Azure Home Lab

In this lab, I set up a basic home SOC in Azure from scratch. Using a free Azure subscription, I walk through creating a virtual machine (VM), opening it to the internet as a honeypot, and forwarding logs to a central repository. I then integrate Microsoft Sentinel to analyse real-world attack data.

In this lab I cover the following:

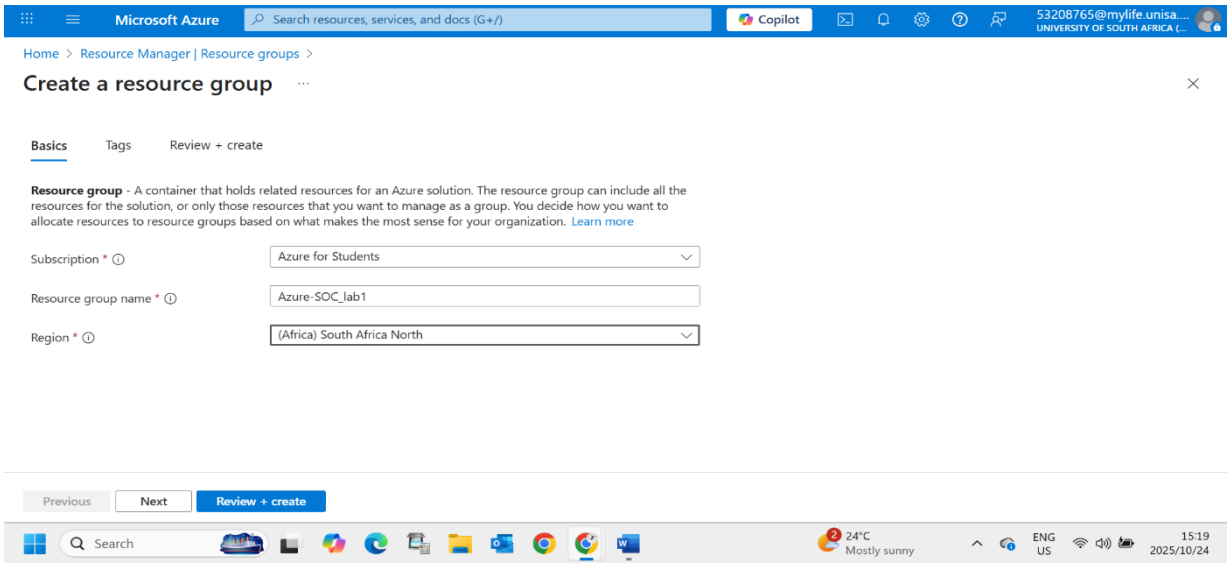
- Creating an Azure subscription and setting up a VM
- Configuring Log Analytics Workspace
- Forwarding logs and integrating with Sentinel
- Querying failed login attempts and visualizing attack sources
- Building an attack map to track real-time hacker activity

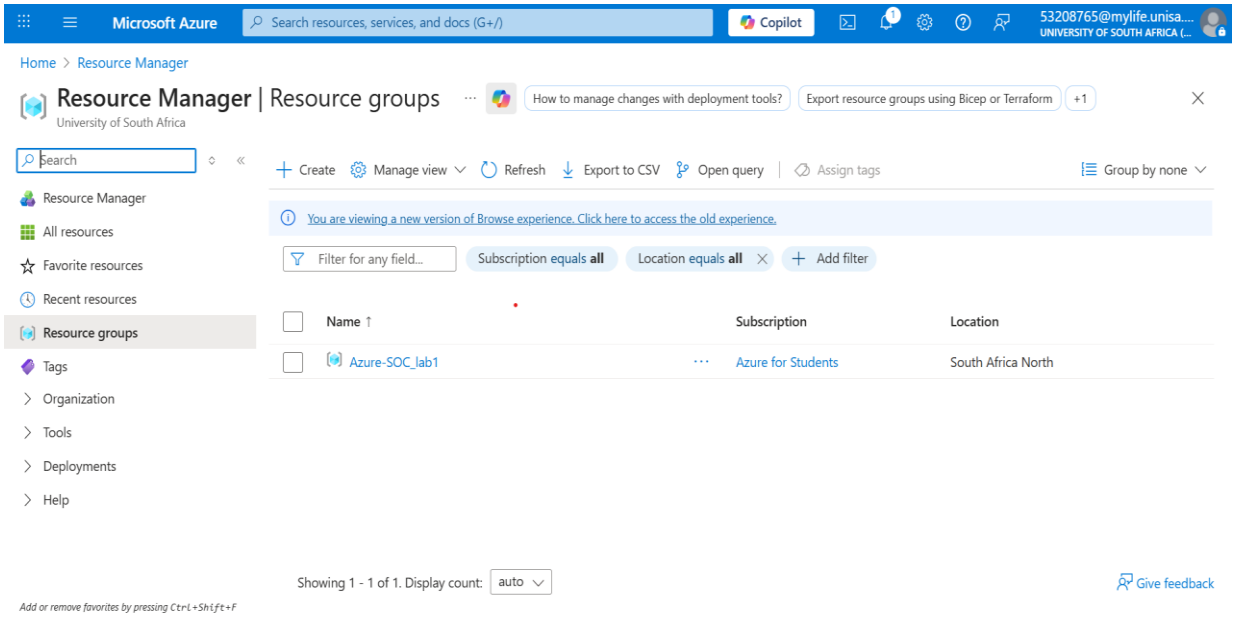
This project is great for cybersecurity personnel, like myself, looking to practice log analysis, threat detection, and SOC operations in a real-world cloud environment.

<u>The initial steps will encompass the setting up of all the resources I need for this lab.</u>

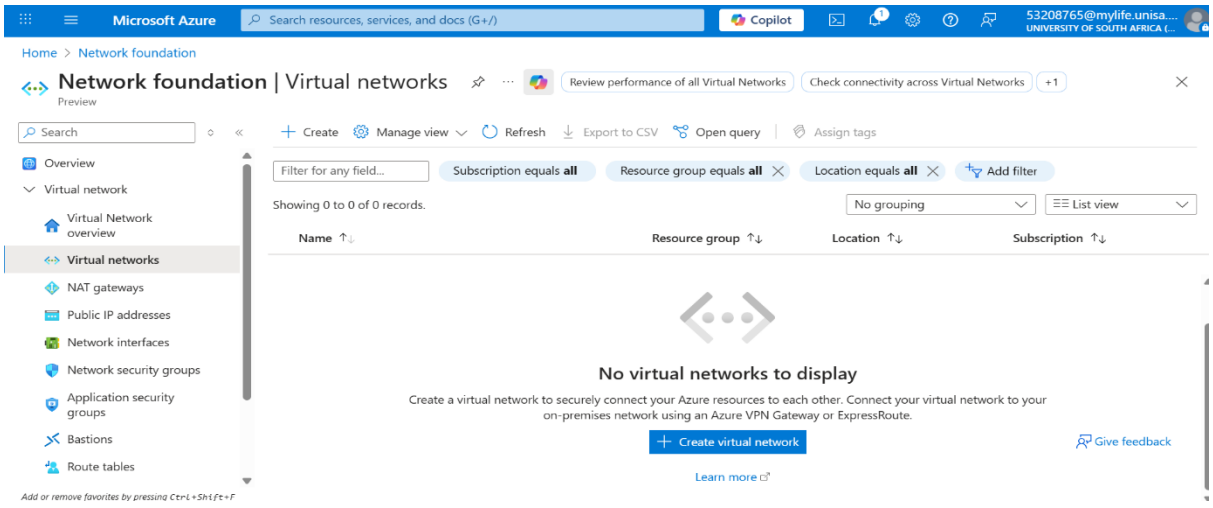
Step 1:

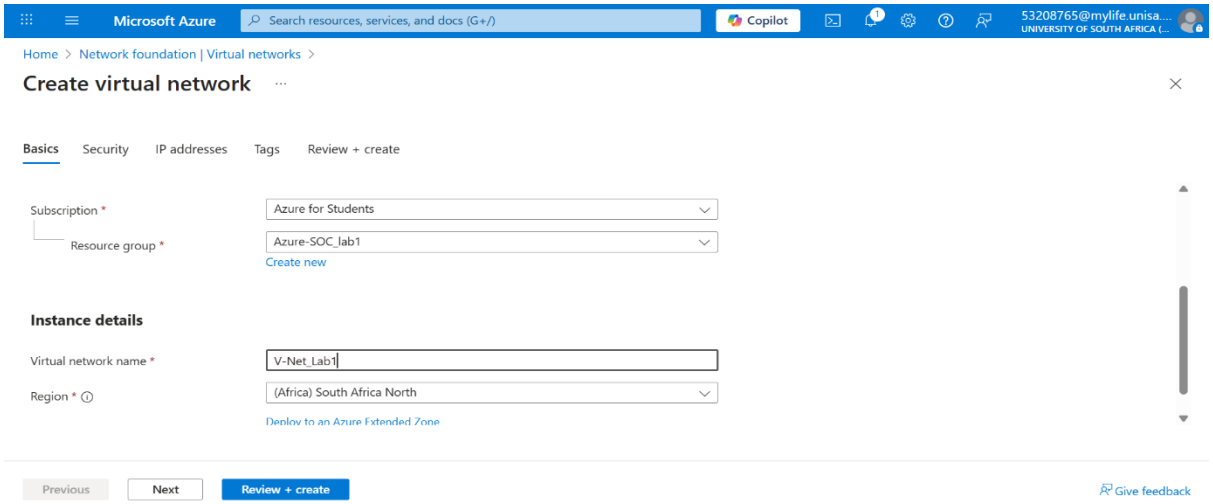
After signing up for my Azure free tier account, the first step is to create a **Resource Group** within the Azure portal. The Resource Group will house all my resources for this lab.

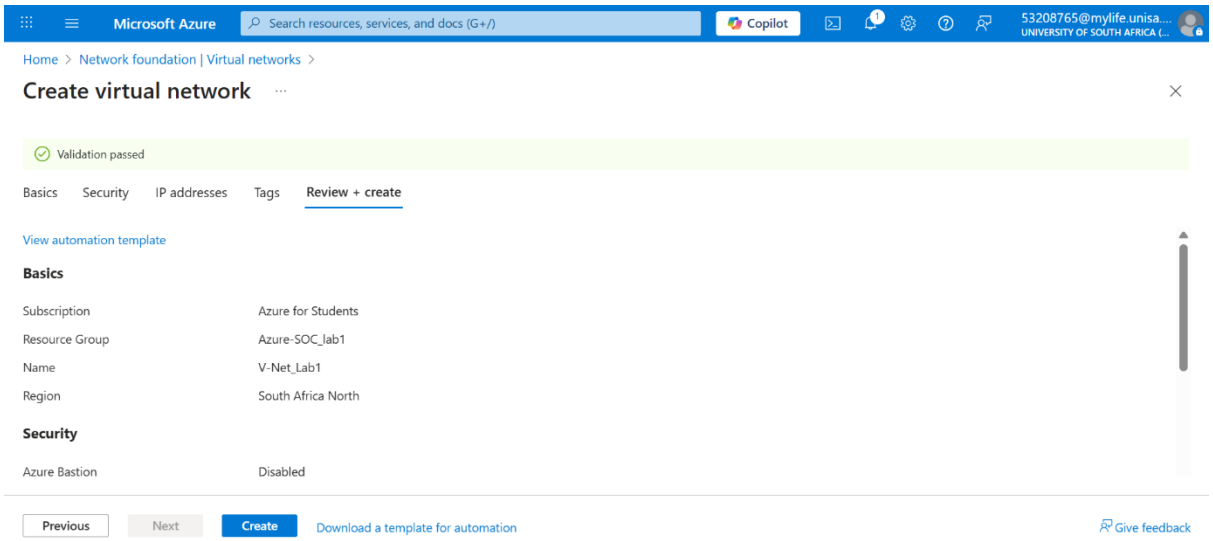


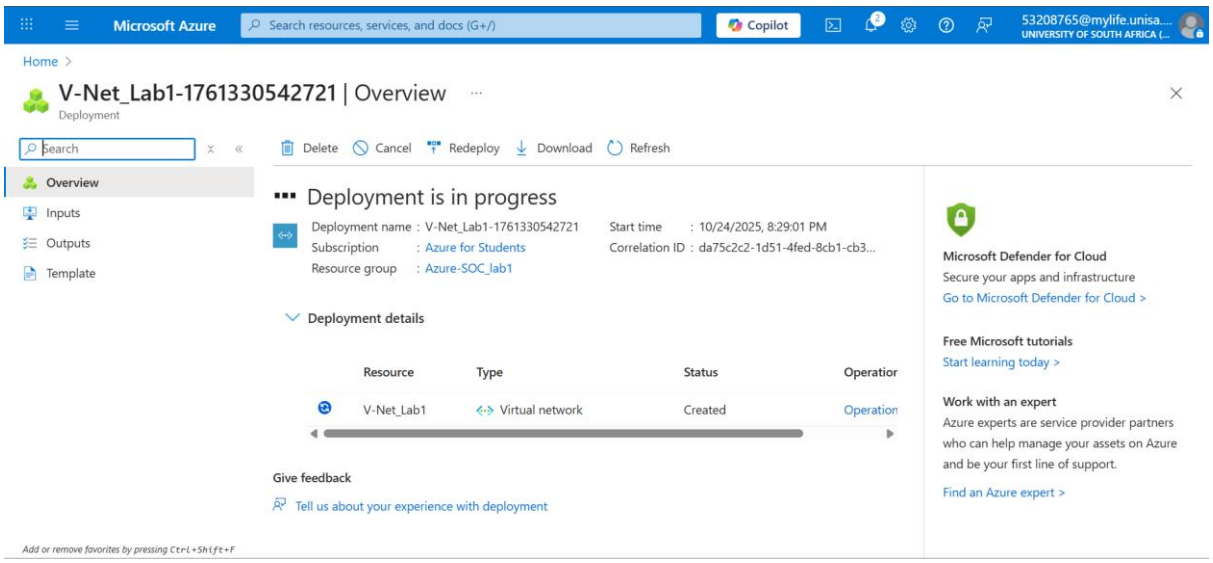


Next, I created a **Virtual Network.** In essence, a virtual network uses software to create and manage a virtual version of a physical computer network. This allows devices to communicate with each other over the internet or a cloud infrastructure, offering greater flexibility and scalability than traditional hardware-based networks.

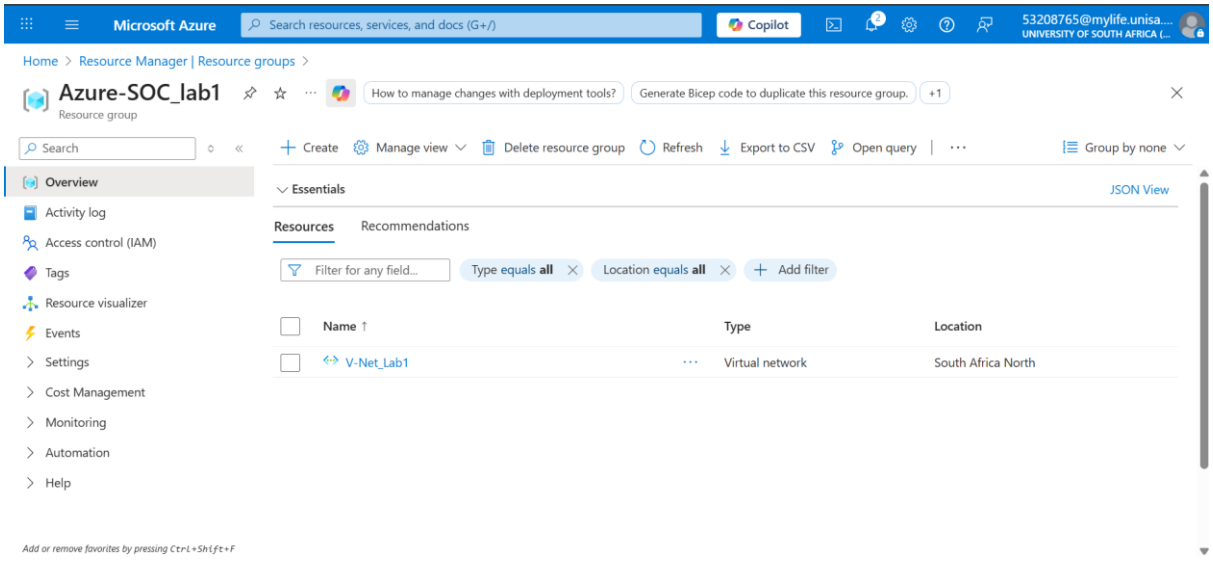



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
53208765@mylife.unisa....
UNIVERSITY OF SOUTH AFRICA (...
Home > Network foundation | Virtual networks >
Create virtual network
Basics Security IP addresses Tags Review + create
Subscription *
Azure for Students
Resource group *
Azure-SOC_lab1
Create new
Instance details
Virtual network name *
V-Net_Lab1
Region *
(Africa) South Africa North
Deploy to an Azure Extended Zone
Previous
Next
Review + create
Give feedback

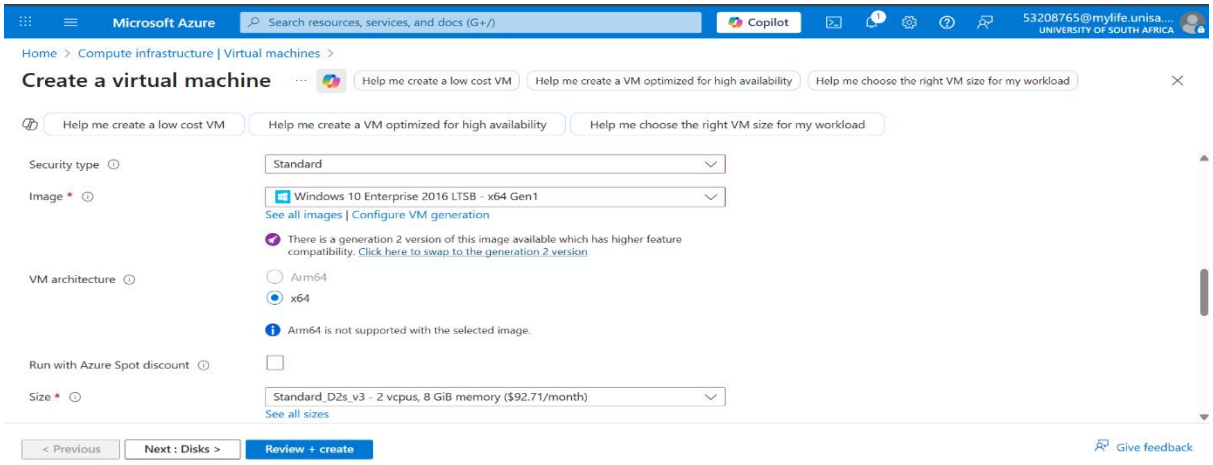

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
53208765@mylife.unisa....
UNIVERSITY OF SOUTH AFRICA (...
Home > Network foundation | Virtual networks >
Create virtual network
Validation passed
Basics Security IP addresses Tags Review + create
View automation template
Basics
Subscription Azure for Students
Resource Group Azure-SOC_lab1
Name V-Net_Lab1
Region South Africa North
Security
Azure Bastion Disabled
Previous
Next
Create
Download a template for automation
Give feedback

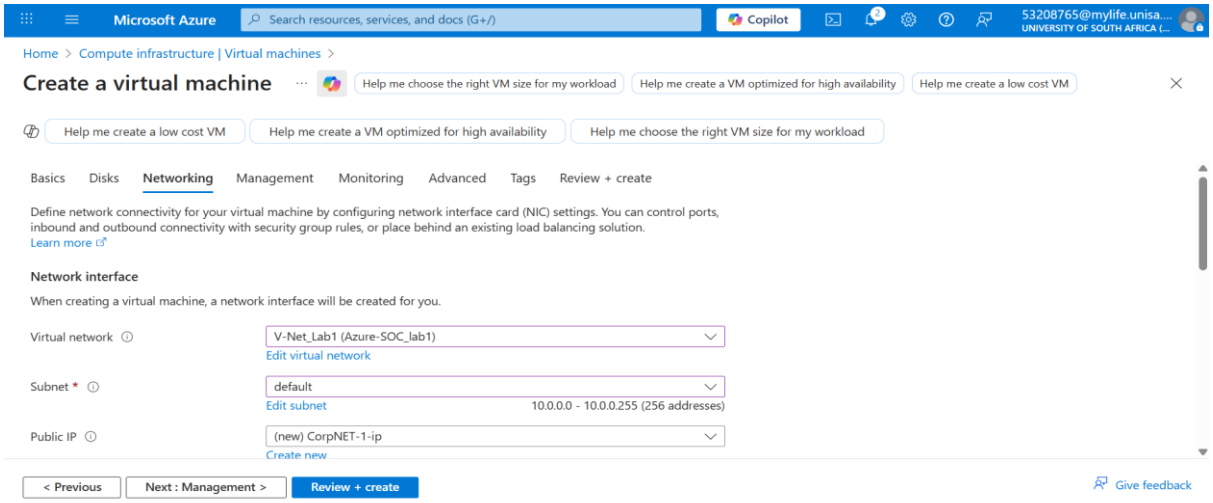

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
53208765@mylife.unisa....
UNIVERSITY OF SOUTH AFRICA (...
Home >
V-Net_Lab1-1761330542721 | Overview
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Deployment is in progress
Deployment name : V-Net_Lab1-1761330542721
Subscription : Azure for Students
Resource group : Azure-SOC_lab1
Start time : 10/24/2025, 8:29:01 PM
Correlation ID : da75c2c2-1d51-4fed-8cb1-cb3...
Deployment details
Resource
Type
Status
Operation
V-Net_Lab1
Virtual network
Created
Operation
Give feedback
Tell us about your experience with deployment
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >
Add or remove favorites by pressing Ctrl+Shift+F

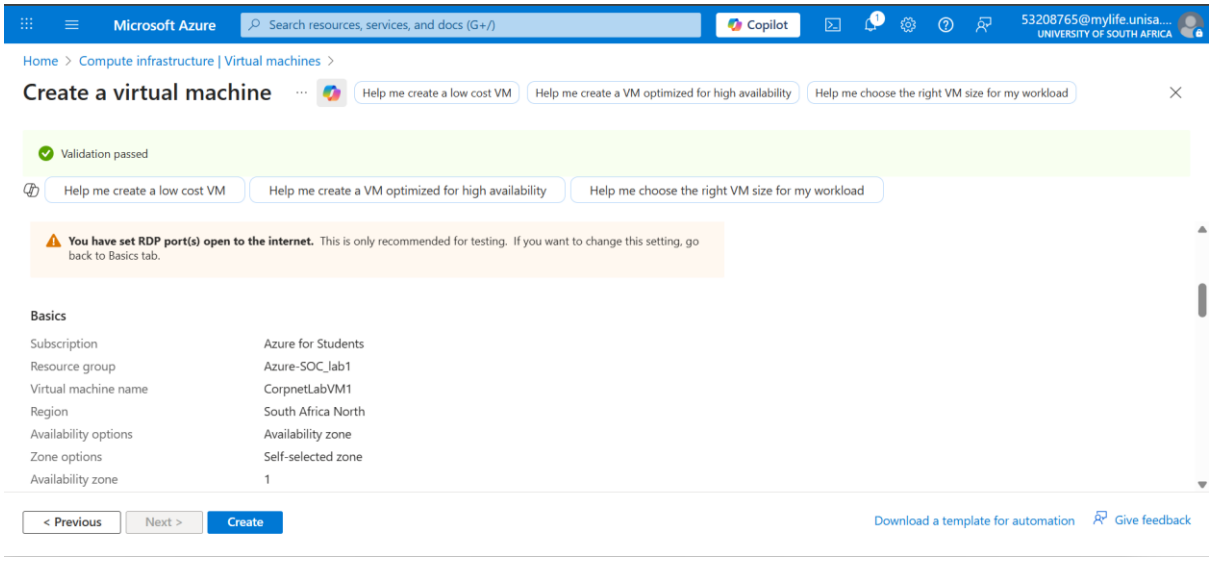
Below, you will notice that my **Virtual Network** has been created within my **Resource Group.**

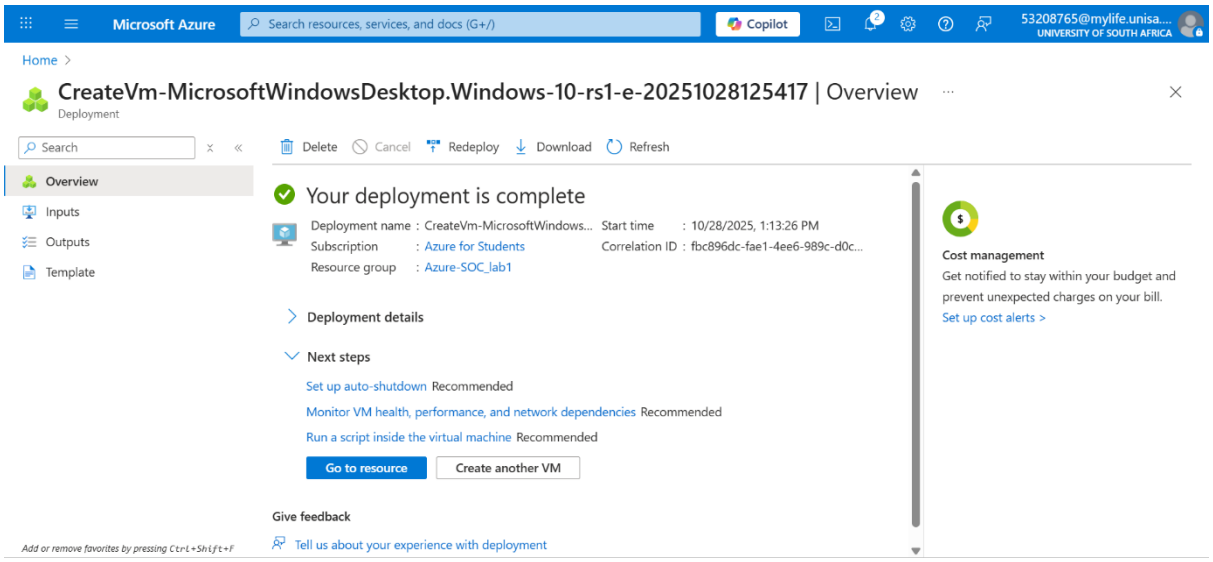


Next, I will create a **Virtual Machine** which will act as the **honey pot**. In cybersecurity, a **honey pot** is a decoy system set up to attract and trap cyber attackers.

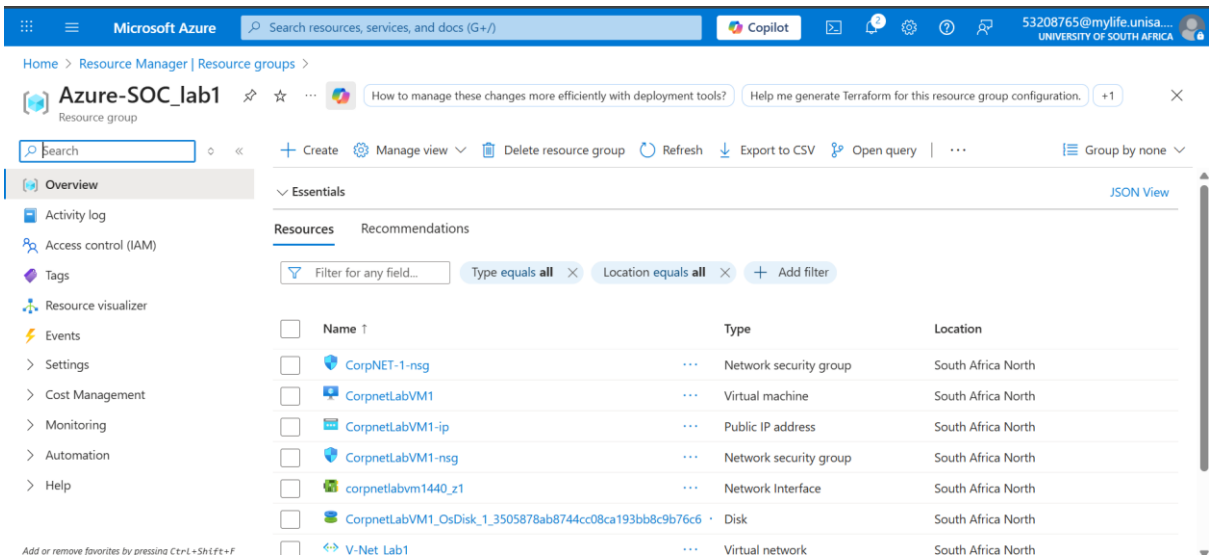






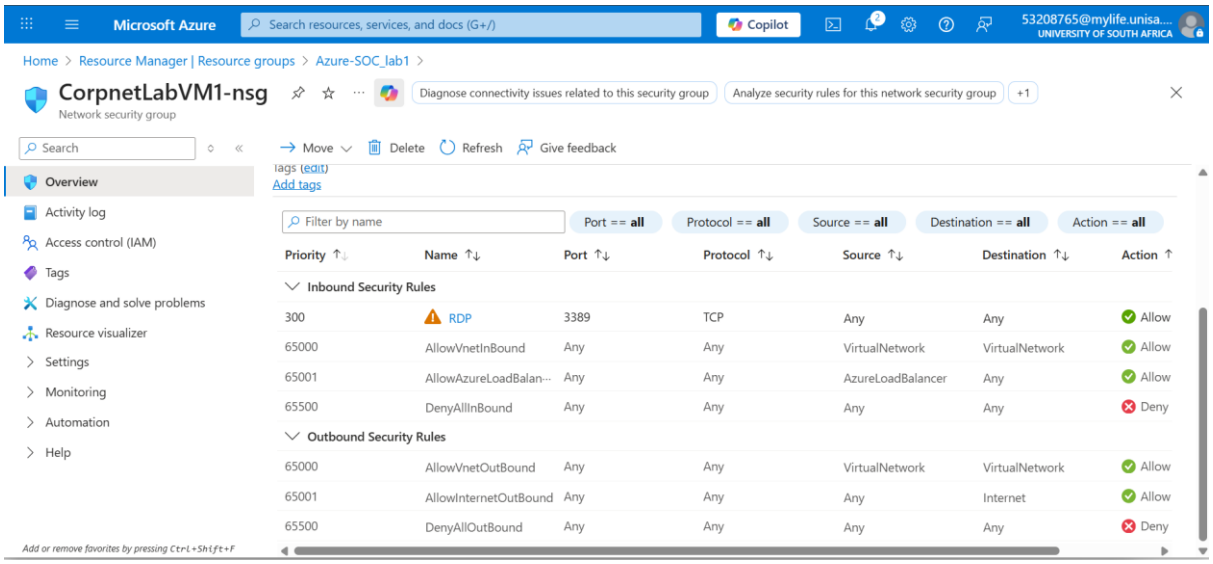


After successful deployment I went to my **Resource Group** to confirm that everything is in order.

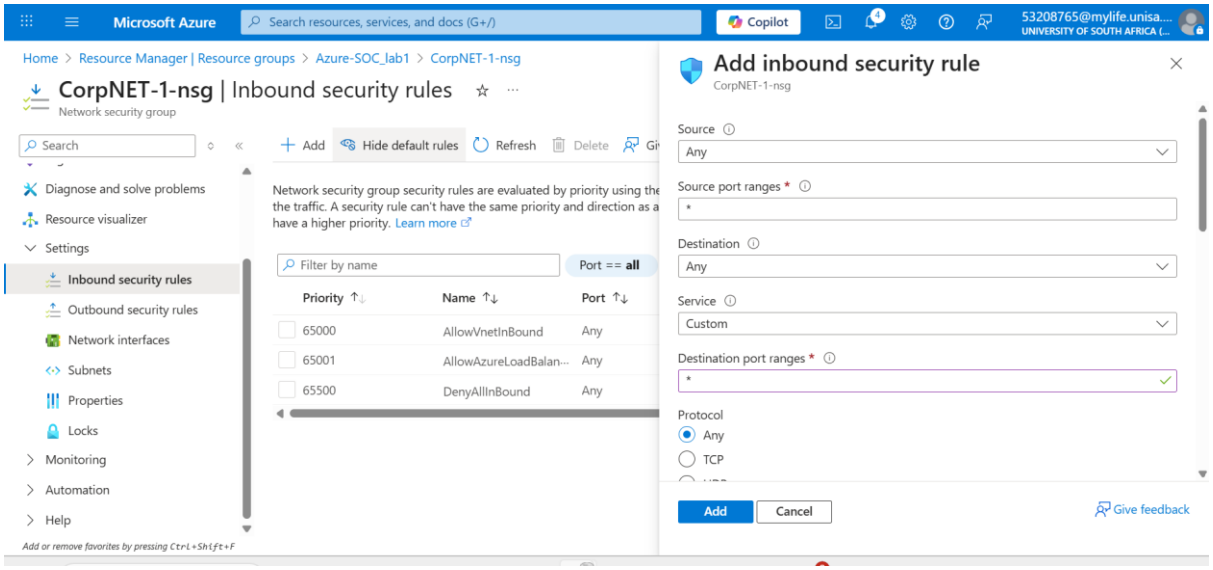


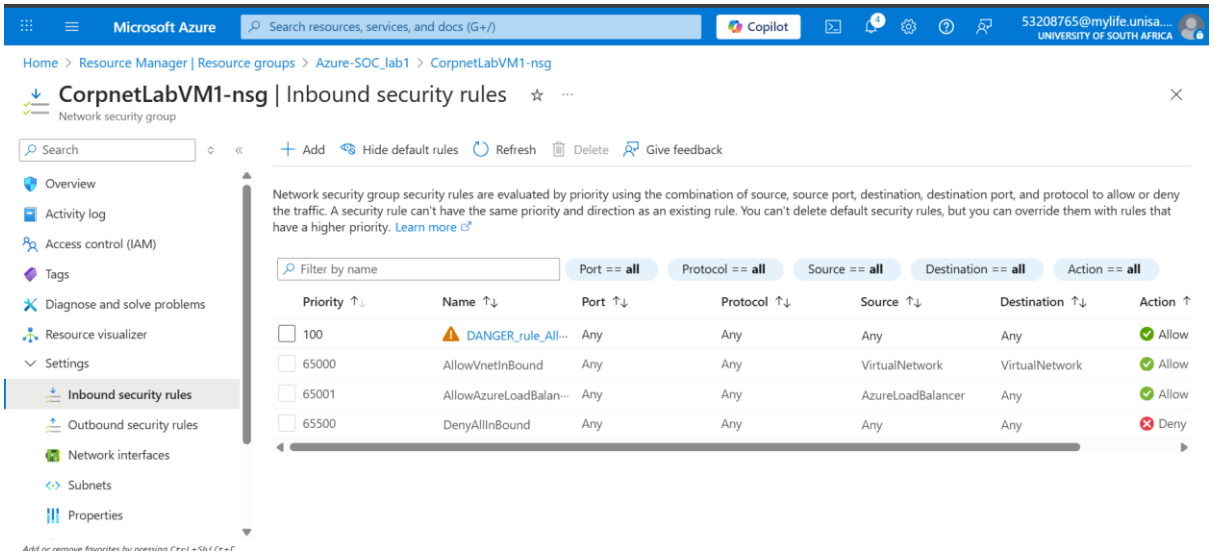
Step 2

Now that my initial resources have been created, I will edit my **Network Security Group** and open it up to the internet. I do this so that my network is accessible from all traffic and make it discoverable to potential attackers as part of the honey trap.



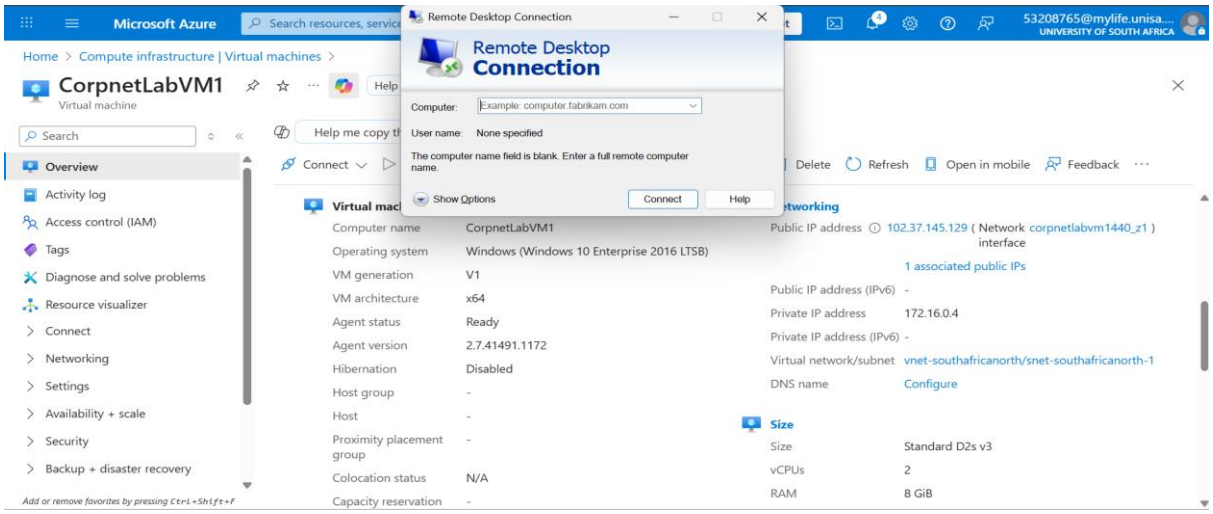
I continued to delete my default **Remote Desktop Protocol (RDP)** inbound rule and create a new inbound rule that allows all inbound traffic.

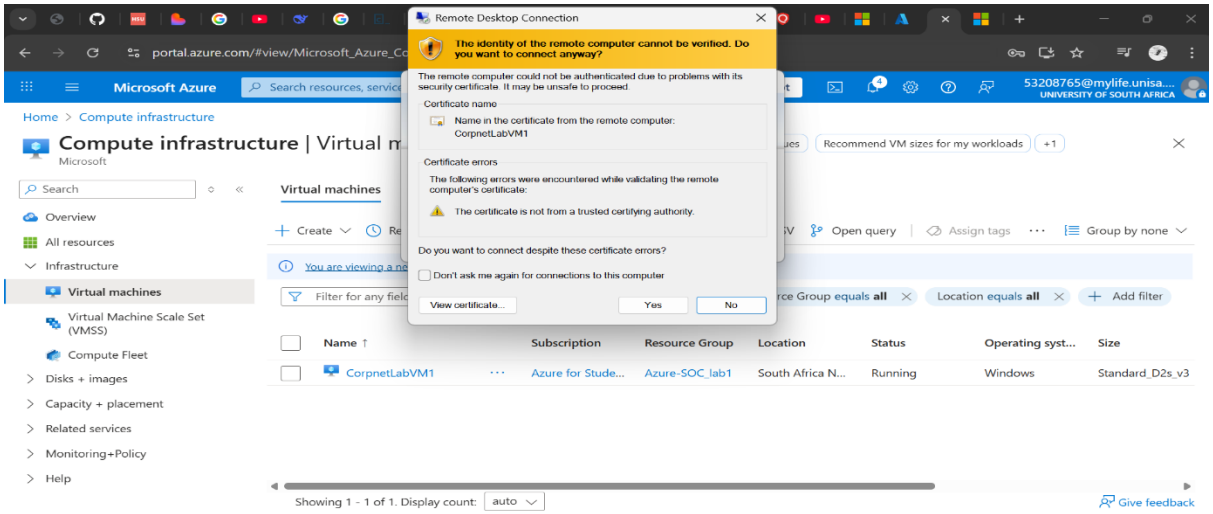




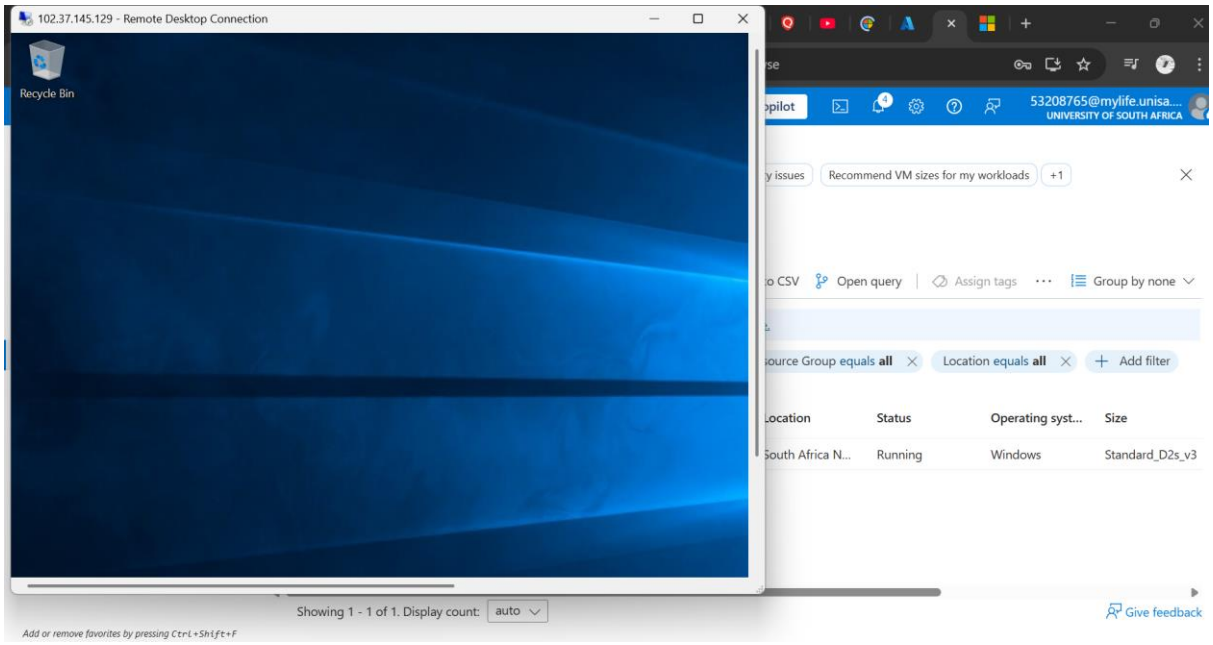
Step 3

I proceeded to my Virtual Machine (VM) to disable the internal Windows Firewall. I start this process by first remote connecting my Virtual Machines Public IP Address.

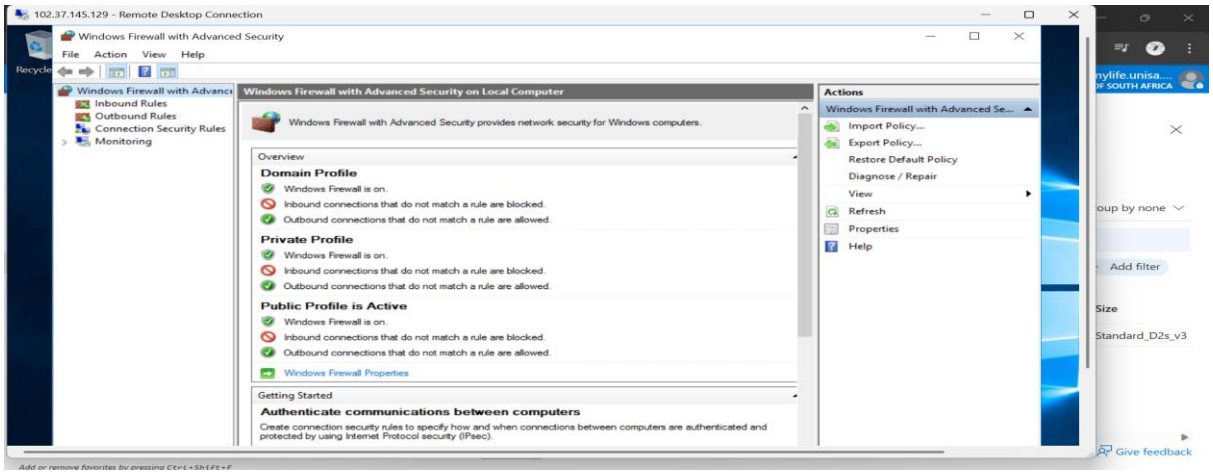


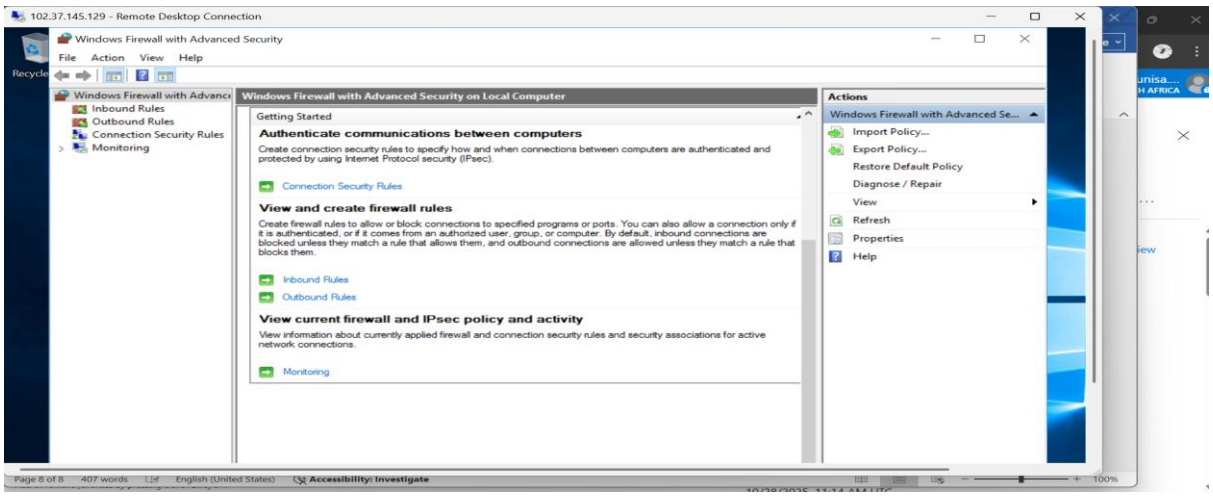


I have successfully connected to my Windows Virtual Machine.

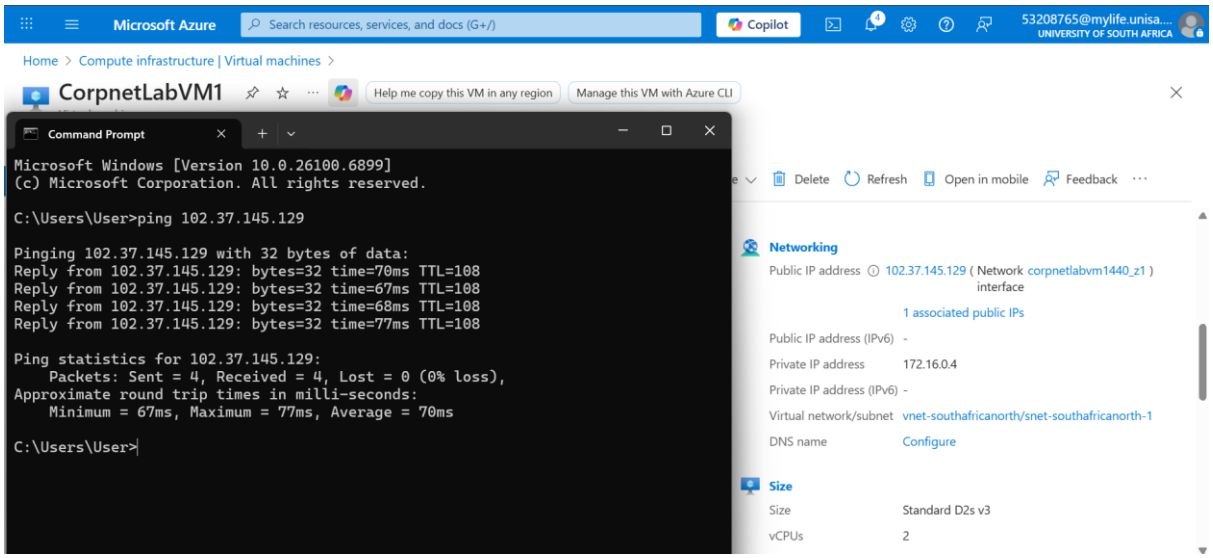


The next step was to turn off the **Windows Firewall** (VM) for my Virtual Machine.



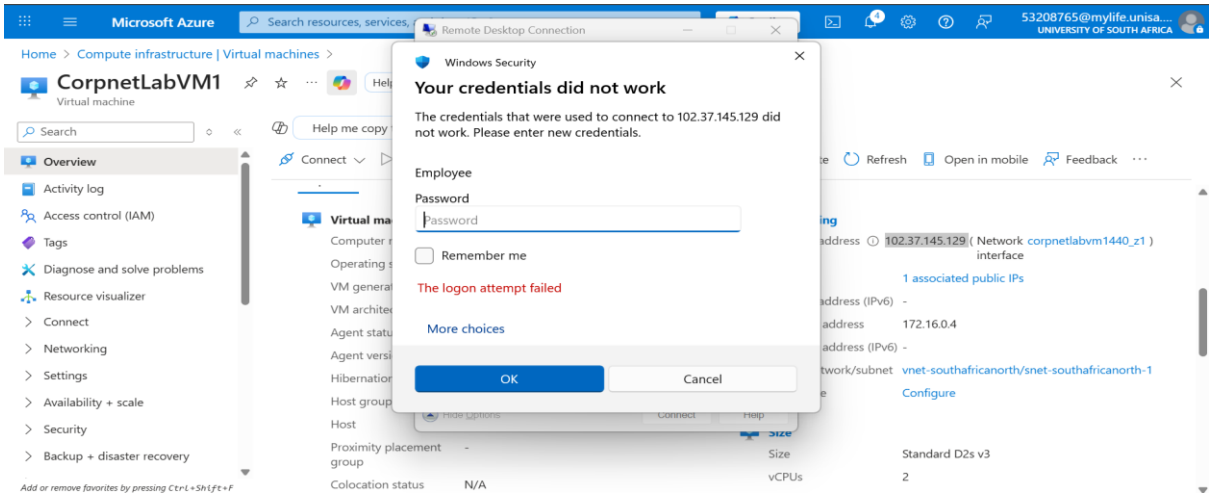


I attempted to **ping** my VM, the **ping** was successful.

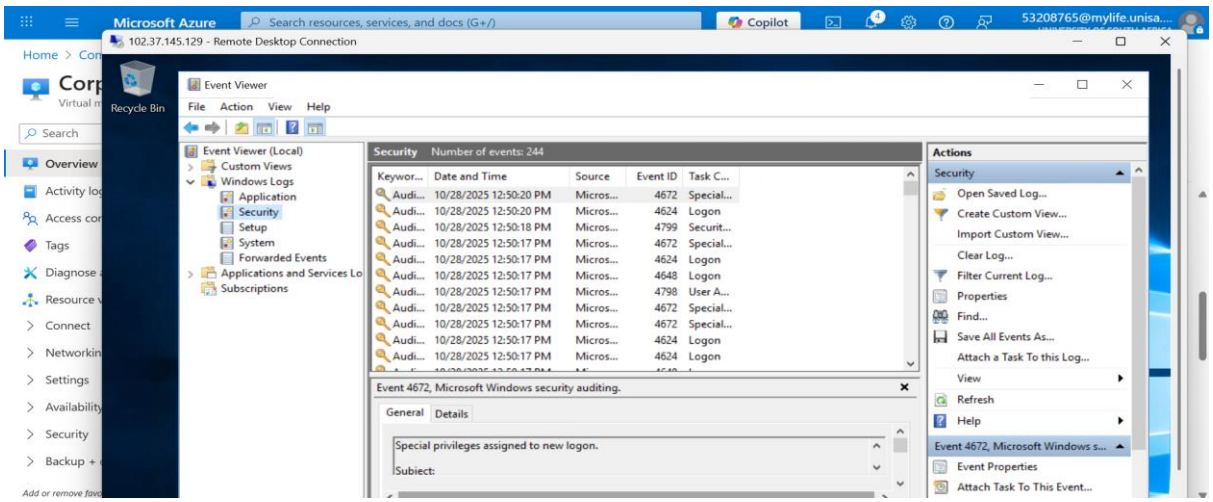


Step 4

In this step, I'll review some raw logs from my VM. I started off by purposely attempting to log into the virtual machine using **incorrect** signing in **credentials**.

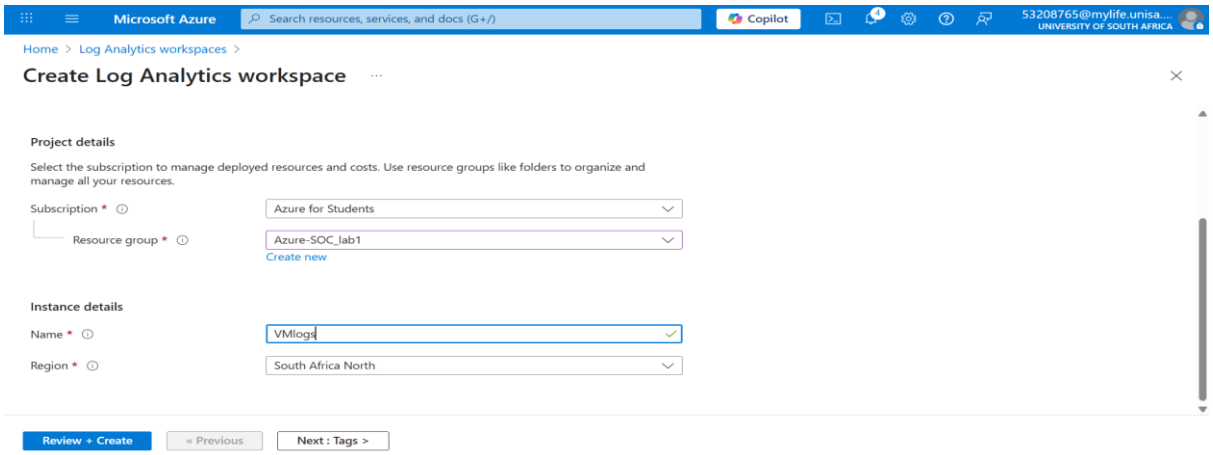


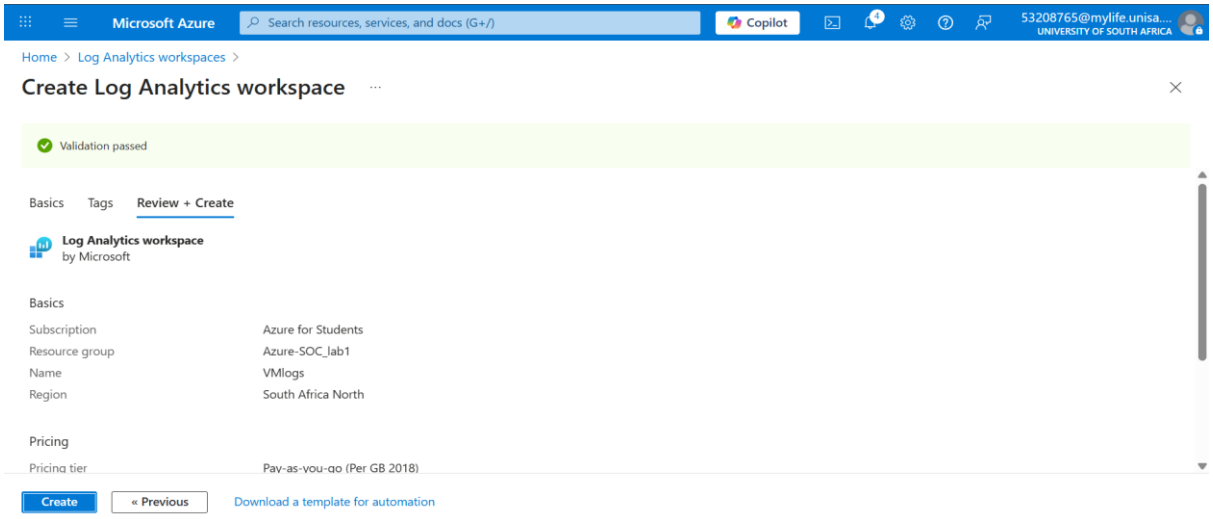
Below is the log with "all' the security events that place on the virtual machine.

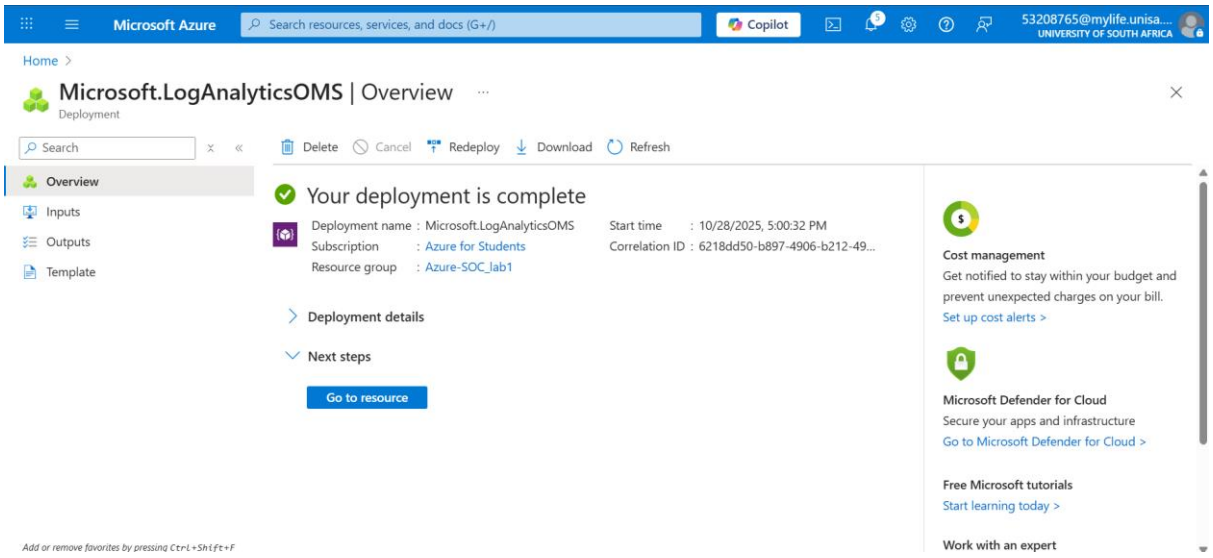


Step 5

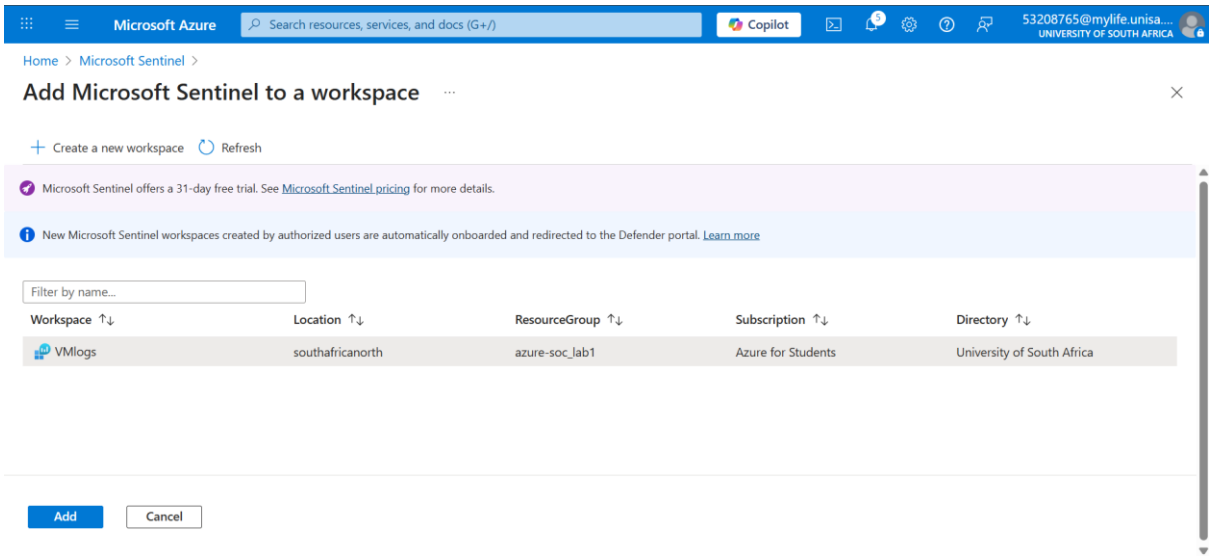
Next, as I wait for potential attackers to try attack my VM, I'll configure a **Log Repository** in Azure and forward my VM logs into it.



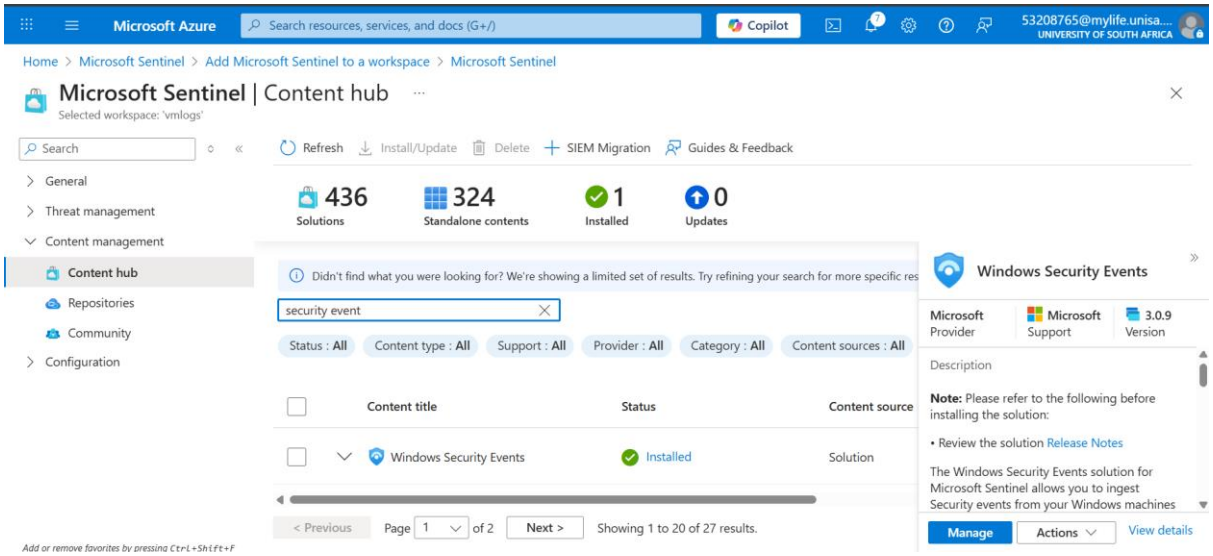




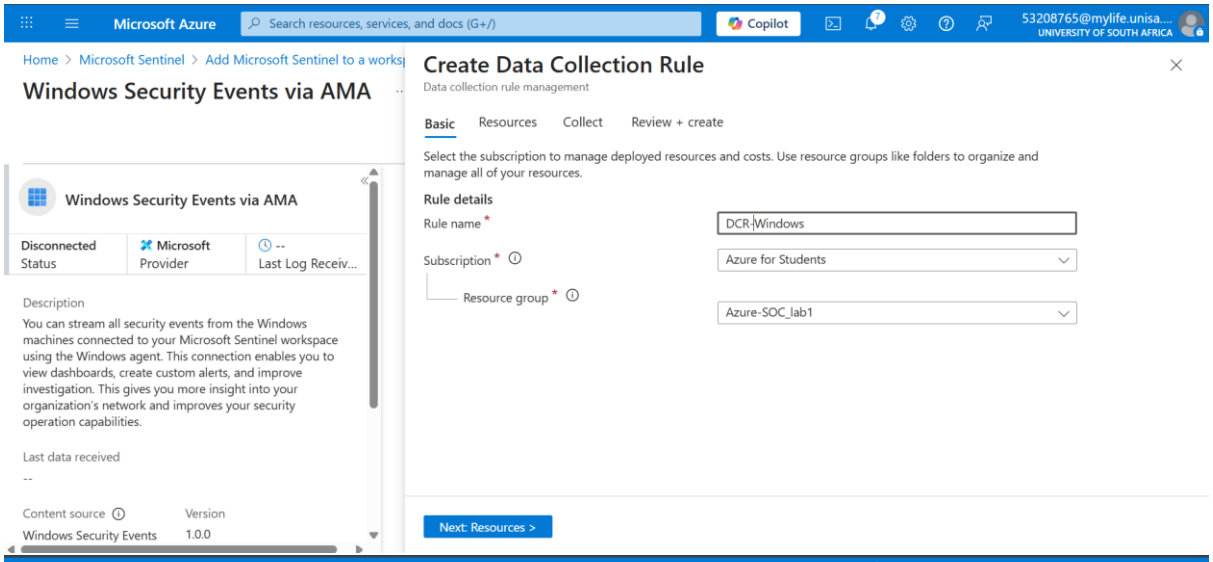
Next up, I create my **Sentinel** Instance and link my VM logs to the **Sentinel** workspace. Microsoft Sentinel a cloud-native security information and event management **(SIEM**) and security orchestration, automation, and response **(SOAR)** platform that provides a unified view of your organization's security posture. It uses AI and machine learning to help detect, investigate, and respond to security threats across multi-cloud and on-premises environments by collecting and analysing data from various sources.

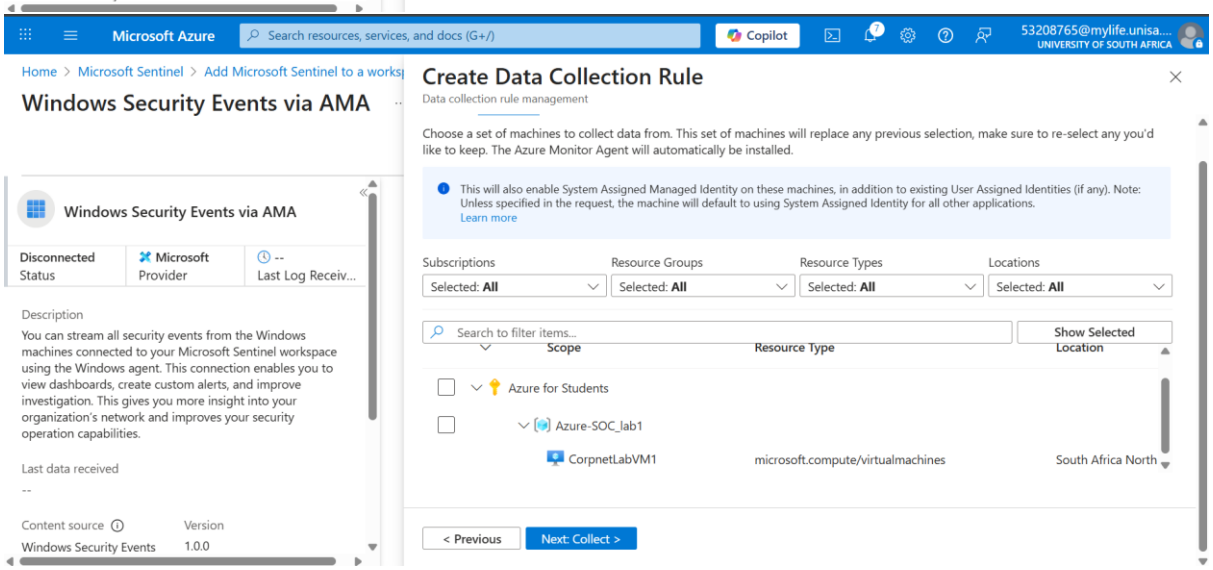


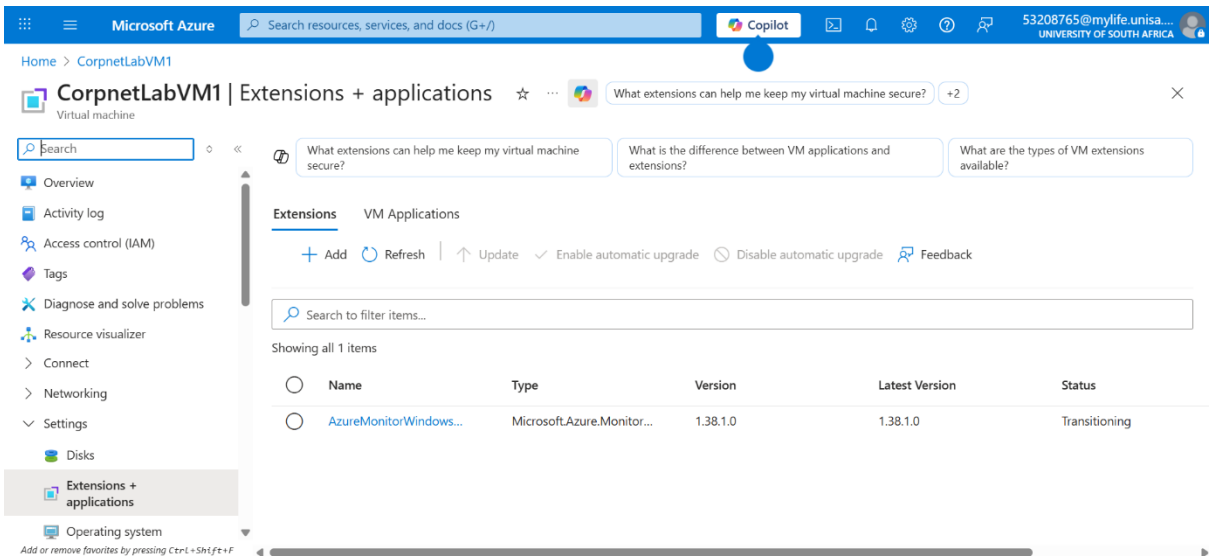
Below I install the **Windows Security Events** connector. **Microsoft security events** are logs of activities related to security in a Microsoft environment, including Windows operating systems and services. These events can include anything from successful or failed login attempts to file deletions, and they are collected to help detect threats, investigate incidents, and monitor security posture. They are also the data fed into platforms like Microsoft Sentinel, which analyses them to identify potential security breaches.



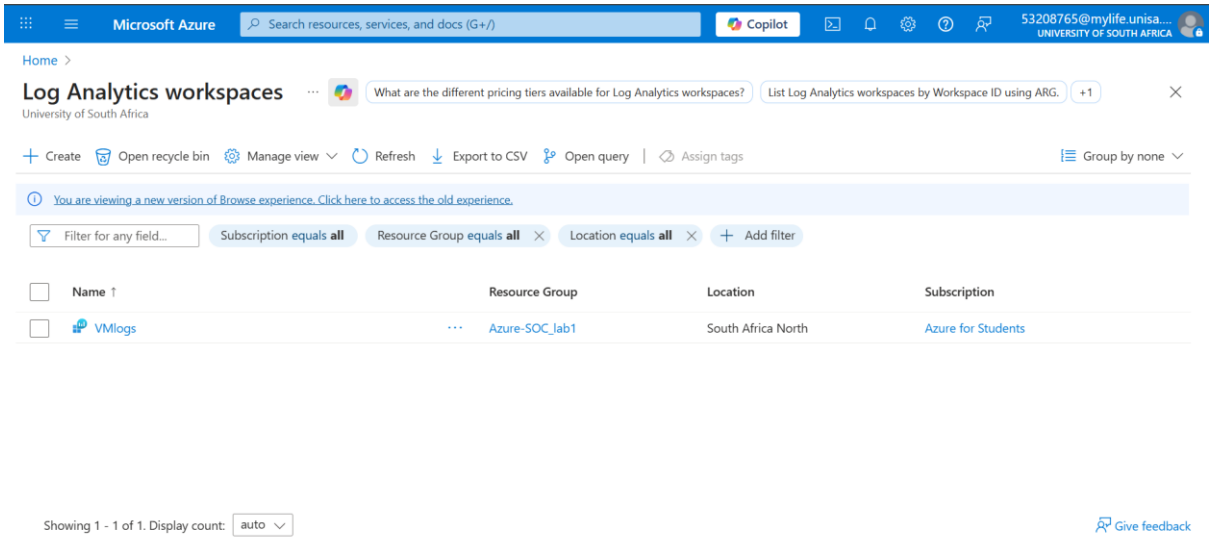
I also configured the connector page (**Windows Security Events via AMA)** via the **Create Data Collection Rule**. These rules govern the communication between my VM and the **Logs Analytics workspace**, this then allows me to access these logs in **Sentinel**.



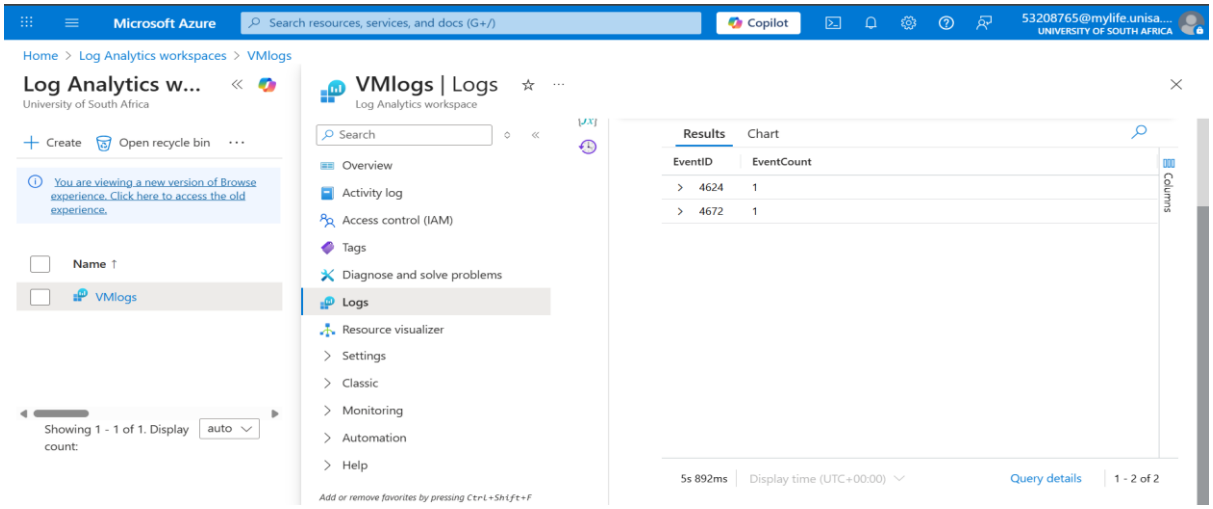


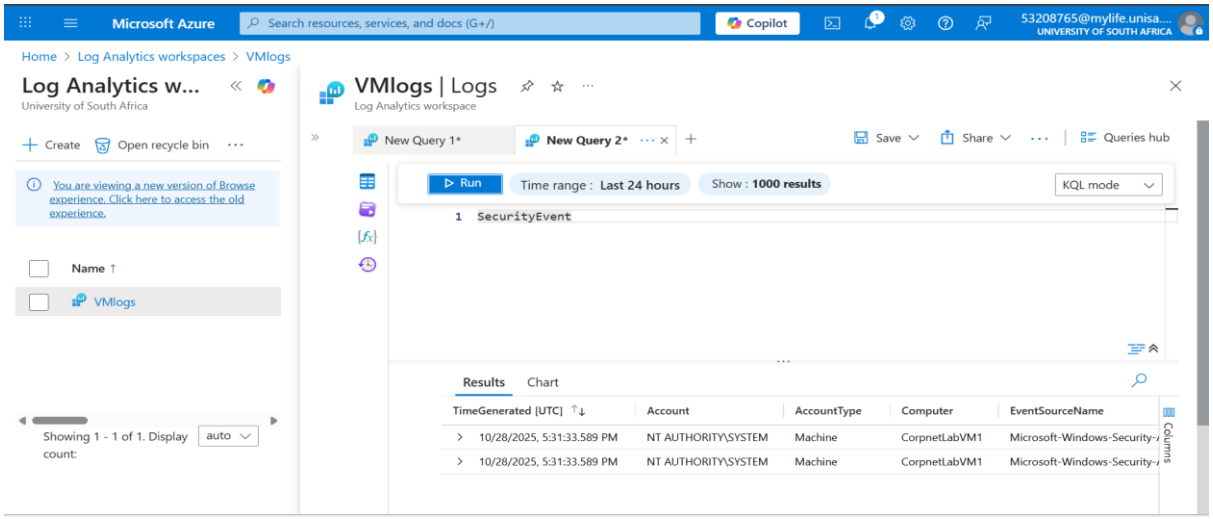


Successfully connected to my **Logs Analytics workspace**.

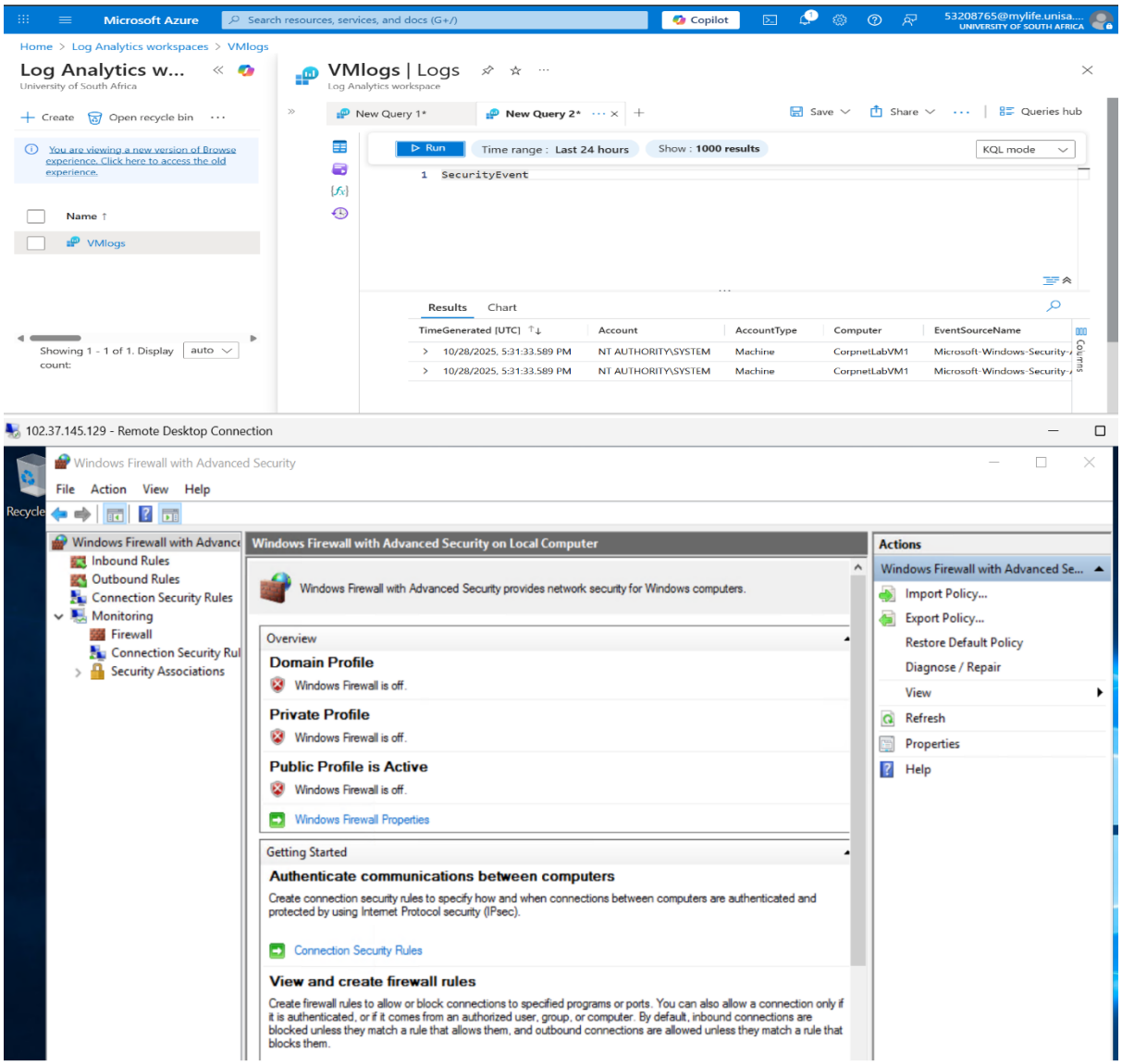


I ran a quick search (security event) to see which logs are being tracked. I went back to see the status of my connection and it was still transitioning. I then reattempted the search after the provisioning was successful in both **simple** and **KQL mode**





I expected to see more logs so I ran a ping and double checked my firewall settings on my VM. Everything seemed to be in order but for some reason my honey pot was not attracting any hits.



After two hours I came back to run the “SecurityEvent” **KQL** command, I got some positive results. Unfortunately, none of the log results were hackers attempting to enter my VM.