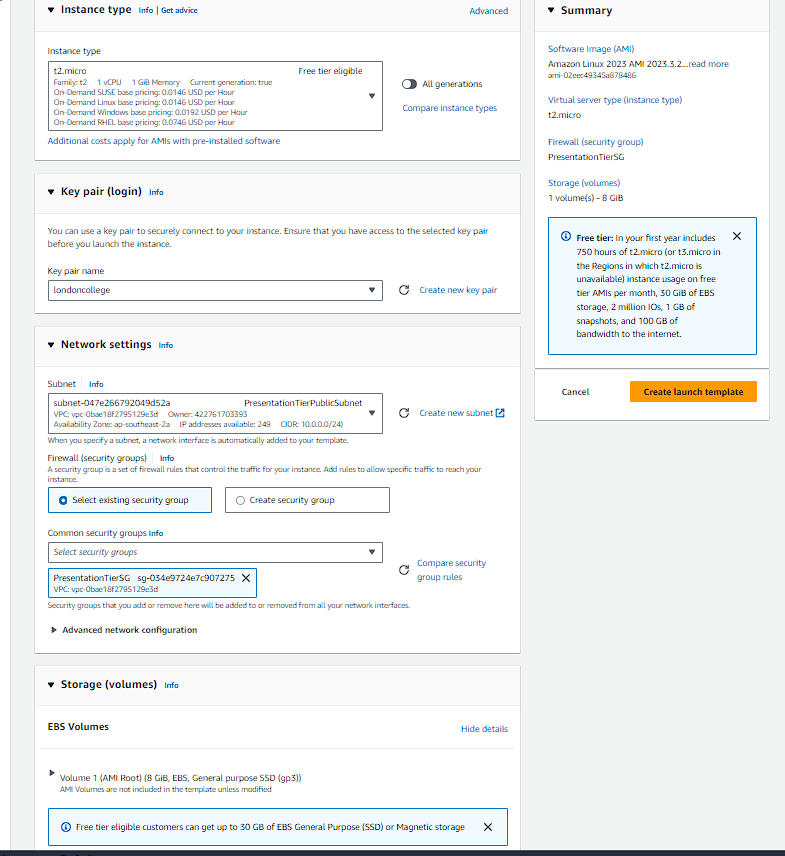




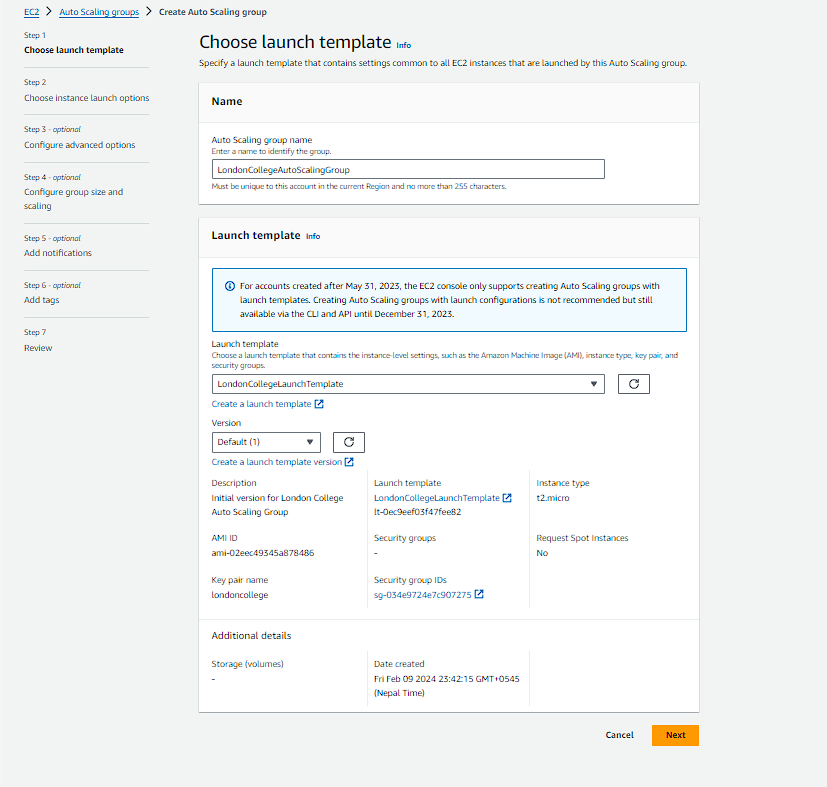


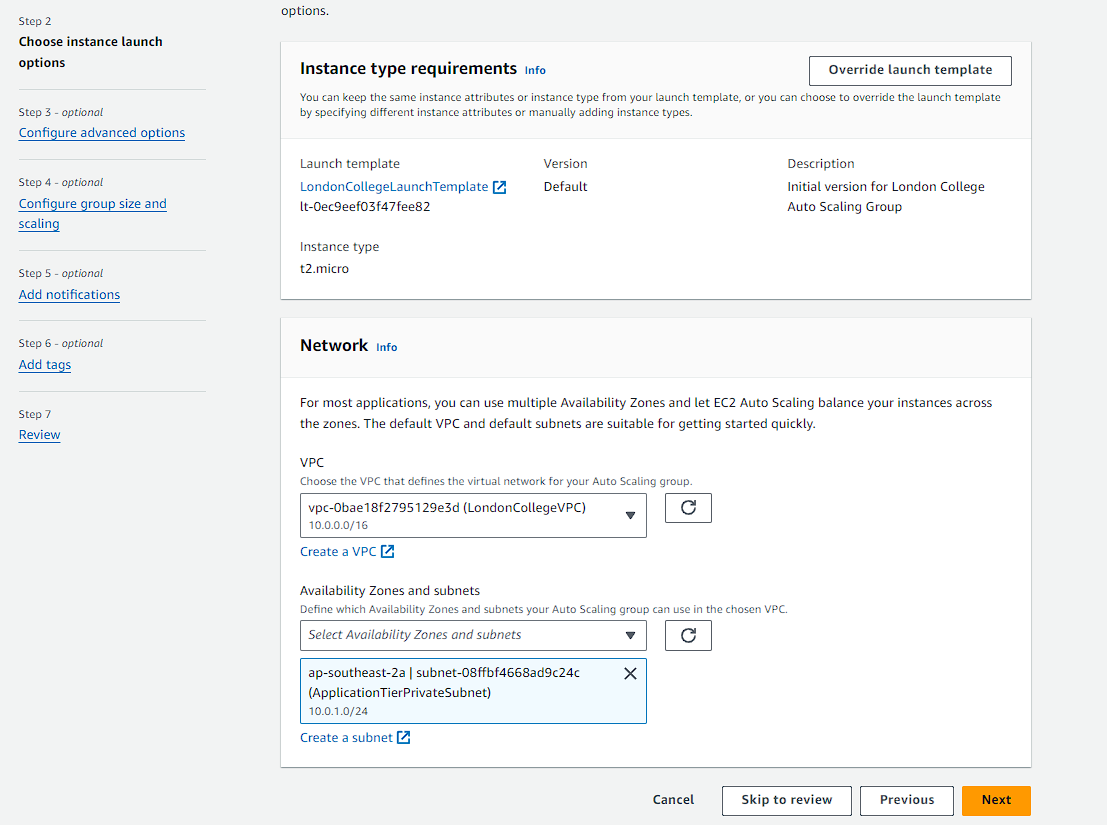
**Step 12: Creating EC2 Template for Academic Portal Likewise creating for Administration Portal and Student Portal**

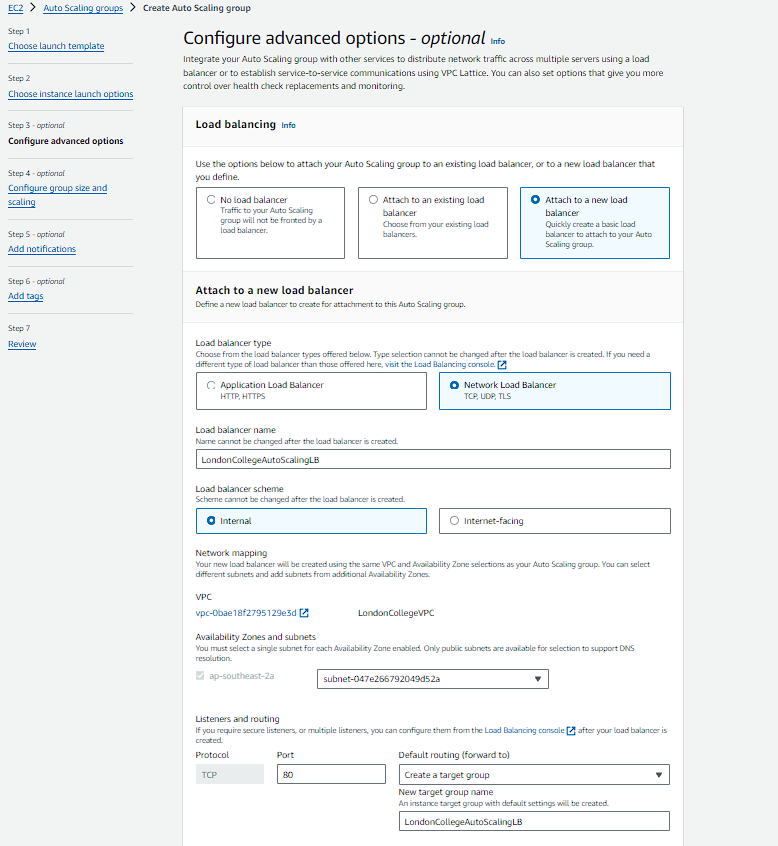


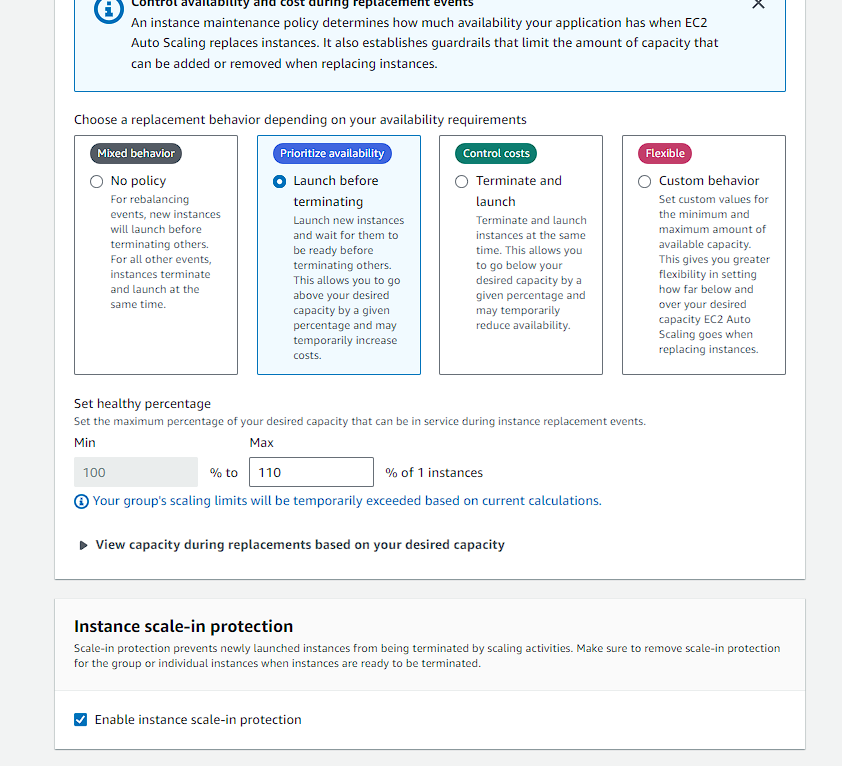


**Step 12: Creating Auto Scaling Group for Academic Portal Likewise creating for Administration Portal and Student Portal**

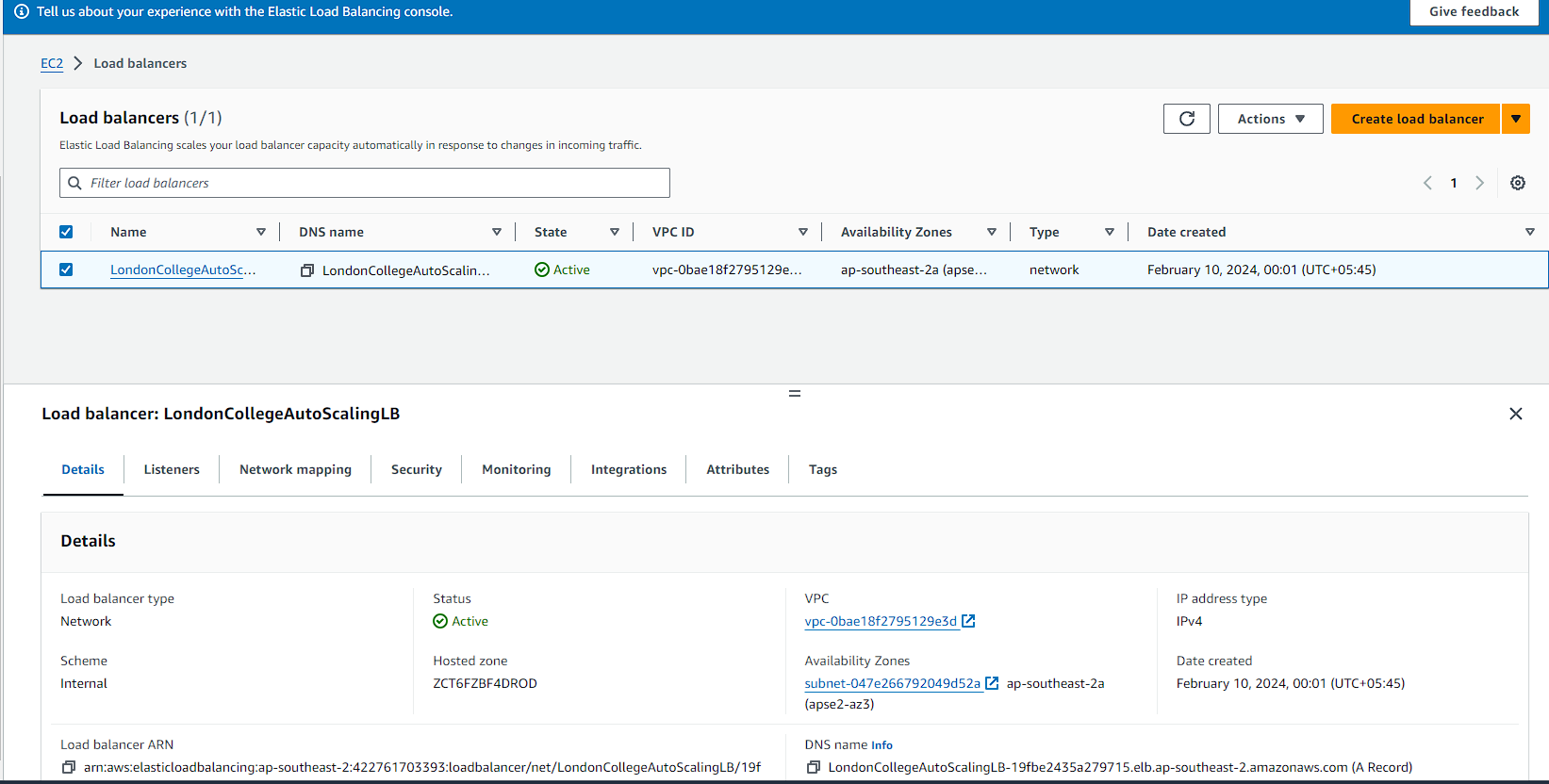




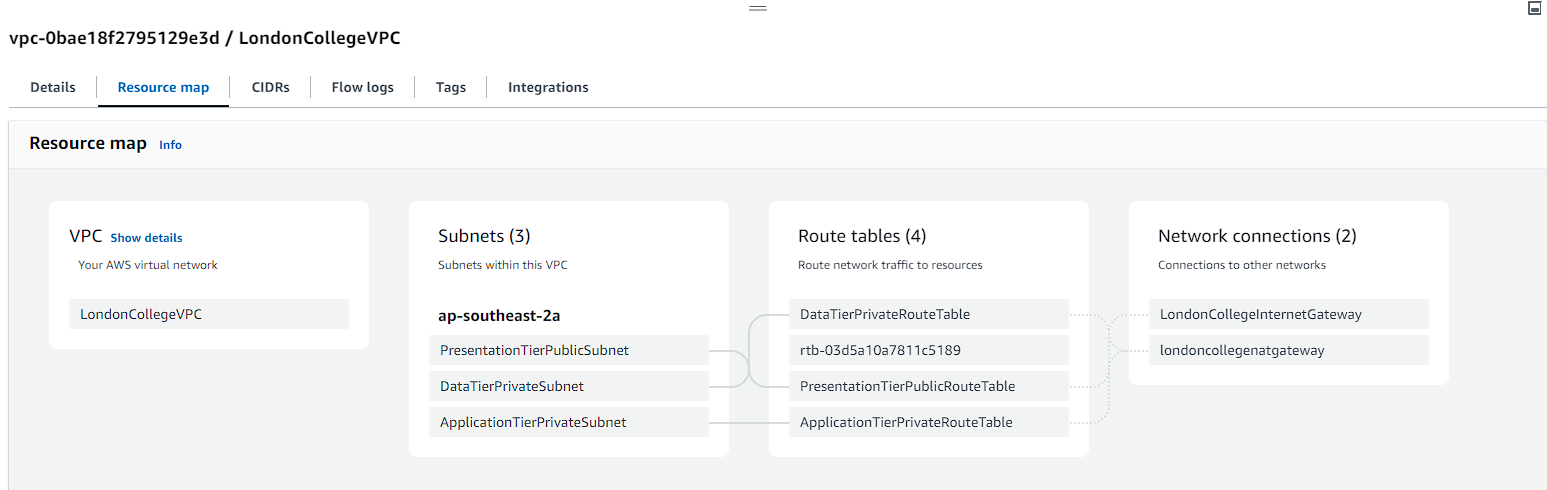




**Step 13: Creating Load Balancer for Academic Portal Likewise creating Load Balancer for Administration Portal and Student Portal**

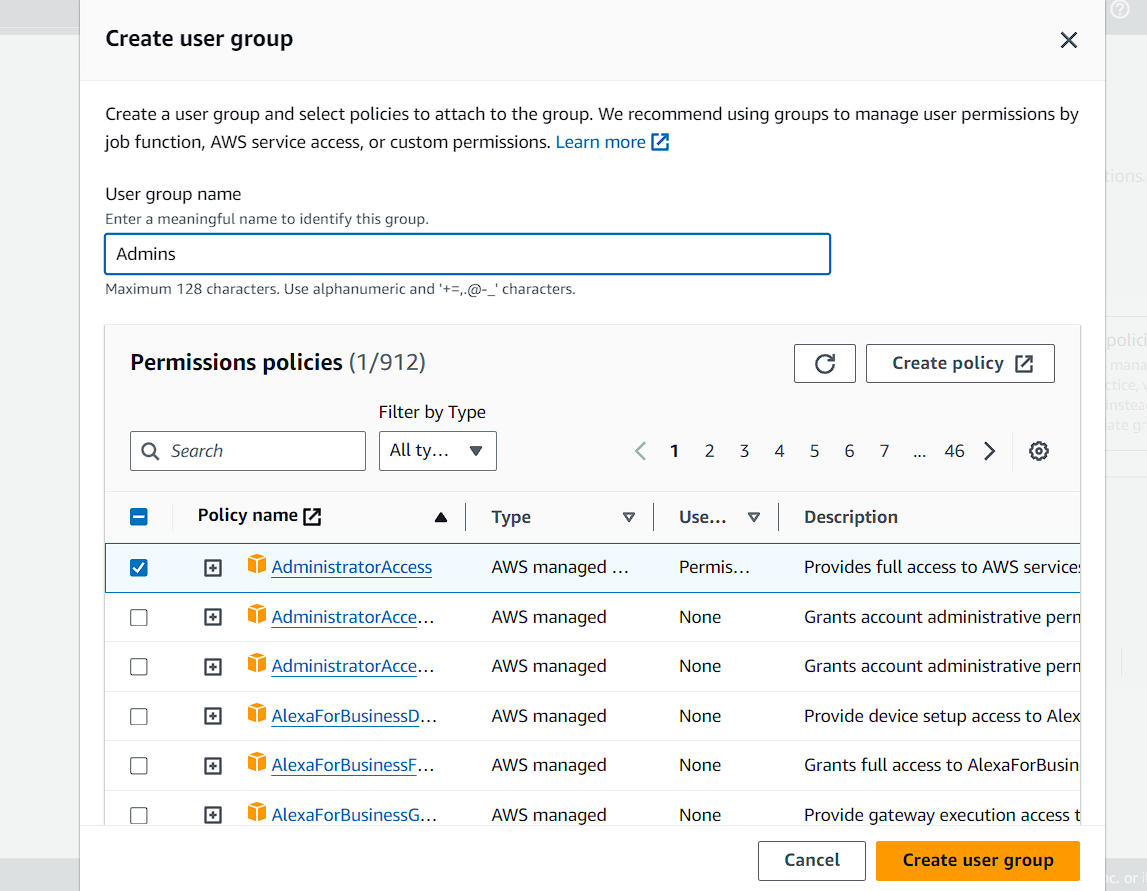


**VPC MAP**

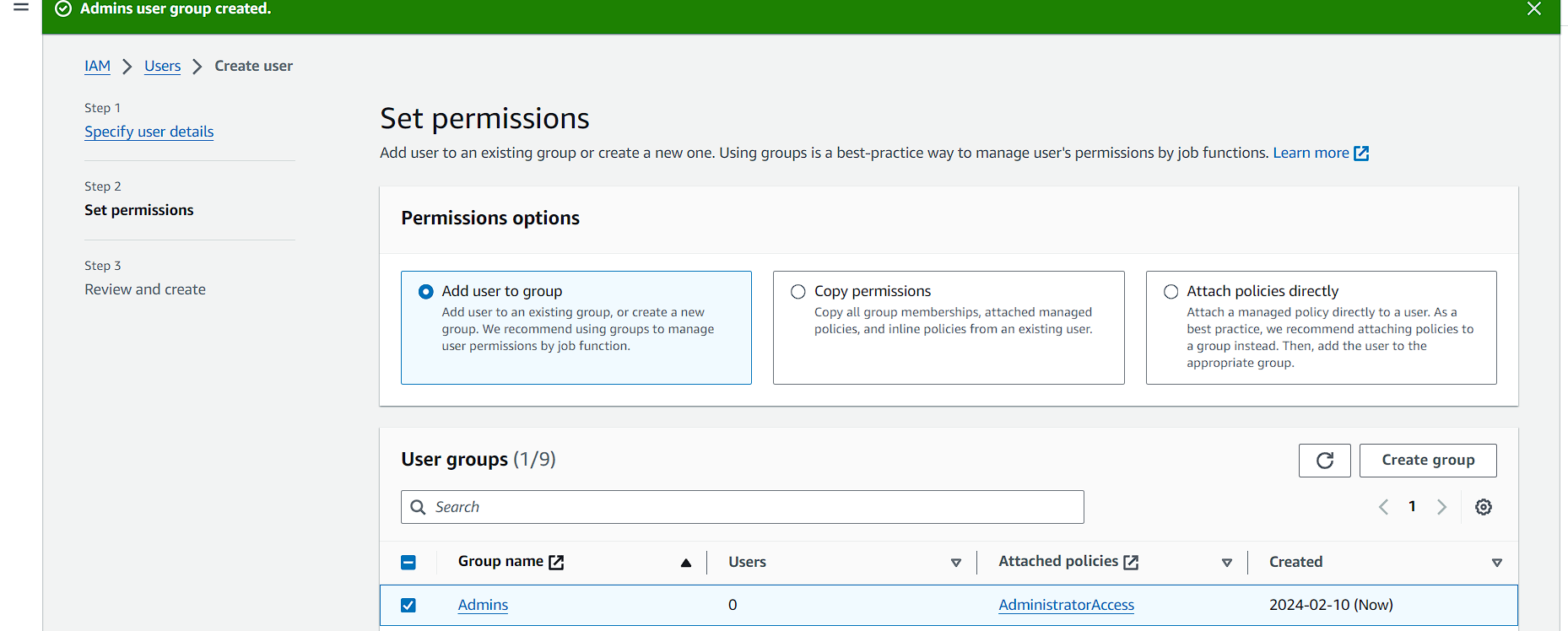


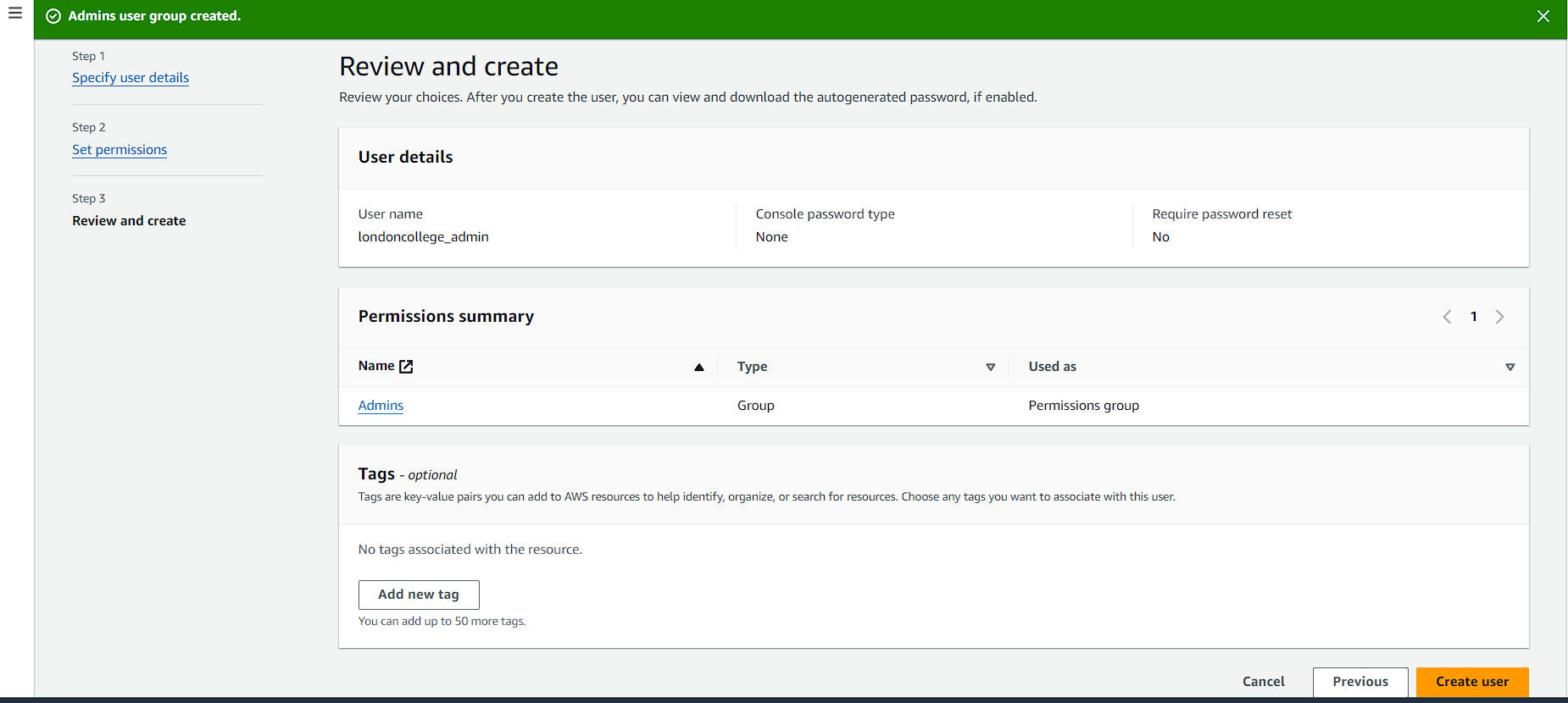
**Step 14: Creating IAM for London College**

**Creating User Group:**

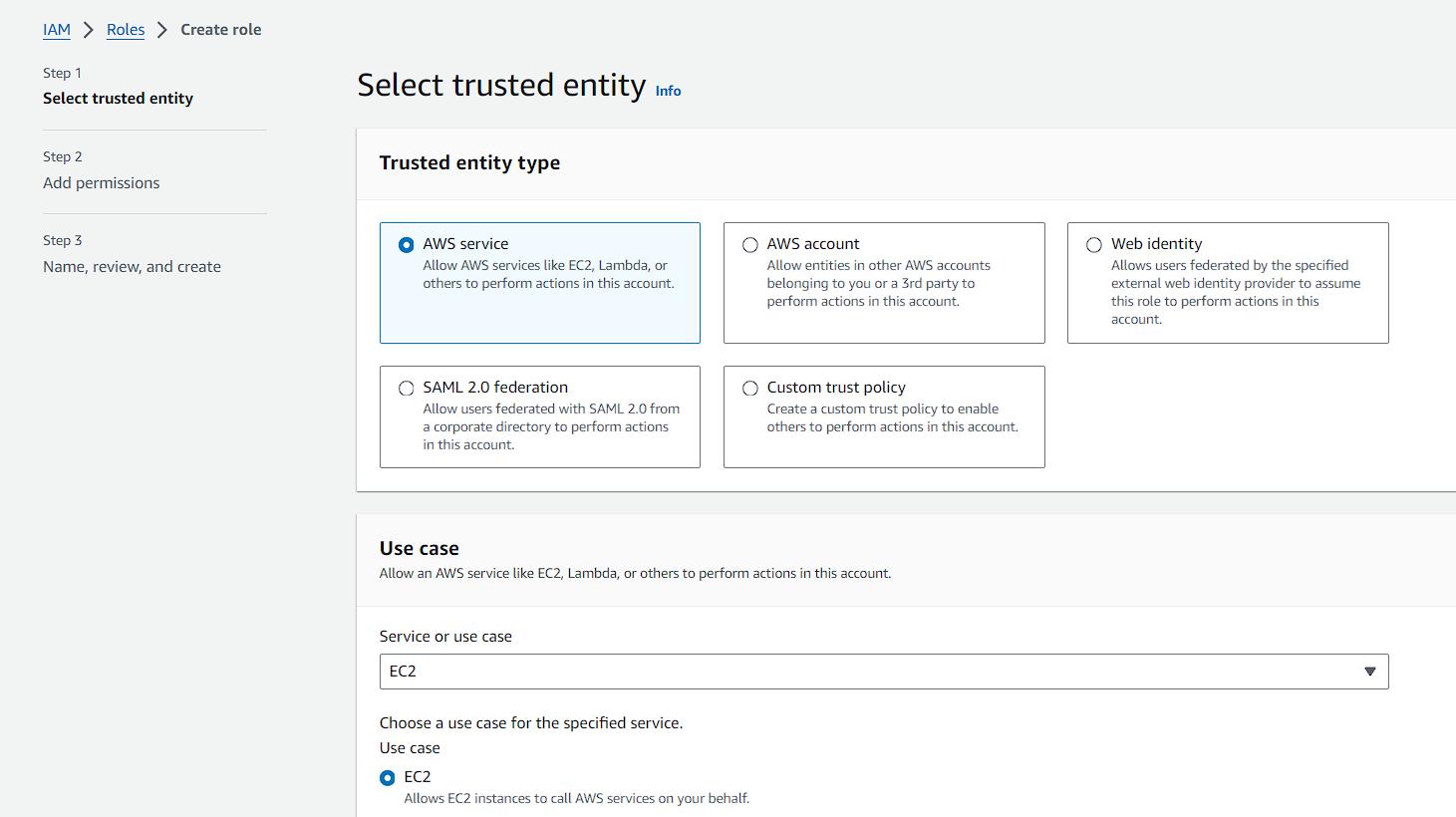
****

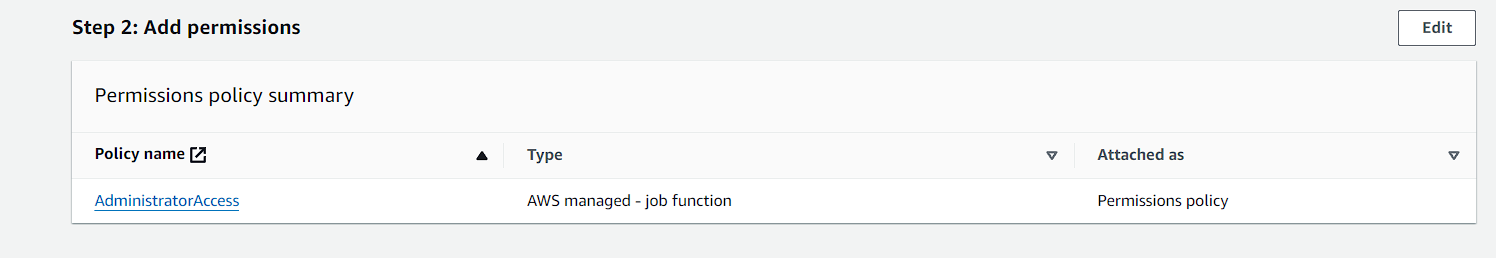
**Setting permission for User of Academic Portal like Setting permission for User of Administration Portal and Student Portal**

****

****

**Adding role IAM**

****

****

# Implement a Cloud Computing Platform using Open-Source Tools

To implement a cloud computing platform using open-source tools for The London College, we leverage various open-source technologies to complement and enhance the services provided on AWS. Here's how we proceed:

## OpenStack for Private Cloud Management

OpenStack is an open-source software platform for building and managing both public and private clouds. We deploy OpenStack to create a private cloud infrastructure within the AWS environment, providing additional flexibility and control over resource management. With OpenStack, we manage compute, storage, and networking resources, allowing for self-service provisioning of virtual machines, storage volumes, and networking configurations. This approach empowers The London College with autonomy in managing their cloud resources while benefiting from AWS's robust infrastructure (Zhu, 2016).

## Kubernetes for Container Orchestration

Kubernetes is an open-source container orchestration platform that automates the deployment, scaling, and management of containerized applications. By integrating Kubernetes with AWS, we deploy containerized applications efficiently, utilizing AWS EC2 instances as Kubernetes nodes. Kubernetes provides features like auto-scaling, load balancing, and self-healing, ensuring high availability and scalability for applications hosted on the cloud platform. Leveraging Kubernetes alongside AWS enables The London College to achieve seamless deployment, scalability, and reliability for their applications.

## Docker for Containerization

Docker is a platform that's source and used for creating, delivering and operating applications within containers. We containerize applications using Docker, creating lightweight, portable, and isolated environments that can run consistently across different cloud environments. Docker containers can be deployed on AWS EC2 instances or managed Kubernetes clusters, enabling seamless deployment and scaling of applications. By utilizing Docker alongside AWS services, The London College ensures compatibility and consistency in their application deployments, simplifying the management of cloud resources.

## Ansible for Configuration Management

Ansible is an open-source automation tool that simplifies the configuration management and deployment of infrastructure and applications. With Ansible, we automate the provisioning and configuration of cloud resources on AWS, ensuring consistency and repeatability in infrastructure deployments. Ansible playbooks are used to define the desired state of the infrastructure, making it easy to manage and scale cloud resources efficiently. Integrating Ansible with AWS empowers The London College to streamline their infrastructure management processes, reducing manual efforts and minimizing the risk of configuration errors (Rodriguez-Martinez, 2010).

## Prometheus and Grafana for Monitoring and Metrics

Prometheus is an open-source monitoring and alerting toolkit designed for cloud-native environments. Grafana is an open-source analytics and visualization platform that integrates with Prometheus to create dashboards and visualizations for monitoring metrics. By deploying Prometheus and Grafana on the cloud platform, we monitor the health, performance, and utilization of resources, enabling proactive monitoring and troubleshooting of issues. This comprehensive monitoring solution ensures optimal performance and reliability for The London College's cloud infrastructure.

By integrating these open-source tools with the existing AWS framework, we enhance the capabilities of the cloud computing platform for The London College. This approach allows for greater flexibility, scalability, and customization while leveraging the benefits of both proprietary and open-source technologies. Additionally, it promotes vendor-agnosticism and avoids vendor lock-in, ensuring long-term sustainability and cost-effectiveness for the college's cloud infrastructure.

# Potential issues and constraints that may arise during the development process of the cloud computing solutions

The process of developing cloud computing solutions is intricate, presenting both opportunities and challenges. A notable difficulty that may arise is data migration. As The London College shifts from on-premises servers to a cloud environment, transferring substantial data volumes can lead to delays and potential downtime. Successfully navigating the complexities of data migration without disrupting ongoing operations requires careful planning and execution.

Another challenge involves ensuring compatibility between existing applications on on-premises servers and the cloud environment. This disparity may result in functionality issues, necessitating adjustments to the applications or even a complete rethinking of their architecture. Adapting custom scripts or configurations to align with the cloud infrastructure introduces complexity and could lead to delays in the development process.

Security is a significant concern in cloud development, especially considering the sensitivity of academic and administrative data at The London College. Effectively addressing potential vulnerabilities, such as unauthorized access, data breaches, or inadequate encryption practices, requires meticulous planning to balance accessibility with security measures and maintain compliance with data protection regulations.

Cost management is another consideration. While the cloud offers scalability, there is a risk of overspending due to suboptimal resource allocation or underutilized instances. Implementing effective cost monitoring and optimization strategies, such as considering reserved instances, spot instances, or utilizing auto-scaling to align resources with actual demand, is essential to prevent budget overruns throughout the development process.

Furthermore, reliance on third-party cloud service providers introduces a constraint related to service-level agreements (SLAs). The cloud solution must navigate potential downtime or service disruptions, highlighting the need for robust disaster recovery and business continuity planning. Negotiating comprehensive SLAs, including uptime guarantees, support responsiveness, and data recovery protocols, is vital to ensure the continuity of services for The London College.

In conclusion, the development process of cloud computing solutions for The London College presents various challenges, including data migration complexities, application compatibility issues, security concerns, cost management considerations, and dependencies on external service providers. Successfully addressing these challenges requires a thorough understanding of the institution's specific needs, coupled with meticulous planning and execution to ensure a successful and adaptable transition to the cloud.

# The issues and contractions faced during the development process can be overcome

Overcoming the challenges and constraints encountered during the development process of cloud computing solutions demands a nuanced and strategic approach. Addressing data migration complexities involves meticulous planning and execution. Leveraging tools for efficient data transfer, adopting incremental migration strategies, and conducting thorough testing in a controlled environment can mitigate potential downtime and latency issues. Additionally, maintaining constant communication with stakeholders ensures transparency and minimizes disruptions (Kadhim, 2018).

Application compatibility issues necessitate an adaptable mindset. Employing containerization or microservices architecture enables the seamless integration of existing applications with the cloud environment. This approach facilitates the isolation of components, allowing for easier adjustments and reducing the need for complete re-architecting. Collaborative efforts between development and operations teams, adopting agile methodologies, and utilizing continuous integration/continuous deployment (CI/CD) pipelines contribute to a more flexible and responsive development process.

Security concerns require a holistic and proactive approach. Implementing robust identity and access management (IAM) policies, encryption protocols, and regular security audits are paramount. The establishment of a robust security culture within the development team, continuous training on the latest security threats, and adherence to industry best practices contribute to safeguarding sensitive data effectively. Collaboration with cloud service providers and staying abreast of their security features and updates further enhances the overall security posture.

Effective cost management involves a combination of strategic planning and ongoing optimization. Implementing a robust cloud cost management strategy includes leveraging cost monitoring tools, optimizing resource allocation through reserved instances and spot instances, and implementing auto-scaling based on actual demand. Regular financial reviews, accountability measures, and fostering a cost-conscious culture within the development team contribute to preventing budget overruns (Ahmad, 2013).

Dependencies on third-party cloud service providers necessitate comprehensive service-level agreement (SLA) negotiations and diligent ongoing management. Establishing clear expectations regarding uptime guarantees, support responsiveness, and data recovery protocols is crucial. Developing contingency plans for potential service disruptions, including disaster recovery and business continuity measures, ensures a resilient cloud solution. Regularly reviewing and updating SLAs based on evolving needs and changes in the cloud landscape further strengthens the partnership with service providers.

In conclusion, overcoming the challenges and constraints in cloud computing development requires a multifaceted and adaptive approach. It involves technological solutions, collaborative teamwork, proactive security measures, and strategic financial management. Critically assessing each issue and applying tailored strategies ensures a resilient, secure, and cost-effective development process, ultimately leading to the successful implementation of cloud computing solutions.

# Conclusion

The development of cloud computing solutions for The London College involves configuring a robust AWS framework and implementing an open-source tool-based platform. By addressing potential issues and constraints through security measures, cost optimization, and compatibility testing, a successful and resilient cloud infrastructure can be established.

# Introduction

In the dynamic landscape of information technology, cloud computing has emerged as a transformative force, offering unprecedented scalability and flexibility. However, this transition to the cloud is not without its challenges. This article delves into common problems faced in cloud computing platforms, explores contemporary security issues, and provides insights into safeguarding data during migration.

# Most common problems that arise in a cloud computing platform and discuss appropriate solutions

The common problems that arise in a cloud computing platform has several key challenges and requires thoughtful solutions for effective mitigation. One prevalent issue is downtime, which can result from service outages or disruptions. To address this, cloud providers should implement redundancy measures, distribute data across multiple availability zones, and develop robust disaster recovery plans. Employing load balancing mechanisms and implementing failover strategies further enhances resilience against unexpected service interruptions.

**Security Enhancement Measures**

Another common problem revolves around security concerns, encompassing data breaches, unauthorized access, and inadequate encryption practices. A comprehensive security strategy involves implementing robust identity and access management (IAM) protocols, employing encryption technologies, and conducting regular security audits. Educating users on security best practices and ensuring compliance with industry standards contribute to a more secure cloud computing environment (Turab, 2013).

**Performance Optimization Techniques**

Performance bottlenecks, such as slow data transfer or application latency, can impede the efficiency of cloud platforms. Solutions include optimizing data transfer protocols, leveraging content delivery networks (CDNs) for faster content delivery, and implementing caching mechanisms. Additionally, monitoring and analyzing performance metrics provide insights for further optimization and resource scaling.

**Data Integrity and Availability Safeguards**

Data loss and corruption pose significant challenges in cloud computing. Implementing regular data backups, versioning, and snapshot mechanisms help safeguard against data loss. Cloud providers should offer robust backup and recovery services, and users must actively manage their data lifecycle to ensure data integrity and availability.

**Cost Management Strategies**

Cost management is a pervasive concern, with challenges such as unexpected spikes in expenses or suboptimal resource allocation. Employing cost monitoring tools, implementing budgeting controls, and utilizing cloud pricing models effectively contribute to managing costs. Periodic financial reviews and optimizing resource usage based on actual demand help prevent budget overruns (Alashoor, 2014).

**Vendor Lock-In**

Vendor lock-in, where users become overly dependent on a specific cloud service provider, is another challenge. To mitigate this, adopting multi-cloud or hybrid cloud strategies provides flexibility and reduces dependency. Ensuring compatibility with industry standards and using open-source technologies contribute to minimizing the risks associated with vendor lock-in.

In conclusion, the analysis of common problems in a cloud computing platform underscores the need for a comprehensive and strategic approach to problem-solving. Solutions range from technological measures such as redundancy and encryption to operational practices like regular monitoring and financial reviews. A holistic and proactive stance is essential to ensure the reliability, security, and cost-effectiveness of cloud computing platforms.

# Assessment of Common Contemporary Security Issues in the Cloud Environment

In the rapidly evolving landscape of cloud computing, security remains a paramount concern for organizations leveraging cloud services. Several common contemporary security issues persist, posing challenges to the integrity, confidentiality, and availability of data in the cloud. One prevalent issue is Data Breaches and Unauthorized Access. As organizations entrust sensitive information to cloud service providers, the risk of unauthorized access and data breaches intensifies. Misconfigurations, weak access controls, and inadequate identity management contribute to instances where malicious actors exploit vulnerabilities, gaining unauthorized access to critical data (Fernandes, 2013).

Another significant challenge is Inadequate Identity and Access Management (IAM). The complexity of cloud environments often results in suboptimal management of user identities and permissions. Inadequate IAM practices can lead to unauthorized privilege escalation, exposure of critical resources, and compromised confidentiality. Ensuring robust identity governance, implementing the principle of least privilege, and regularly auditing access controls are essential measures to mitigate this security concern.

Insufficient Data Encryption is a prevalent issue that emerges as data traverses between the user and cloud servers or within the cloud infrastructure itself. Inadequate encryption protocols may expose sensitive information during transit, leaving it susceptible to interception by malicious entities. Employing strong encryption algorithms and enforcing the use of secure communication channels are imperative to safeguard data integrity and maintain confidentiality in the cloud.

The emergence of Shared Responsibility Model Challenges introduces complexities in defining the boundaries of responsibility between cloud service providers and customers. Organizations may mistakenly assume that all security aspects are managed by the cloud service provider, neglecting their own obligations. This misunderstanding can lead to vulnerabilities in areas such as data protection, network security, and application security. Clarifying and understanding the shared responsibility model is crucial for a comprehensive and effective security strategy (Singh, 2018).

Compliance and Regulatory Issues pose a significant hurdle for organizations operating in the cloud. The dynamic nature of the cloud environment may result in non-compliance with industry regulations and legal requirements. Navigating the intricate landscape of regulatory frameworks and ensuring that cloud deployments adhere to specific standards demand meticulous attention. Failure to comply with these regulations can lead to severe consequences, including legal actions and reputational damage.

Lastly, the Challenges in Cloud Service Configuration contribute to security vulnerabilities. Misconfigurations of cloud services, storage buckets, and network settings may expose sensitive data inadvertently. Automated tools and scripts, while enhancing efficiency, can sometimes introduce errors in configurations. Regular audits, robust change management processes, and continuous monitoring are essential to identifying and rectifying misconfigurations promptly.

In conclusion, as organizations increasingly migrate to the cloud, addressing these common contemporary security issues is imperative to establish a resilient and secure cloud infrastructure. Continuous education, robust security practices, and a proactive approach to risk management are key elements in mitigating these challenges and ensuring the sustained security of data in the cloud environment (Singh, 2017).

# ****Addressing and Overcoming Common Contemporary Security Issues in Building a Secured Cloud Computing Platform****

Building a secured cloud computing platform necessitates a holistic approach to mitigate the challenges posed by common contemporary security issues. To address Data Breaches and Unauthorized Access, robust access controls and encryption mechanisms are indispensable. Employing Multi-Factor Authentication (MFA) ensures an additional layer of verification, reducing the risk of unauthorized access. Regularly auditing and monitoring user activities help in promptly detecting suspicious behavior, allowing for immediate response and remediation.

In the context of Inadequate Identity and Access Management (IAM), a well-defined and diligently implemented IAM strategy becomes pivotal. Adopting the principle of least privilege ensures that users have the minimum necessary access rights, reducing the potential for unauthorized privilege escalation. Regular reviews and updates of user permissions, coupled with continuous monitoring, help in identifying and rectifying any deviations from established access controls (Singh, 2016).

To combat Insufficient Data Encryption, organizations must prioritize the use of strong encryption algorithms for data at rest, in transit, and during processing. Implementing end-to-end encryption and employing secure key management practices add an additional layer of protection. Regularly updating encryption protocols to align with industry best practices is crucial for adapting to evolving security standards.

The Shared Responsibility Model Challenges can be addressed through clear communication and understanding of the responsibilities between the cloud service provider and the organization. Organizations must proactively educate their teams on their role in security, implement internal policies, and conduct regular training sessions. Leveraging cloud-native security tools provided by the service provider can further enhance visibility into the shared responsibility landscape.

Addressing Compliance and Regulatory Issues involves establishing a comprehensive compliance framework within the cloud platform. Organizations should conduct regular compliance assessments, ensuring that the cloud infrastructure aligns with industry regulations and legal requirements. Engaging with legal experts to stay abreast of evolving regulatory landscapes and promptly adapting the cloud environment to comply with new standards is crucial for mitigating compliance risks.

In combating Challenges in Cloud Service Configuration, organizations should implement rigorous change management processes. Automated configuration management tools can help in ensuring consistency and correctness across the cloud environment. Regular security audits, penetration testing, and continuous monitoring are essential to identifying and rectifying misconfigurations promptly. Implementing Infrastructure as Code (IaC) practices through tools like Terraform or Ansible can also enhance the reliability and security of cloud configurations.

Building a secure cloud computing platform involves addressing a myriad of challenges, and one critical aspect is mitigating the risks associated with Advanced Persistent Threats (APTs). Organizations should deploy advanced threat detection mechanisms, leveraging machine learning and artificial intelligence to identify anomalous patterns and behaviors. Implementing threat intelligence feeds and collaborating with industry security consortiums enhance the platform's ability to detect and respond to emerging threats proactively.

Furthermore, concerns related to data loss necessitate robust Data Loss Prevention (DLP) strategies. Implementing content discovery tools to identify sensitive data within the cloud environment, encryption, tokenization techniques, regular backups, and a well-defined incident response plan are integral components of an effective DLP strategy.

The reliance on third-party services and the interconnected nature of supply chains expose cloud platforms to additional risks related to supply chain and third-party risks. Conducting thorough security assessments of third-party vendors, ensuring adherence to security standards, and implementing a risk management framework with continuous monitoring help identify and mitigate potential vulnerabilities introduced by external entities.

Additionally, addressing the persistent threat of Zero-Day Exploits and Vulnerabilities requires prioritizing prompt patch management, continuous vulnerability scanning, automated patch deployment processes, and utilizing virtual patching solutions to reduce the window of exposure.

Mitigating Insider Threats involves fostering a security-aware organizational culture, implementing user behavior analytics, anomaly detection tools, regular employee training programs on security best practices, and enforcing strict access controls.

As cloud platforms adopt containerization technologies, Container Security becomes paramount. Organizations should implement measures such as image scanning for vulnerabilities, runtime protection, and network segmentation for containers. Integrating security into the DevOps pipeline ensures that security measures are applied throughout the application development lifecycle (Kumar, 2017).

In conclusion, building a secured cloud computing platform demands a proactive and multi-faceted approach. It involves a combination of technological measures, robust policies, continuous education, and regular assessments. By addressing each security issue with specific, tailored strategies, organizations can create a resilient and secure cloud infrastructure that safeguards against contemporary threats and challenges. Regular reviews and updates to security practices ensure that the platform remains adaptive and robust in the face of evolving security landscapes.

# London College should protect its data when migrating to the cloud solution

The London College, in the process of migrating to a cloud solution, must meticulously address the protection of its diverse and sensitive datasets. Firstly, it is crucial to understand the nature of the data held by The London College. The institution likely possesses a vast array of data, including student records, academic materials, financial transactions, and administrative documents.

The importance of this data cannot be overstated. Student records, for instance, contain personally identifiable information (PII), making them a prime target for malicious actors. Academic materials, proprietary research, and intellectual property constitute invaluable assets that demand stringent protection. Financial transactions and administrative documents contain sensitive information vital for the college's operations and compliance (Rao 1, 2021).

In migrating to the cloud, one of the primary considerations for The London College should be the implementation of robust security measures to safeguard its data assets. A critical aspect involves choosing a reputable and secure cloud service provider with a strong track record in data protection. The provider should comply with industry standards and regulations, ensuring the highest level of security and confidentiality for The London College's data.

The implementation of encryption mechanisms is paramount during data migration. The London College should employ end-to-end encryption to protect data at rest, in transit, and during processing. Encryption not only adds an additional layer of security but also aligns with best practices for data protection in cloud environments.

Another crucial consideration is the establishment of precise access controls and identity management protocols. The London College should adopt a principle of least privilege, ensuring that users and systems only have access to the minimum necessary data and functionalities. This minimizes the risk of unauthorized access and potential data breaches during the migration process (Abdou Hussein, 2021).

Regular auditing and monitoring mechanisms must be in place to detect and respond to any anomalous activities or security incidents promptly. Continuous monitoring is essential for identifying potential threats or vulnerabilities in real-time, allowing for immediate remediation.

In addition to technological measures, employee training and awareness programs are vital. The London College should educate its staff about the importance of data security, best practices in handling sensitive information, and the specific security measures in place during the migration. Human error remains a significant factor in data breaches, making staff awareness a critical component of overall data protection efforts.

Furthermore, The London College should develop a comprehensive data backup and recovery strategy. Regularly scheduled backups and a well-defined incident response plan ensure that in the event of a data loss or security incident, the college can swiftly recover and resume its operations.

In conclusion, the protection of data during the migration to a cloud solution is a multifaceted challenge that demands a strategic and comprehensive approach from The London College. The institution must prioritize the selection of a secure cloud service provider, employ encryption, establish precise access controls, implement continuous monitoring, conduct employee training, and develop a robust backup strategy to ensure the security and integrity of its invaluable data assets (Abdou Hussein, 2021).

# Conclusion

The journey to the cloud is marked by immense potential but necessitates a vigilant approach to mitigate challenges and ensure robust security. By addressing common problems through strategic solutions and adopting comprehensive security measures, organizations like The London College can confidently embark on their cloud migration journey, unlocking the full benefits of cloud computing while safeguarding their valuable data.

# References

Abdou Hussein, A., 2021. Data Migration Need, Strategy, Challenges, Methodology, Categories, Risks, Uses with Cloud Computing, and Improvements in Its Using with Cloud Using Suggested Proposed Model (DMig 1). *Journal of Information Security,* 12(1), pp. 79-103.

Ahmad, 2013. Development of Cloud Computing and Security Issues. *Information and Knowledge Management,* 3(1).

Alashoor, T., 2014. Cloud computing: a review of security issues and solutions. *International Journal of Cloud Computing,* 3(3), p. 228.

Amazon, 2023. *What is Cloud Computing? - Amazon Web Services.* [Online]   
Available at: https://aws.amazon.com/what-is-cloud-computing/

B. Patel, P. a. K. P., 2021. Cloud Computing Deployment Models: A Comparative Study. *International Journal of Innovative Research in Computer Science & Technology,* 9(2), pp. 45-50.

B. Patel, P. H. ,. a. P. N. K., 2021. Cloud Computing Deployment Models: A Comparative Study. *International Journal of Innovative Research in Computer Science & Technology,* 9(2), pp. 45-50.

Brandao, P., 2018. Cloud Computing: Fundamentals. 9(2).

Chafi, S. B. Y. M. S. F. M. B. M. a. B. B., 2021. Cloud computing services, models and simulation tools. *International Journal of Cloud Computing,* 10(6), p. 533.

Fernandes, D. S. L. G. J. F. M. a. I. P., 2013. Security issues in cloud environments: a survey. *International Journal of Information Security,* 13(2), pp. 113-170.

Huang, k. a. L., 2021. The campus cloud platform setup based on virtualization technology. *Procedia Computer Science,* Volume 183, pp. 73-78.

Jena, S. S. R. S. K. a. K. S., 2020. Cloud Computing Tools: Inside Views and Analysis. *Procedia Computer Science,* Volume 173, pp. 382-391.

Kadhim, Q. Y. R. M. H. A. A.-s. S. a. S. S., 2018. A Review Study on Cloud Computing Issues. *Journal of Physics: Conference Series,* Volume 1018, p. 012006.

Kaleem, M. a. K. P., 2015. Commonly used simulation tools for cloud computing research. pp. 1104-1111.

Kumar, P. R. P. a. J. P., 2017. Exploring Security Issues and Solutions in Cloud Computing Services – A Survey. *Cybernetics and Information Technologies,* 17(4), pp. 3-31.

Moscoso-Zea, O. e. a., 2018. Moving the IT Infrastructure to the Cloud. *Enfoque UTE,* 9(1), pp. 79-89.

Padhy, R. P. a. M. R. P., 2012. Evolution of Cloud Computing and Enabling Technologies. *International Journal of Cloud Computing and Services Science (IJ-CLOSER),* 1(4).

Patel, H. a. K. N., 2021. *Cloud Computing Deployment Models: A Comparative Study.* [Online]   
Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3827705

Patel, H. a. N. K., 2021. *Cloud Computing Deployment Models: A Comparative Study.* [Online]   
Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3827705

Rajeswari, M. &. M. S., 2019. OVERVIEW OF CLOUD COMPUTING AND ITS TYPES. *SSRN Electronic Journal,* Issue 6, pp. 61-67.

Rao 1, G. S. K. 1. S. S. 2. V. K. 3. D. P. 4. R. 5. L. Y. G. 5. 1. D. o. C. a. E. K., 2021. A Secure and Efficient Data Migration Over Cloud Computing. *ProQuest.*

Rodriguez-Martinez, M. S. J. a. G. M., 2010. Open Source Cloud Computing Tools: A Case Study with a Weather Application. *IEEE Xplore,* p. 443–449.

Sether, A., 2016. Cloud Computing Benefits. *SSRN Electronic Journal.*

Singh, A. a. C. K., 2017. Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications,* Volume 79, pp. 88-115.

Singh, S. J. Y.-S. a. P. J., 2016. A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications,* Volume 75, pp. 200-222.

Singh, S. M. P. T. R. a. V. V., 2018. Cloud Computing and Security Issues in the Cloud. *Trinity Journal of Management, IT & Media,* 9(1), pp. 22-27.

Tang, A. e. a., 2019. *A comparative analysis of architecture frameworks.* [Online]   
Available at: https://ieeexplore.ieee.org/abstract/document/1371981/authors#authors

Turab, N. T. A. a. M. S., 2013. Cloud Computing Challenges And Solutions. *International journal of Computer Networks & Communications,* 5(5), pp. 209-216.

Xue, C. T. S. a. F. T. W. X., 2016. Benefits and Challenges of the Adoption of Cloud Computing in Business. *International Journal on Cloud Computing: Services and Architecture,* 6(6), pp. 01-15.

Zhu, L., 2016. Study on Open Source Software Based on Cloud Computing Platform.