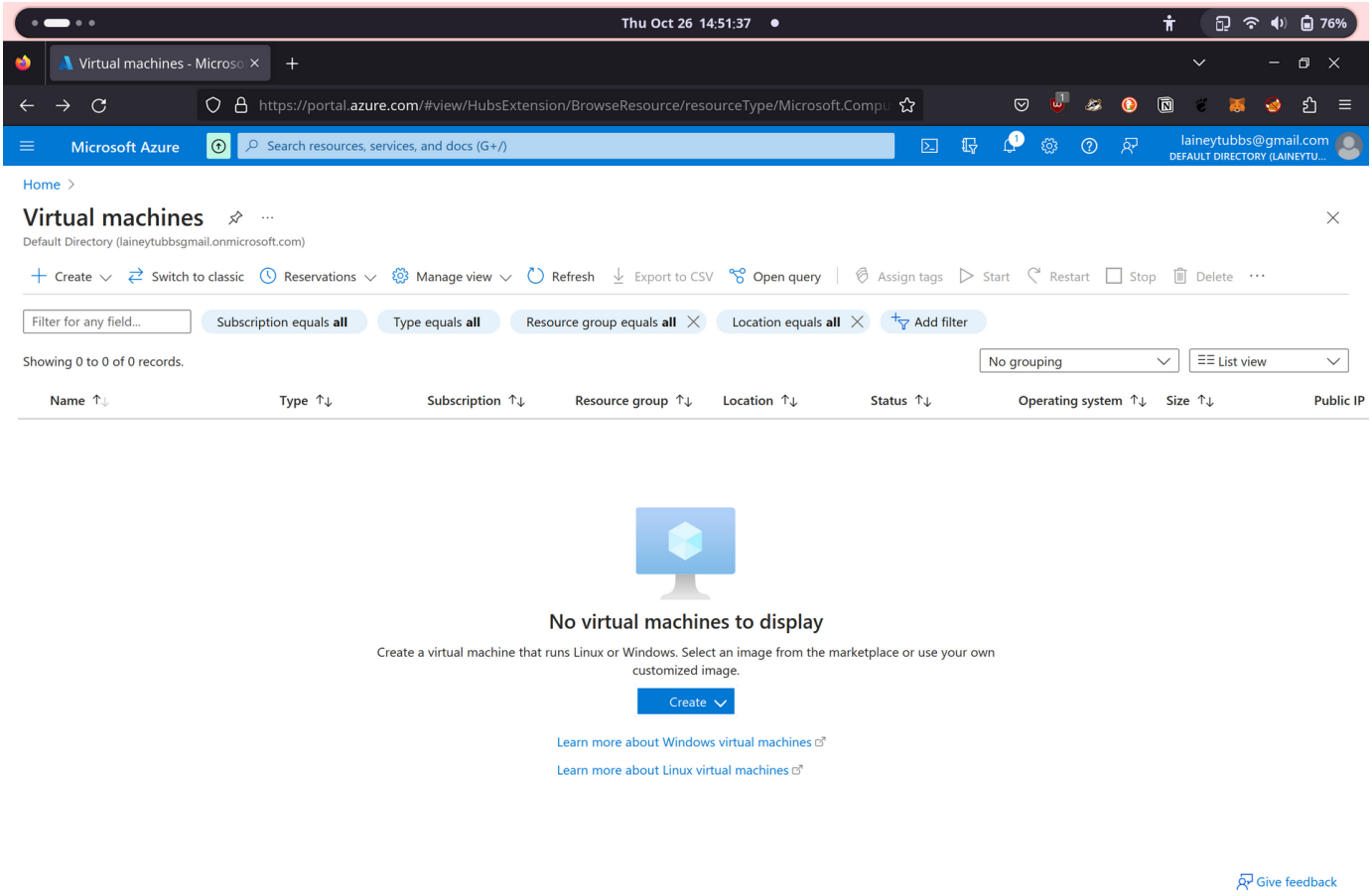
Siem Lab in Azure

Siem Lab with Honeypot in Azure

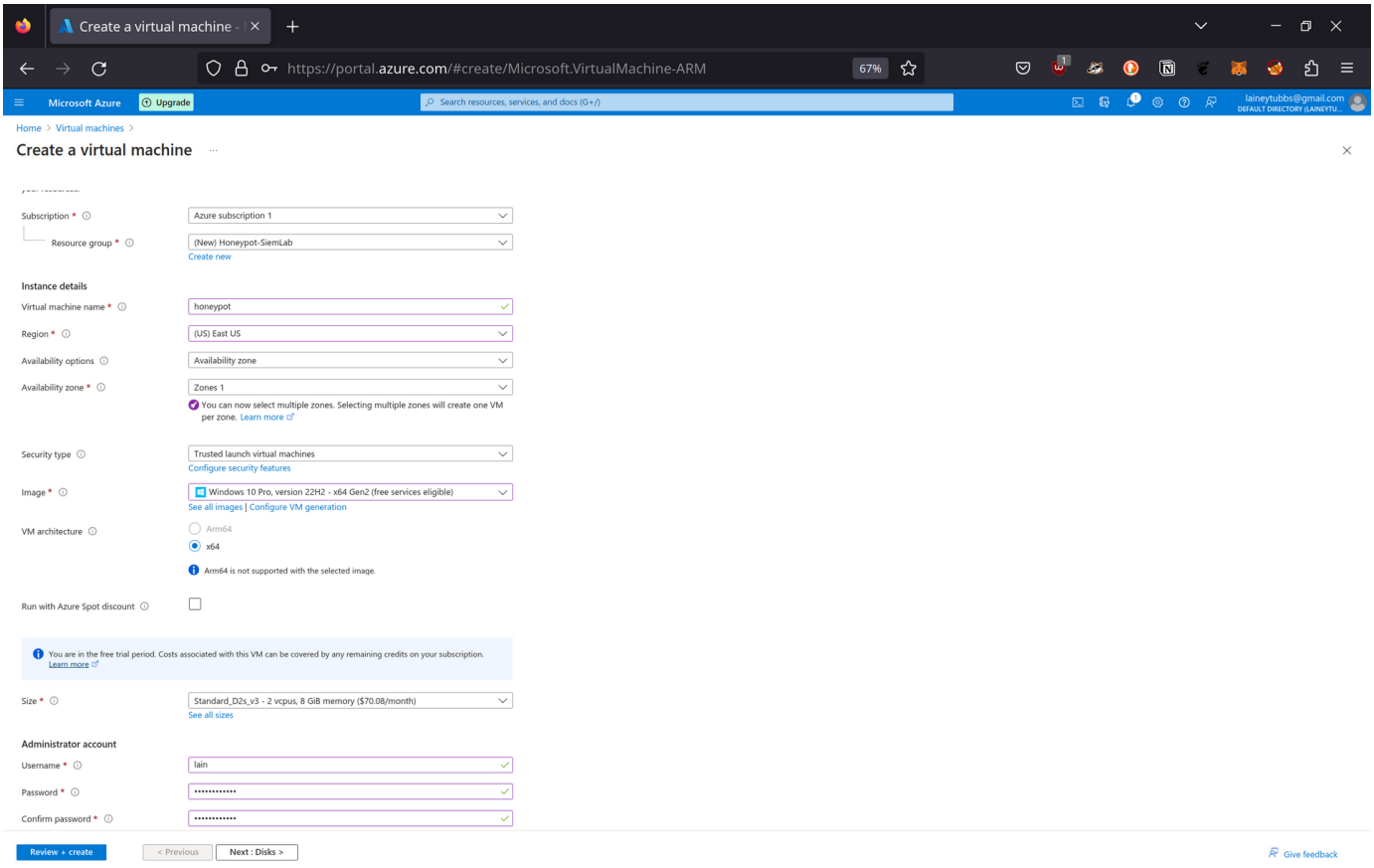
Lab done by Lainey Tubbs

This Lab in Azure is us designing a honeypot that allows attackers to come at this vm from all over the world. We are going to use the Siem Azure Sentinel to monitor this activity and report all incidents.

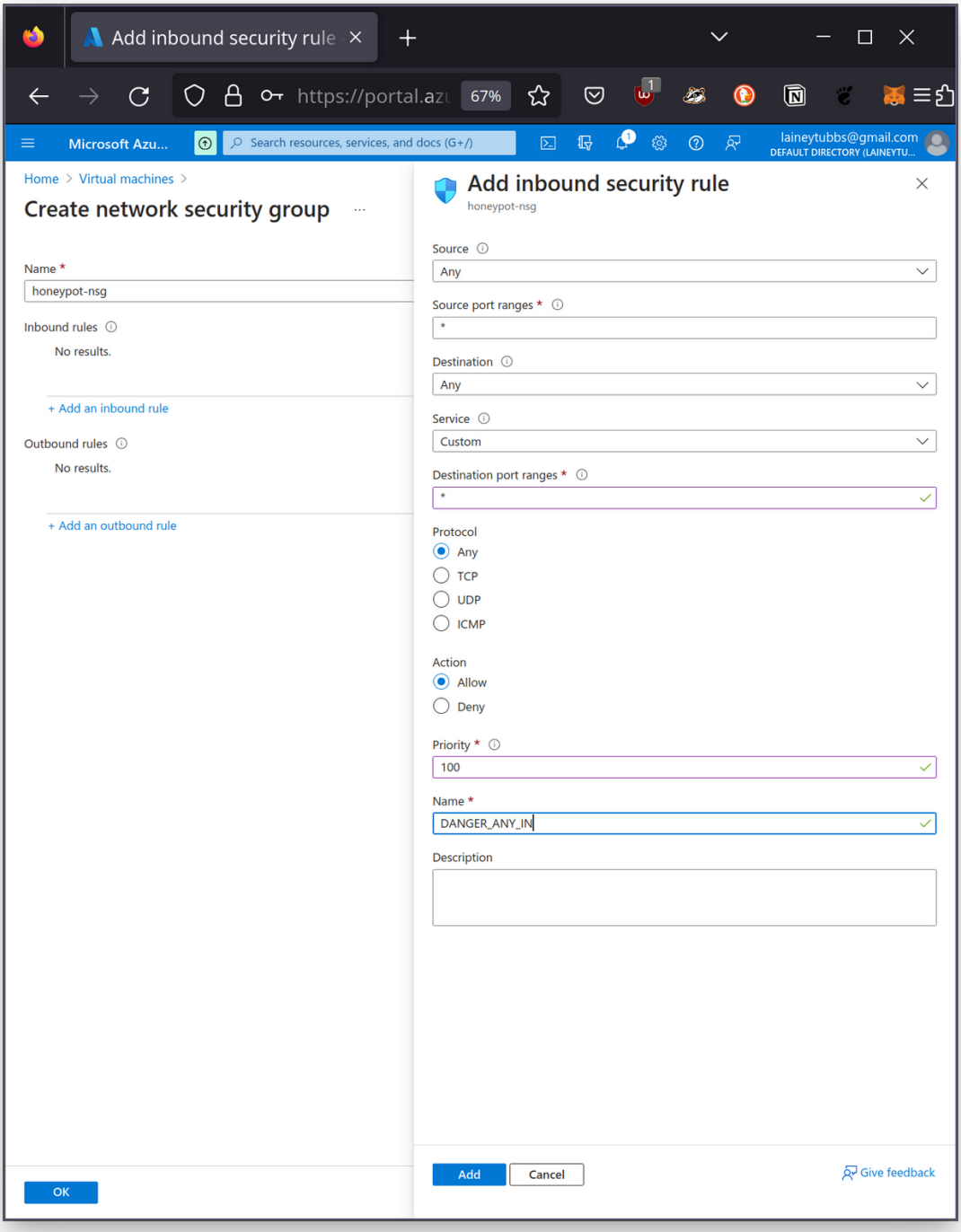
First step is creating the VM in Azure



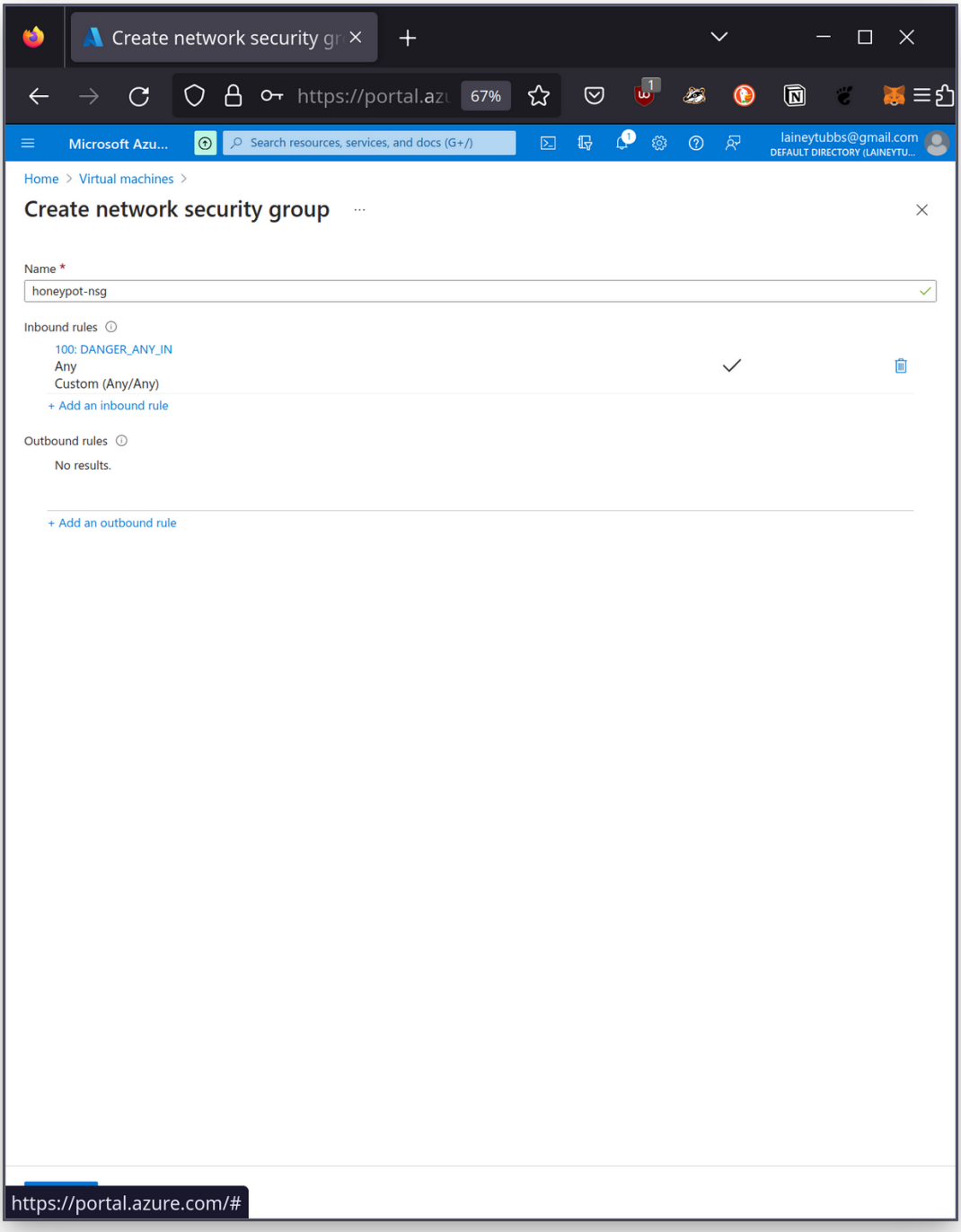
Starting configurations for honeypotvm



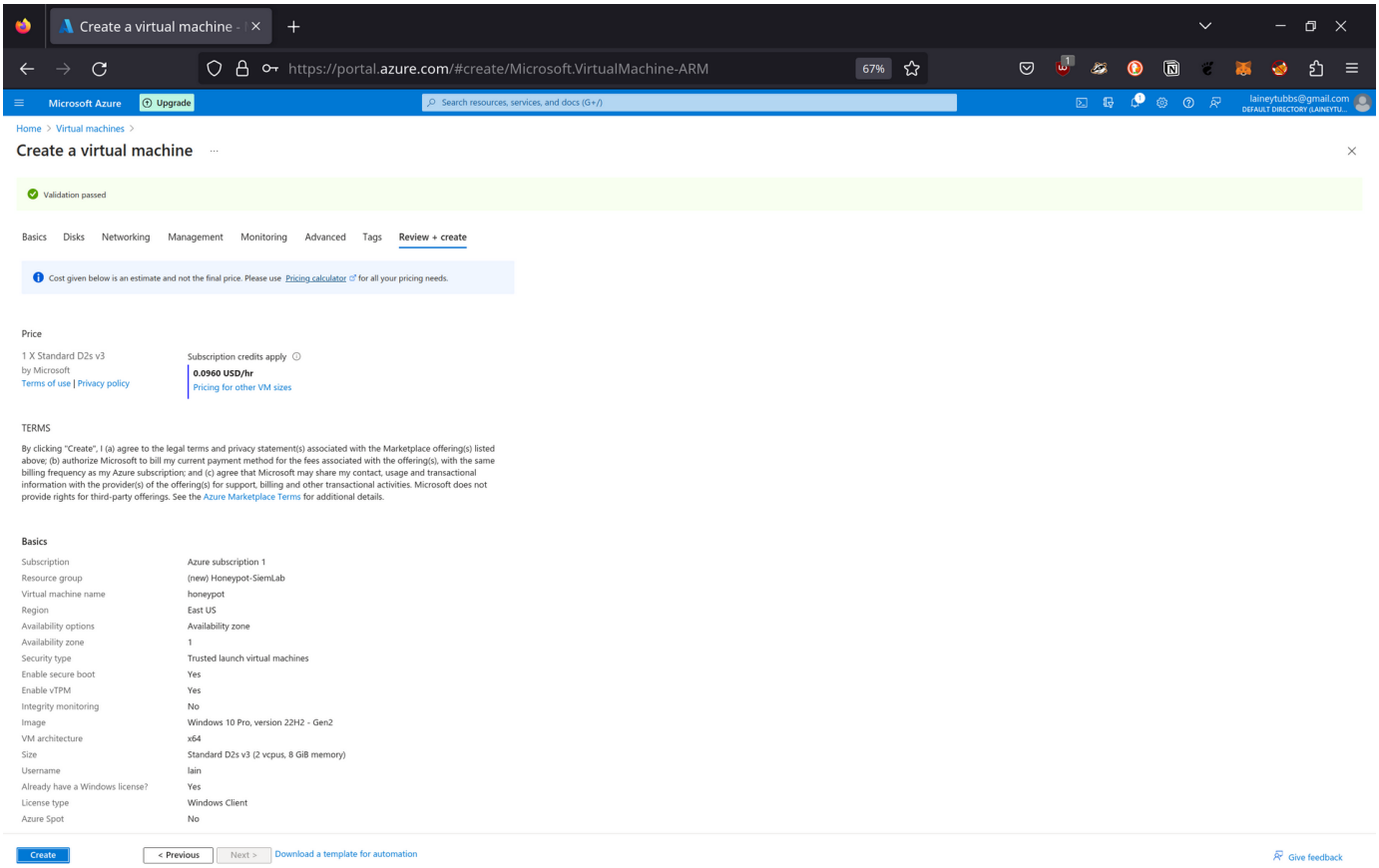
Setting inbound network security rule so that it allows any type of traffic in from any port



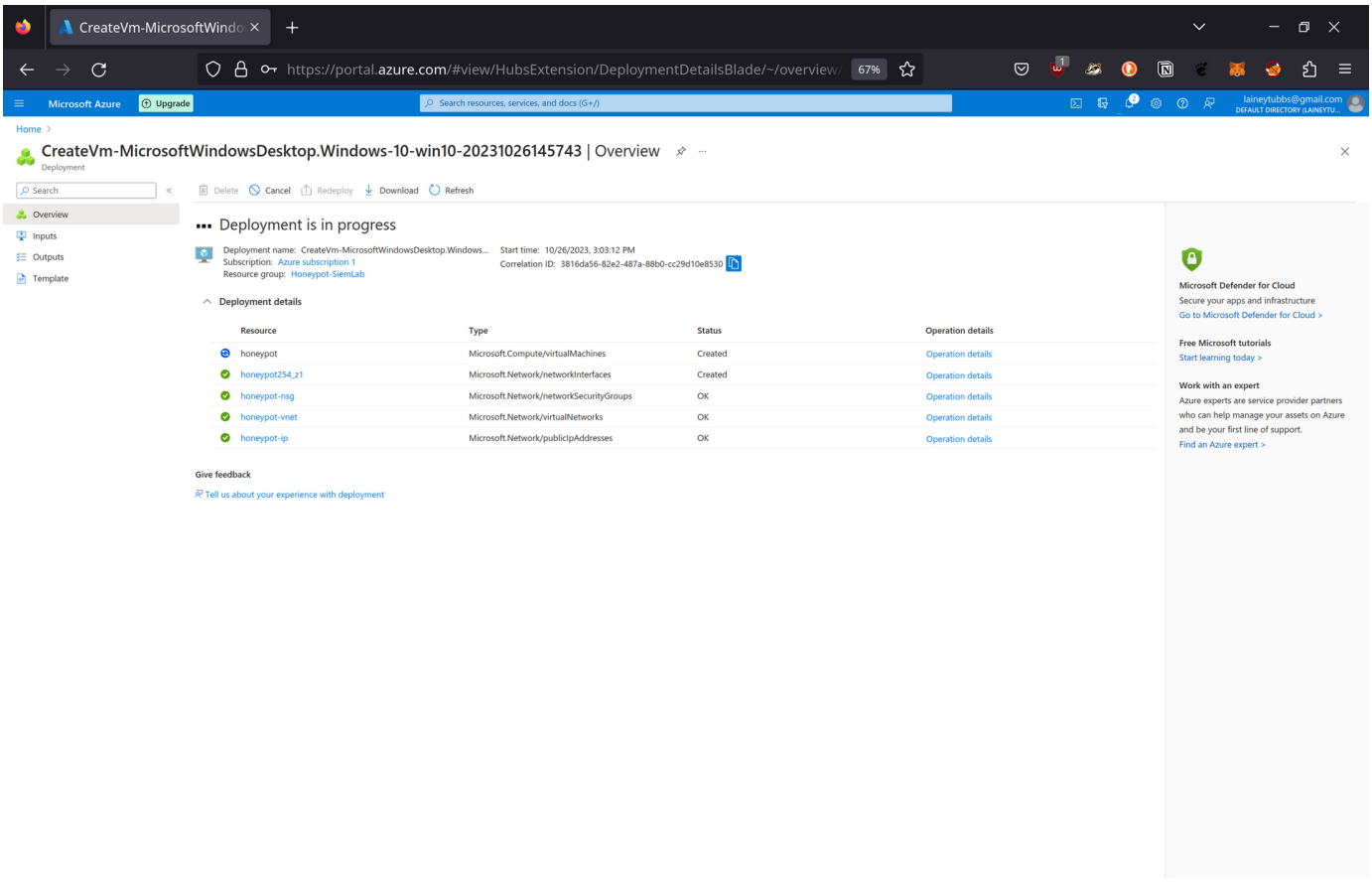
Finished creating the network security group with the new rule we set



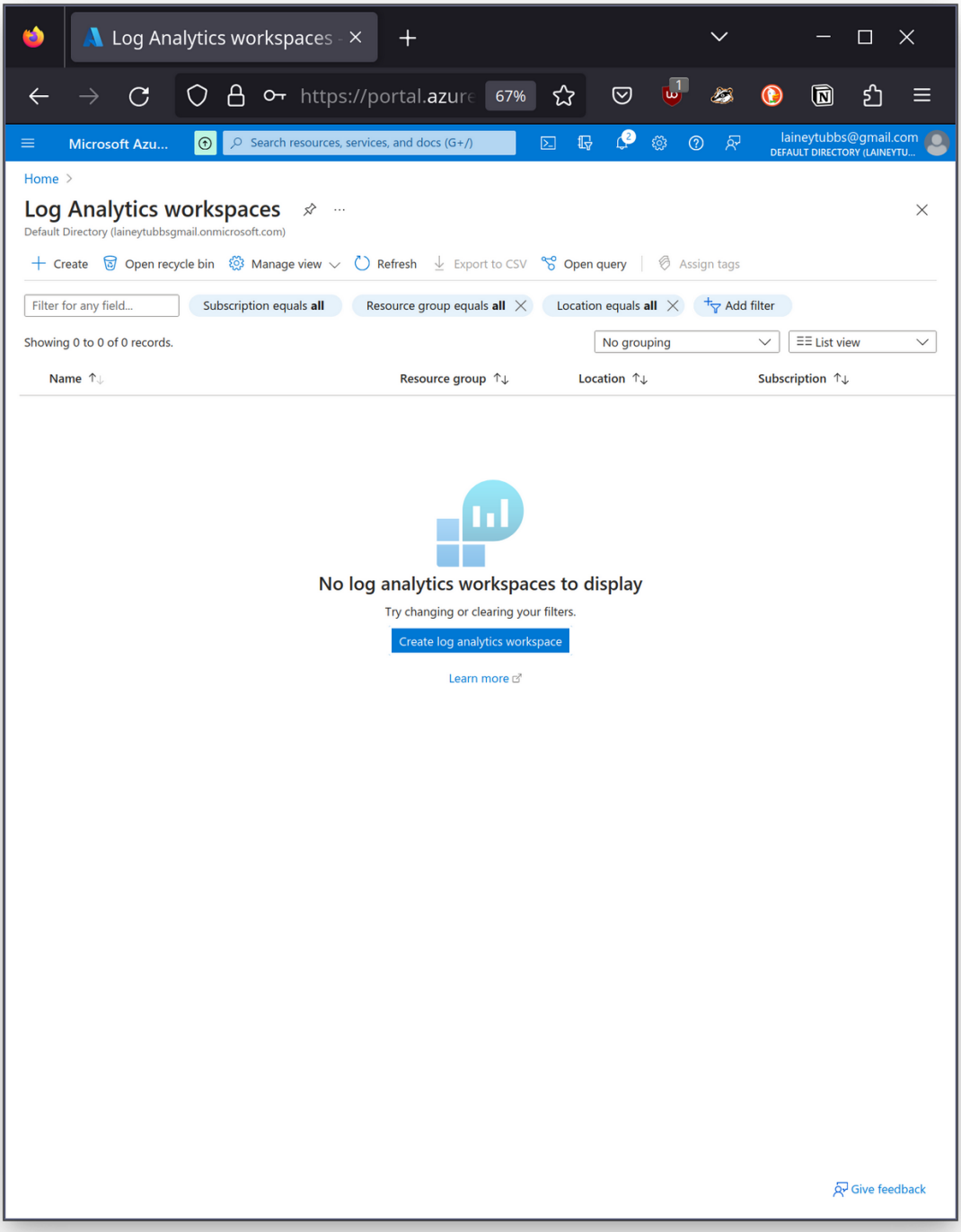
showing config for the vm prior to finalizing its creation



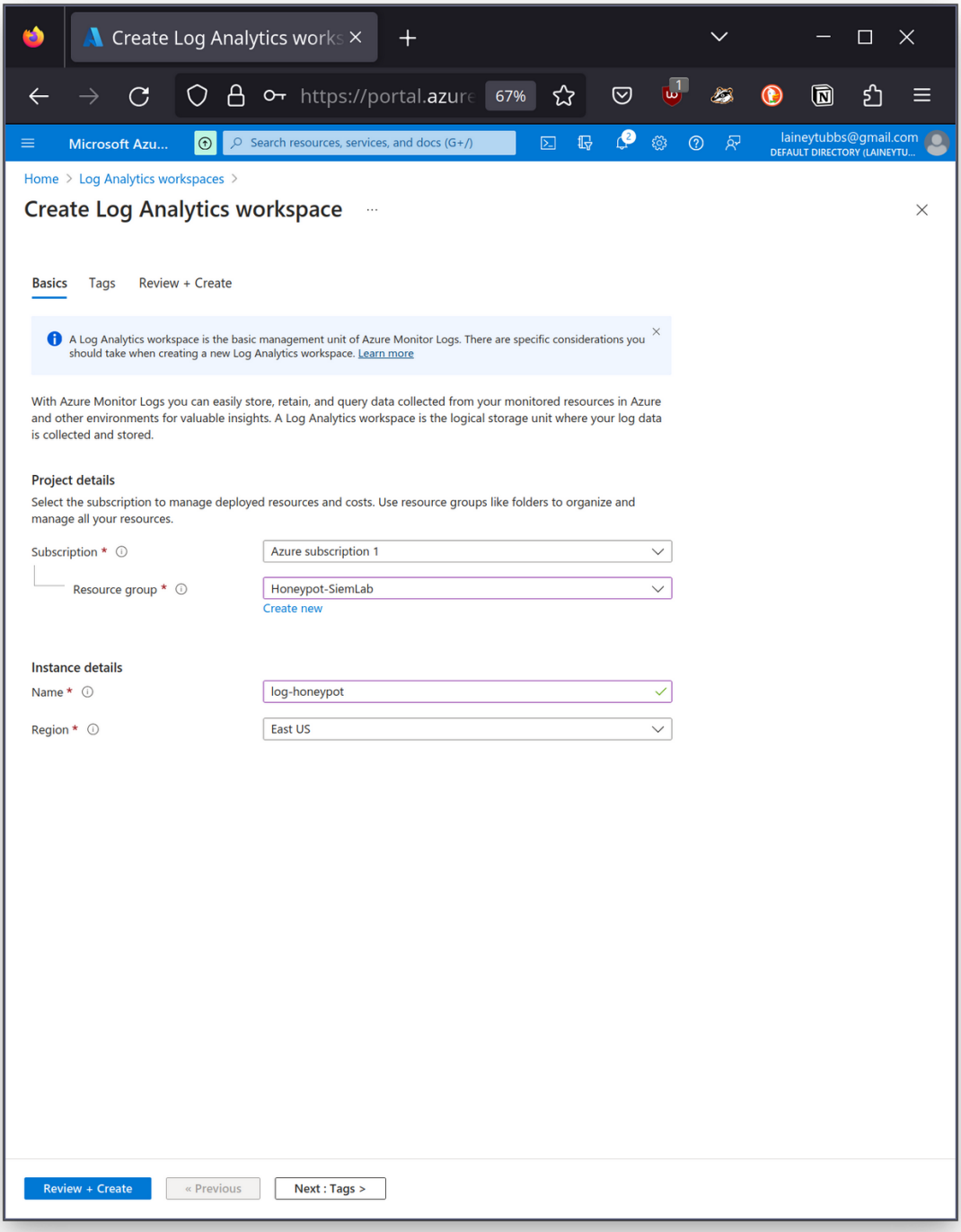
Deploying the VM



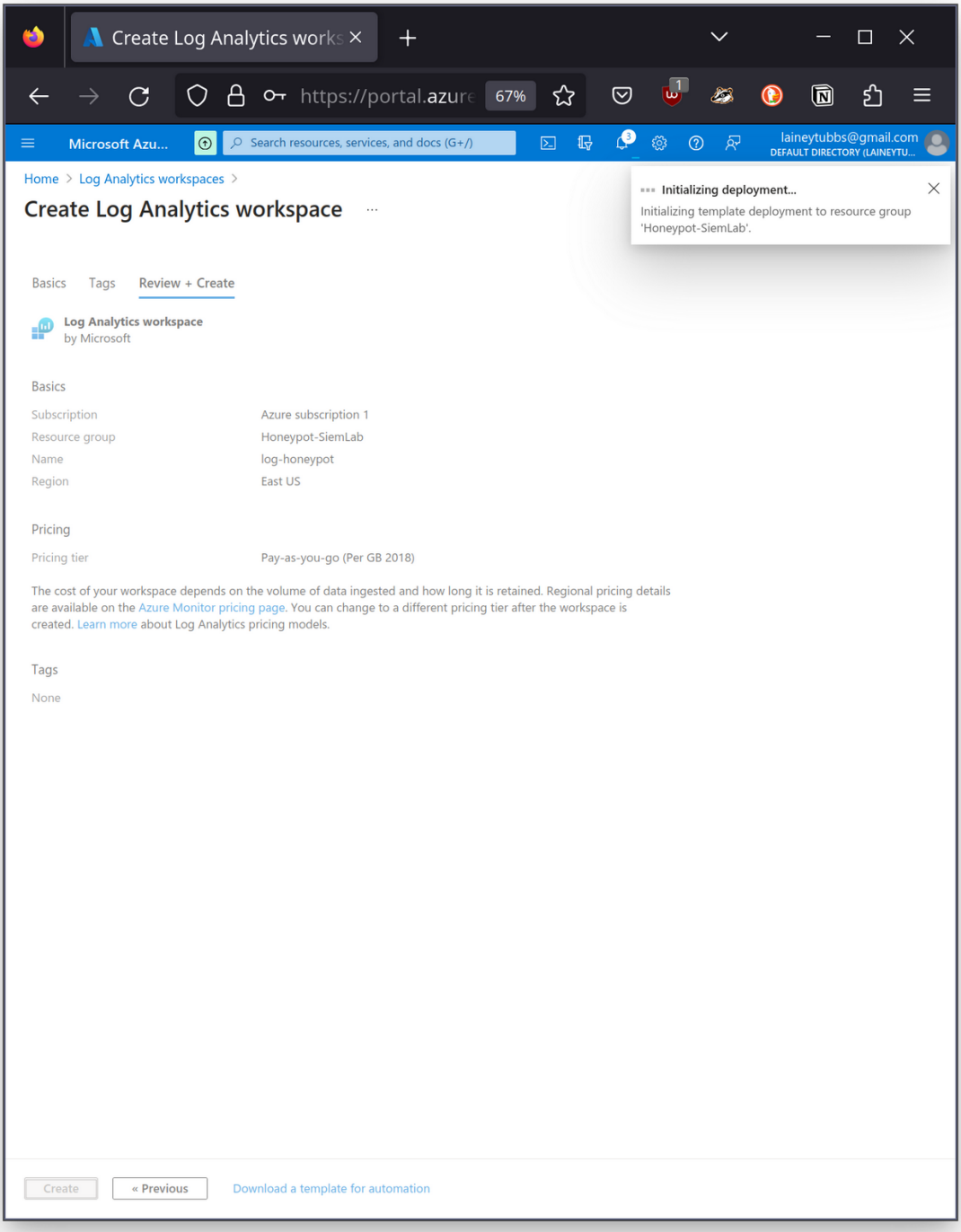
Creating log analytics workspace so that we can connect it to Azure Sentinel Later to show where the attackers are coming from across the world



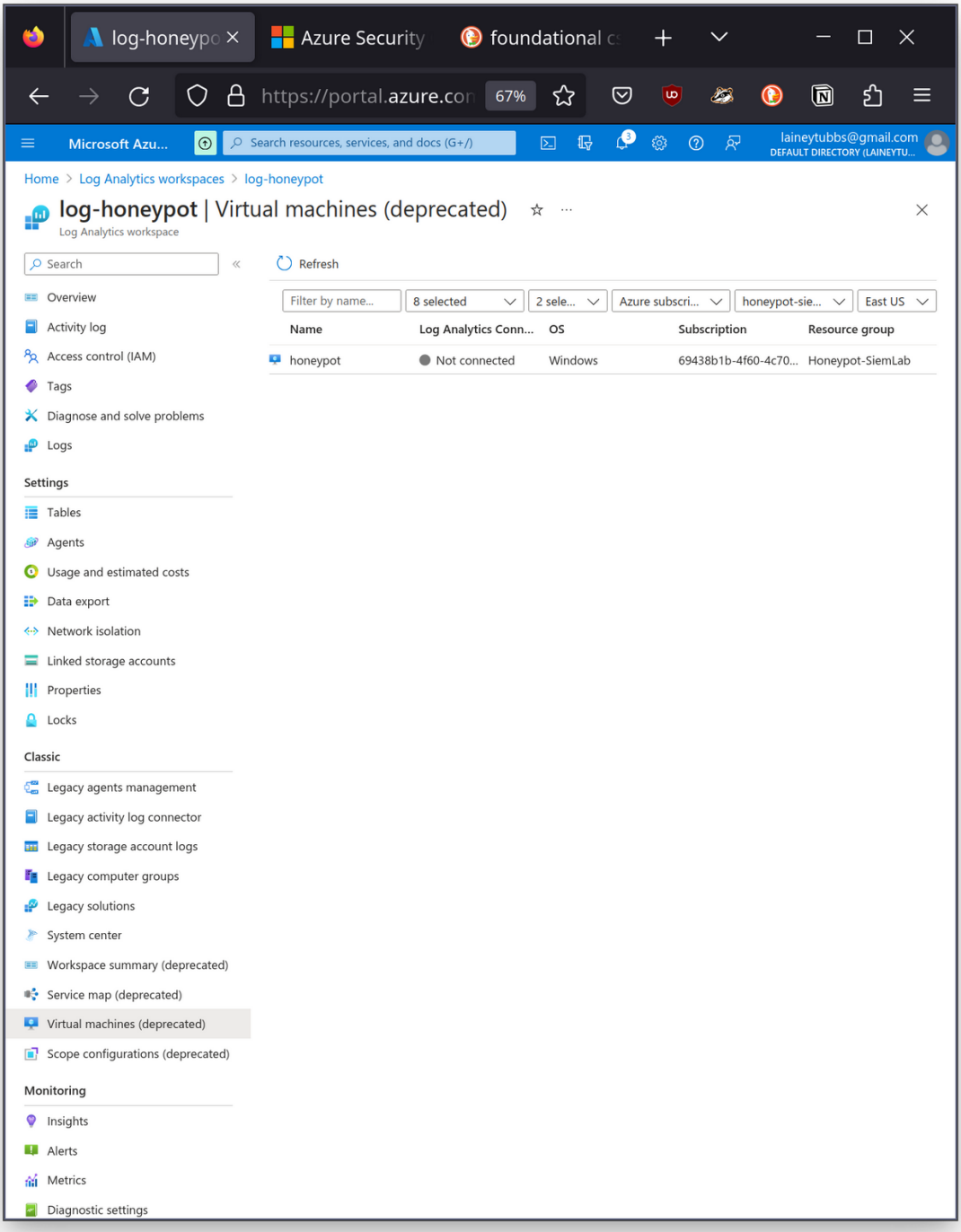
creating log analytics workspace



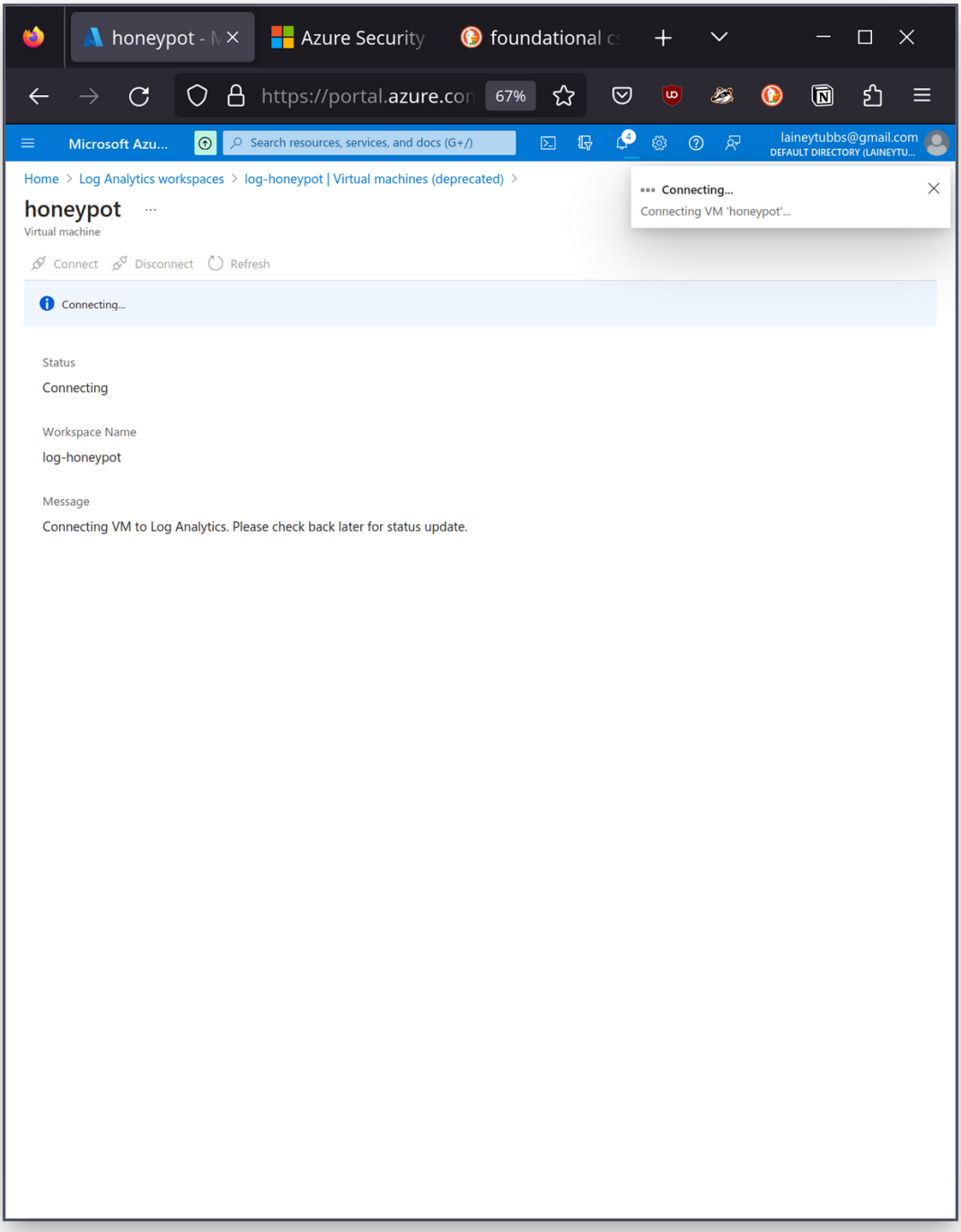
finalizing the analitics workspace



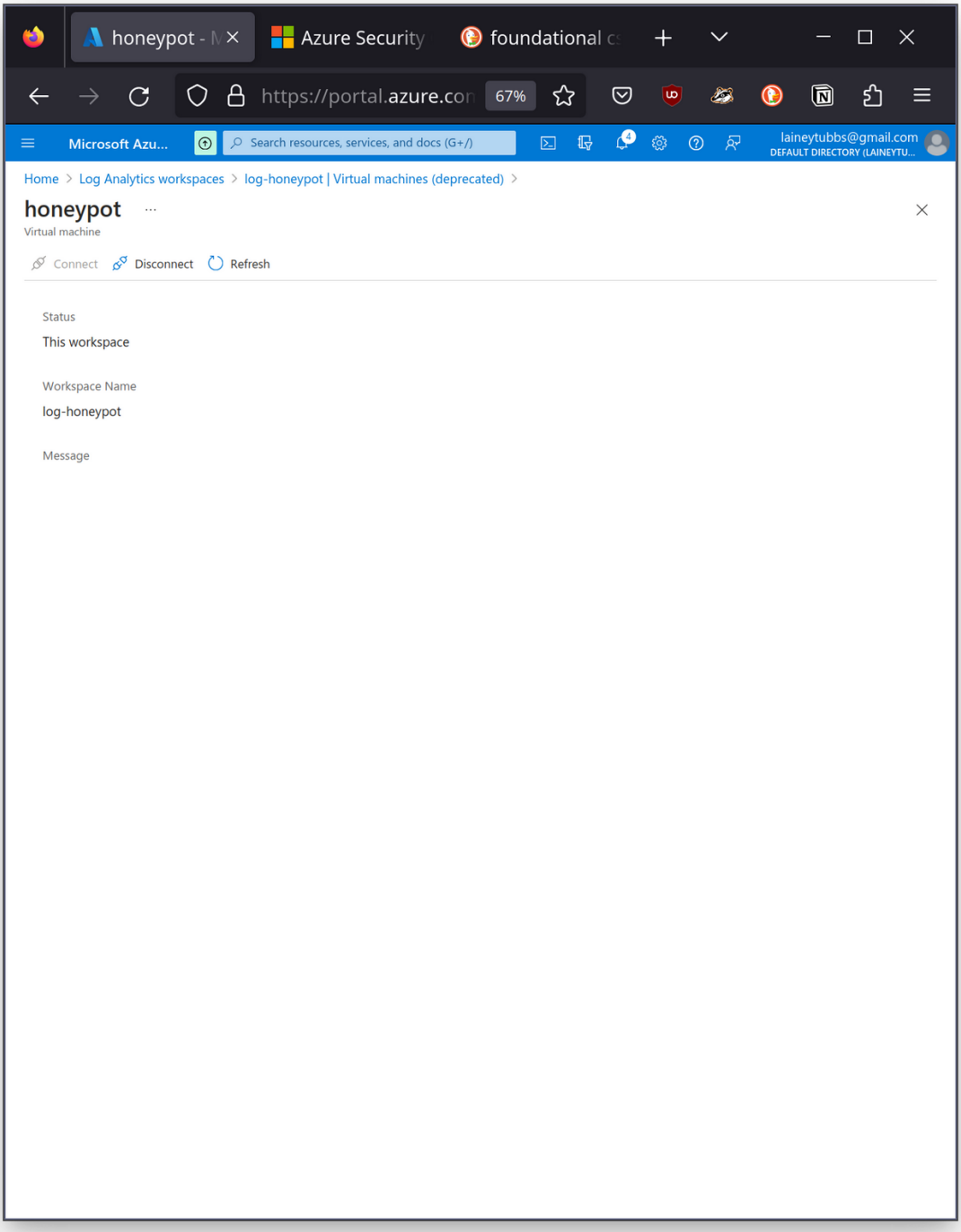
Looking at VM we created to eventually connect to the Log Analytics Workspace



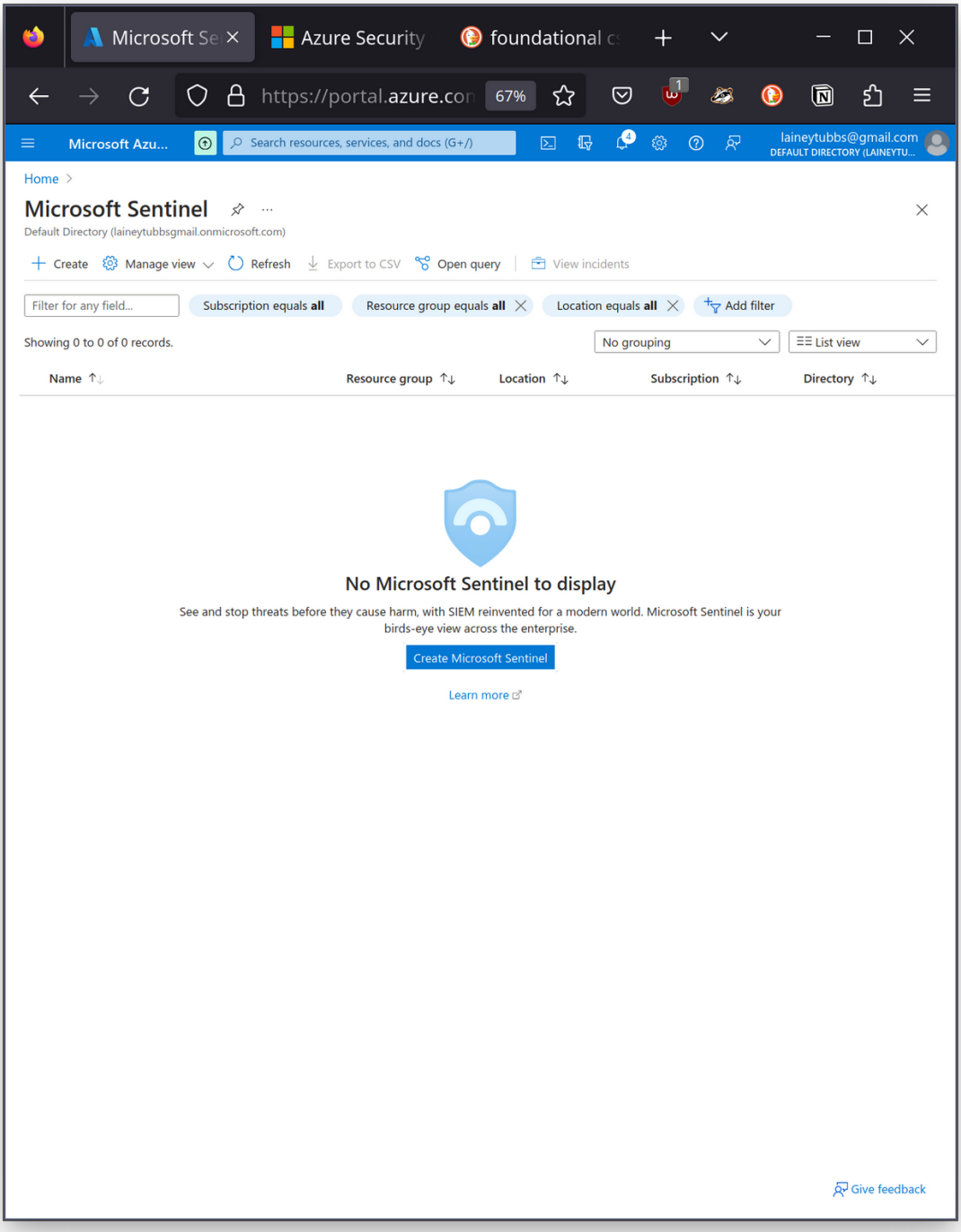
Connecting the VM we created to the Log Analytics Workspace



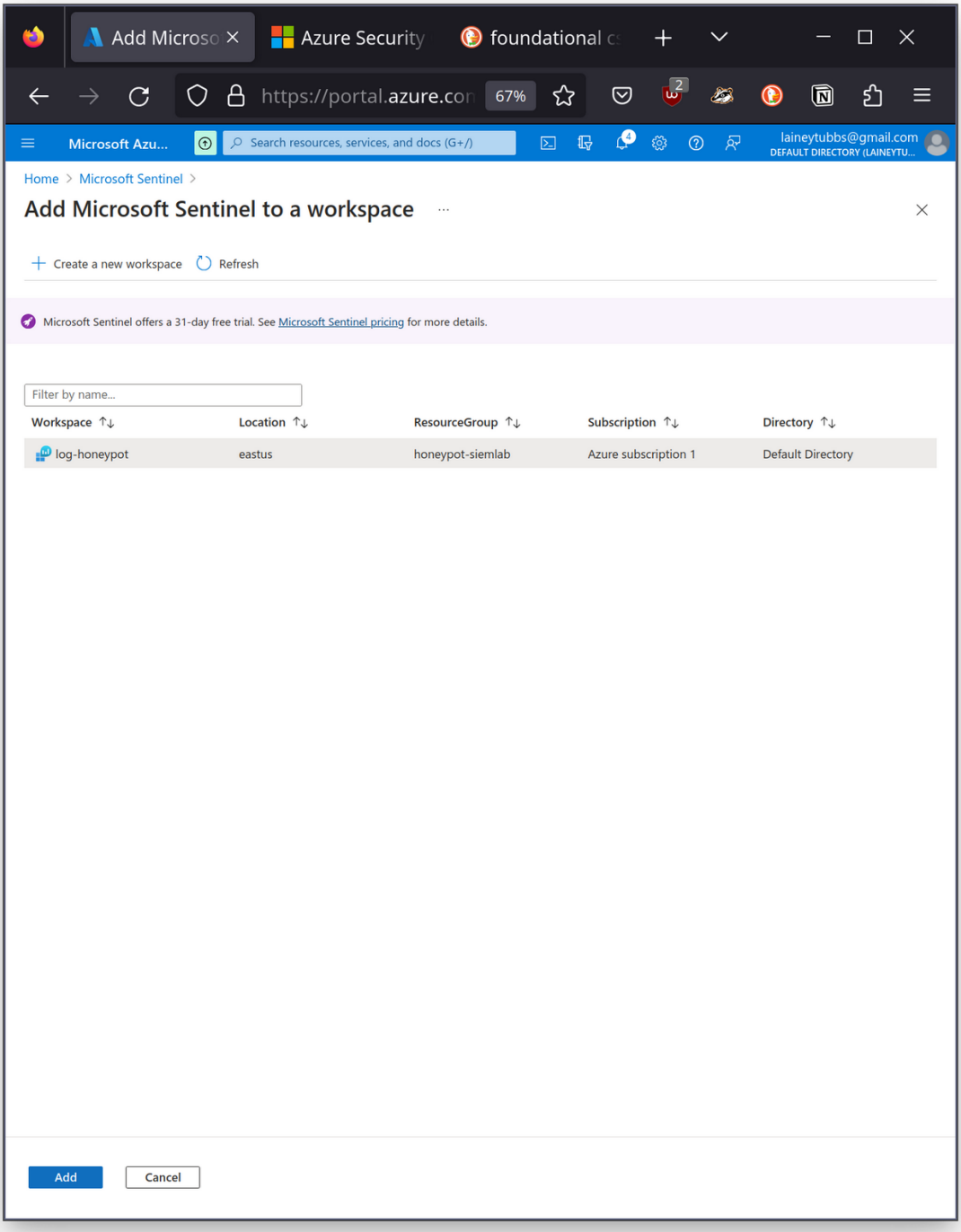
Log Analytics Workspace Created and connected to the VM



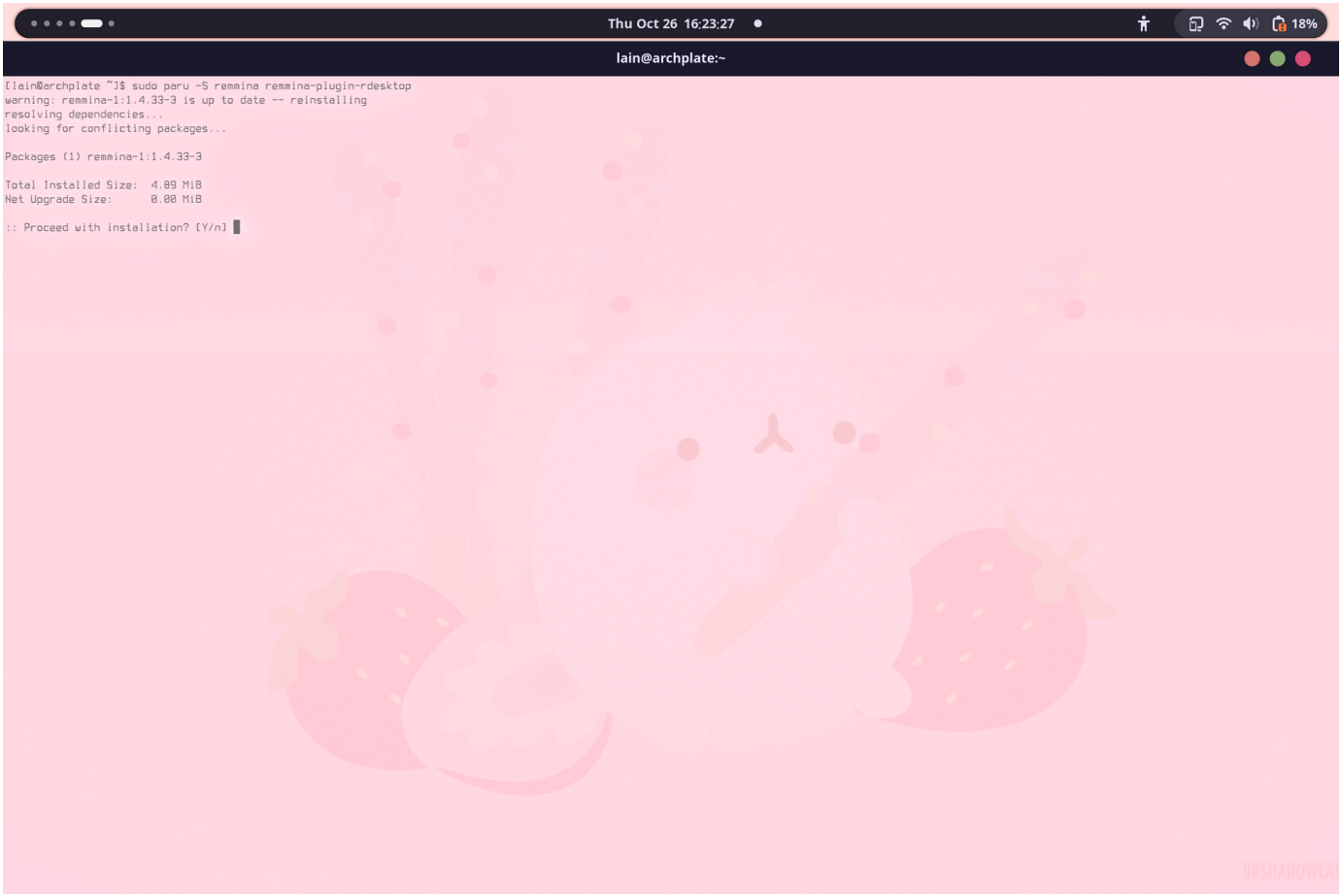
Moving to Azure Sentinel, the Siem I used that is already integrated into Azure.



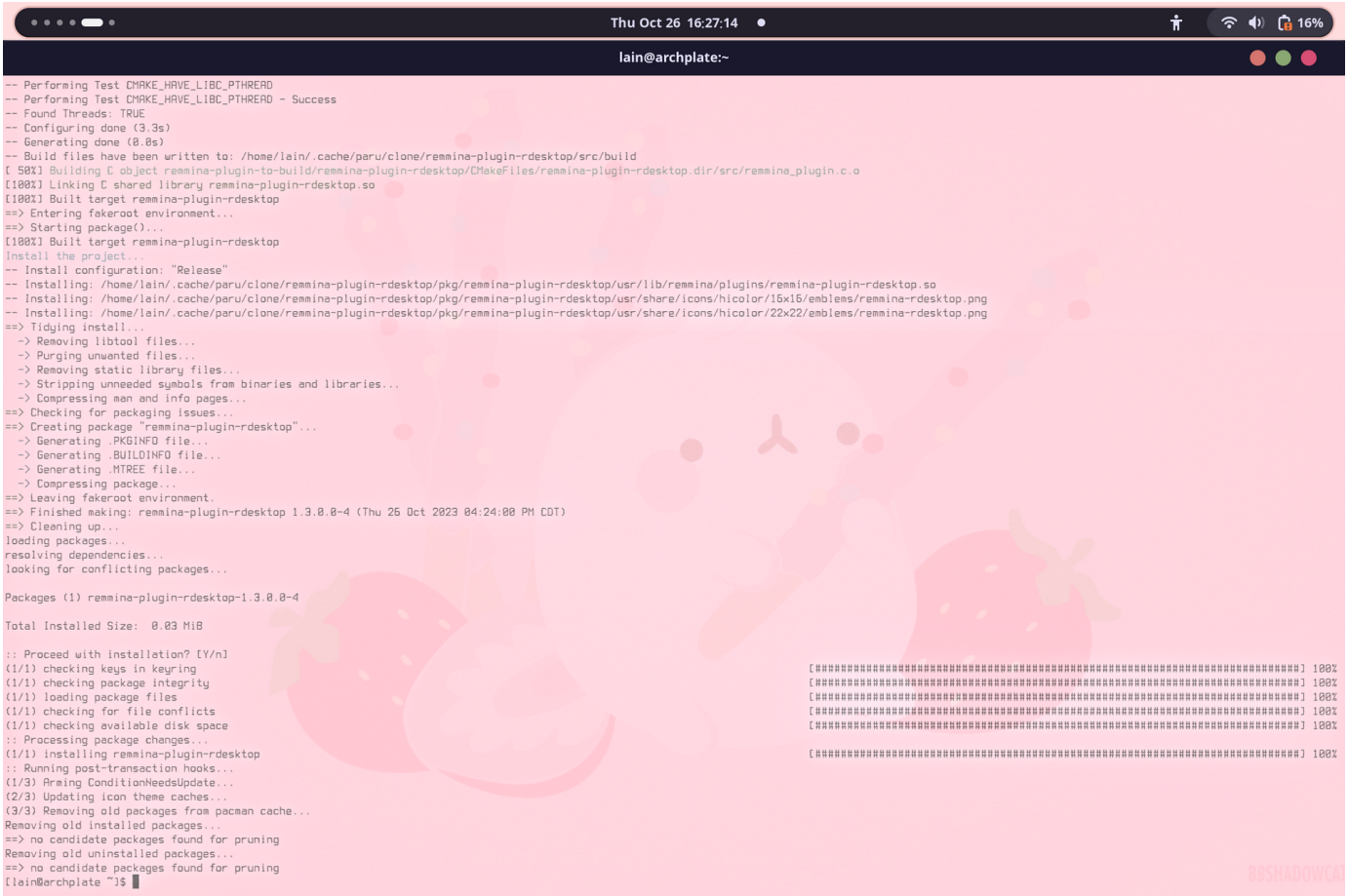
Adding the Log Analytics Workspace with the HoneyPot to Azure Sentinel



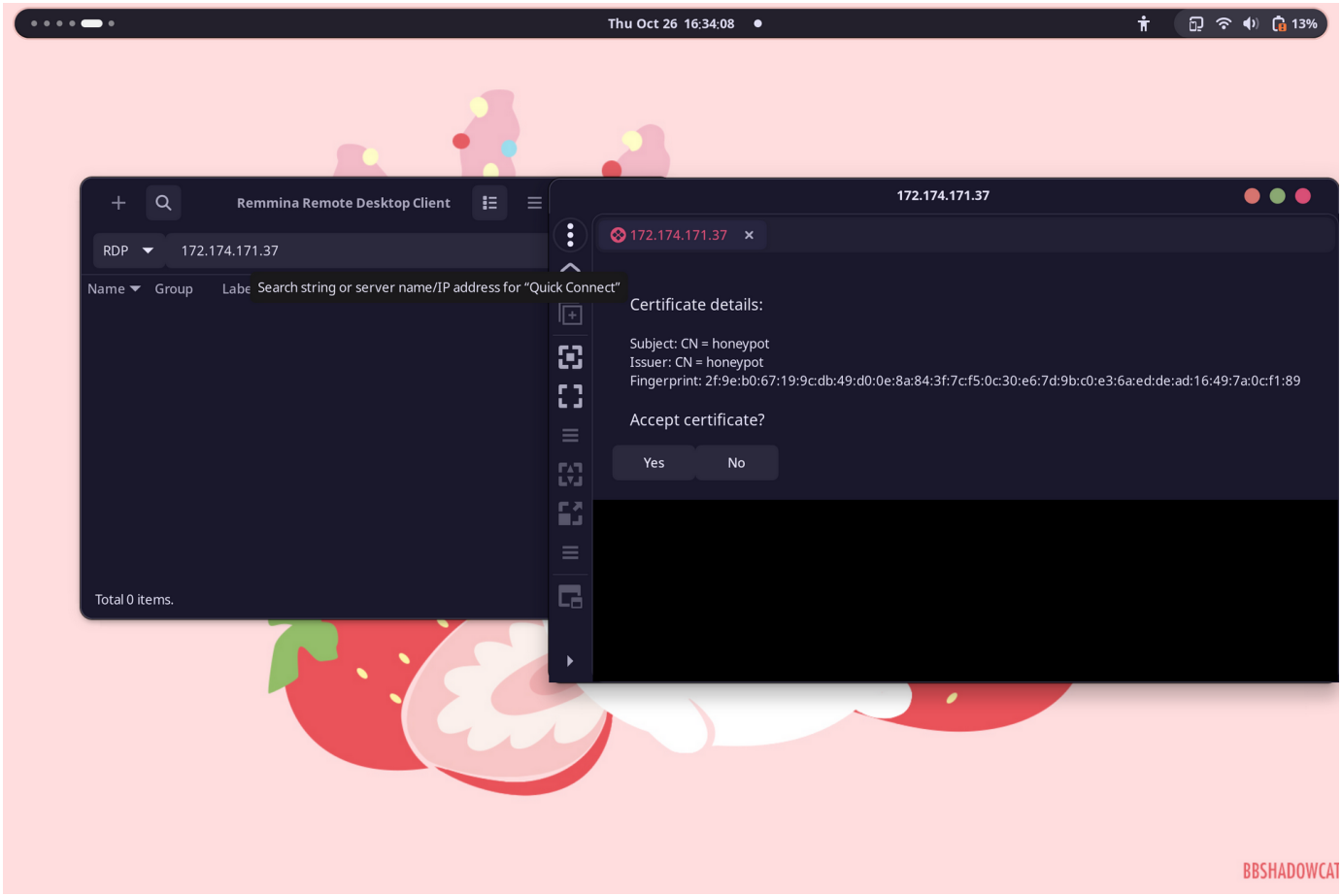
Downloaded Remmina so that I can remote into the VM from my PC



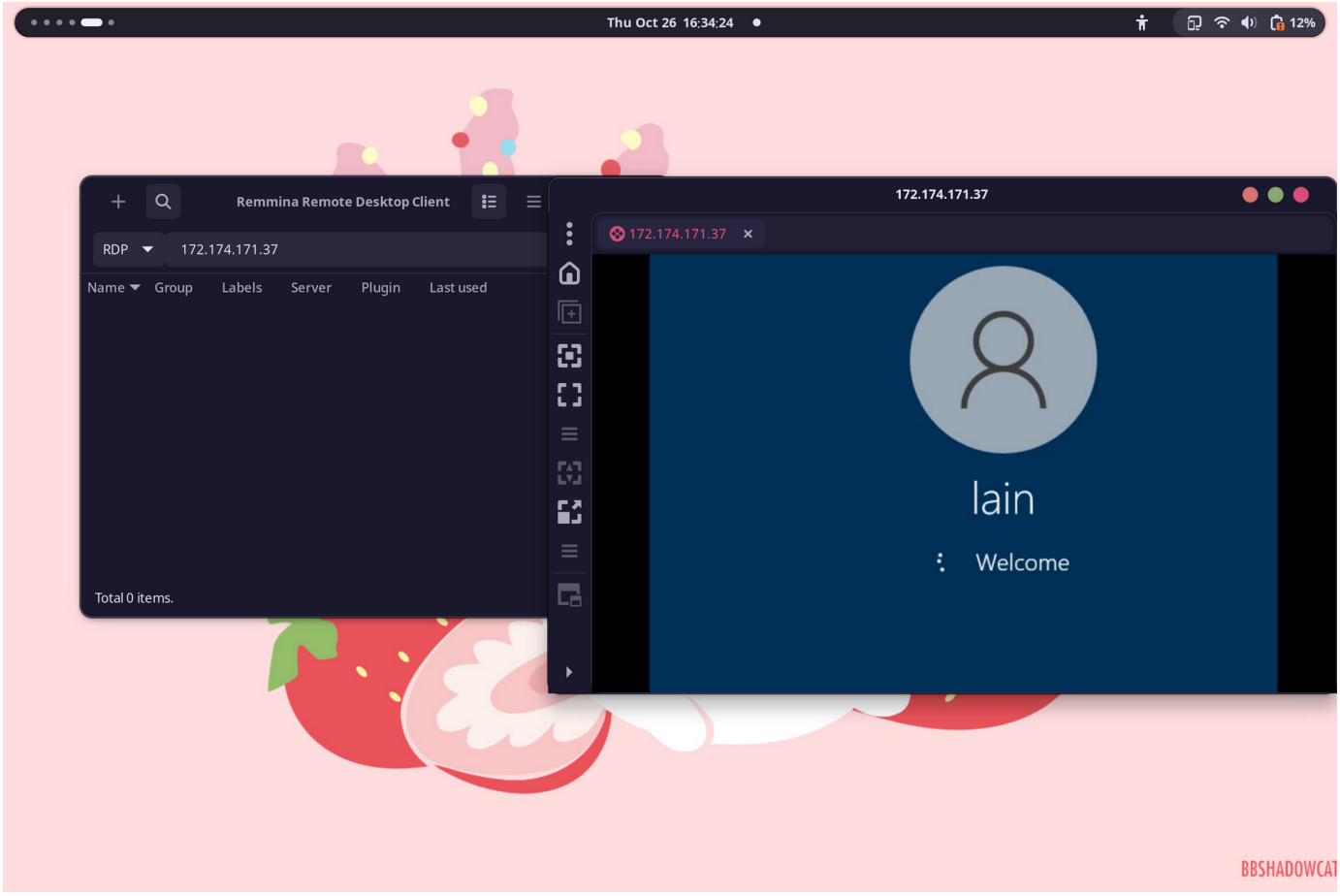
Finished Downloading Remmina



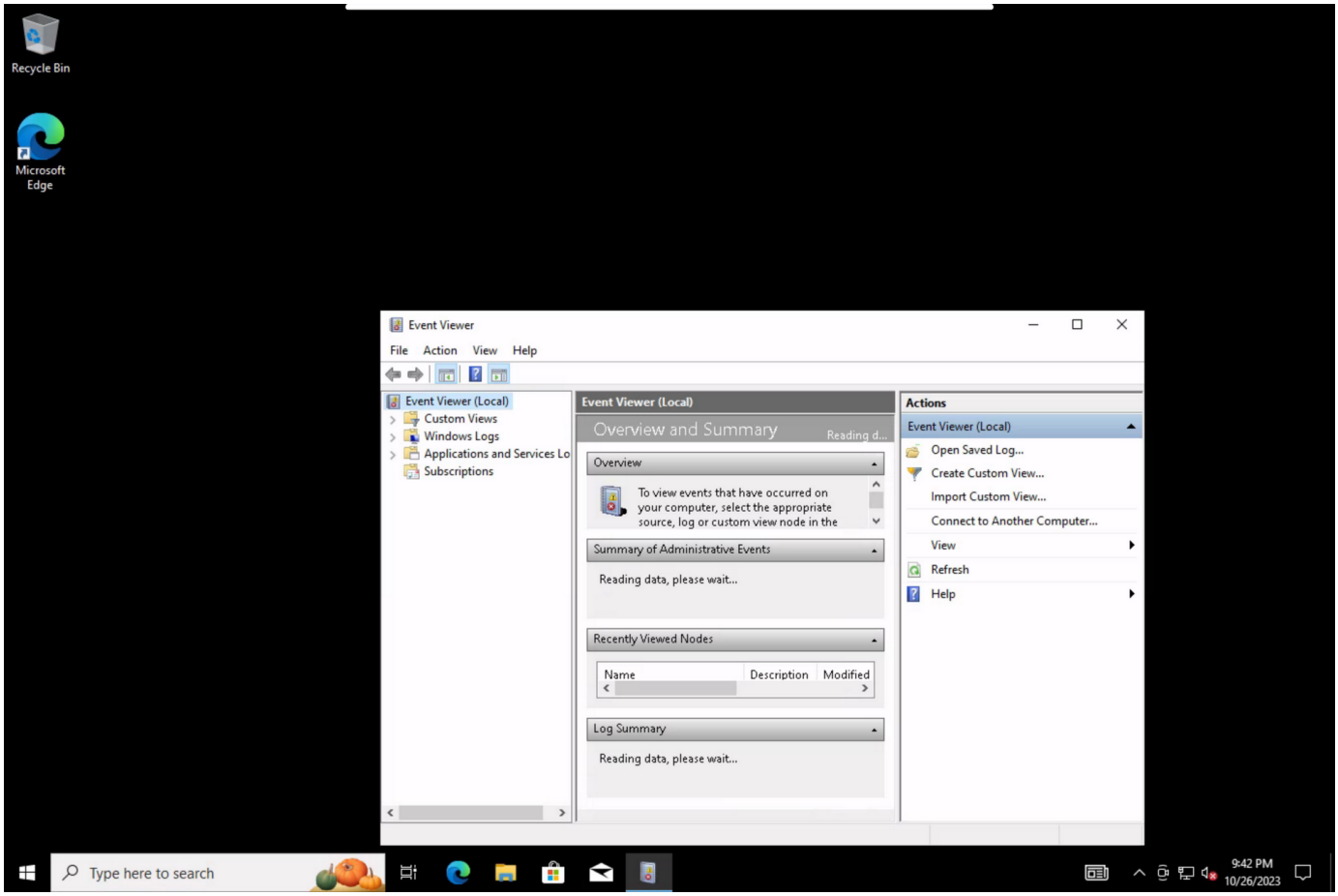
Remoted into the VM from Remmina



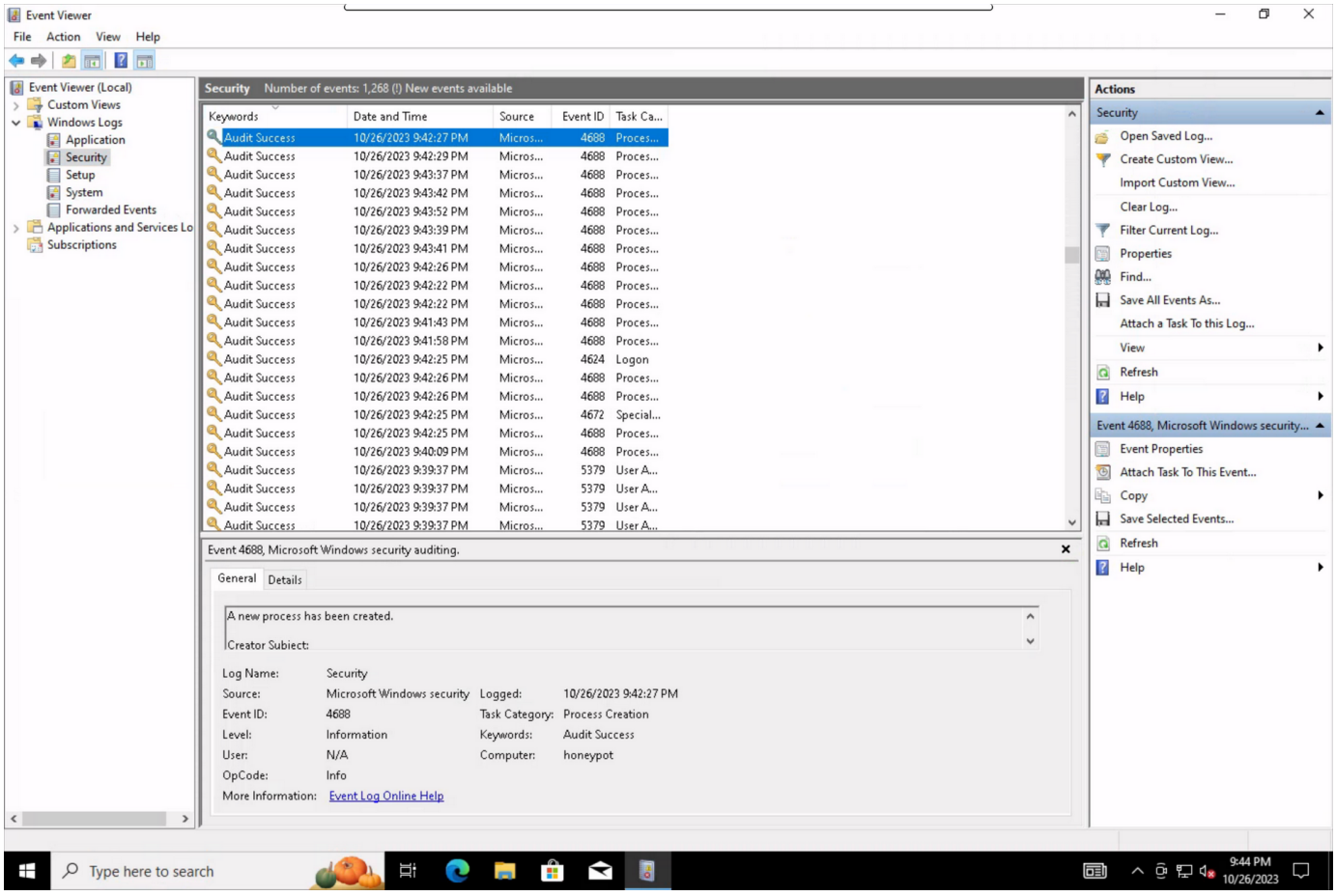
Signed into the Honeypot VM



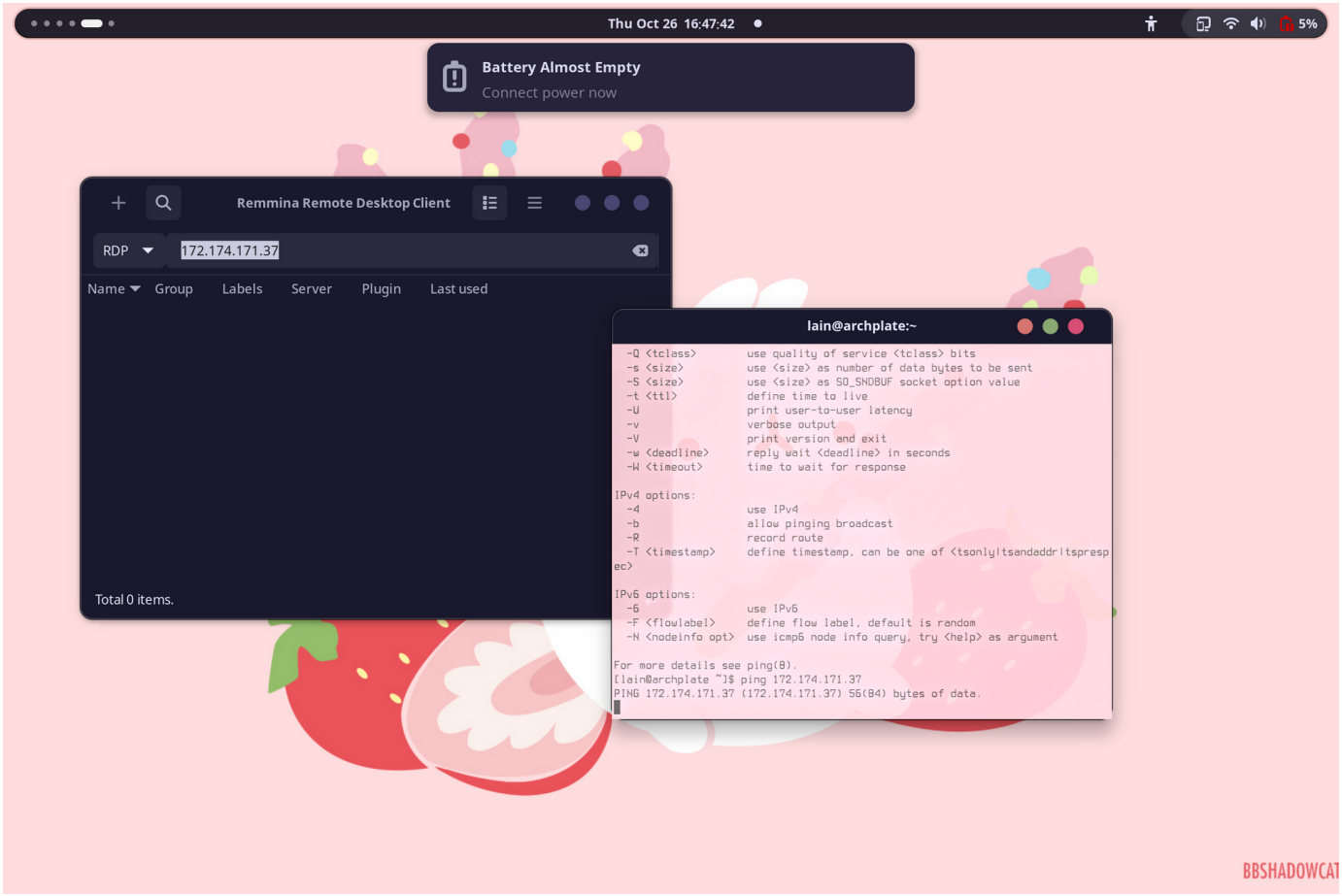
Inside the VM I opened Event Viewer so that I can see the log files

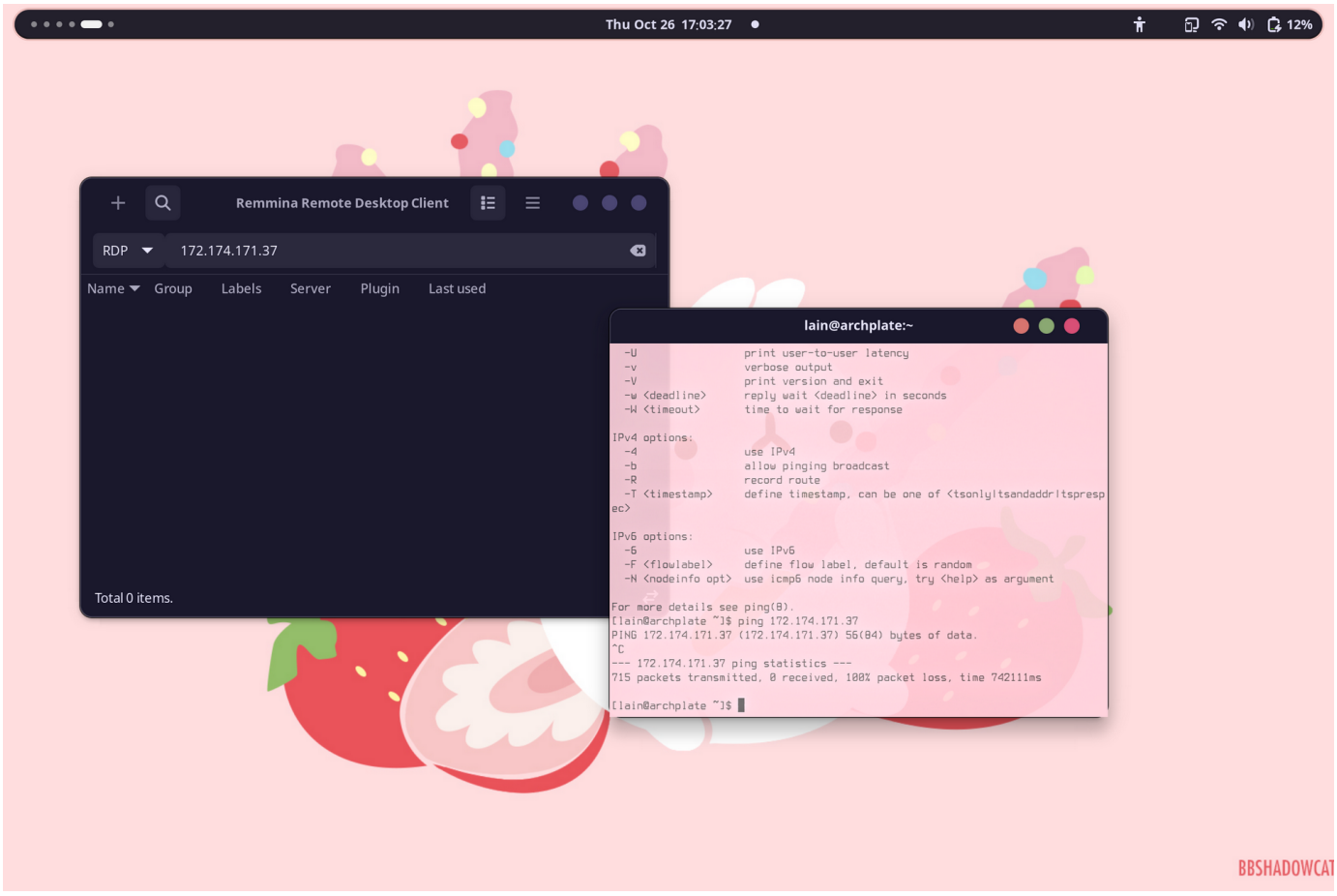


Viewing the Security Events

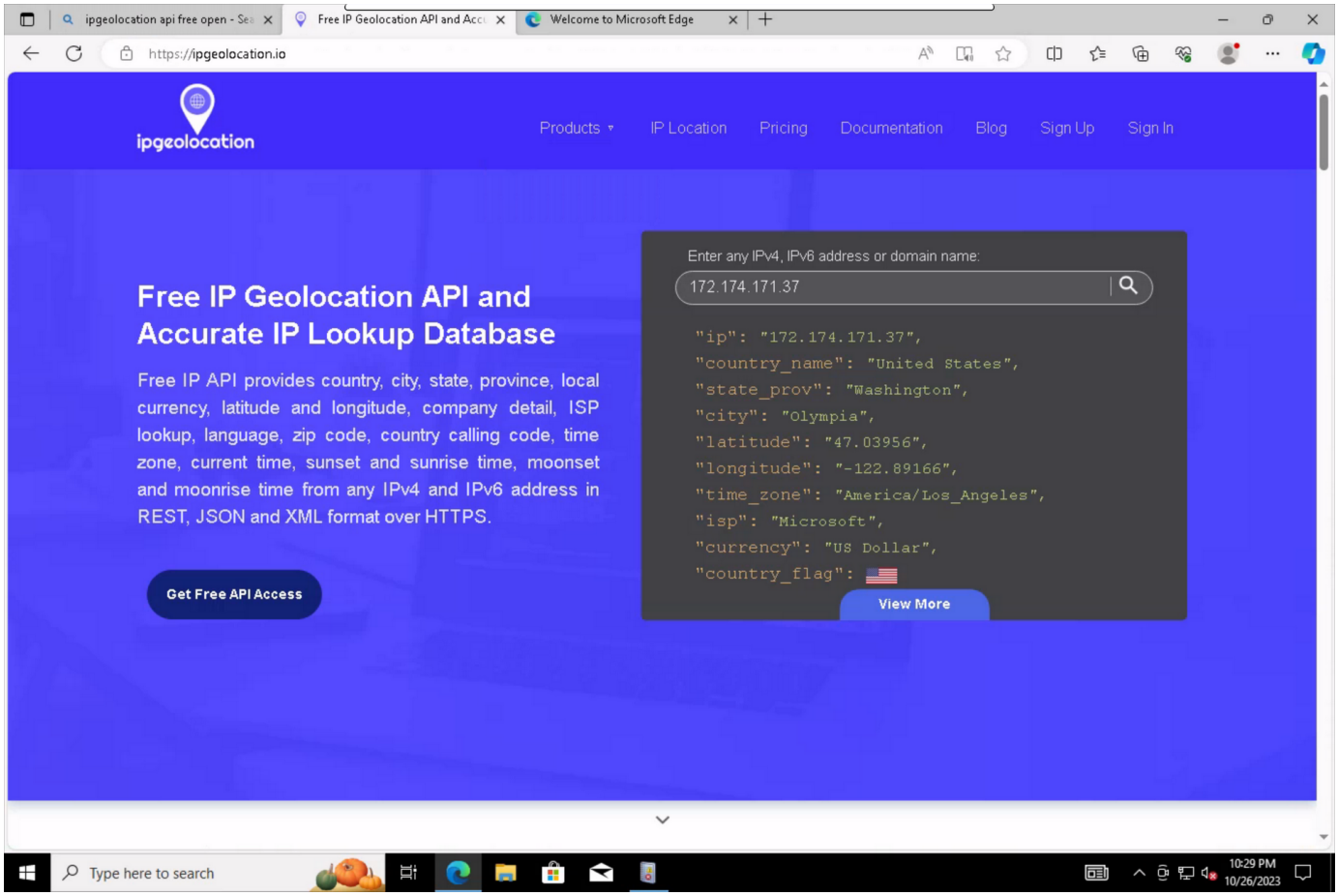


Pinging the VM from my PC to see that the icmp requests aren't going through

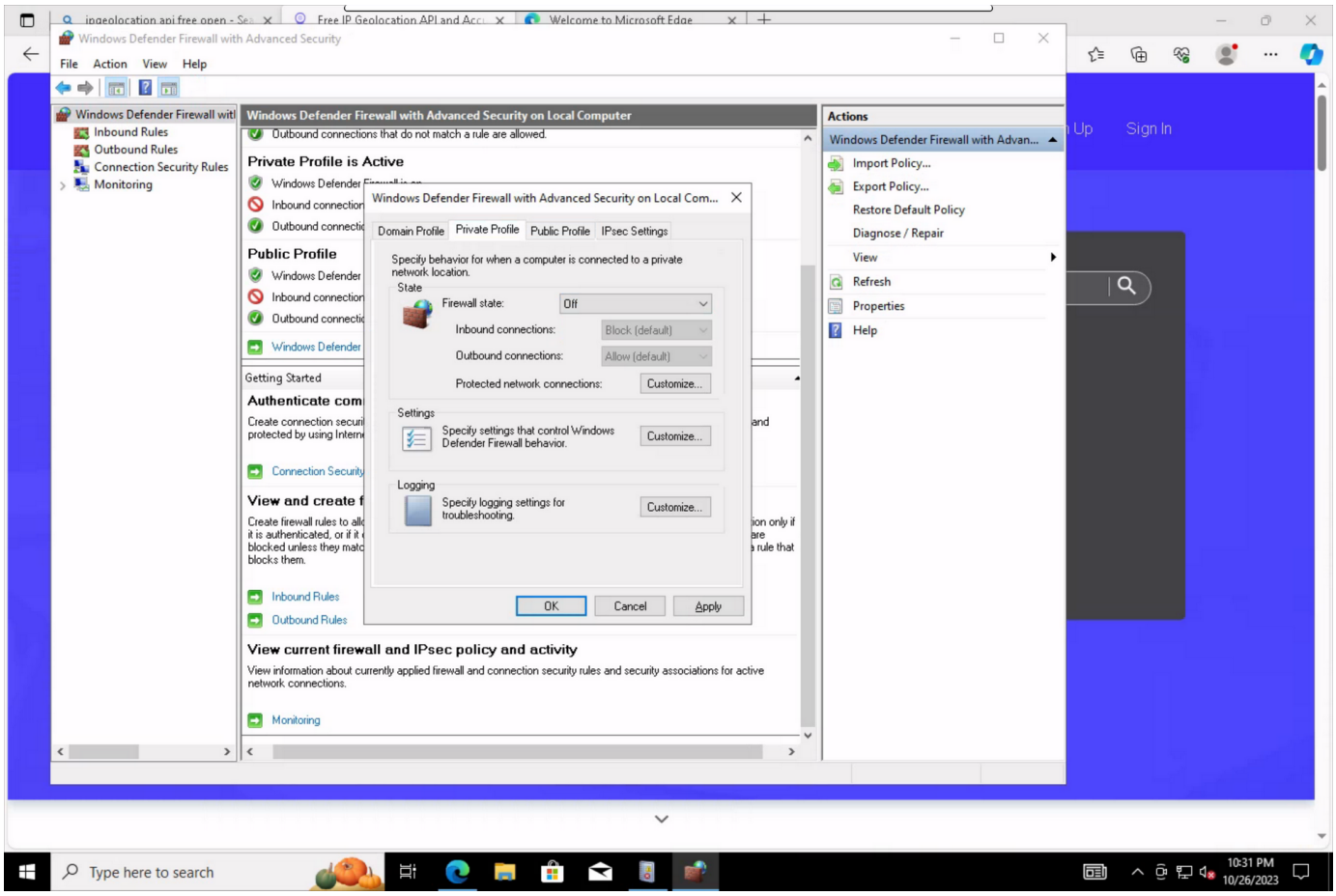


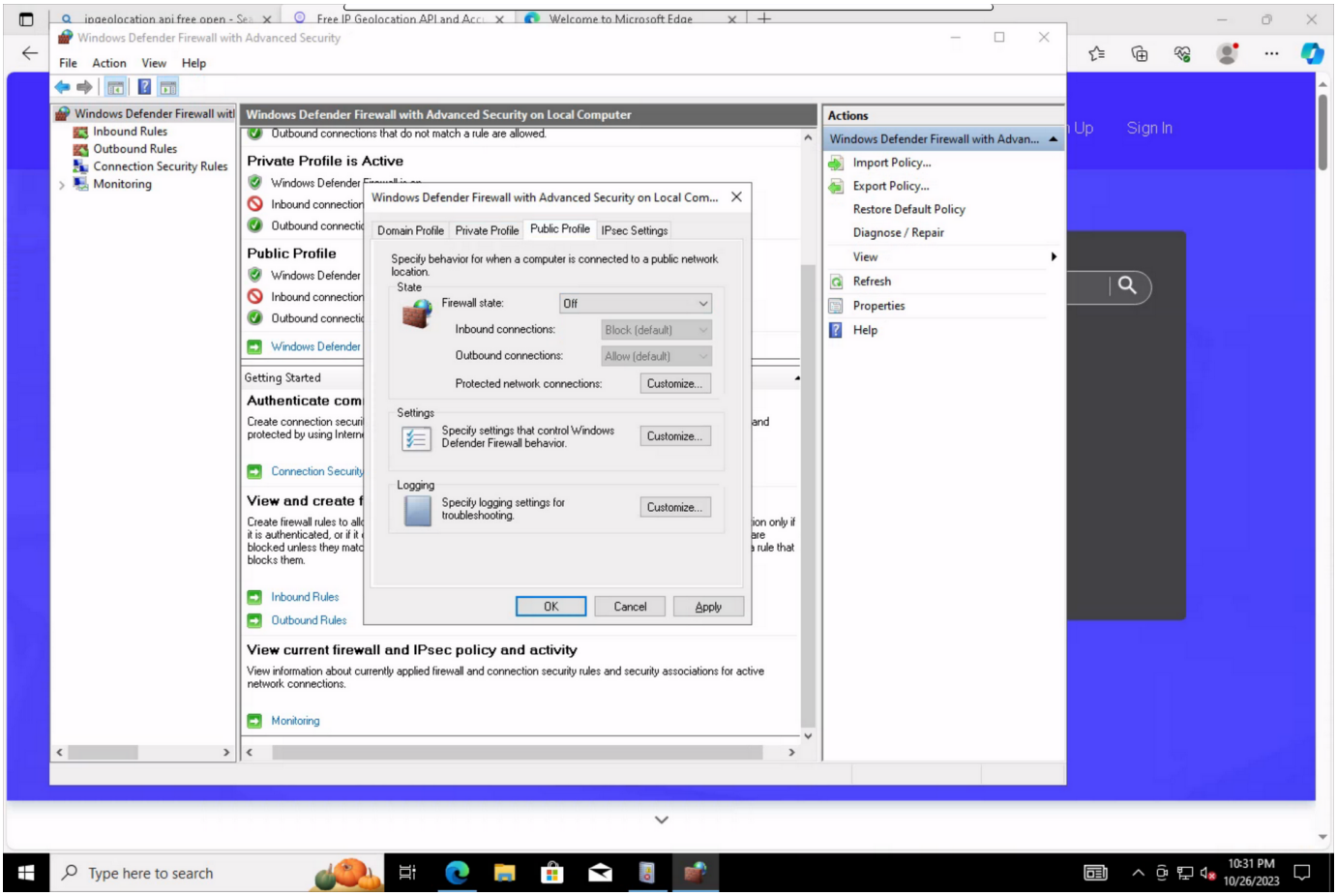


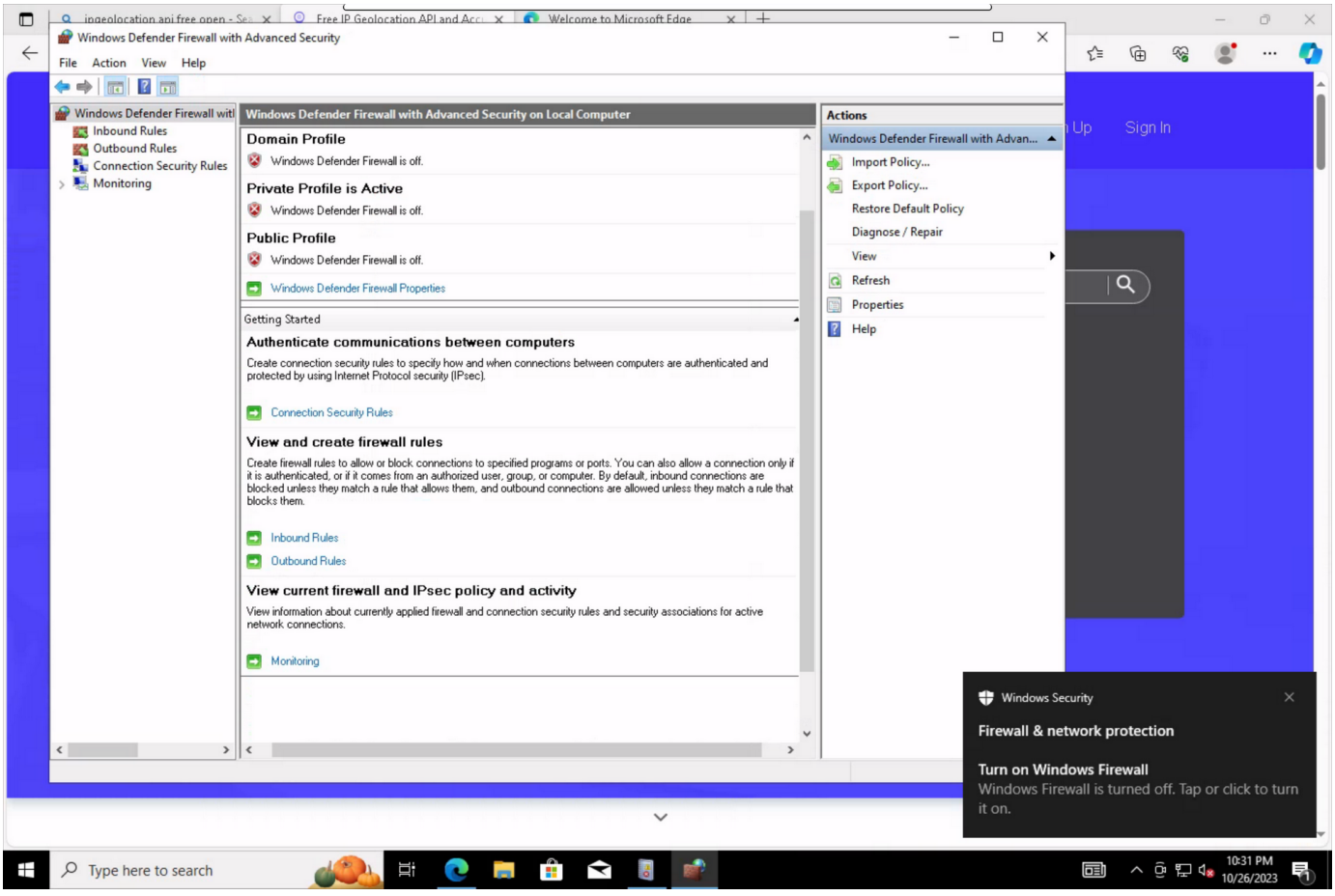
Accessing the website for the IP address Geolocation API for the script that I'll run later



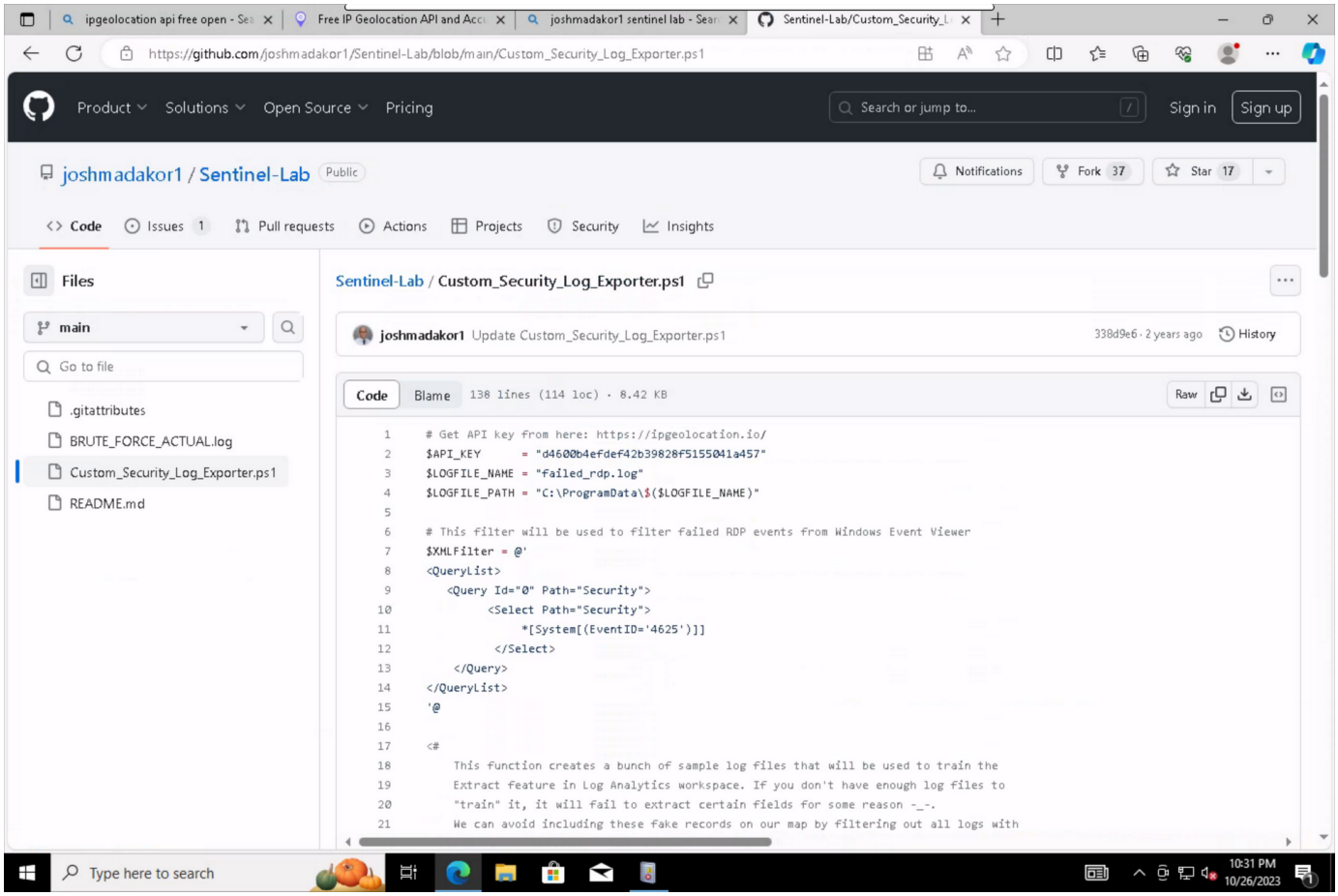
Turning off the firewall on the VM so that I can receive inbound traffic fromm all sources



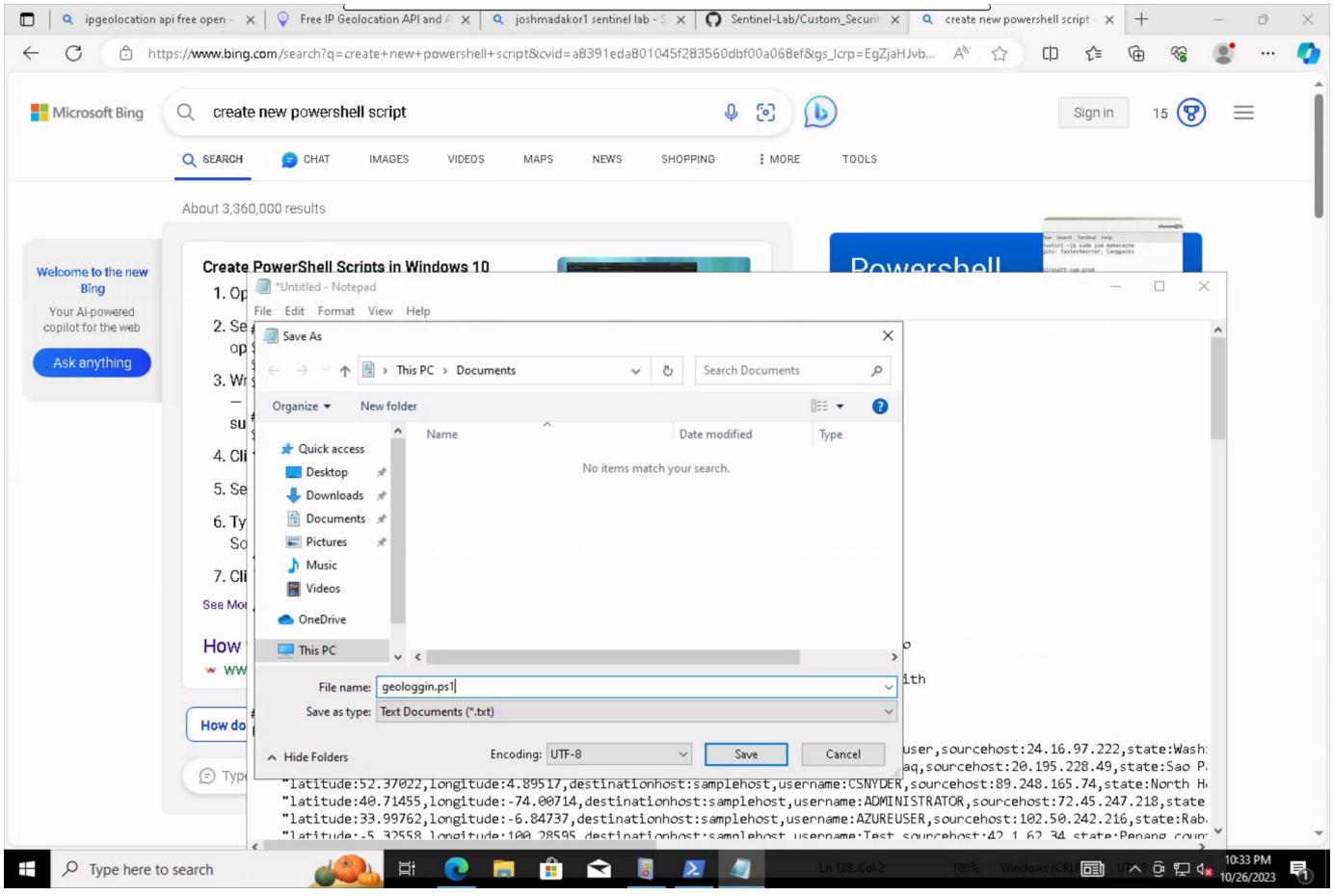




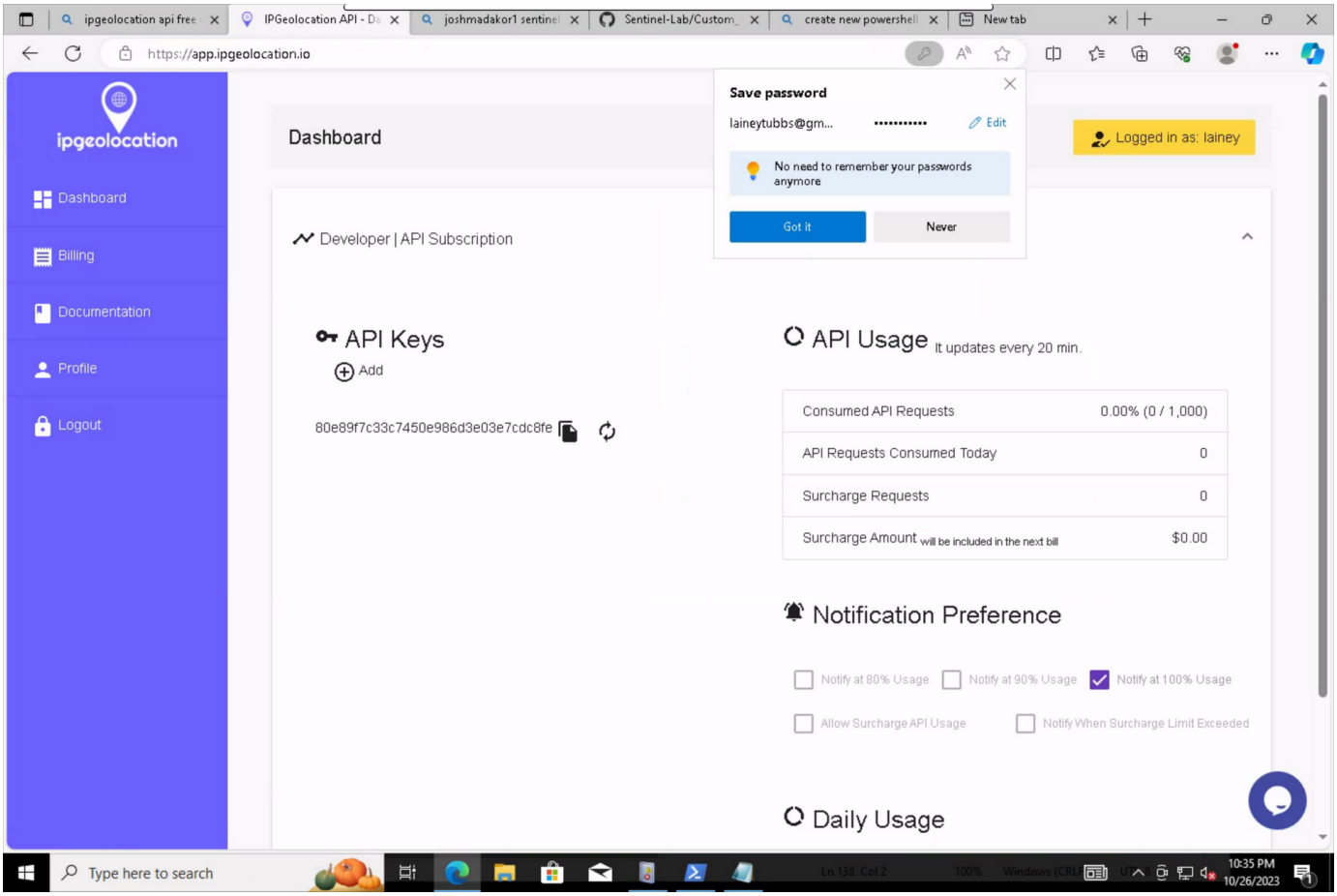
Navigated to Josh Madakor's Github page to download the Powershell script that logs all failed login attempts, the attacker's IP addreesses and their geolocation



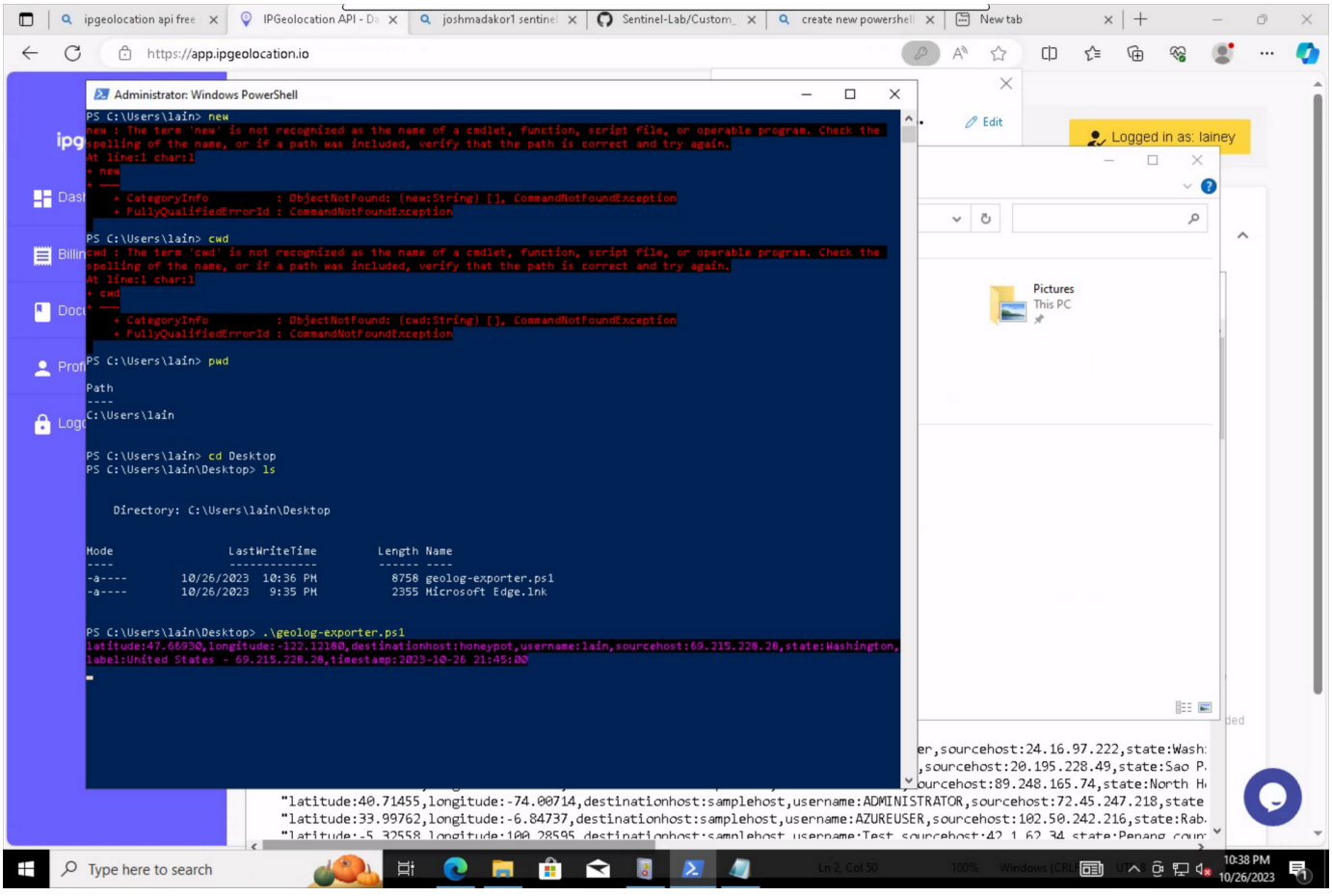
Saving the powershell onto the desktop



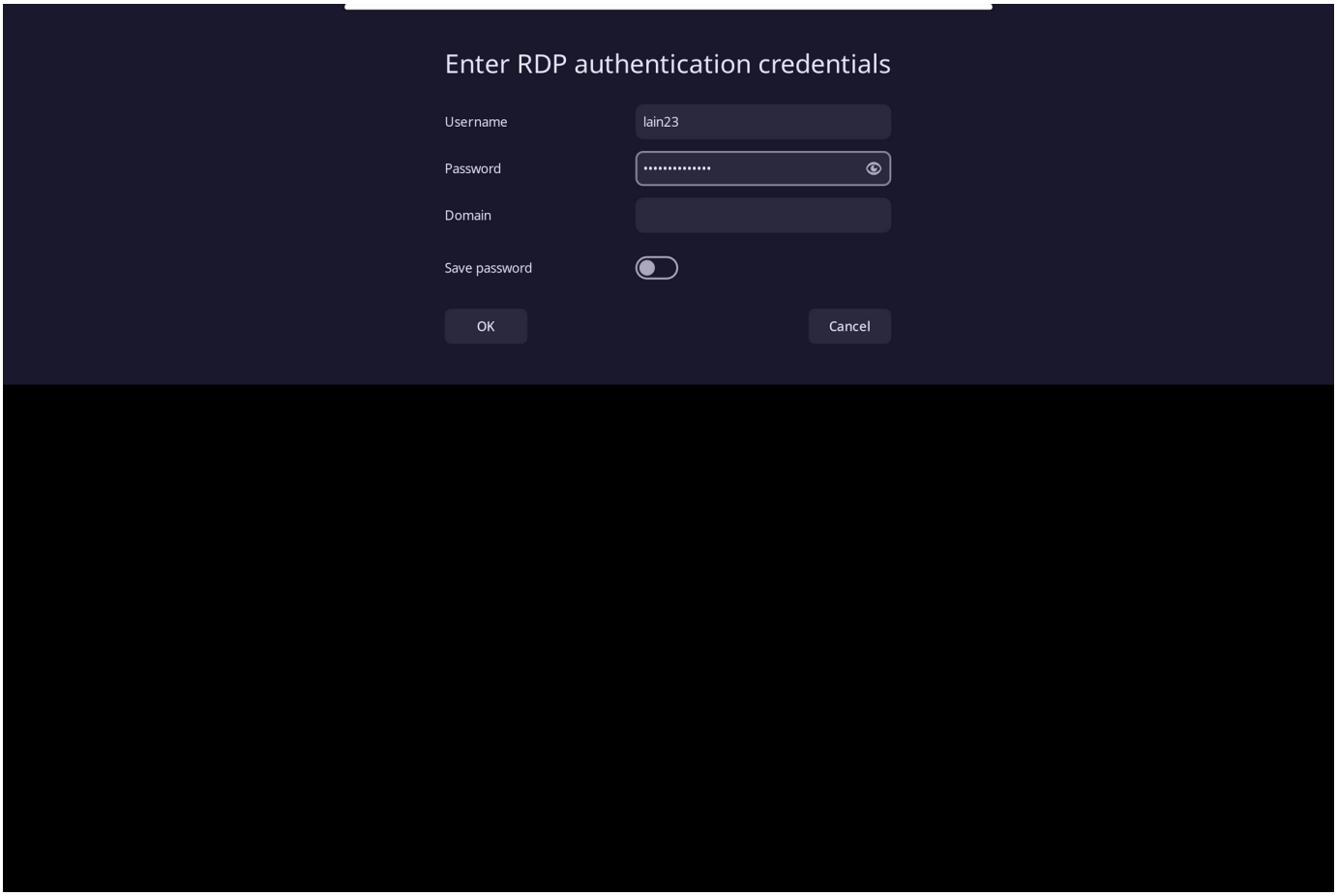
Copying the API key and replacing it



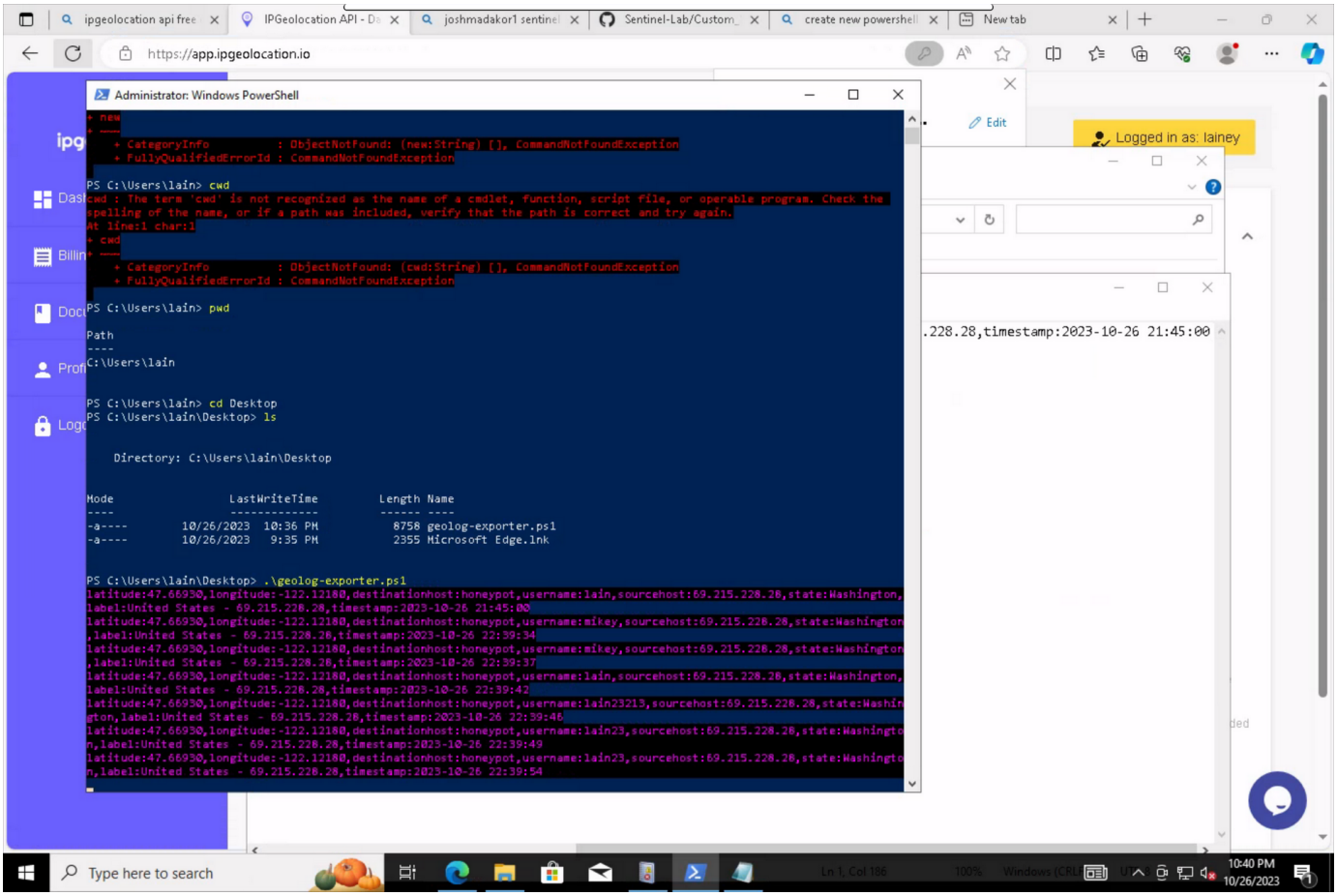
Ran the Geologgin powershell script



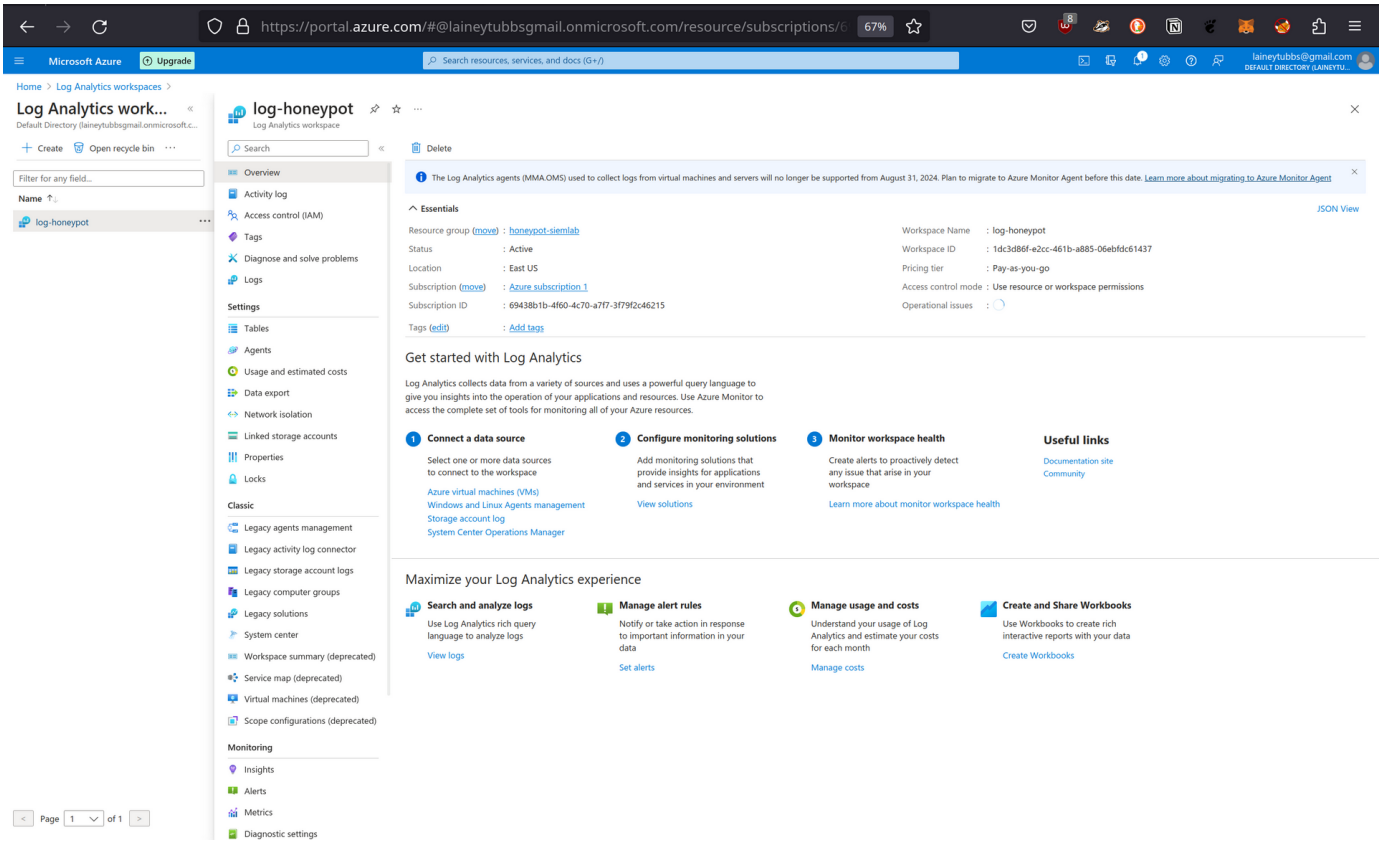
Attempting bad login credentials so that I can see it be logged in the script



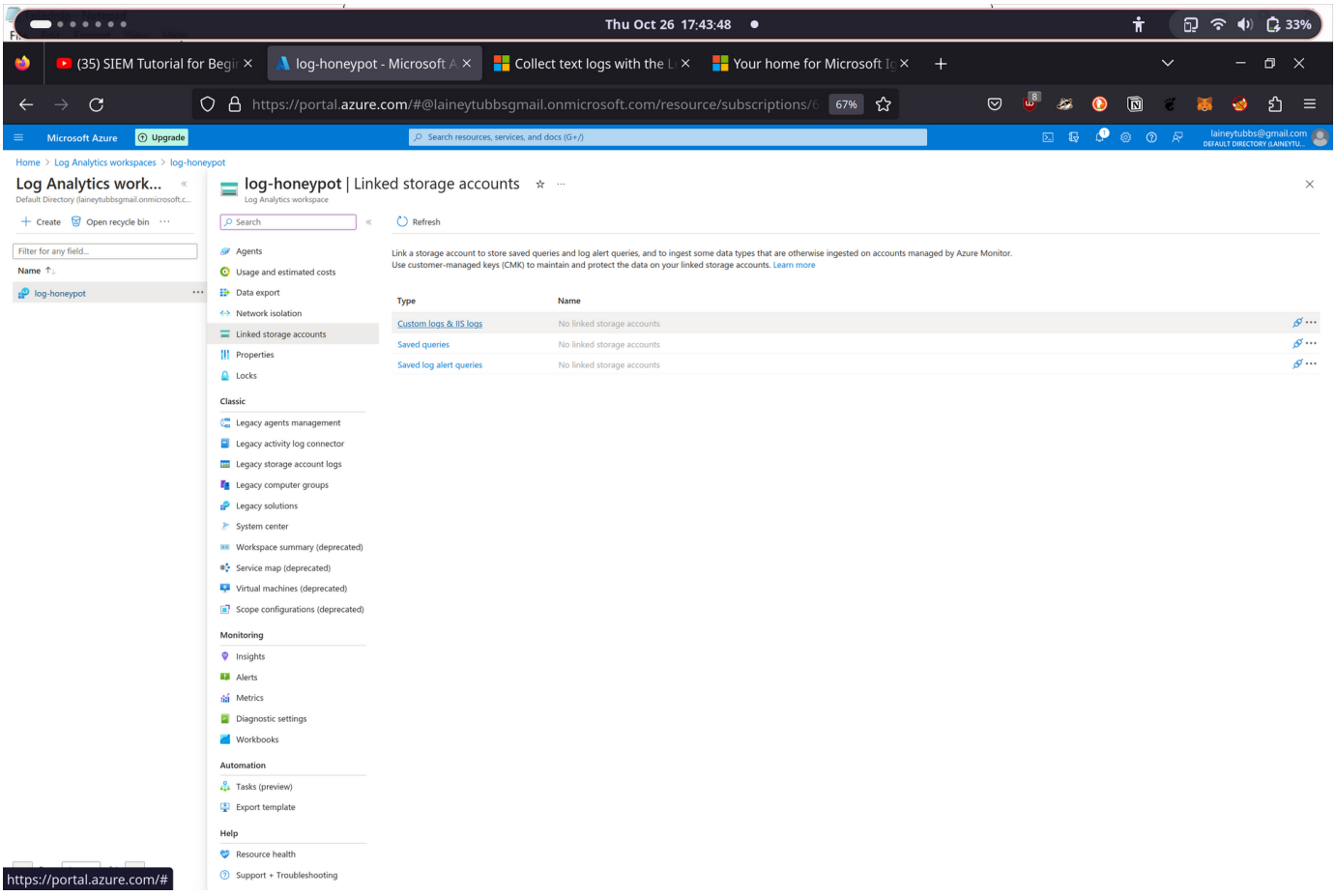
After a few attempts of failed logons, I seee them come up on the output of the script

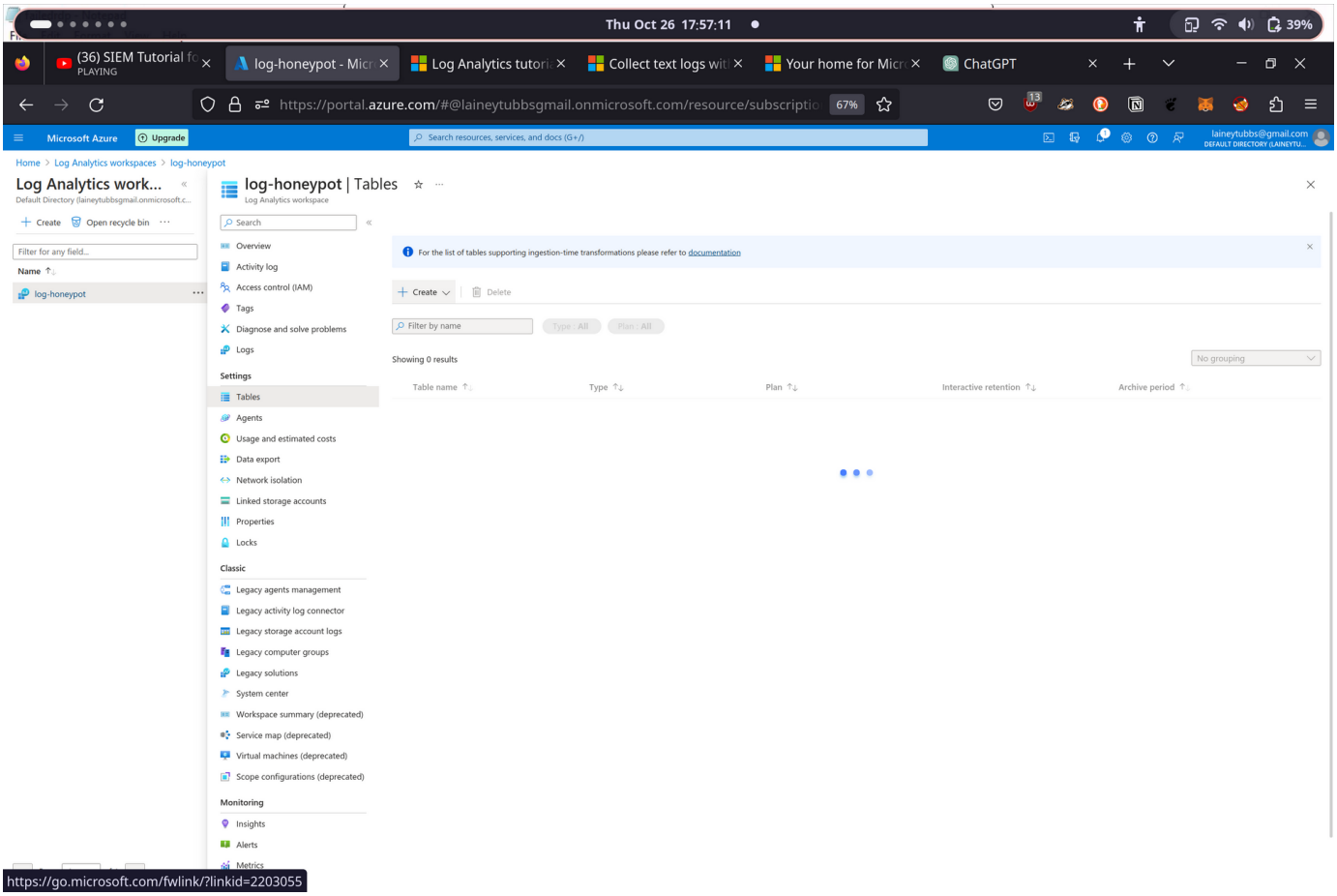


Back to the Log Analytics Workspace

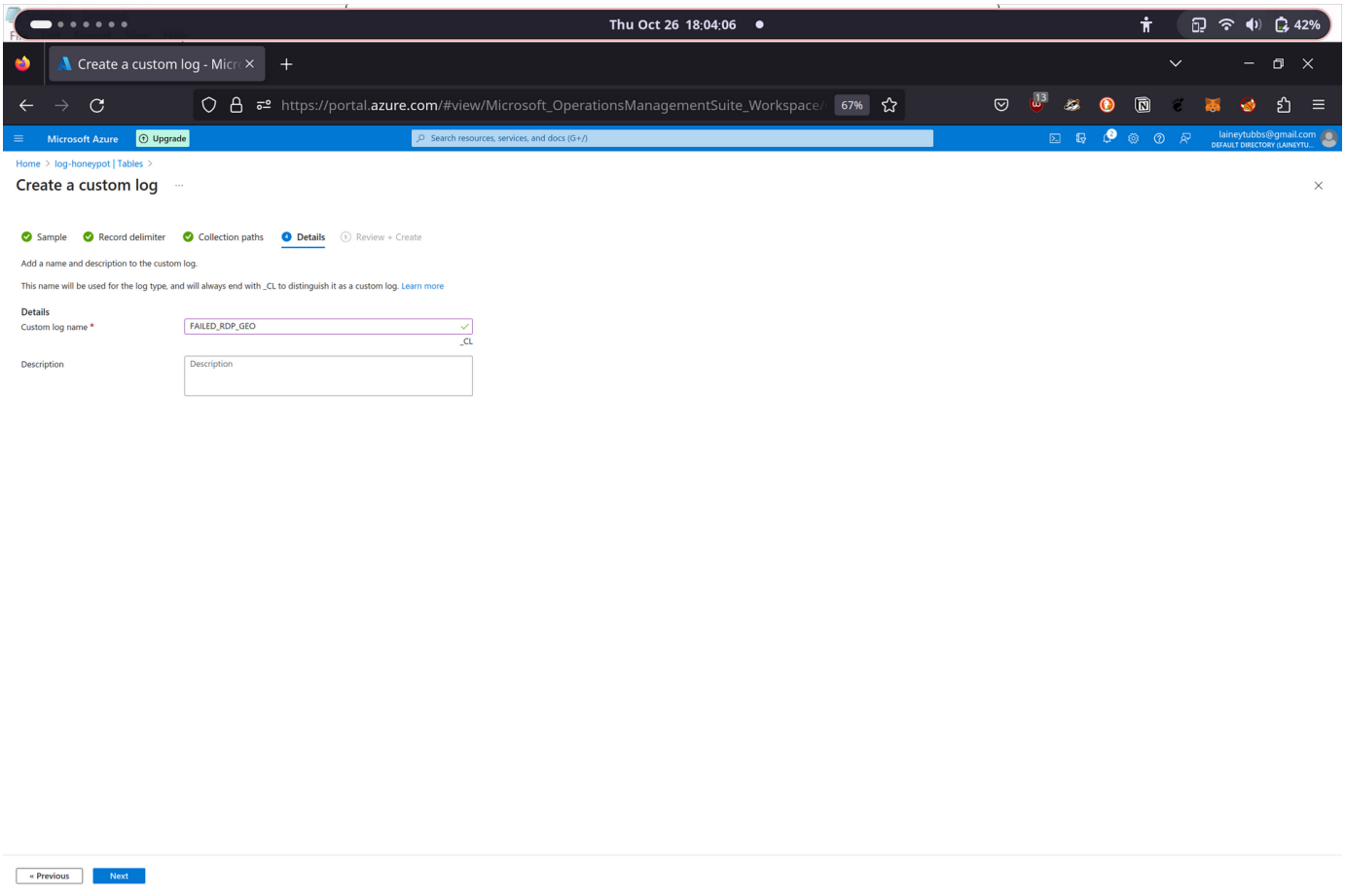


Going to the Tables tab in Log Analytics workspace

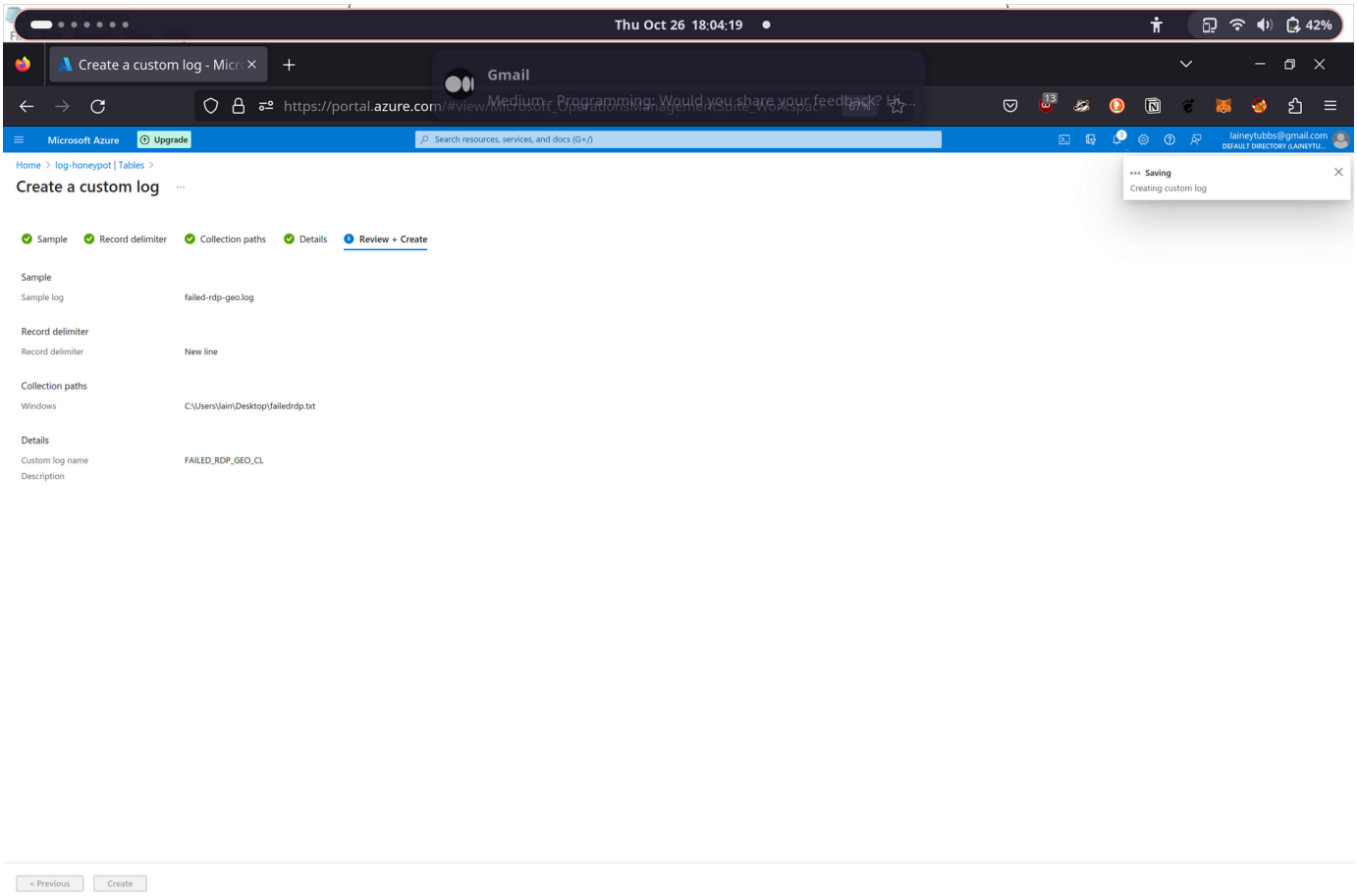




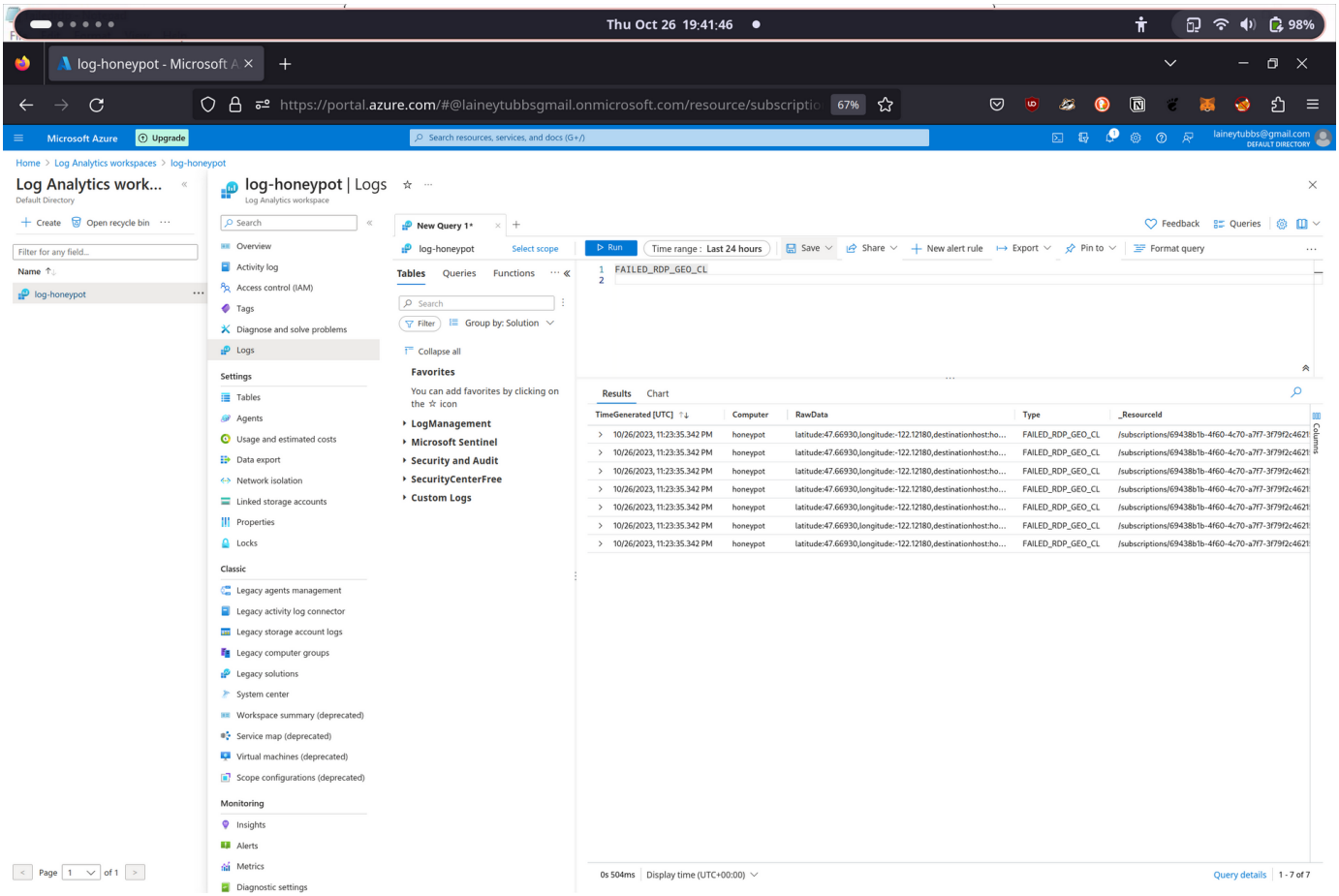
Naming custom log Failed-rdp-geo



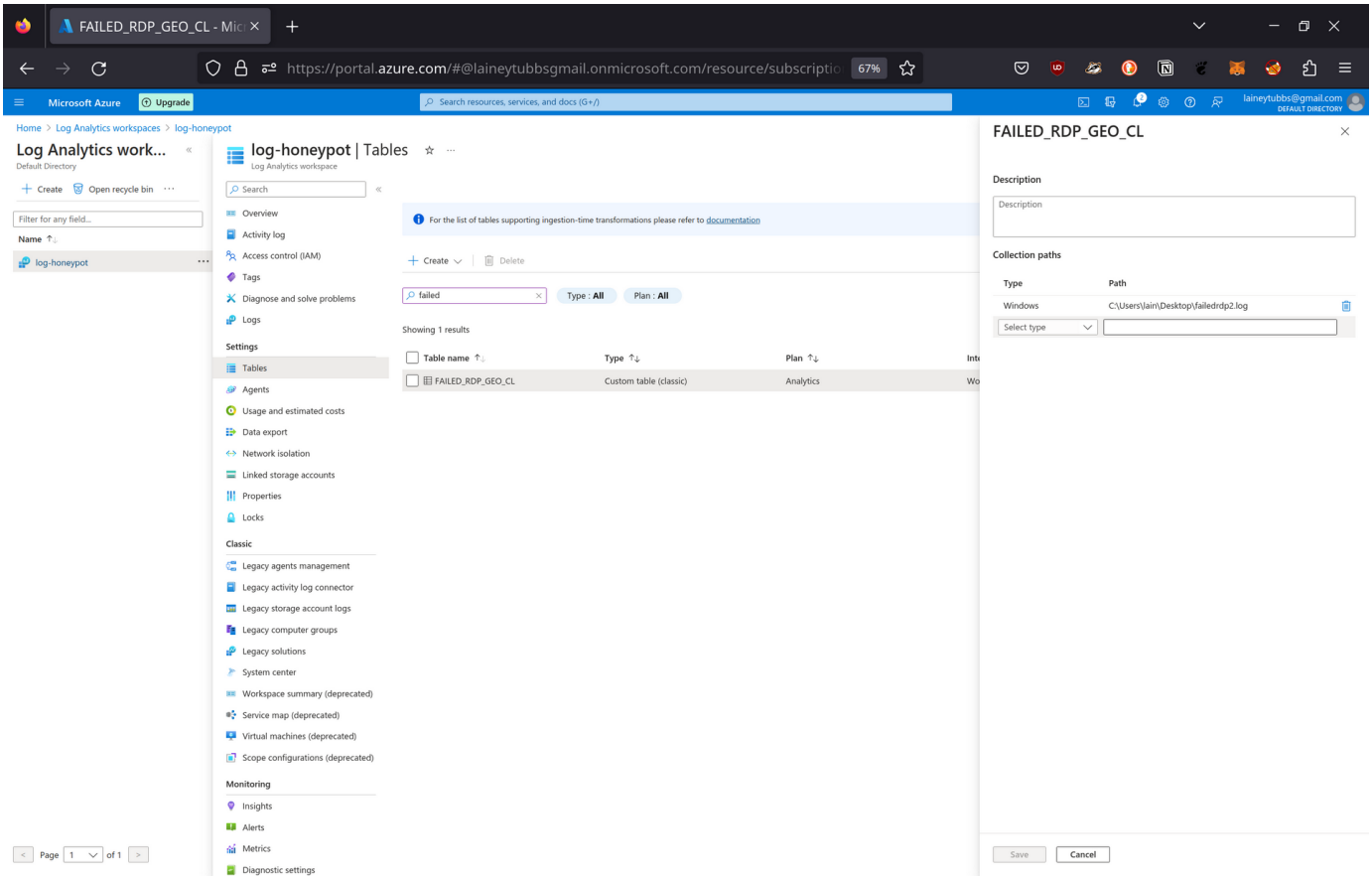
Finishing creating the custom log to be collected by Log Analytics Workspace



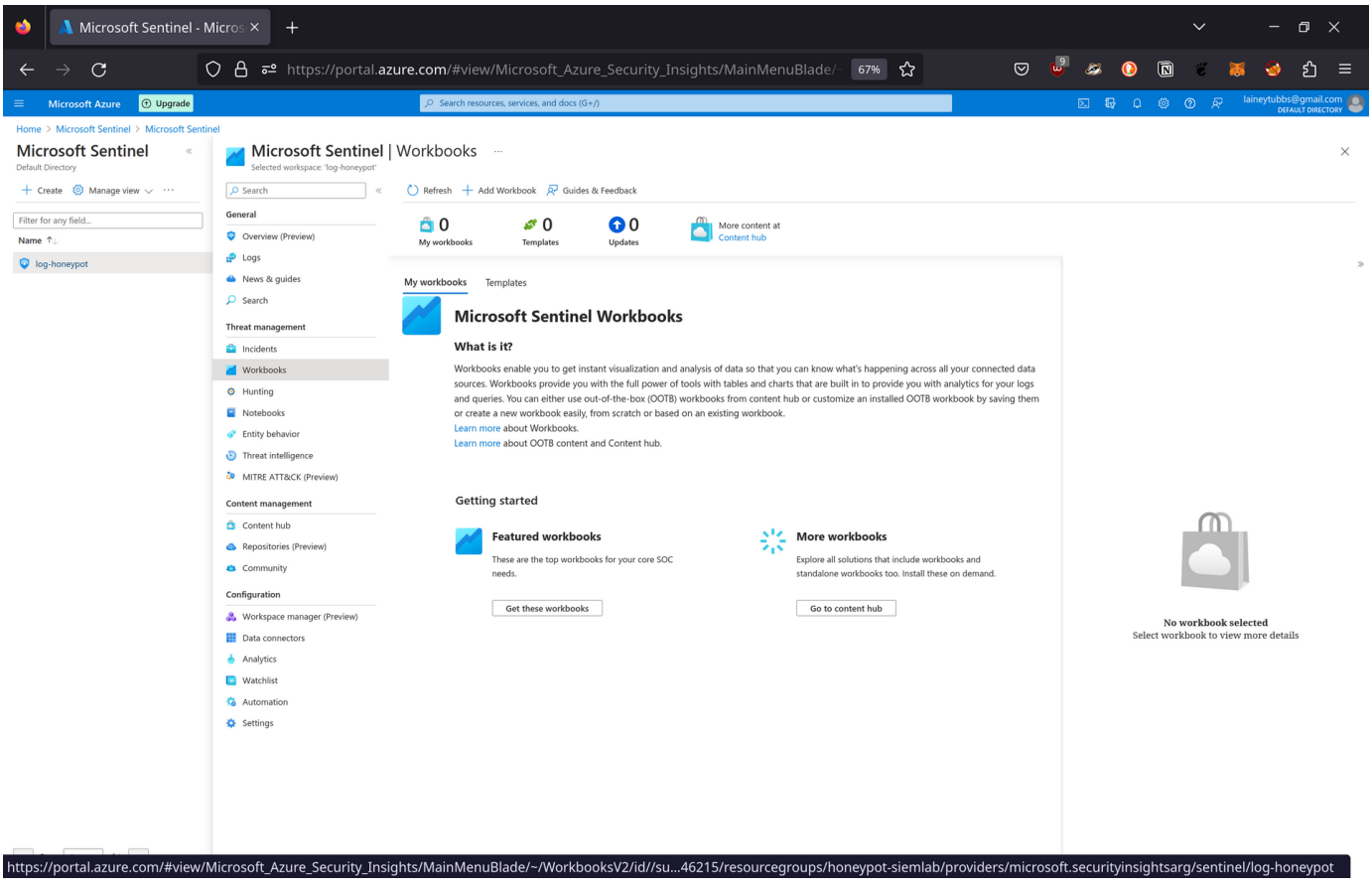
After waiting a little bit, I queried the log to get the entries



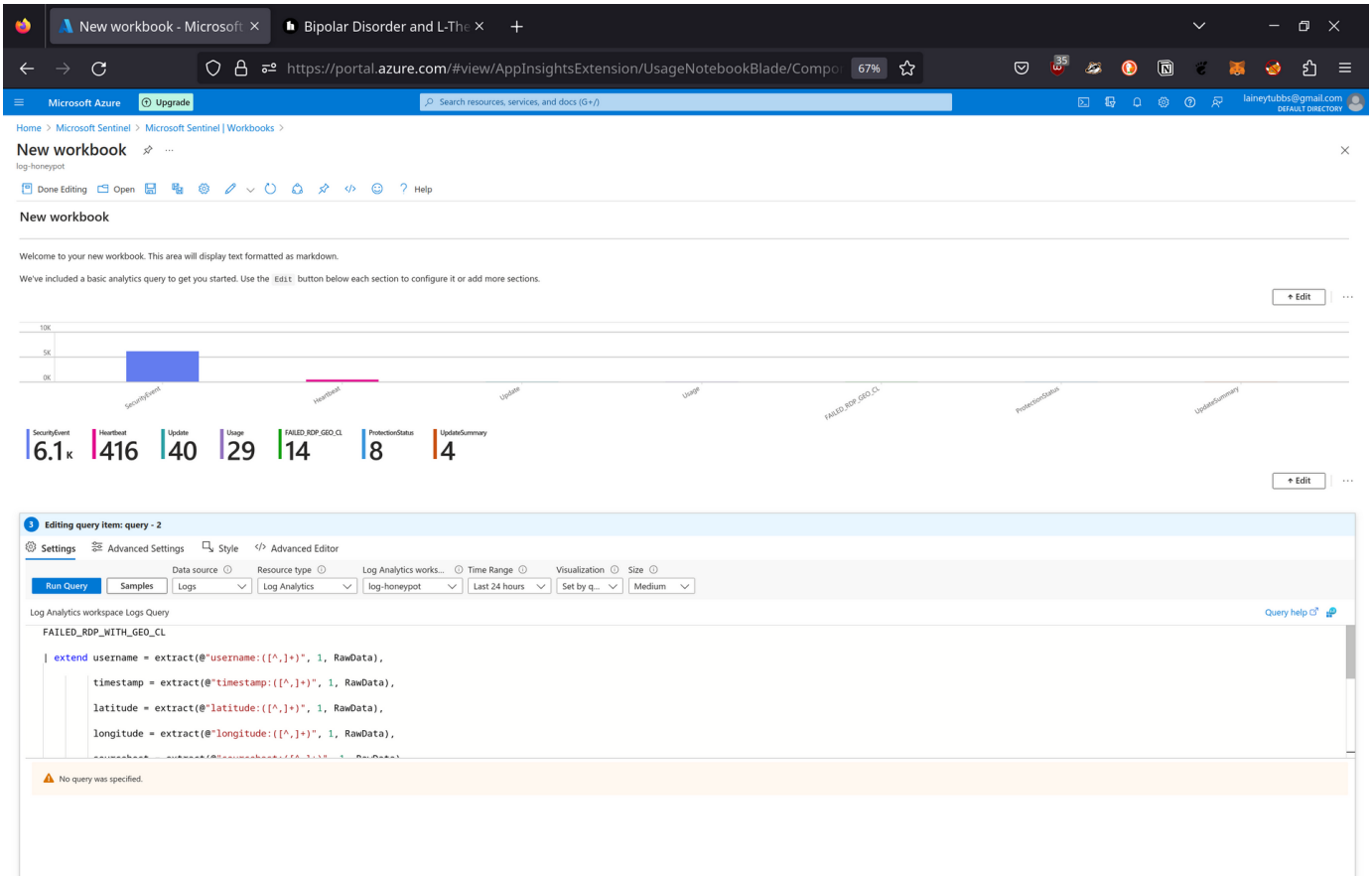
Looking at the custom log and the log file entry*



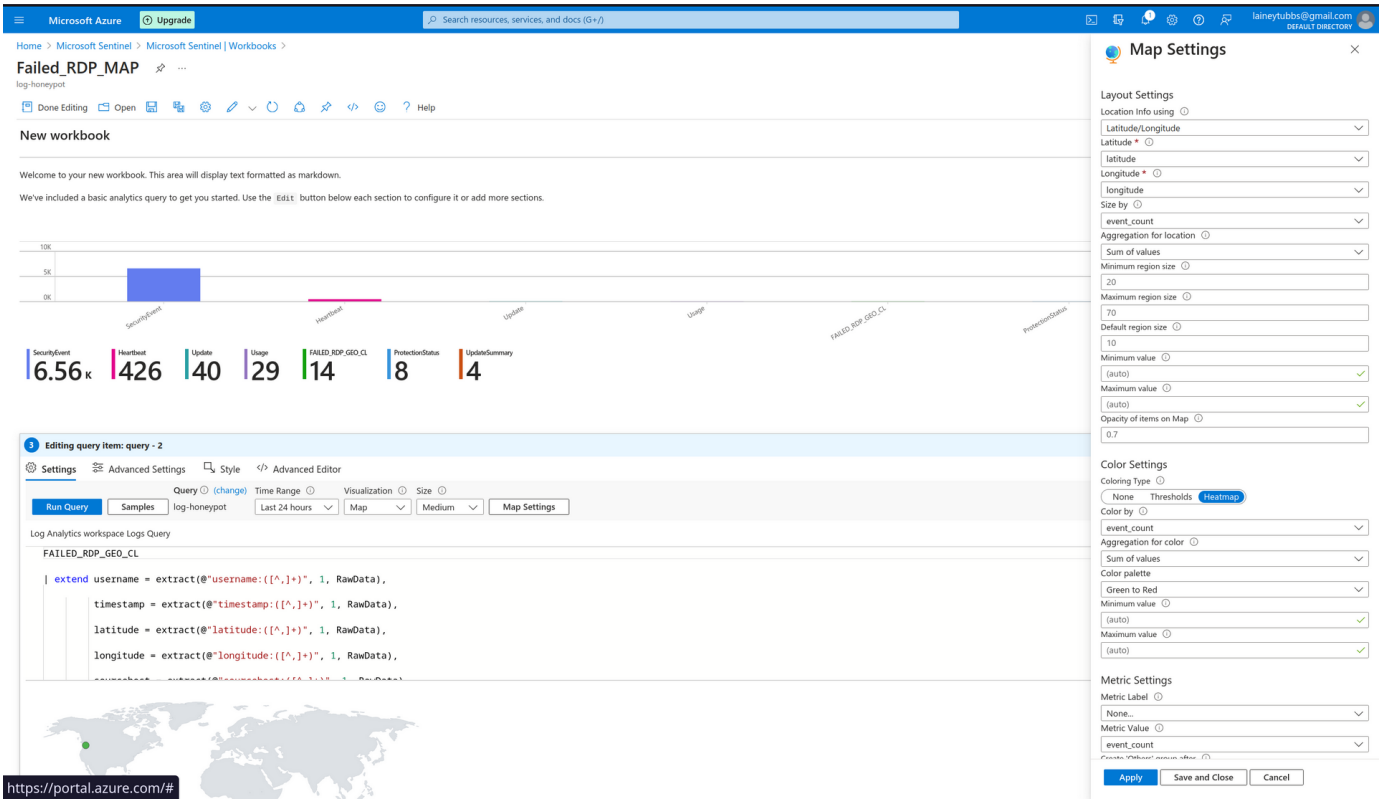
Back to Azure Sentinel

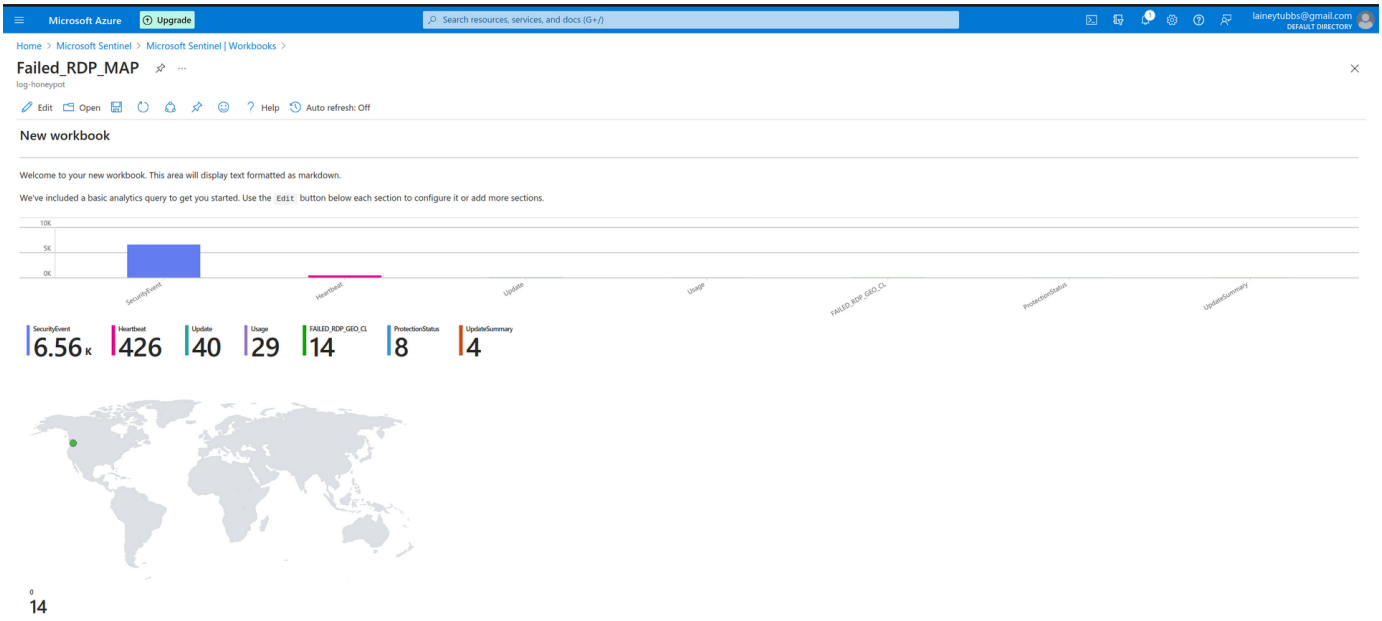


Creating a Rule for the Siem to sort the entries by geographic location



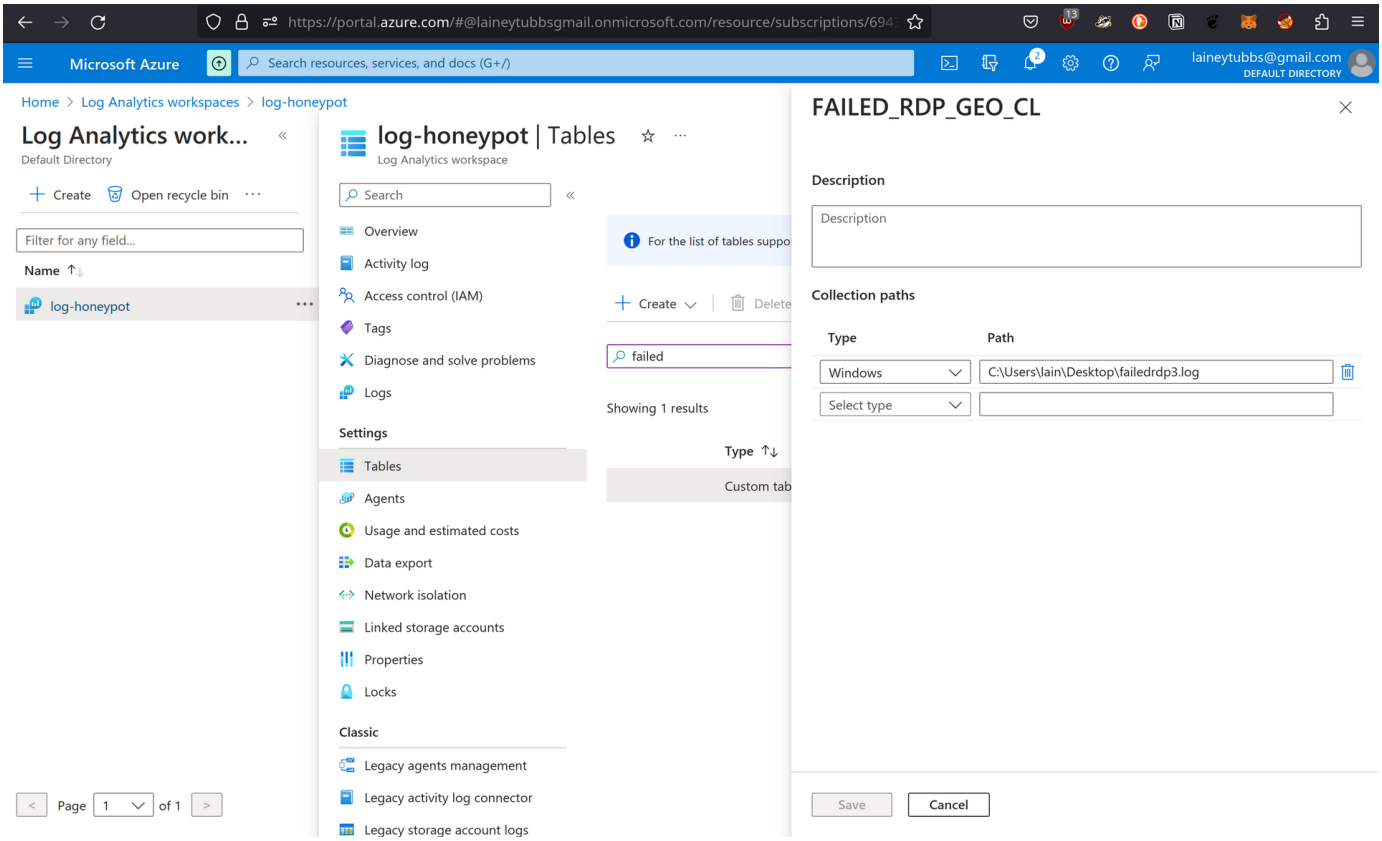
Switched to Map View to show indicators by location



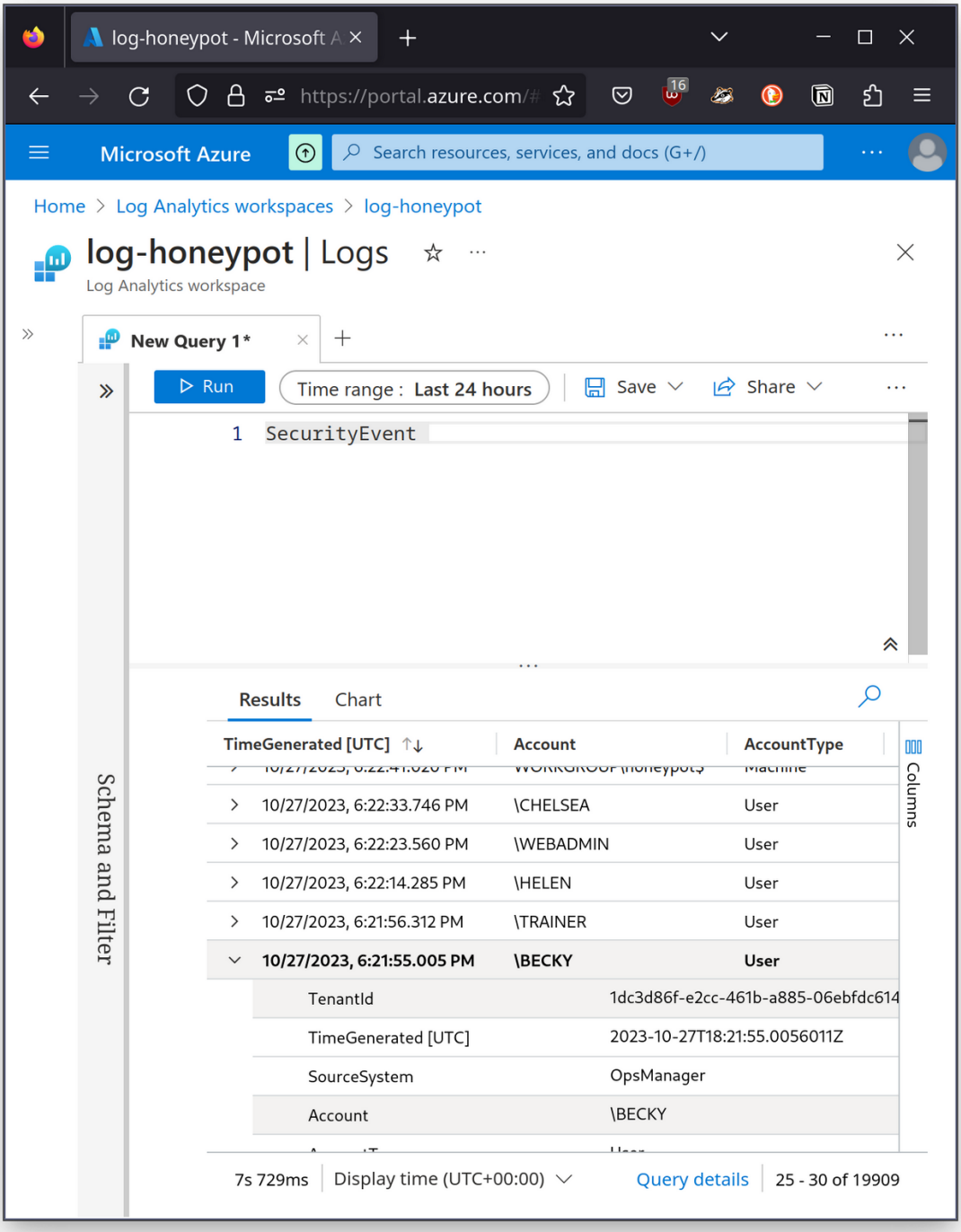


https://portal.azure.com/#

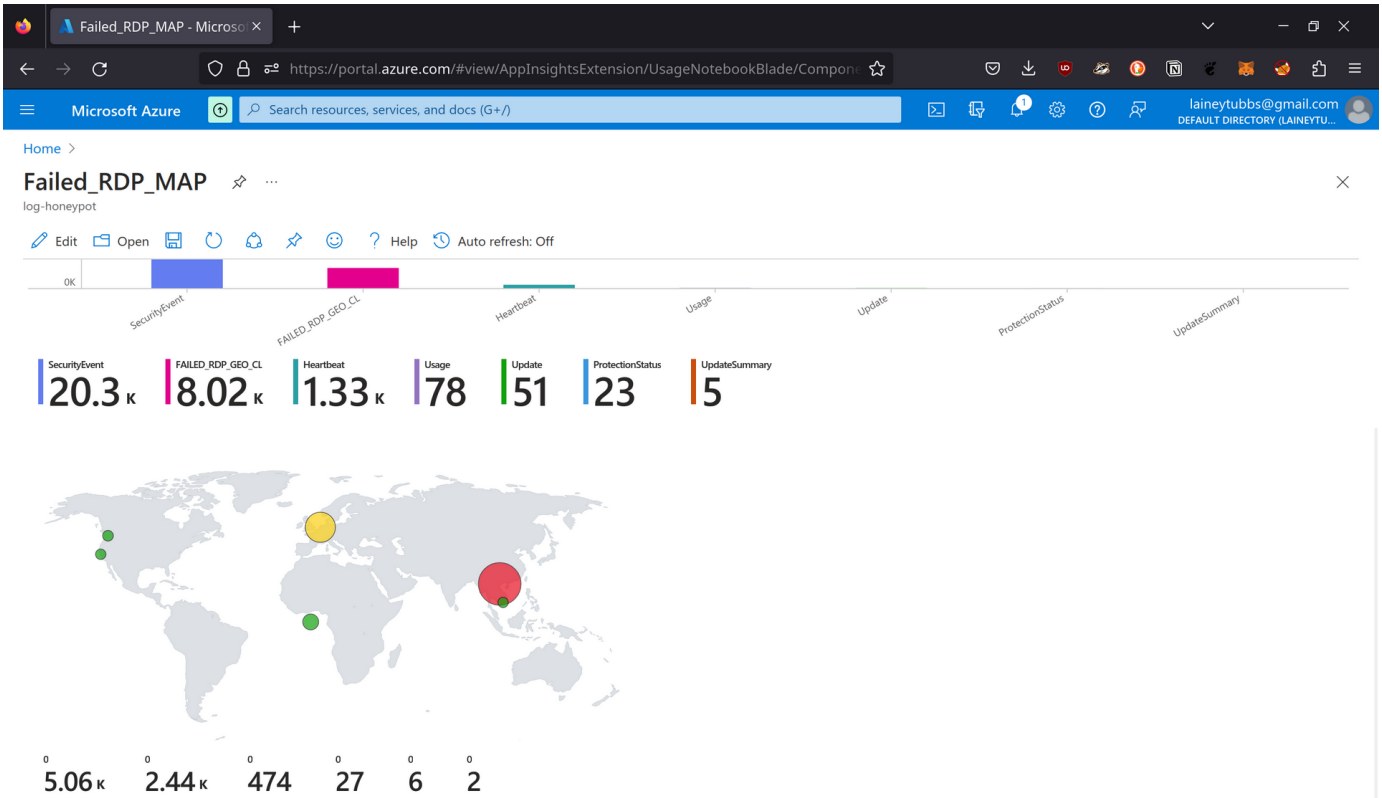
Corrected the path of the log entry on the VM in the Log Analytics Workspace



After waiting for a few minutes for the log entry to update



Checking the map to see all the updated entries from the people attempting to access the Honeypot.


Failed_RDP_MAP - Microso
https://portal.azure.com/#view/AppInsightsExtension/UsageNotebookBlade/Compon
Microsoft Azure
Search resources, services, and docs (G+/)
laineytubbs@gmail.com
DEFAULT DIRECTORY (LAINEYTU...
Home
Failed_RDP_MAP
log-honeypot
Edit
Open
Help
Auto refresh: Off
0K
SecurityEvent
FAILED_RDP_GEO_CL
Heartbeat
Usage
Update
ProtectionStatus
UpdateSummary
SecurityEvent
20.3 K
FAILED_RDP_GEO_CL
8.02 K
Heartbeat
1.33 K
Usage
78
Update
51
ProtectionStatus
23
UpdateSummary
5
0
5.06 K
0
2.44 K
0
474
0
27
0
6
0
2