Experiment no. 8

Aim: To study and Implement Security as a Service on AWS/Azure

Requirements: Azure account

Theory:

We know that security is job one in the cloud and how important it is that you find accurate and timely information about Azure security. One of the best reasons to use Azure for your applications and services is to take advantage of its wide array of security tools and capabilities. These tools and capabilities help make it possible to create secure solutions on the secure Azure platform. Microsoft Azure provides confidentiality, integrity, and availability of customer data, while also enabling transparent accountability.

General Azure security

Microsoft Defender for Cloud A cloud workload protection solution that provides security management and advanced threat protection across hybrid cloud workloads.

Azure Key Vault A secure secrets store for the passwords, connection strings, and other information you need to keep your apps working.

Azure Monitor logs A monitoring service that collects telemetry and other data, and provides a query language and analytics engine to deliver operational insights for your apps and resources. Can be used alone or with other services such as Defender for Cloud.

Azure Dev/Test Labs A service that helps developers and testers quickly create environments in Azure while minimizing waste and controlling cost.

Storage security

Azure Storage Service Encryption A security feature that automatically encrypts your data in Azure storage.

StorSimple Encrypted Hybrid Storage An integrated storage solution that manages storage tasks between on-premises devices and Azure cloud storage.

Azure Client-Side Encryption A client-side encryption solution that encrypts data inside client applications before uploading to Azure Storage; also decrypts the data while downloading.

Azure Storage Shared Access Signatures A shared access signature provides delegated access to resources in your storage account.

Azure Storage Account Keys An access control method for Azure storage that is used for authentication when the storage account is accessed.

Azure File shares with SMB 3.0 Encryption A network security technology that enables automatic network encryption for the Server Message Block (SMB) file sharing protocol.

Azure Storage Analytics A logging and metrics-generating technology for data in your storage account.

Database security

Azure SQL Firewall A network access control feature that protects against network-based attacks to database.

Azure SQL Cell Level Encryption A database security technology that provides encryption at a granular level.

Azure SQL Connection Encryption To provide security, SQL Database controls access with firewall rules limiting connectivity by IP address, authentication mechanisms requiring users

to prove their identity, and authorization mechanisms limiting users to specific actions and data.

Azure SQL Always Encryption Protects sensitive data, such as credit card numbers or national identification numbers (for example, U.S. social security numbers), stored in Azure SQL Database or SQL Server databases.

Azure SQL Transparent Data Encryption A database security feature that encrypts the storage of an entire database.

Azure SQL Database Auditing A database auditing feature that tracks database events and writes them to an audit log in your Azure storage account.

Identity and access management

Azure role-based access control An access control feature designed to allow users to access only the resources they are required to access based on their roles within the organization.

Azure Active Directory A cloud-based authentication repository that supports a multi-tenant, cloud-based directory and multiple identity management services within Azure.

Azure Active Directory B2C An identity management service that enables control over how customers sign-up, sign-in, and manage their profiles when using Azure-based applications.

Azure Active Directory Domain Services A cloud-based and managed version of Active Directory Domain Services.

Azure AD Multi-Factor Authentication A security provision that employs several different forms of authentication and verification before allowing access to secured information.

Backup and disaster recovery

Azure Backup An Azure-based service used to back up and restore data in the Azure cloud.

Azure Site Recovery An online service that replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location to enable recovery of services after a failure.

Networking

Network Security Groups A network-based access control feature using a 5-tuple to make allow or deny decisions.

Azure VPN Gateway A network device used as a VPN endpoint to allow cross-premises access to Azure Virtual Networks.

Azure Application Gateway An advanced web application load balancer that can route based on URL and perform SSL-offloading.

Web application firewall (WAF) A feature of Application Gateway that provides centralized protection of your web applications from common exploits and vulnerabilities

Azure Load Balancer A TCP/UDP application network load balancer.

Azure ExpressRoute A dedicated WAN link between on-premises networks and Azure Virtual Networks.

Azure Traffic Manager A global DNS load balancer.

Azure Application Proxy An authenticating front-end used to secure remote access for web applications hosted on-premises.

Azure Firewall A managed, cloud-based network security service that protects your Azure Virtual Network resources.

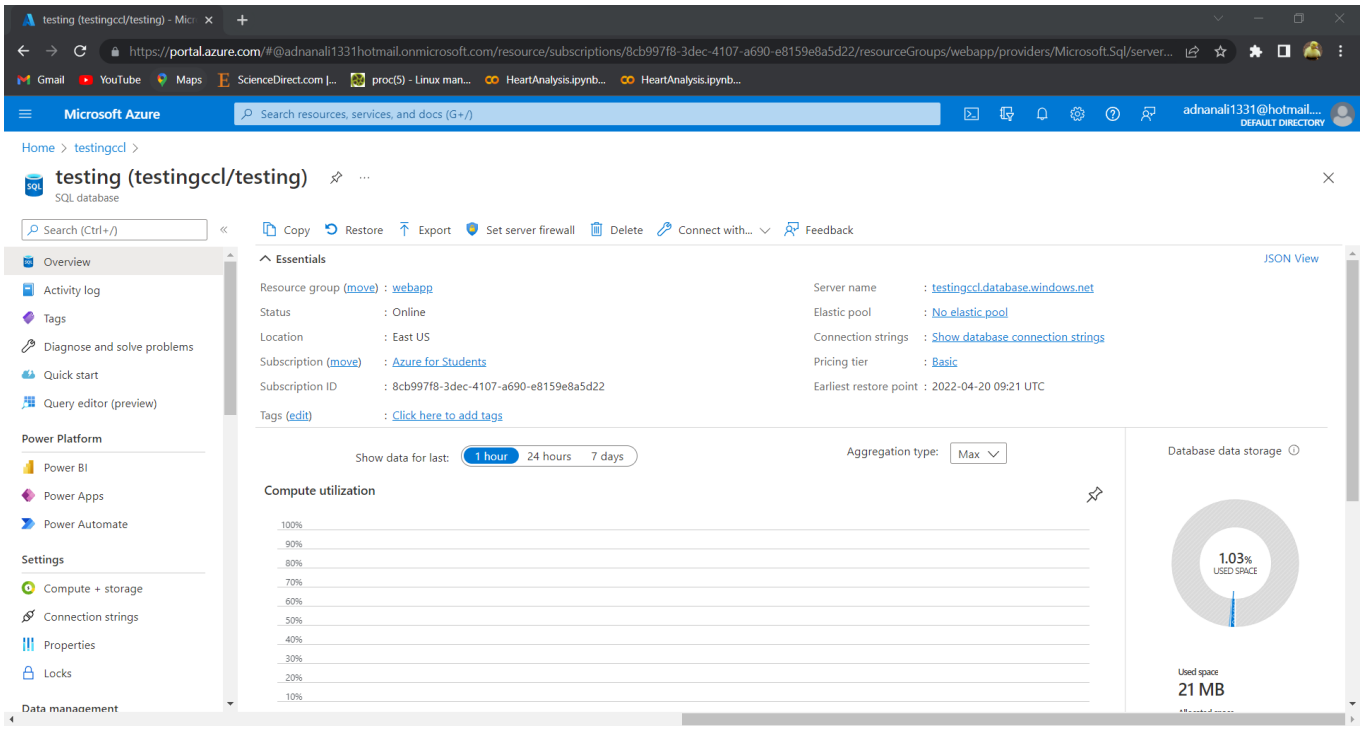
Azure DDoS protection Combined with application design best practices, provides defense against DDoS attacks.

Virtual Network service endpoints Extends your virtual network private address space and the identity of your VNet to the Azure services, over a direct connection.

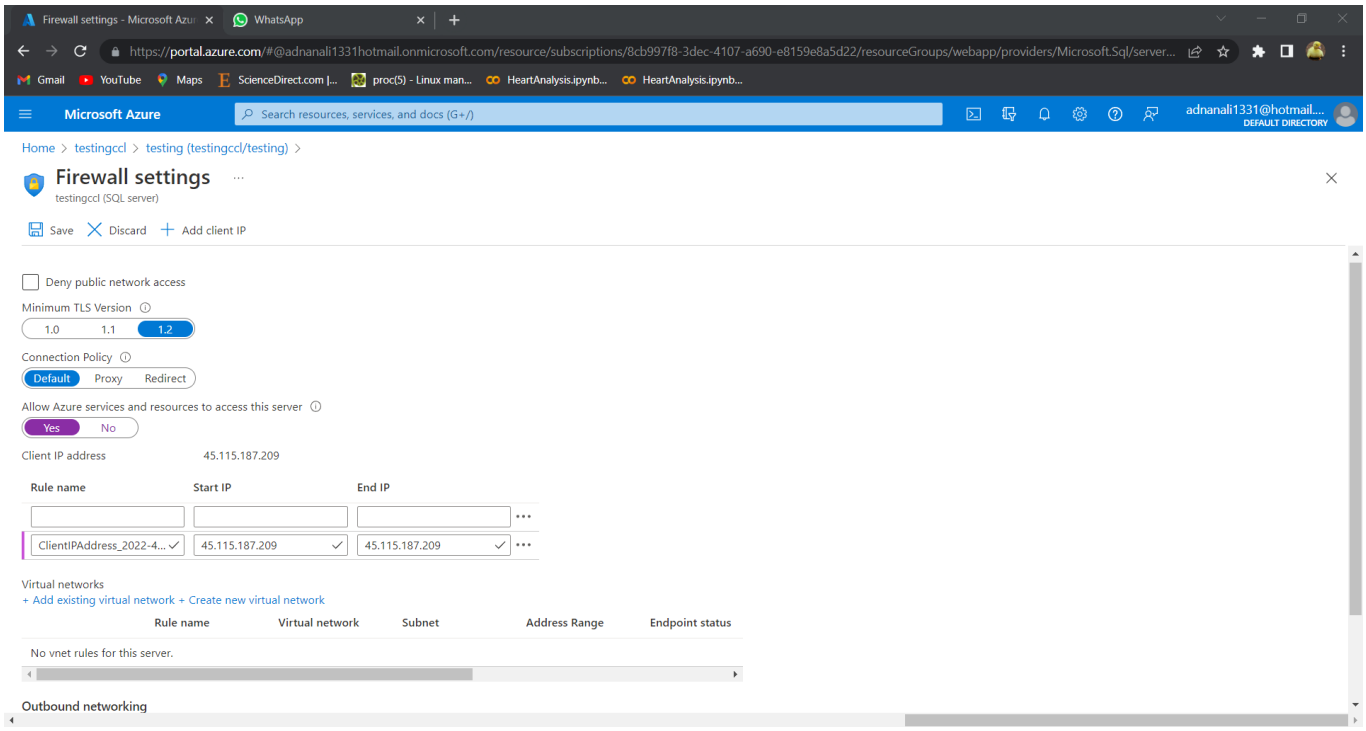
Output:

Database Firewall protection

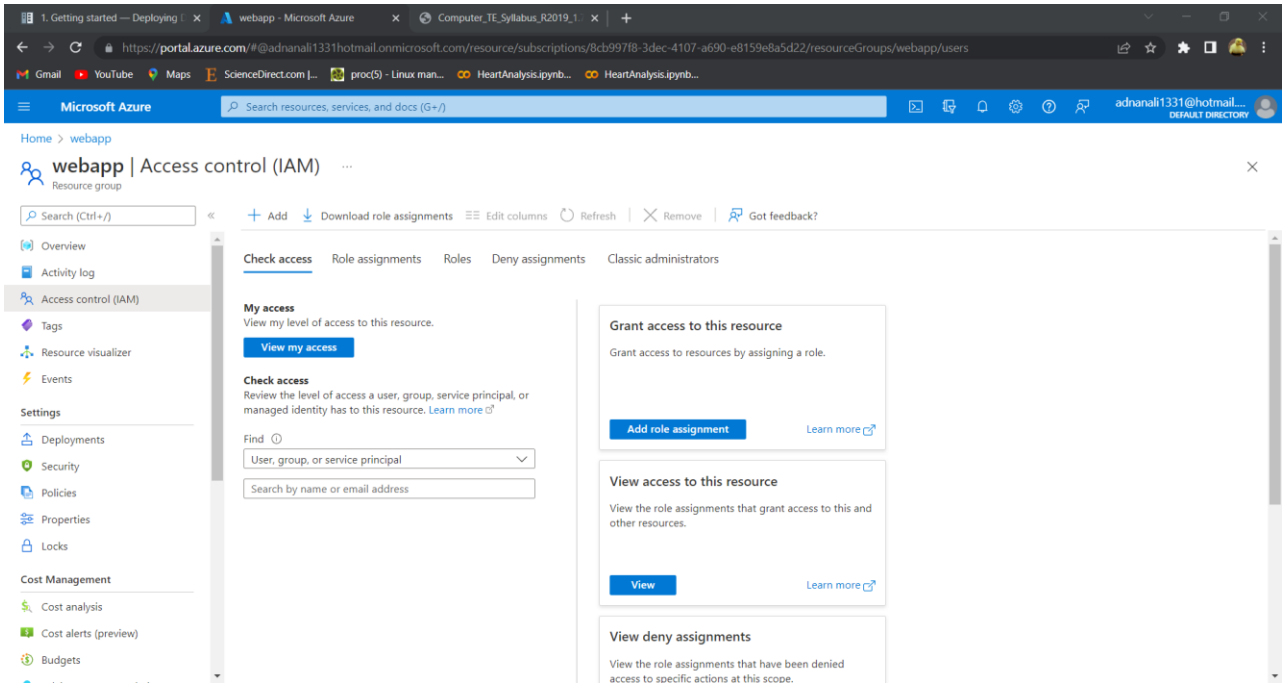
Database:



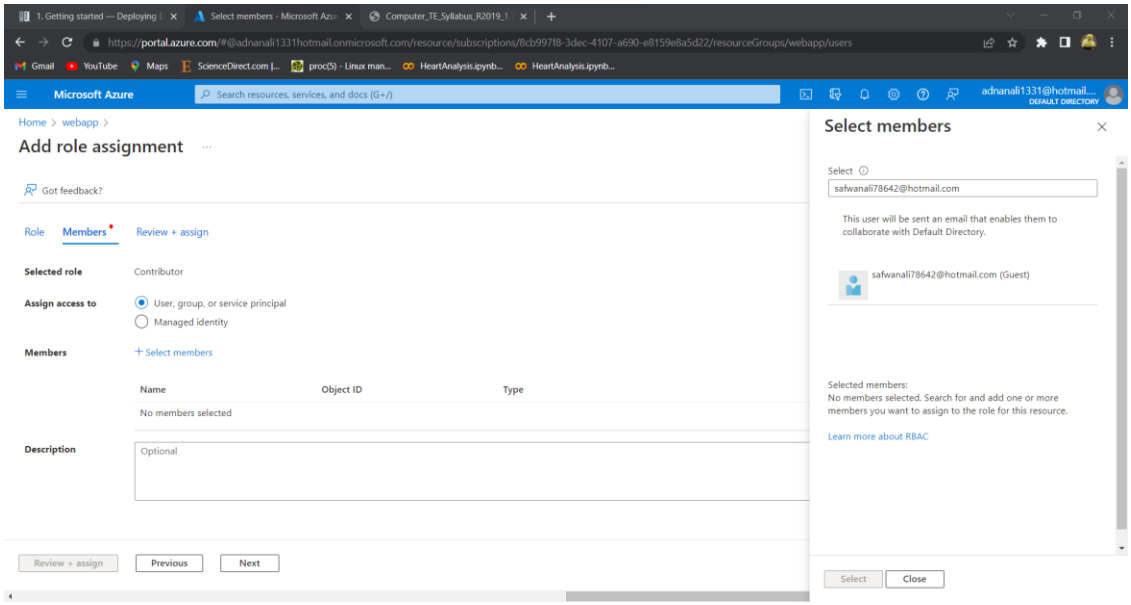
Adding Firewall security:

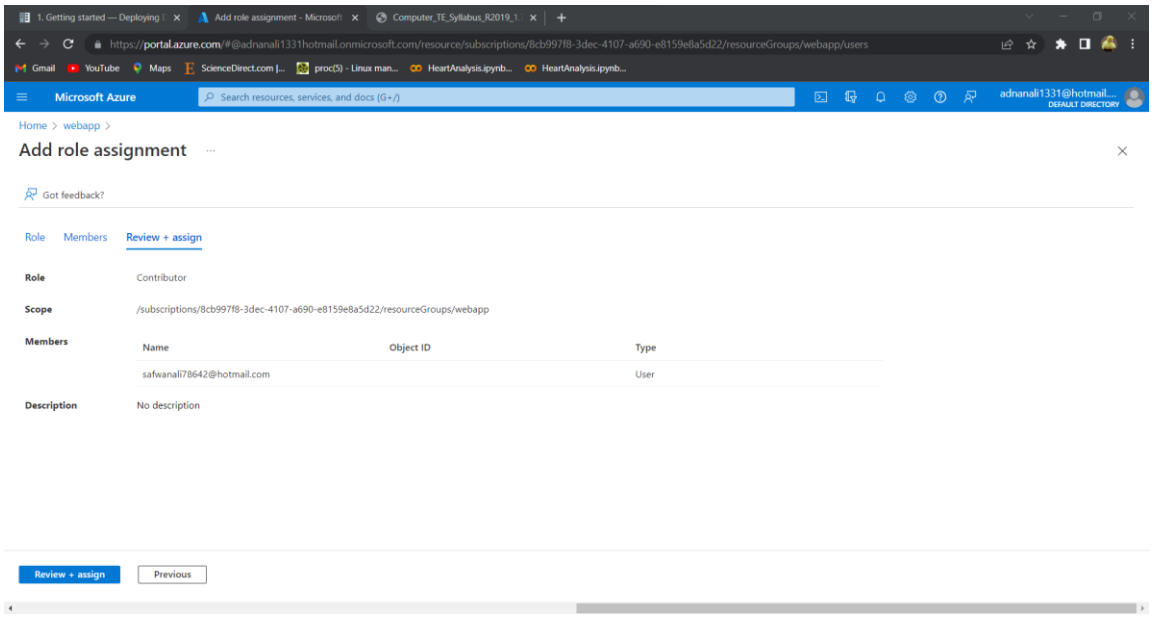


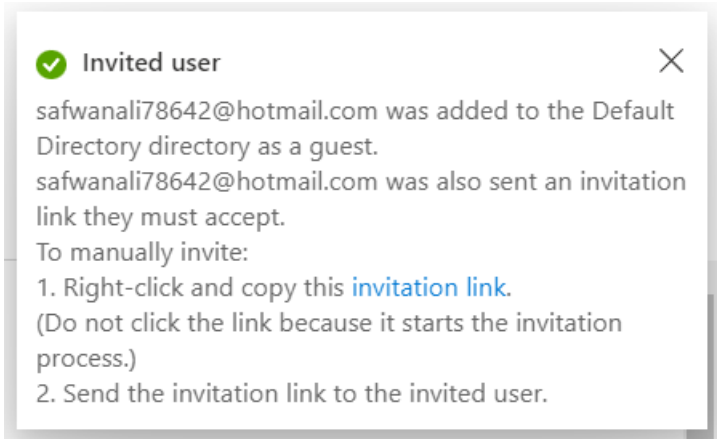
Access Control (IAM)



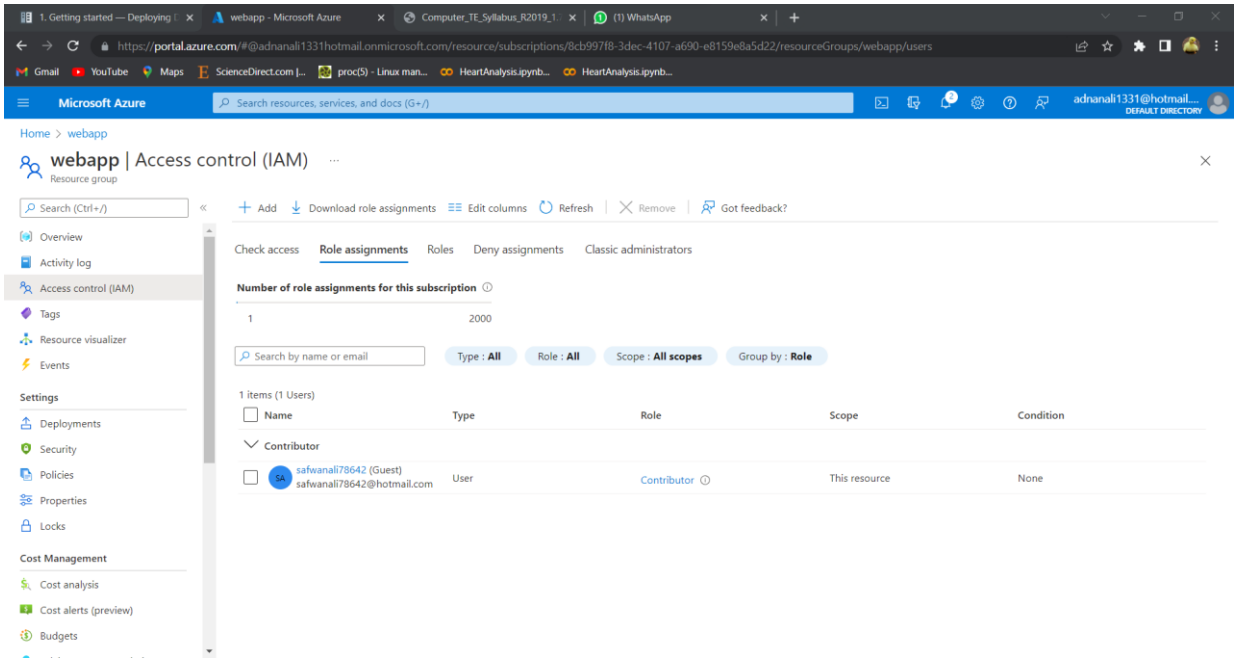
76_Adnan Shaikh





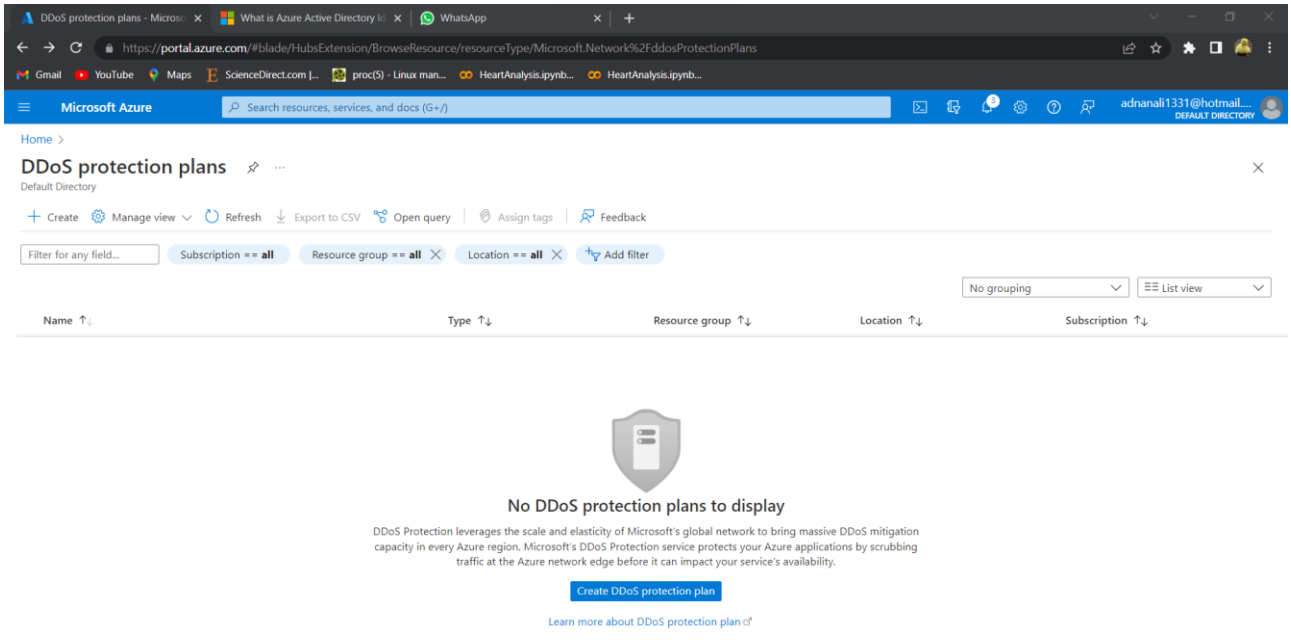


76_Adnan Shaikh

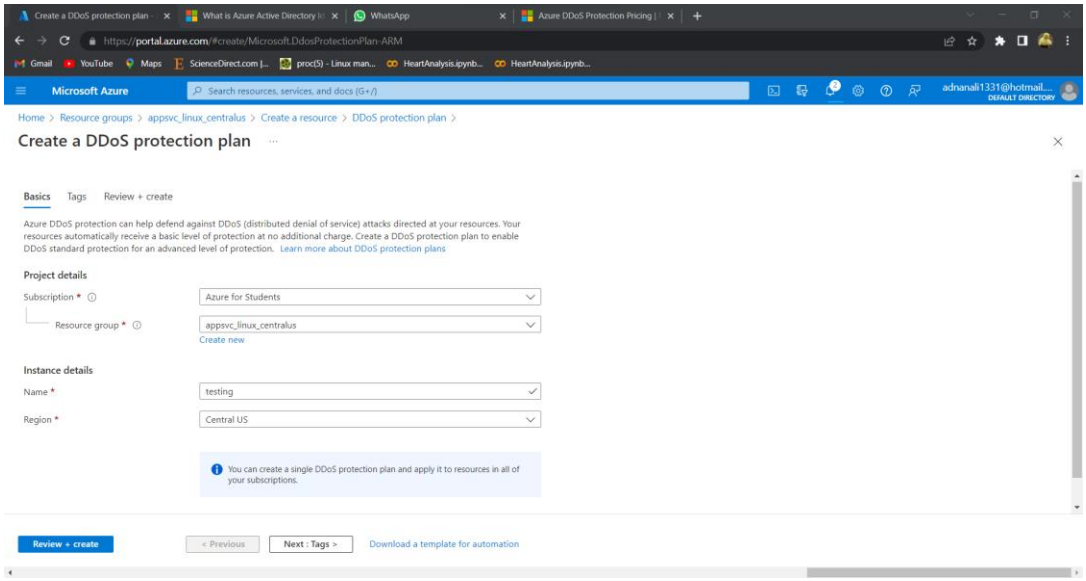


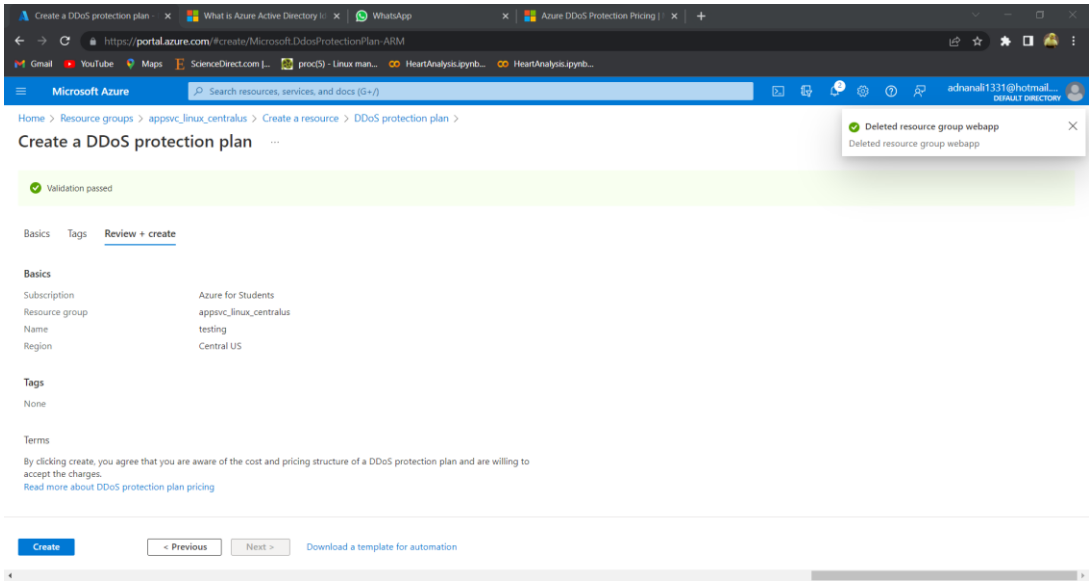
DDOS

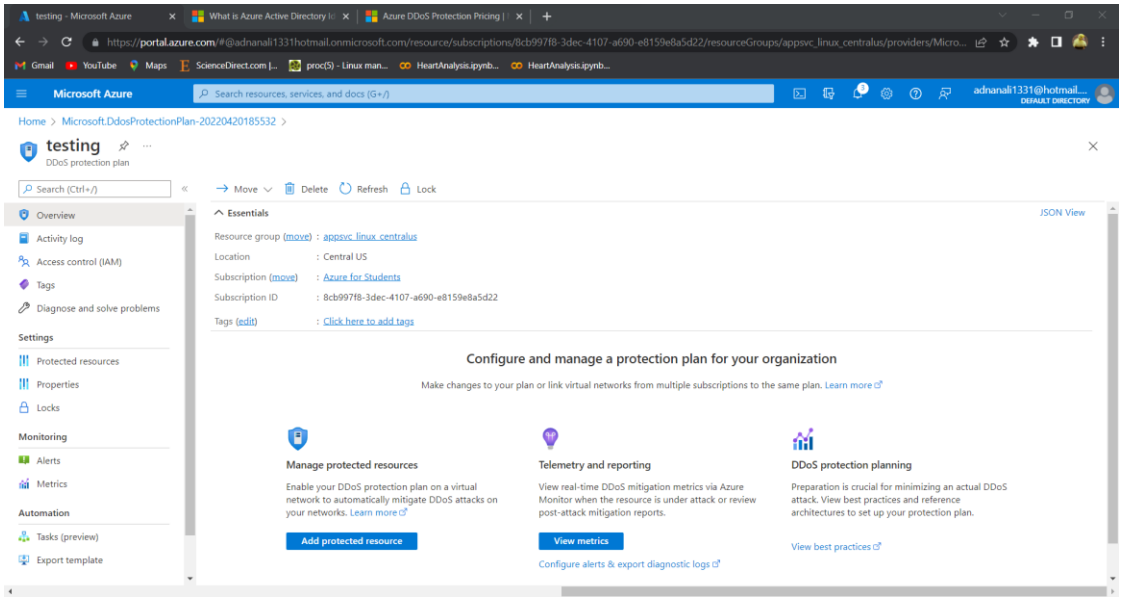
Creating DDOS plan:



76_Adnan Shaikh

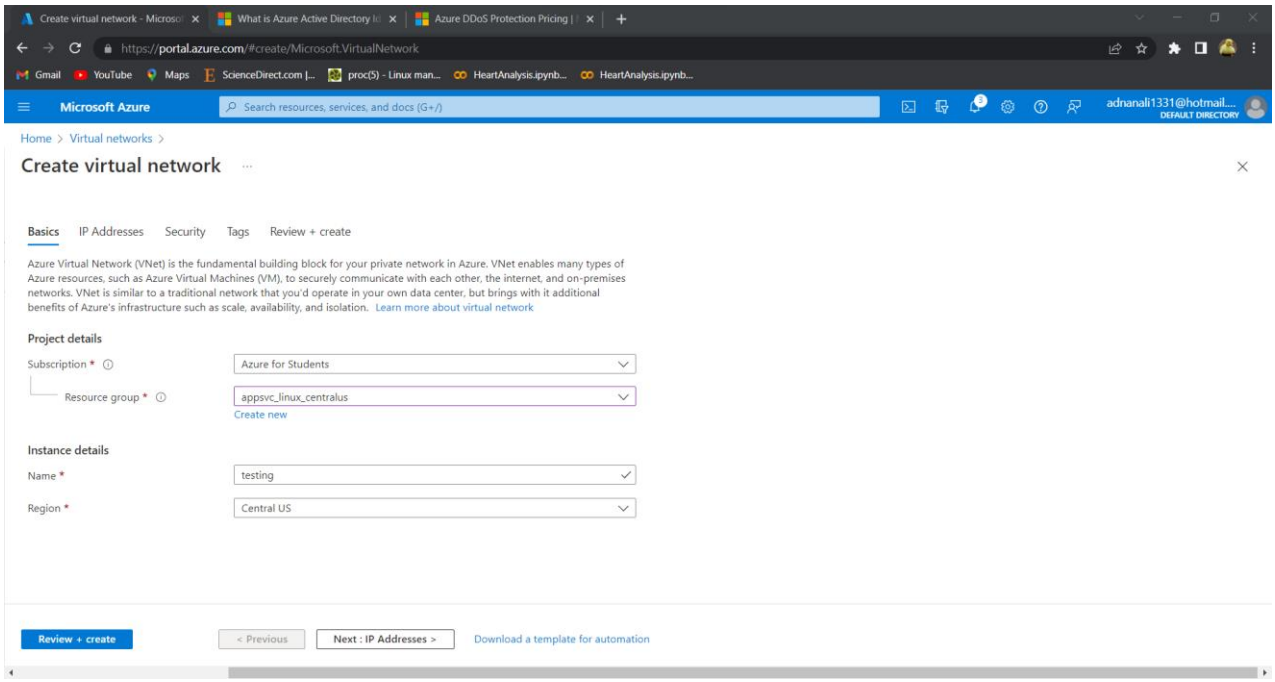




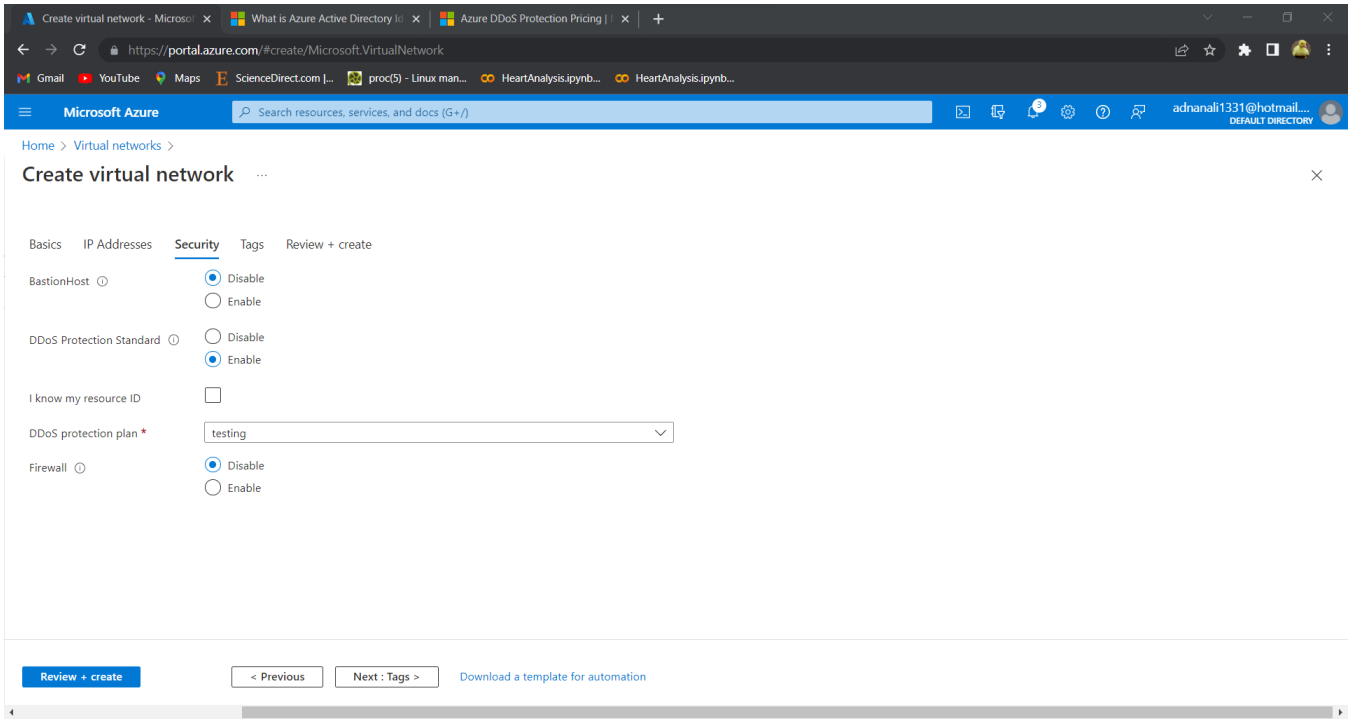


76_Adnan Shaikh

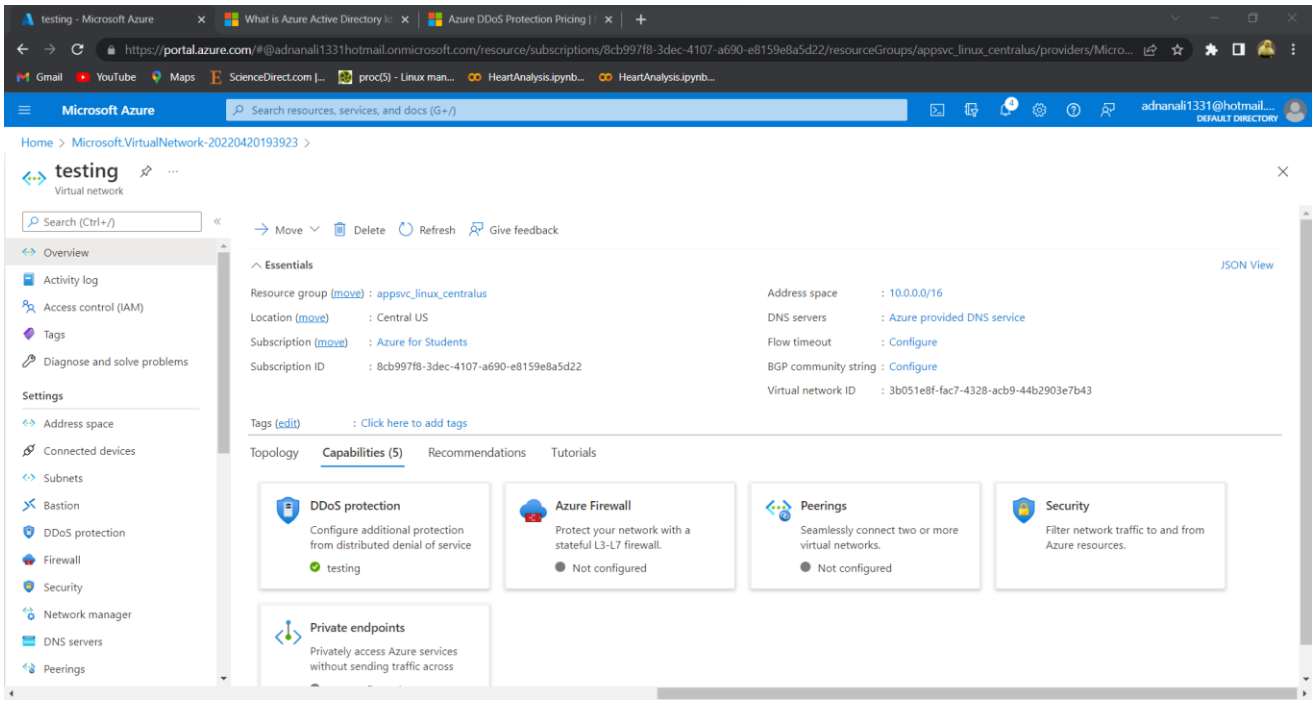
Creating Network with DDOS plan:



Adding DDOS plan as security:

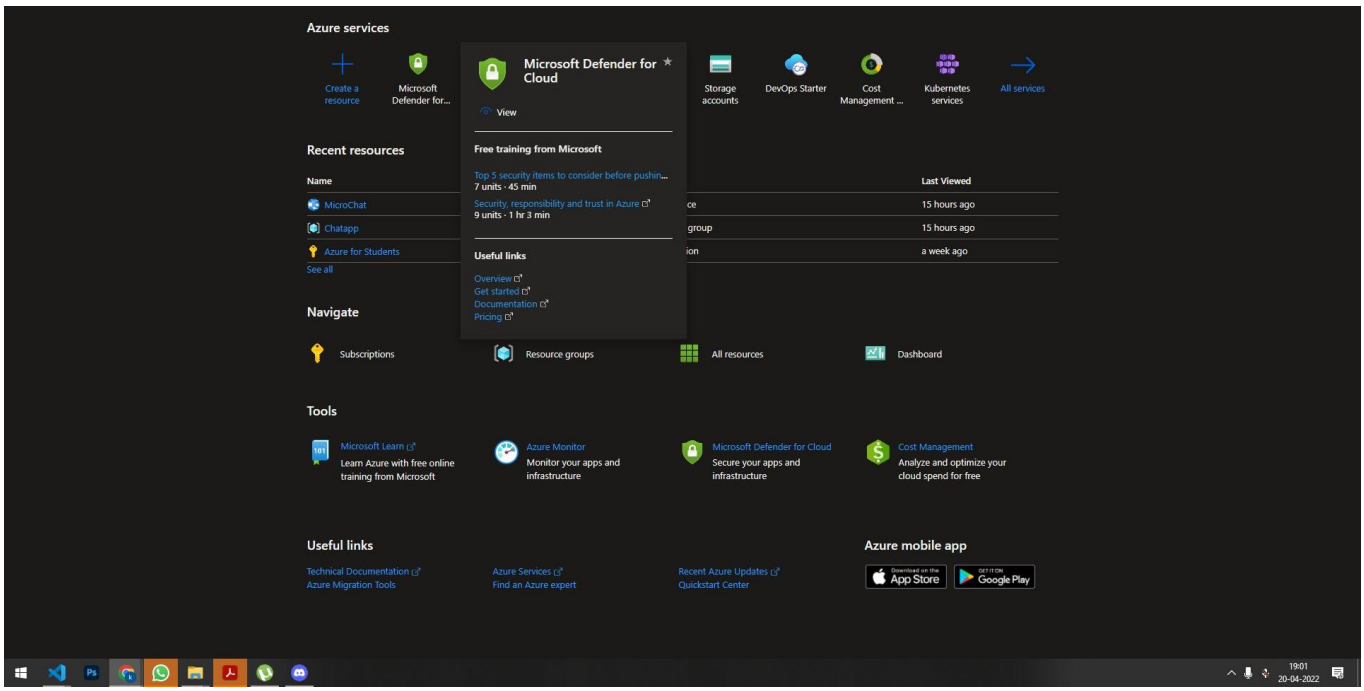


Network with active DDOS plan:



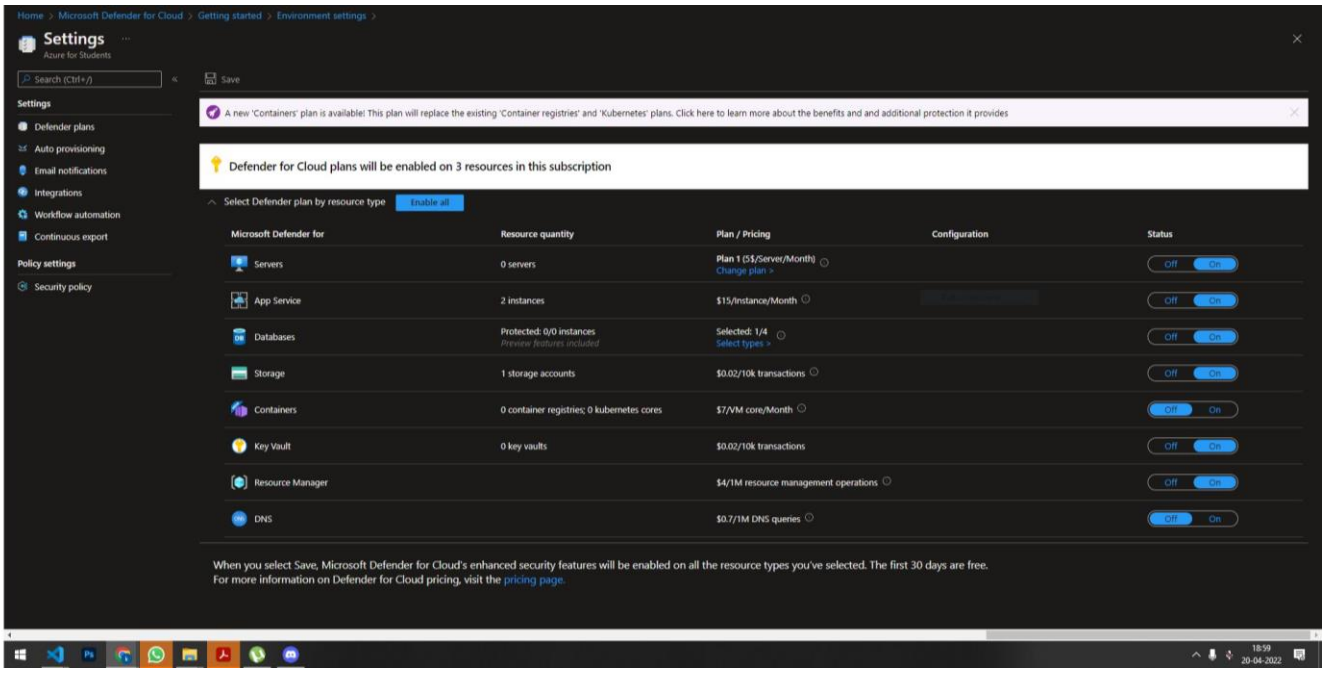
Microsoft Defender Security

Creating Microsoft defender resource:

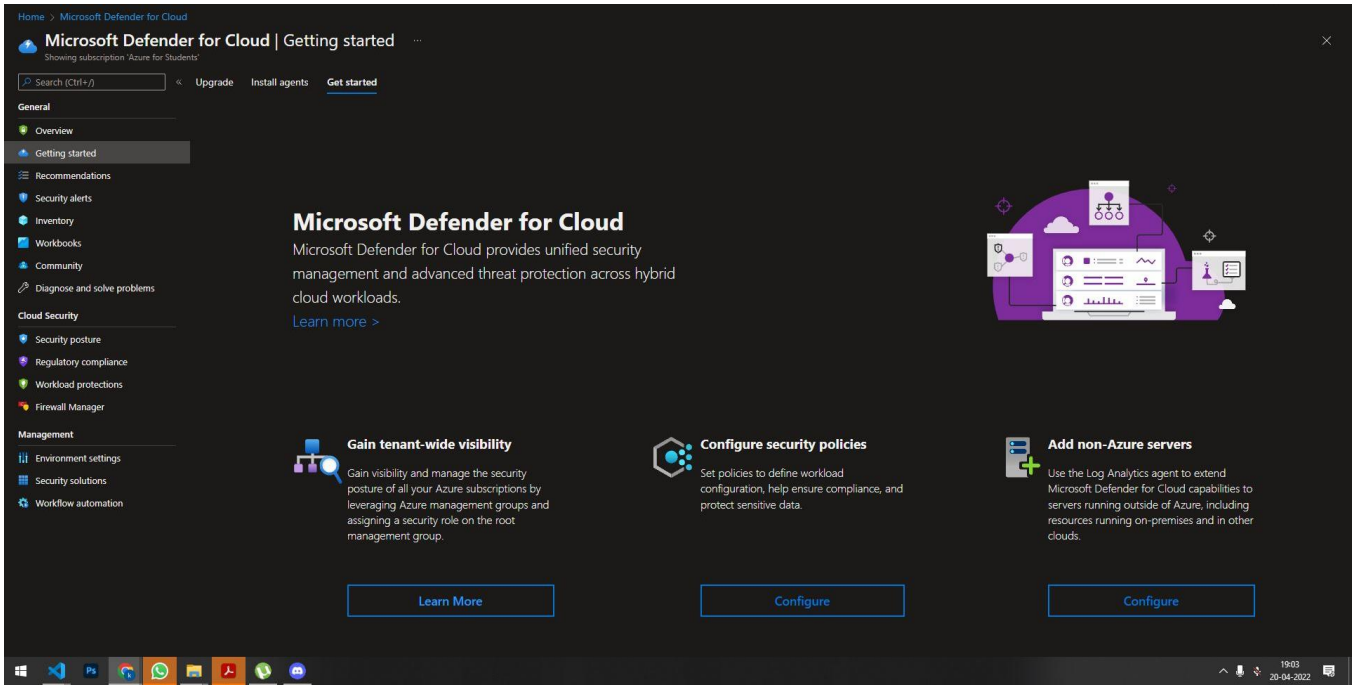


76_Adnan Shaikh

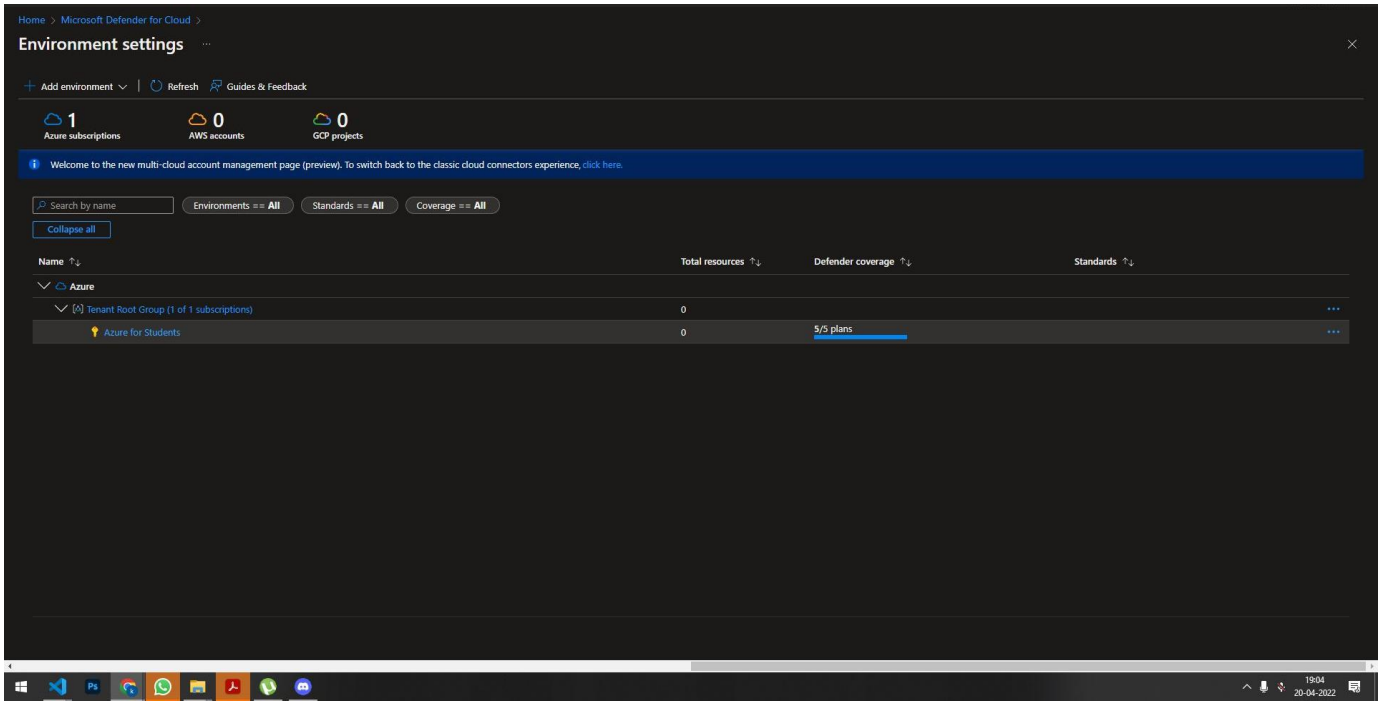
Adding resources:



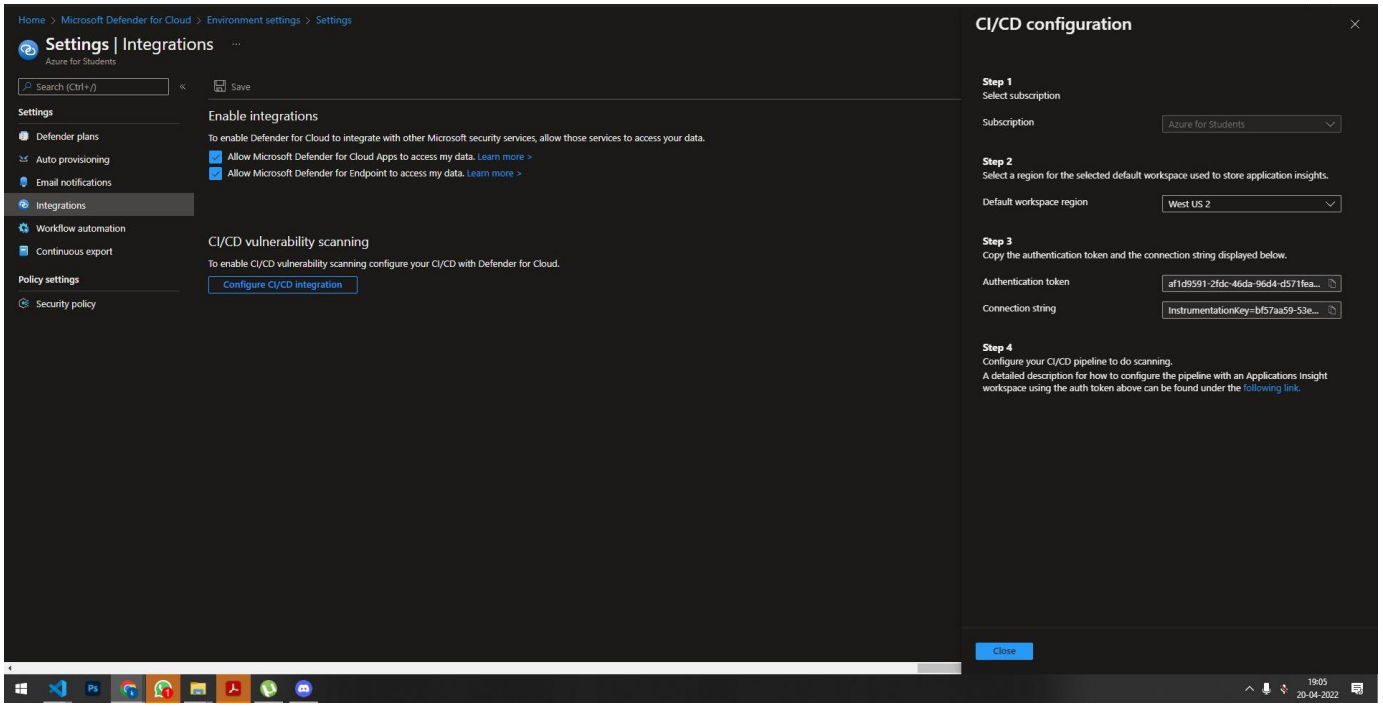
Checking active plan:



76_Adnan Shaikh

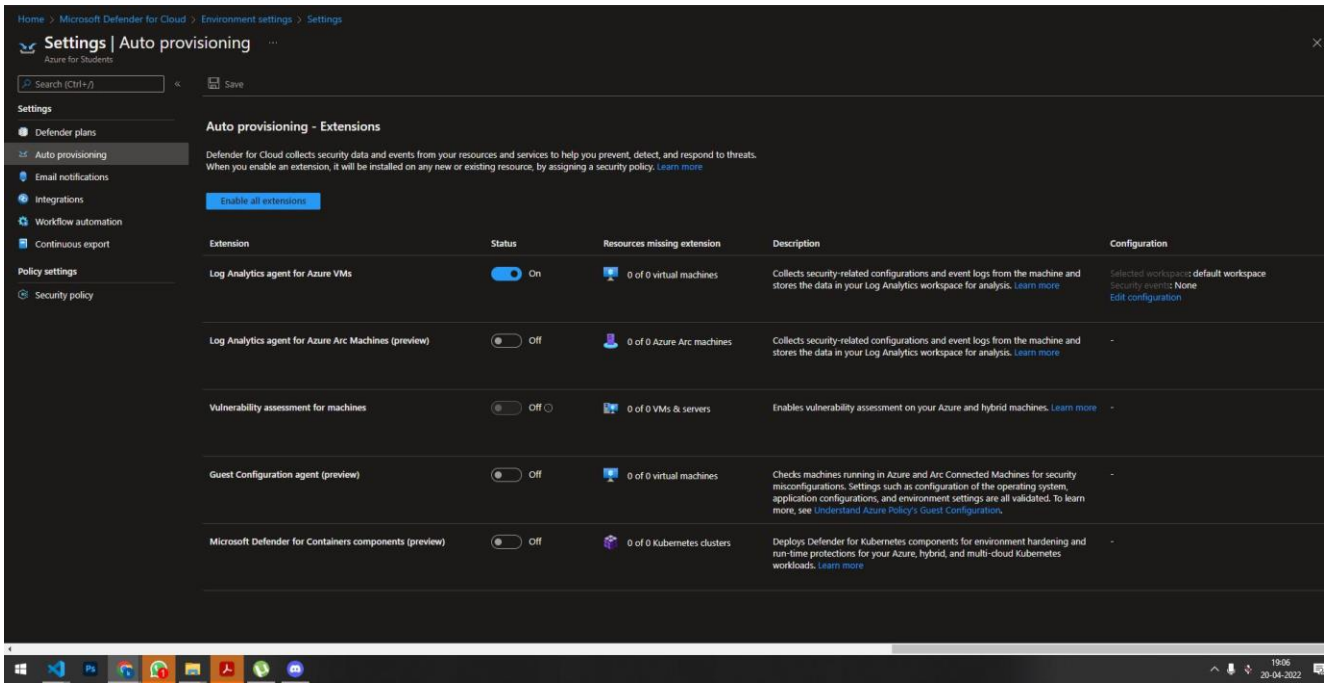


Enabling Integration:

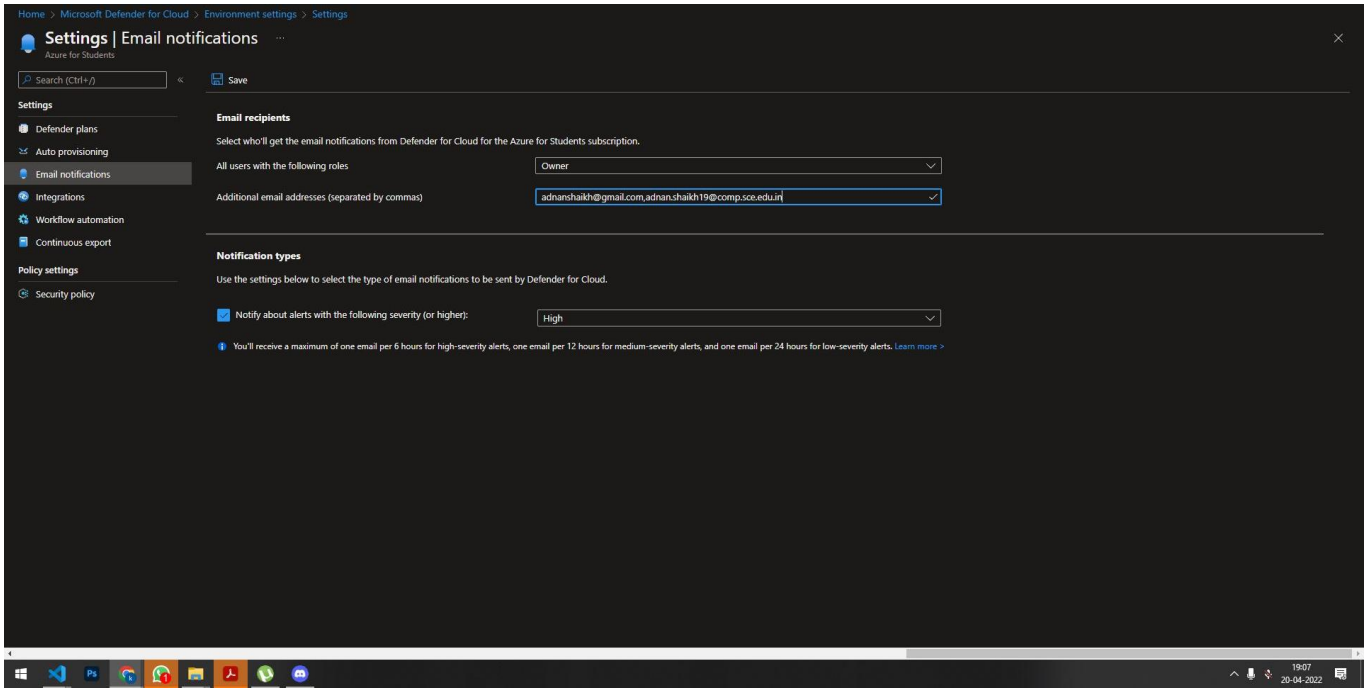


76_Adnan Shaikh

Enable Logging:

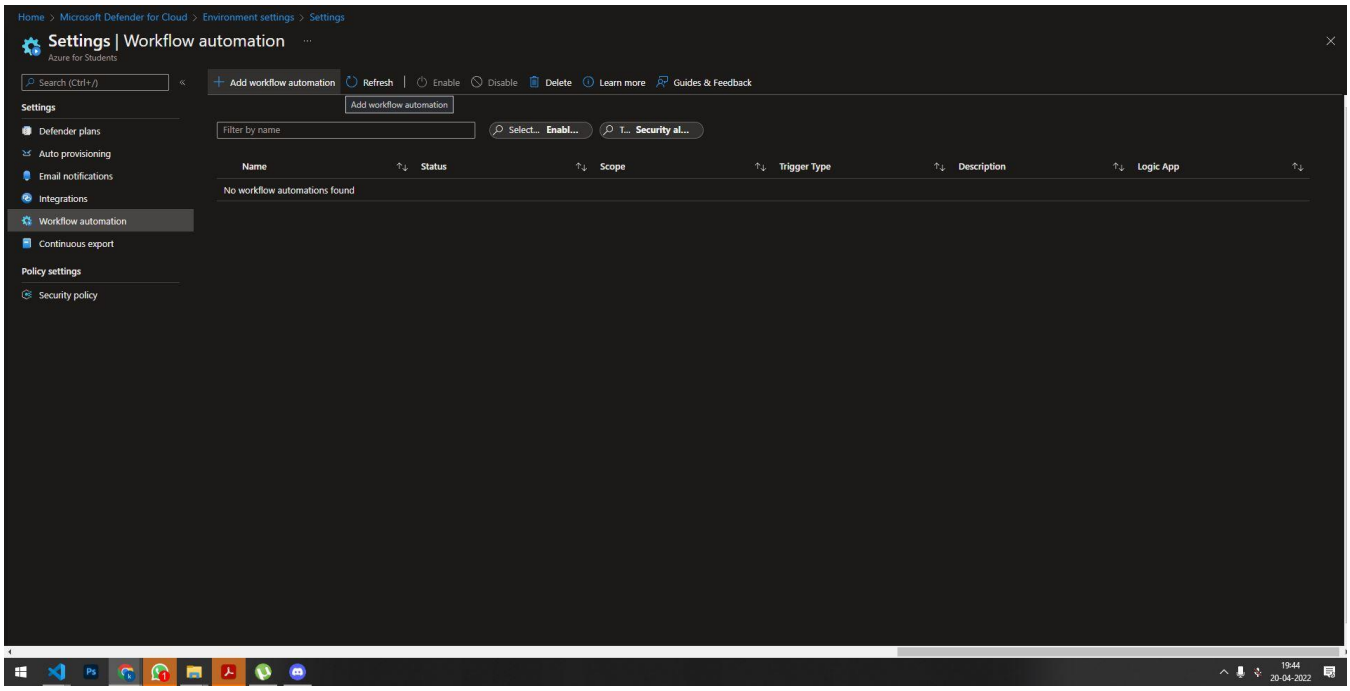


Setting Email for notification:

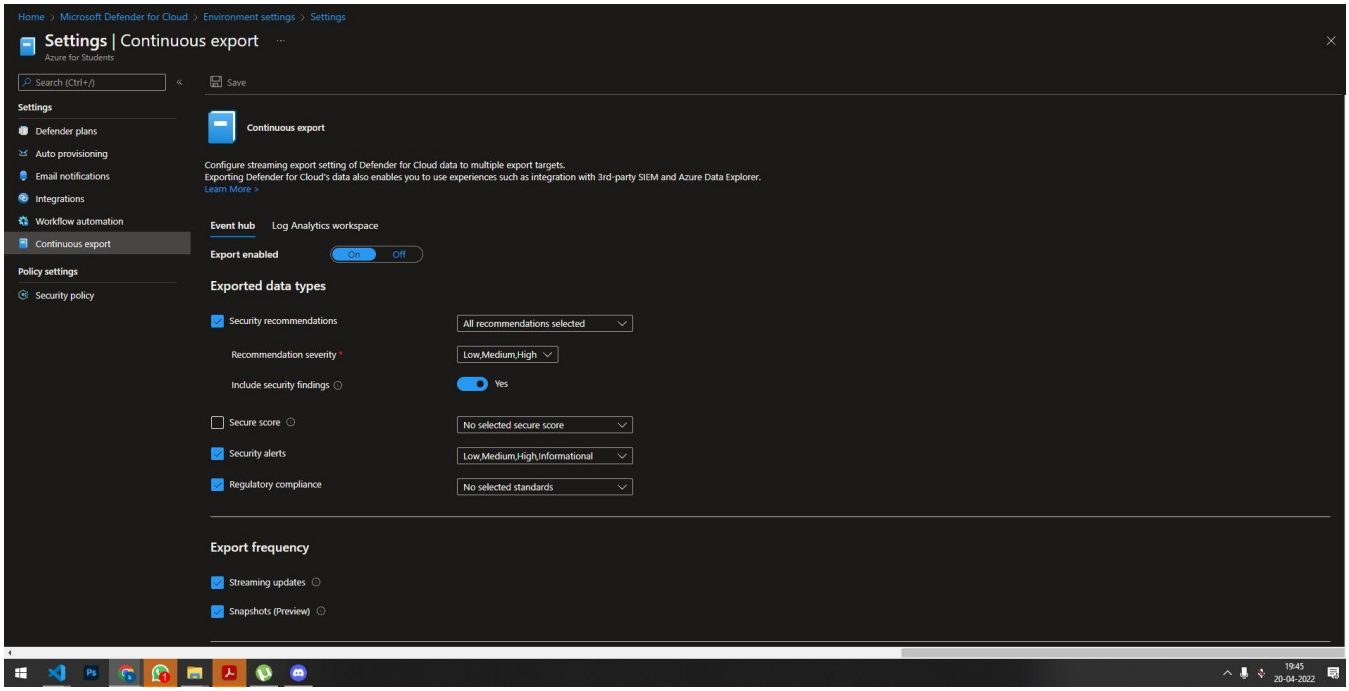


76_Adnan Shaikh

Work flow automation:

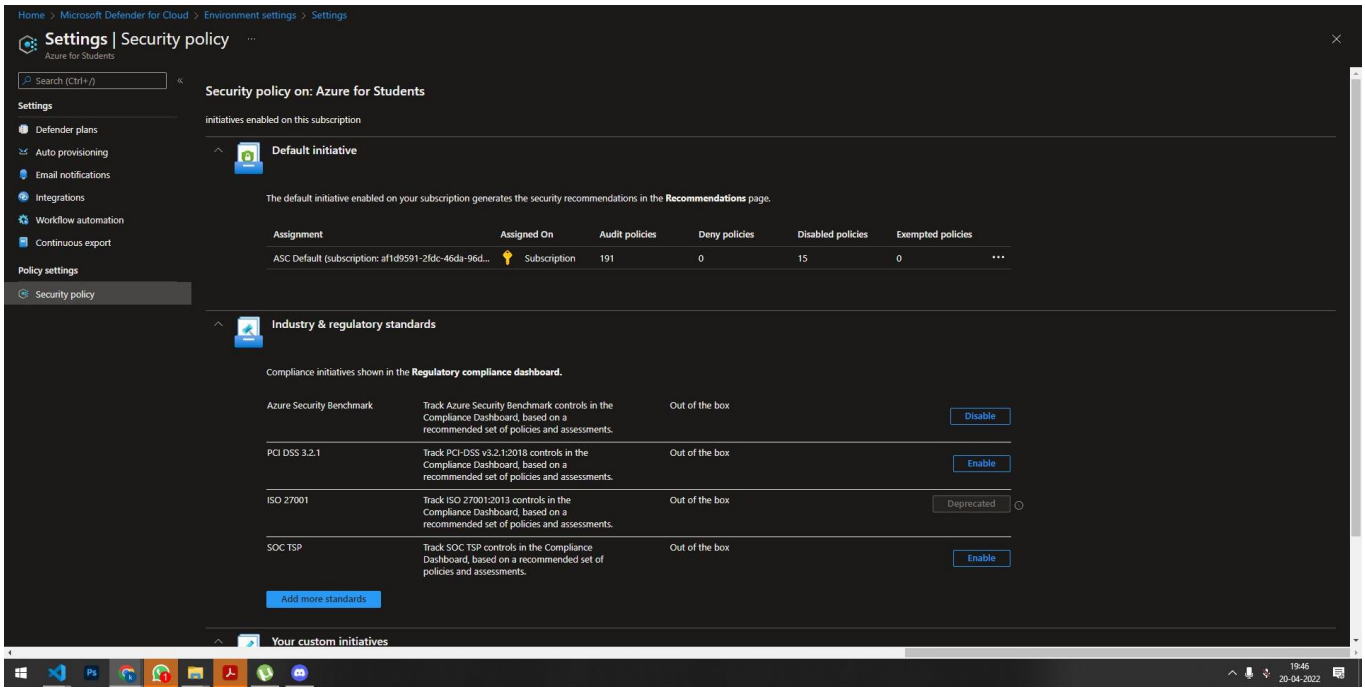


Continuous export:



76_Adnan Shaikh

Security Policy:



Conclusion: We have successfully implemented Security as a service on Azure