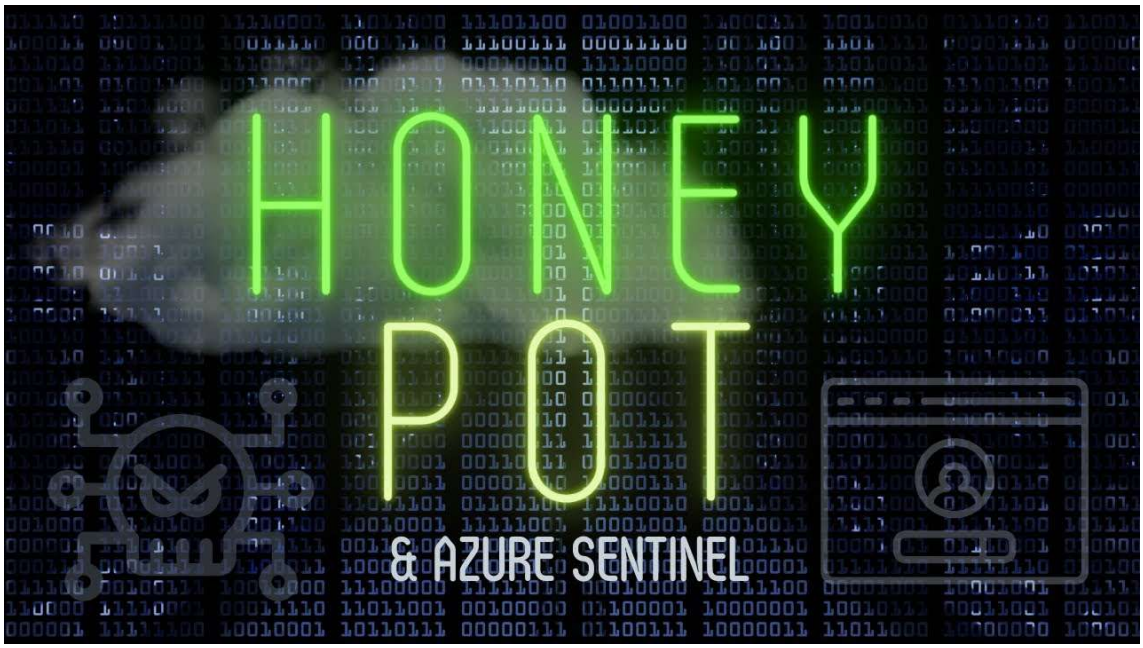
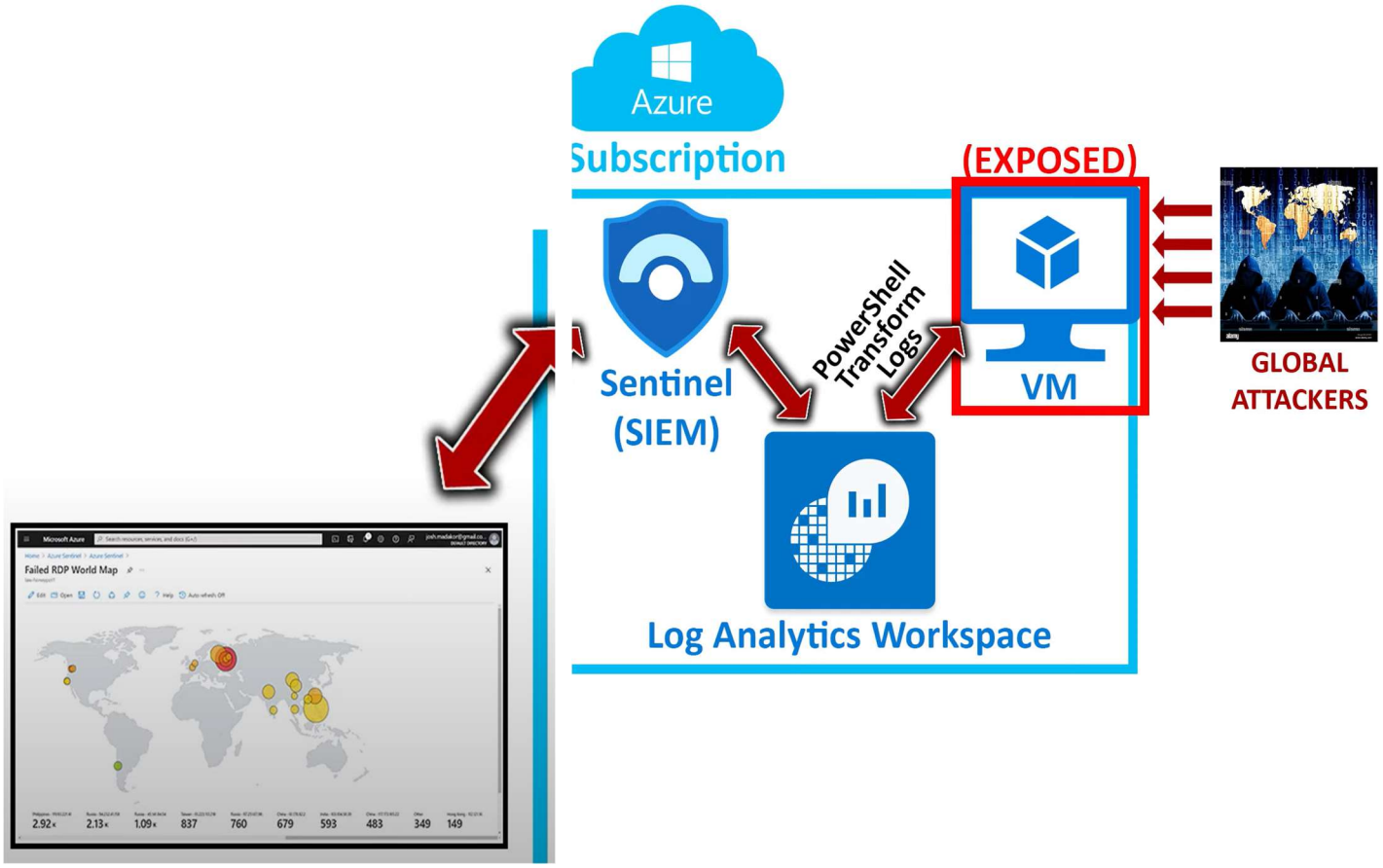


In this project I have set up the Microsoft Azure Sentinel (Cloud-based SIEM) and connected it to Honeypot created in Virtual Machine in Azure. This project has given me the opportunity to gain practical experience in the cybersecurity field.

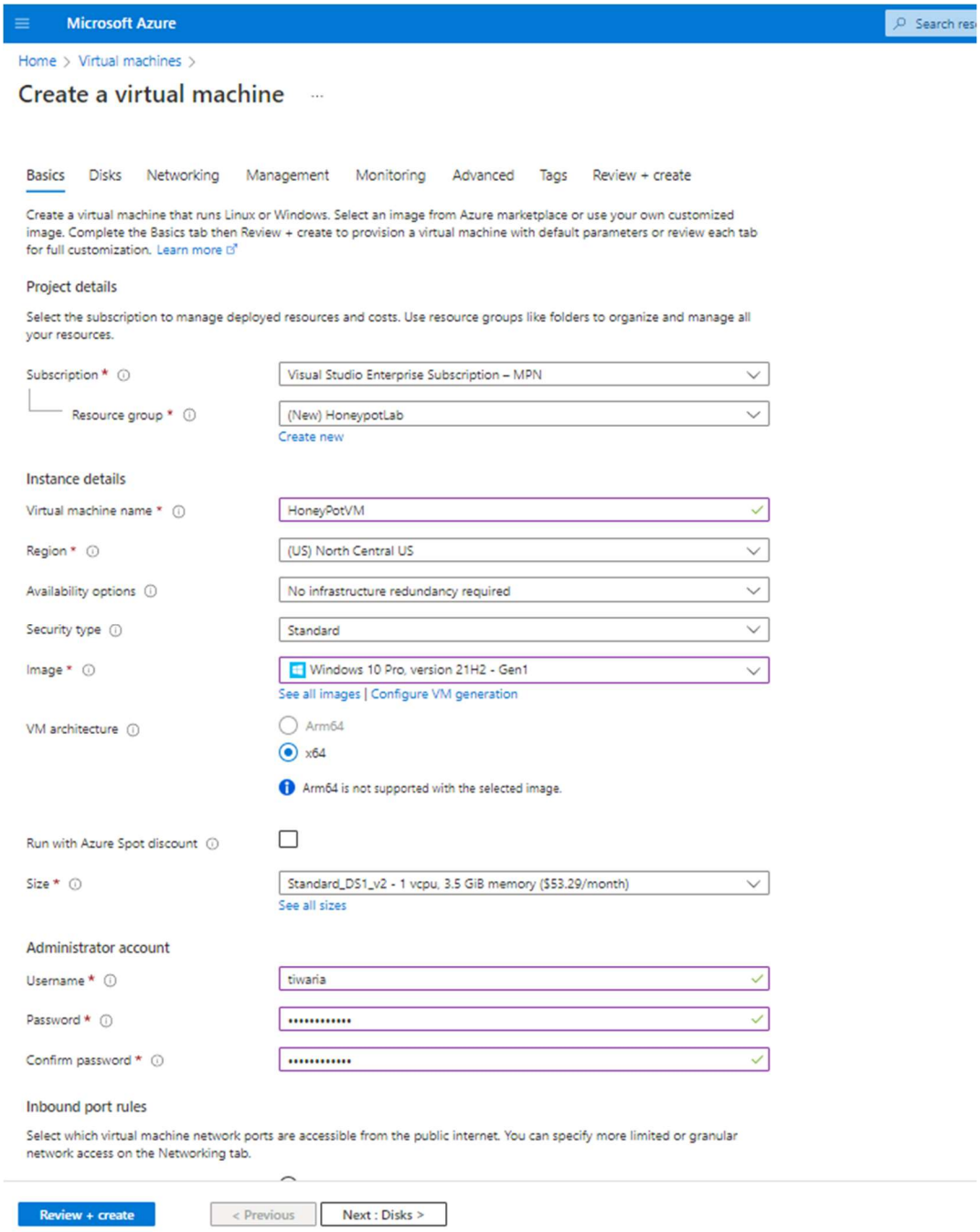
Tasks completed in this project include:

- Used custom PowerShell script to extract metadata from Windows
- Event Viewer to be forwarded to third party API to derive the geolocation data.
- Configured Log Analytics workspace in azure to ingest custom logs from windows Virtual Machine containing geographic information (Latitude, Longitude, state/Province, and country) using third party API.
- Configured custom fields in Log Analytics workspace with the intent of mapping geo-data in Azure sentinel.
- Configure Azure Sentinel (Microsoft Cloud SIEM) workbook to display global attack data (RDP Brute Force) on world map based on physical location and magnitude of attacks.

Diagram of the project

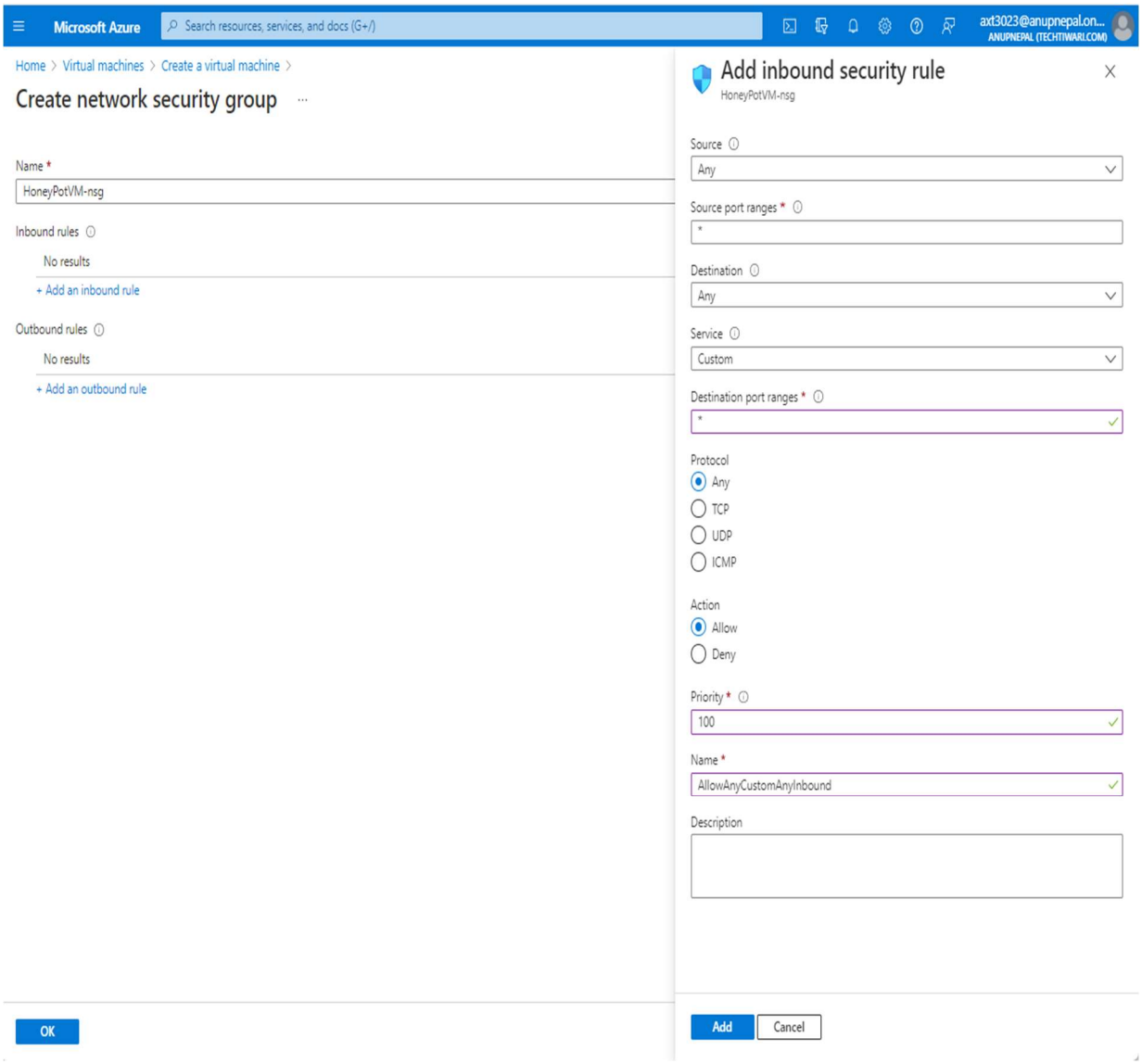


Create a virtual machine using Virtual Machine Resource and set up the basics with the data as shown below

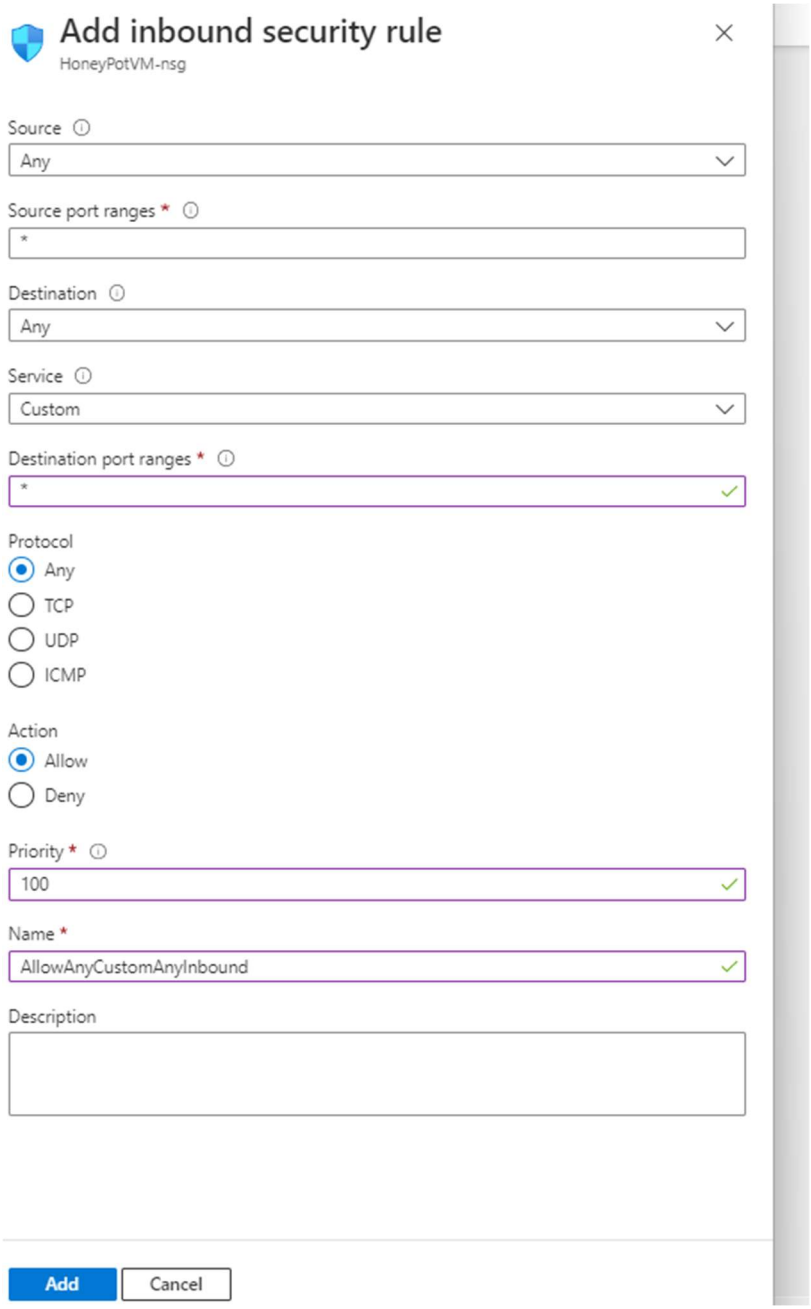


Under the Networking tab configure the new security group and remove the

existing rule and create new rule as shown below

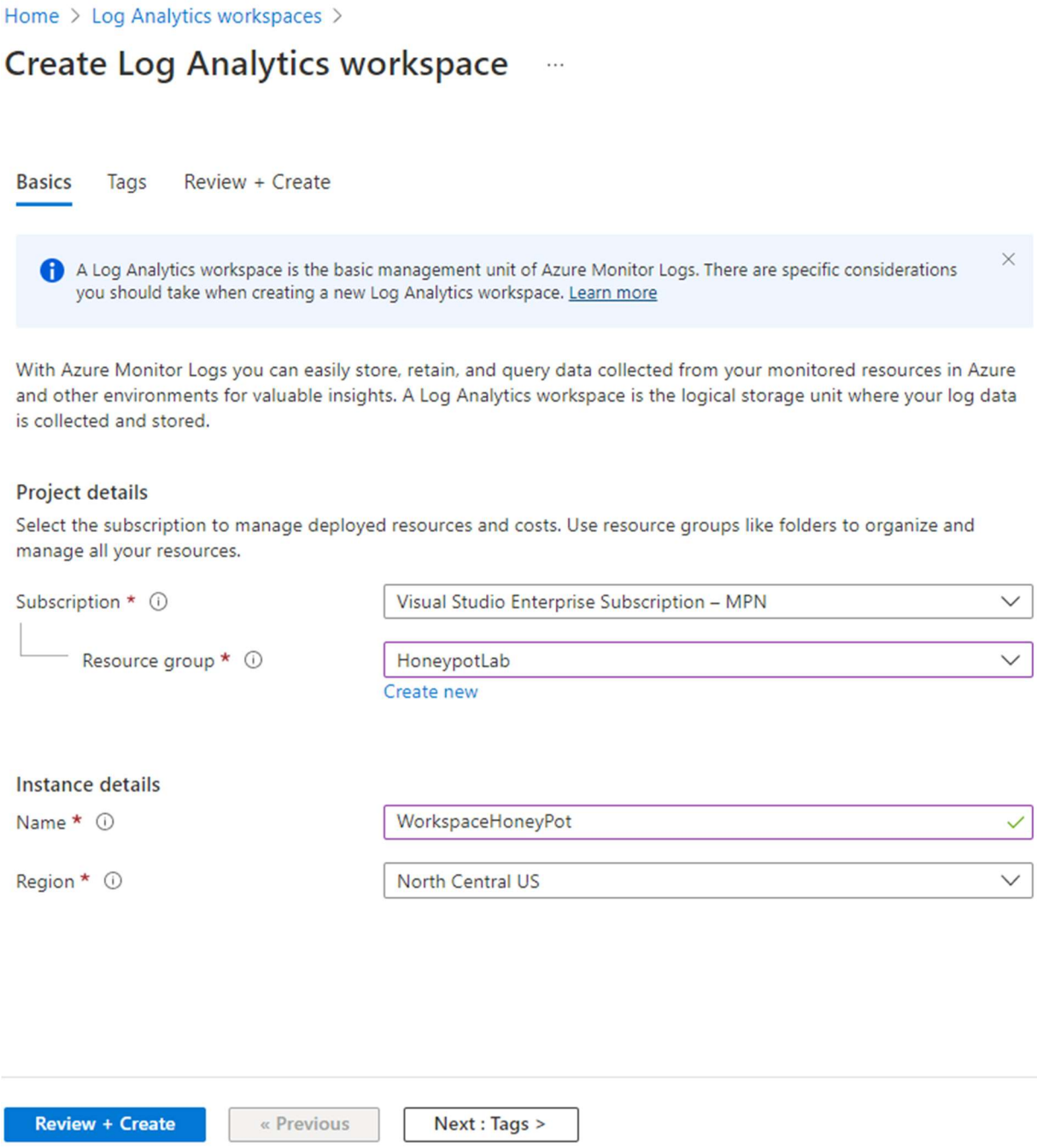


Since this virtual machine is being used as Honeypot, it is made easily accessible to hackers which will attract them to conduct brute force attack With following inbound rules.

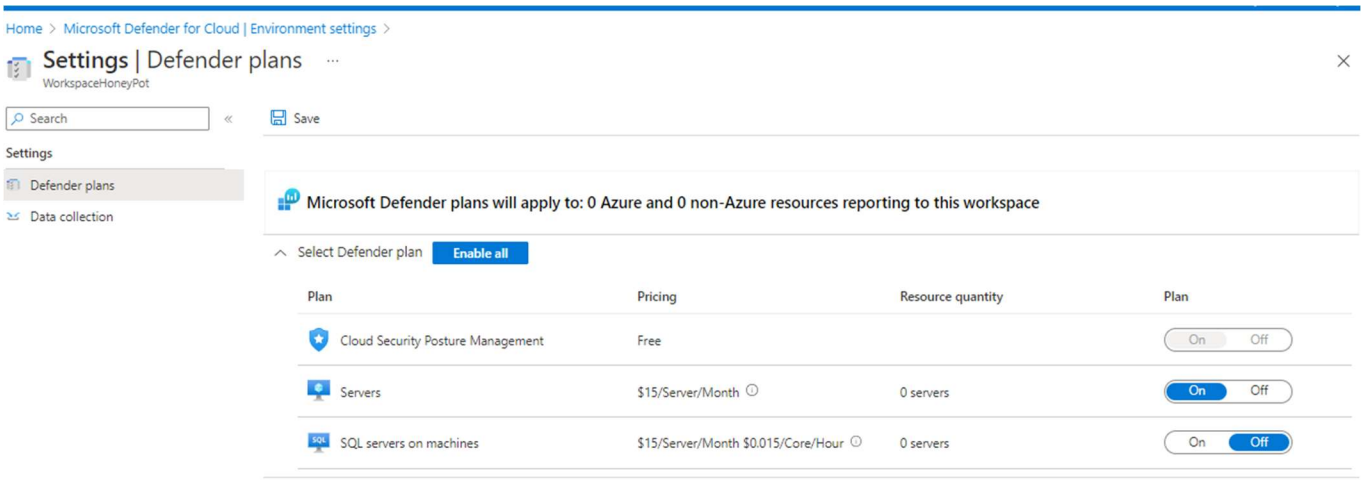


Creating Log Analytics workspace:

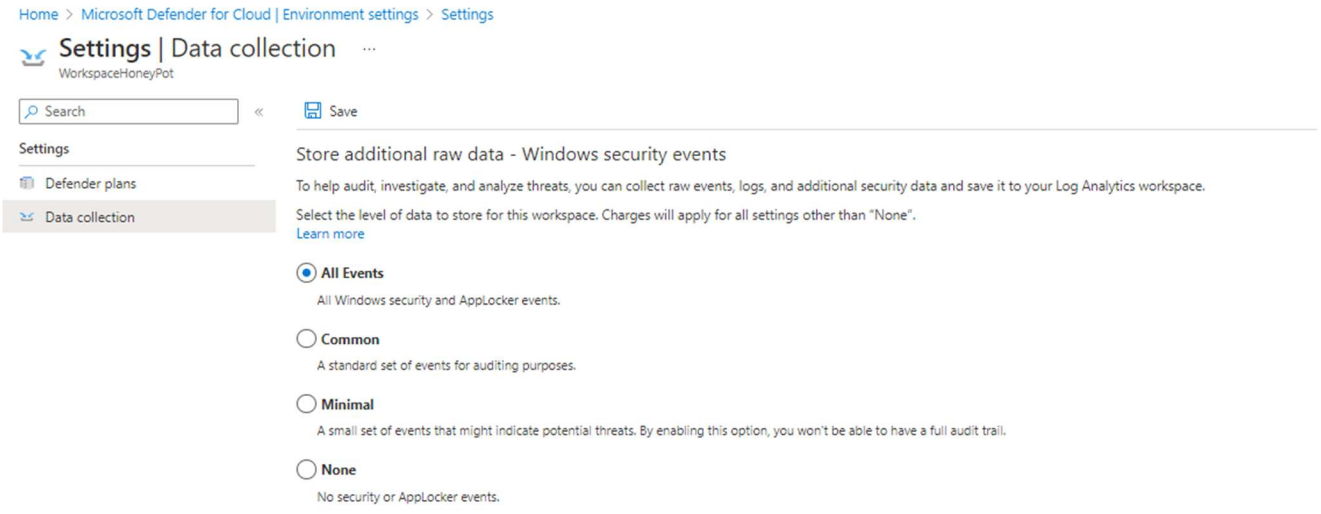
It is created to ingest custom logs from virtual machine that contains geographic location



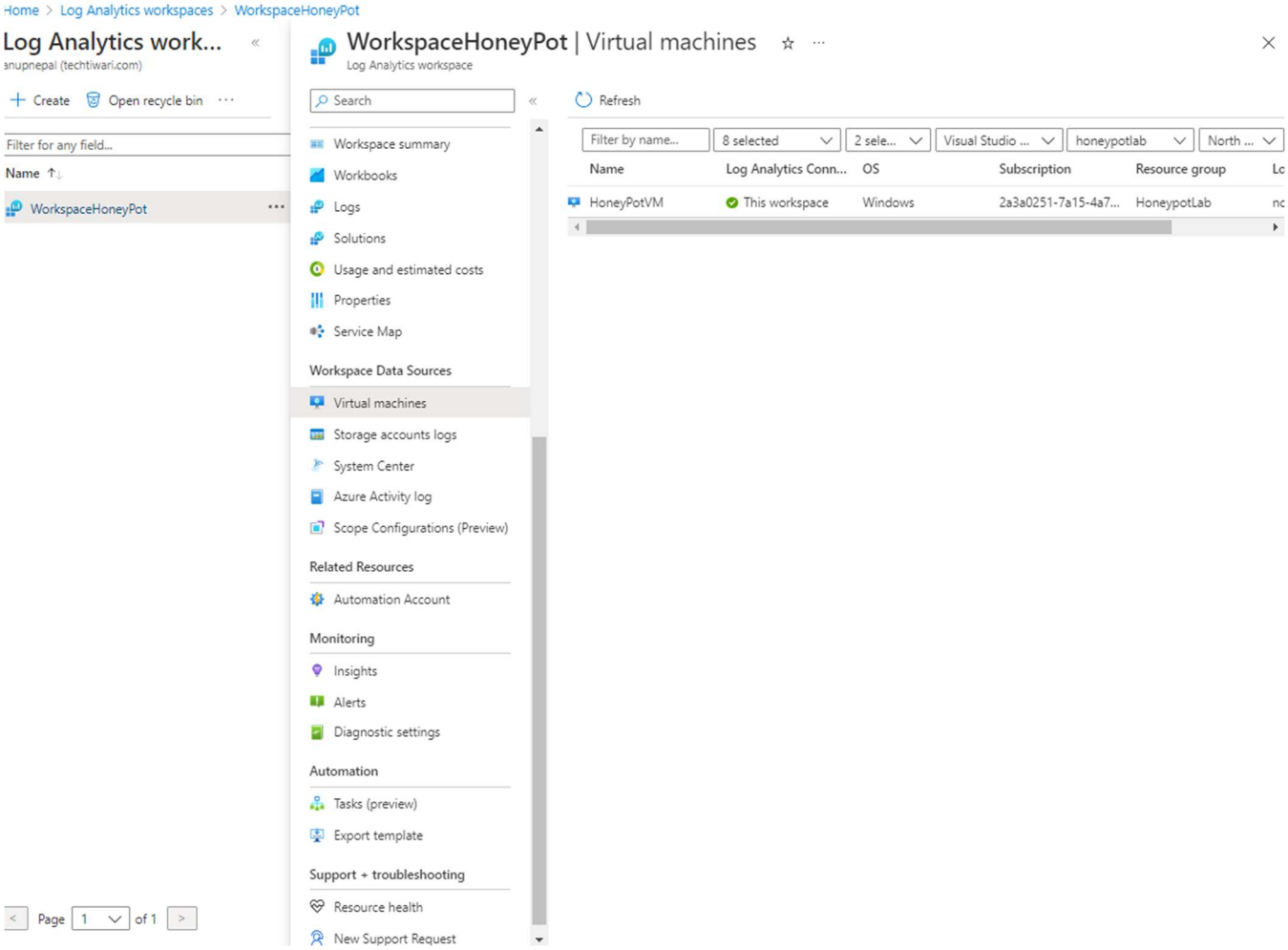
Turn on Microsoft Defender on for the virtual server by going into Microsoft Defender for cloud



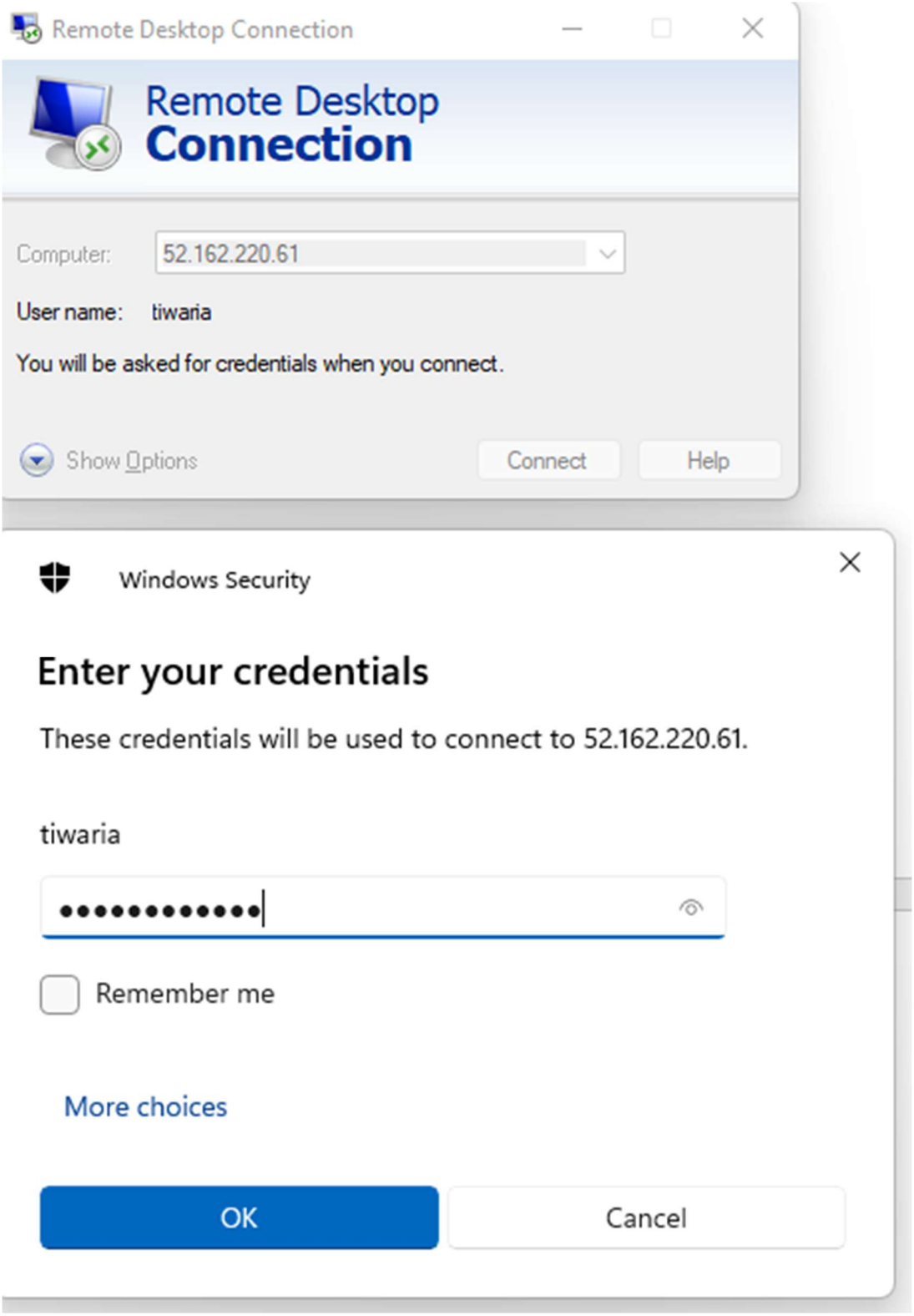
Click on All Events in Data collection to enable collection of all events which will eventually be sent to log Analytics



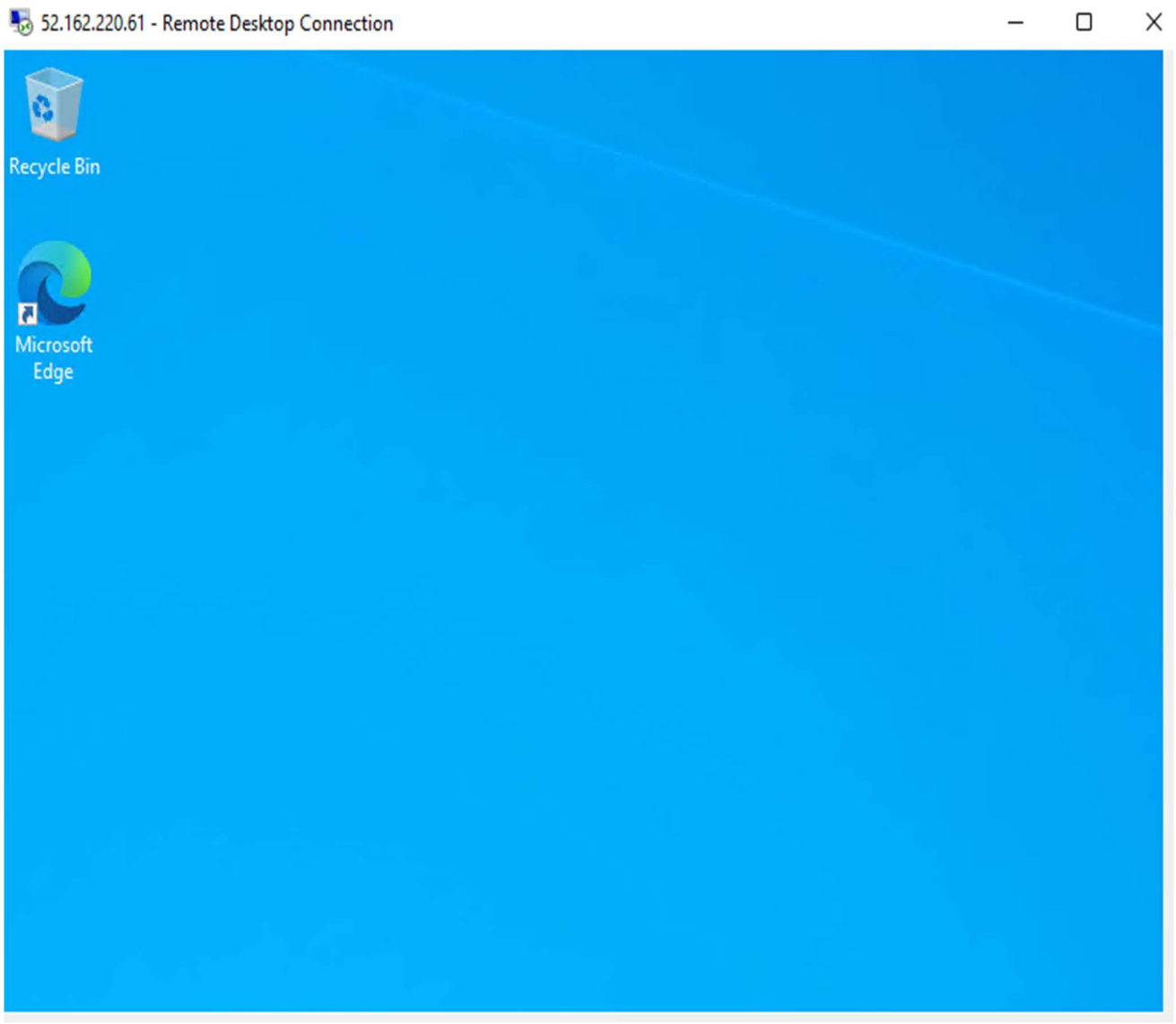
Connect Log Analytics Workspaces to the Virtual Machine. This will collect all logs from Virtual machine



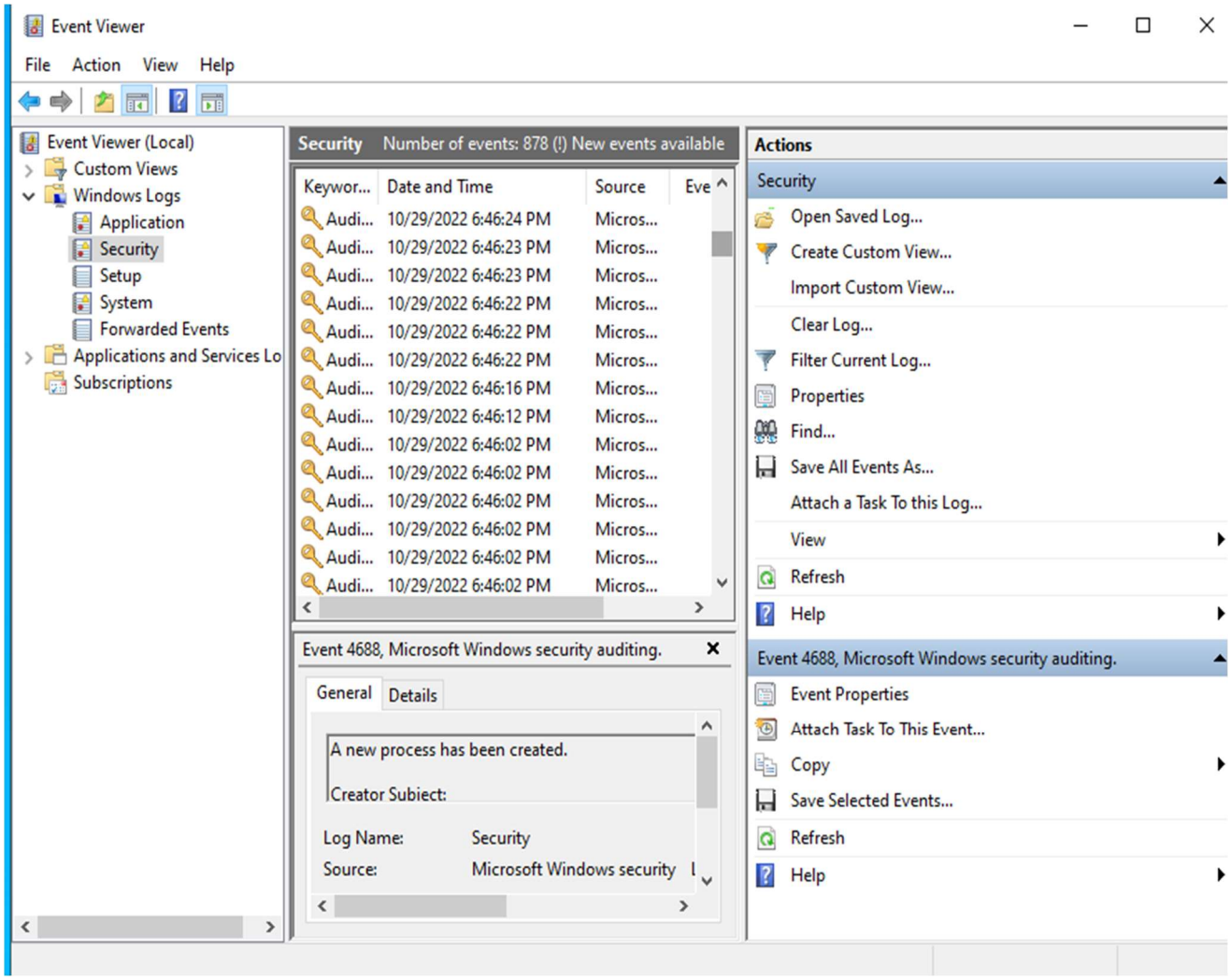
Login to the virtual Machine with the remote Desktop



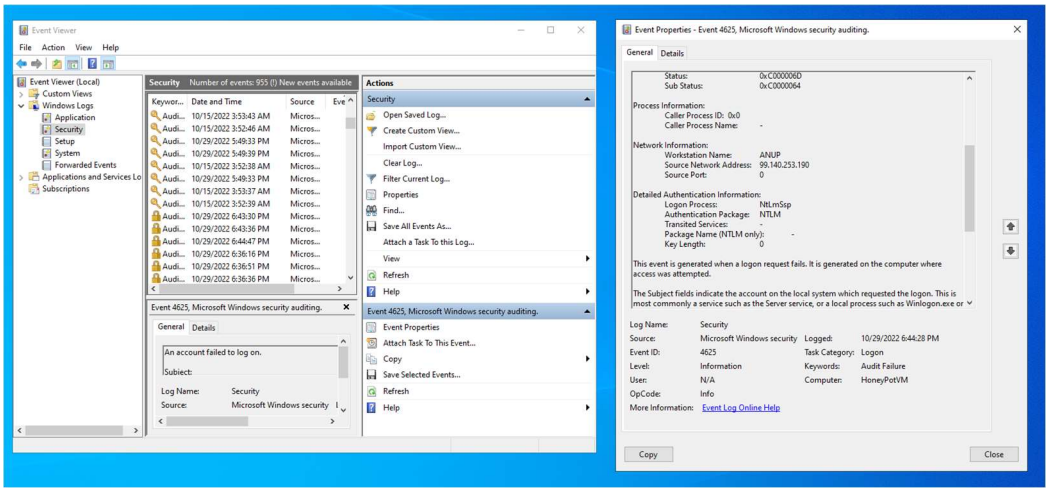
This is how the virtual machine looks like after Remote Desktop Connection



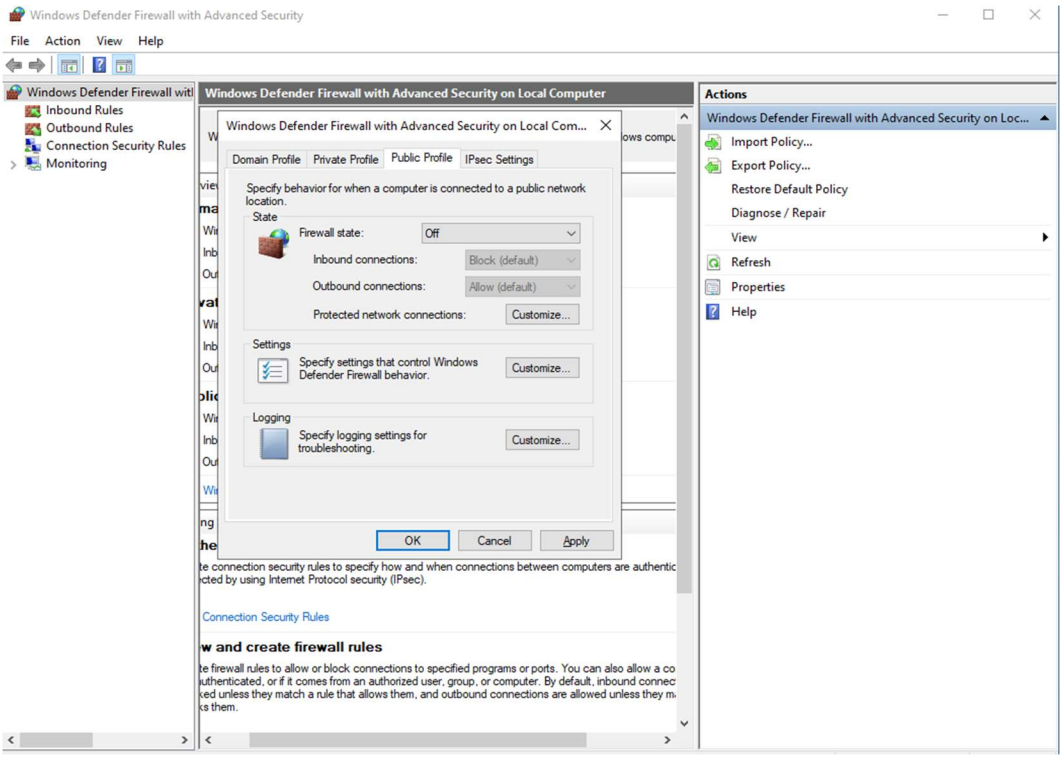
Go to Event Viewer > Windows Logs > Security. It takes some time for event logs to be visible. I am going to focus on Event ID 4625 which is Audit failure



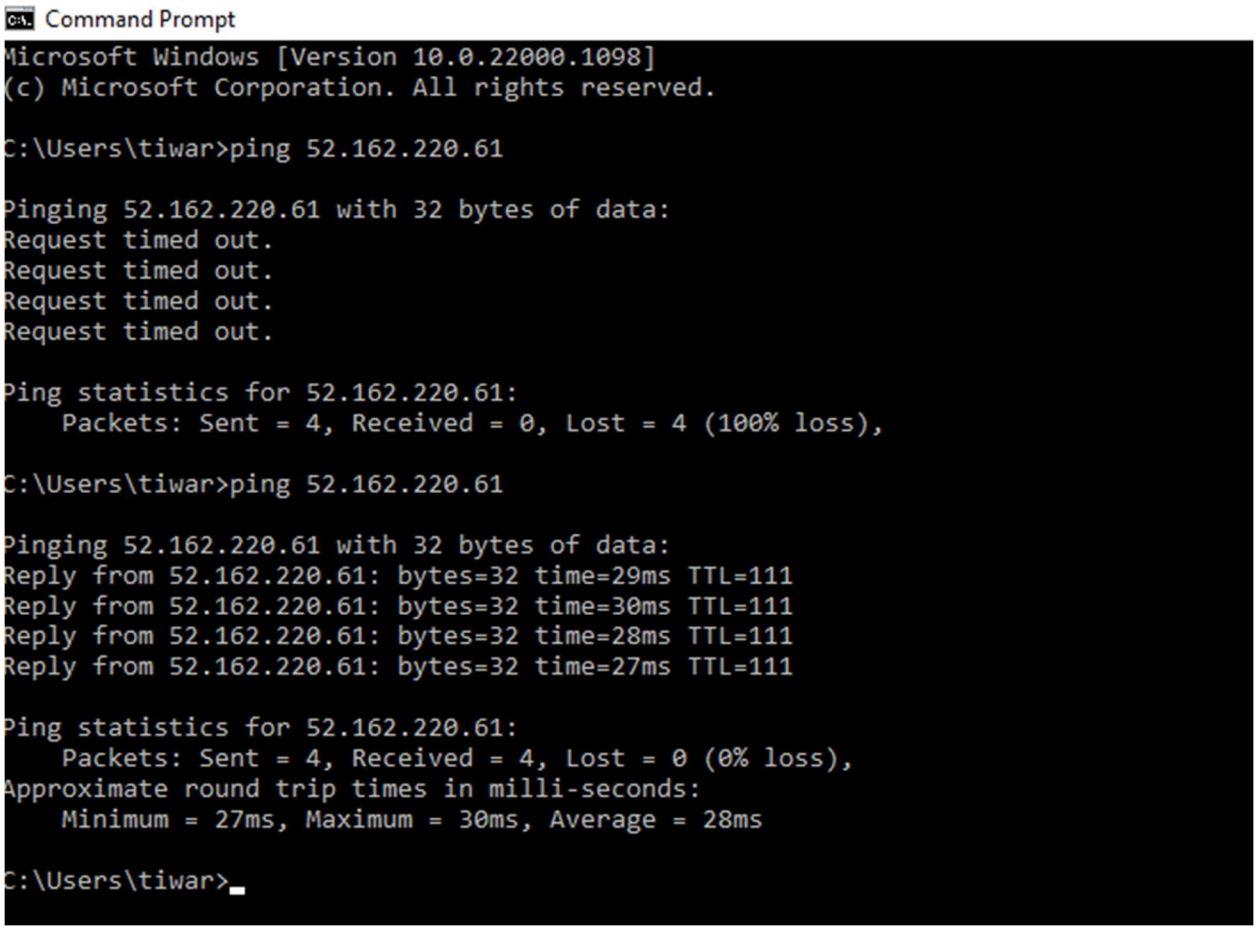
If we click on one event id, it will show details about that failed login including Ip address



Open Windows Defender Firewall in VM and change the firewall state to off for all Domain Profile, Private Profile and Public Profile.



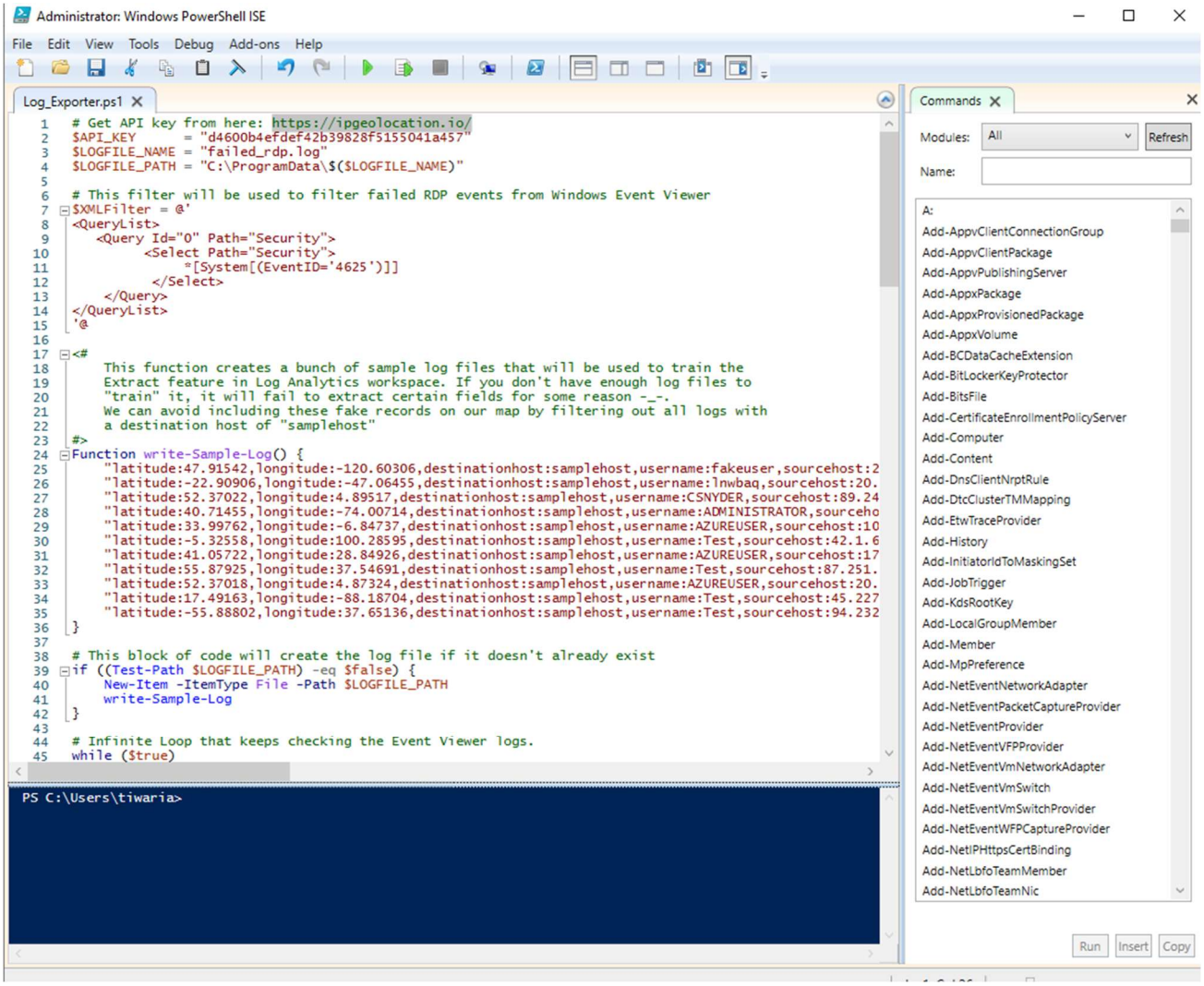
Ping the Ip address of virtual machine. It will start receiving ICMP packets after turning off the firewall



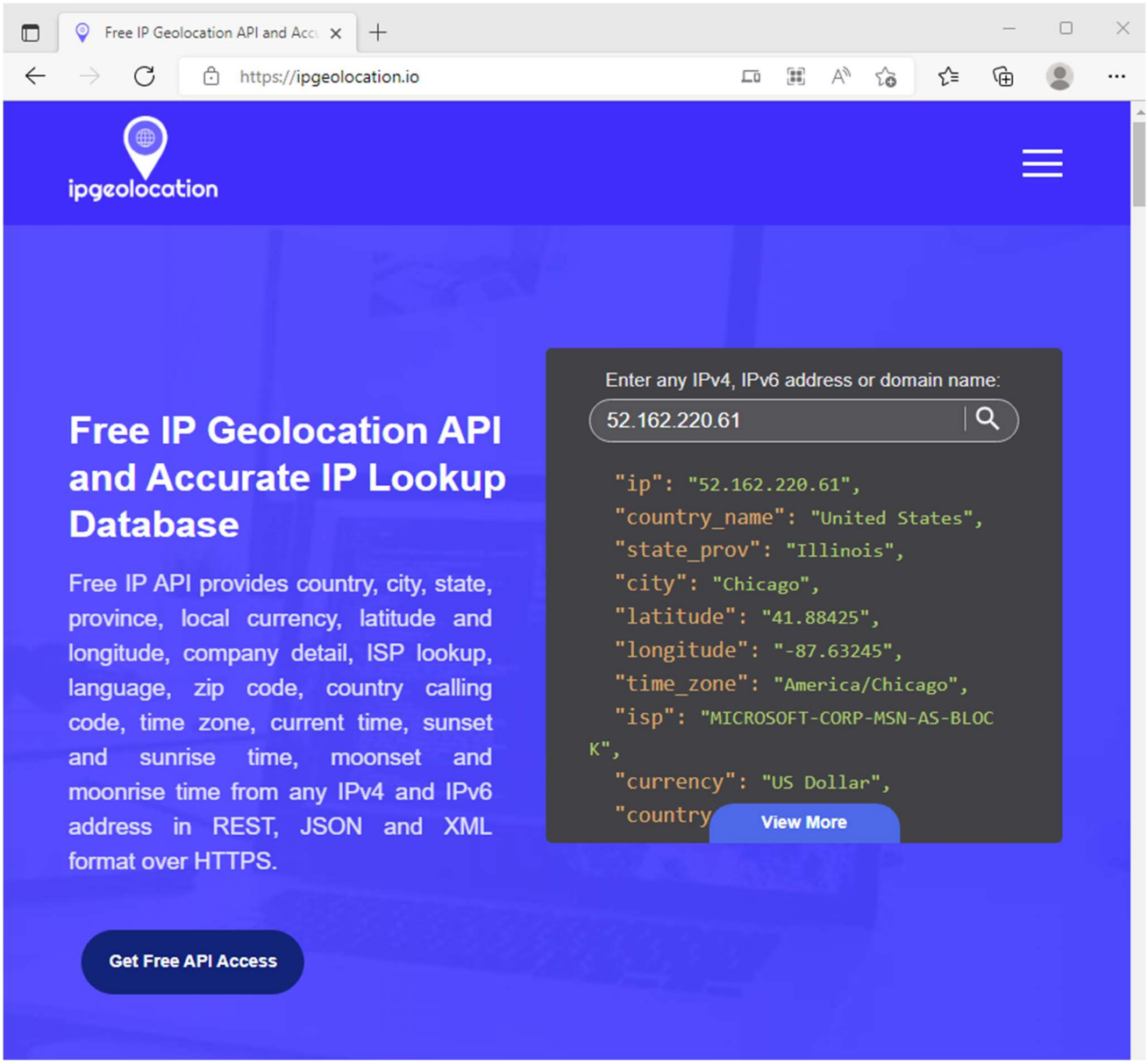
Run the Following PowerShell Script in Virtual machine which exports logs from Virtual machine to Log Analytics

https://github.com/axt3023/Powerrshell-Script-to-extract-geolocation--from-event-viewer

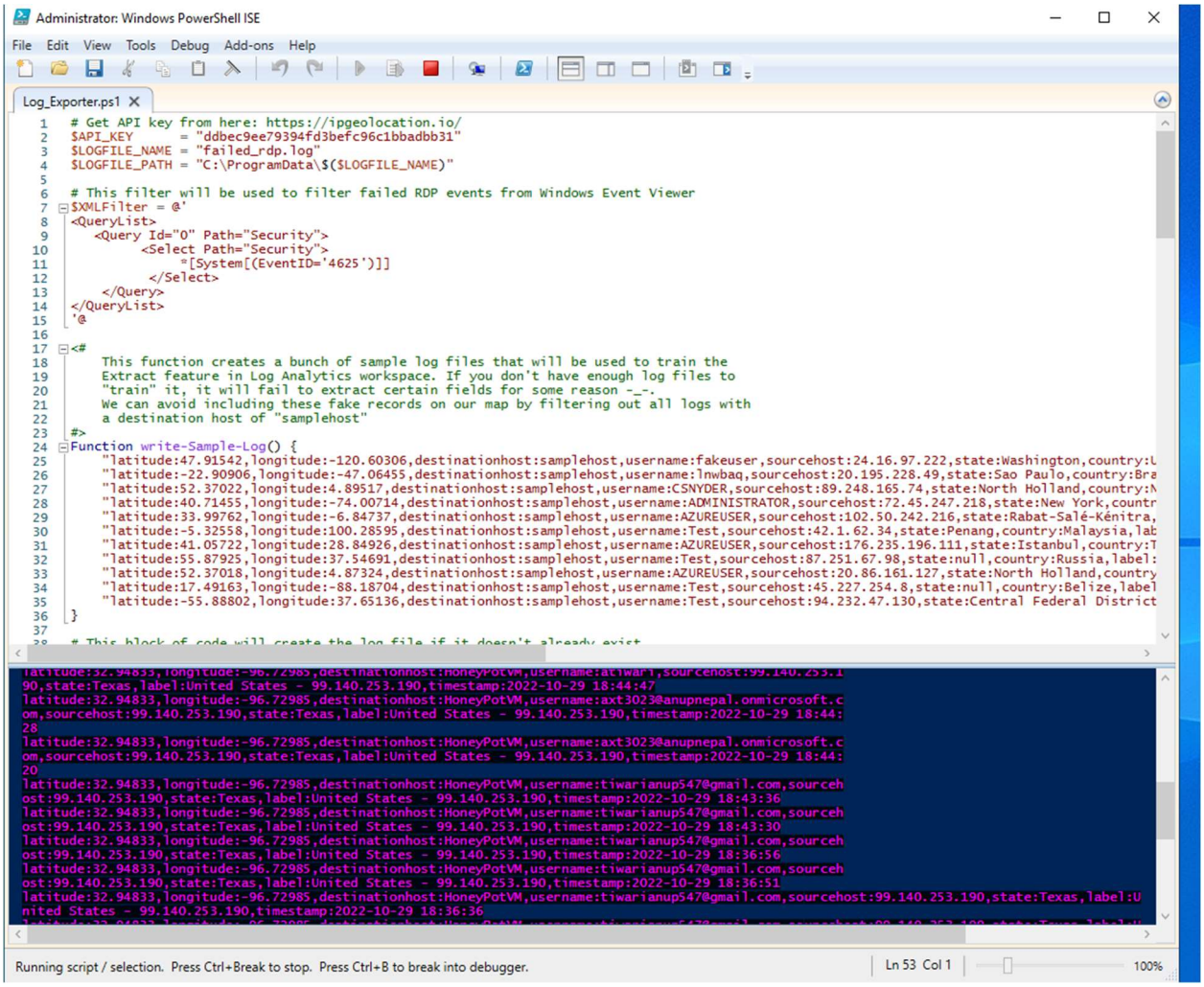
Copy the PowerShell scripts in the virtual machine and save it in the VM desktop



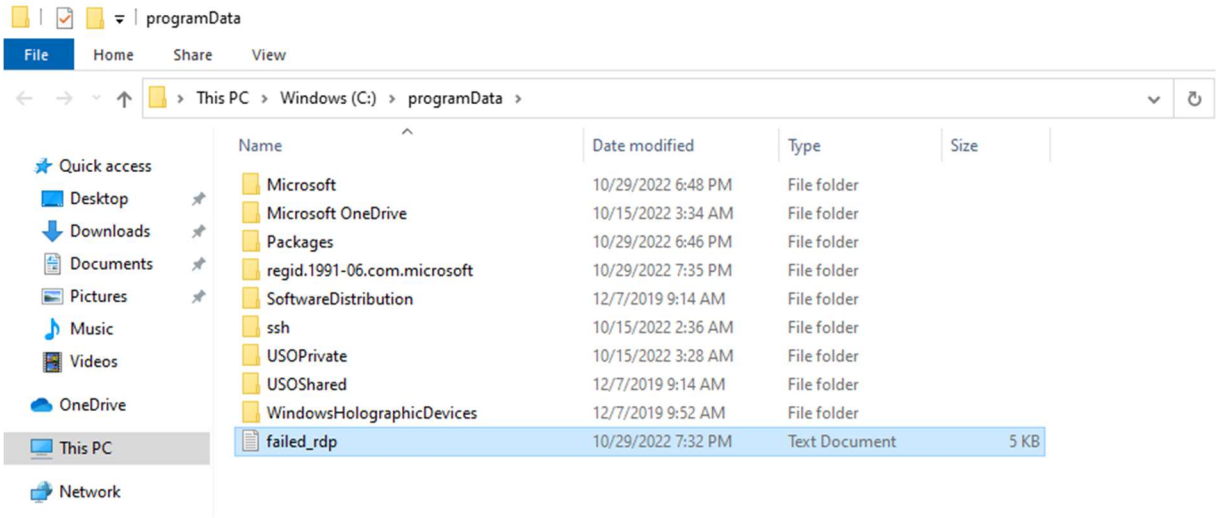
Get the own API_Key from ipgeolocation.io and update in the PowerShell script



Run the PowerShell script which will save the logs of failed data in the mentioned location in the scripts. The purple lines come as output every time there is failed login attempt

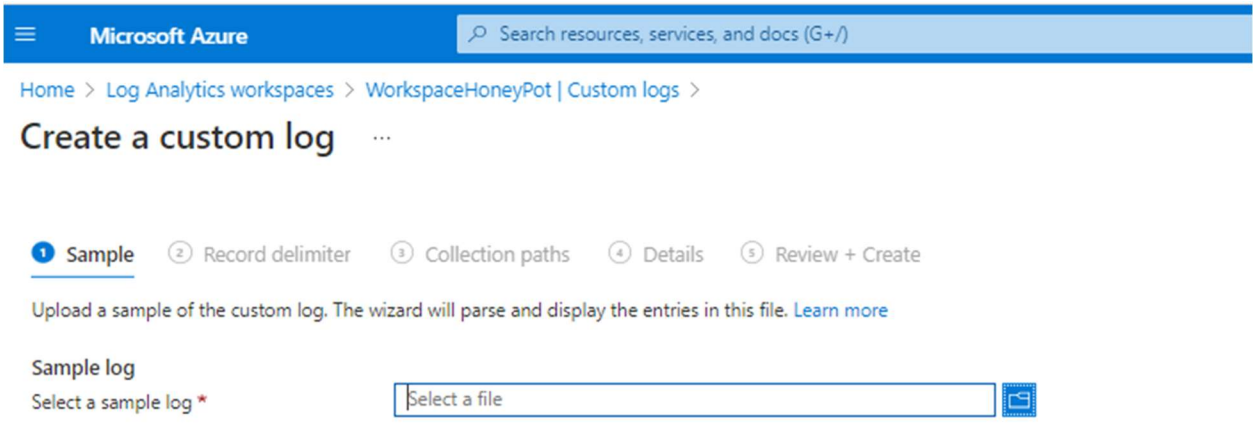


There is a failed_rdp text documents in the programData location which is usually hidden. It should be accessed manually



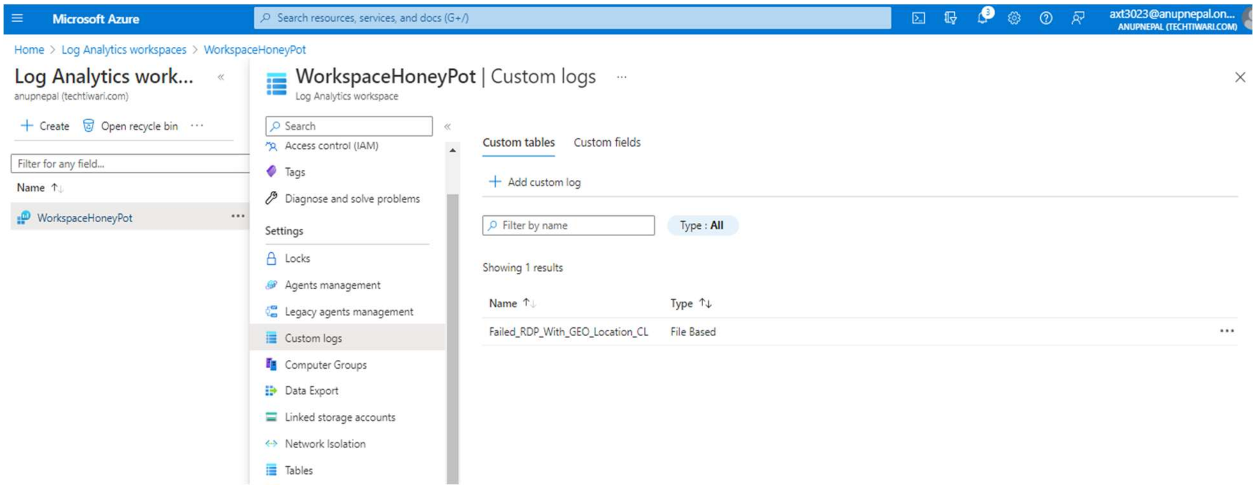
Copy the data of failed_rdp and paste it into the device save it as failed_rdp.log file

Which is used in creating a custom log in log Analytics in Azure



Specify the location C:\ProgramData\failed_Rdp.log so that it collects the log from t

Virtual machine

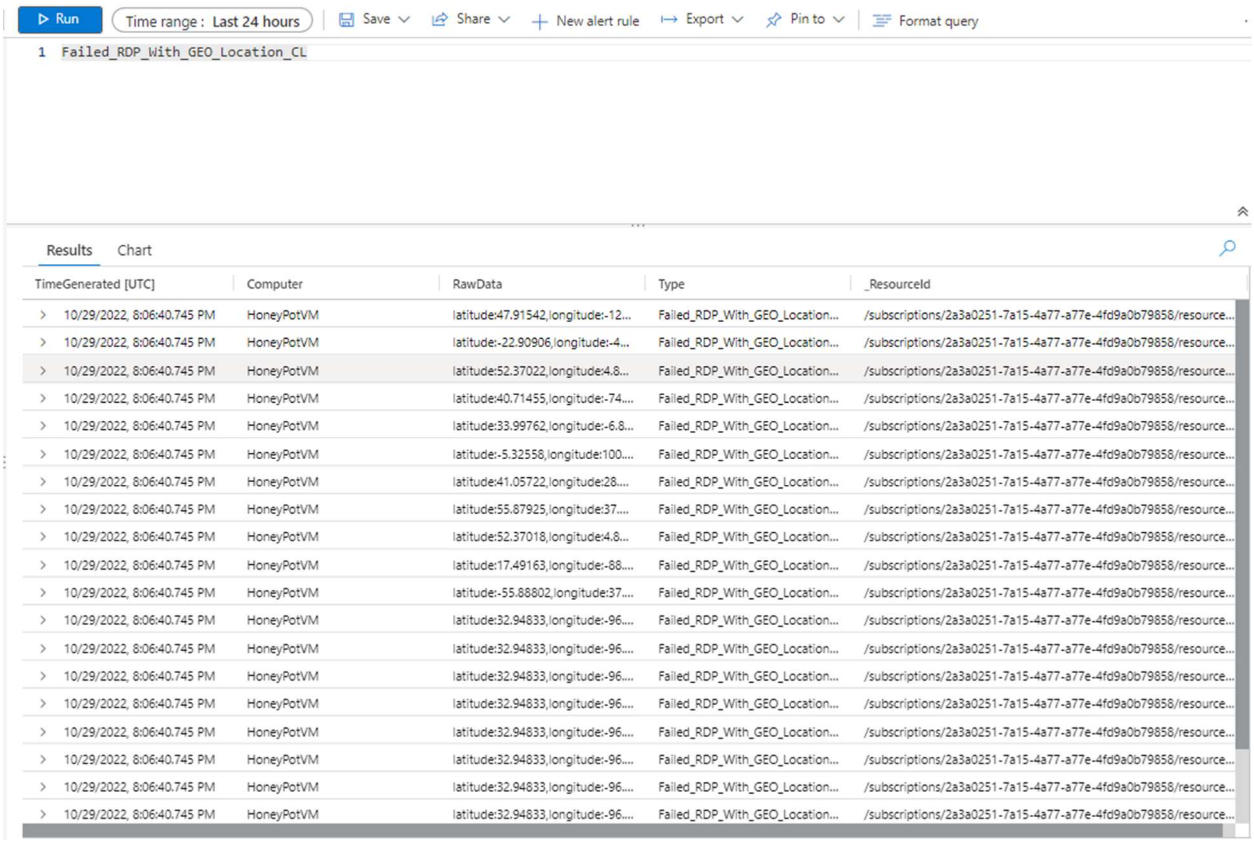


One failed login attempt from Thailand can be seen immediately in failed_rdp log file

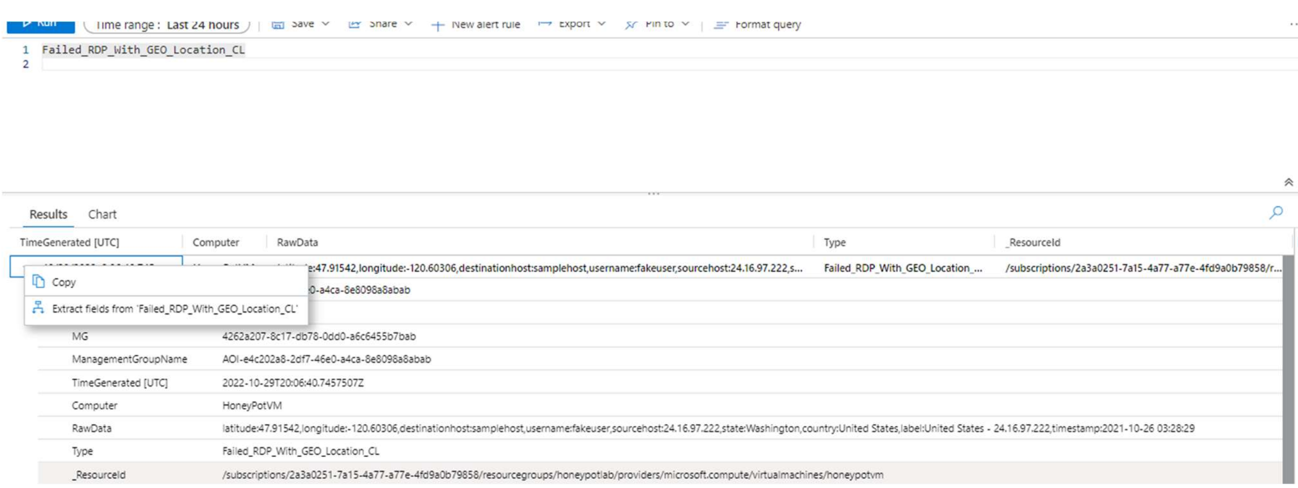
in VM

```
latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washington,country:United States,
latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country:Brazil,label:Bra
latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:North Holland,country:Netherlands,la
latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.247.218,state:New York,country:United Stat
latitude:33.99762,longitude:-6.84737,destinationhost:samplehost,username:AZUREUSER,sourcehost:102.50.242.216,state:Rabat-Salé-Kénitra,country:Moroc
latitude:-5.32558,longitude:100.28595,destinationhost:samplehost,username:Test,sourcehost:42.1.62.34,state:Penang,country:Malaysia,label:Malaysia -
latitude:41.05722,longitude:28.84926,destinationhost:samplehost,username:AZUREUSER,sourcehost:176.235.196.111,state:Istanbul,country:Turkey,label:T
latitude:55.87925,longitude:37.54691,destinationhost:samplehost,username:Test,sourcehost:87.251.67.98,state:null,country:Russia,label:Russia - 87.2
latitude:52.37018,longitude:4.87324,destinationhost:samplehost,username:AZUREUSER,sourcehost:20.86.161.127,state:North Holland,country:Netherlands,
latitude:17.49163,longitude:-88.18704,destinationhost:samplehost,username:Test,sourcehost:45.227.254.8,state:null,country:Belize,label:Belize - 45.
latitude:-55.88802,longitude:37.65136,destinationhost:samplehost,username:Test,sourcehost:94.232.47.130,state:Central Federal District,country:Russ
latitude:32.94833,longitude:-96.72985,destinationhost:HoneyPotVM,username:atiwari,sourcehost:99.140.253.190,state:Texas, country:United States,labe
latitude:32.94833,longitude:-96.72985,destinationhost:HoneyPotVM,username:axt3023@anupnepal.onmicrosoft.com,sourcehost:99.140.253.190,state:Texas,
latitude:32.94833,longitude:-96.72985,destinationhost:HoneyPotVM,username:axt3023@anupnepal.onmicrosoft.com,sourcehost:99.140.253.190,state:Texas,
latitude:32.94833,longitude:-96.72985,destinationhost:HoneyPotVM,username:tiwarianup547@gmail.com,sourcehost:99.140.253.190,state:Texas, country:Un
latitude:32.94833,longitude:-96.72985,destinationhost:HoneyPotVM,username:tiwarianup547@gmail.com,sourcehost:99.140.253.190,state:Texas, country:Un
latitude:32.94833,longitude:-96.72985,destinationhost:HoneyPotVM,username:tiwarianup547@gmail.com,sourcehost:99.140.253.190,state:Texas, country:Un
latitude:32.94833,longitude:-96.72985,destinationhost:HoneyPotVM,username:tiwarianup547@gmail.com,sourcehost:99.140.253.190,state:Texas, country:Un
latitude:32.94833,longitude:-96.72985,destinationhost:HoneyPotVM,username:tiwarianup547@gmail.com,sourcehost:99.140.253.190,state:Texas, country:Un
latitude:32.94833,longitude:-96.72985,destinationhost:HoneyPotVM,username:tiwarianup547@gmail.com,sourcehost:99.140.253.190,state:Texas, country:Un
latitude:32.94833,longitude:-96.72985,destinationhost:HoneyPotVM,username:tiwarianup547@gmail.com,sourcehost:99.140.253.190,state:Texas, country:Un
latitude:13.78445,longitude:100.57659,destinationhost:HoneyPotVM,username:azureuser,sourcehost:210.1.57.98,state:null, country:Thailand,label:Thail
```

All failed login attempt Logs can be seen in workspace too now

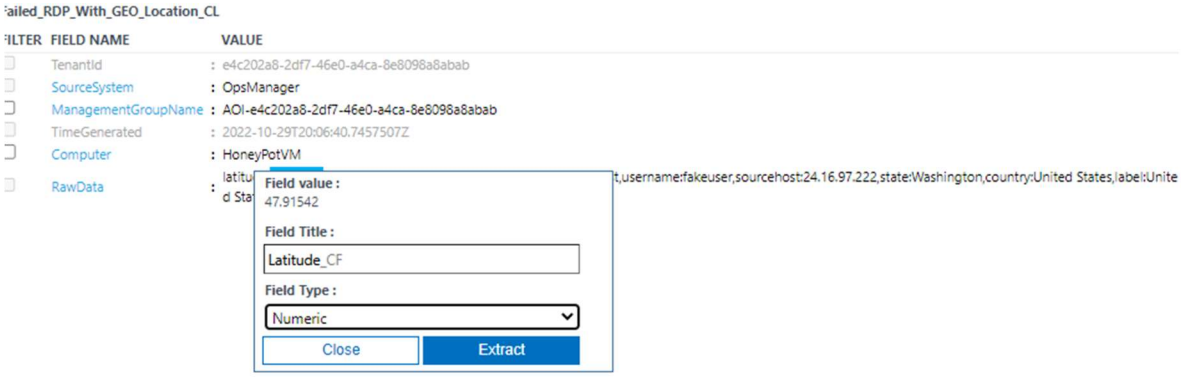


Click on one of the results and extract raw data to customize it

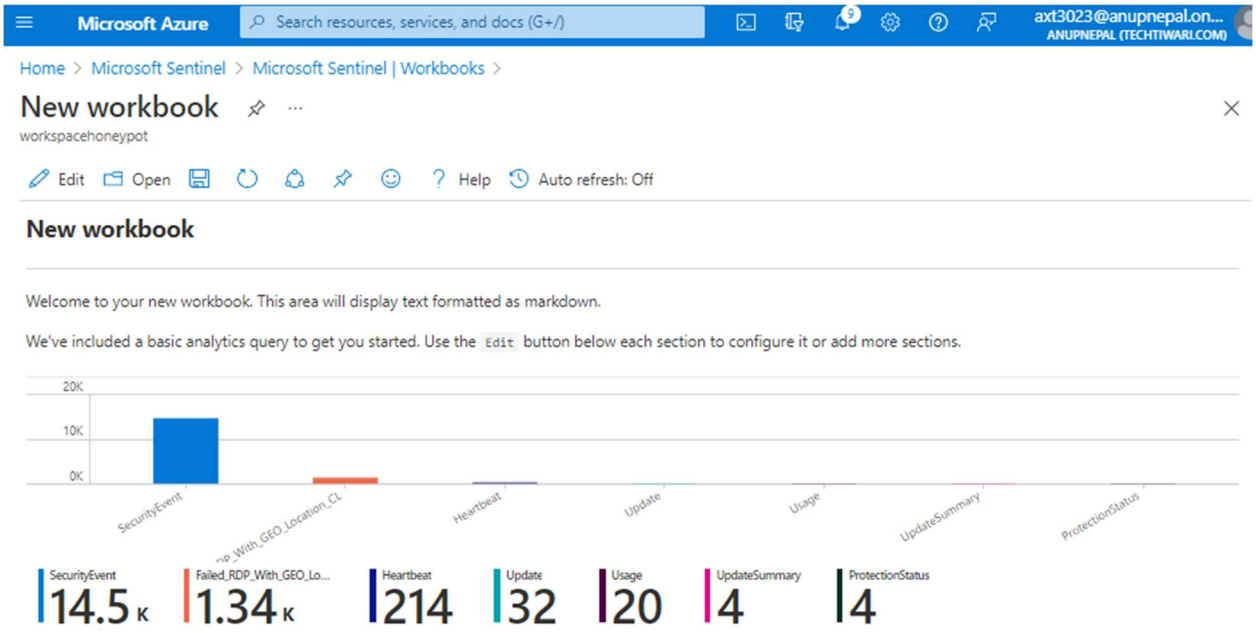


Extract Latitude, Longitude, and other Parameters and name them properly. This is how we train the

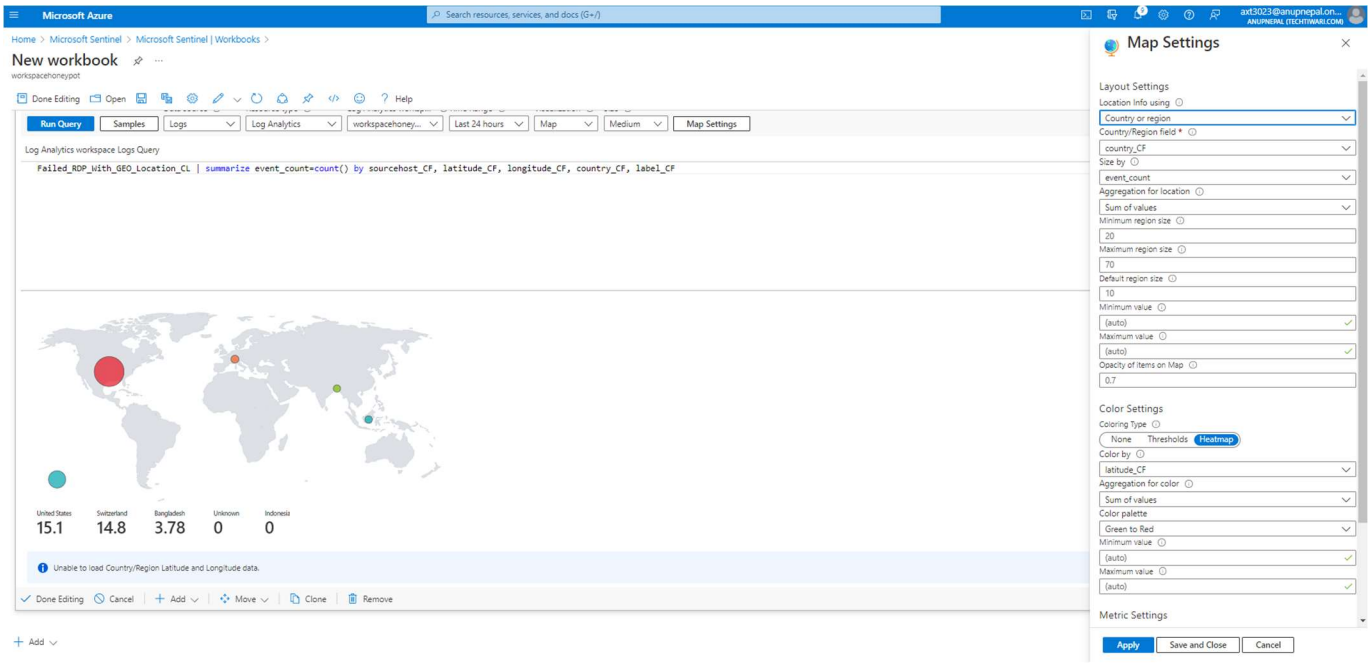
extraction to be accurate.



Set up Map in Azure Sentinel by adding new workbook



Add new query and use map as a visualization option



After the setup is complete, the attacks can be seen in the world map.