CYBERINFINITI LTD

# Security Operations Center (SOC) Enterprise Cloud Security Assessment Report using Microsoft Azure

**Report Title:** Microsoft Azure Enterprise Cloud Security Assessment

---

**Organization:** Cyberinfiniti ltd.

**Report ID:** TIR-CTI-2026-INT-002

**Report Date:** February 2026

**Classification:** Confidential / Internal Use

**Analysts:** John Ofulue, Halimat Omorinsola Adepegba, Favour Obisike, Ikenna Emerole, Blessing Ibe, Ayodimeji Omole, Divine Ezewele, Andrew Moses, Odunayo Balogun.

**Report Version:** 1.0

**Distribution:** CyBlack Team, SOC Team, Executive Management

---

# Table of Contents

# 1.0 Executive Summary

This report presents the results of a comprehensive **Enterprise Cloud Security Assessment** conducted for **Cyberinfiniti Ltd** within a realistic Microsoft Azure production environment with nine practice labs. The objective of the assessment was to evaluate the organization's cloud security posture across identity governance, access control, monitoring, threat detection, and incident response capabilities, while aligning technical security controls with executive risk, governance, and resilience priorities.

The assessment evaluated how effectively Azure-native security services can be configured and operationalized to defend cloud workloads against modern threat scenarios, including unauthorized access, misconfiguration exploitation, lateral movement, and delayed threat detection. Particular emphasis was placed on the effectiveness of **preventive**, **detective**, and **responsive** security controls required for organizations operating in security-sensitive and cyber-driven business environments.

Actionable, leadership-focused insights were produced by correlating observed control behavior with industry-aligned security principles such as **Zero Trust Architecture**, **defense-in-depth**, and **least-privilege access**. Findings were mapped to operational risk, potential business impact, and security maturity indicators to support informed executive decision-making.

Overall, the assessment demonstrated that Microsoft Azure's integrated security ecosystem, when correctly implemented and governed, can significantly reduce organizational attack surface, enhance security visibility, and enable faster, more consistent incident response. Strategic gaps were also identified in areas such as configuration complexity, governance consistency, and skills dependency, informing targeted recommendations for Cyberinfiniti Ltd's cloud security roadmap.

# 2.0 Scenario Overview & Objectives

## 2.1 Scenario Overview

Cyberinfiniti Ltd operates as a technology and cybersecurity-focused organization leveraging Microsoft Azure to host workloads, manage identities, and support centralized security operations. As part of its cloud adoption and maturity strategy, executive leadership required assurance that Azure resources were securely configured, monitored, and capable of supporting effective threat detection and response.

The assessment simulated real-world enterprise operating conditions where cloud administrators, service desk personnel, and security analysts interact with Azure resources. The environment was intentionally designed to reflect common enterprise risks, including excessive privileges, exposed management interfaces, inconsistent logging, and delayed incident response.

The assessment team functioned as Cyberinfiniti Ltd's internal cloud security and SOC capability, evaluating existing security controls and demonstrating how Azure-native services can be leveraged to strengthen the organization's overall cloud security posture.

## 2.2 Assessment Objectives

The primary objectives of the assessment were to:

- Evaluate identity and access controls to ensure enforcement of least privilege and role separation.
- Assess centralized visibility and monitoring across cloud workloads.
- Validate the ability to detect misconfigurations, vulnerabilities, and active threats.
- Measure the effectiveness of attack surface reduction controls.
- Demonstrate incident detection and automated response aligned with modern SOC operations.
- Translate technical findings into executive-level risk, impact, and maturity insights.

# 3.0 Scope of Assessment

The assessment focused on the following cloud security domains across the Azure Environment:

- **Identity and Access Management (Microsoft Entra ID & RBAC)** : In modern cloud ecosystems, where identities effectively replace traditional network perimeters, robust IAM practices are essential for maintaining security, compliance, and operational integrity.

  During this cloud security sprint, Microsoft Entra ID (formerly Azure Active Directory) and Azure Role-Based Access Control (RBAC) were strategically implemented to manage digital identities and regulate access across the Azure environment. Microsoft Entra ID functioned as the centralized identity provider, enabling secure authentication of users, groups, and service principals, while RBAC was used to define and enforce authorization policies aligned with operational roles and responsibilities.

  By applying the principle of least privilege, access rights were carefully assigned to ensure that users and administrators possessed only the permissions necessary to perform their designated tasks. This approach minimized the risk of privilege misuse, accidental misconfigurations, and potential insider threats. Collectively, these IAM controls strengthened governance, improved accountability, and reinforced the overall security posture of the deployed cloud infrastructure.

- **Monitoring, Logging, and Telemetry Collection** : Monitoring, logging, and telemetry collection are important components of an effective cloud security framework. In Microsoft Azure environments, they provide continuous visibility into system activities, user behavior, configuration changes, and potential security threats. Cloud monitoring involves the continuous observation of infrastructure, applications, and identity activities to ensure operational health and detect anomalies. Azure Monitor was utilized to track performance metrics, use of resources, and security-relevant events across deployed services.

  Logging constitutes the foundational evidence base for effective security monitoring, incident response, and forensic investigation within cloud environments. It provides verifiable records of system activities, user actions, configuration changes, and administrative operations, enabling organizations to reconstruct events, identify root causes, and assess the scope and impact of potential security incidents. During the sprint, different log sources such as Microsoft Entra ID sign-in logs, Audit logs e.t.c were carefully configured and

these provided insights into role assignments, privilege changes,Resource creation, modification, or deletion.

Telemetry refers to the automated collection and transmission of data from cloud resources to centralized monitoring systems. Log Analytics Workspace was configured to aggregate logs from various Azure services, creating a unified data repository for analysis. Effective monitoring and logging significantly reduce organizational risk. Misconfigurations, unauthorized access attempts, and abnormal behavior can only be detected if visibility mechanisms are properly implemented. Monitoring, logging, and telemetry collection are indispensable pillars of cloud security operations. By leveraging Azure Monitor, Log Analytics, and Microsoft Sentinel, the sprint environment established continuous visibility and reinforced governance controls. These mechanisms ensure that cloud environments remain resilient, auditable, and responsive to evolving security threats.

- **Cloud Workload Protection and Posture Managemen**t: Cloud Workload Protection (CWP) and Cloud Security Posture Management (CSPM) are crucial for securing workloads and ensuring compliance in Azure cloud environments. IT is important to note that both concepts are applied to safeguard deployed workloads—including virtual machines, containerized applications, and serverless functions—while continuously assessing the security posture of the cloud infrastructure.
    - ➔ **Cloud Workload Protection** ensures that all workloads are adequately secured against potential threats, vulnerabilities, and unauthorized access. The sprint involved implementing endpoint protection, configuring policies, and applying measures to both virtual machines and containers.
    - ➔ **Cloud Security Posture Management** complements workload protection by providing a comprehensive view of the overall security and compliance state of cloud resources.This process ensures that security controls are not only deployed but continuously monitored for effectiveness. By integrating workload protection with posture management, a safe approach to cloud security is achieved.
- **Privileged Access**: Privileged access management is a cornerstone of cloud security, as it governs who can perform sensitive operations across Azure resources. Microsoft Entra ID (Azure AD) and Role-Based Access Control (RBAC) were employed to enforce least-privilege access, ensuring that users and service accounts only had permissions necessary for their roles. Privileged Identity Management (PIM) was leveraged to provide just-in-time (JIT) access, time-bound permissions for elevated roles, significantly reducing the risk of credential abuse and insider threats.

- **SIEM, SOAR, and Incident Response Capabilities**: Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and structured Incident Response capabilities form the operational backbone of modern cloud security operations. During the sprint, Microsoft Sentinel was deployed as the central SIEM platform, while Azure Logic Apps supported SOAR functions to automate and streamline response workflows. Microsoft Sentinel served as the cloud-native SIEM solution, enabling centralized collection, correlation, and analysis of security logs and telemetry across the Azure environment. To complement detection capabilities, SOAR functionality was implemented using Azure Logic Apps integrated with Microsoft Sentinel. SOAR automation reduced manual intervention in repetitive and time-sensitive tasks by enabling predefined responses to specific security triggers.

  The implementation of SIEM, SOAR, and incident response capabilities during the cloud security sprint demonstrated the importance of combining visibility, automation, and structured response processes in modern cloud environments. By leveraging Microsoft Sentinel and Azure Logic Apps, the sprint environment achieved centralized monitoring, automated threat mitigation, and enhanced operational resilience against cyber threats.

All resources were deployed in the **East US** region and implemented within dedicated resource groups(TEAM8) to ensure isolation, governance clarity, and cost control.

# 4.0 Azure Environment Setup & Subscription Configuration

## 4.1 Subscription and Access Model

- **Azure Pay-As-You-Go subscription**: An Azure Pay-As-You-Go (PAYG) subscription is a consumption-based billing model that allows organizations to pay only for the cloud resources they use, without long-term commitments or upfront licensing costs.

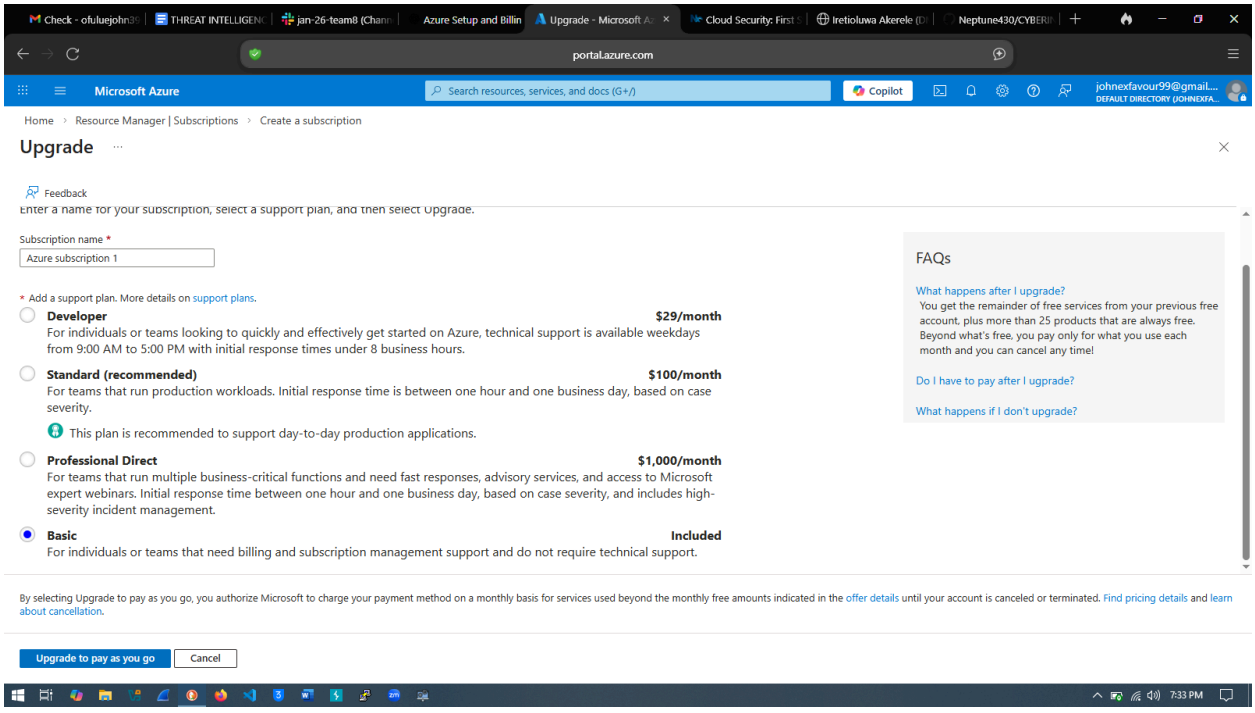


Fig. 1 .0: Azure subscription options

- **Contributor and Owner role access for assessment execution**: In Azure environments, Contributor and Owner roles are commonly assigned during assessment, lab, or security testing activities to ensure sufficient privileges for deploying, modifying, and validating cloud resources.

  The **Owner** role provides full management access to all resources within a subscription or resource group, including:

  - Creating, modifying, and deleting resources

- Assigning roles to other users (RBAC management)
- Managing access control policies

The **Contributor** role allows users to create and manage all types of Azure resources but **does not allow role assignment or access management**.

Permissions include:

- Deploying virtual machines
- Configuring networking components
- Creating storage accounts

However, Contributors cannot:

- Grant access to other users
- Change RBAC permissions

- **Dedicated Microsoft Entra ID tenant for identity management**: A dedicated Microsoft Entra ID tenant is like your own private space in the cloud for managing users and access. It keeps all accounts, roles, and security settings organized and separate from other environments, making it easier and safer to control who can access your Azure and Microsoft 365 resources.

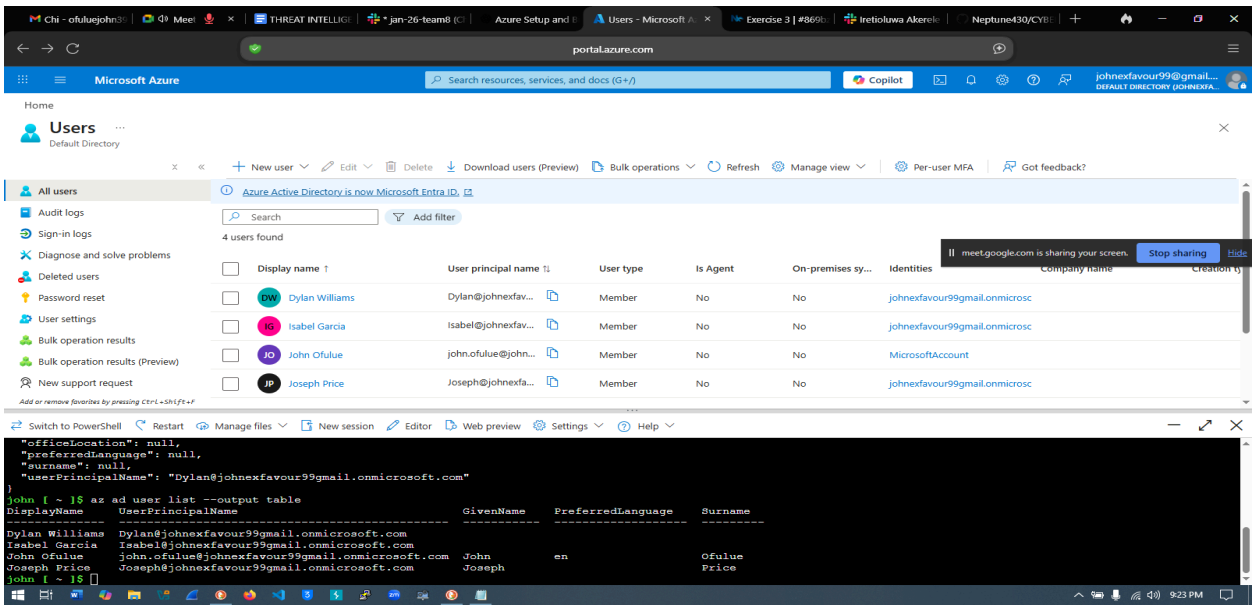


Fig1.1 users

## 4.2 Design Principles

- **Least privilege access & IAM enforcement**: In Azure, enforcing least privilege access means giving users and applications only the permissions they absolutely need to perform their tasks and nothing more. This principle reduces the risk of accidental or malicious misuse of resources.

  During this cloud security sprint, Identity and Access Management (IAM) policies were applied using Microsoft Entra ID and Azure Role-Based Access Control (RBAC). Each user, group, and service was assigned the minimal necessary roles to complete their activities. This approach strengthened security by limiting exposure and preventing unauthorized access to sensitive resources. By combining least privilege access with IAM enforcement, organizations can maintain tighter control over who can do what in the environment, improving both compliance and security posture.

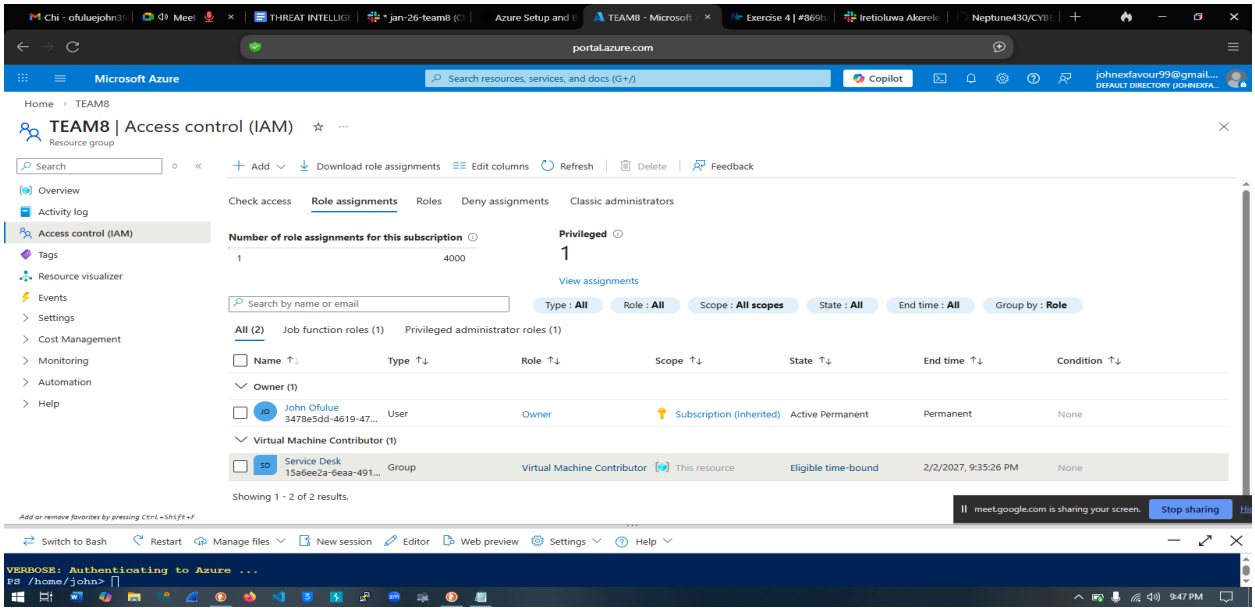


Fig1.2 IAM enforcement

- **Group-based RBAC**: Group-based RBAC in Azure allows administrators to assign roles to groups rather than individual users. This simplifies permission management, ensures consistency, and reduces administrative overhead. When a user is added to a group, they automatically inherit the group's permissions, and when removed, the permissions are revoked.

  Here, the team made use of group-based RBAC to manage access efficiently across resources. For example, specific groups were created for **junior admins,**

**senior admins and service desk**, each with tailored roles matching their responsibilities. This method ensured that access was aligned with job functions, supporting the principle of least privilege while maintaining streamlined administration.

- **Resource group segmentation**: Resource group segmentation is a critical organizational and security practice in Azure, where resources such as virtual machines, storage accounts, and networking components are grouped logically based on function, environment, or project. During the sprint, resource group segmentation was used to isolate workloads, manage access, and simplify monitoring and policy enforcement. By separating resources into distinct groups the team was able to apply access controls, enforce role-based permissions, and reduce the potential blast radius in case of a security incident. Each resource group could also have tailored policies, providing visibility and governance over cloud usage. This segmentation strategy enhances security posture by limiting exposure, improving compliance, and enabling more effective incident response, as any anomalies can be traced back to specific, well-defined resource boundaries.
- **Azure-native security tooling adoption**: Adopting Azure-native security tools is critical for ensuring a resilient, scalable, and well-governed cloud environment. These tools are purpose built to integrate seamlessly with Azure workloads, providing automated protection, visibility, and compliance monitoring. During the cloud security sprint, several Azure-native tools such as Microsoft defender for cloud, Azure AD, Azure monitor & log analytics were leveraged to strengthen security operations and reduce risk exposure.

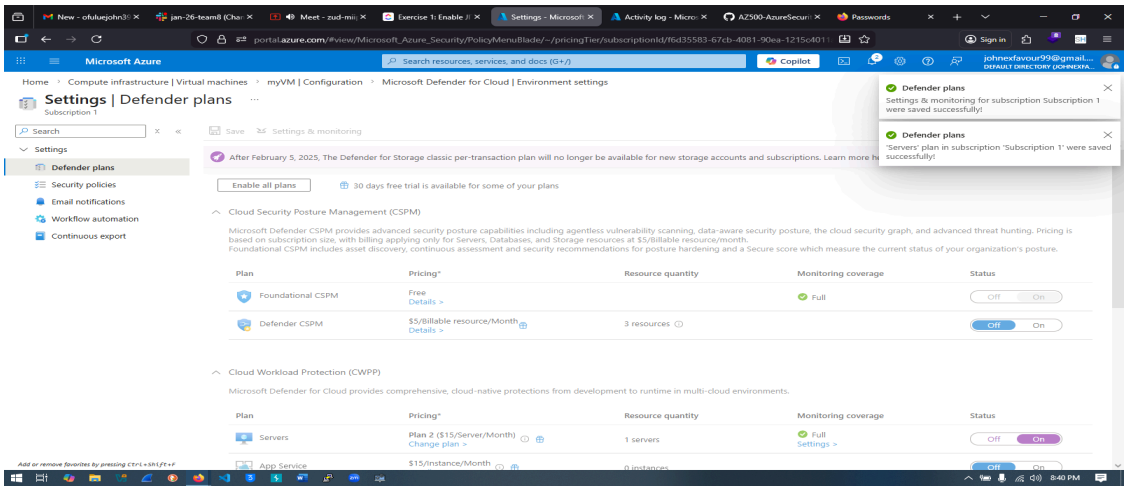


Fig1.3 Microsoft defender for cloud

# 5.0 Methodology & Tooling

## 5.1 Assessment Methodology

The assessment followed a structured, industry-aligned security evaluation methodology:

1. **Planning & Direction** – Defined scope based on organizational risk and cloud usage.
2. **Environment Review** – Evaluated secure-by-design and configured security states.
3. **Control Implementation & Validation** – Enabled and tested security controls.
4. **Threat Simulation & Observation** – Validated logging, detection, and alerting.
5. **Risk Analysis** – Mapped outcomes to business impact and maturity.
6. **Reporting** – Produced executive-focused findings and recommendations.

## 5.2 Tooling and Technologies

- **Microsoft Entra ID (Azure AD)**: In simple terms, Entra ID is where identities live in Azure. Whenever you create a user, assign roles, configure authentication policies, or enforce access controls, you are working within Entra ID.

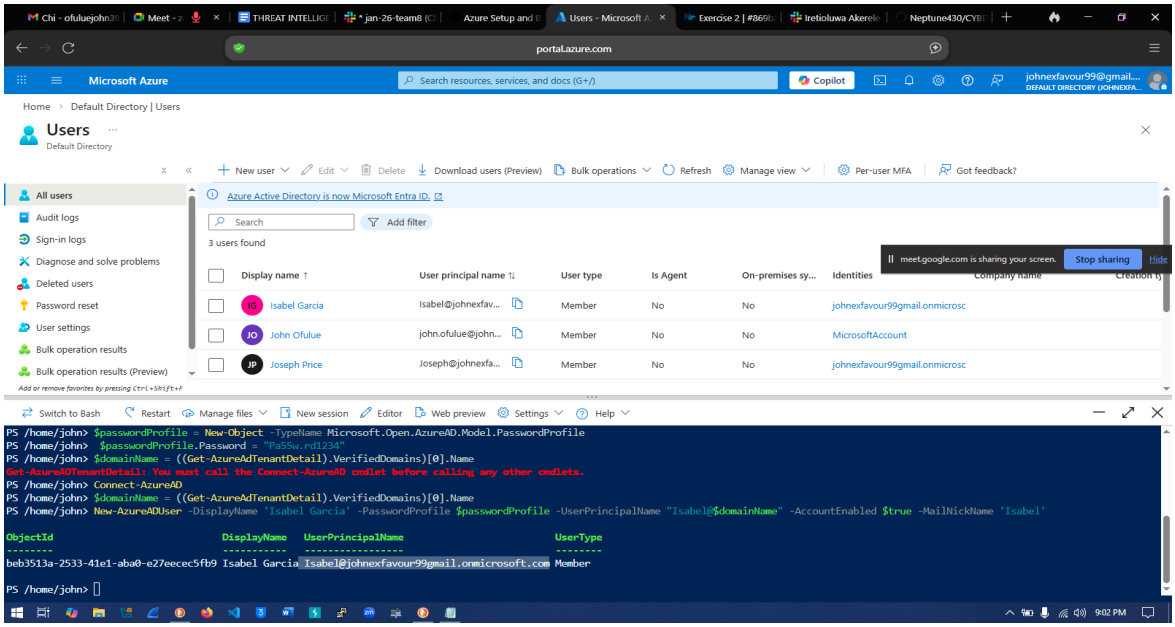


Fig 2.0 List of users in the entra id

- **Azure RBAC**: Azure Role-Based Access Control (RBAC) is Azure's authorization system used to manage who can access specific resources and what actions they can perform within an Azure environment. While Microsoft Entra ID manages identities (users, groups, and applications), Azure RBAC controls their permissions on Azure resources. It ensures that users are granted only the level of access necessary to perform their responsibilities. This supports the principle of least privilege, which is fundamental to cloud security.

  For example, instead of assigning Owner access to every team member, access can be restricted using group-based RBAC—granting Contributor access only to required resource groups.

  If Microsoft Entra ID defines **who you are**,

  Azure RBAC defines **what you are allowed to do**.

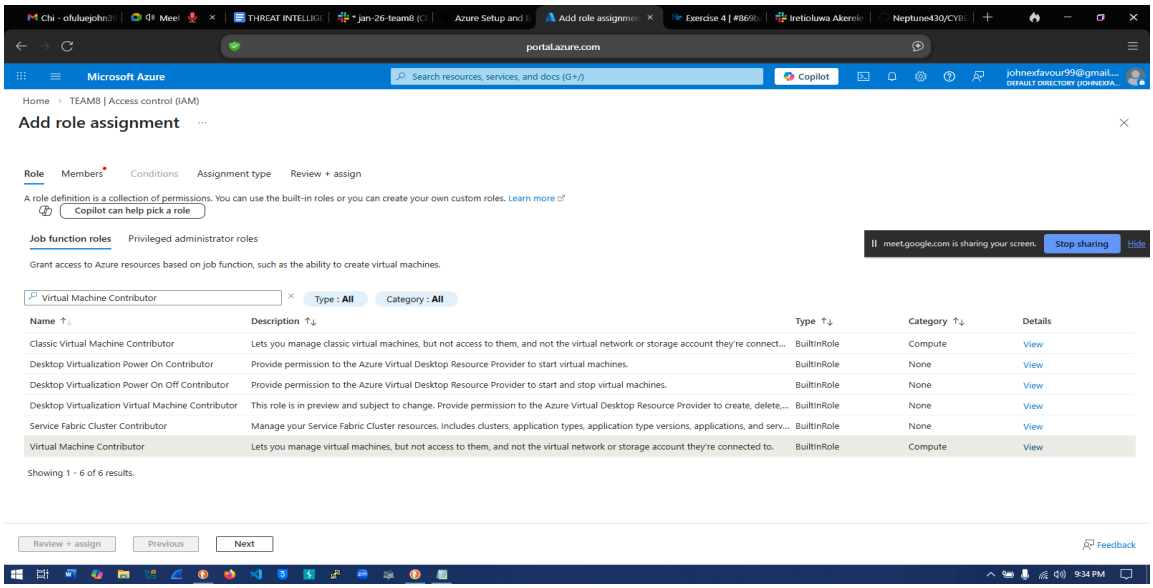


Fig2.1 Azure RBAC

- **Azure Monitor & Log Analytics**: **Azure Monitor** is Microsoft's centralized monitoring platform that collects, analyzes, and acts on telemetry data from Azure resources, on-premises systems, and hybrid environments. It provides visibility into performance, availability, and security events across the cloud environment.

  **Log Analytics** is a core component of Azure Monitor that stores and enables advanced querying of log data using the **Kusto Query Language (KQL)**. It

allows security and operations teams to investigate events, detect anomalies, and generate actionable insights from collected logs.

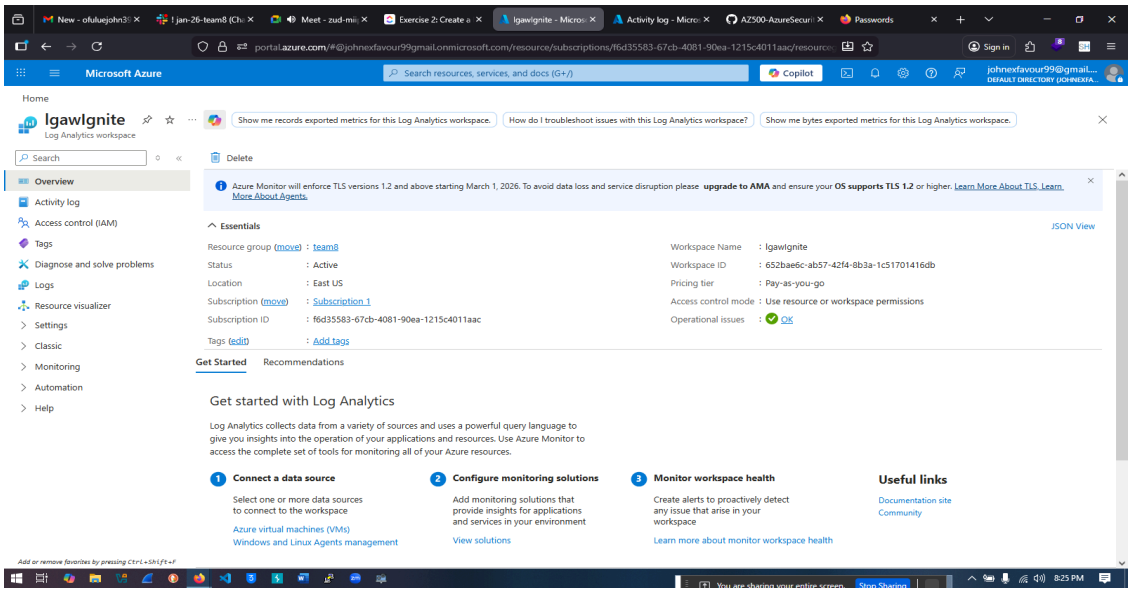


Fig2.2 Log analytics workspace

- **Data Collection Rules (DCRs):** in Azure define **what data is collected, from which resources, and where it is sent** within Azure Monitor. They provide detailed control over telemetry collection, ensuring that only relevant logs and metrics are ingested into Log Analytics workspaces or other destinations

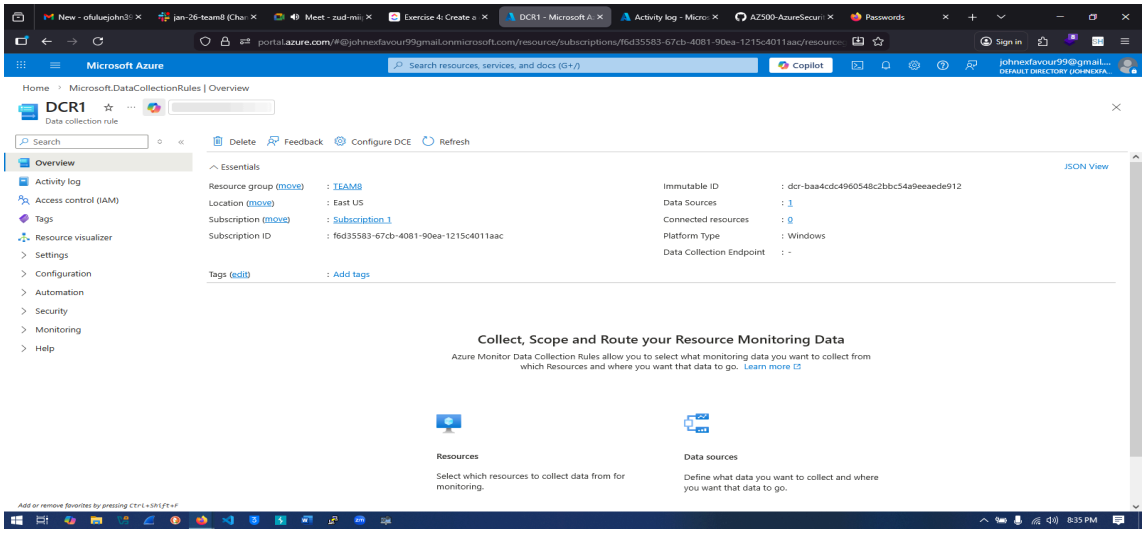


Fig2.3 Data Collection Rules(DCRs)

- **Microsoft Defender for Cloud (Servers Plan 2)**: Microsoft Defender for Cloud (Servers Plan 2) is an advanced security service that protects Azure and hybrid virtual machines. It goes beyond basic security checks by providing stronger threat detection, vulnerability scanning, and endpoint protection.

  While the basic tier of Defender for Cloud mainly offers security recommendations and visibility into misconfigurations, Servers Plan 2 adds advanced, behavior-based threat detection powered by Microsoft Defender for Endpoint. This means it can actively detect and respond to real attacks, not just identify security gaps.

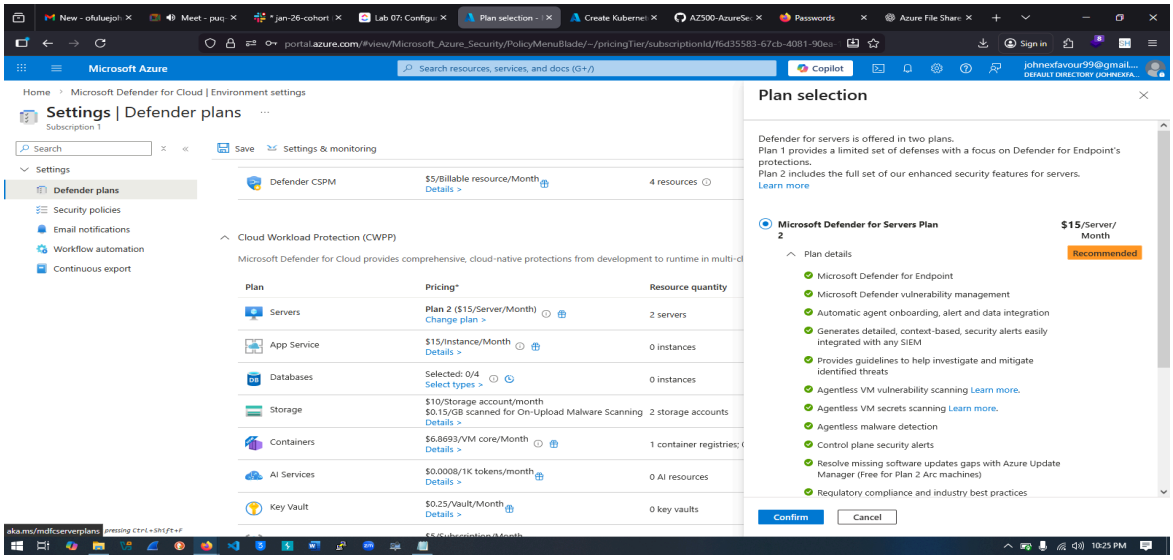


Fig 2.4 Microsoft Defender for Cloud (Servers Plan 2)

- **Just-in-Time (JIT) VM Access**: Just-in-Time (JIT) VM Access is a security feature in Microsoft Defender for Cloud that helps protect virtual machines by limiting exposure of management ports such as RDP (3389) and SSH (22).

  Instead of leaving these ports permanently open to the internet, which increases the risk of brute-force attacks and unauthorized access, JIT keeps them **closed by default**. Access is only granted when an authorized user requests it, and only for a specific period of time.

  Management ports are blocked at the network level using Network Security Groups (NSGs). When administrative access is required, an authorized user submits an access request.
  If approved, access is granted only:

1. For a specific IP address

2. For a defined duration (e.g., 1–3 hours)

   Once the time window expires, the port is automatically closed again.

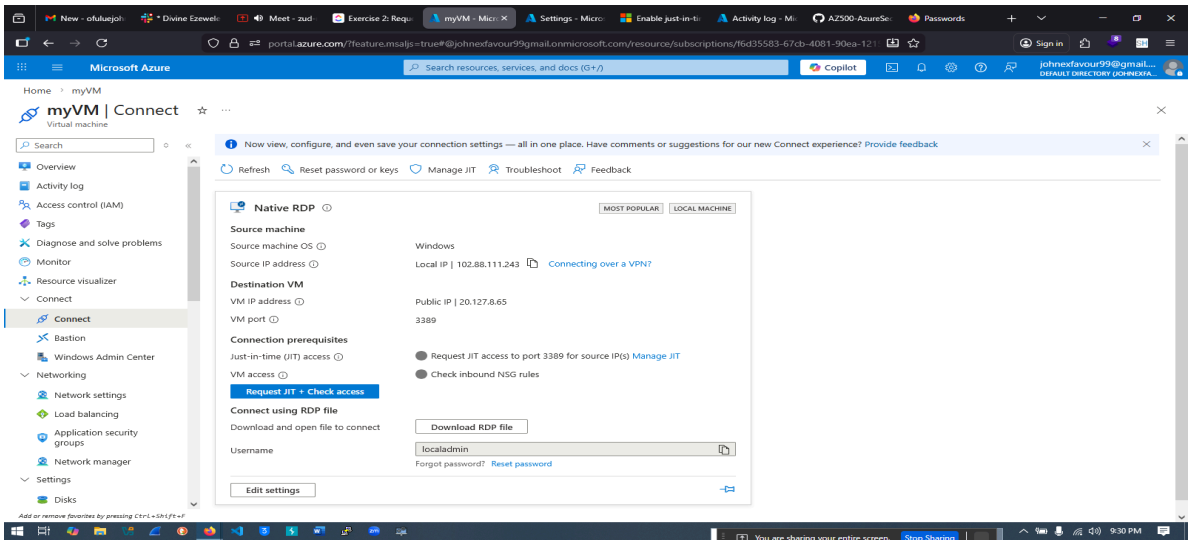


Fig2.5 Request for JIT access

- **Azure Logic Apps**: Azure Logic Apps is a cloud-based automation service that enables users to build and run automated workflows that integrate applications, services, and data across cloud and on-premises environments. It is designed to simplify process automation without requiring extensive coding.

  During the sprint, Logic Apps were leveraged to:

  - Automate repetitive incident response actions, saving time for the security team.
  - Enforce security policies consistently across Azure resources.
  - Test and deploy playbooks for real-world attack simulations, ensuring rapid mitigation when incidents occur.

- **Microsoft Sentinel (SIEM & SOAR)**: Microsoft Sentinel is a cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platform designed to provide comprehensive threat detection, investigation, and response across cloud and on-premises environments. It centralizes security data, enabling organizations to gain

real-time visibility into their infrastructure and detect suspicious activities before they escalate.

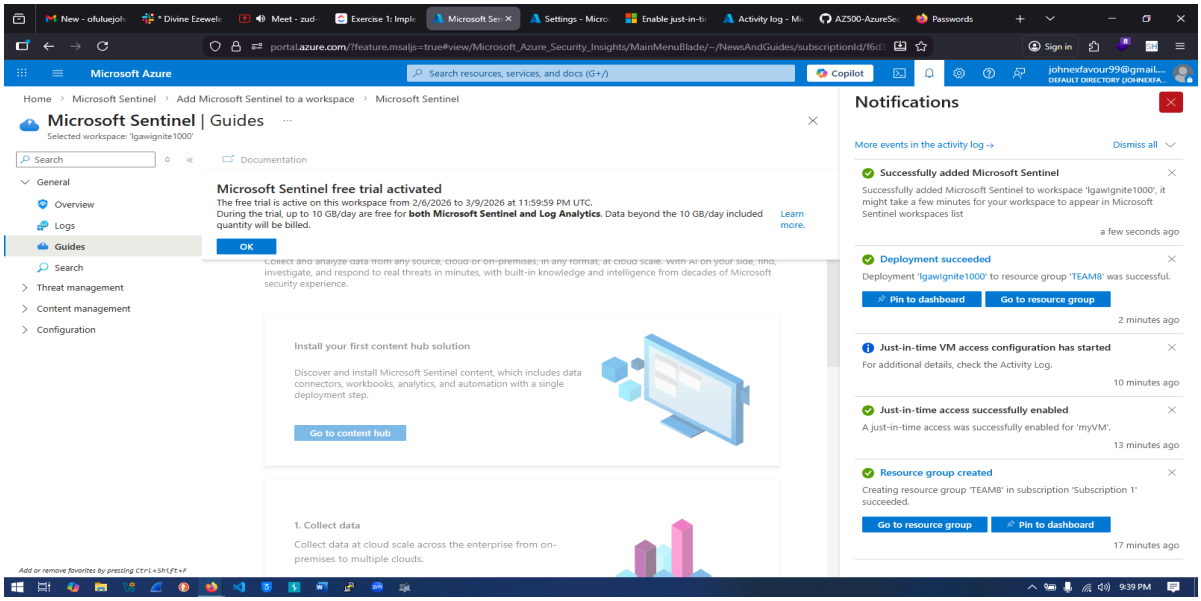


Fig2.6 Microsoft sentinel

# 6.0 Lab 01: Role-Based Access Control

This chapter demonstrates the implementation of Azure Role-Based Access Control (RBAC) through the creation of users and groups to manage permissions effectively. Three Azure Active Directory groups were created: Senior Admins, Junior Admins, and Service Desk, each containing their respective user accounts. RBAC was used to assign the Virtual Machine Contributor role to the Service Desk group, allowing delegated management of virtual machines while maintaining controlled and least-privilege access across the environment.

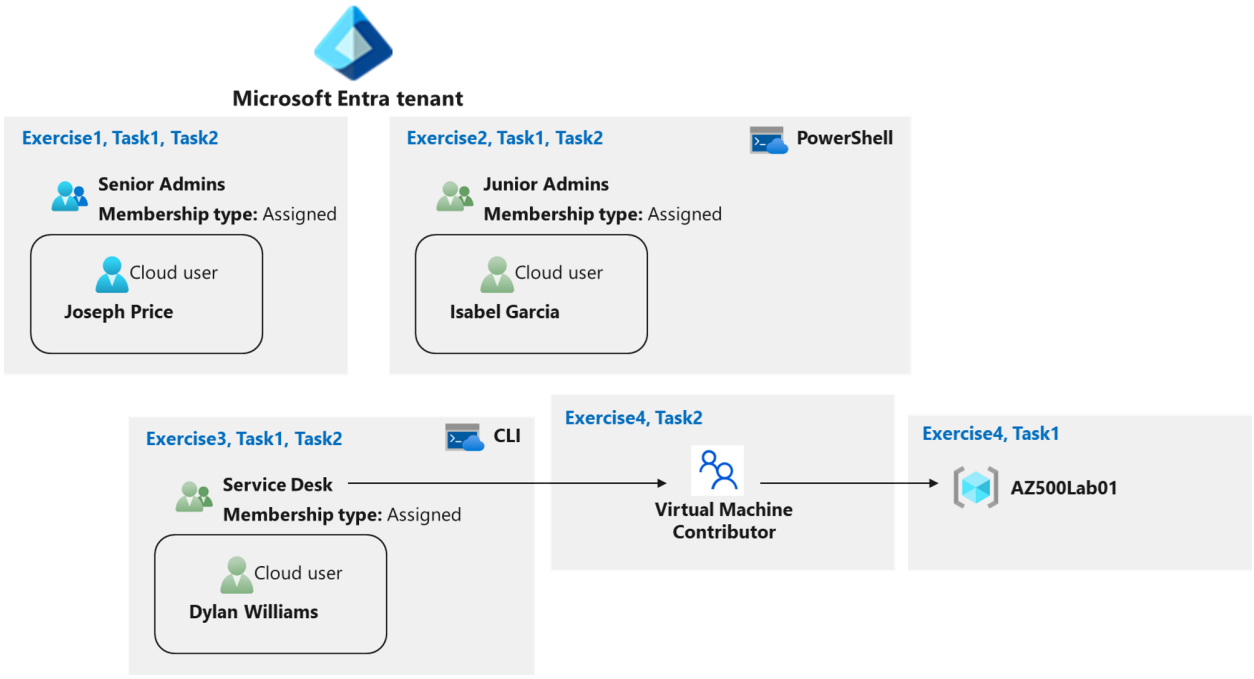


Plate 1.0 Role-Based Access Control architecture diagram

## 6.1. Exercise 1: Create the Senior Admins group with the user account Joseph Price as its member (the Azure portal).

- Task 1: Use the Azure portal to create a user account for Joseph Price.

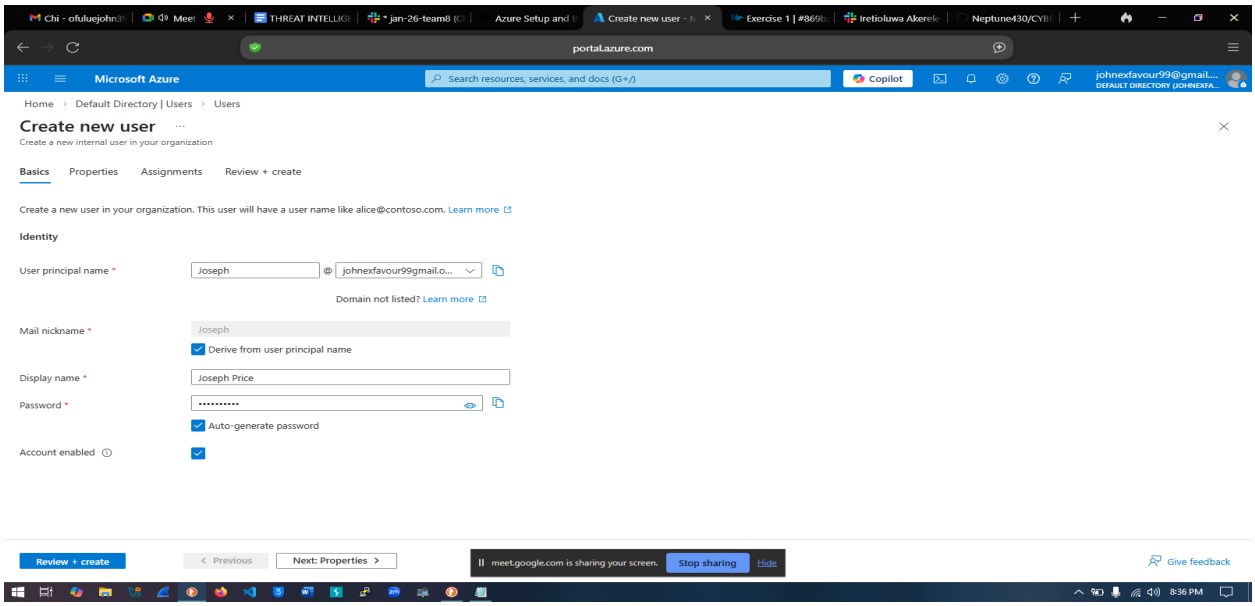


Fig3.0 User Joseph Price being created

- Task 2: Use the Azure portal to create a Senior Admins group and add the user account of Joseph Price to the group.

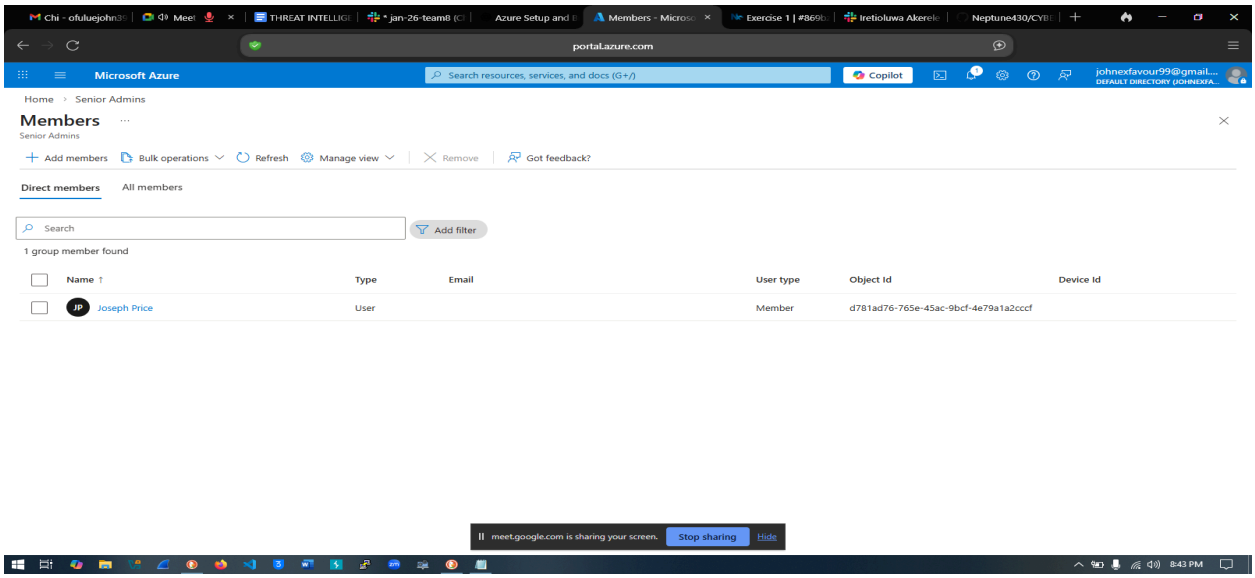


Fig3.1 Joseph Price in the created Senior Admins group

## 6.2. Exercise 2: Create the Junior Admins group with the user account Isabel Garcia as its member (PowerShell).

- Task 1: Use PowerShell to create a user account for Isabel Garcia.

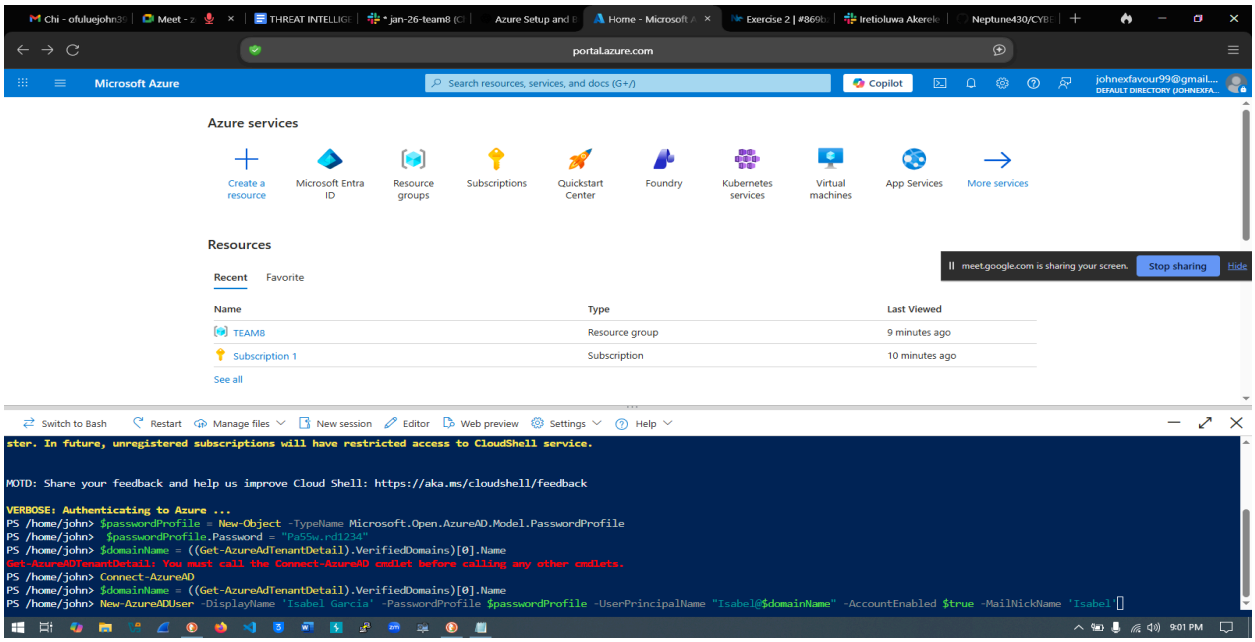


Fig 3.2 Powershell session creating the user Isabel Garcia

- Task 2: Use PowerShell to create the Junior Admins group and add the user account of Isabel Garcia to the group.

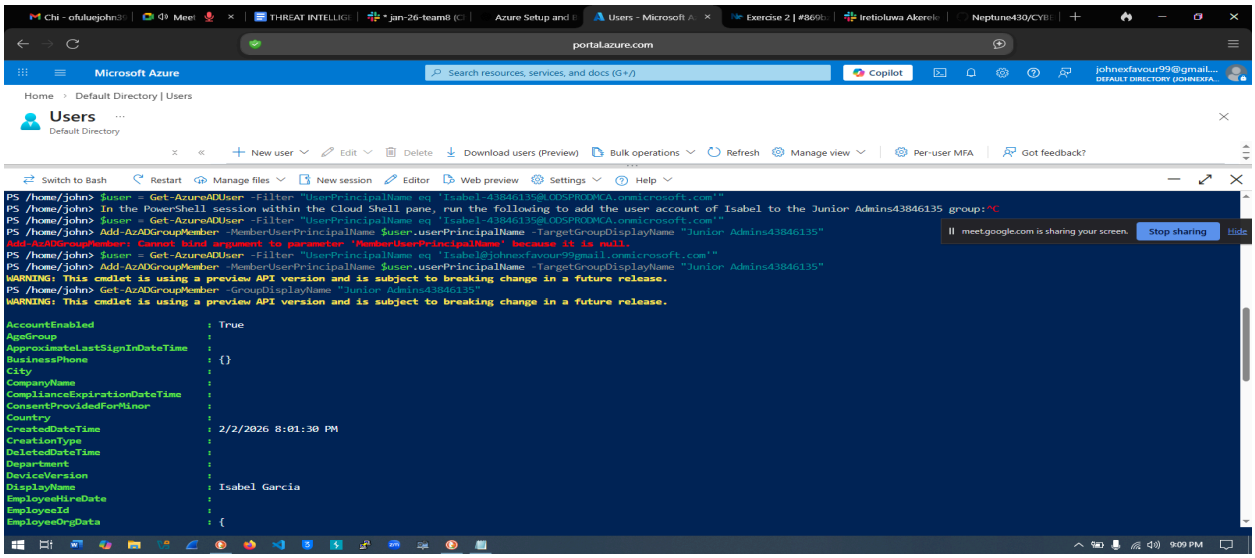


Fig. 3.3 Junior admin group being created, and Isabel Garcia added

## 6.3. Exercise 3: Create the Service Desk group with the user Dylan Williams as its member (Azure CLI).

- Task 1: Use Azure CLI to create a user account for Dylan Williams.

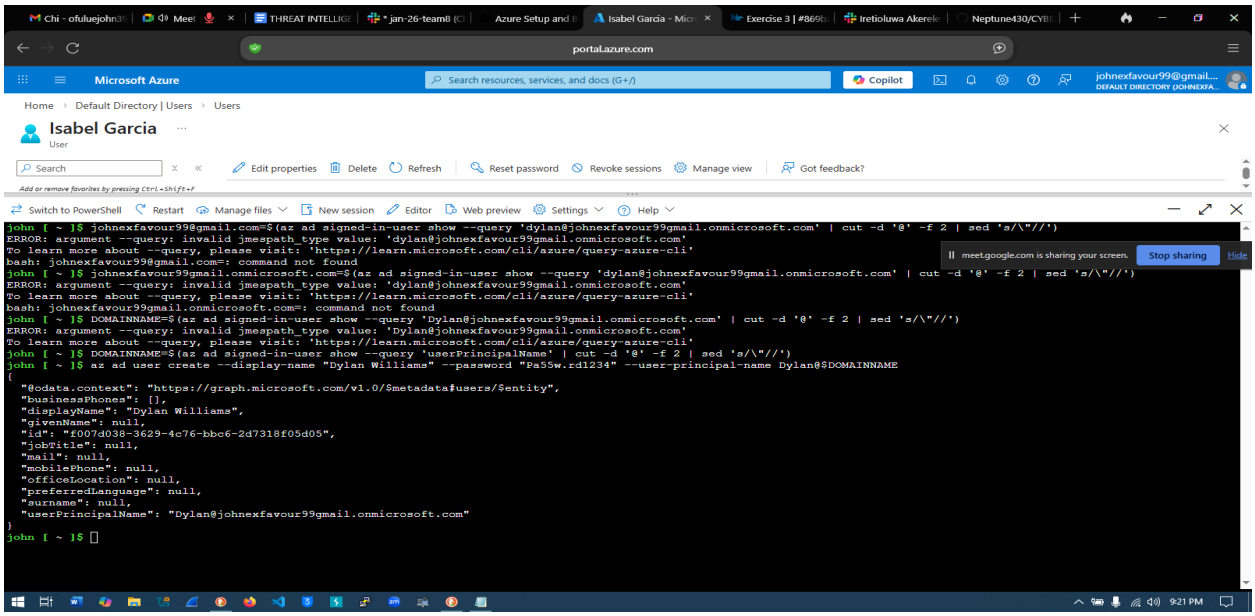


Fig 3.4 Dylan williams user account created using the Azure CLI

- Task 2: Use Azure CLI to create the Service Desk group and add the user account of Dylan to the group.

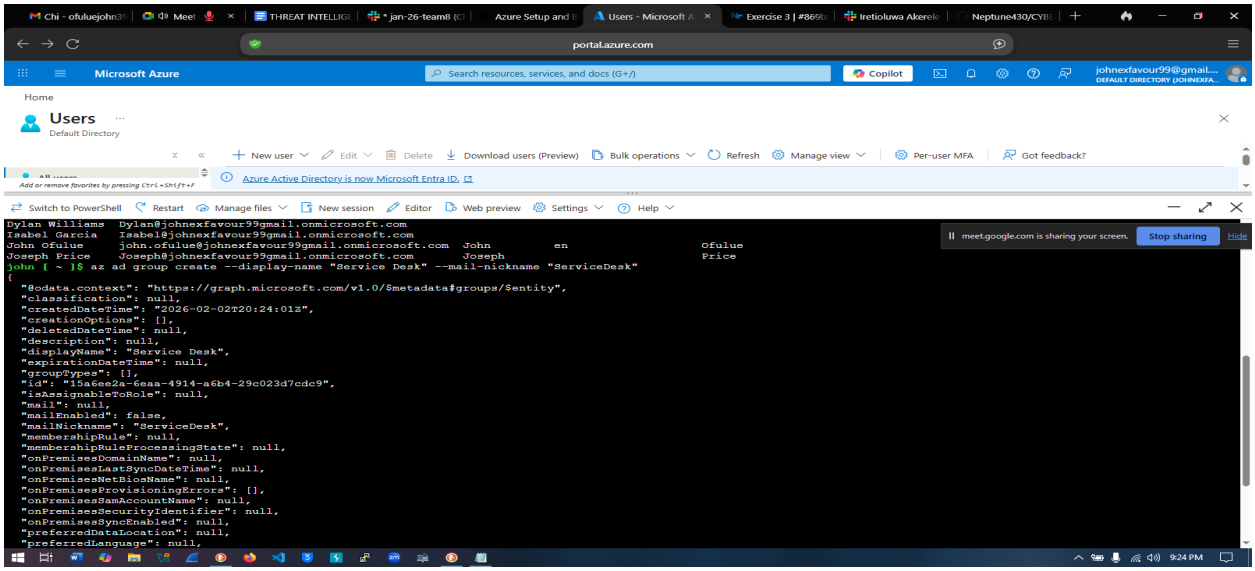


Fig3.5 Dylan Williams added to the new service desk group

## 6.4. Exercise 4: Assign the Virtual Machine Contributor role to the Service Desk group.

- Task 1: Create a resource group.

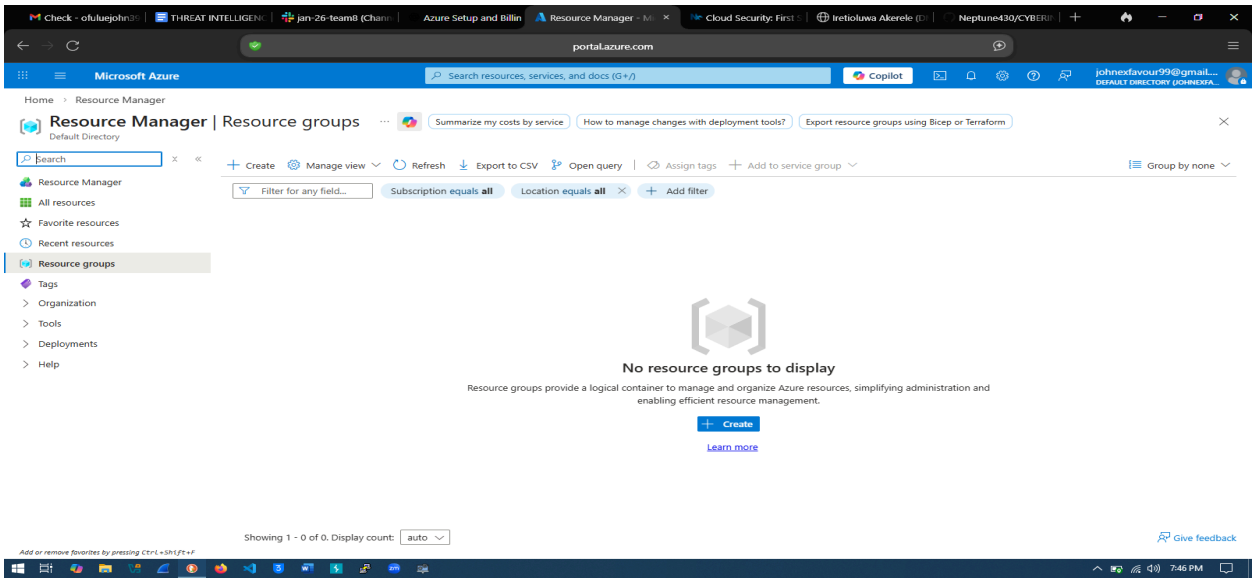


Fig3.6 Created resource group

- Task 2: Assign the Service Desk Virtual Machine Contributor permissions to the resource group.

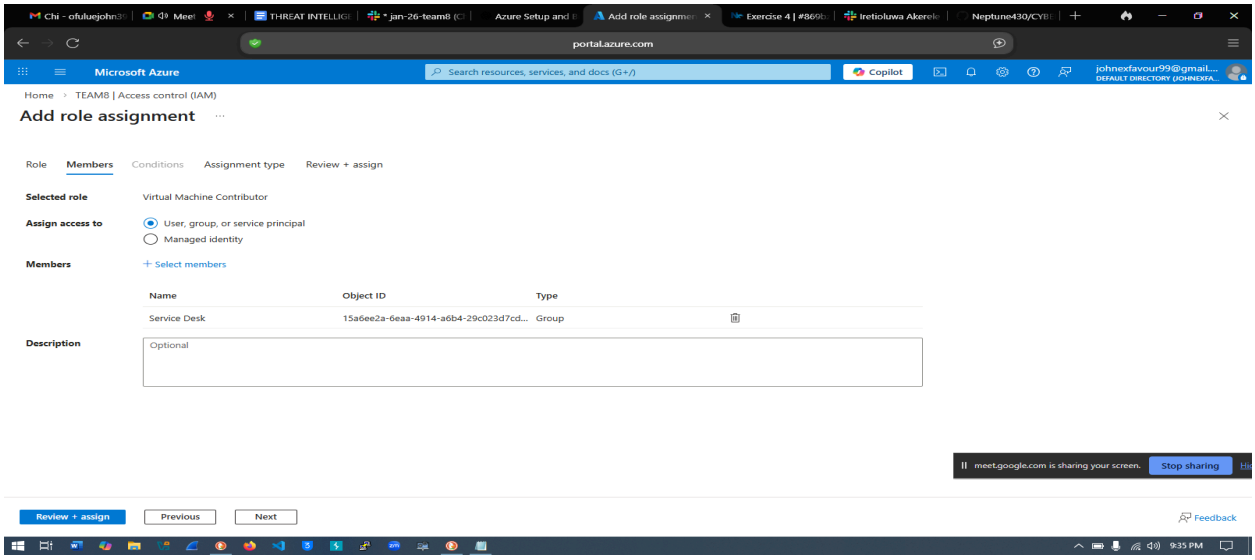


Fig 3.7 Assigning the Service Desk VM contributor to the resource group

# 7.0. Lab 02: Network Security Groups and Application Security Groups

This chapter focuses on implementing network security using Network Security Groups (NSGs) and Application Security Groups (ASGs) within an Azure virtual network. Two server groups were created: Web Servers and Management Servers, with each group placed in its own Application Security Group. Network security group rules were configured to allow Remote Desktop Protocol (RDP) access to the Management Servers while restricting RDP access to the Web Servers. Additionally, inbound rules were implemented to allow internet access to the Web Servers, enabling them to display the IIS web page, thereby validating proper network segmentation and access control.

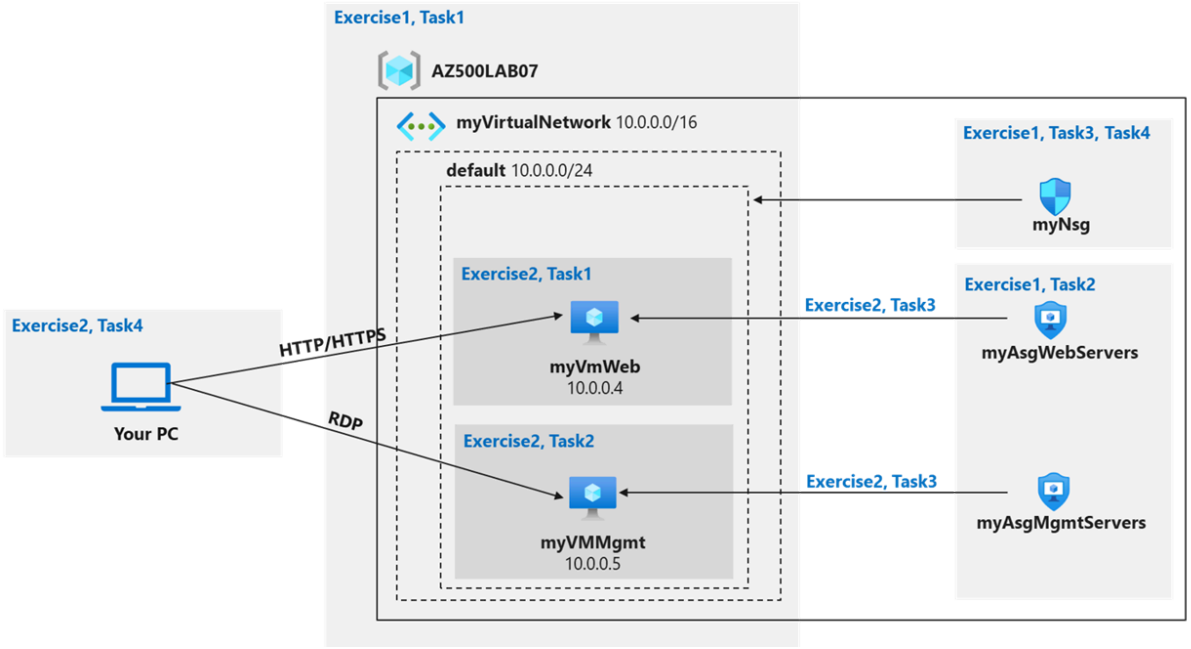


Plate 2.0 Network and Application Security Groups diagram

# 7.1 Exercise 1: Create the virtual networking infrastructure

- Task 1: Create a virtual network with one subnet.

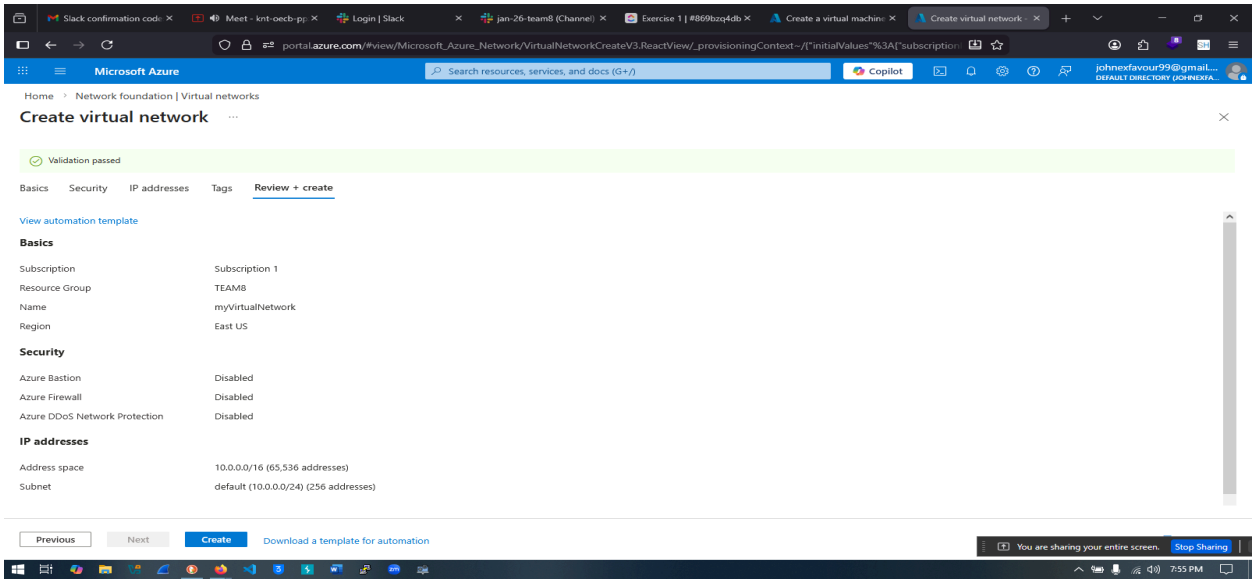


Fig4.0 Creation of a virtual network with one subnet

- Task 2: Create two application security groups.

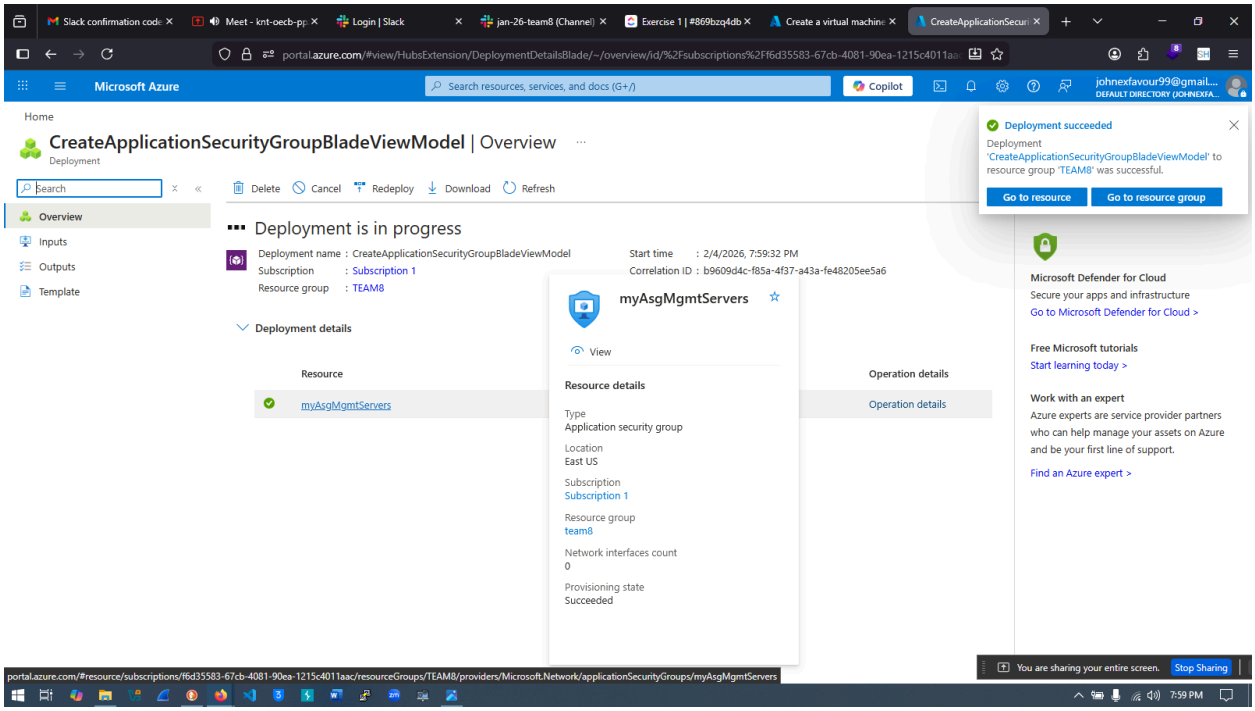


Fig4.1 AppSec Groups being created

- Task 3: Create a network security group and associate it with the virtual network subnet.

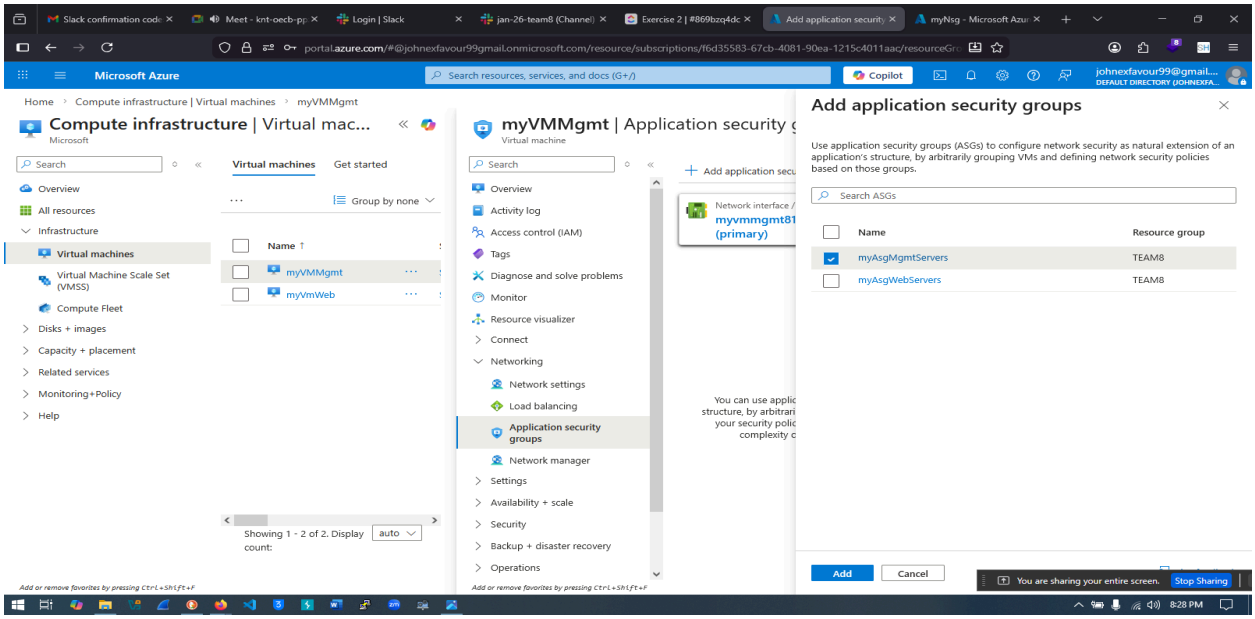


Fig 4.2 network security group and associated with the virtual network subnet.

- Task 4: Create inbound NSG security rules to all traffic to web servers and RDP to the management servers.

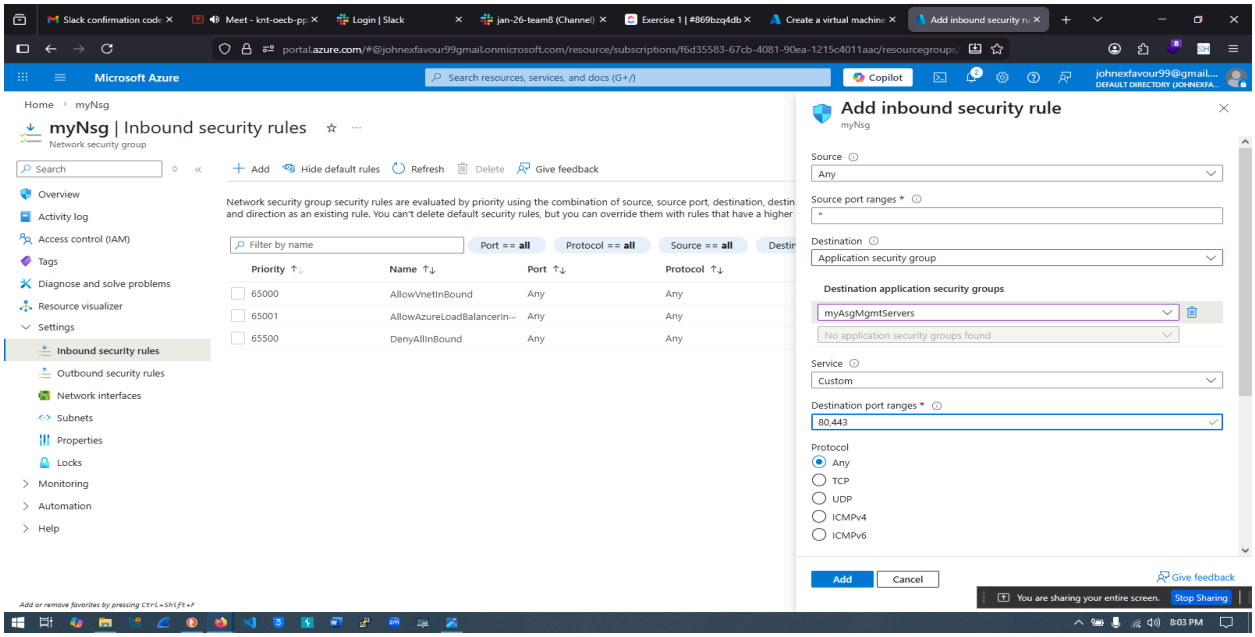


Fig4.3 Inbound NSG security rules been configured

## 7.2 Exercise 2: Deploy virtual machines and test the network filters

- Task 1: Create a virtual machine to use as a web server.

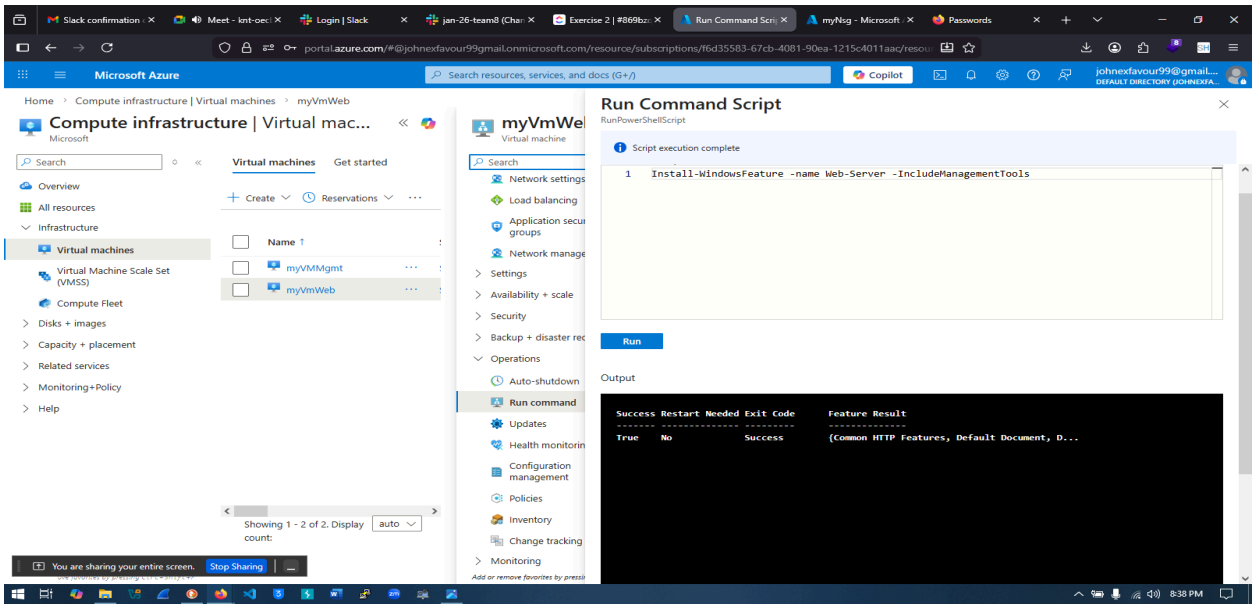


Fig4.4 virtual machine to use as a web server

- Task 2: Create a virtual machine to use as a management server.

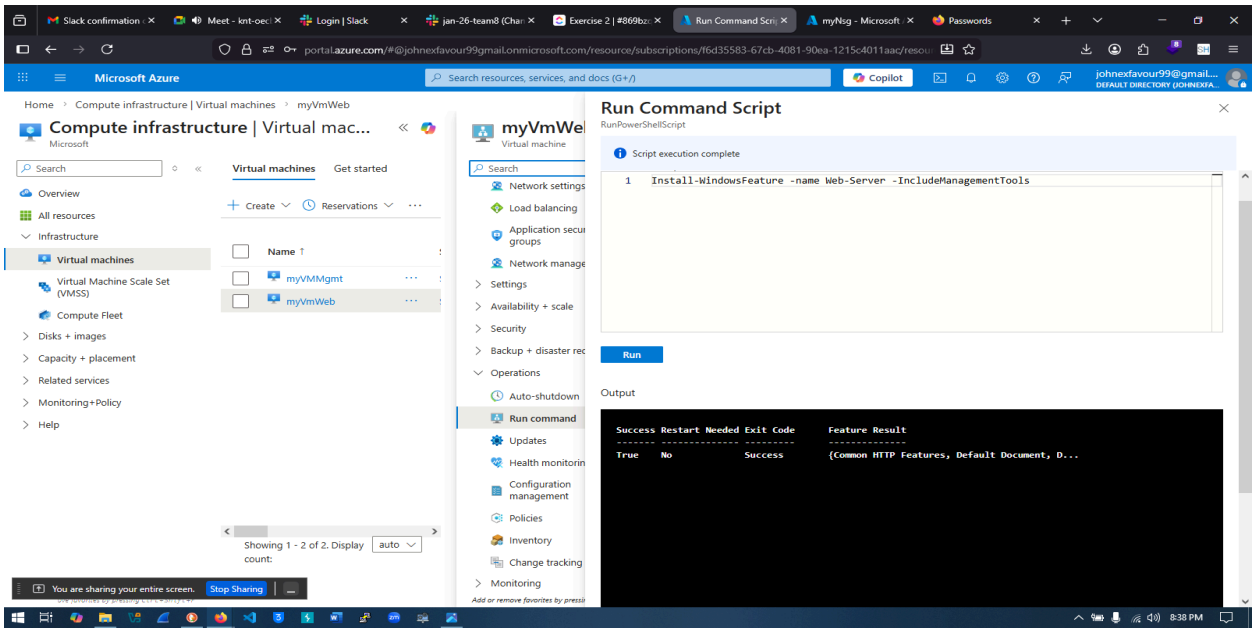


Fig 4.5 virtual machine to use as a management server

- Task 3: Associate each virtual machine's network interface with its application security group.

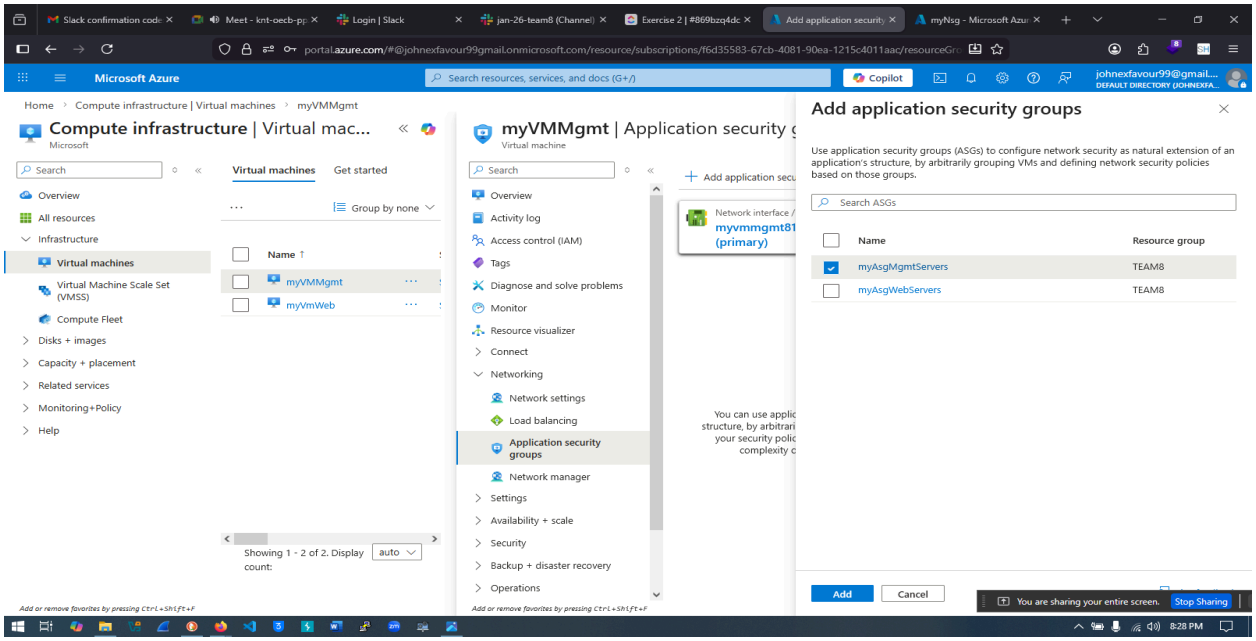


Fig 4.6 virtual machine's network interface associated with its application security group.

- Task 4: Test the network traffic filtering.

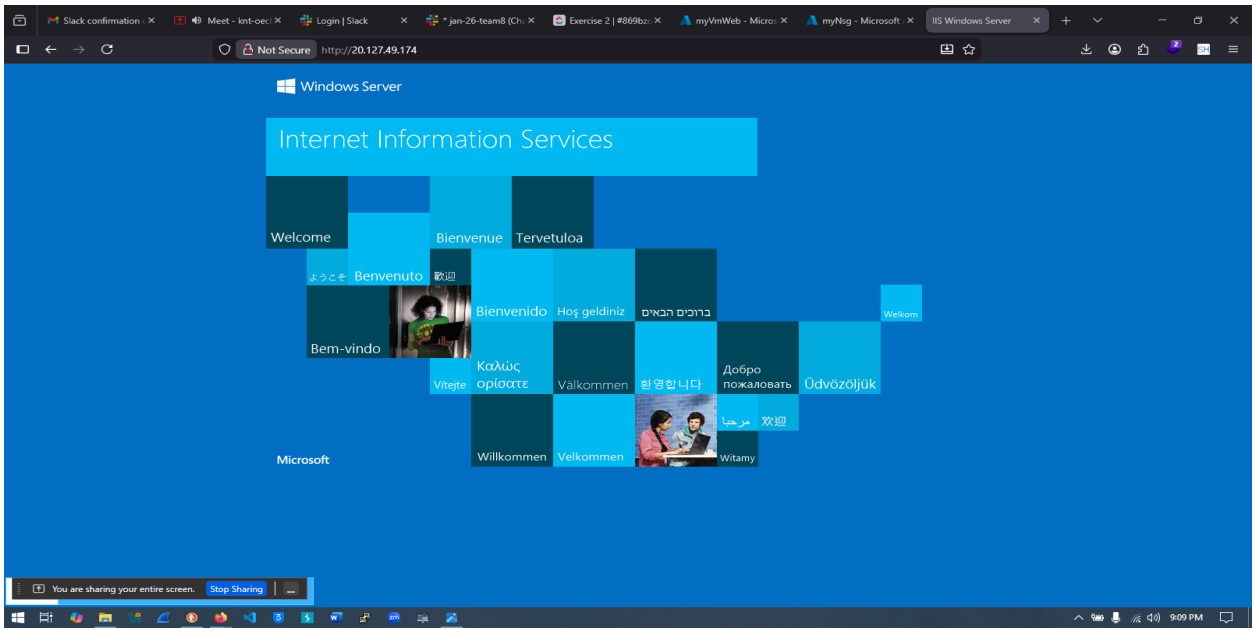


Fig 4.7 The default IIS welcome page

# 8.0 Lab 03: Azure Firewall

This chapter covers the deployment and configuration of Azure Firewall to control inbound and outbound network traffic as part of an overall network security strategy. A virtual network was created with separate workload and jump host subnets, each containing a virtual machine. A custom route was configured to ensure all outbound traffic from the workload subnet was forced through the Azure Firewall. Firewall application rules were implemented to restrict outbound web access to only www.bing.com while network rules were configured to allow external DNS queries, validating controlled and secure network communication.

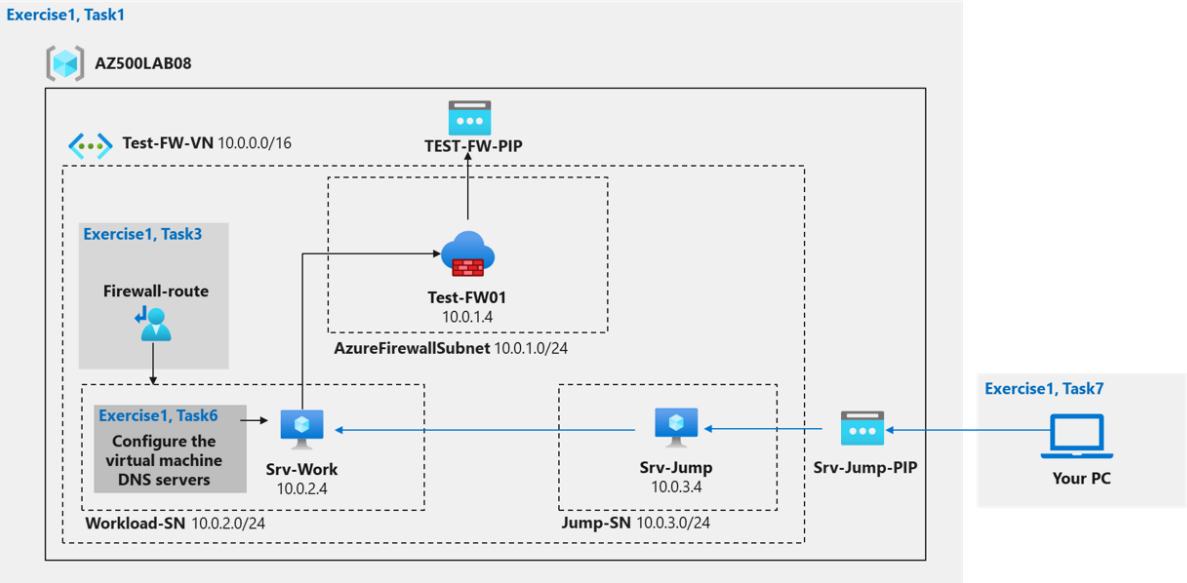


Plate 3.0 Azure Firewall diagram

# Exercise 1: Deploy and test an Azure Firewall

- Task 1: Use a template to deploy the lab environment.

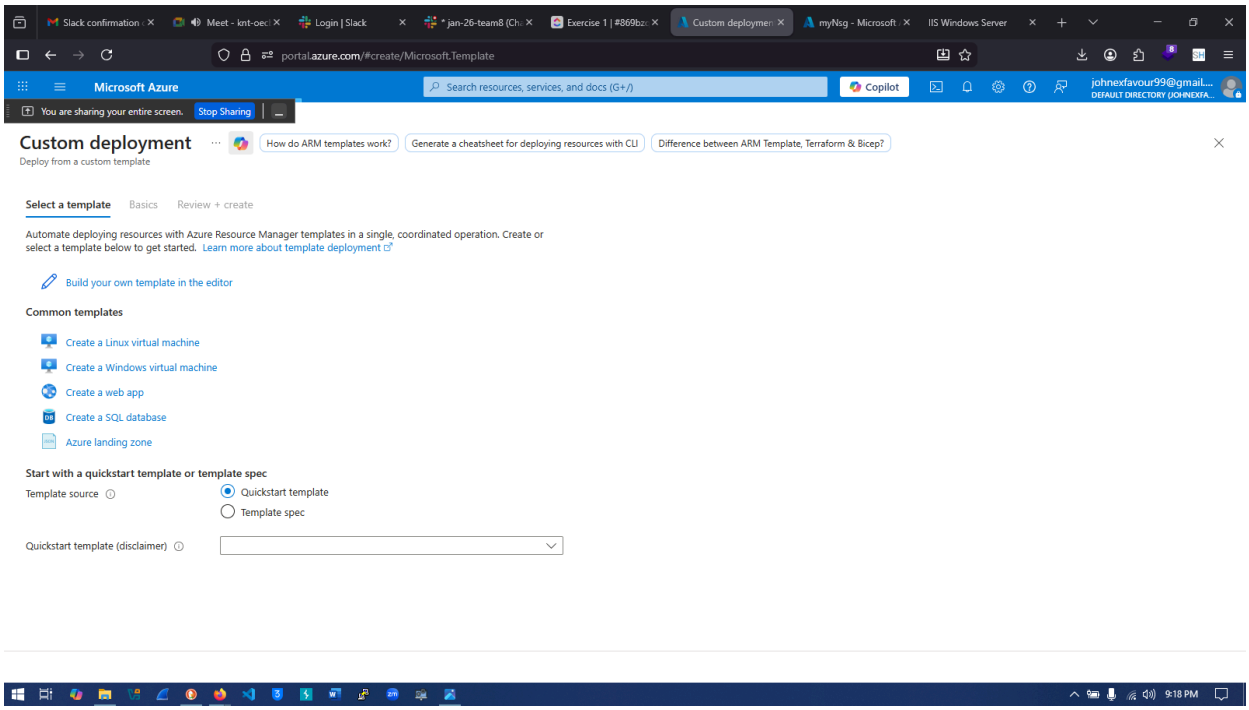


Fig 5.0 Lab environment deployment I

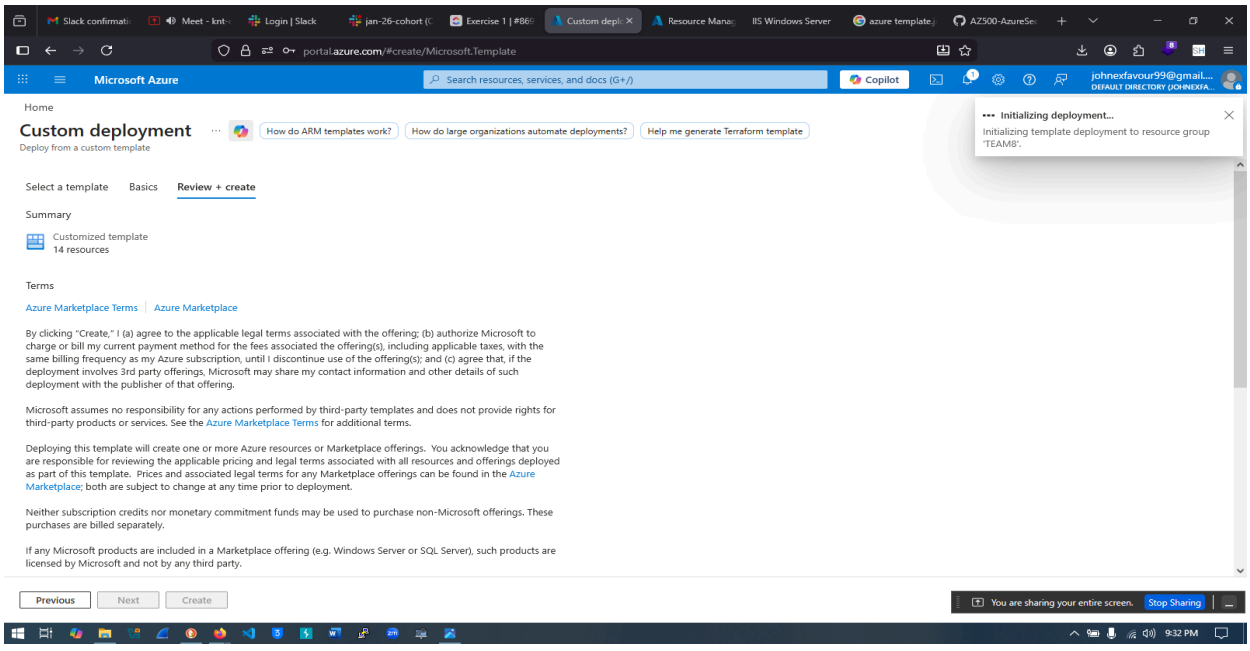


Fig 5.1 Lab environment deployment II

- Task 2: Deploy an Azure firewall.

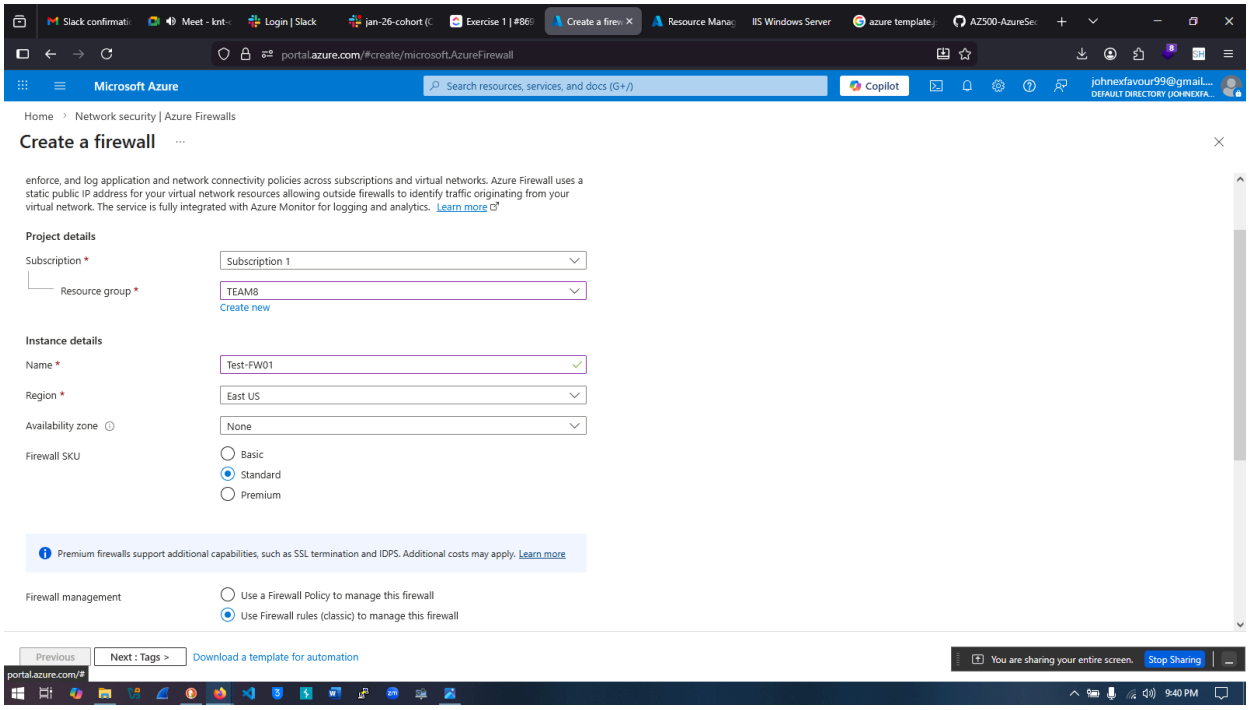


Fig 5.2 Azure Firewall creation

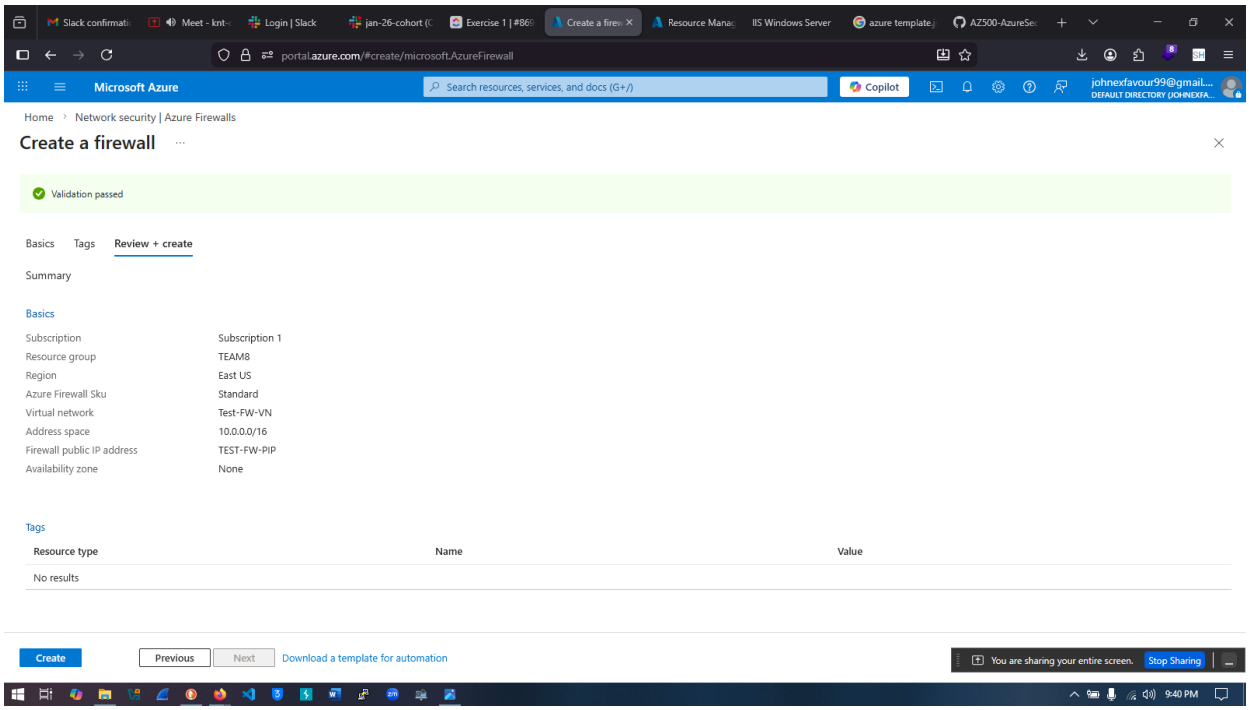


Fig 5.3 Azure Firewall deployment

- Task 3: Create a default route.

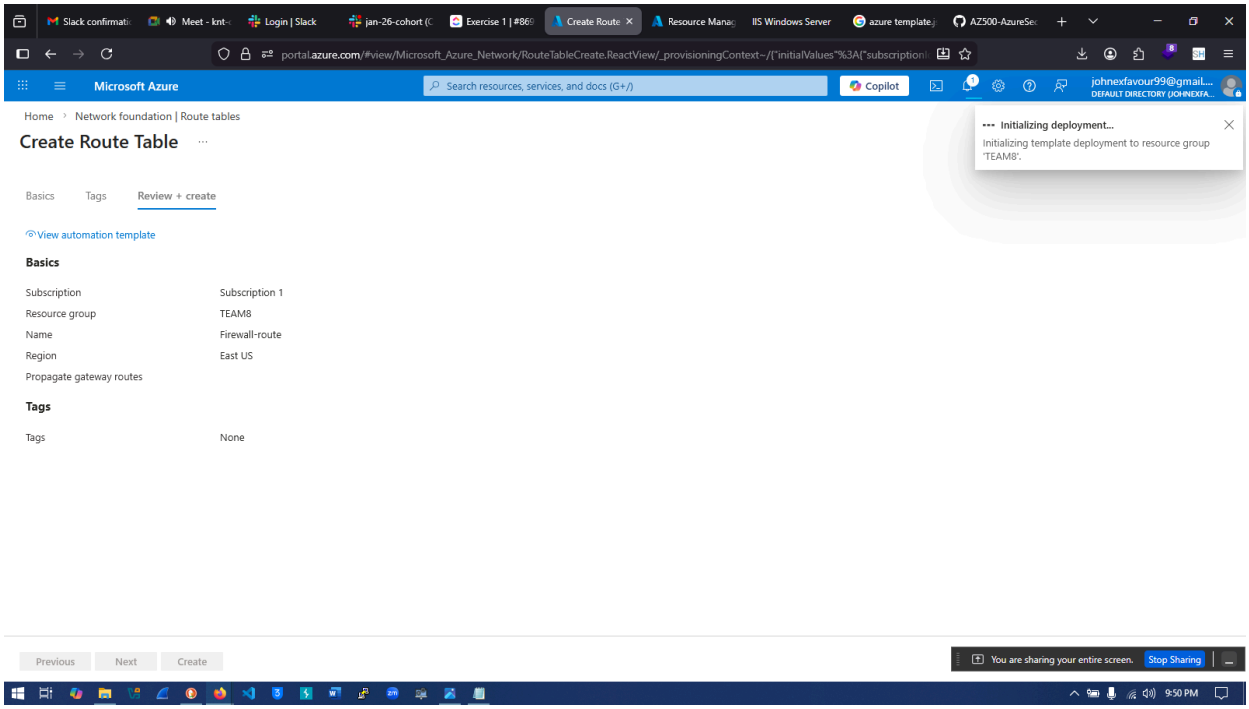


Fig 5.4 Creating a default route

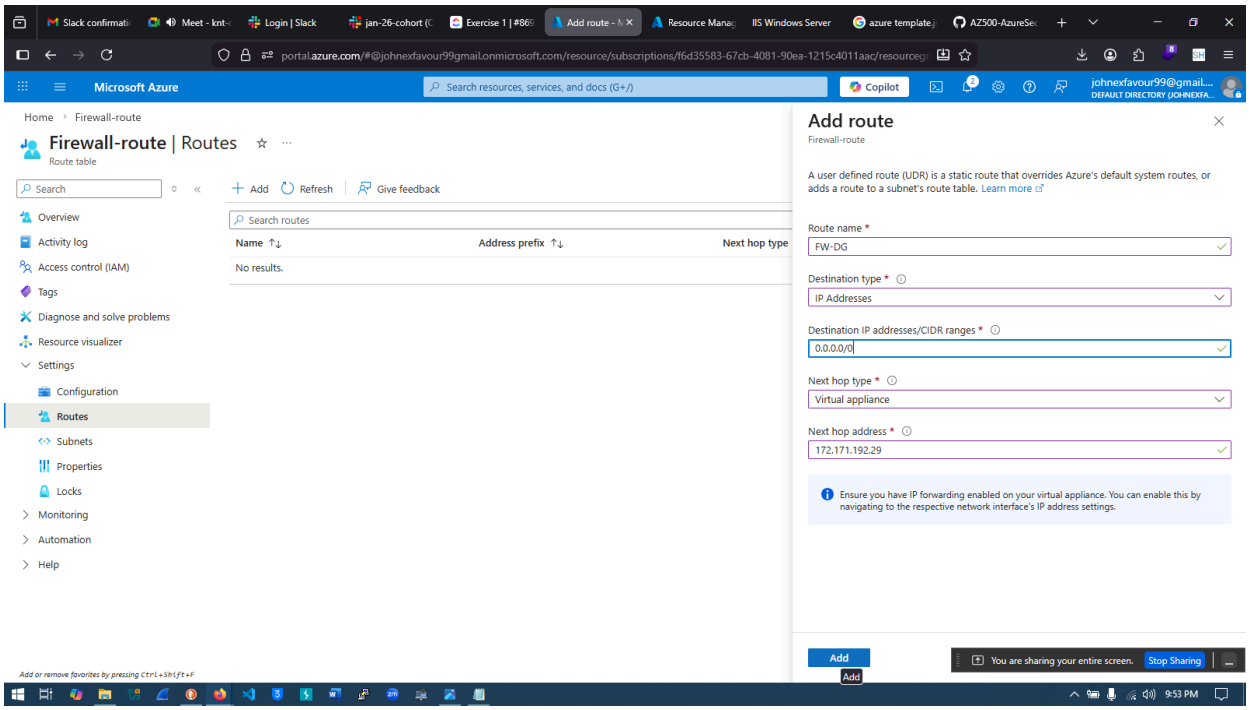


Fig 5.5 Adding a route

- Task 4: Configure an application rule.

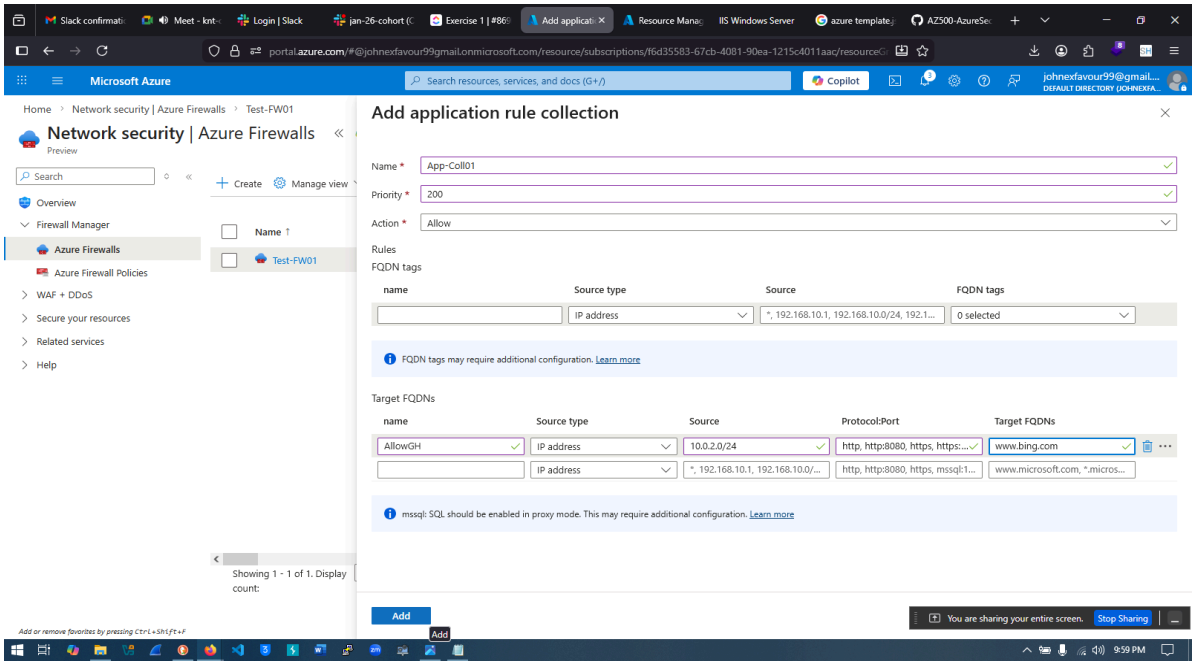


Fig 5.6 Application rule creation

- Task 5: Configure a network rule.

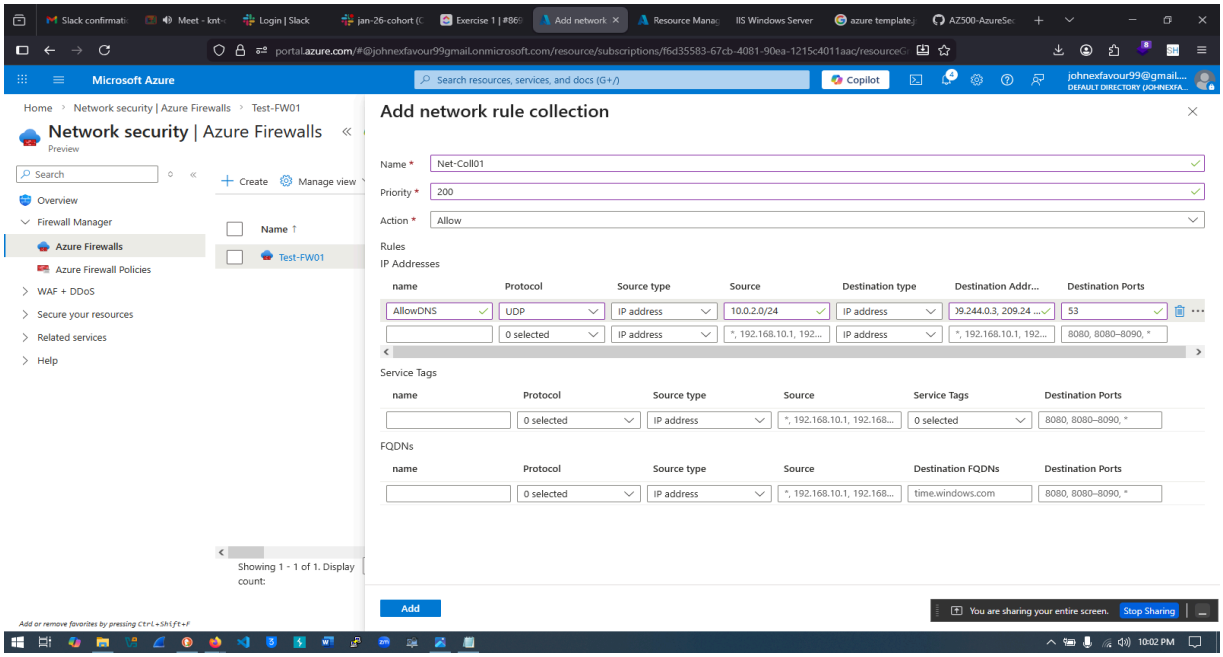


Fig 5.7 Configuring a network rule

- Task 6: Configure DNS servers.

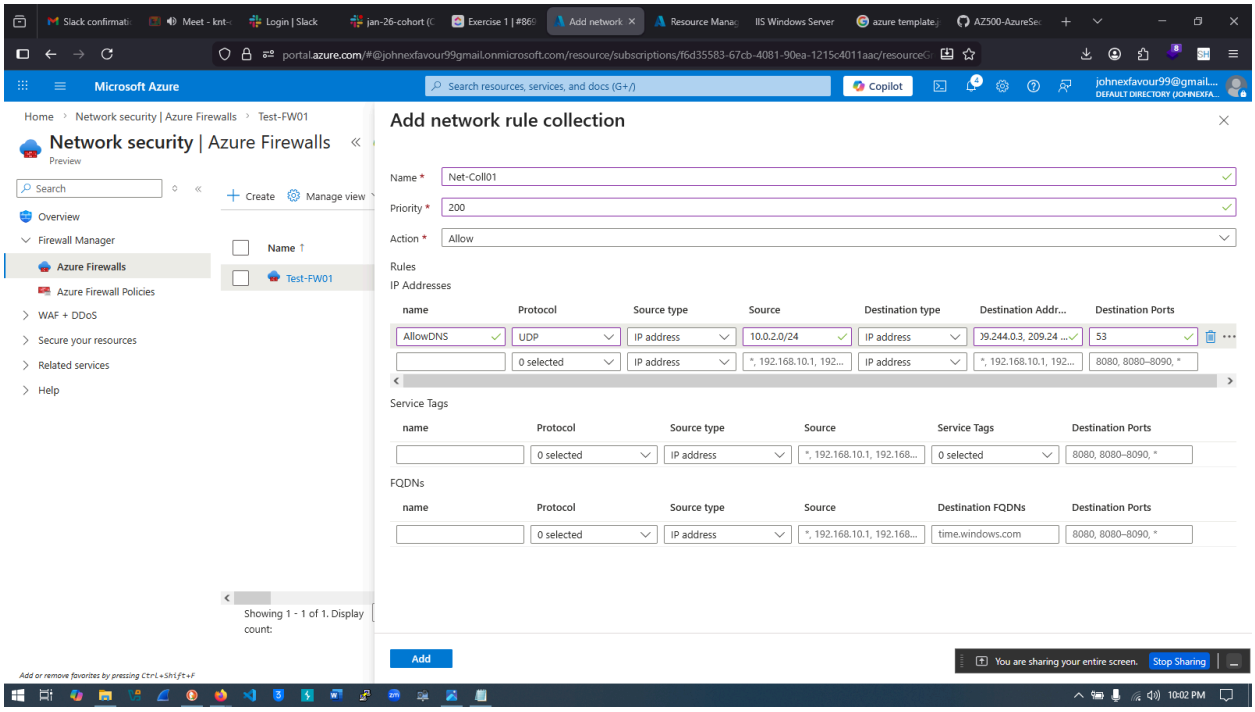


Fig 5.8 Configuring DNS servers on the network rule

- Task 7: Test the firewall.

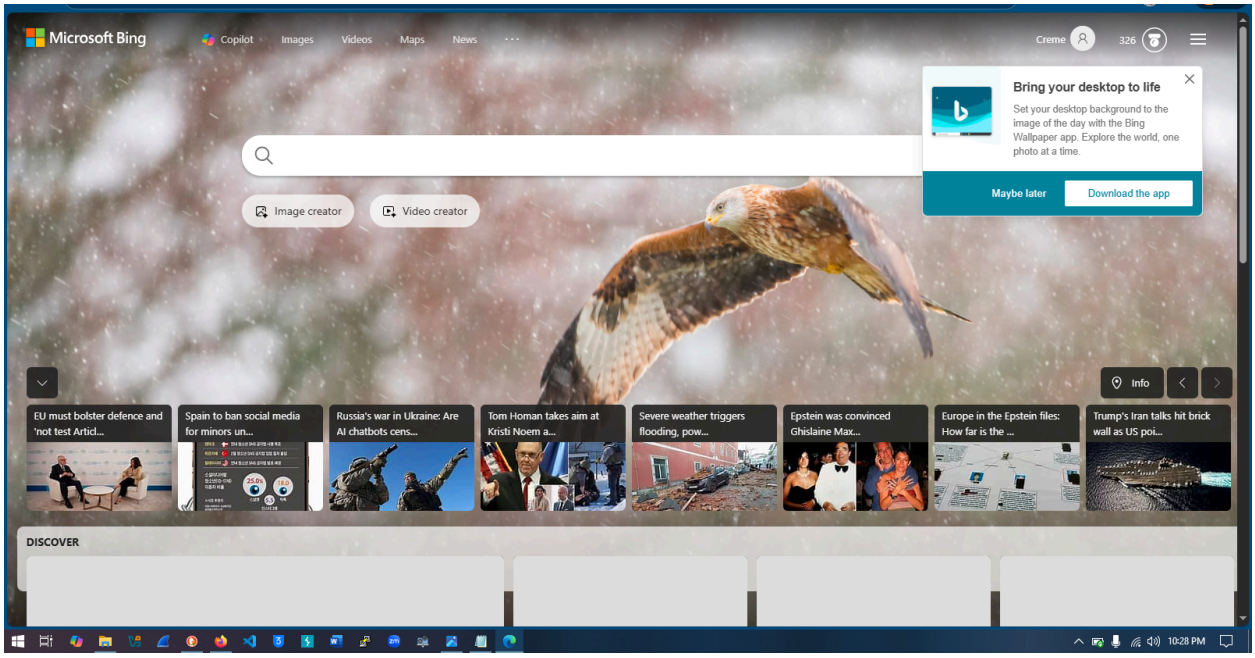


Fig 5.9 Loaded Bing.com page showing the firewall is functional

# 9.0. Lab 04: Configuring and Securing ACR and AKS

This lab documents the configuration and security of Azure Container Registry (ACR) and Azure Kubernetes Service (AKS) as part of a proof-of-concept deployment. A Dockerfile was used to build a container image, which was then stored securely in ACR. An AKS cluster was configured to pull images from the private registry and deploy the containerized application. Security considerations included controlled access to the container registry and secure exposure of the application, allowing both internal and external access through Kubernetes services.

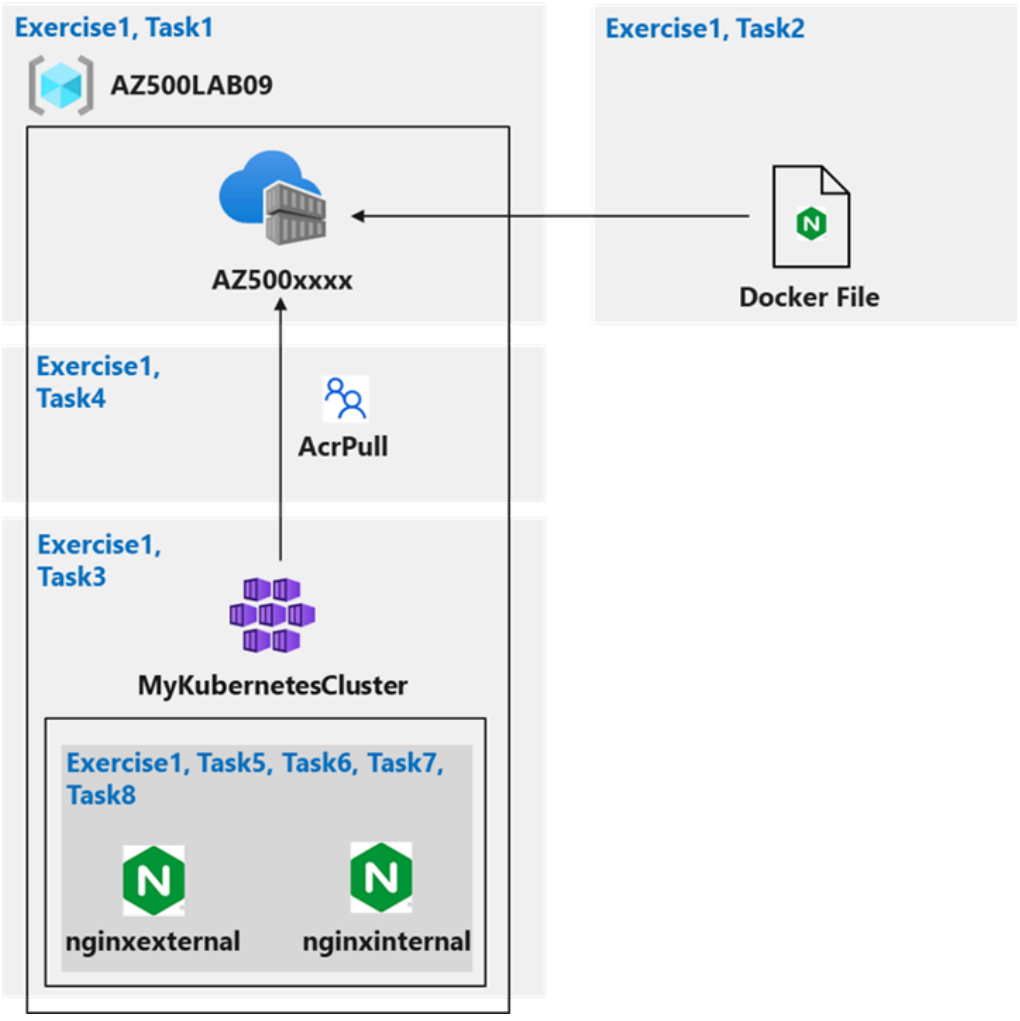


Plate 4.0. Configuring and Securing ACR and AKS diagram

# 9.1. Exercise 1: Configuring and Securing ACR and AKS

## Task 1: Create an Azure Container Registry

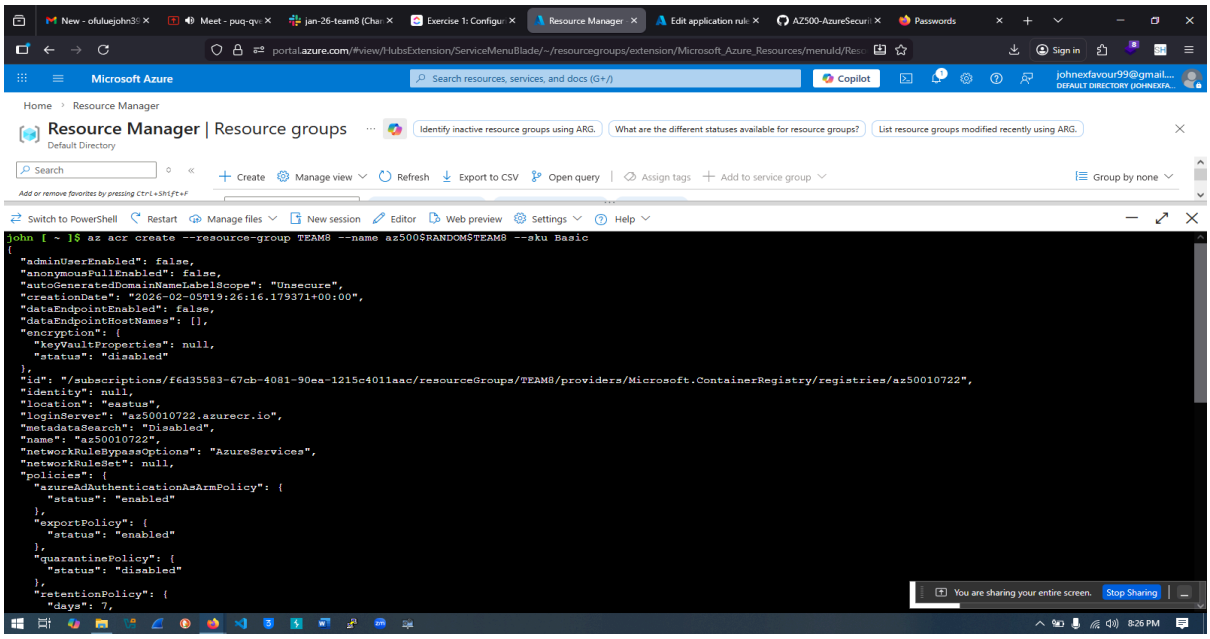


Fig 6.0 Creating an ACR in the azure CLI

## Task 2: Create a Dockerfile, build a container and push it to Azure Container Registry

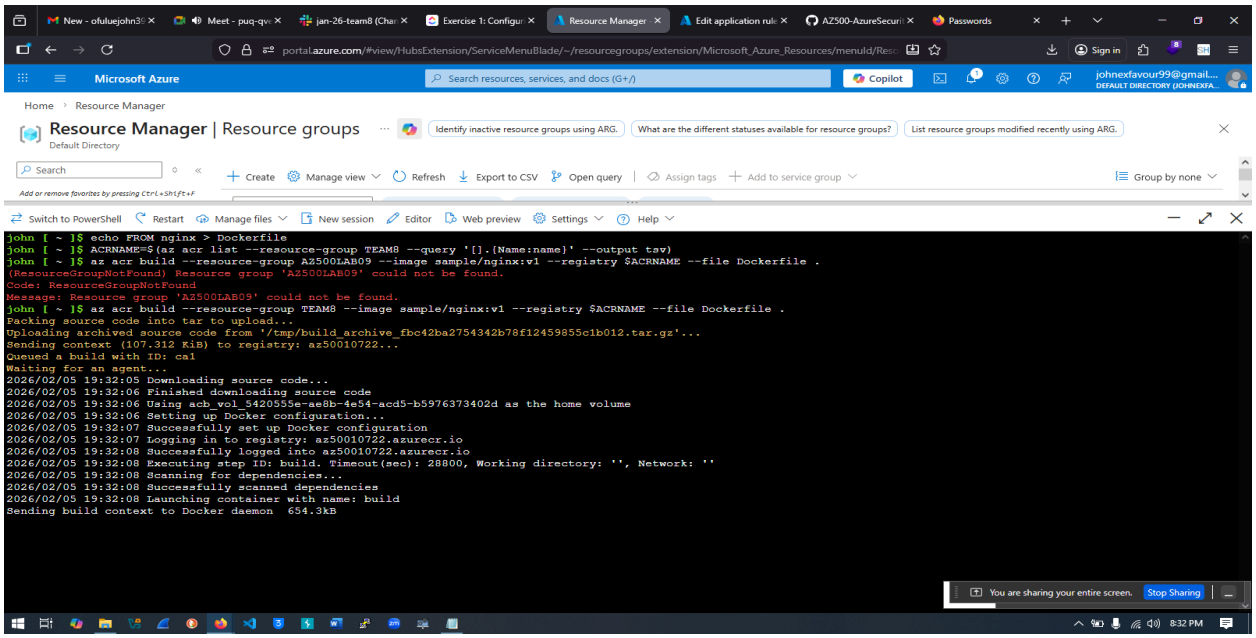


Fig 6.1 Creating a Dockerfile, building a container and pushing to ACR

## Task 3: Create an Azure Kubernetes Service cluster

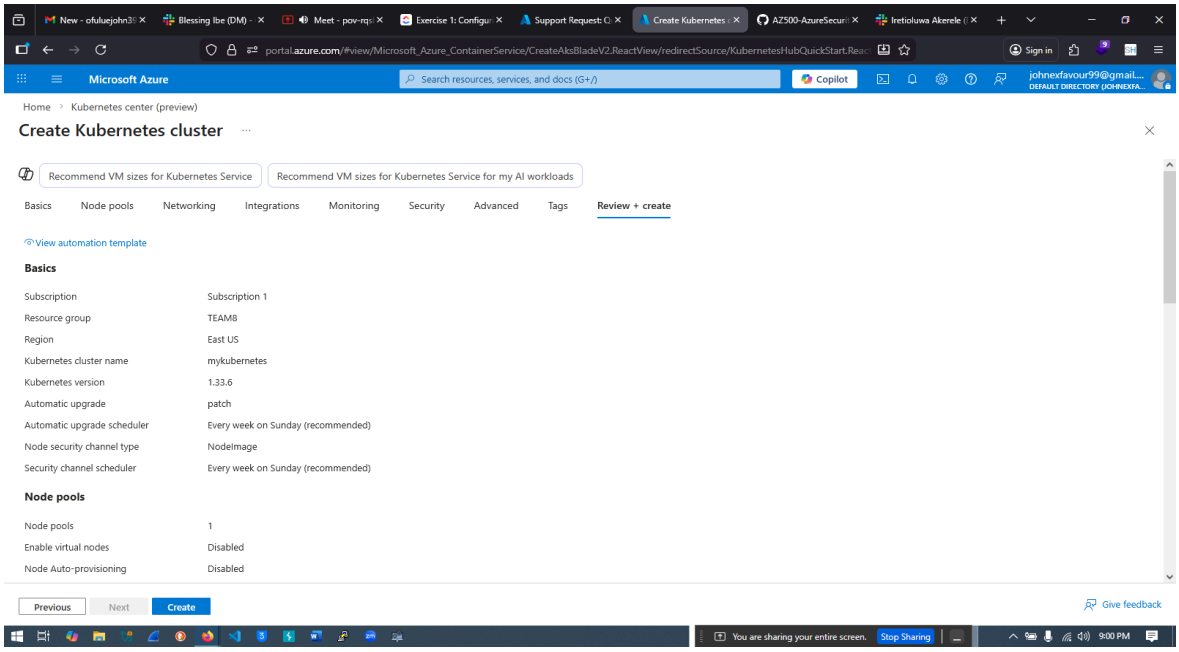


Fig 6.2 Creating an AKS Cluster

## Task 4: Grant the AKS cluster permissions to access the ACR

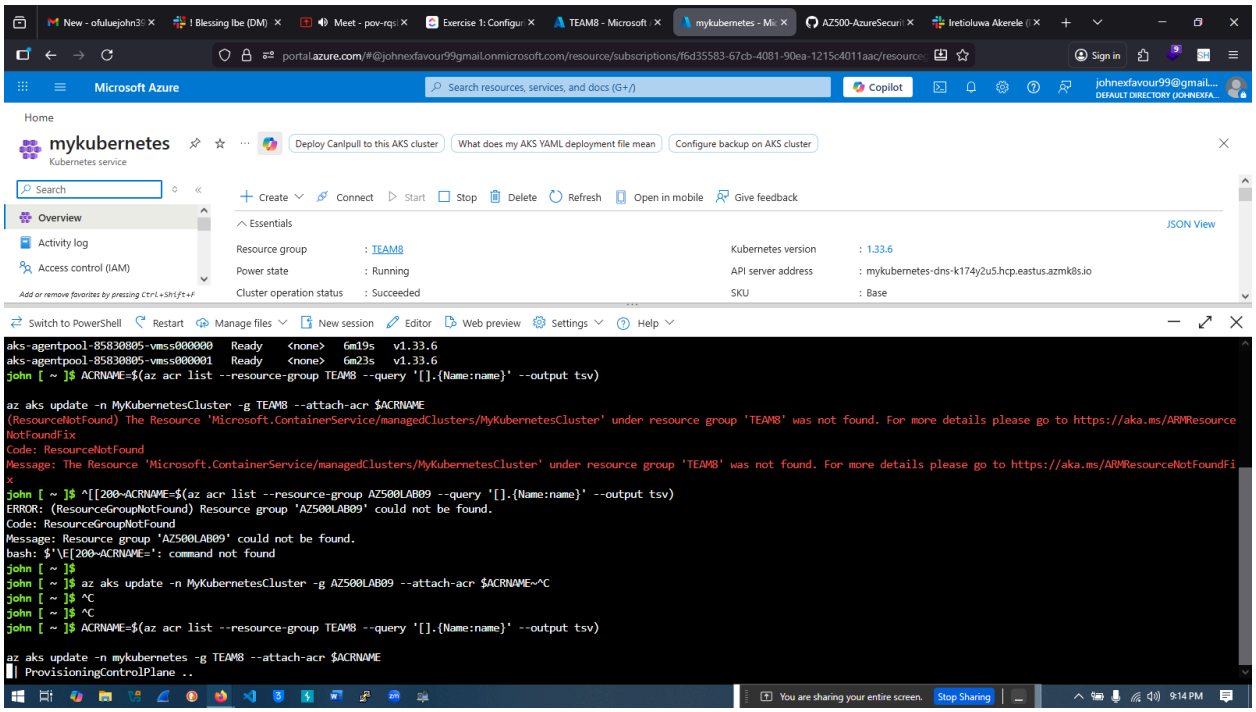


Fig 6.3 Granting the AKS cluster permissions to access the ACR

Task 5: Deploy an external service to AKS

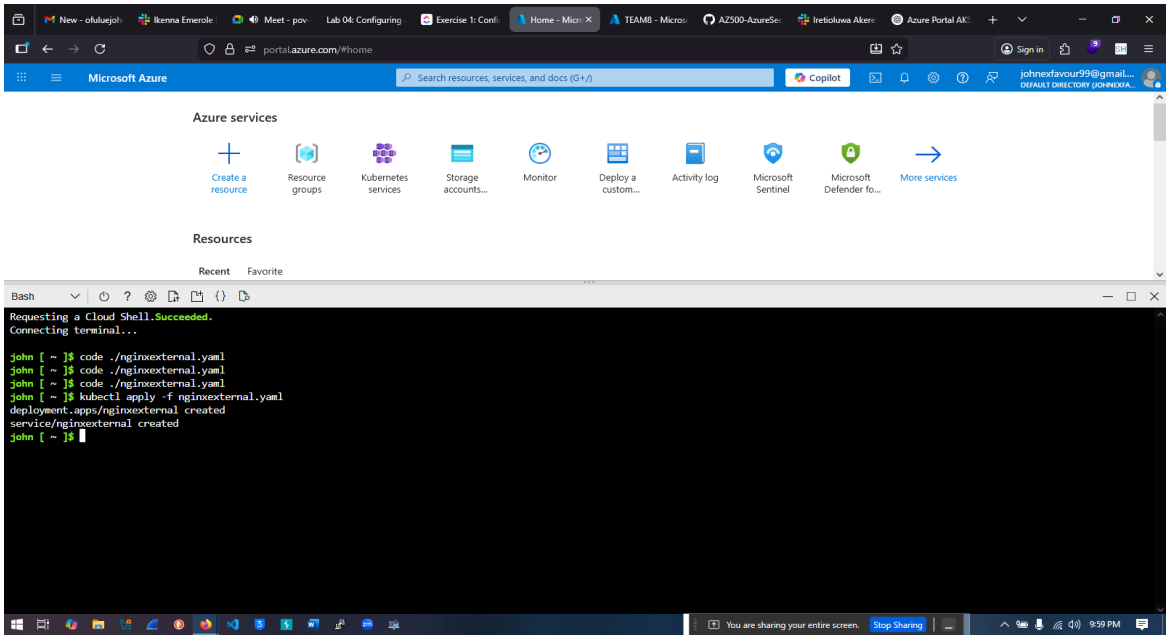


Fig 6.4 Code showing the deployment of an external service using aks

Task 6: Verify the you can access an external AKS-hosted service

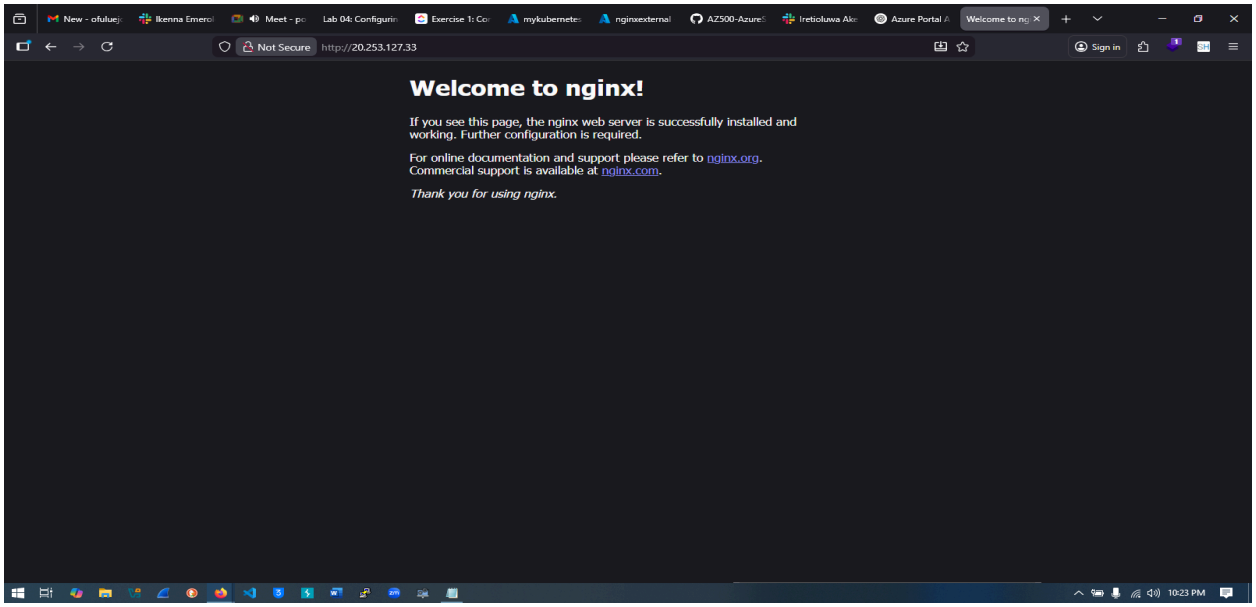


Fig 6.5 Loaded nginx page showing the successful deployment of an external service using aks

## Task 7: Deploy an internal service to AKS

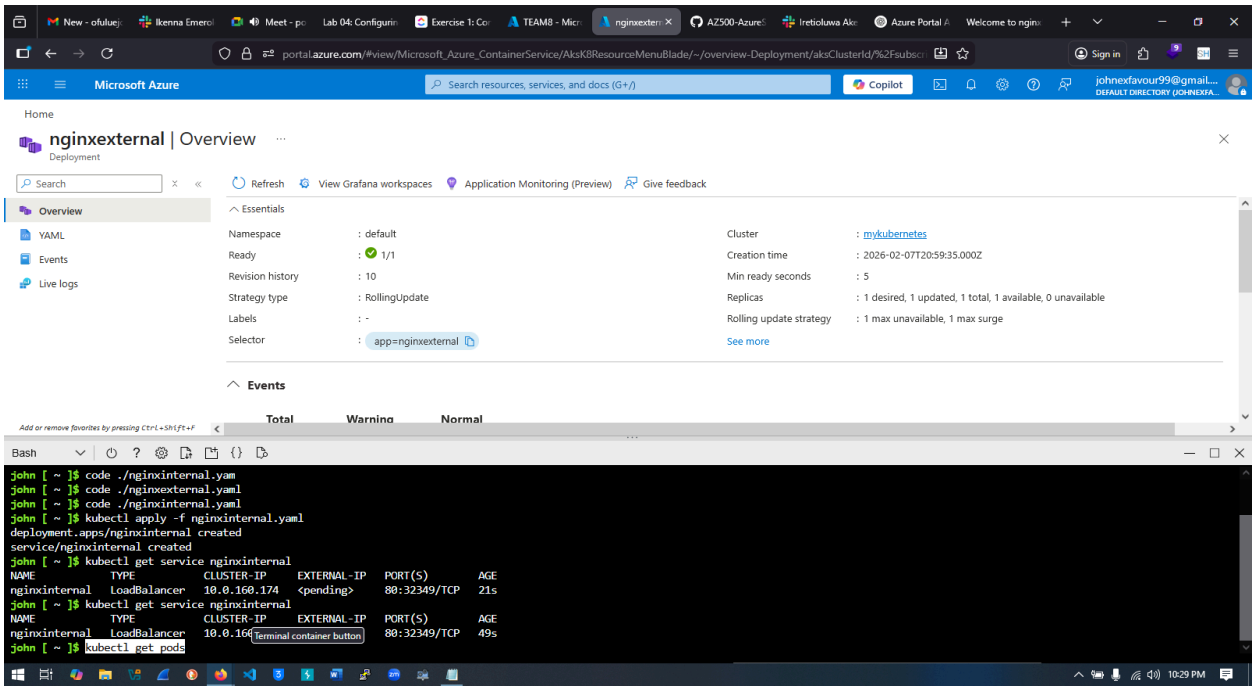


Fig 6.6 Code showing the deployment of an internal service using aks

## Task 8: Verify that you can access an internal AKS-hosted service

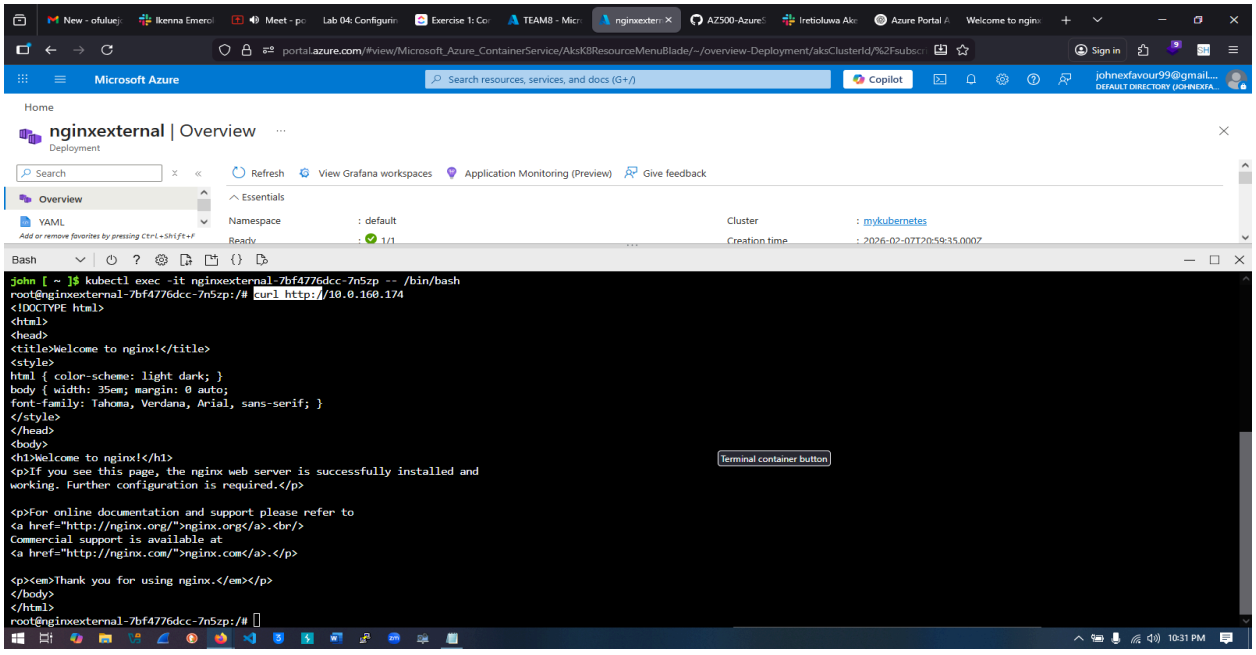


Fig 6.7 Verifying the access to an internal AKS-hosted service

# 10.0. Lab 05: Service Endpoints and Securing Storage

This chapter demonstrates the use of Azure service endpoints to secure access to Azure Storage as part of a proof-of-concept deployment. A storage service endpoint was configured to ensure that traffic destined for Azure Storage remained on the Azure backbone network. Access to the storage account was restricted to a specific subnet, allowing only authorized resources to connect. Validation testing confirmed that resources outside the designated subnet were unable to access the storage, demonstrating effective network-level security controls.

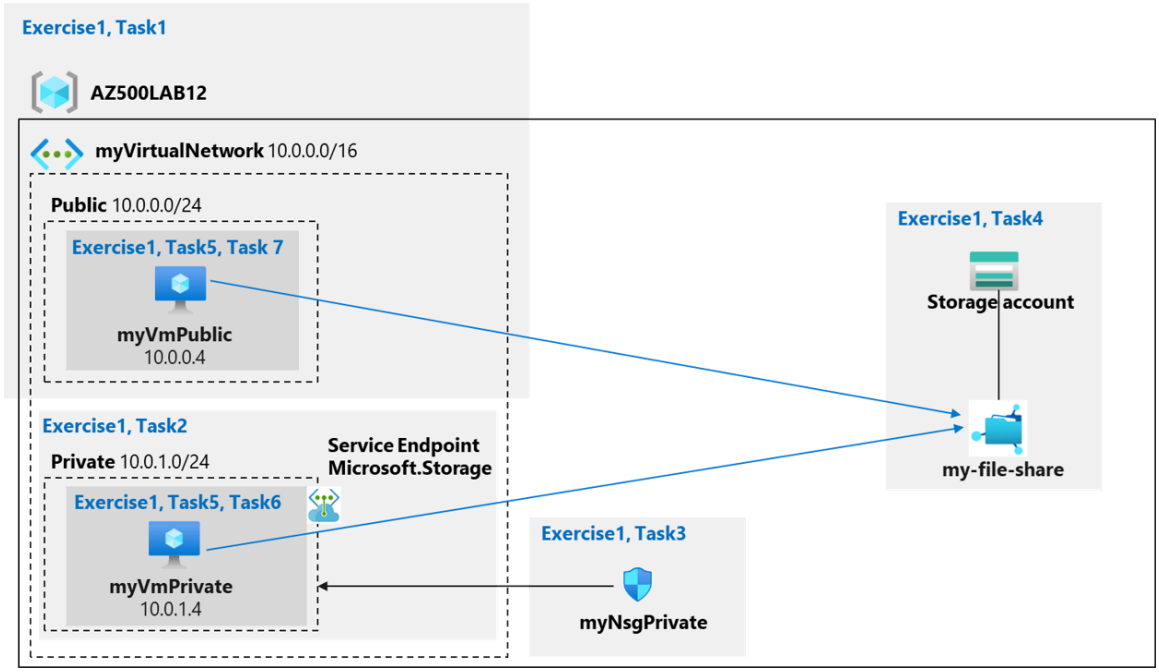


Plate 5.0 Service Endpoints and Securing Storage diagram

# 10.1 Exercise 1: Service endpoints and security storage

## Task 1: Create a virtual network

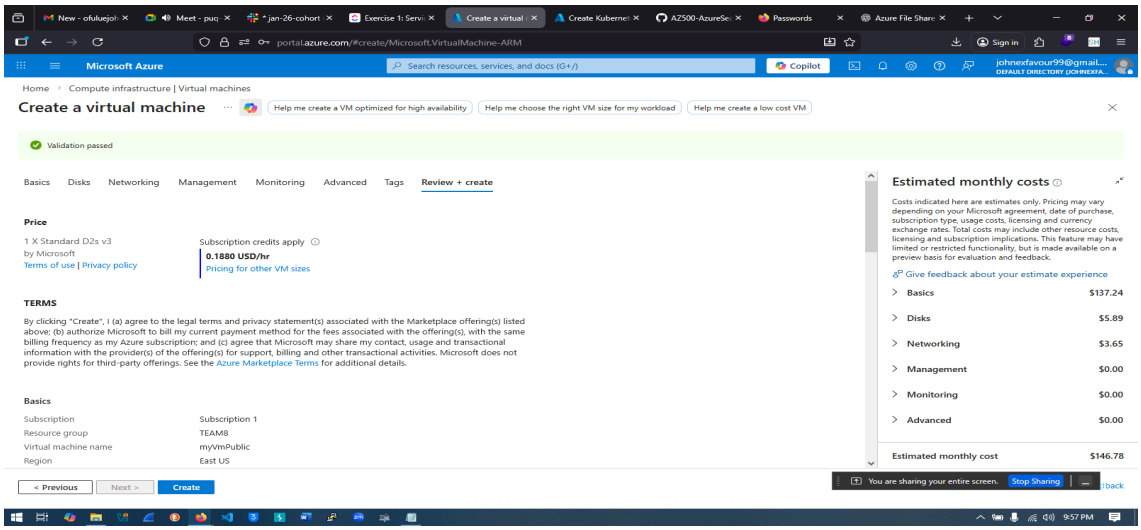


Fig 7.0 Virtual network being created

## Task 2: Add a subnet to the virtual network and configure a storage endpoint

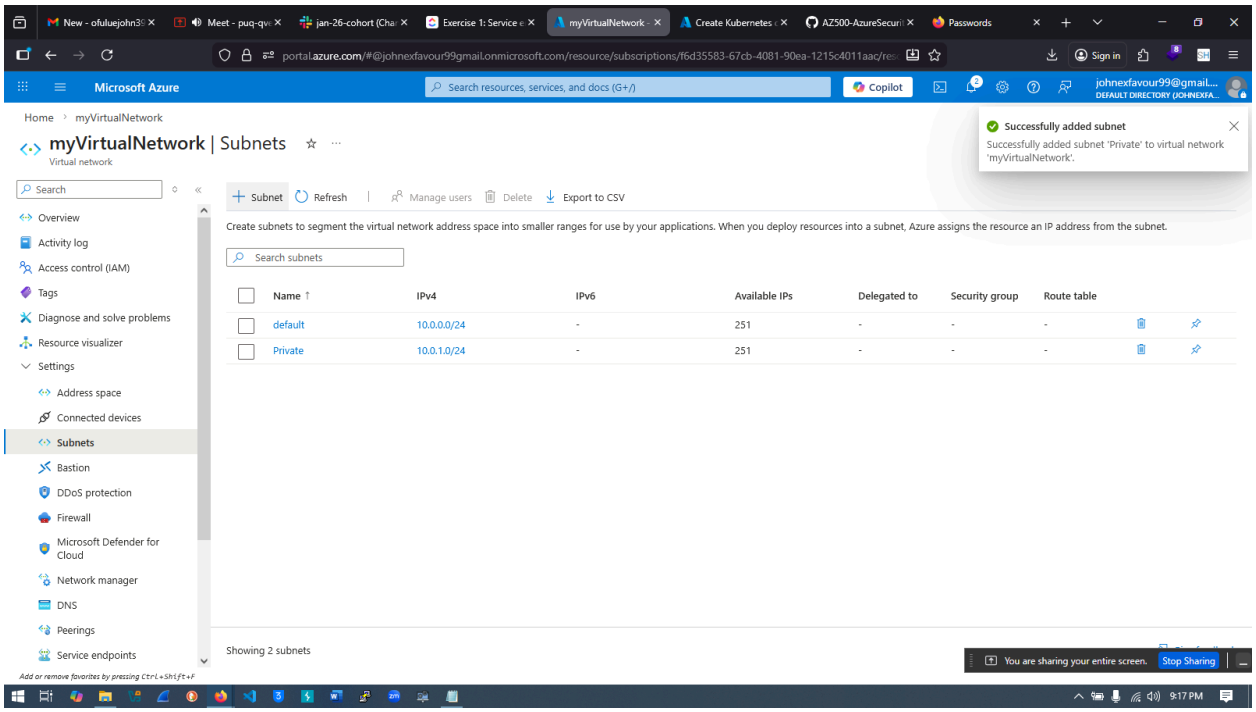


Fig 7.1 Adding a subnet to the virtual network and configuring a storage endpoint

Task 3: Configure a network security group to restrict access to the subnet

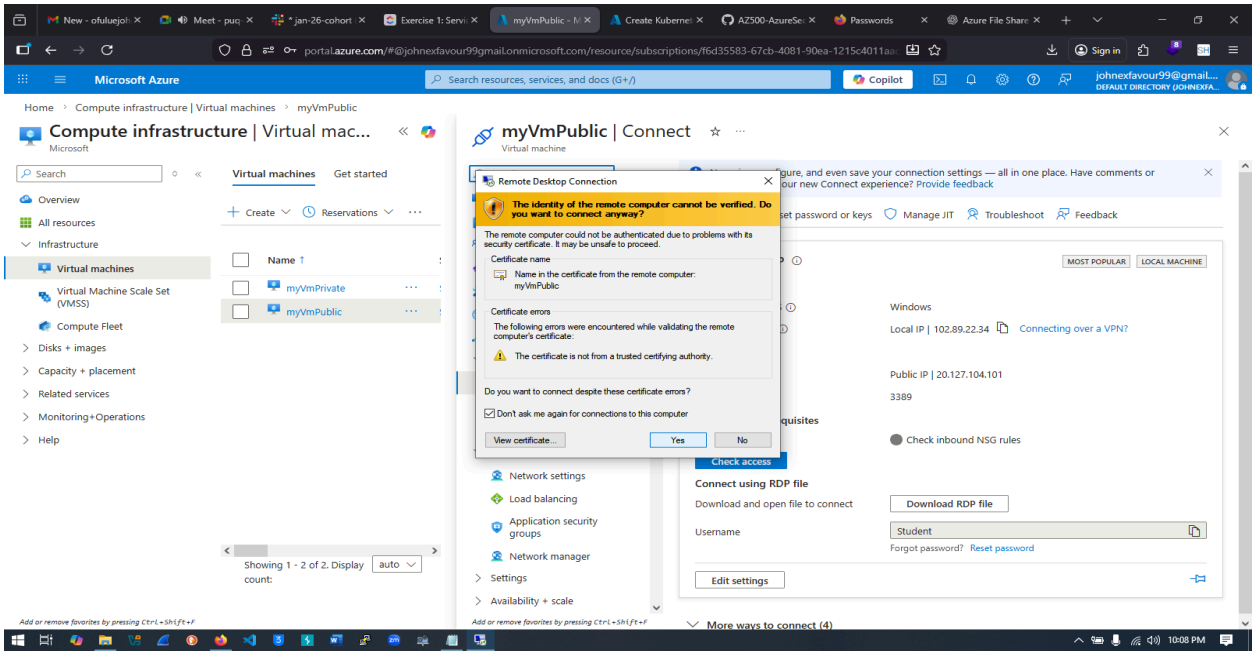


Fig 7.2 Configuring a network security group to restrict access to the subnet

Task 4: Configure a network security group to allow rdp on the public subnet

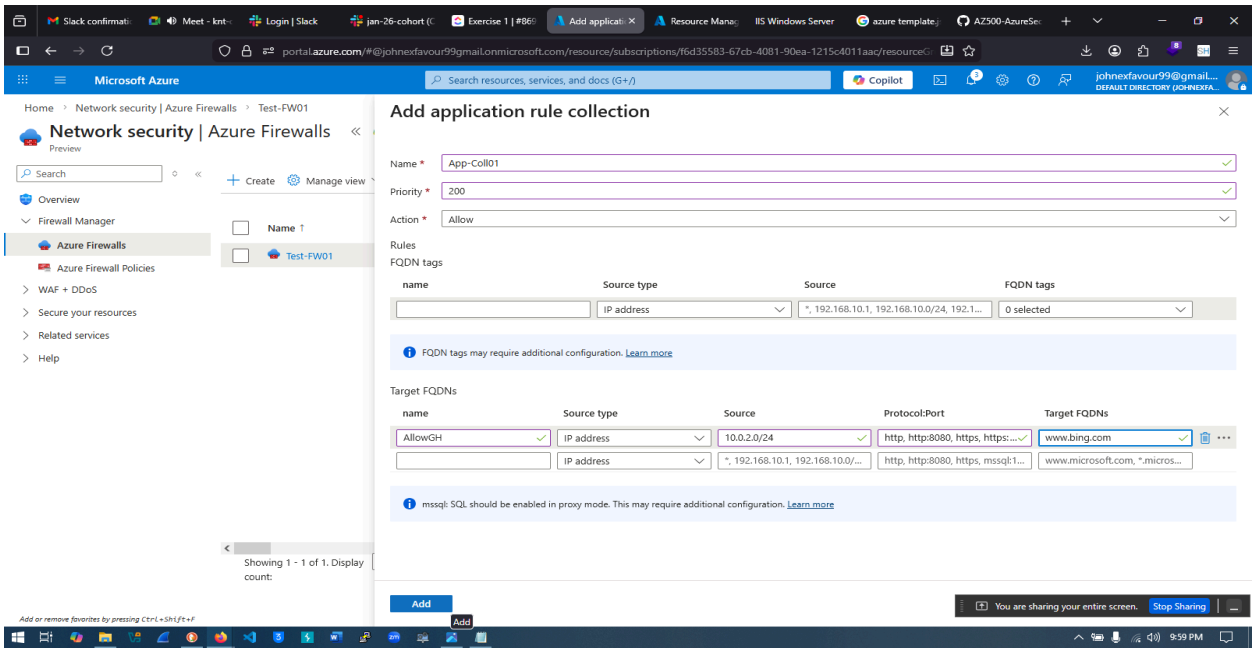


Fig 7.3 Configuring a network security group to allow rdp on the public subnet

## Task 5: Create a storage account with a file share

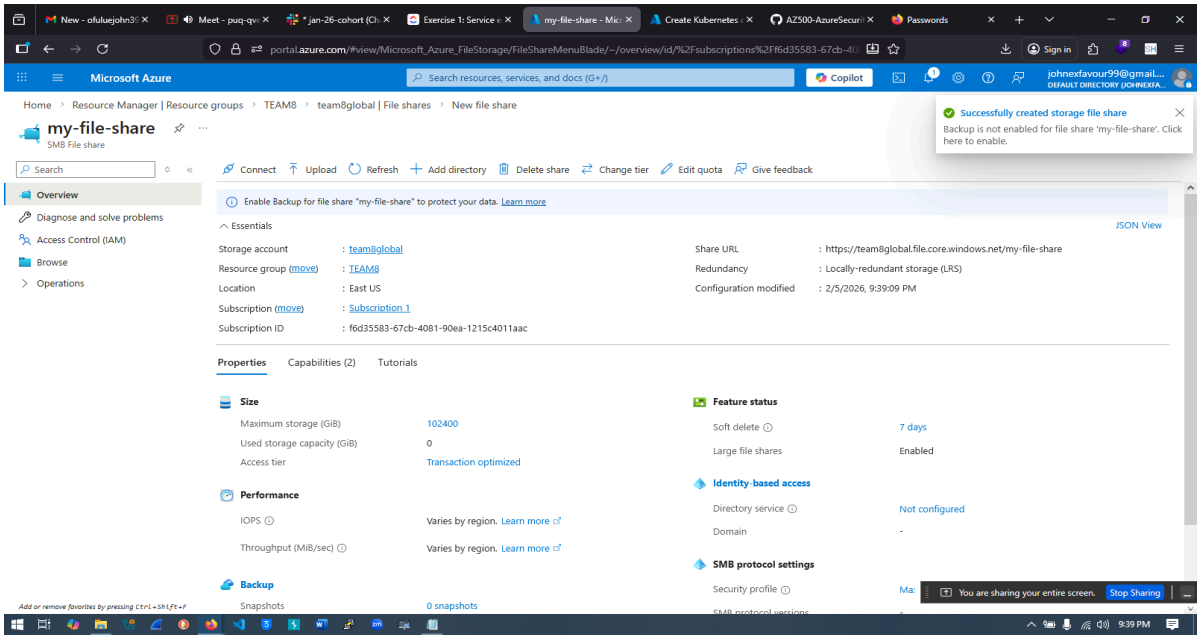


Fig 7.4 Creating a storage account with a file share

## Task 6: Deploy virtual machines into the designated subnets

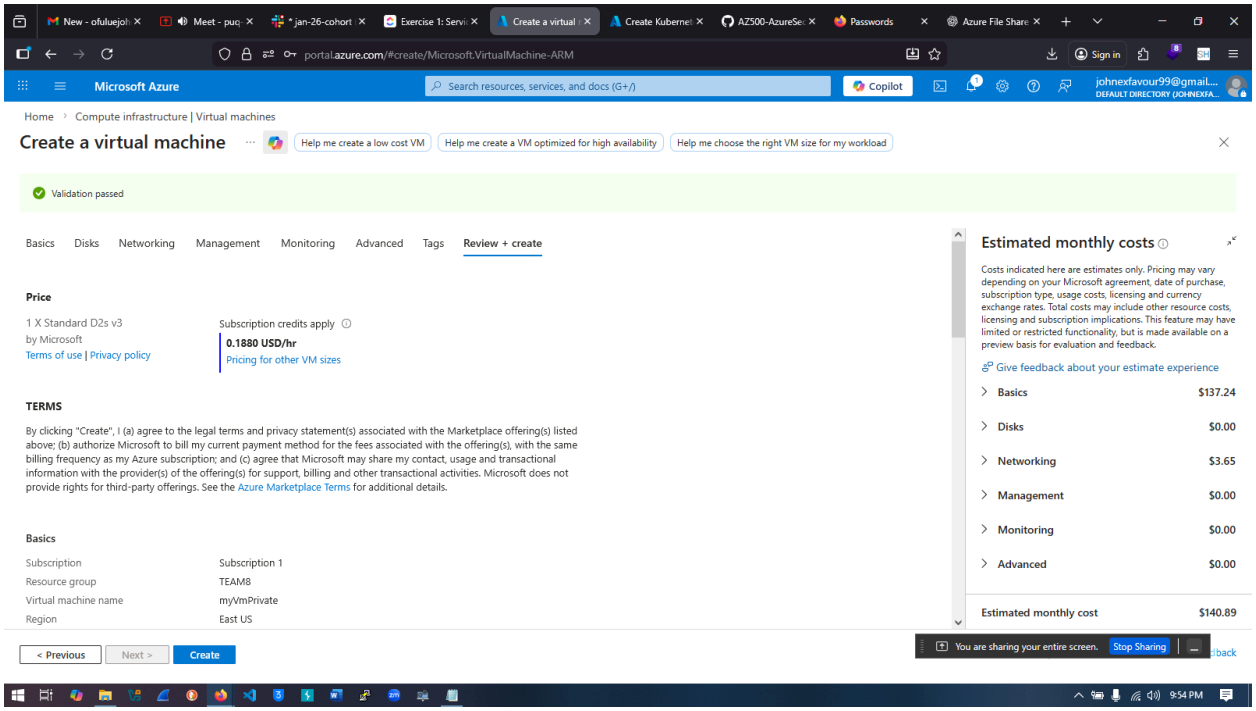


Fig 7.5 Deploying virtual machines into the designated subnets

Task 7: Test the storage connection from the private subnet to confirm that access is allowed

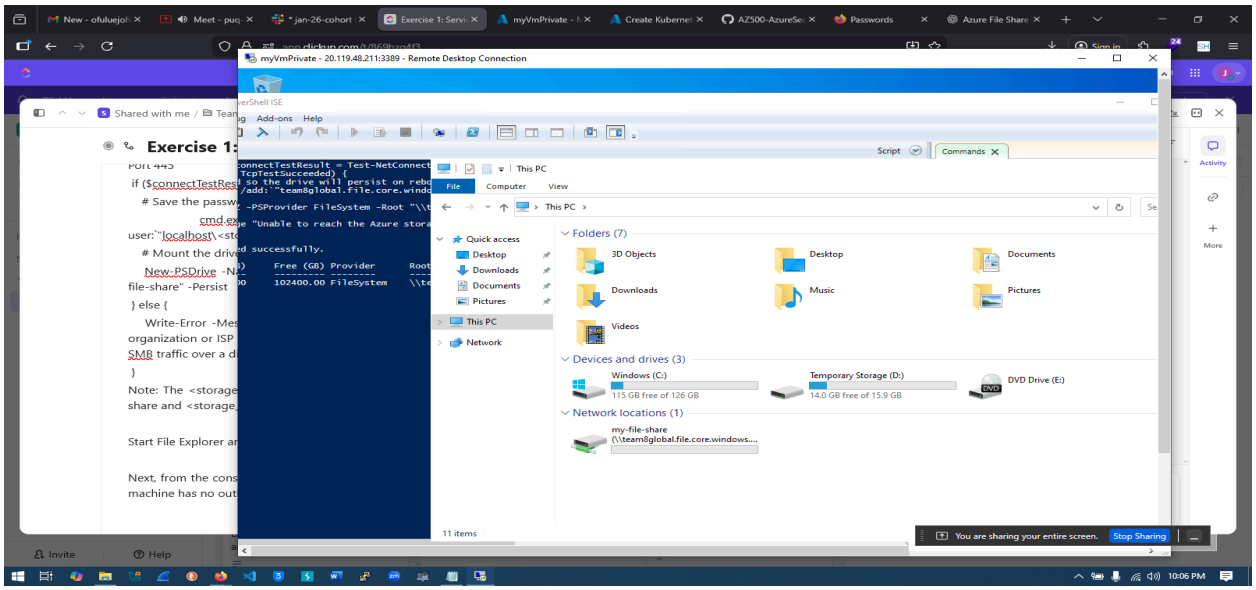


Fig 7.6 Testing the storage connection from the private subnet to confirm that access is allowed

Task 8: Test the storage connection from the public subnet to confirm that access is denied

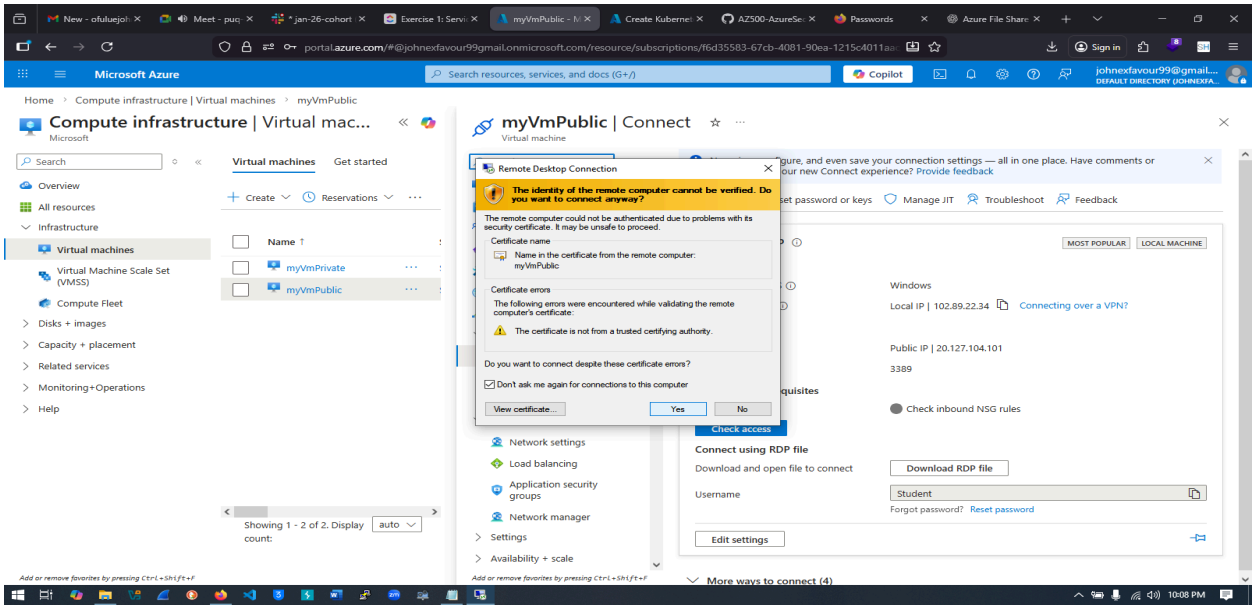


Fig 7.7 Testing the storage connection from the public subnet to confirm that access is denied

# 11.0. Lab 06: Create a Log Analytics Workspace, Azure Storage Account, and Data Collection Rule (DCR)

This chapter focuses on enhancing monitoring and security visibility for Azure virtual machines by implementing Azure Monitor Agent (AMA) and Data Collection Rules (DCRs). A virtual machine was deployed in the East US region, followed by the creation of a Log Analytics workspace and an Azure Storage account to centralize log and data storage. Data Collection Rules were configured to collect security events, system logs, and performance counters from the virtual machine, enabling centralized monitoring, improved threat detection, and performance analysis across the environment.

## 11.1 Exercise 1: Deploy an Azure virtual machine

### Task 1: Deploy an Azure virtual machine

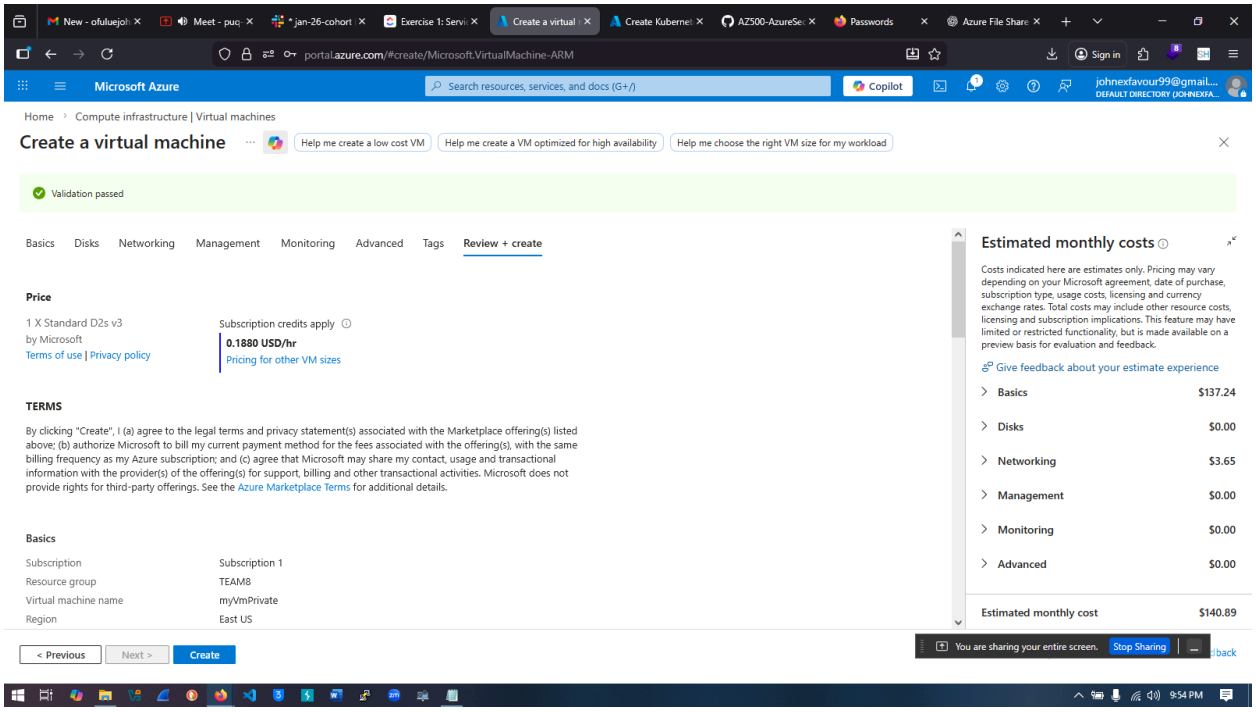


Fig 8.0 Deploying an azure vm

# 11.2 Exercise 2: Create a Log Analytics workspace

## Task 1: Create a Log Analytics workspace

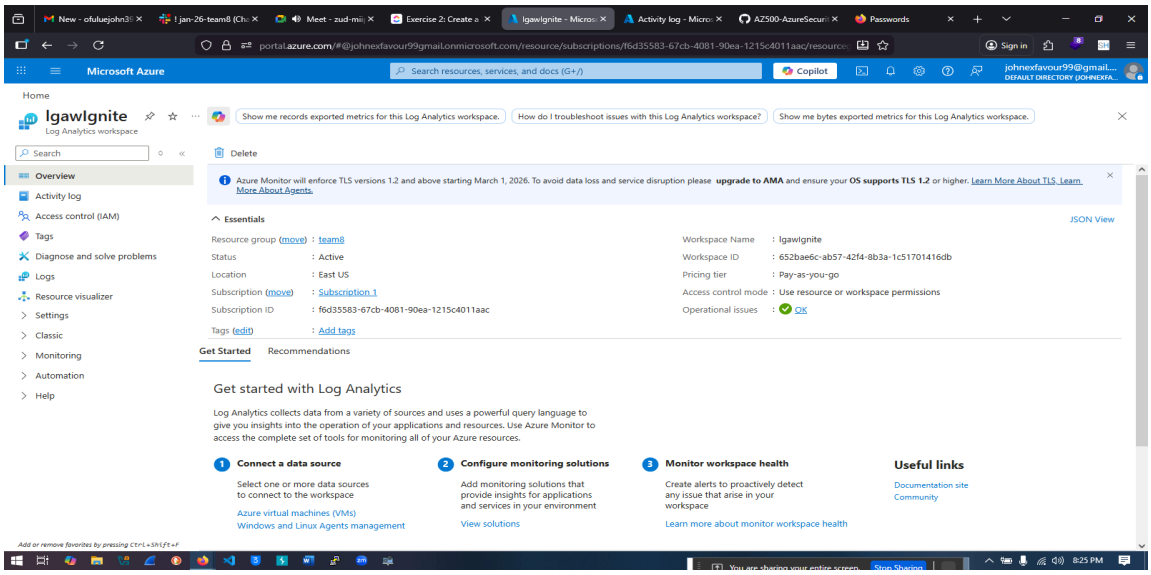


Fig 8.1 Created log analytics workspace

# 11.3 Exercise 3: Create an Azure storage account

## Task 1: Create an Azure storage account

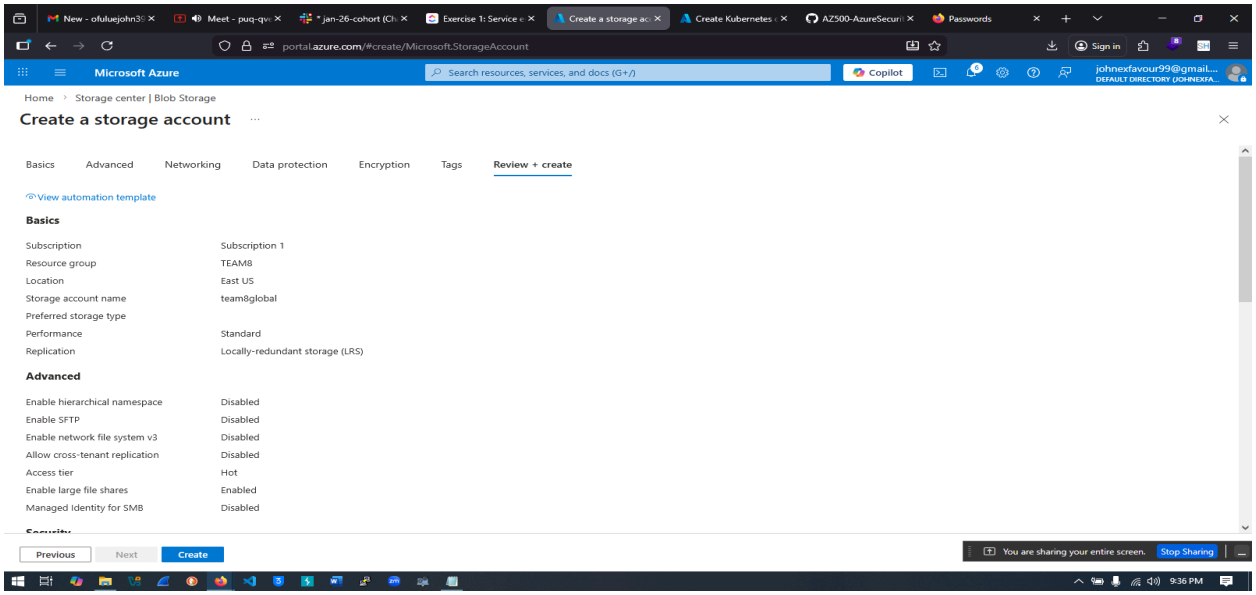


Fig 8.2 Creating an azure storage account

# 11.4 Exercise 4: Create a data collection rule

## Task 1: Create a Data Collection Rule.

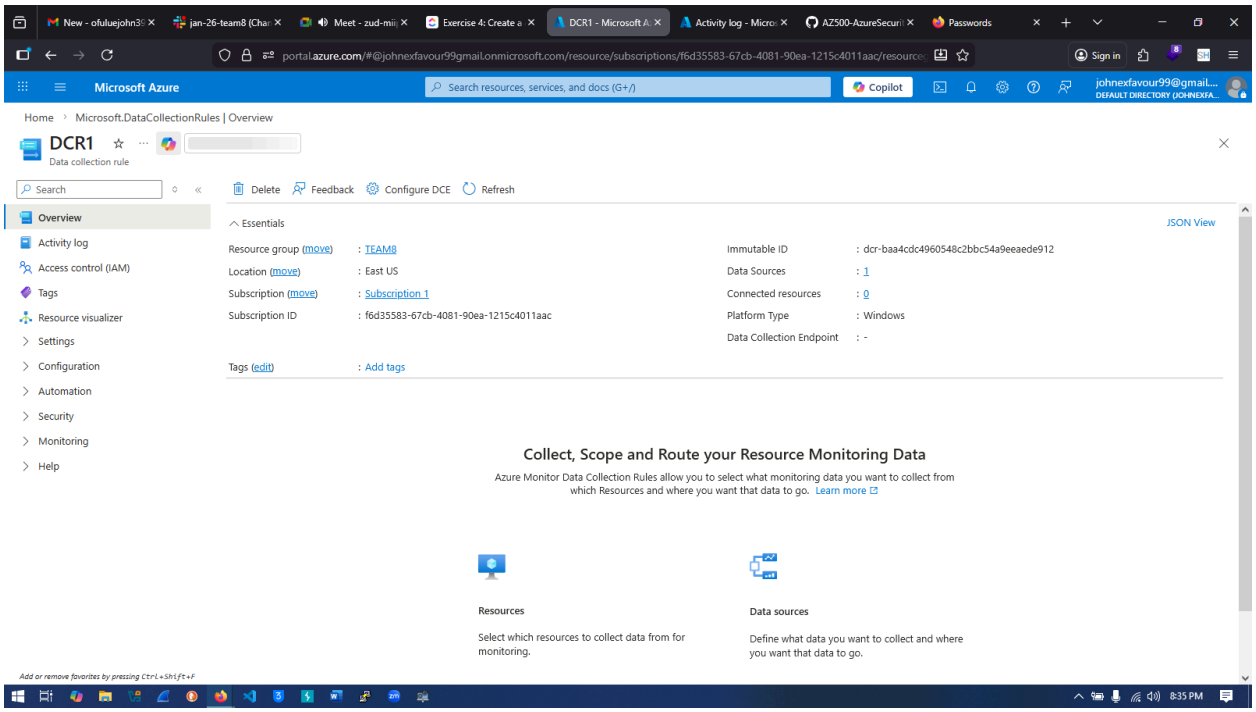


Fig 8.3 Created DCR

# 12.0 Lab 07: Configuring Microsoft Defender for Cloud Enhanced Security Features for Servers

This chapter covers the configuration of Microsoft Defender for Cloud enhanced security features for servers to protect both Azure virtual machines and hybrid environments. Microsoft Defender for Servers was enabled to provide advanced threat protection, vulnerability management, and continuous security monitoring. The enhanced features available in Defender for Servers Plan 2 were reviewed and applied, improving visibility into security posture, identifying misconfigurations, and strengthening protection against potential cyber threats across the organization's server infrastructure.

## Exercise 1: Configure Microsoft Defender for Cloud Enhanced Security Features for Servers

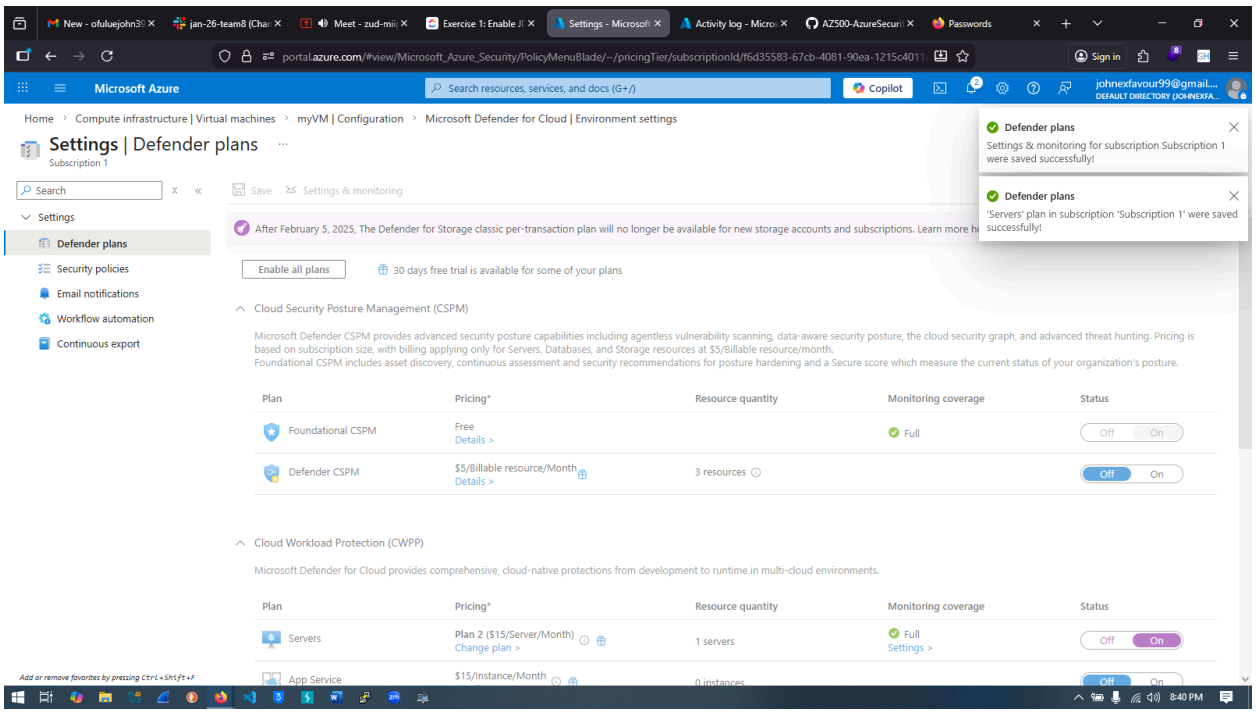


Fig 9.0 Configured Microsoft Defender for Cloud Enhanced Security Features for Servers

## Exercise 2: Review the enhanced security features for Microsoft Defender for Servers Plan 2

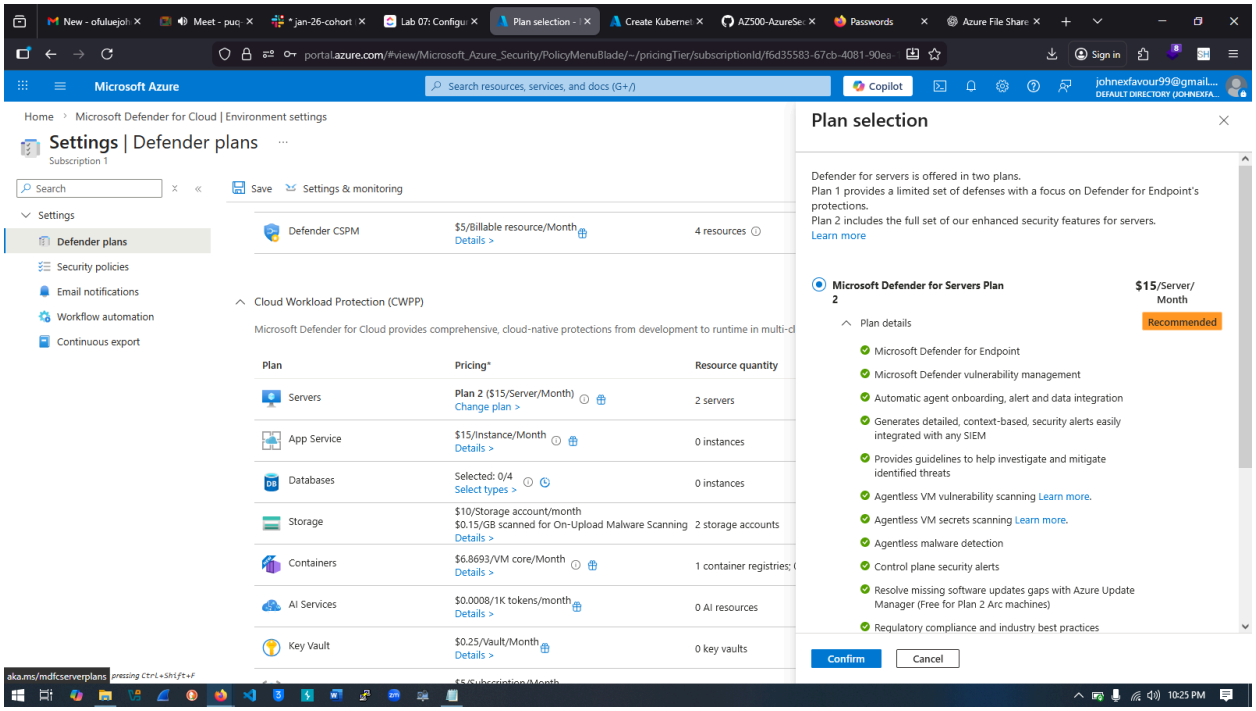


Fig 9.1 Enhanced security features for Microsoft Defender for Servers Plan 2

# 13.0 Lab 08: Enable just-in-time access on VMs

This chapter demonstrates the implementation of Just-in-Time (JIT) access to enhance the security of Azure virtual machines hosting critical applications. JIT access was enabled on a selected virtual machine to reduce exposure to brute-force attacks by limiting inbound management access to approved time windows. Access requests were made through the Azure portal, allowing temporary and controlled connectivity to the VM, thereby strengthening overall security while maintaining necessary administrative access.

## Exercise 1: Enable JIT on your VMs from the Azure portal.

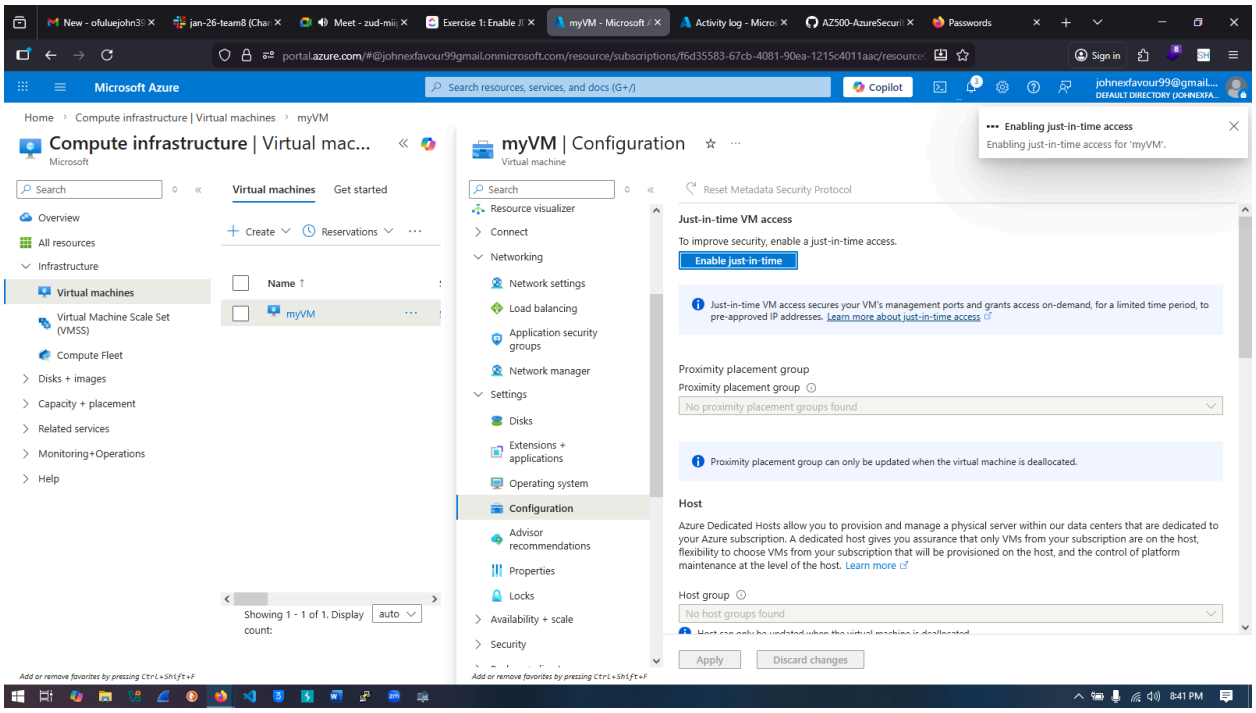


Fig 10.0 JIT being enabled on the VM from azure portal

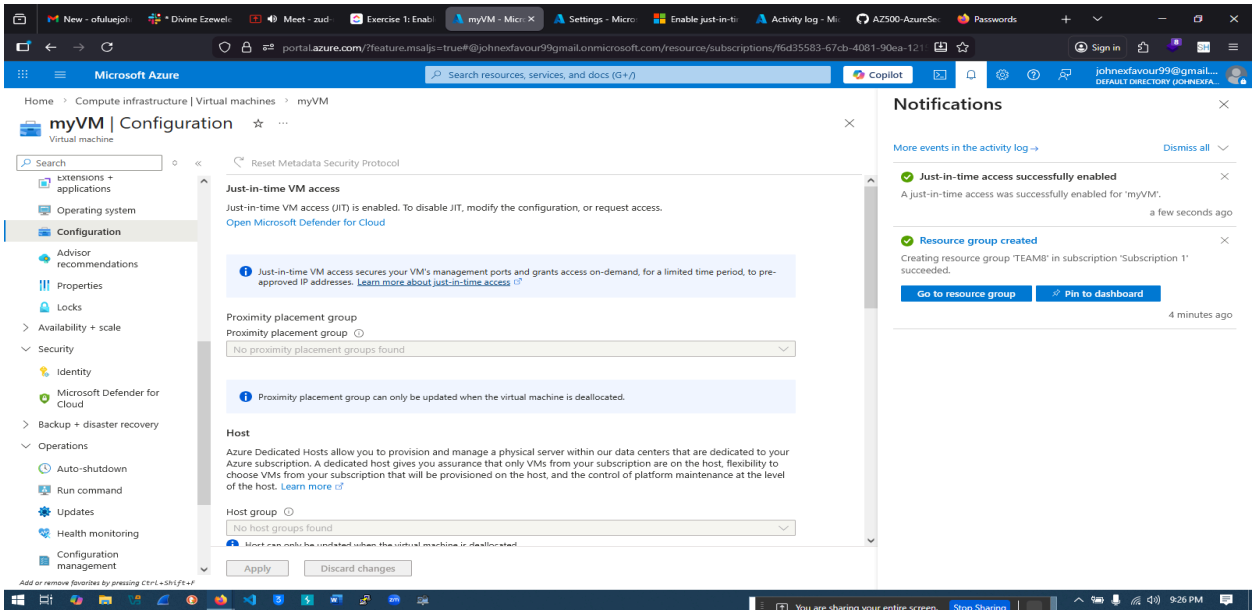


Fig 10.1 JIT has been enabled on the VM from azure portal

## Exercise 2: Request access to a VM that has JIT enabled from the Azure portal.

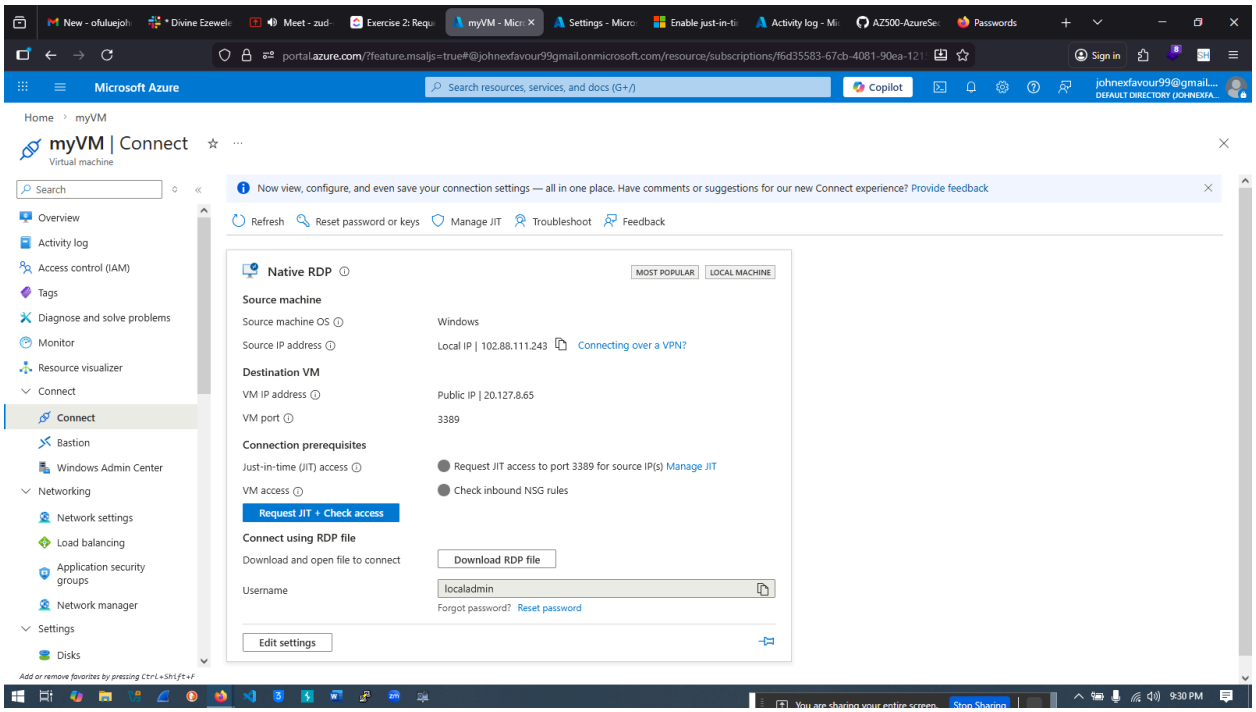


Fig 10.2 Requested access to a VM that has JIT

# 14.0. Lab 09: Microsoft Sentinel

This chapter presents a proof of concept for threat detection and incident response using Microsoft Sentinel. Data collection was enabled for Azure Activity logs and Microsoft Defender for Cloud to provide centralized security visibility. Built-in and custom analytics rules were configured to generate alerts for suspicious activity, and the use of playbooks was reviewed to demonstrate how automated responses can be triggered to remediate and manage security incidents efficiently.

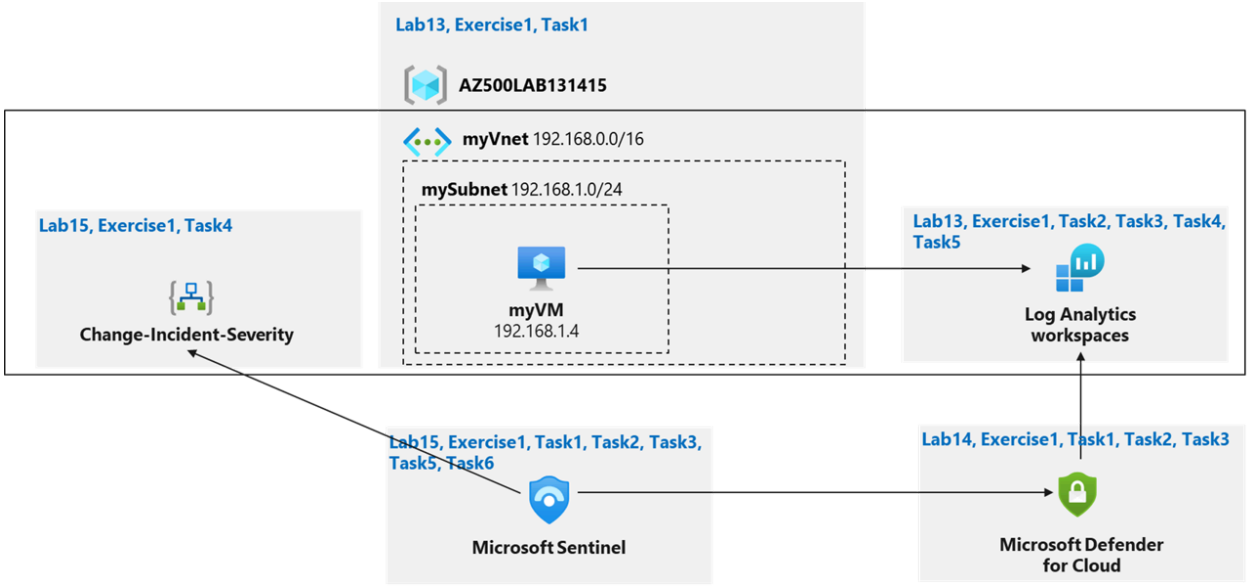


Plate 6.0 Microsoft Sentinel diagram

# 14.1. Exercise 1: Implement Microsoft Sentinel

## Task 1: On-board Microsoft Sentinel

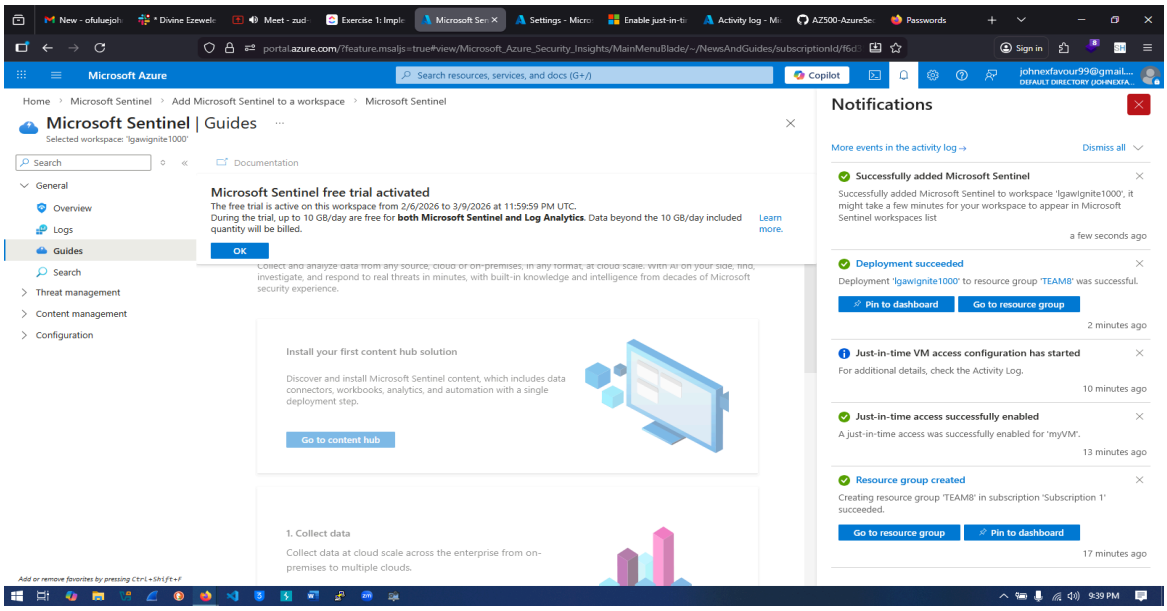


Fig 11.0 On boarded Microsoft Sentinel

## Task 2: Connect Azure Activity to Sentinel

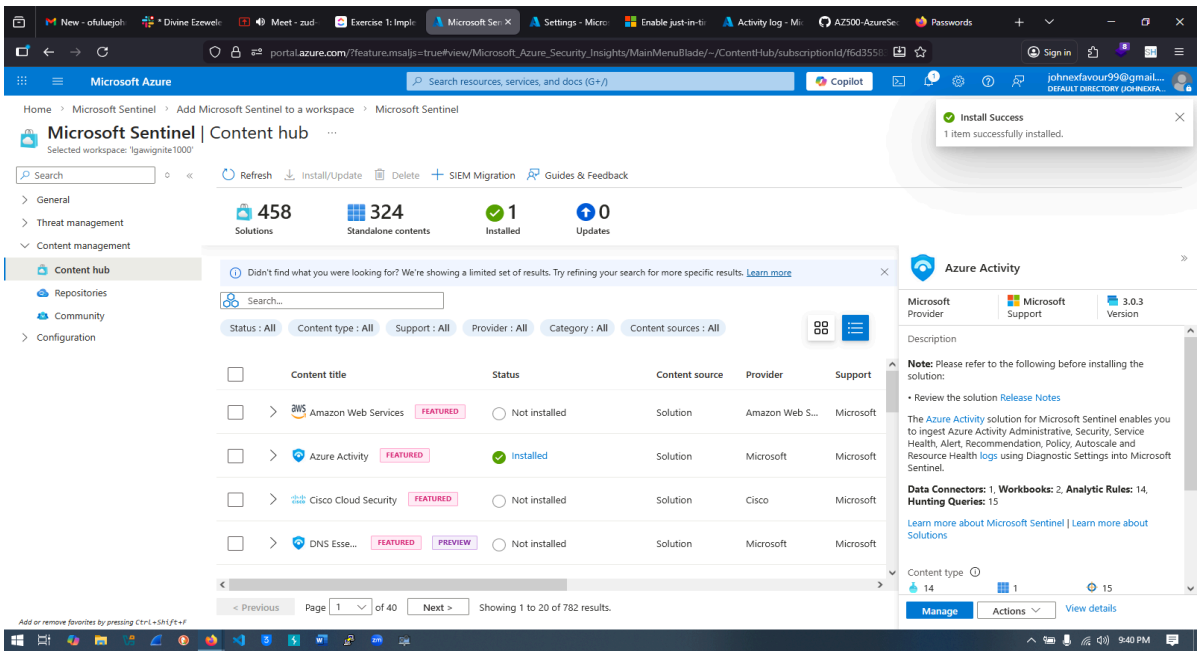


Fig 11.1 Azure activity successfully installed

Task 3: Create a rule that uses the Azure Activity data connector.

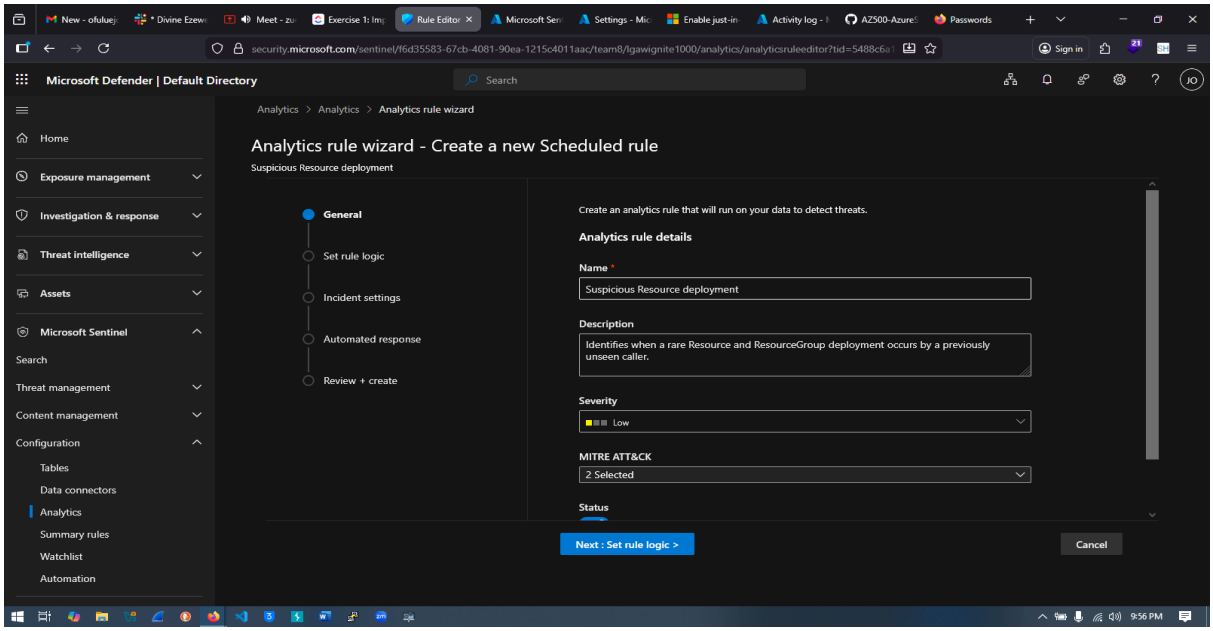


Fig 11.2 Creating a rule that uses the Azure Activity data connector

Task 4: Create a playbook

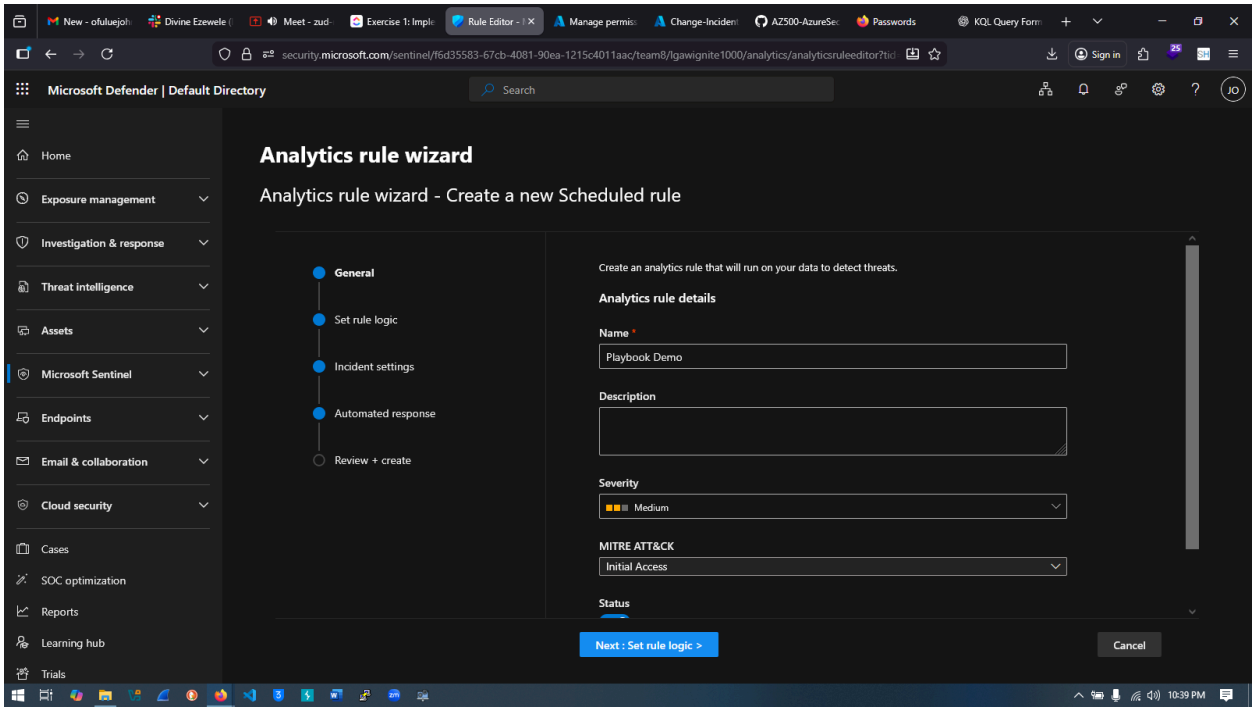


Fig 11.3 Creating a playbook

Task 5: Create a custom alert and configure the playbook as an automated response.

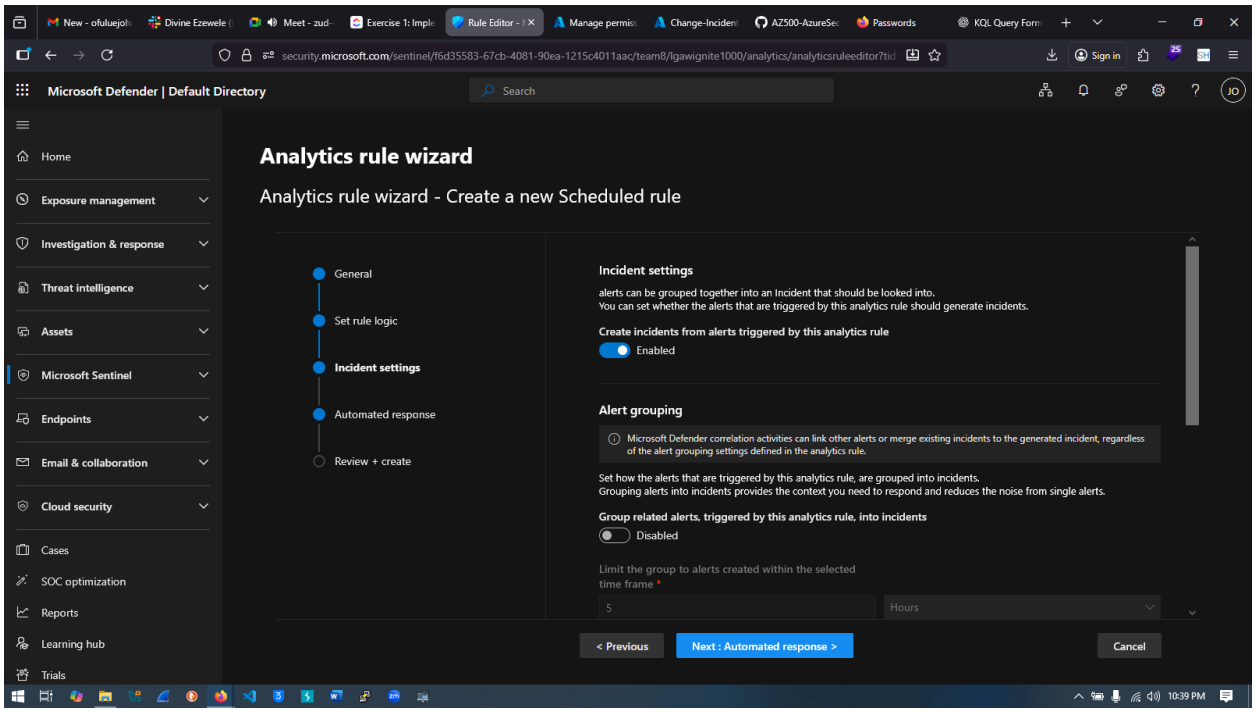


Fig 11.4 Creating a custom alert

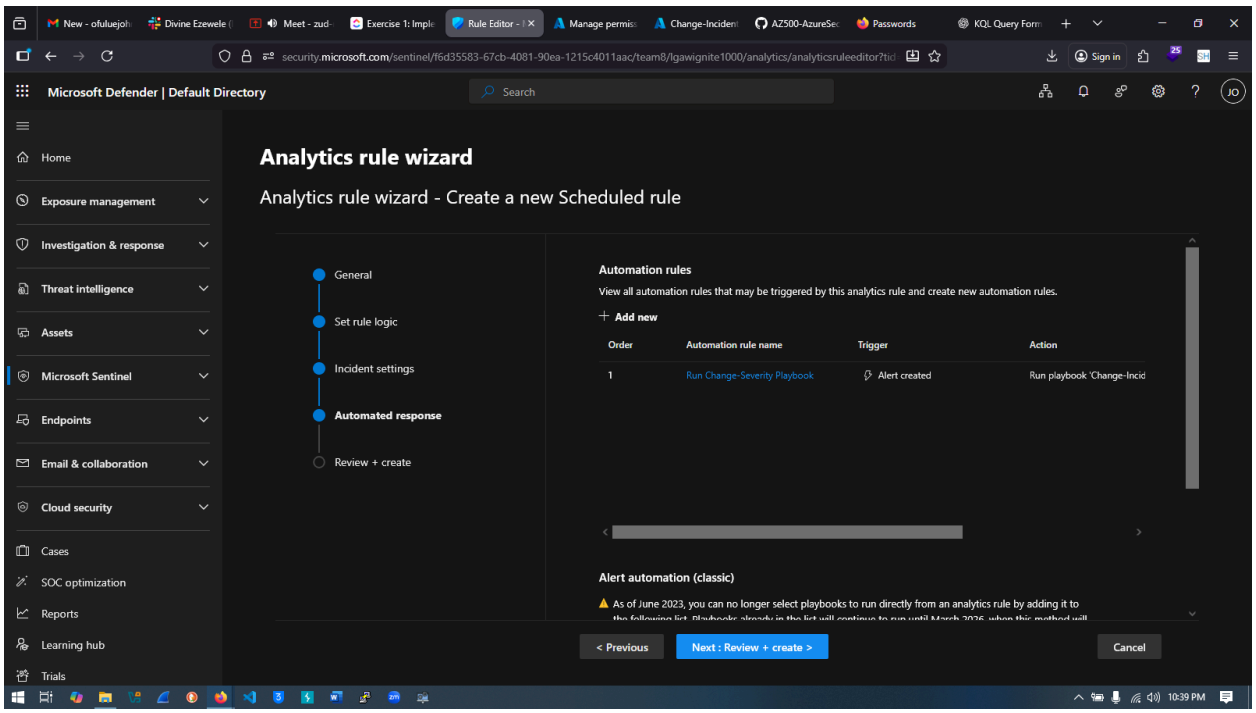


Fig 11.5 Configuring the playbook

Task 6: Invoke an incident and review the associated actions.

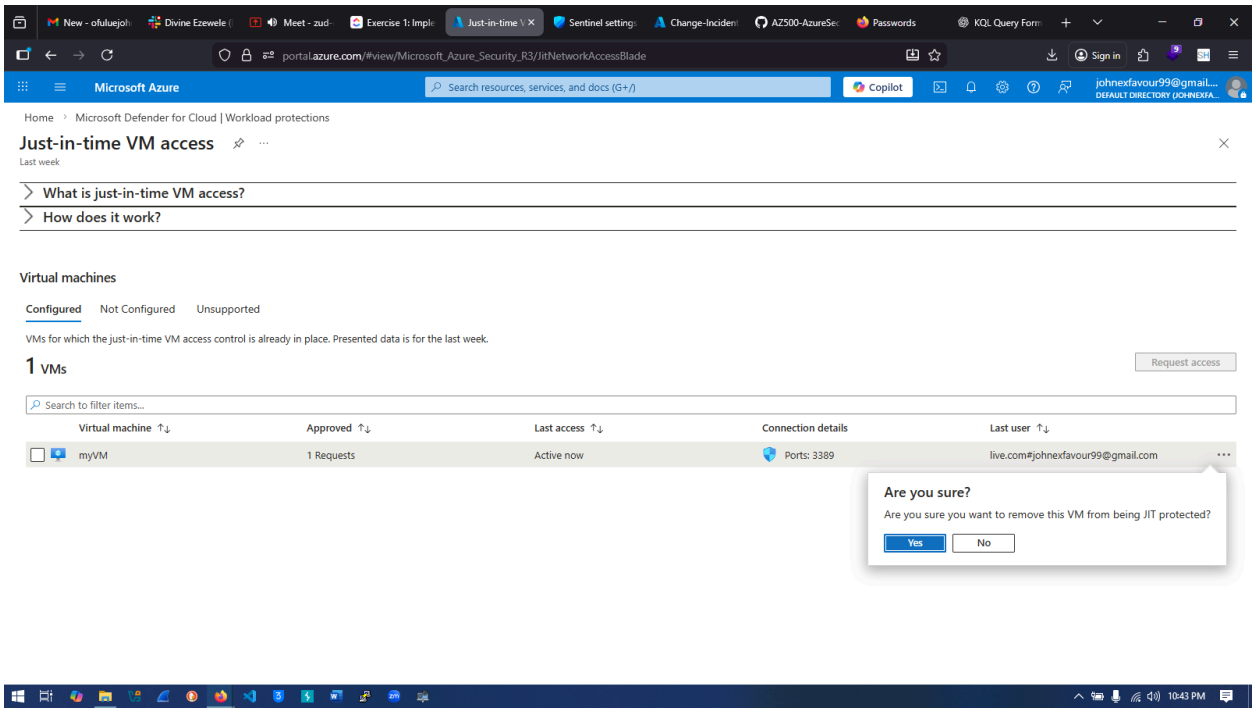


Fig 11.6 Invoking an incident I

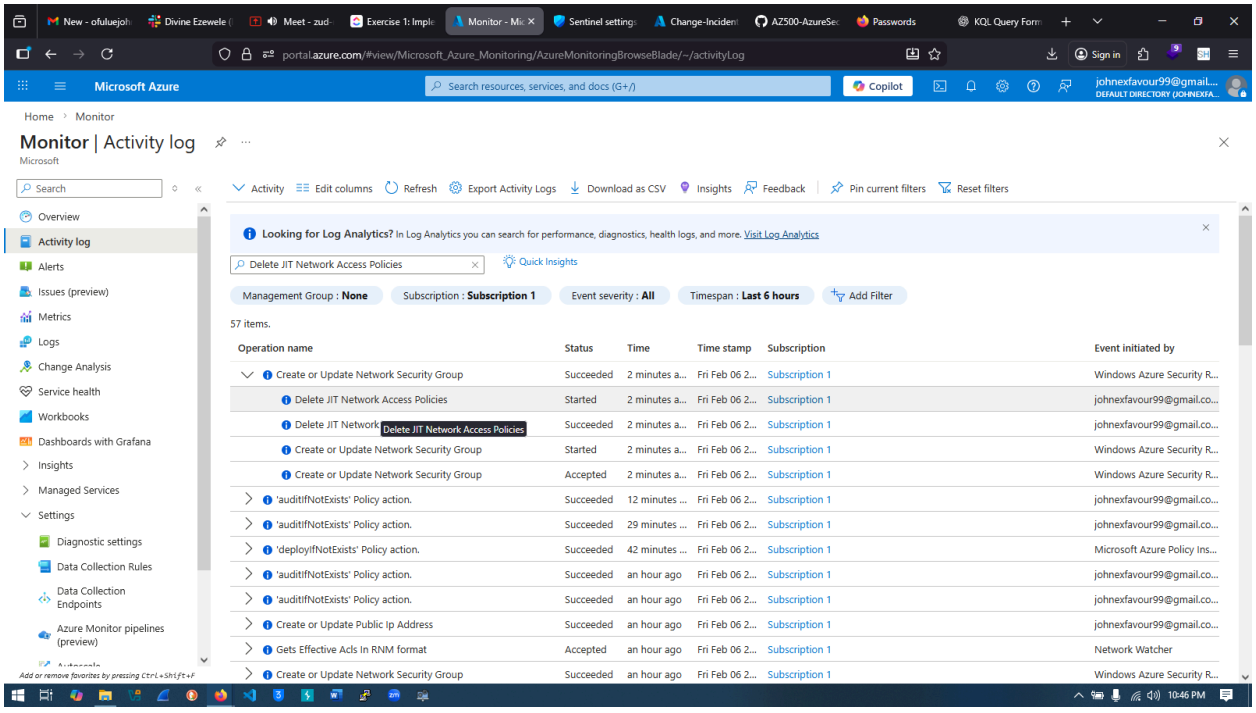


Fig 11.7 Invoking an incident II

# 15.0 Key Assessment Areas & Findings

## 15.1 Identity & Access Management

Identity and Access Management forms the cornerstone of cloud security in Azure environments. During the sprint, Microsoft Entra ID (formerly Azure Active Directory) was leveraged as the central identity provider to manage users, groups, and authentication policies across the environment. A dedicated Entra ID tenant ensured that all identities and access policies were isolated, centralized, and securely managed, preventing conflicts with external environments.

Azure Role-Based Access Control (RBAC) was used to enforce **least privilege access**, ensuring that users and service accounts had only the permissions necessary for their roles. Group-based RBAC simplified permission management by assigning roles to groups rather than individual users, reducing administrative overhead and improving governance.

Segmentation of resources into distinct resource groups further strengthened access control, limiting the potential impact of misconfigured permissions. Together, these IAM measures provided a robust foundation for secure operations, compliance, and risk reduction. Group-based RBAC significantly reduced administrative risk and improved auditability. The assessment highlighted the importance of continuous access reviews to prevent privilege creep.

## 15.2 Monitoring, Logging & Visibility

Effective monitoring and logging are critical for maintaining visibility into cloud operations and identifying potential security threats. During the sprint, Azure-native tools such as **Azure Monitor** and **Log Analytics** were leveraged to collect telemetry and generate actionable insights across resources.

Data Collection Rules (DCRs) were implemented to define what data is captured from virtual machines, applications, and network resources. This allowed for fine-grained visibility into system events, security alerts, and operational metrics. Logs from multiple sources were collected to support analysis, auditing, and forensic investigations. By centralizing telemetry and logs, the team could monitor system health, track anomalous activity, and detect misconfigurations or potential attacks in near real-time. This approach ensures that security incidents can be investigated quickly, reducing response times and improving overall cloud security posture.

## 15.3 Threat Protection & Security Posture Management

Maintaining a strong security posture requires continuous monitoring and proactive threat protection. During the sprint, Microsoft Defender for Cloud (Servers Plan 2) was deployed to safeguard both Azure and hybrid workloads. This service provided vulnerability assessments, endpoint protection, and behavior-based threat detection, going beyond basic recommendations to actively detect potential attacks.

By combining automated threat detection with proactive posture management, the environment remained resilient against known and emerging threats, ensuring that risks were minimized and compliance requirements were maintained. Just-in-Time VM access reduced attack surfaces for critical servers

## 15.4 Attack Surface Reduction

Reducing the attack surface is critical to minimizing potential entry points for threats. During the cloud security sprint, strategies were implemented to limit exposure across Azure resources. This included segmentation of resource groups, enforcement of least-privilege access through RBAC, and just-in-time (JIT) VM access. By restricting unnecessary permissions, closing unused ports, and applying security policies consistently, the environment was hardened against unauthorized access and potential exploits. Continuous monitoring and automated alerts ensured that any deviations from security baselines were promptly detected and addressed, further reducing risk.

These measures collectively strengthened the overall security posture, making it more difficult for attackers to gain footholds in the environment.

## 15.5 Detection, Incident Response & Automation

Detection, incident response, and automation are critical components of a resilient cloud security strategy. During the sprint, Microsoft Sentinel served as the central SIEM and SOAR platform, providing real-time visibility into security events across Azure resources. Sentinel's advanced analytics allowed the team to correlate events from multiple sources, identify anomalies, and prioritize alerts based on risk.

Integration with Azure Monitor, Log Analytics, and Logic Apps enabled automated response workflows.Additionally, the sprint highlighted the importance of continuous monitoring and telemetry collection, allowing for proactive threat hunting and the ability to anticipate potential security incidents before they escalate. By combining detection, automation, and structured incident response, the environment demonstrated a proactive and scalable approach to maintaining security, resilience, and operational continuity in Azure.

# 16.0 Strategic Risk Insights

Strategic risk insights involve identifying, assessing, and prioritizing potential threats to the organization's cloud environment at a high level. During the sprint, data collected from Microsoft Sentinel, Azure Monitor, and Defender for Cloud provided visibility into recurring patterns, vulnerabilities, and misconfigurations across resources. These insights help security teams and executives understand which risks could have the most significant operational, financial, or reputational impact.

They include that;

- Excessive privileges remain a high-impact risk without continuous governance.
- Centralized visibility is critical for early threat detection.
- Automation is essential for scalable cloud security operations.
- Advanced capabilities require appropriate licensing and skilled configuration.

# 17.0 Executive Recommendations

**1. Enforce Least-Privilege Access**

- Continuously review roles and privileges in Microsoft Entra ID and Azure RBAC.
- Remove unnecessary permissions and enforce group-based access to reduce risk.
- Implement automated alerts for unusual or elevated access to catch potential misuse early.

**2. Strengthen Visibility & Monitoring**

- Centralize log collection from Azure Monitor, Log Analytics, and Microsoft Sentinel.
- Use dashboards and alerts to detect suspicious activity and respond before incidents escalate.
- Regularly review audit logs and Data Collection Rules to ensure all resources are taken care of.

**3. Automate Security Operations**

- Deploy Logic Apps and Sentinel playbooks to automate repetitive tasks, such as account reviews, alert triaging, and remediation actions.
- Automation reduces human error, improves response times, and enables scalable security management across large cloud environments.

4. **Leverage Advanced Security Features**

- Ensure appropriate licensing for Microsoft Defender for Cloud Plan 2 and Sentinel to access threat detection, vulnerability assessments, and endpoint protection.
- Train security teams to configure these tools effectively, ensuring behavioral alerts, JIT VM access, and attack surface reduction are properly implemented.

5. **Regularly Review & Harden Resources**

- Segment resource groups and enforce conditional access policies to isolate sensitive workloads.
- Limit the number of privileged accounts and implement credential rotation policies.
- Conduct periodic security posture assessments to identify misconfigurations or gaps and remediate them promptly.

6. Standardize security governance across subscriptions.
7. Invest in continuous cloud security skills development.

# 18.0 Conclusion

This Enterprise Cloud Security Assessment demonstrates that Cyberinfiniti Ltd can achieve a resilient and scalable cloud security posture by fully leveraging Microsoft Azure's integrated security capabilities. When supported by governance, automation, and skilled operations, these controls provide meaningful risk reduction and executive confidence in secure cloud adoption.

The assessment highlighted several key areas critical to maintaining security in the cloud: effective Identity and Access Management, continuous Monitoring and Logging, robust Threat Protection and Security Posture Management, proactive Attack Surface Reduction, and efficient Detection, Incident Response, and Automation. Implementing best practices in these areas ensures that excessive privileges are minimized, threats are detected early, and resources are managed securely.

By adopting the tailored recommendations outlined in this report, Cyberinfiniti Ltd can strengthen its cloud defenses, streamline security operations, and maximize the value of Azure-native security tools such as Microsoft Entra ID, Azure RBAC, Microsoft Defender for Cloud, and Microsoft Sentinel. With continuous improvement and adherence to these practices, the organization can confidently scale its cloud infrastructure while maintaining a secure and compliant environment.

# References

AZ500-Azure Security Technology
MicrosoftLearning. (n.d.). *AZ500-AzureSecurityTechnologies - Allfiles/Labs/08* [Repository]. GitHub. Retrieved February 2026, from https://github.com/MicrosoftLearning/AZ500-AzureSecurityTechnologies/tree/master/Allfiles/Labs/08

Microsoft Azure Documentation
Microsoft. (n.d.). *Azure documentation - product docs, tutorials & guides*. Microsoft Learn. Retrieved February 2026, from https://learn.microsoft.com/azure/

# Appendix A: Sprint Timeline & Meetings

| **Dates** | **Times** | **Attendees** |
|---|---|---|
| 2nd-Feb -2026 | 8:10 pm | John Ofulue, Halimat Omorinsola Adepegba, Favour Obisike, Ikenna Emerole, Blessing Ibe, Ayodimeji Omole, Divine Ezewele, Andrew Moses, Odunayo Balogun |
| 3rd-Feb-2026 | 8:10 pm | John Ofulue, Halimat Omorinsola Adepegba, Favour Obisike, Ikenna Emerole, Blessing Ibe, Ayodimeji Omole, Divine Ezewele, Andrew Moses, Odunayo Balogun |
| 4th-Feb-2026 | 8:10 pm | John Ofulue, Halimat Omorinsola Adepegba, Favour Obisike, Ikenna Emerole, Blessing Ibe, Ayodimeji Omole, Divine Ezewele, Andrew Moses, Odunayo Balogun |
| 5th-Feb-2026 | 8:10 pm | John Ofulue, Halimat Omorinsola Adepegba, Favour Obisike, Ikenna Emerole, Blessing Ibe, Divine Ezewele, Andrew Moses, Odunayo Balogun |
| 6th-Feb-2026 | 8:10 pm | John Ofulue, Halimat Omorinsola Adepegba, Favour Obisike, Ikenna Emerole, Blessing Ibe, Ayodimeji Omole, Divine Ezewele, Andrew Moses, Odunayo Balogun |
| 7th-Feb-2026 | 8:10 pm | John Ofulue, Halimat Omorinsola Adepegba, Favour Obisike, Ikenna Emerole, Blessing Ibe, Ayodimeji Omole, Divine Ezewele, Andrew Moses, Odunayo Balogun |

# Appendix B: Team Contributions

| **Names** | **Roles and Responsibilities** |
|---|---|
| John Ofulue | Team lead, assigned tasks, helped with the technical walkthrough of the labs in Azure, and with the report. |
| Halimat Omorinsola Adepegba | Assistant Team Lead. Helped with the presentation slides and also contributed during the labs |
| Favour Obisike | Worked on lab 7,8 and 9 and contributed during the lab report |
| Ikenna Emerole | Compiled and modified the team's report and also contributed during the labs |
| Blessing Ibe | Compiled and modified the report, created Appendix A and B, and also contributed during the labs |
| Ayodimeji Omole | Worked on the presentation slides and also contributed during the labs |
| Divine Ezewele | Worked on lab 5 and contributed during the labs |
| Andrew Moses | Responsible for presenting our task and also contributed during the labs |

| | |
|---|---|
| Odunayo Balogun | Assisted Moses in presenting our task and also contributed during the labs |