Creating a SIEM with Azure VM + Sentinel

horizontal line

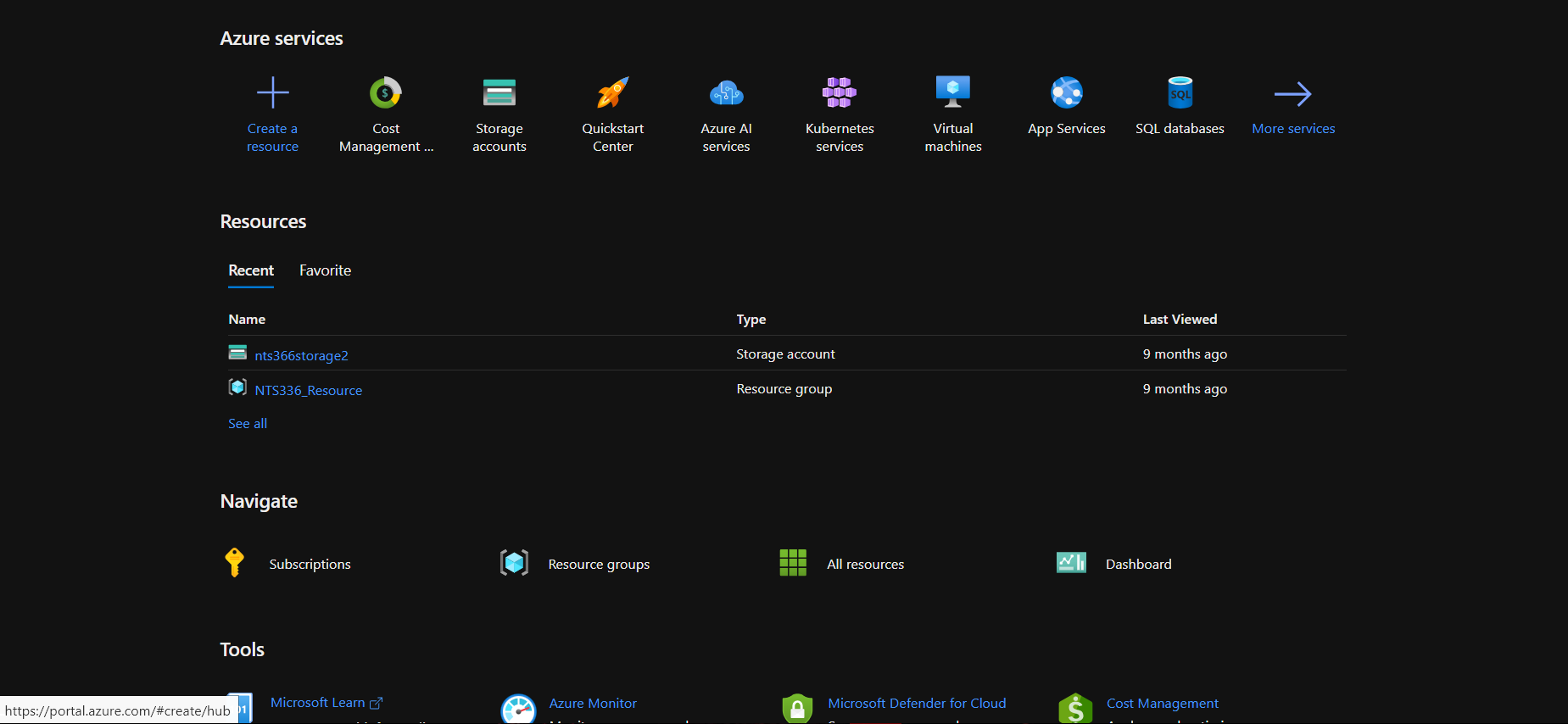
# 

# Introduction

A SIEM (Security Information and Event Management) is a security overview that collects and sorts data from various sources within the organization that it is used in. This can also be used for personal use, but is more widely used within SOC Analyst positions. A SIEM is usually a dashboard that issues alerts, and detects incidents in real-time.

## 

## Create Virtual Machine



After logging in, or creating your free trial azure account from [https://azure.microsoft.com/en-us/free](https://azure.microsoft.com/en-us/free/) click ‘Create a resource’ from the top left. Under ‘Popular Azure services’ click on ‘Create’ under ‘Virtual machine’

First Page Basics: Subscription: Azure Subscription 1 . (For this lab, I will be using Azure for Students)

Resource Group\*: SIEM.

Instance Details:VM

Name: HoneypotLab

Region: US West 3

Availability options: No Infrastructure Redundancy Required

Security Type: Standard

Image\*: Windows 10 Pro, Version 22 H2 Gen 1

Size: Standard D2s\_v3–2 vcpus 8GiB memory ($70.08/month)

Create your own administrator username and password, make sure to remember it

Leave inbound port rules as default (Allow selected ports, RDP 3389)

Check the box for licensing

Click Next : Disks >

Do nothing, Click Next : Networking >

### Networking Page

Under ‘NIC Security Group’, change from Basic to Advanced

‘Configure network security group’ click ‘Create New’

Click ‘Add an inbound rule’

Leave everything default except the following:

Destination port ranges → \*

Priority → 100

Name → I will be naming this “DANGER\_ANY\_IN’

Click Add, doing this will allow all traffic coming in from the internet.

Click ‘OK’

Click ‘Review + Create’

Click ‘Create’

### Log Analytics Workspace

In a new tab. Under ‘Popular Azure services’ search for ‘Log Analytics Workspace’ and click ‘Create’

Subscription: Azure Subscription 1

Resource Group\*: SIEM

Instance Details:

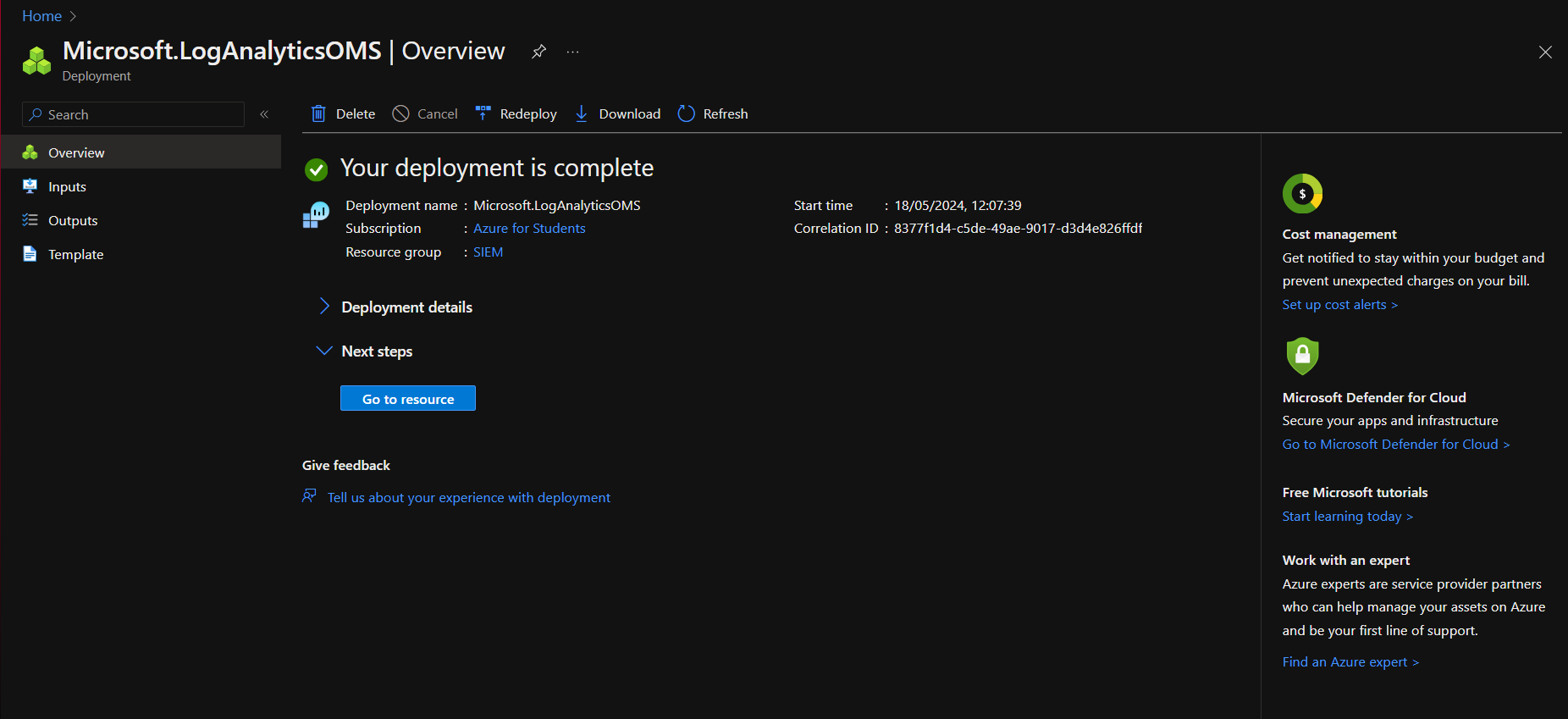
Name: law-honeypot-1

Region: US West 2

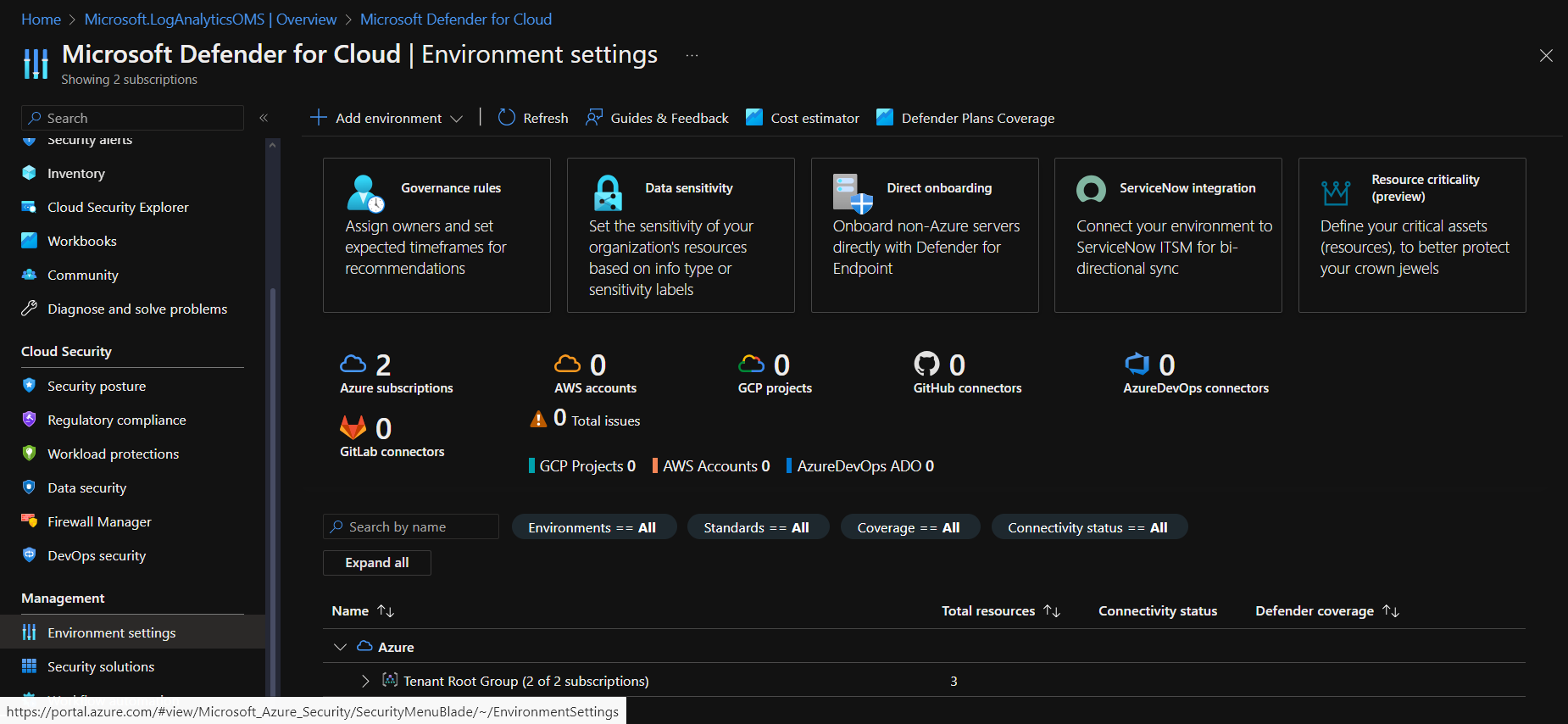
Click ‘Review + Create’

Click ‘Create’

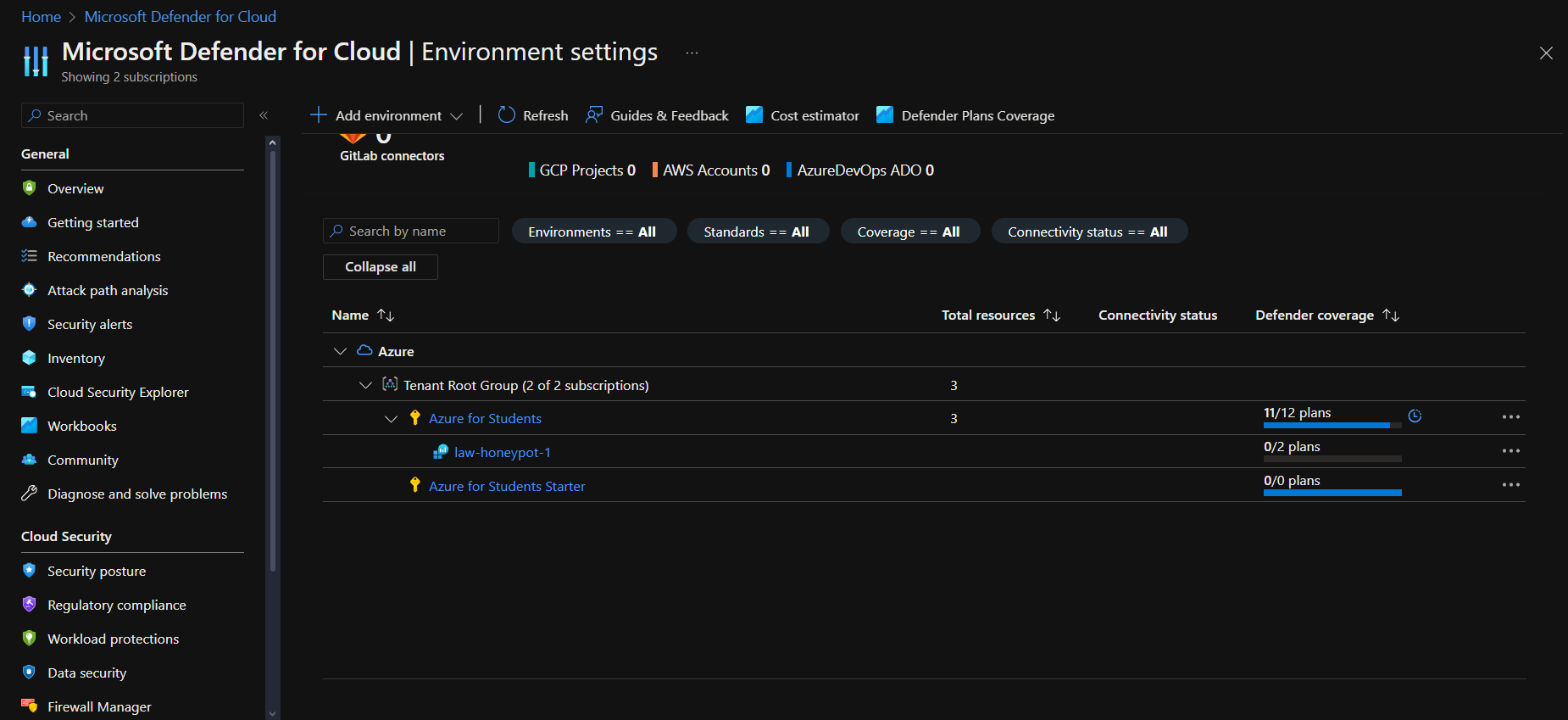
### Microsoft Defender for Cloud



Click on ‘Go to Microsoft Defender for Cloud >’ on the right side pane.



Now, on the left pane, scroll down to ‘Environment settings’



Click on ‘law-honeypot-1’

Turn ‘Foundational CSPM’ as well as ‘Servers’ to ‘On’

Click ‘Save’ at the top left. It may take a few minutes to save.

Click ‘Data collections’

Select ‘All Events’ and Save.

### Connect Log Analytics Workspace to VM

Go to your Azure homepage and click on your Log Analytics Workspace (law-honeypot-1)

In the left pane, find ‘Virtual machines (deprecated)’

Select ‘HoneypotLab’ and click ‘Connect’

### Connect Log Analytics Workspace to VM

Go to your homepage, and search for ‘Microsoft Sentinel’

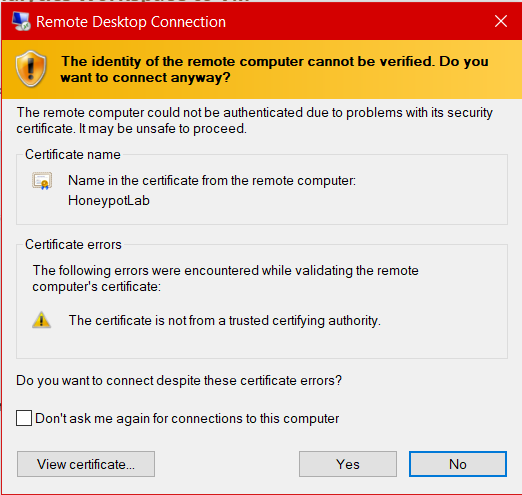
Click on ‘law-honeypot-1’ and Add

### Login to VM using Remote Desktop

Go to your homepage, and click on your Honeypot VM (HoneypotLab)

Copy your Public IP Address and put it into Remote Desktop

When asked for your credentials, enter in the credentials you created at the beginning.



If this pop-up comes up, select Yes.

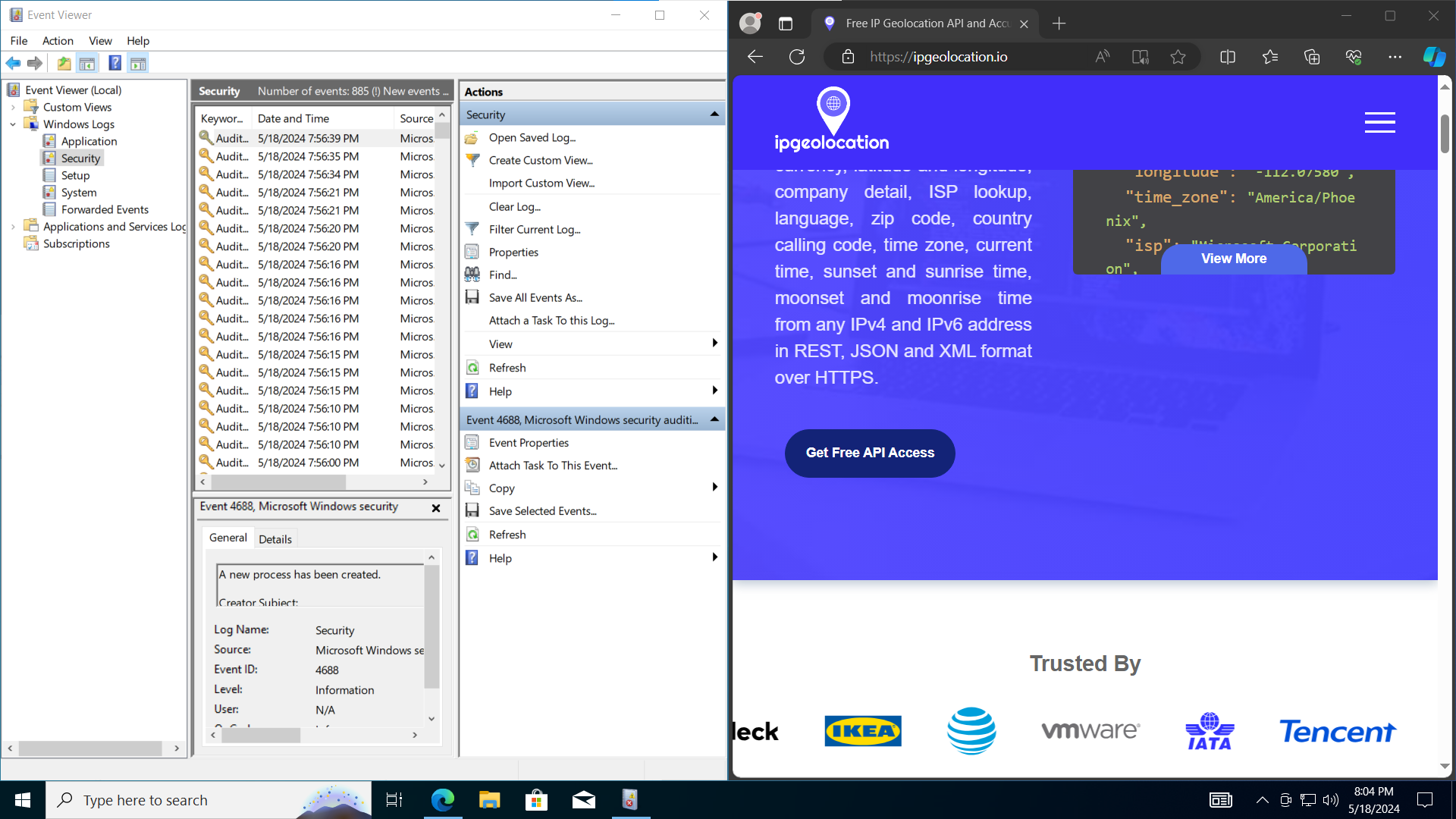


Select No on all options and click Accept.

Once inside your machine, open ‘Event Viewer’ and setup Microsoft Edge.

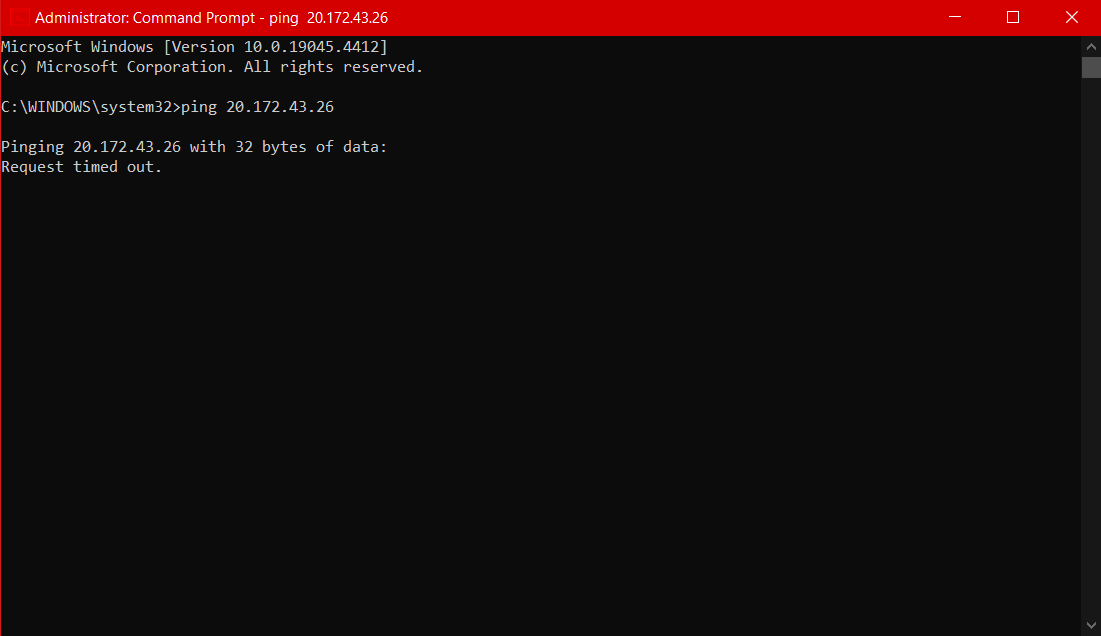
In Microsoft Edge, open up ipgeolocation.io, create an account, and get your API Key.

In Event Viewer, Open Windows Logs → Security



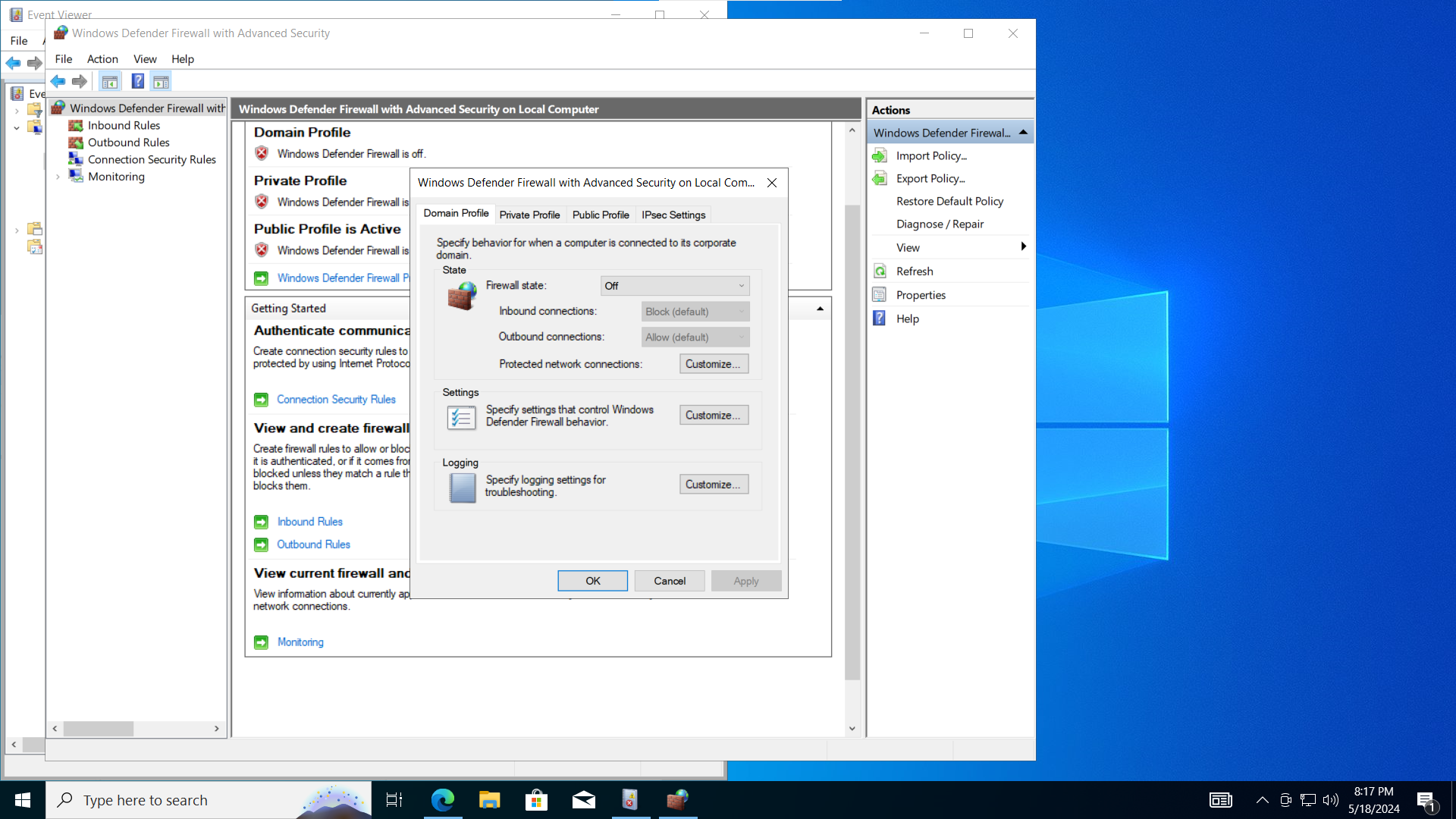
On your physical machine, ping your VM.

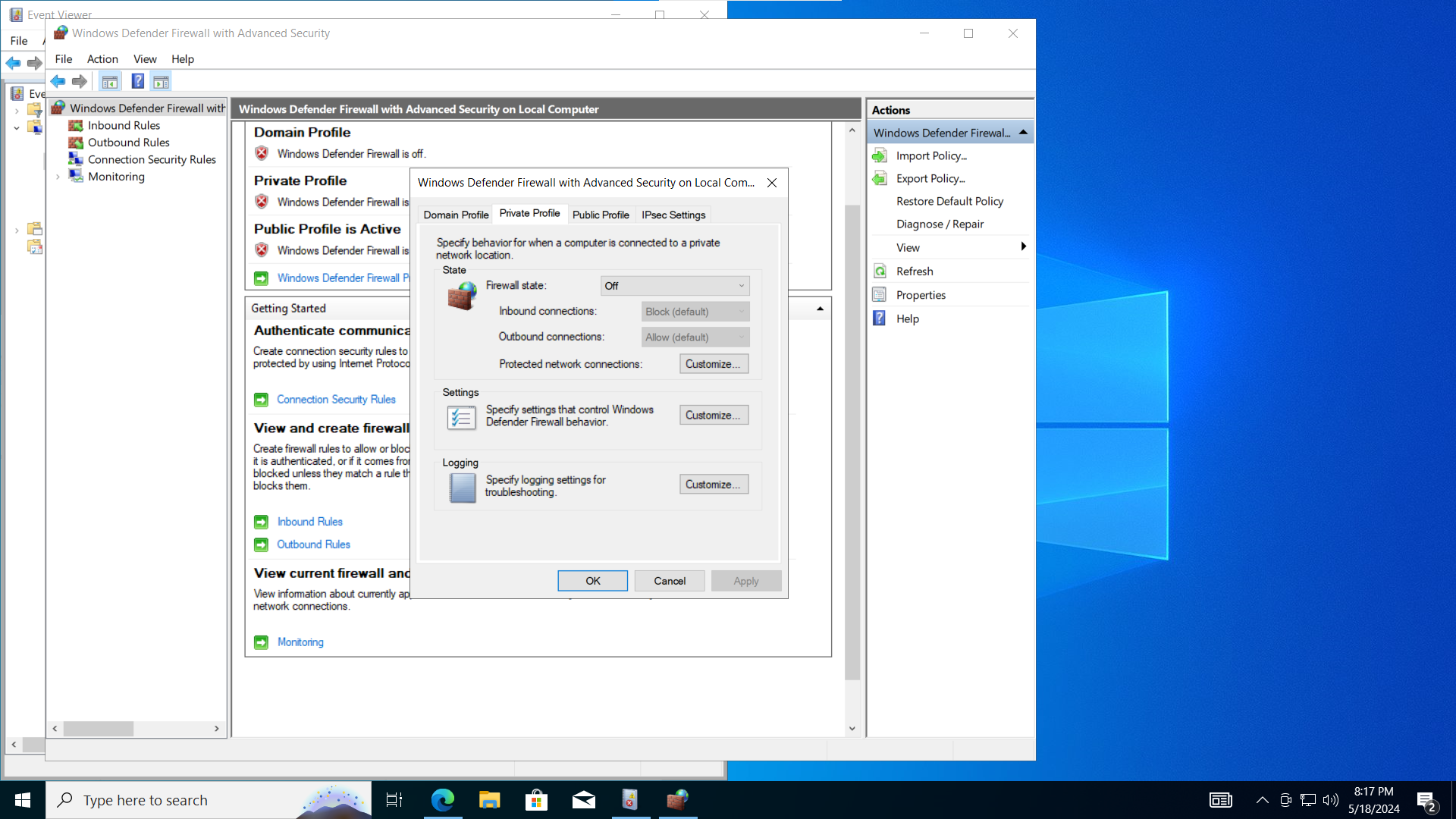
You will notice, this ping will fail.

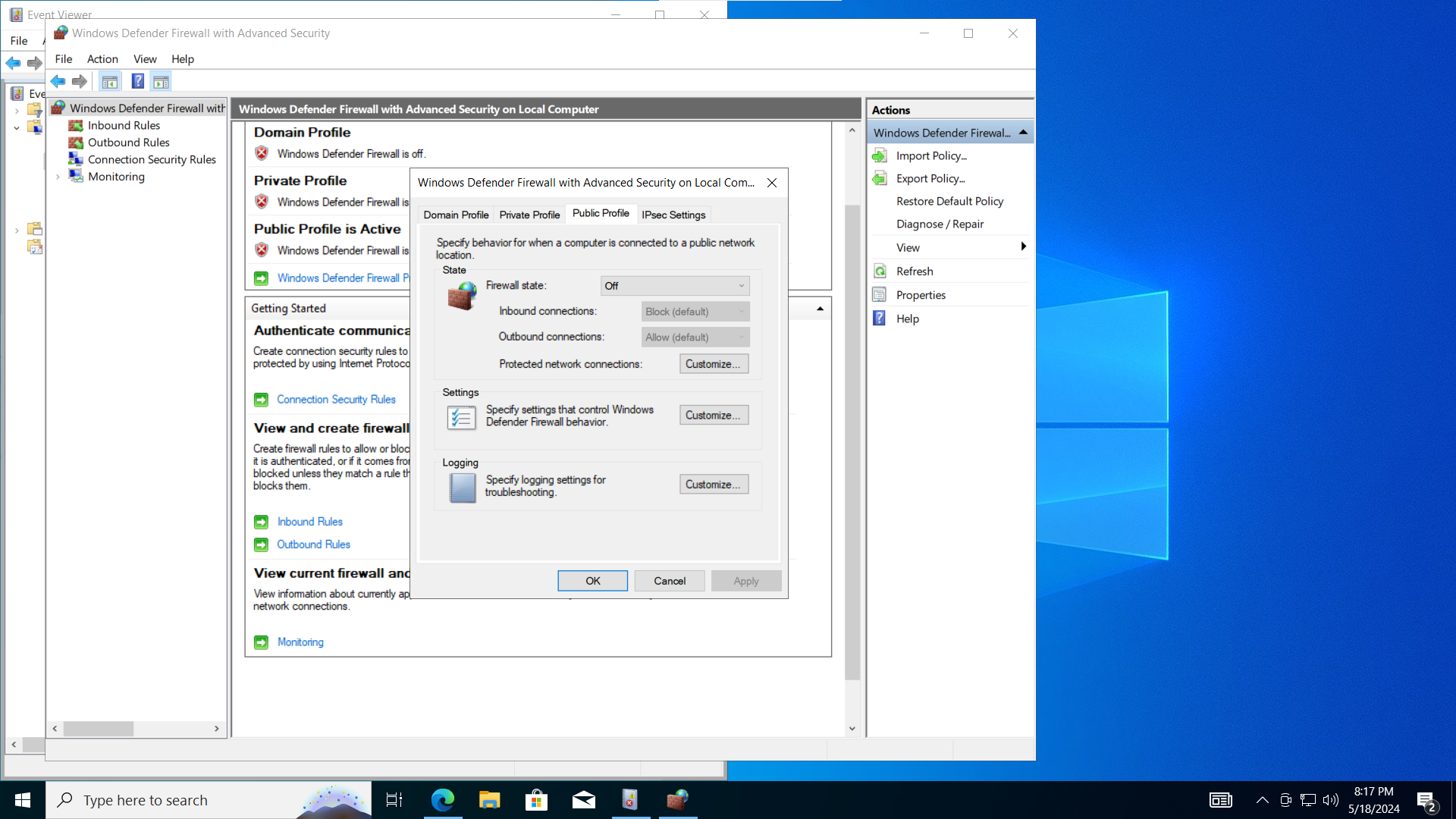


**On your VM**, Open windows defender firewall and click on ‘Windows Defender Firewall Properties.

Turn off Domain profile , Private profile , and Public profile.







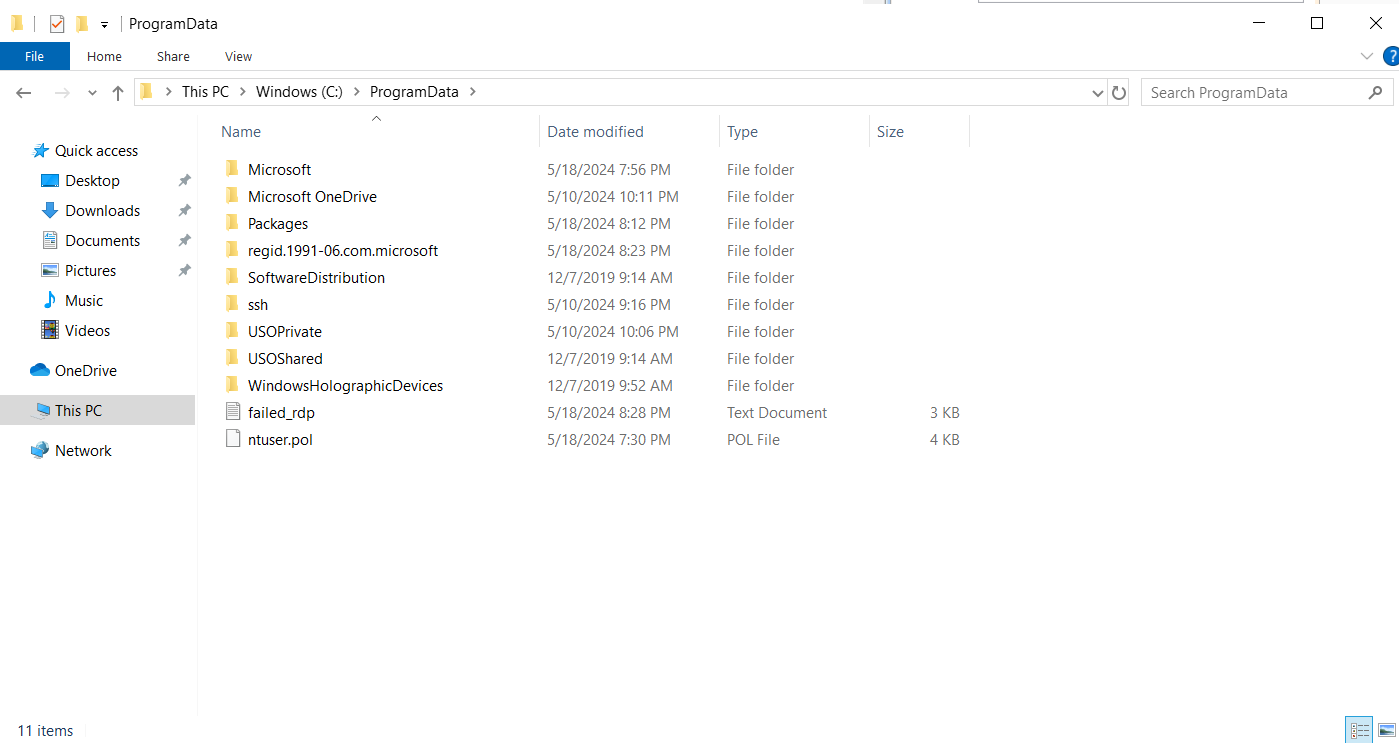
Copy the code from <https://github.com/Pozse/SIEM/blob/main/Security_Log_Expo.ps1>

Open Windows Powershell ISE, Click new, and paste the script.

Replace $API\_KEY = "d4600b4efdef42b39828f5155041a457" with your own API Key

Go to file → Save as → Log Exporter, and save it to desktop.

In powershell, type “run C:\ProgramData\failed\_rdp.log\”, go to file, and select run



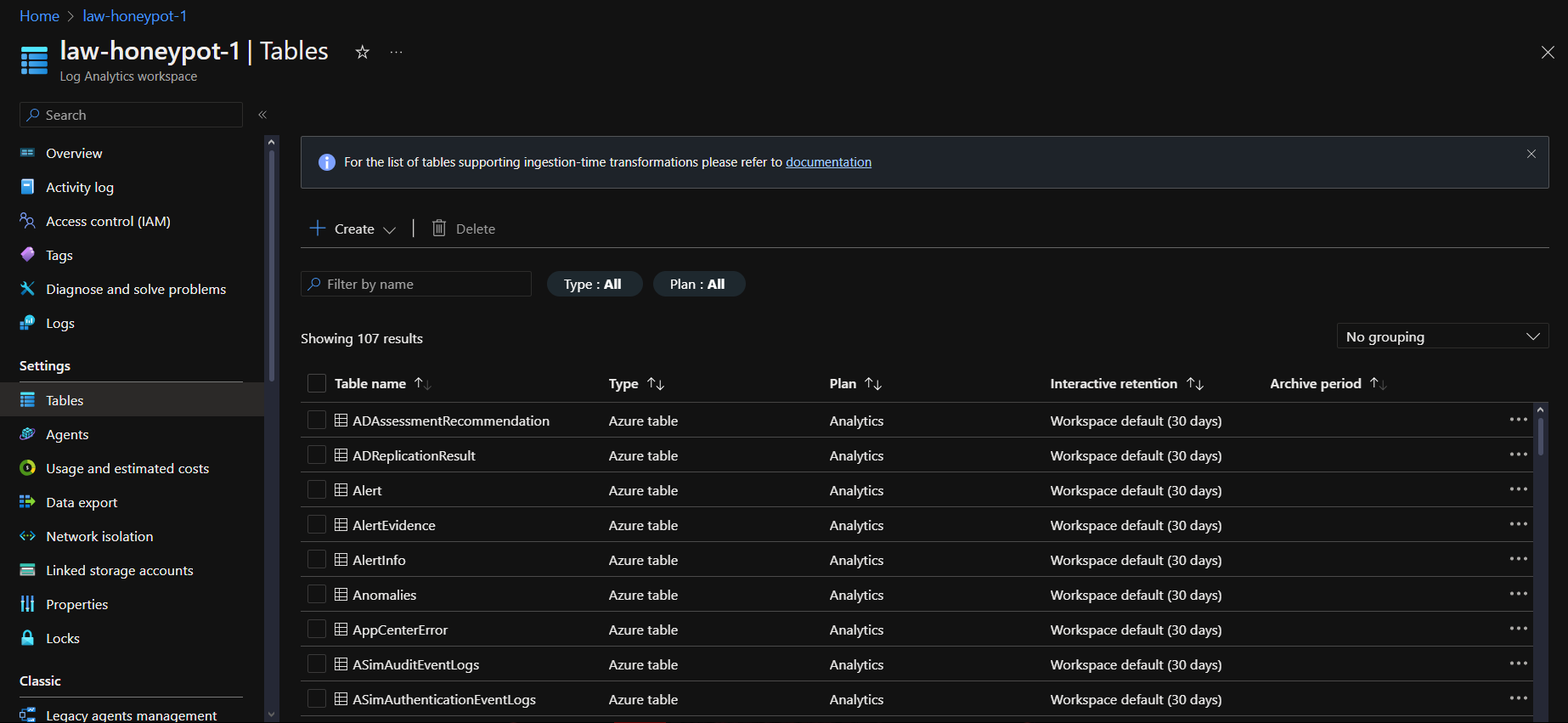
This will create a .txt file in C:\ProgramData\ called “failed\_rdp”.

Copy the text from this text file, open your physical machine, and create a notepad file on your desktop.

Paste the information you previously copied, and save it as failed\_rdp.log

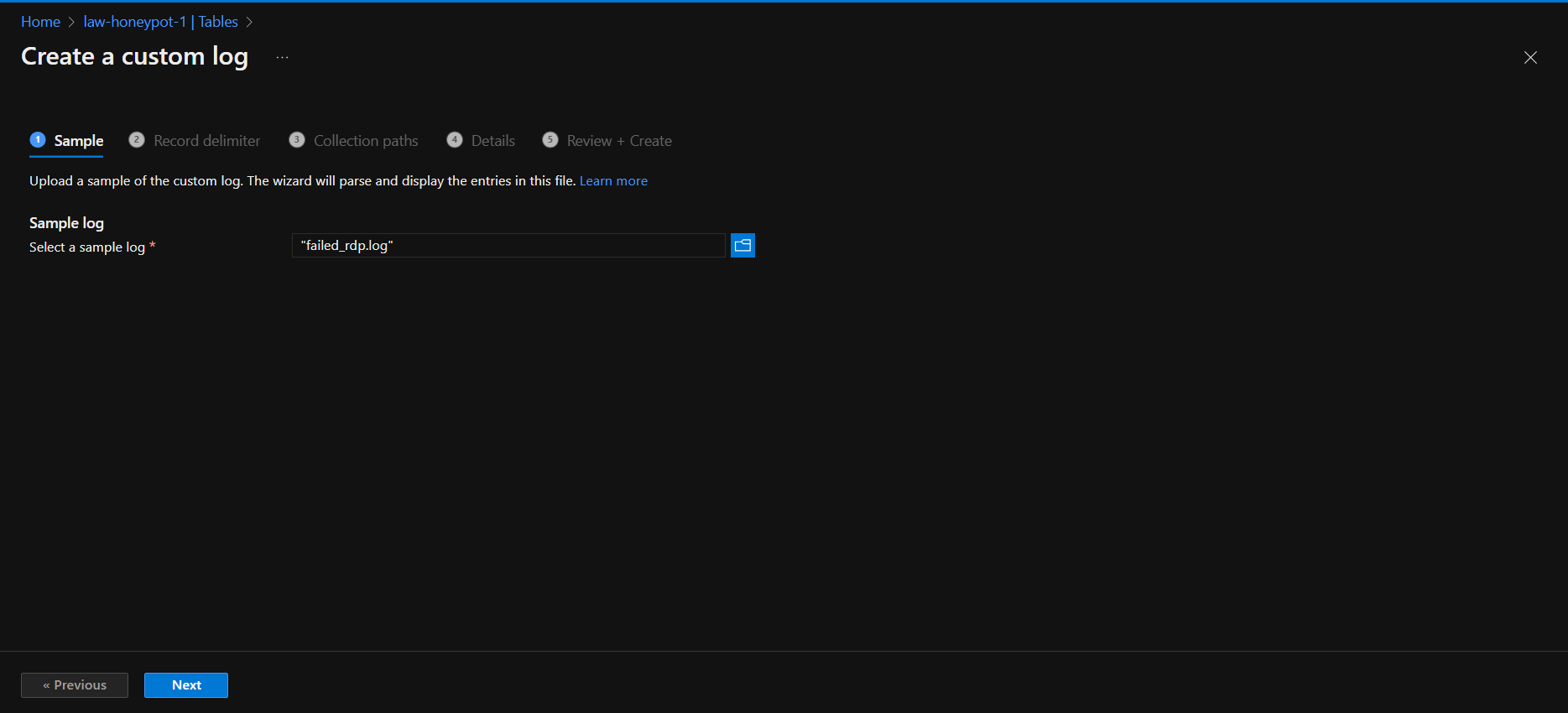
### Custom Log in Log Analytics Workspaces

In Azure, go into your law-honeypot-1 Log Analytics Workspace,



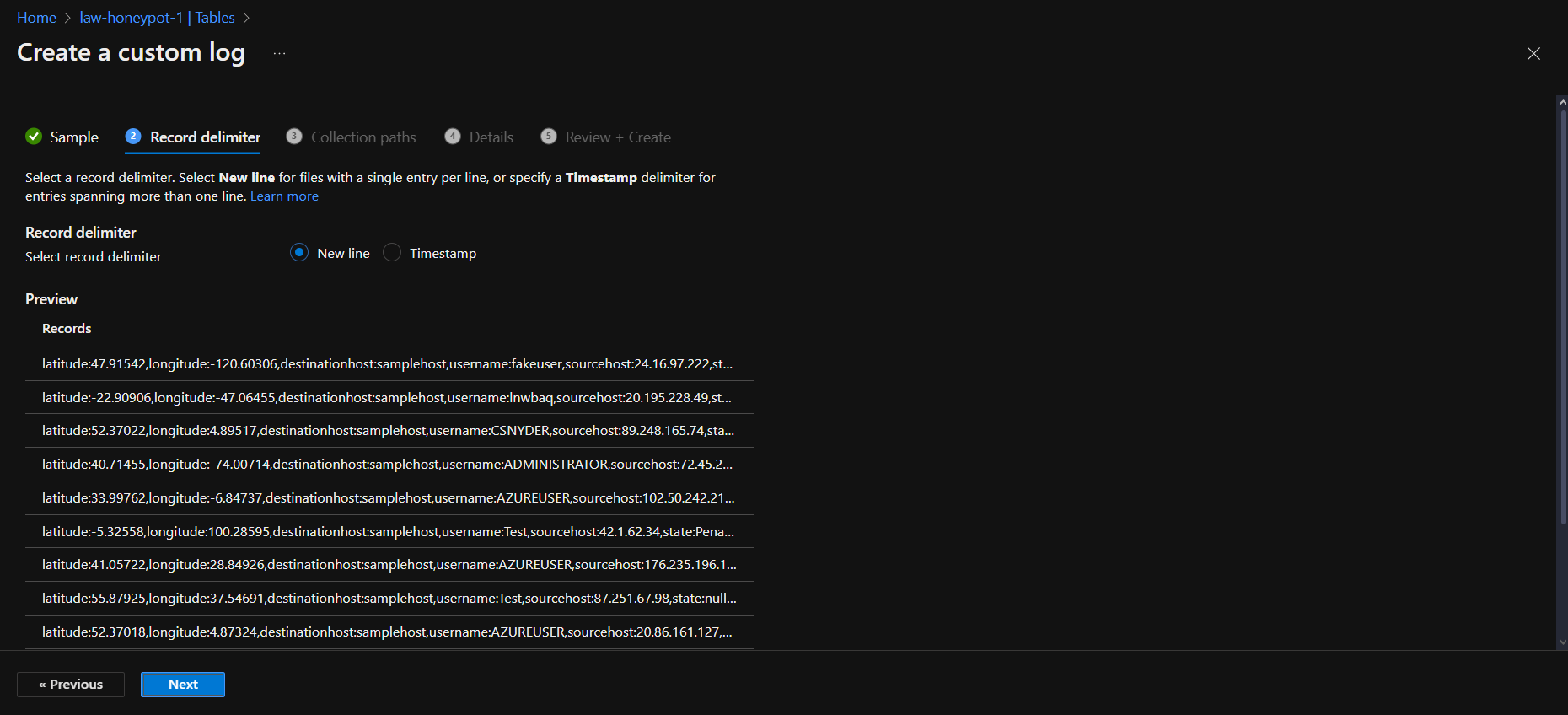
Once in Azure, click on ‘Tables’ on the left pane, and then click ‘Create’

Select ‘New Custom Log (MMA-based)’



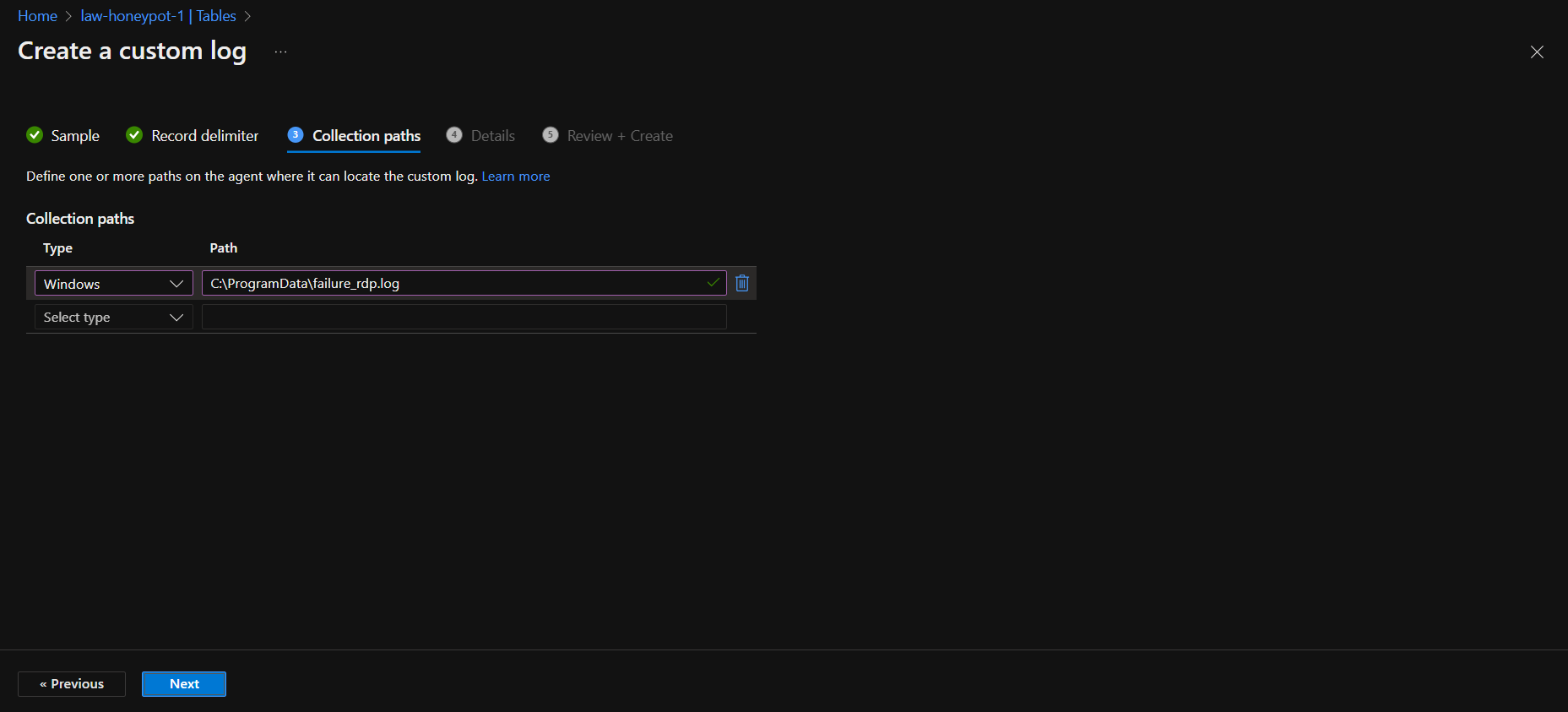
Select your failed\_rdp.log file from wherever you placed it.

Click Next



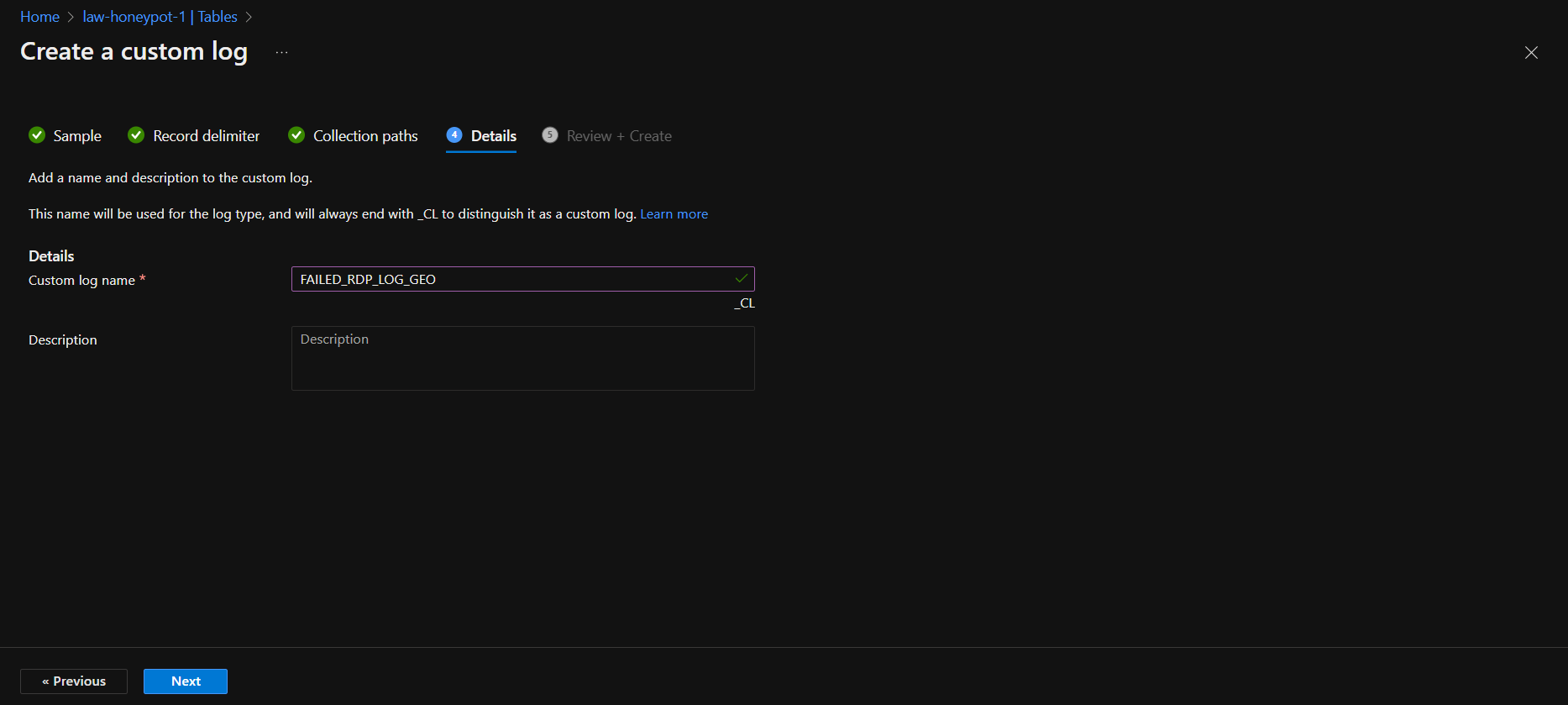
On Record Delimiter, make sure it is set as ‘New Line’

Click Next



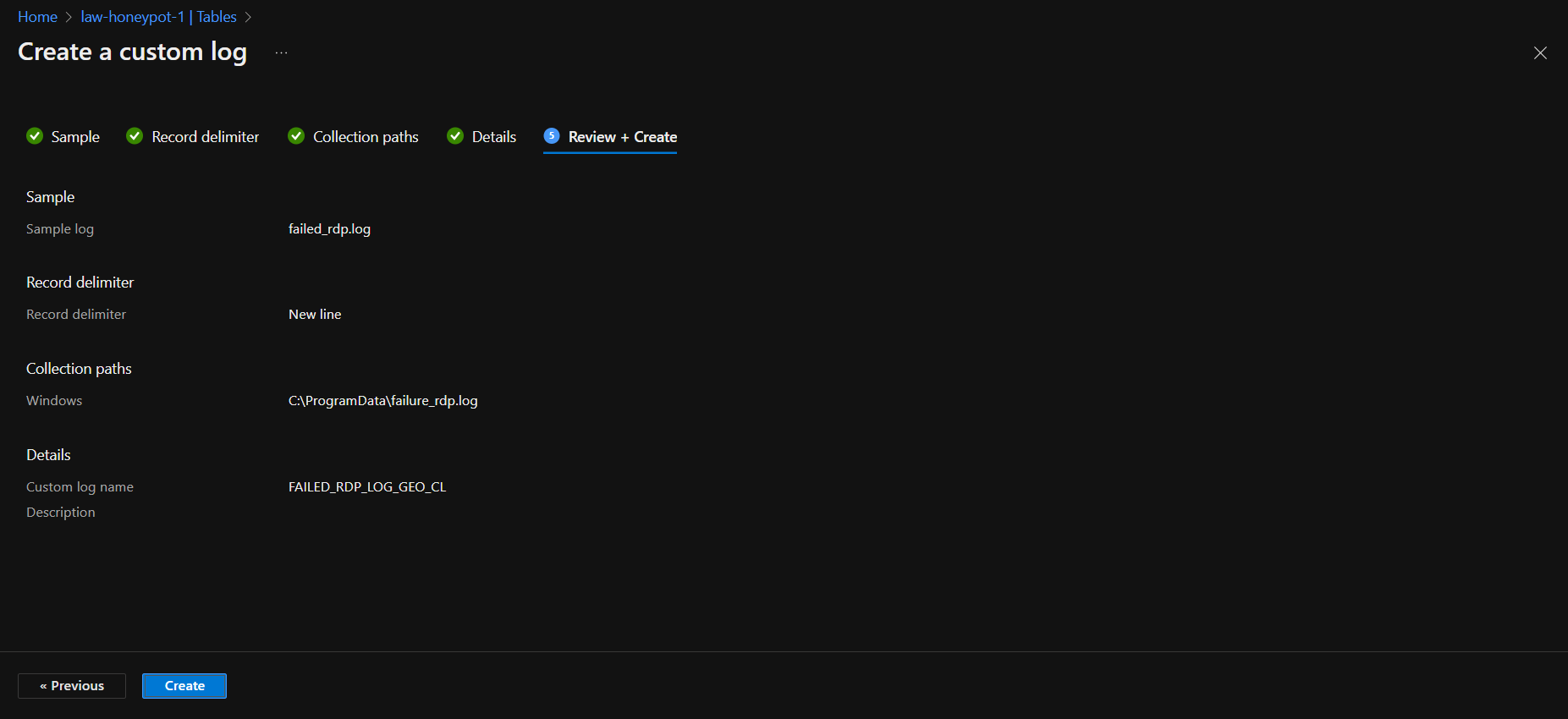
On the next screen, the collection path type will be Windows, and the path will be C:\ProgramData\failure\_rdp.log

Click Next

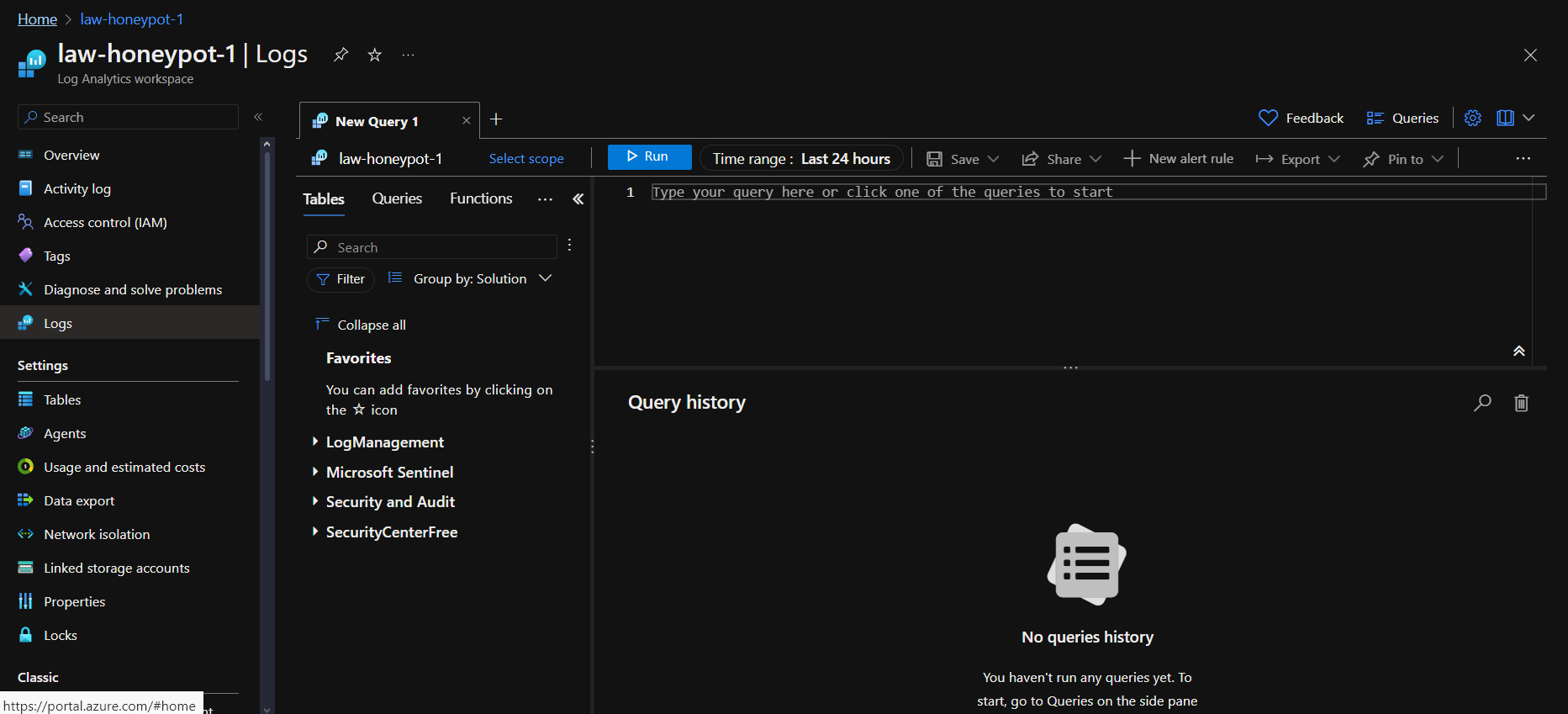


On Custom Log name, put FAILED\_RDP\_LOG\_GEO

Click Next



Click Create



On the left pane, click on logs and paste in The following

SecurityEvent | where EventID == 4625

I replaced the first line with the name from earlier FAILED\_RDP\_LOG\_GEO

