Microsoft Azure

Project Name :

Observing Live RDP Brute Force Attacks from Around the World with Azure Sentinel and a Custom PowerShell Script.

Team Members :

- Nishant Choutele
- Shrikant Meher

INDEX

Azure Sentinel is a cloud-native security information and event management (SIEM) solution that helps organizations detect, investigate, and respond to security threats. It provides a unified view of security data from across your organization, including your on-premises and cloud environments.

In this topic, we will set up Azure Sentinel and connect it to a live virtual machine acting as a honey pot. We will then use a custom PowerShell script to look up the attackers' geolocation information. This will allow us to observe live RDP brute force attacks from all around the world and track the location of the attackers.

This topic is relevant to security professionals who want to learn how to use Azure Sentinel to detect and investigate RDP brute force attacks. It is also relevant to anyone who is interested in learning more about how to use PowerShell to gather geolocation information.

Benefits of using Azure Sentinel to detect and investigate RDP brute force attacks:

Azure Sentinel provides a unified view of security data from across your organization, including your on-premises and cloud environments. This makes it easier to detect and investigate security threats.

Azure Sentinel uses machine learning to identify patterns and anomalies in your security data. This can help you to detect threats that you would not be able to detect manually.

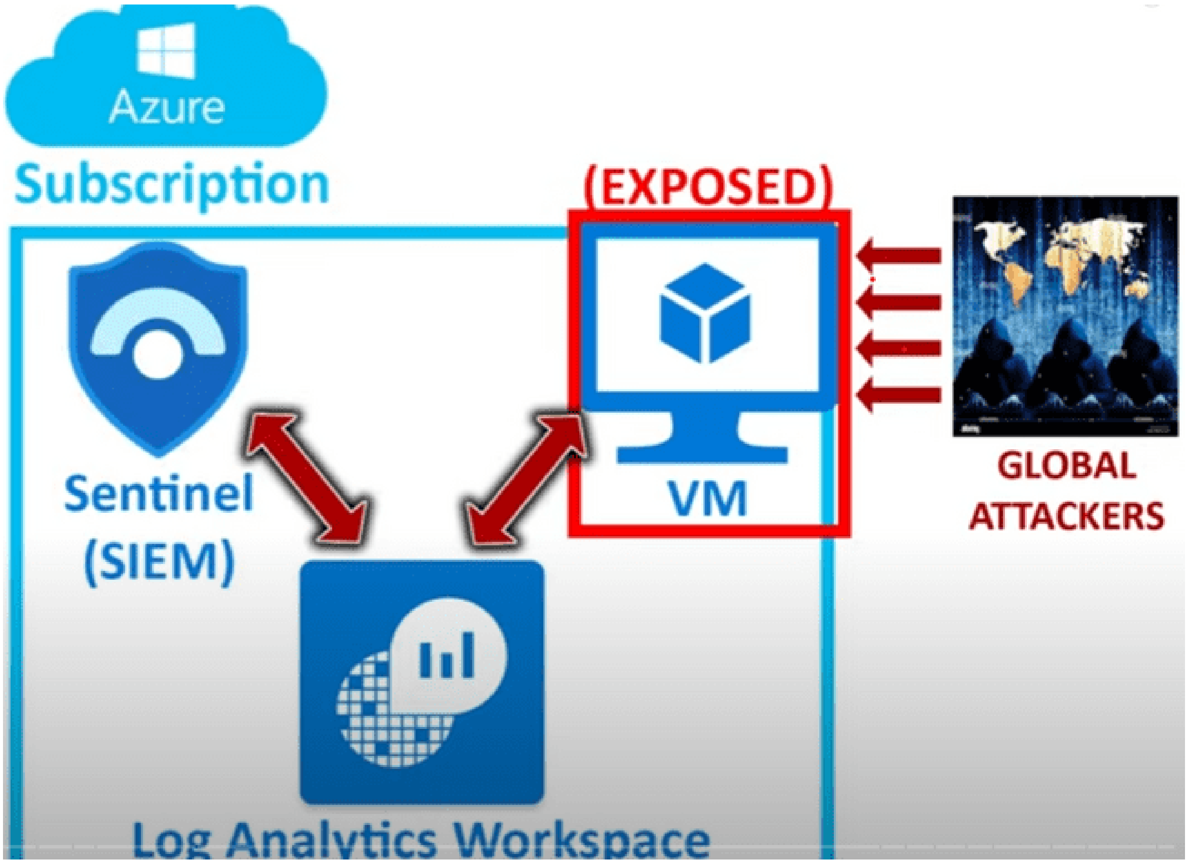
Azure Sentinel provides a variety of tools to help you investigate security threats. These tools include incident response tools, threat hunting tools, and forensics tools.

Benefits of using a custom PowerShell script to look up attackers' geolocation information:

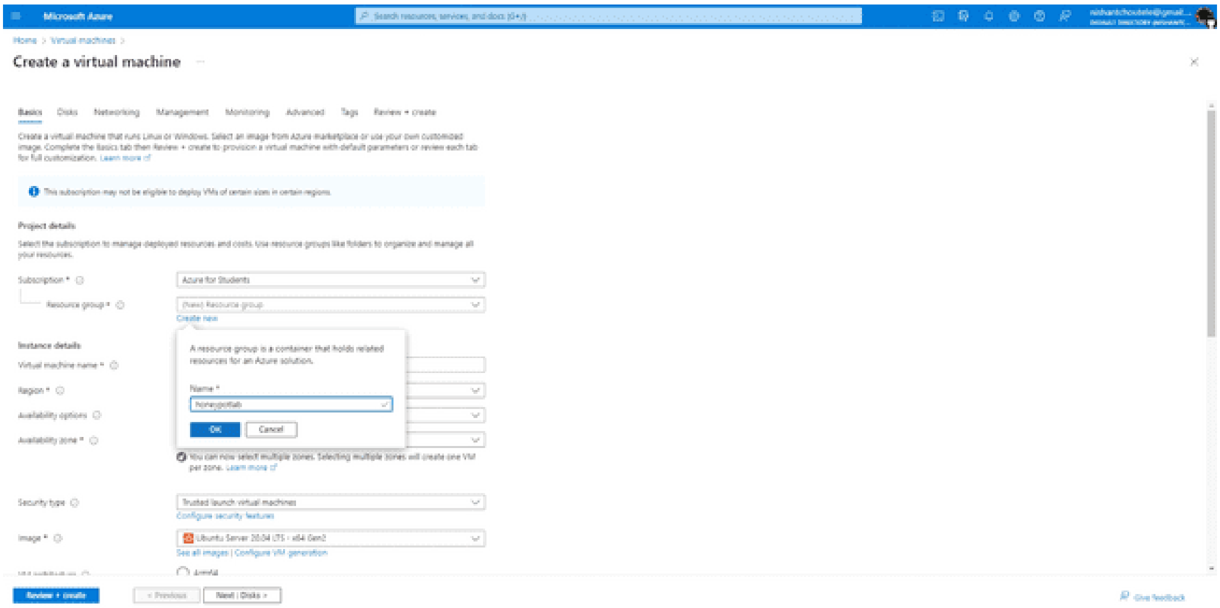
PowerShell is a powerful scripting language that can be used to automate a variety of tasks.

The custom PowerShell script that we will be using in this topic is very efficient and can quickly look up the geolocation information of a large number of IP addresses.

The custom PowerShell script is also very flexible and can be modified to meet your specific needs.



1. Creating a virtual machine



Create a virtual machine

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Azure for Students

Resource group * : (New) Resource group

Create new

A resource group is a container that holds related resources for an Azure solution.

Name * : honeypotlab

OK Cancel

Instance details

Virtual machine name *

Region *

Availability options

Availability zone *

You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more

Security type : Trusted launch virtual machines

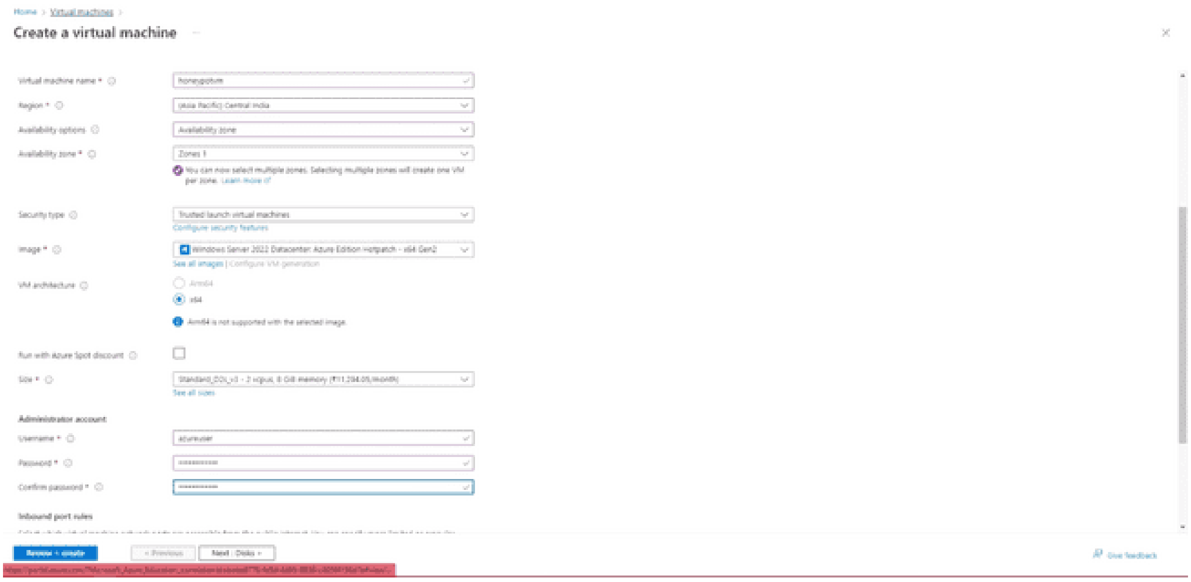
Configure security features

Image * : Ubuntu Server 20.04 LTS - x64 Gen2

See all images | Configure VM generation

VM architecture : ○ Arm64

Resource group honeypot lab and vm name honey pot



Home > Virtual machines >

Create a virtual machine

Virtual machine name * : honeypotvm

Region * : (Asia Pacific) Central India

Availability options : Availability zone

Availability zone * : Zones 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more

Security type : Trusted launch virtual machines

Configure security features

Image * : Windows Server 2022 Datacenter: Azure Edition Hotpatch - x64 Gen2

See all images | Configure VM generation

VM architecture : ○ Arm64 ● x64

Arm64 is not supported with the selected image.

Run with Azure Spot discount : □

Size * : Standard_D2s_v3 - 2 vcpus, 8 GiB memory (₹11,284.05/month)

See all sizes

Administrator account

Username * : azureuser

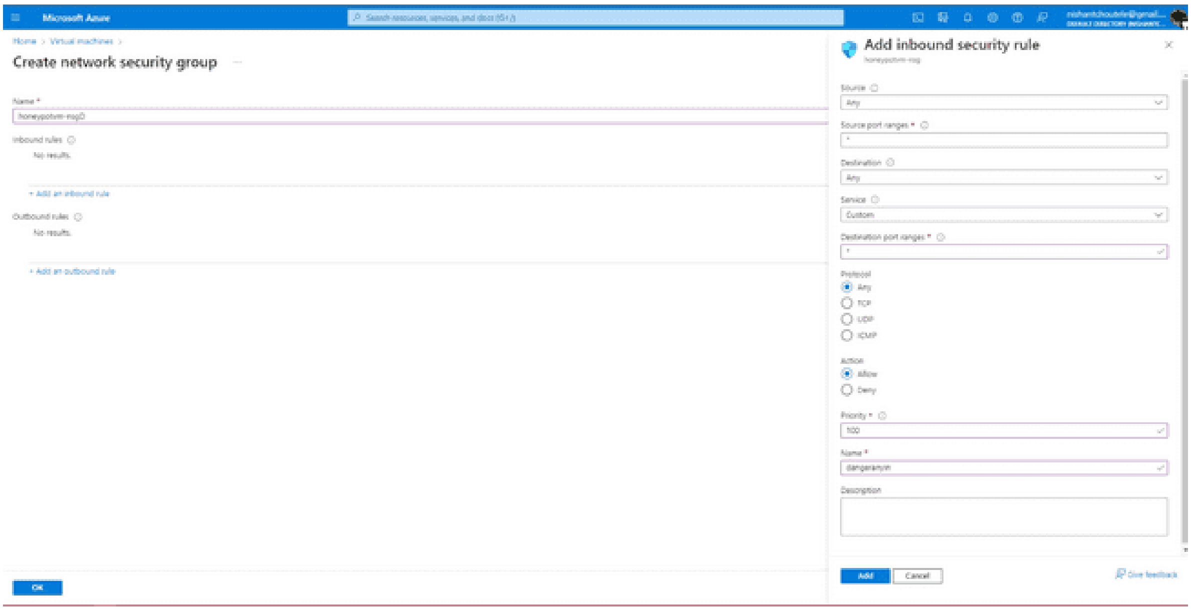
Password * : ••••••••••••

Confirm password * : ••••••••••••

Inbound port rules

2. Allow all in firewall

create a new network security group by giving destination port a * and setting priority to 100 so that security goes to its minimal stage



Home > Virtual machines >

Create network security group

Name * : honeypotvm-nsg

Inbound rules

No results.

+ Add an inbound rule

Outbound rules

No results.

+ Add an outbound rule

Add inbound security rule

honeypotvm-nsg

Source : Any

Source port ranges * : *

Destination : Any

Service : Custom

Destination port ranges * : *

Protocol : ● Any ○ TCP ○ UDP ○ ICMP

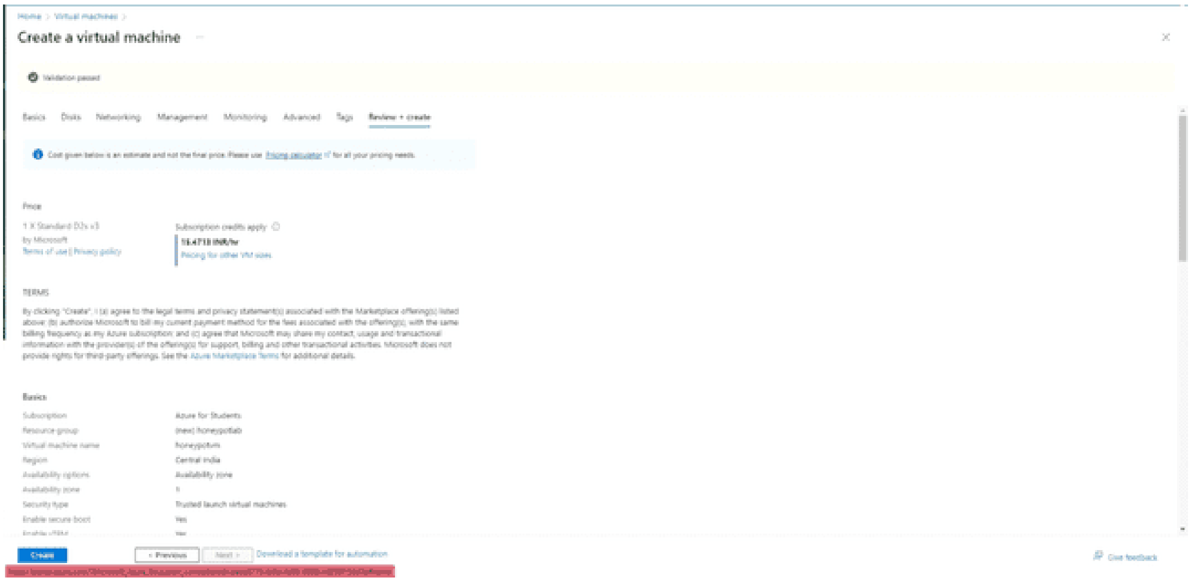
Action : ● Allow ○ Deny

Priority * : 100

Name * : dangeranyin

Description

Review and create



Home > Virtual machines >

Create a virtual machine

Validation passed

Cost given below is an estimate and not the final price. Please use Pricing calculator for all your pricing needs.

Price

1 X Standard D2s v3
by Microsoft
Terms of use | Privacy policy

Subscription credits apply
15.4718 INR/hr
Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

Basics

Subscription	Azure for Students
Resource group	(new) honeypotlab
Virtual machine name	honeypotvm
Region	Central India
Availability options	Availability zone
Availability zone	1
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes

[illegible]

3.Create a log analytics workspace

A Log Analytics workspace is a unique environment in Azure Monitor for storing and analyzing log data from Azure Monitor and other Azure services, such as Microsoft Sentinel and Microsoft Defender for Cloud. Each workspace has its own data repository and configuration, but it might combine data from multiple services.

Log Analytics workspaces are used to collect, store, and analyze log data to identify trends, patterns, and insights. Log Analytics workspaces can also be used to create alerts and notifications to help you quickly identify and respond to security threats.

Log Analytics workspaces are a powerful tool for monitoring and managing your Azure resources. They can help you to identify and troubleshoot problems, improve performance, and secure your environment.

Benefits of using a Log Analytics workspace:

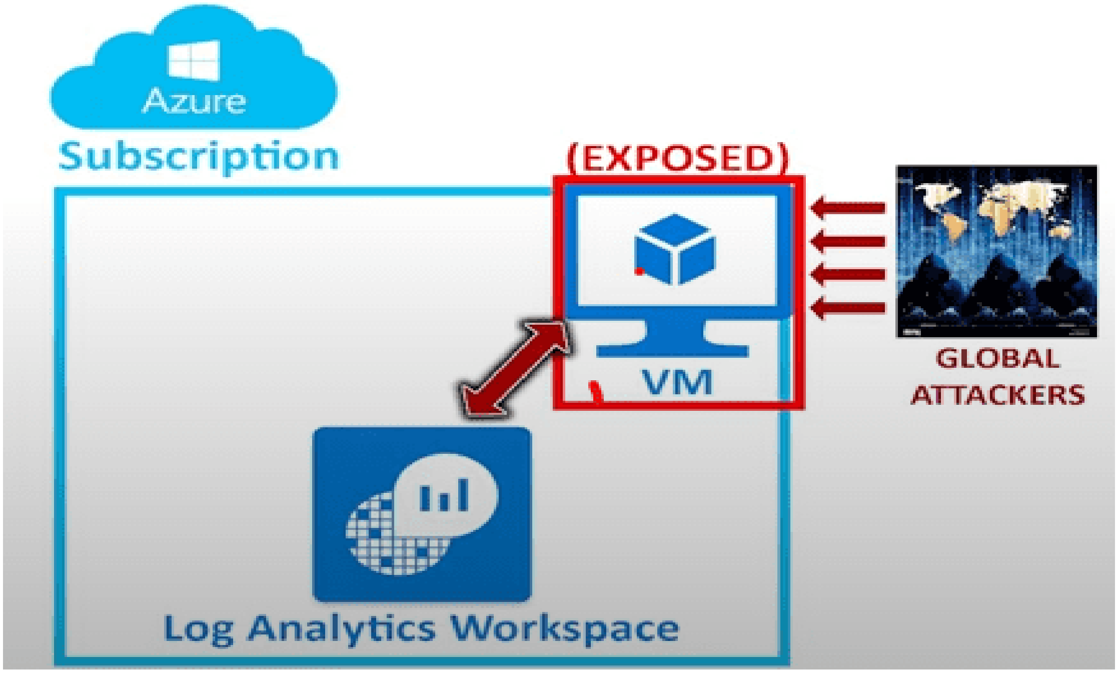
Centralized logging: Log Analytics workspaces provide a centralized location to store and analyze log data from all of your Azure resources. This makes it easier to identify trends and patterns in your data.

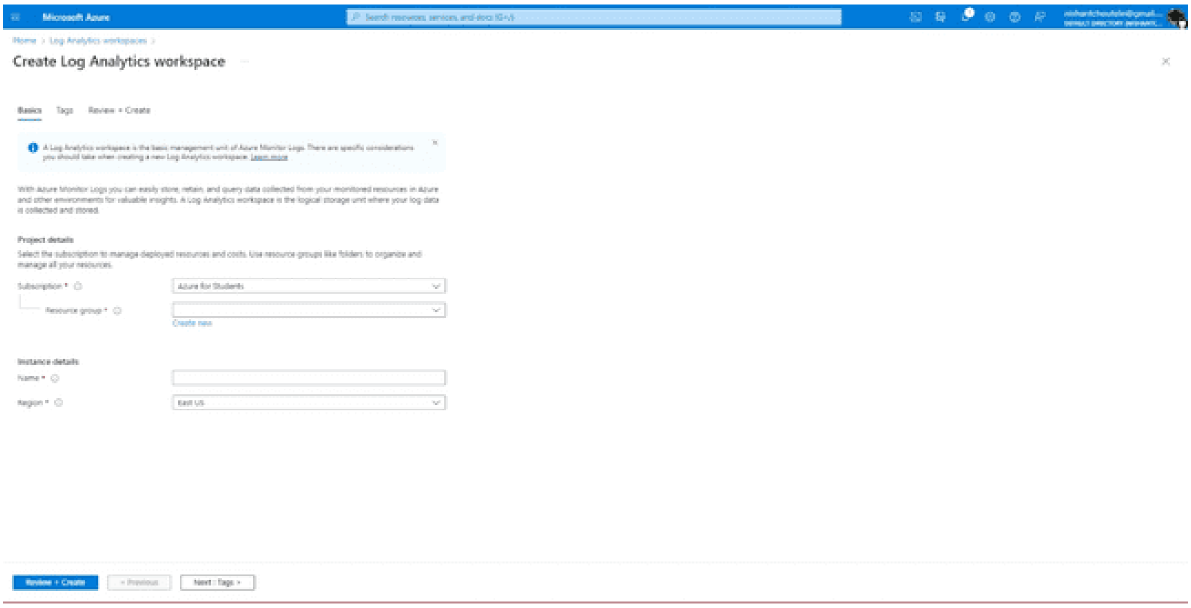
Advanced analytics: Log Analytics workspaces support advanced analytics capabilities, such as machine learning and artificial intelligence. This can help you to identify threats and problems that you would not be able to detect manually.

Alerting and notifications: Log Analytics workspaces can be used to create alerts and notifications to help you quickly identify and respond to security threats.

Compliance: Log Analytics workspaces can help you to comply with industry and regulatory requirements, such as PCI DSS and HIPAA.

If you are using Azure resources, I recommend that you create a Log Analytics workspace to collect and analyze your log data. Log Analytics workspaces are a powerful tool for monitoring and managing your Azure environment.





Create Log Analytics workspace

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Azure for Students

Resource group * :

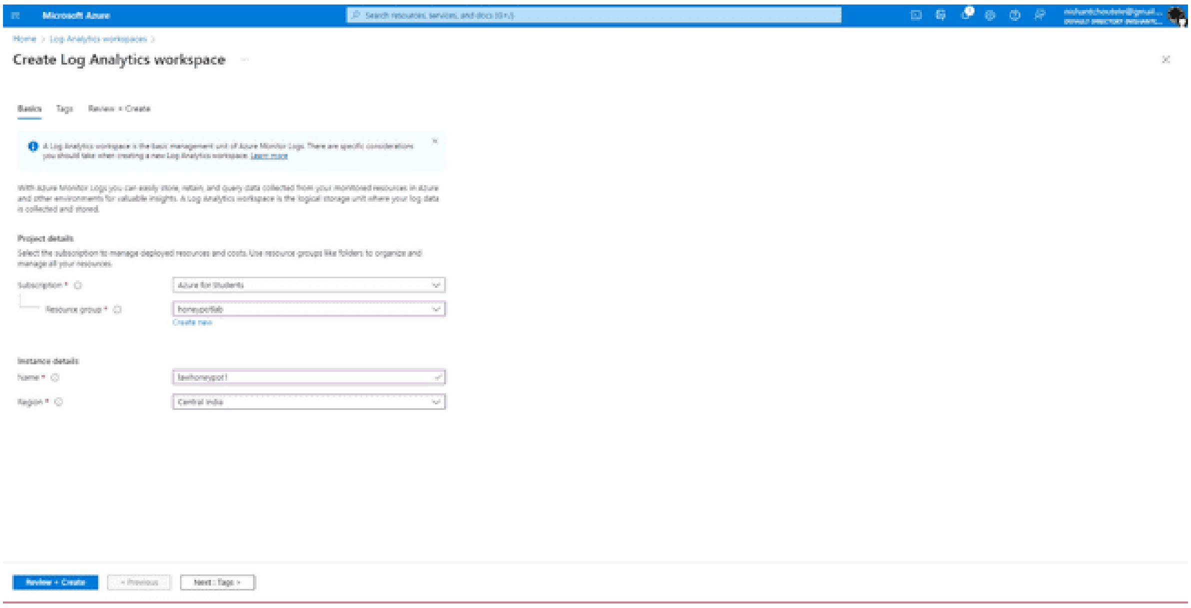
Create new

Instance details

Name * :

Region * : East US

Use the same resource group and create



Home > Log Analytics workspaces >

Create Log Analytics workspace

Basics | Tags | Review + Create

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Azure for Students

Resource group * : honeypotlab

Create new

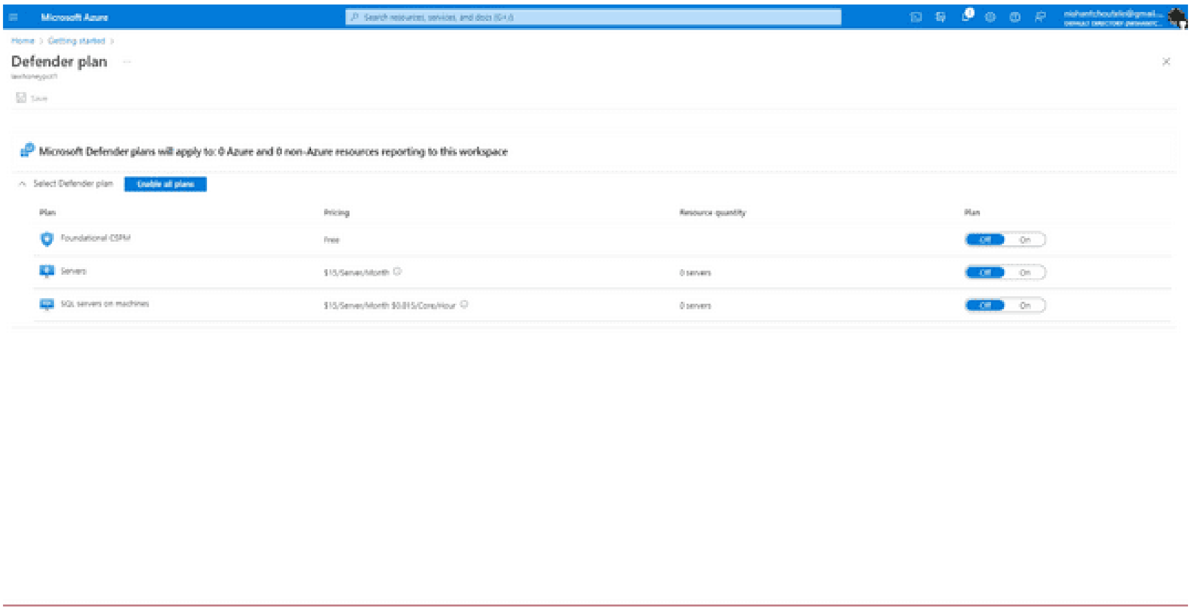
Instance details

Name * : lawhoneypot1

Region * : Central India

4.Enable gathering VM logs in Security Center

After creating go to Azure security center > pricing and settings> choose the created log analytics



Home > Getting started >

Defender plan

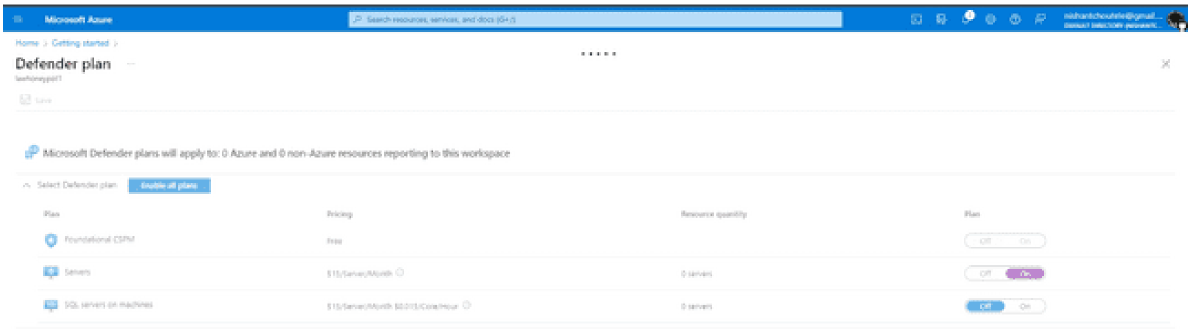
lawhoneypot1

Microsoft Defender plans will apply to: 0 Azure and 0 non-Azure resources reporting to this workspace

Select Defender plan

Plan	Pricing	Resource quantity	Plan
Foundational CSPM	Free		Off On
Servers	$15/Server/Month	0 servers	Off On
SQL servers on machines	$15/Server/Month $0.015/Core/Hour	0 servers	Off On

Set servers on and SQL servers off



Defender plan

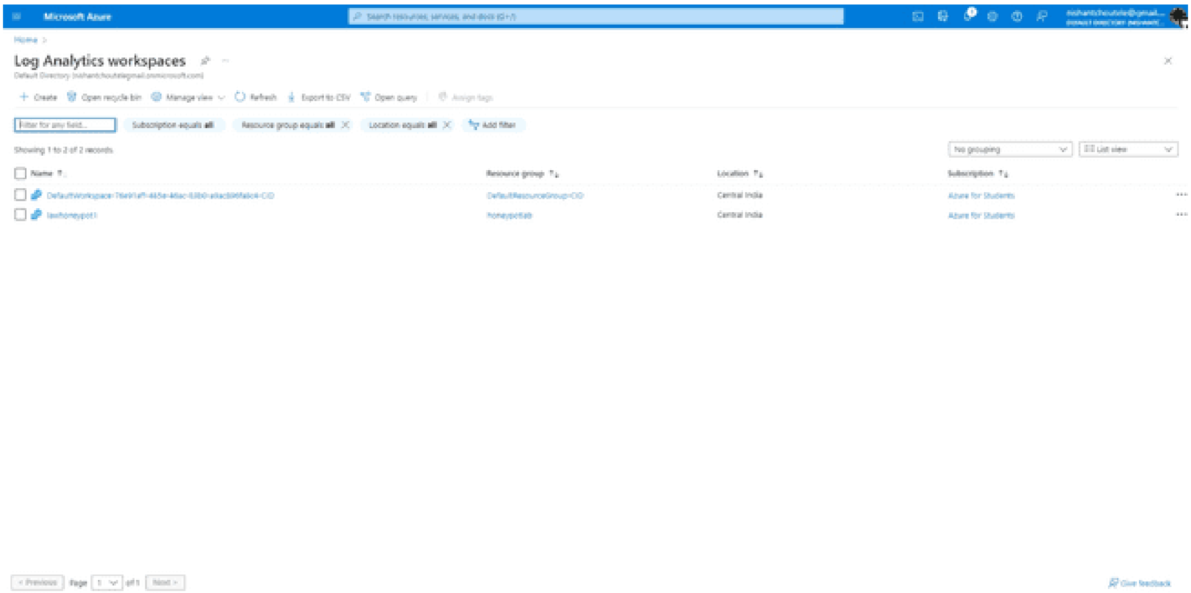
lawhoneypot1

Microsoft Defender plans will apply to: 0 Azure and 0 non-Azure resources reporting to this workspace

Plan	Pricing	Resource quantity	Plan
Foundational CSPM	Free		Off / On
Servers	$15/Server/Month	0 servers	Off / **On**
SQL servers on machines	$15/Server/Month $0.015/Core/Hour	0 servers	**Off** / On

5.Connect Log Analytics to VM

Now go to log analytics workspace and connect the VM

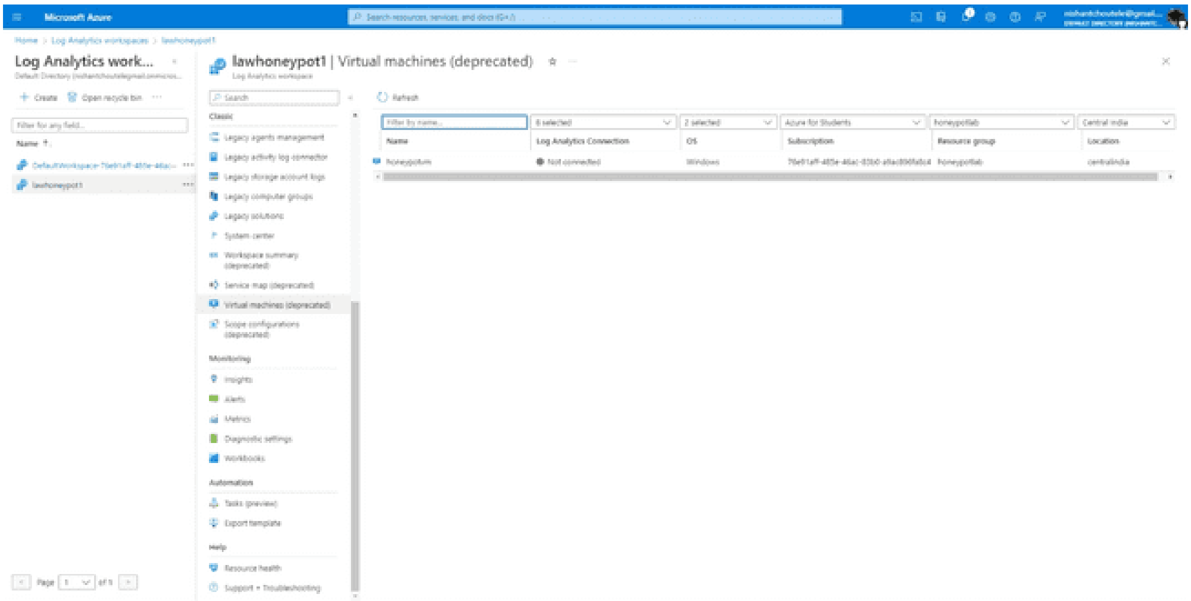


Log Analytics workspaces

Showing 1 to 2 of 2 records.

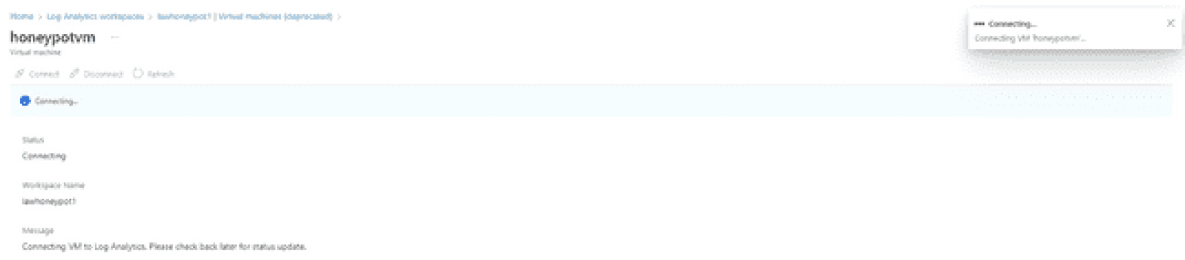
Name	Resource group	Location	Subscription
DefaultWorkspace-[illegible]-CID	DefaultResourceGroup-CID	Central India	Azure for Students
lawhoneypot1	honeypotlab	Central India	Azure for Students

click on the virtual machine



Filter by name...	6 selected	2 selected	Azure for Students	honeypotlab	Central India
Name	Log Analytics Connection	OS	Subscription	Resource group	Location
honeypotvm	● Not connected	Windows	70e91aff-485e-46ac-83b0-a9ac890fa5c4	honeypotlab	centralindia

Connect



Home > Log Analytics workspaces > lawhoneypot1 | Virtual machines (deprecated) >
honeypotvm
Virtual machine
Connect
Disconnect
Refresh
Connecting...
••• Connecting...
Connecting VM 'honeypotvm'...

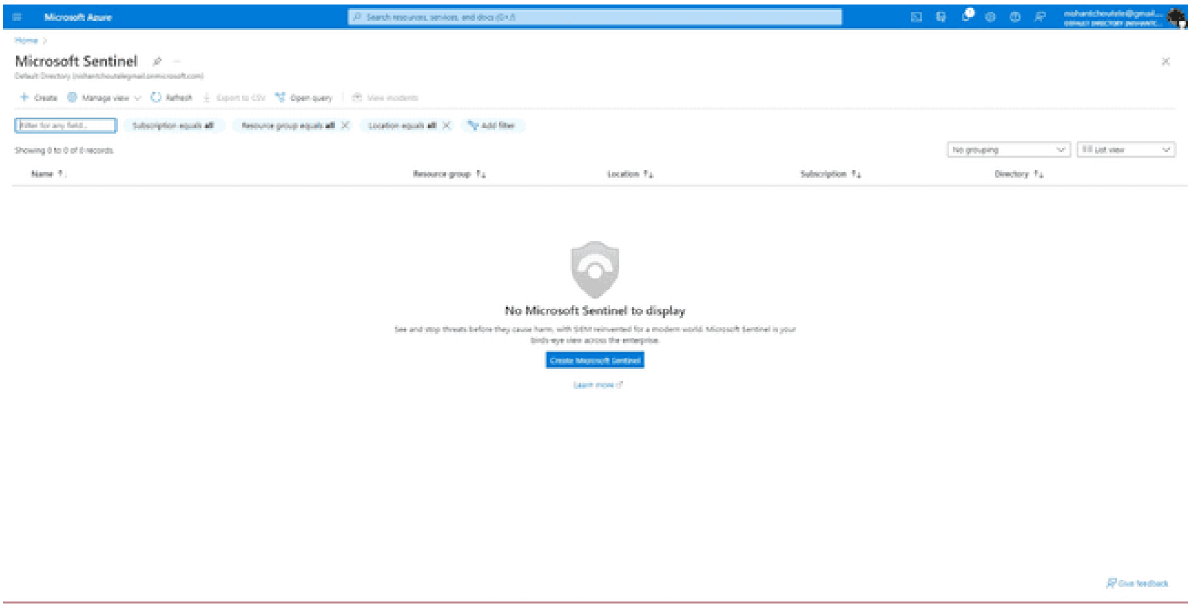
Status
Connecting

Workspace Name
lawhoneypot1

Message
Connecting VM to Log Analytics. Please check back later for status update.

6.Setup Azure Sentinel

create> select the workspace connected to virtual > select ADD

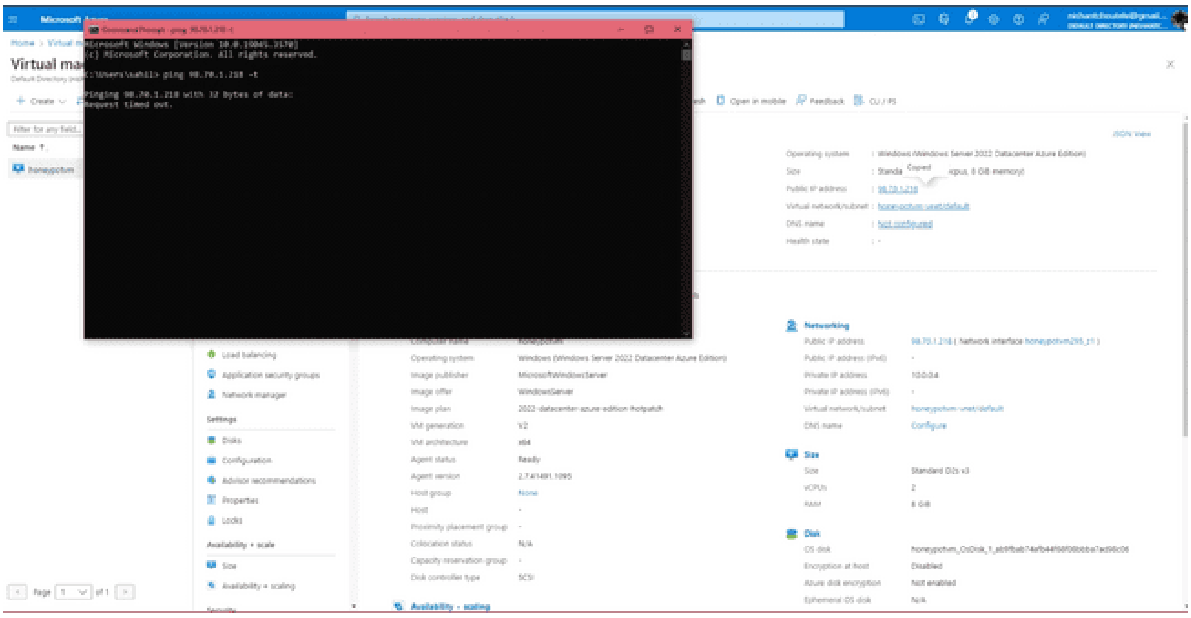


Showing 0 to 0 of 0 records.

No Microsoft Sentinel to display

See and stop threats before they cause harm, with SIEM reinvented for a modern world. Microsoft Sentinel is your birds-eye view across the enterprise.

Before loggin in to virtual machine. Go to cmd and ping the public ip of the virtual machine with the command ping 192.168.0.0 -t



```
Microsoft Windows [Version 10.0.19045.3170]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sahil> ping 98.70.1.218 -t

Pinging 98.70.1.218 with 32 bytes of data:
Request timed out.
```

Operating system : Windows (Windows Server 2022 Datacenter Azure Edition)
Size : Standa Copied vcpus, 8 GiB memory)
Public IP address : 98.70.1.218
Virtual network/subnet : honeypotvm-vnet/default
DNS name : Not configured
Health state : -

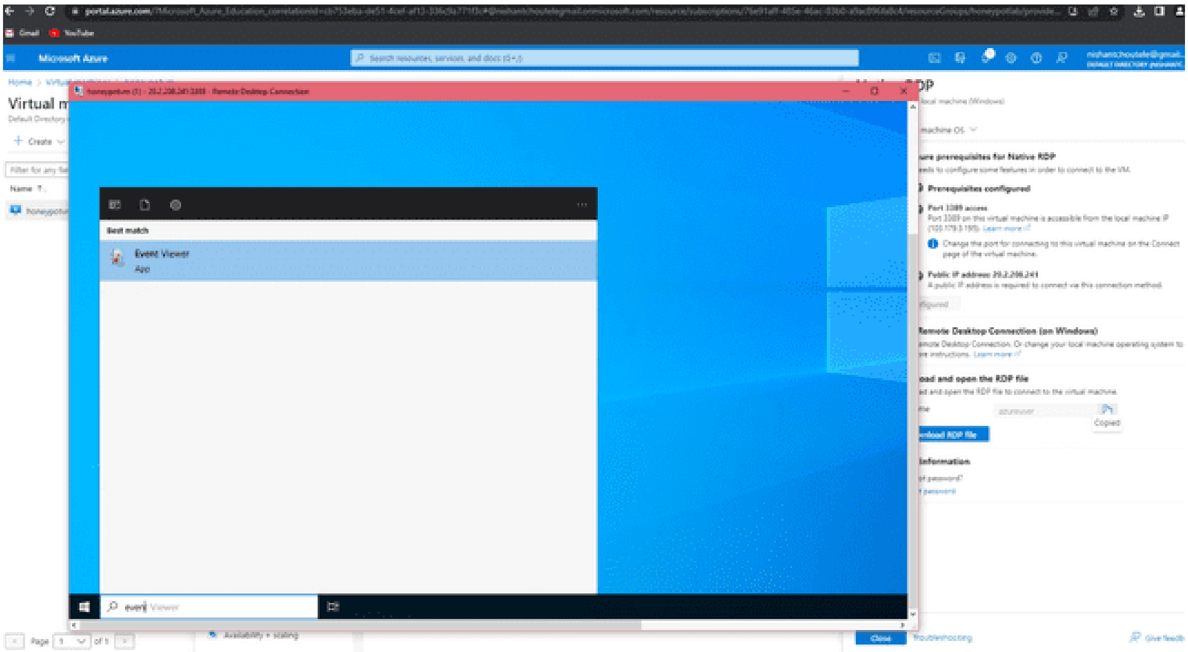
Computer name honeypotvm
Operating system Windows (Windows Server 2022 Datacenter Azure Edition)
Image publisher MicrosoftWindowsServer
Image offer WindowsServer
Image plan 2022-datacenter-azure-edition-hotpatch
VM generation V2
VM architecture x64
Agent status Ready
Agent version 2.7.41491.1095
Host group None
Host -
Proximity placement group -
Colocation status N/A
Capacity reservation group -
Disk controller type SCSI

Networking
Public IP address 98.70.1.218 (Network interface honeypotvm295_z1)
Public IP address (IPv6) -
Private IP address 10.0.0.4
Private IP address (IPv6) -
Virtual network/subnet honeypotvm-vnet/default
DNS name Configure

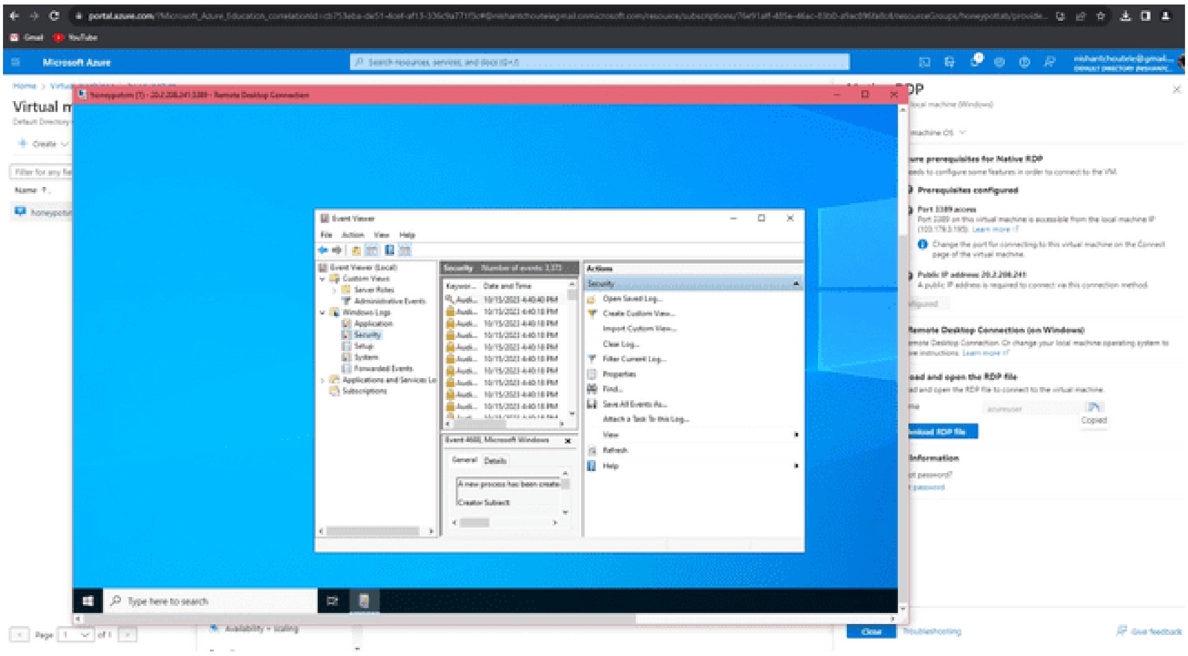
Size
Size Standard D2s v3
vCPUs 2
RAM 8 GiB

Disk
OS disk honeypotvm_OsDisk_1_ab9fbab74afb44f68f08bbba7ad66c06
Encryption at host Disabled
Azure disk encryption Not enabled
Ephemeral OS disk N/A

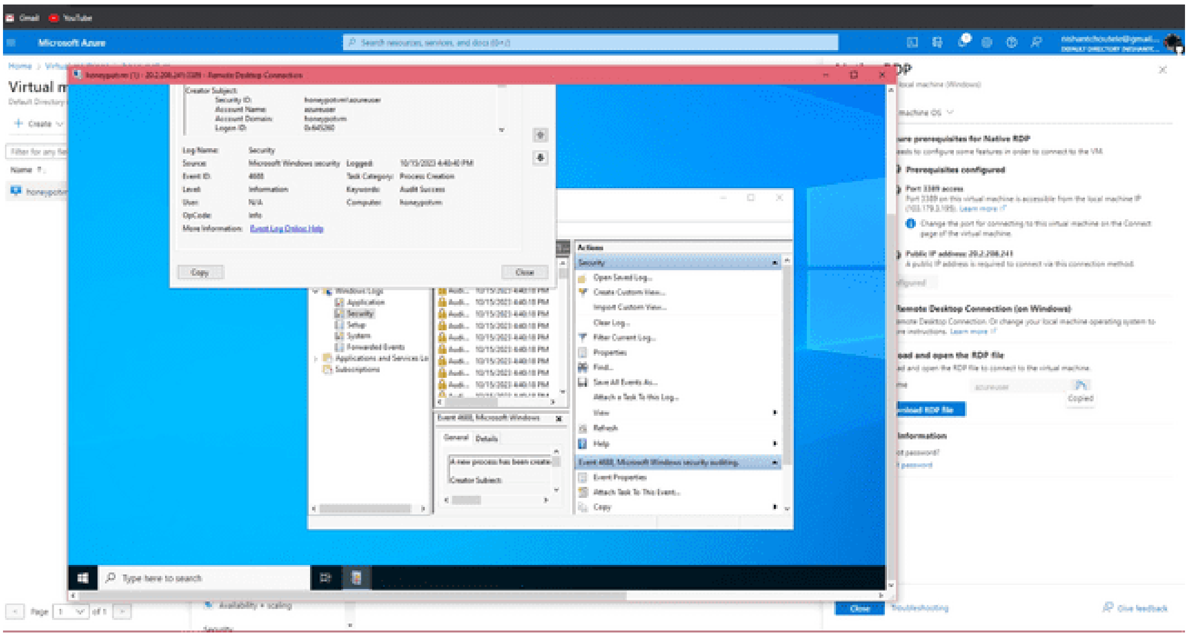
It will show request timeout. connect to the VM and go to Event Viewer



Go to Windows Logs> Security



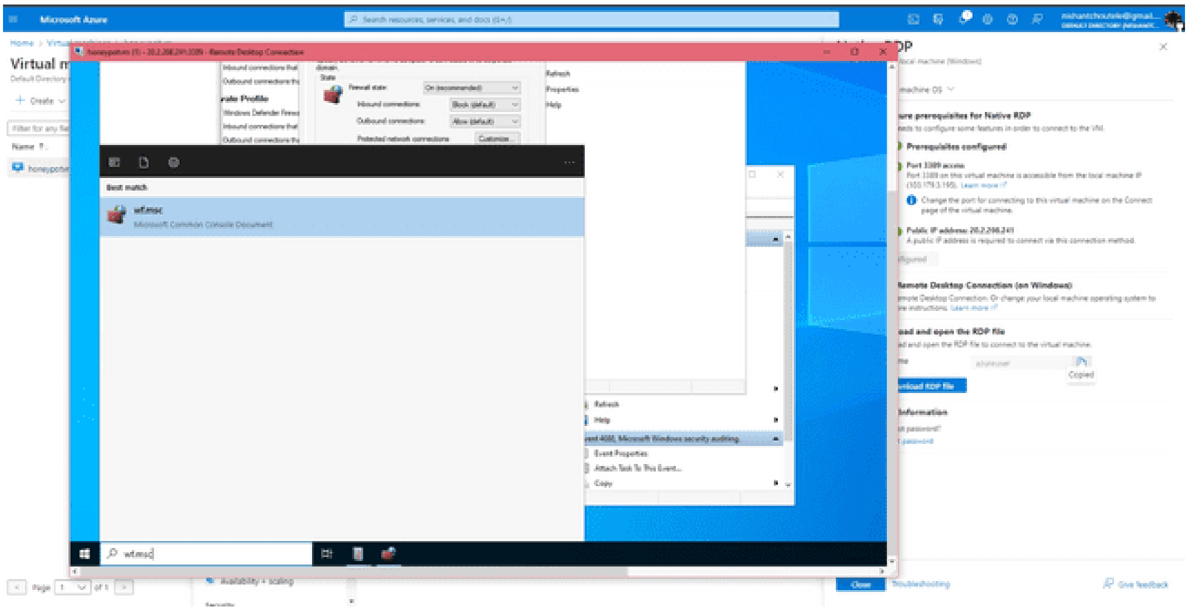
Click on the folders and check the login info of the user who logged in



```
Creator Subject:
        Security ID:        honeypotvm\azureuser
        Account Name:       azureuser
        Account Domain:     honeypotvm
        Logon ID:           0x645260

Log Name:       Security
Source:         Microsoft Windows security   Logged:         10/15/2023 4:40:40 PM
Event ID:       4688                         Task Category:  Process Creation
Level:          Information                  Keywords:       Audit Success
User:           N/A                          Computer:       honeypotvm
OpCode:         Info
More Information:  Event Log Online Help
```

7. Turn of Windows Firewall on VM

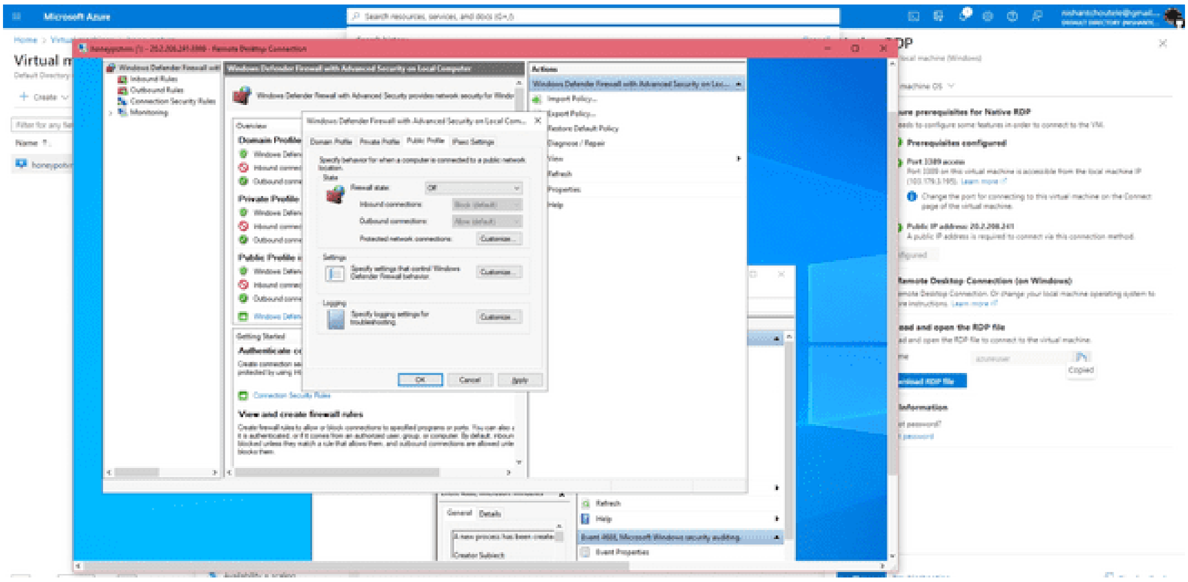
NOW go to wf.msc



```
Firewall state:            On (recommended)
Inbound connections:       Block (default)
Outbound connections:      Allow (default)
Protected network connections:   Customize...
```

Best match
wf.msc
Microsoft Common Console Document

Put Domain profile, private profile and private profile firewall status off so the attackers can see it



Windows Defender Firewall with Advanced Security on Local Computer

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to a public network location.

State

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

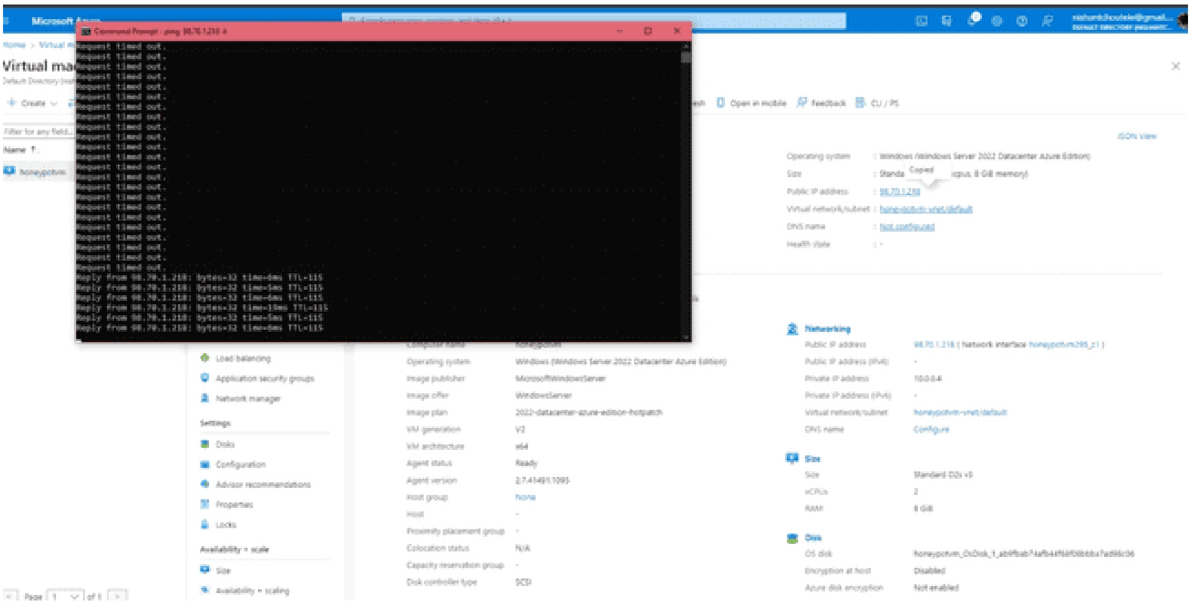
Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

OK Cancel Apply

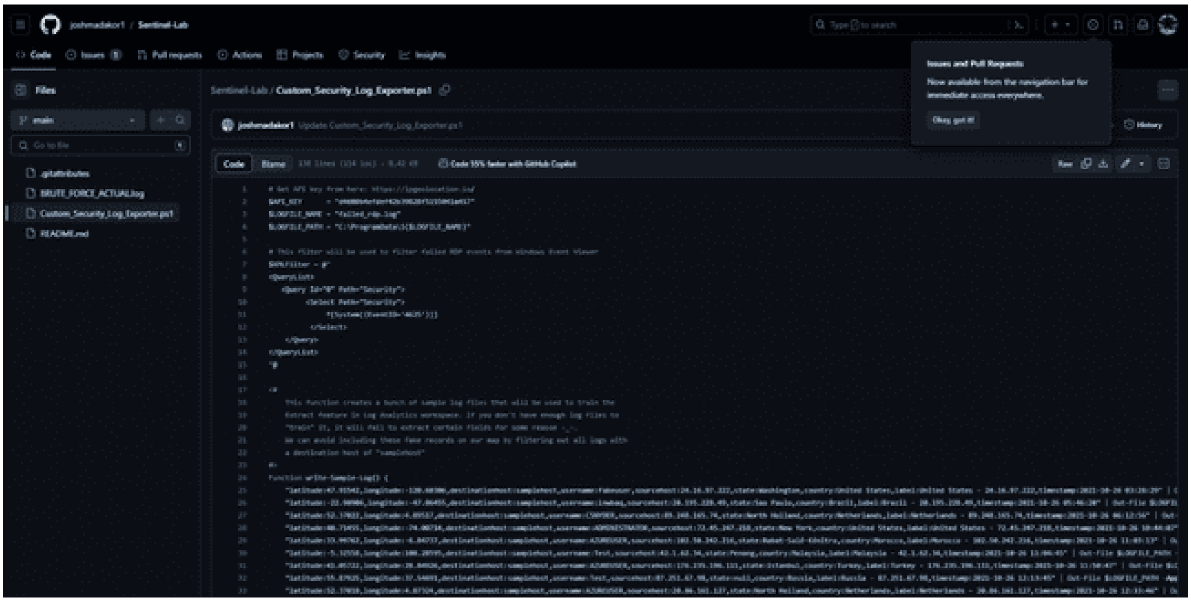
Now check the ping status in cmd



```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 98.70.1.218: bytes=32 time=6ms TTL=115
Reply from 98.70.1.218: bytes=32 time=5ms TTL=115
Reply from 98.70.1.218: bytes=32 time=6ms TTL=115
Reply from 98.70.1.218: bytes=32 time=10ms TTL=115
Reply from 98.70.1.218: bytes=32 time=5ms TTL=115
Reply from 98.70.1.218: bytes=32 time=6ms TTL=115
```

8.Download PowerShell Script

Now copy the script of custom security log

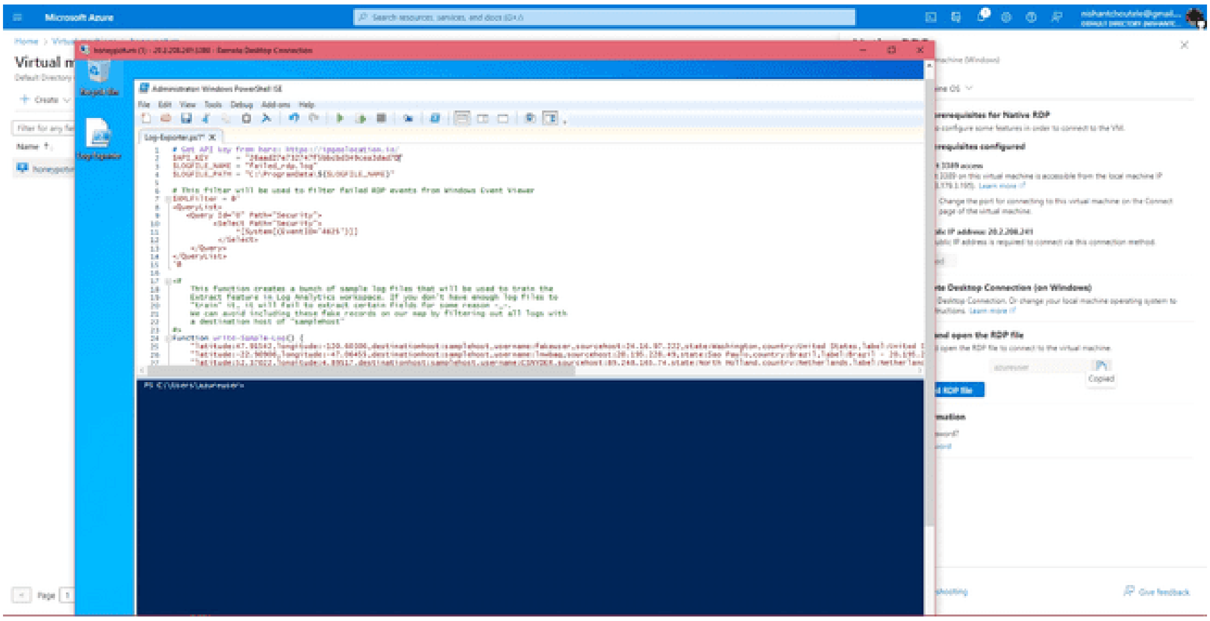


Sentinel-Lab / Custom_Security_Log_Exporter.ps1

joshmadakor1 Update Custom_Security_Log_Exporter.ps1

```
# Get API key from here: https://ipgeolocation.io/
$API_KEY      = "[illegible]"
$LOGFILE_NAME = "failed_rdp.log"
$LOGFILE_PATH = "C:\ProgramData\$($LOGFILE_NAME)"

# This filter will be used to filter failed RDP events from Windows Event Viewer
$XMLFilter = @'
<QueryList>
   <Query Id="0" Path="Security">
         <Select Path="Security">
              *[System[(EventID='4625')]]
          </Select>
    </Query>
</QueryList>
'@

<#
    This function creates a bunch of sample log files that will be used to train the
    Extract feature in Log Analytics workspace. If you don't have enough log files to
    "train" it, it will fail to extract certain fields for some reason -_-.
    We can avoid including these fake records on our map by filtering out all logs with
    a destination host of "samplehost"
#>
Function write-Sample-Log() {
    "latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washington,country:United States,label:United States - 24.16.97.222,timestamp:2021-10-26 03:28:29" | O
    "latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country:Brazil,label:Brazil - 20.195.228.49,timestamp:2021-10-26 05:46:20" | Out-File $LOGFIL
    "latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:North Holland,country:Netherlands,label:Netherlands - 89.248.165.74,timestamp:2021-10-26 06:12:56" | Out-
    "latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.247.218,state:New York,country:United States,label:United States - 72.45.247.218,timestamp:2021-10-26 10:44:07"
    "latitude:33.99762,longitude:-6.84737,destinationhost:samplehost,username:AZUREUSER,sourcehost:102.50.242.216,state:Rabat-Salé-Kénitra,country:Morocco,label:Morocco - 102.50.242.216,timestamp:2021-10-26 11:03:13" | Ou
    "latitude:-5.32558,longitude:100.28595,destinationhost:samplehost,username:Test,sourcehost:42.1.62.34,state:Penang,country:Malaysia,label:Malaysia - 42.1.62.34,timestamp:2021-10-26 11:04:45" | Out-File $LOGFILE_PATH -
    "latitude:41.05722,longitude:28.84926,destinationhost:samplehost,username:AZUREUSER,sourcehost:176.235.196.111,state:Istanbul,country:Turkey,label:Turkey - 176.235.196.111,timestamp:2021-10-26 11:50:47" | Out-File $LO
    "latitude:55.87925,longitude:37.54691,destinationhost:samplehost,username:Test,sourcehost:87.251.67.98,state:null,country:Russia,label:Russia - 87.251.67.98,timestamp:2021-10-26 12:13:45" | Out-File $LOGFILE_PATH -App
    "latitude:52.37018,longitude:4.87324,destinationhost:samplehost,username:AZUREUSER,sourcehost:20.86.161.127,state:North Holland,country:Netherlands,label:Netherlands - 20.86.161.127,timestamp:2021-10-26 12:33:46" | Ou
```

Paste it inside the Powershell.ISE and save it naming log exporter



Administrator: Windows PowerShell ISE

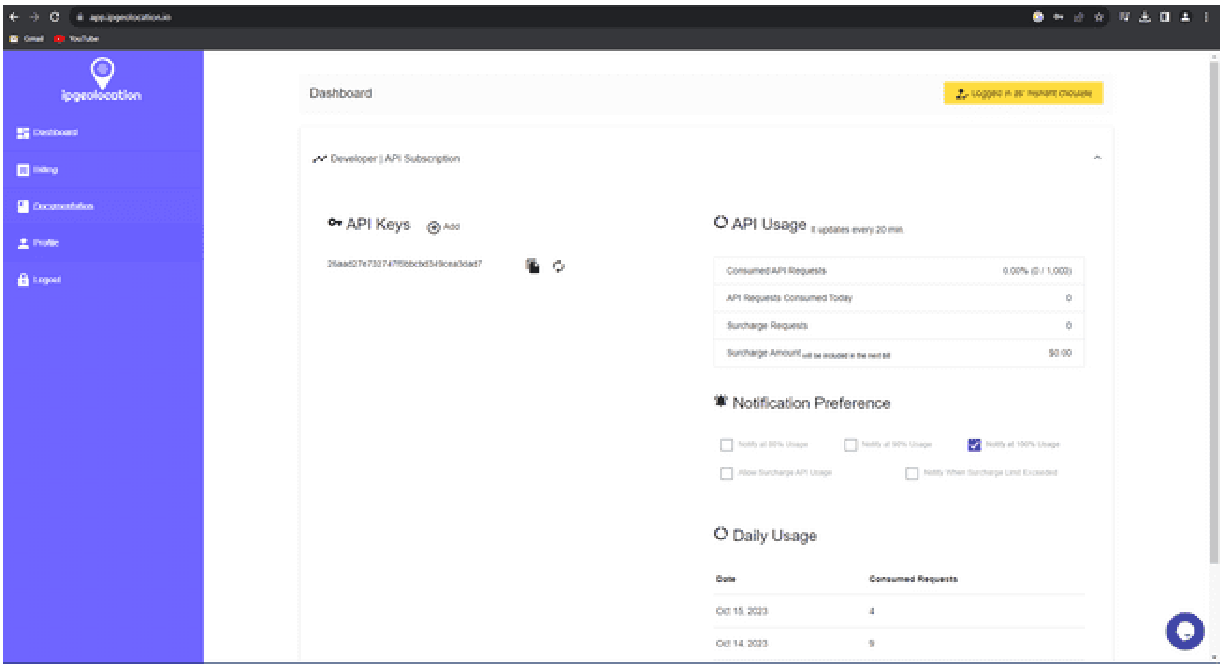
Log-Exporter.ps1*

```
# Get API key from here: https://ipgeolocation.io/
$API_KEY      = "[illegible]"
$LOGFILE_NAME = "failed_rdp.log"
$LOGFILE_PATH = "C:\ProgramData\$($LOGFILE_NAME)"

# This filter will be used to filter failed RDP events from Windows Event Viewer
$XMLFilter = @'
<QueryList>
   <Query Id="0" Path="Security">
         <Select Path="Security">
              *[System[(EventID='4625')]]
          </Select>
    </Query>
</QueryList>
'@

<#
    This function creates a bunch of sample log files that will be used to train the
    Extract feature in Log Analytics workspace. If you don't have enough log files to
    "train" it, it will fail to extract certain fields for some reason -_-.
    We can avoid including these fake records on our map by filtering out all logs with
    a destination host of "samplehost"
#>
Function write-Sample-Log() {
    "latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washington,country:United States,label:United S
    "latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country:Brazil,label:Brazil - 20.195.2
    "latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:North Holland,country:Netherlands,label:Netherlan
```

```
PS C:\Users\azureuser>
```

9.Get Geolocation.io API Key

now go to ipgeolocation for the API key without it we wont be getting the geodata and we wont be getting latitute, longitude etc.



Dashboard

Developer | API Subscription

API Keys ⊕ Add

26aad27e732747f5bbcbd349cea3dad7

API Usage it updates every 20 min.

Consumed API Requests	0.00% (0 / 1,000)
API Requests Consumed Today	0
Surcharge Requests	0
Surcharge Amount will be included in the next bill	$0.00

Notification Preference

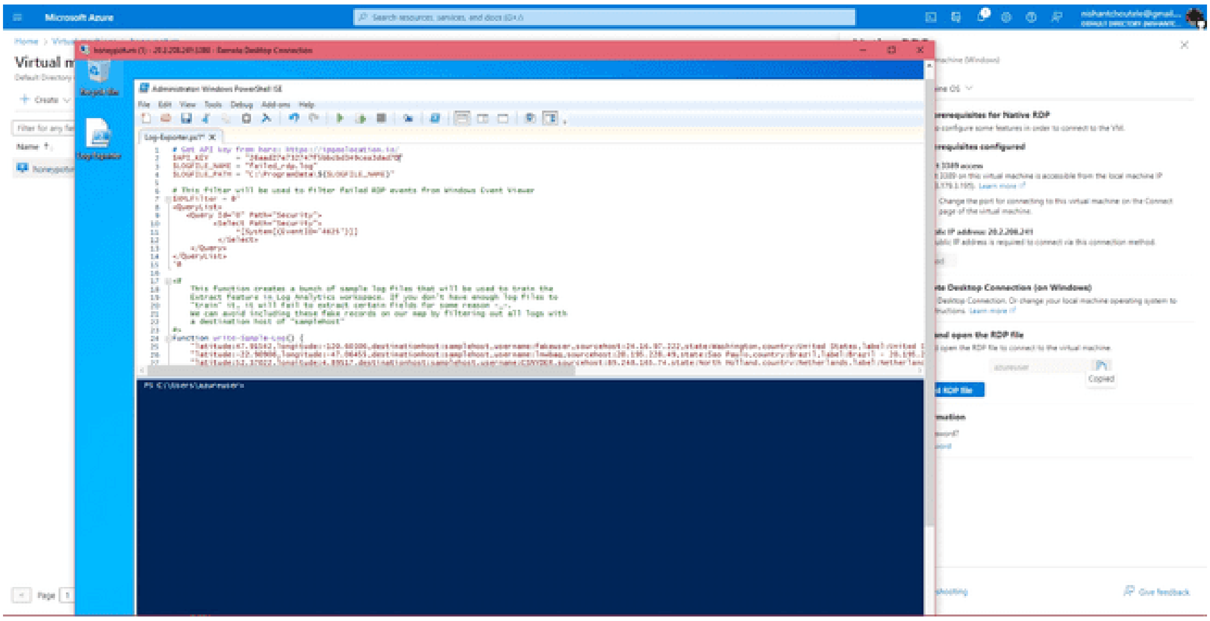
□ Notify at 80% Usage □ Notify at 90% Usage ☑ Notify at 100% Usage
□ Allow Surcharge API Usage □ Notify When Surcharge Limit Exceeded

Daily Usage

Date	Consumed Requests
Oct 15, 2023	4
Oct 14, 2023	9

copy the api key and paste it in the script and Run!

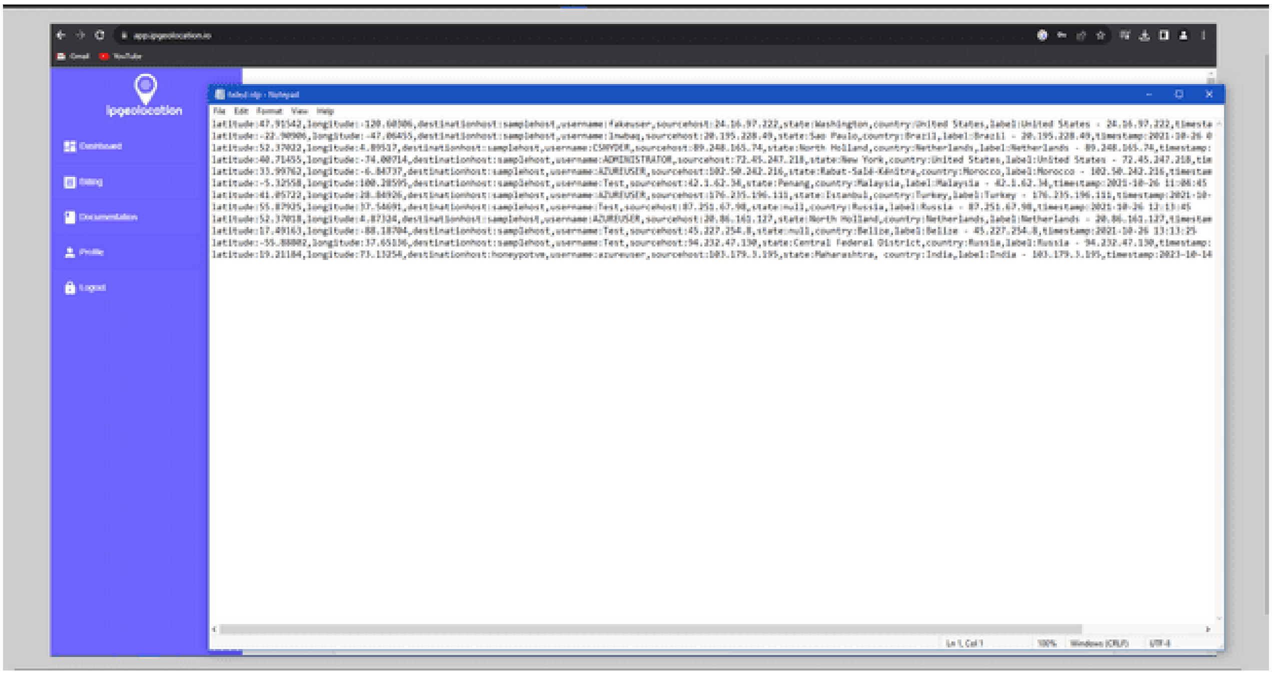
This script runs in a loop. It looks through the event log and all th security log grabs all the events of people who failed to login into the honeypot virtual machine grabs the ip address and gets the geo data through the api key.


Microsoft Azure
Search resources, services, and docs (G+/)
Virtual m
honeypotvm (1) - 20.2.208.241:3389 - Remote Desktop Connection
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Log-Exporter.ps1*
Recycle Bin
Prerequisites for Native RDP
Download RDP file
Copied
Give feedback

```
# Get API key from here: https://ipgeolocation.io/
$API_KEY      = "26aad27e732747f5bbcbd349cea3dad7"
$LOGFILE_NAME = "failed_rdp.log"
$LOGFILE_PATH = "C:\ProgramData\$($LOGFILE_NAME)"

# This filter will be used to filter failed RDP events from Windows Event Viewer
$XMLFilter = @'
<QueryList>
   <Query Id="0" Path="Security">
         <Select Path="Security">
              *[System[(EventID='4625')]]
          </Select>
    </Query>
</QueryList>
'@

<#
    This function creates a bunch of sample log files that will be used to train the
    Extract feature in Log Analytics workspace. If you don't have enough log files to
    "train" it, it will fail to extract certain fields for some reason -_-.
    We can avoid including these fake records on our map by filtering out all logs with
    a destination host of "samplehost"
#>
Function write-Sample-Log() {
    "latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washington,country:United States,label:United S
    "latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country:Brazil,label:Brazil - 20.195.2
    "latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:North Holland,country:Netherlands,label:Netherlan
```

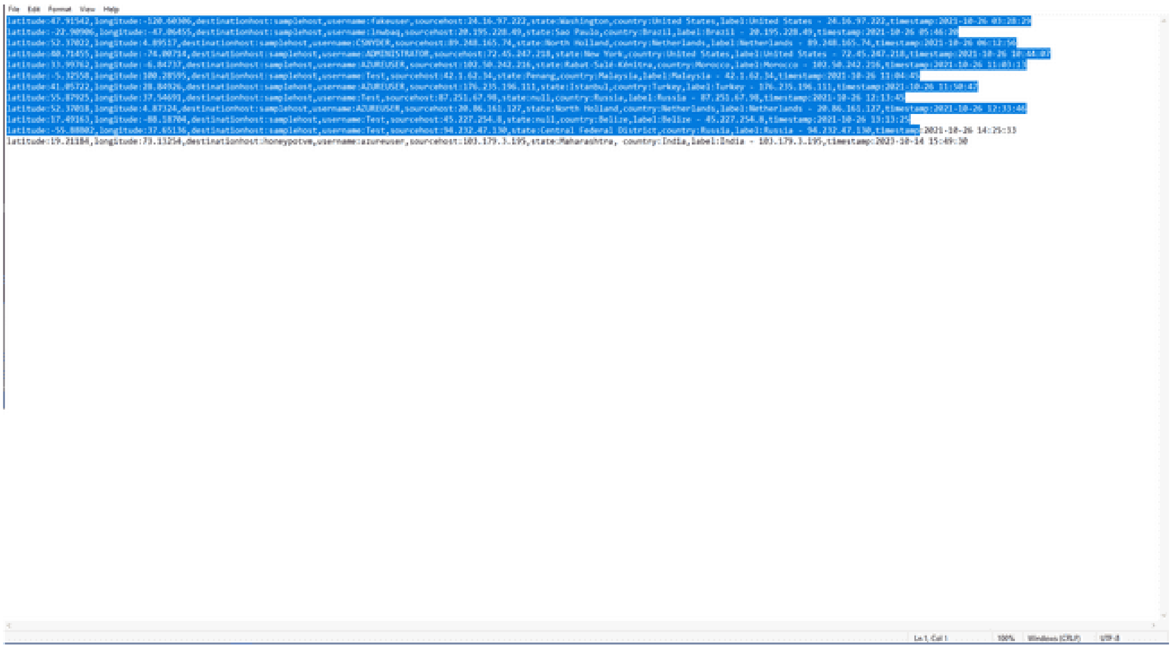
```
PS C:\Users\azureuser>
```

After running a log file get created inside the given path which trains the log analytics workspace to provide the data in a format which get showed in powershell



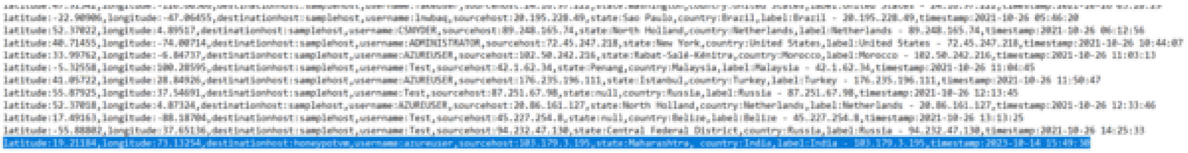
```
latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washington,country:United States,label:United States - 24.16.97.222,timesta
latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country:Brazil,label:Brazil - 20.195.228.49,timestamp:2021-10-26 0
latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:North Holland,country:Netherlands,label:Netherlands - 89.248.165.74,timestamp:
latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.247.218,state:New York,country:United States,label:United States - 72.45.247.218,tim
latitude:33.99762,longitude:-6.84737,destinationhost:samplehost,username:AZUREUSER,sourcehost:102.50.242.216,state:Rabat-Salé-Kénitra,country:Morocco,label:Morocco - 102.50.242.216,timestam
latitude:-5.32558,longitude:100.28595,destinationhost:samplehost,username:Test,sourcehost:42.1.62.34,state:Penang,country:Malaysia,label:Malaysia - 42.1.62.34,timestamp:2021-10-26 11:04:45
latitude:41.05722,longitude:28.84926,destinationhost:samplehost,username:AZUREUSER,sourcehost:176.235.196.111,state:Istanbul,country:Turkey,label:Turkey - 176.235.196.111,timestamp:2021-10-
latitude:55.87925,longitude:37.54691,destinationhost:samplehost,username:Test,sourcehost:87.251.67.98,state:null,country:Russia,label:Russia - 87.251.67.98,timestamp:2021-10-26 12:13:45
latitude:52.37018,longitude:4.87324,destinationhost:samplehost,username:AZUREUSER,sourcehost:20.86.161.127,state:North Holland,country:Netherlands,label:Netherlands - 20.86.161.127,timestam
latitude:17.49163,longitude:-88.18704,destinationhost:samplehost,username:Test,sourcehost:45.227.254.8,state:null,country:Belize,label:Belize - 45.227.254.8,timestamp:2021-10-26 13:13:25
latitude:-55.88802,longitude:37.65136,destinationhost:samplehost,username:Test,sourcehost:94.232.47.130,state:Central Federal District,country:Russia,label:Russia - 94.232.47.130,timestamp:
latitude:19.21184,longitude:73.13254,destinationhost:honeypotvm,username:azureuser,sourcehost:103.179.3.195,state:Maharashtra, country:India,label:India - 103.179.3.195,timestamp:2023-10-14
```

This the sample data to train the logt analytics works space



```
latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washington,country:United States,label:United States - 24.16.97.222,timestamp:2021-10-26 03:28:29
latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country:Brazil,label:Brazil - 20.195.228.49,timestamp:2021-10-26 05:46:20
latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:North Holland,country:Netherlands,label:Netherlands - 89.248.165.74,timestamp:2021-10-26 06:12:56
latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.247.218,state:New York,country:United States,label:United States - 72.45.247.218,timestamp:2021-10-26 10:44:07
latitude:33.99762,longitude:-6.84737,destinationhost:samplehost,username:AZUREUSER,sourcehost:102.50.242.216,state:Rabat-Salé-Kénitra,country:Morocco,label:Morocco - 102.50.242.216,timestamp:2021-10-26 11:03:13
latitude:-5.32558,longitude:100.28595,destinationhost:samplehost,username:Test,sourcehost:42.1.62.34,state:Penang,country:Malaysia,label:Malaysia - 42.1.62.34,timestamp:2021-10-26 11:04:45
latitude:41.05722,longitude:28.84926,destinationhost:samplehost,username:AZUREUSER,sourcehost:176.235.196.111,state:Istanbul,country:Turkey,label:Turkey - 176.235.196.111,timestamp:2021-10-26 11:50:47
latitude:55.87925,longitude:37.54691,destinationhost:samplehost,username:Test,sourcehost:87.251.67.98,state:null,country:Russia,label:Russia - 87.251.67.98,timestamp:2021-10-26 12:13:45
latitude:52.37018,longitude:4.87324,destinationhost:samplehost,username:AZUREUSER,sourcehost:20.86.161.127,state:North Holland,country:Netherlands,label:Netherlands - 20.86.161.127,timestamp:2021-10-26 12:33:46
latitude:17.49163,longitude:-88.18704,destinationhost:samplehost,username:Test,sourcehost:45.227.254.8,state:null,country:Belize,label:Belize - 45.227.254.8,timestamp:2021-10-26 13:13:25
latitude:-55.88802,longitude:37.65136,destinationhost:samplehost,username:Test,sourcehost:94.232.47.130,state:Central Federal District,country:Russia,label:Russia - 94.232.47.130,timestamp:2021-10-26 14:25:33
latitude:19.21184,longitude:73.13254,destinationhost:honeypotvm,username:azureuser,sourcehost:103.179.3.195,state:Maharashtra, country:India,label:India - 103.179.3.195,timestamp:2023-10-14 15:49:30
```

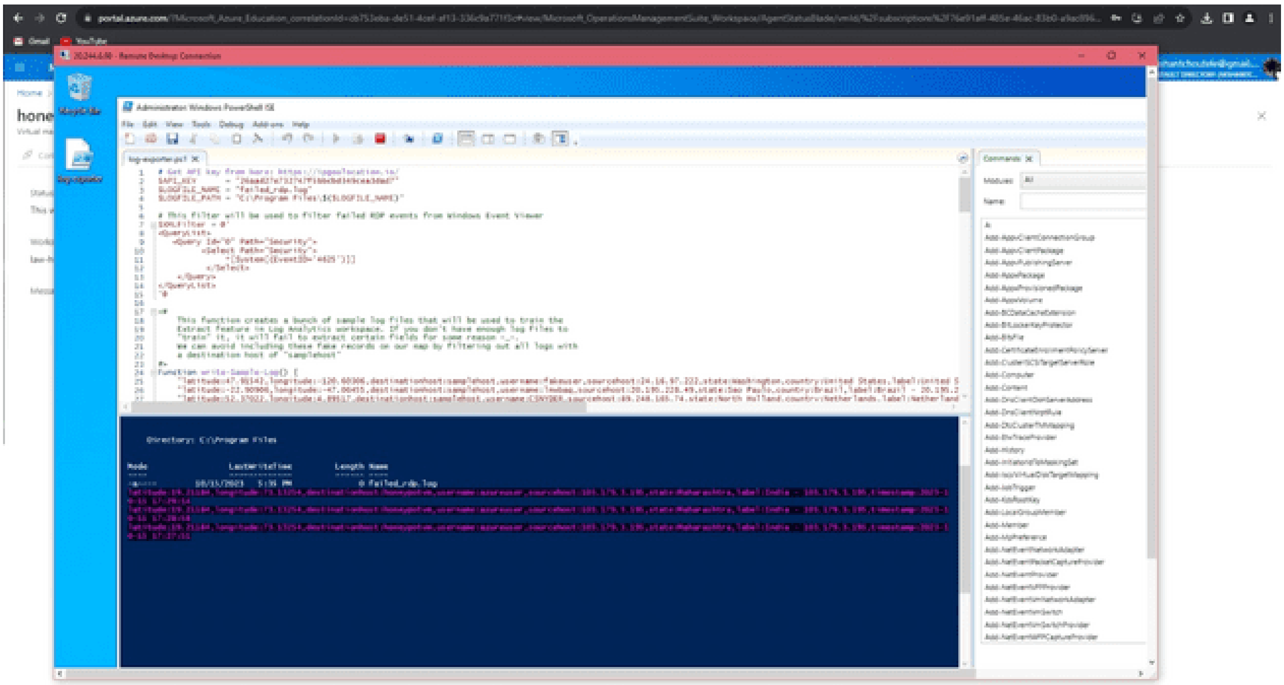
This is the data that is actual failed logon dummy attack we did



```
latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washington,country:United States,label:United States - 24.16.97.222,timestamp:2021-10-26 03:28:29
latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country:Brazil,label:Brazil - 20.195.228.49,timestamp:2021-10-26 05:46:20
latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:North Holland,country:Netherlands,label:Netherlands - 89.248.165.74,timestamp:2021-10-26 06:12:56
latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.247.218,state:New York,country:United States,label:United States - 72.45.247.218,timestamp:2021-10-26 10:44:07
latitude:33.99762,longitude:-6.84737,destinationhost:samplehost,username:AZUREUSER,sourcehost:102.50.242.216,state:Rabat-Salé-Kénitra,country:Morocco,label:Morocco - 102.50.242.216,timestamp:2021-10-26 11:03:13
latitude:-5.32558,longitude:100.28595,destinationhost:samplehost,username:Test,sourcehost:42.1.62.34,state:Penang,country:Malaysia,label:Malaysia - 42.1.62.34,timestamp:2021-10-26 11:04:45
latitude:41.05722,longitude:28.84926,destinationhost:samplehost,username:AZUREUSER,sourcehost:176.235.196.111,state:Istanbul,country:Turkey,label:Turkey - 176.235.196.111,timestamp:2021-10-26 11:50:47
latitude:55.87925,longitude:37.54691,destinationhost:samplehost,username:Test,sourcehost:87.251.67.98,state:null,country:Russia,label:Russia - 87.251.67.98,timestamp:2021-10-26 12:13:45
latitude:52.37018,longitude:4.87324,destinationhost:samplehost,username:AZUREUSER,sourcehost:20.86.161.127,state:North Holland,country:Netherlands,label:Netherlands - 20.86.161.127,timestamp:2021-10-26 12:33:46
latitude:17.49163,longitude:-88.18704,destinationhost:samplehost,username:Test,sourcehost:45.227.254.8,state:null,country:Belize,label:Belize - 45.227.254.8,timestamp:2021-10-26 13:13:25
latitude:-55.88802,longitude:37.65136,destinationhost:samplehost,username:Test,sourcehost:94.232.47.130,state:Central Federal District,country:Russia,label:Russia - 94.232.47.130,timestamp:2021-10-26 14:25:33
latitude:19.21184,longitude:73.13254,destinationhost:honeypotvm,username:azureuser,sourcehost:103.179.3.195,state:Maharashtra, country:India,label:India - 103.179.3.195,timestamp:2023-10-14 15:49:30
```

10.Run Script To get Geo Data from attackers

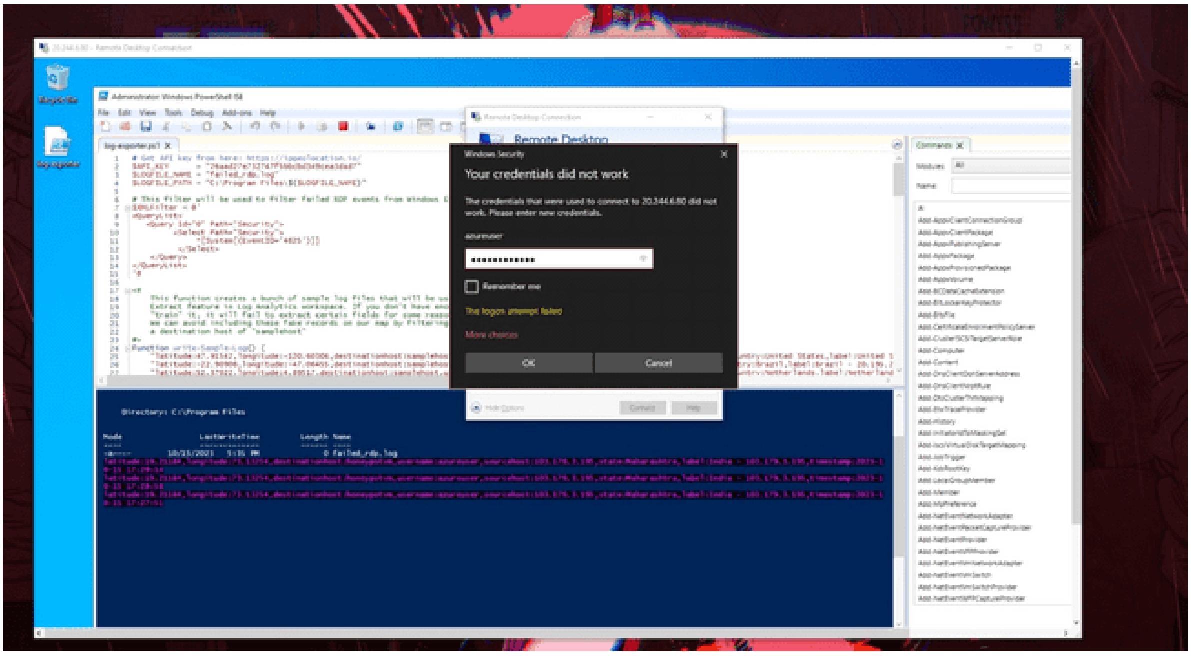
This is how the data looks in powershell after multiple dummy attacks.


20.244.6.80 - Remote Desktop Connection
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
log-exporter.ps1
Commands
Modules: All
Name:

```
# Get API key from here: https://ipgeolocation.io/
$API_KEY      = "26aad27e73274ff5b6cbd349cea3dad7"
$LOGFILE_NAME = "failed_rdp.log"
$LOGFILE_PATH = "C:\Program Files\$($LOGFILE_NAME)"

# This filter will be used to filter failed RDP events from Windows Event Viewer
$XMLFilter = @'
<QueryList>
   <Query Id="0" Path="Security">
         <Select Path="Security">
              *[System[(EventID='4625')]]
          </Select>
    </Query>
</QueryList>
'@

<#
    This function creates a bunch of sample log files that will be used to train the
    Extract feature in Log Analytics workspace. If you don't have enough log files to
    "train" it, it will fail to extract certain fields for some reason -_-.
    We can avoid including these fake records on our map by filtering out all logs with
    a destination host of "samplehost"
#>
Function write-Sample-Log() {
    "latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washington,country:United States,label:United S
    "latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country:Brazil,label:Brazil - 20.195.2
    "latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:North Holland,country:Netherlands,label:Netherland
```

```
    Directory: C:\Program Files


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/15/2023   5:35 PM              0 failed_rdp.log
latitude:19.21184,longitude:73.13254,destinationhost:honeypotvm,username:azureuser,sourcehost:103.179.3.195,state:Maharashtra,label:India - 103.179.3.195,timestamp:2023-1
0-15 17:29:14
latitude:19.21184,longitude:73.13254,destinationhost:honeypotvm,username:azureuser,sourcehost:103.179.3.195,state:Maharashtra,label:India - 103.179.3.195,timestamp:2023-1
0-15 17:28:58
latitude:19.21184,longitude:73.13254,destinationhost:honeypotvm,username:azureuser,sourcehost:103.179.3.195,state:Maharashtra,label:India - 103.179.3.195,timestamp:2023-1
0-15 17:27:51
```

Logging into the virtual machine entering a wrong password aka dummy brutforce attack.


20.244.6.80 - Remote Desktop Connection
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
log-exporter.ps1
Remote Desktop Connection
Remote Desktop
Windows Security
Hide Options
Connect
Help
Commands
Modules: All

Your credentials did not work

The credentials that were used to connect to 20.244.6.80 did not work. Please enter new credentials.

azureuser

●●●●●●●●●●●●●

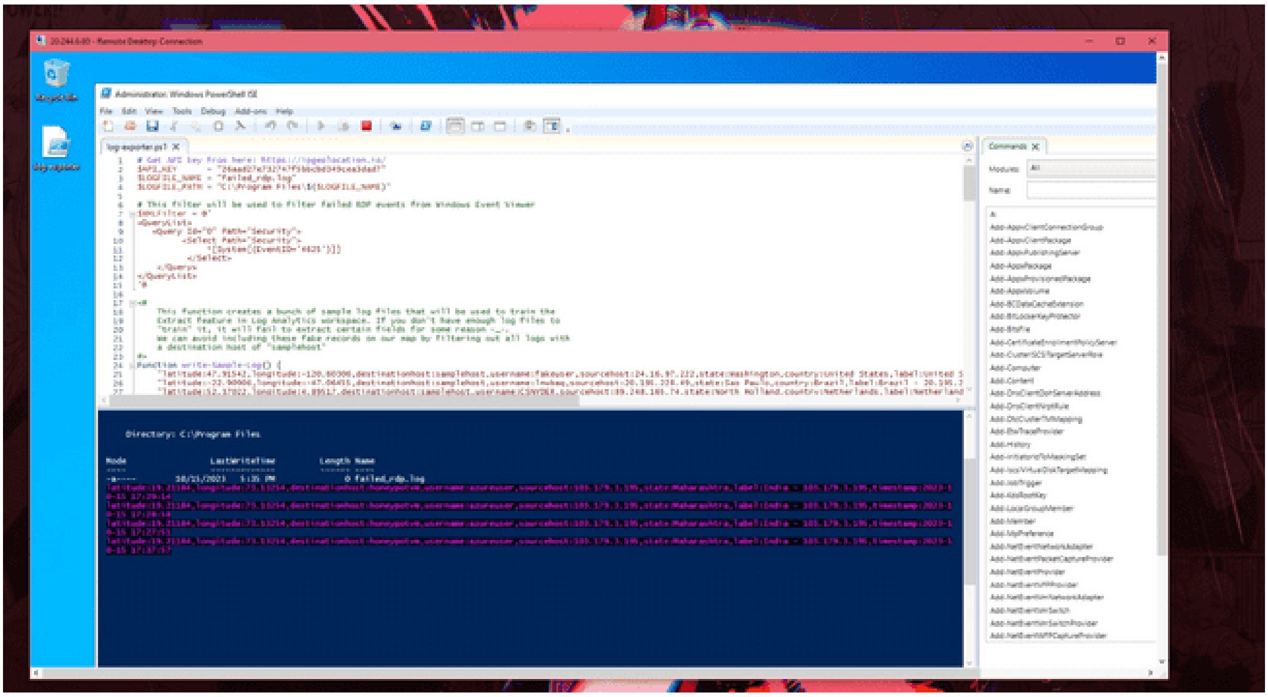
□ Remember me

The logon attempt failed

More choices

OK | Cancel

LOGIN gets failed and it shows the data with an exact time and location from when it was done.

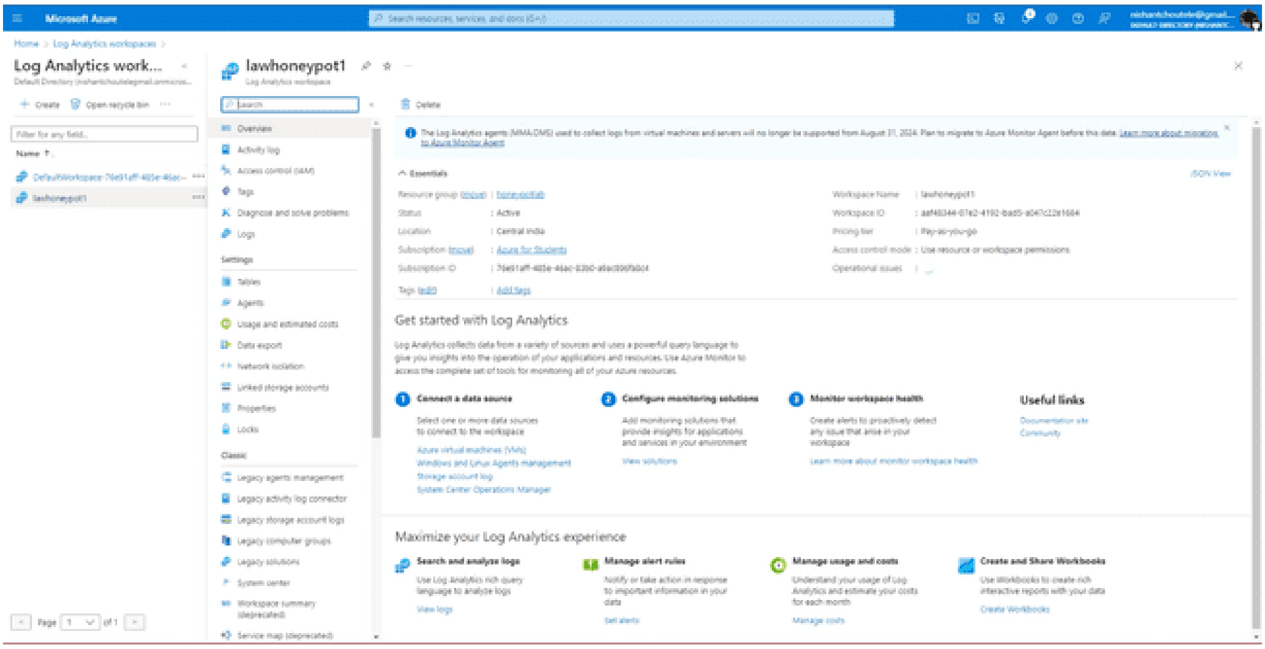


```
# Get API key from here: https://ipgeolocation.io/
$API_KEY      = "26aad27e73274 7f5bbcbd349cea3dad7"
$LOGFILE_NAME = "failed_rdp.log"
$LOGFILE_PATH = "C:\Program Files\$($LOGFILE_NAME)"

# This filter will be used to filter failed RDP events from Windows Event Viewer
$XMLFilter = @'
<QueryList>
   <Query Id="0" Path="Security">
         <Select Path="Security">
              *[System[(EventID='4625')]]
          </Select>
    </Query>
</QueryList>
'@

<#
    This function creates a bunch of sample log files that will be used to train the
    Extract feature in Log Analytics workspace. If you don't have enough log files to
    "train" it, it will fail to extract certain fields for some reason -_-.
    We can avoid including these fake records on our map by filtering out all logs with
    a destination host of "samplehost"
#>
Function write-Sample-Log() {
    "latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washington,country:United States,label:United S
    "latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country:Brazil,label:Brazil - 20.195.2
    "latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:North Holland,country:Netherlands,label:Netherland
```

```
    Directory: C:\Program Files


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/15/2023   5:35 PM              0 failed_rdp.log
latitude:19.21184,longitude:73.13214,destinationhost:honeypotvm,username:azureuser,sourcehost:103.179.1.195,state:Maharashtra,label:India - 103.179.1.195,timestamp:2023-1
0-15 17:26:14
latitude:19.21184,longitude:73.13214,destinationhost:honeypotvm,username:azureuser,sourcehost:103.179.1.195,state:Maharashtra,label:India - 103.179.1.195,timestamp:2023-1
0-15 17:26:14
latitude:19.21184,longitude:73.13214,destinationhost:honeypotvm,username:azureuser,sourcehost:103.179.1.195,state:Maharashtra,label:India - 103.179.1.195,timestamp:2023-1
0-15 17:27:51
latitude:19.21184,longitude:73.13214,destinationhost:honeypotvm,username:azureuser,sourcehost:103.179.1.195,state:Maharashtra,label:India - 103.179.1.195,timestamp:2023-1
0-15 17:37:57
```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
log-exporter.ps1
Commands
Modules: All
Name:
Add-AppvClientConnectionGroup
Add-AppvClientPackage
Add-AppvPublishingServer
Add-AppxPackage
Add-AppxProvisionedPackage
Add-AppxVolume
Add-BCDataCacheExtension
Add-BitLockerKeyProtector
Add-BitsFile
Add-CertificateEnrollmentPolicyServer
Add-ClusterSCSITargetServerRole
Add-Computer
Add-Content
Add-DnsClientDohServerAddress
Add-DnsClientNrptRule
Add-DtcClusterTMMapping
Add-EtwTraceProvider
Add-History
Add-InitiatorIdToMaskingSet
Add-IscsiVirtualDiskTargetMapping
Add-JobTrigger
Add-KdsRootKey
Add-LocalGroupMember
Add-Member
Add-MpPreference
Add-NetEventNetworkAdapter
Add-NetEventPacketCaptureProvider
Add-NetEventProvider
Add-NetEventVFPProvider
Add-NetEventVmNetworkAdapter
Add-NetEventVmSwitch
Add-NetEventVmSwitchProvider
Add-NetEventWFPCaptureProvider

Now go to log analytics workspace> overview> tables



Home > Log Analytics workspaces >

Log Analytics work...

lawhoneypot1

Log Analytics workspace

The Log Analytics agents (MMA/OMS) used to collect logs from virtual machines and servers will no longer be supported from August 31, 2024. Plan to migrate to Azure Monitor Agent before this date. Learn more about migrating to Azure Monitor Agent

Essentials

Resource group (move) : honeypotlab
Status : Active
Location : Central India
Subscription (move) : Azure for Students
Subscription ID : 76e91aff-485e-46ac-83b0-a6ac8b6fd6d4
Tags (edit) : Add tags

Workspace Name : lawhoneypot1
Workspace ID : aaf48344-07e2-4192-bad5-a047c22e1684
Pricing tier : Pay-as-you-go
Access control mode : Use resource or workspace permissions
Operational issues :

Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

1 Connect a data source
Select one or more data sources to connect to the workspace
Azure virtual machines (VMs)
Windows and Linux Agents management
Storage account logs
System Center Operations Manager

2 Configure monitoring solutions
Add monitoring solutions that provide insights for applications and services in your environment
View solutions

3 Monitor workspace health
Create alerts to proactively detect any issue that arise in your workspace
Learn more about monitor workspace health

Useful links
Documentation site
Community

Maximize your Log Analytics experience

Search and analyze logs
Use Log Analytics rich query language to analyze logs
View logs

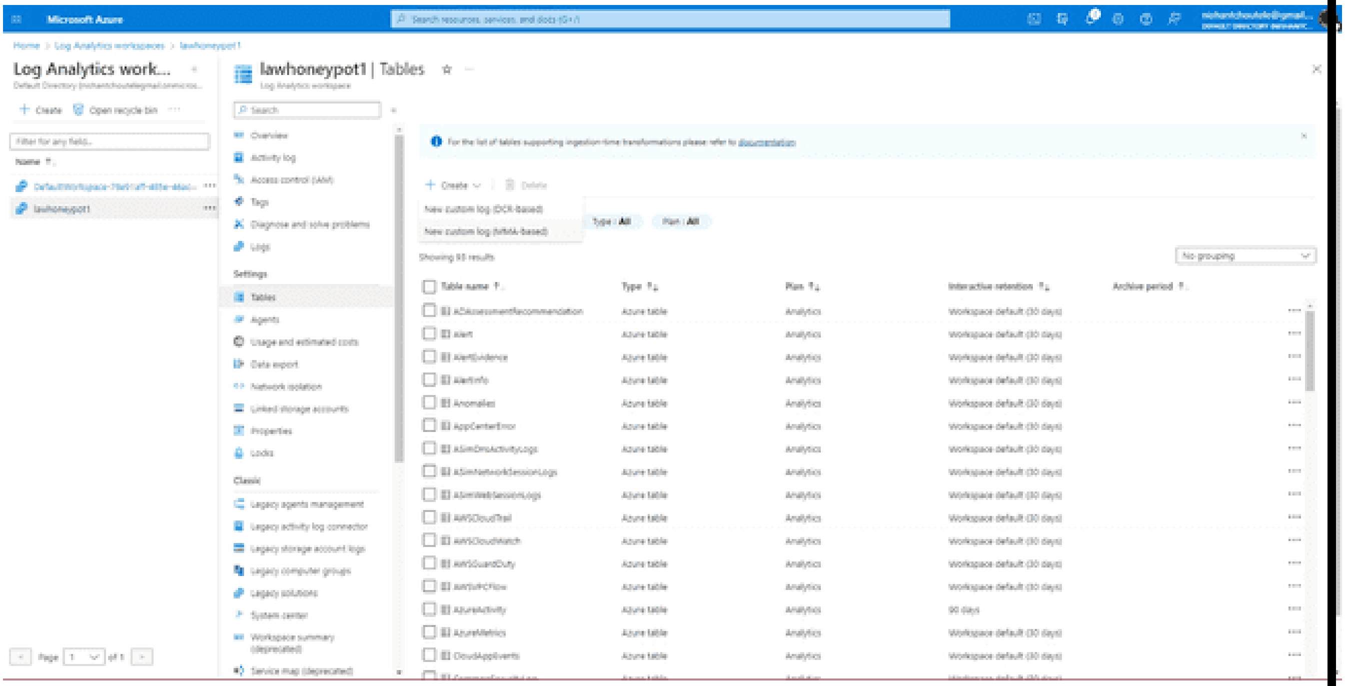
Manage alert rules
Notify or take action in response to important information in your data
Set alerts

Manage usage and costs
Understand your usage of Log Analytics and estimate your costs for each month
Manage costs

Create and Share Workbooks
Use Workbooks to create rich interactive reports with your data
Create Workbooks

11.Create custom log in LAW to bring in our custom log

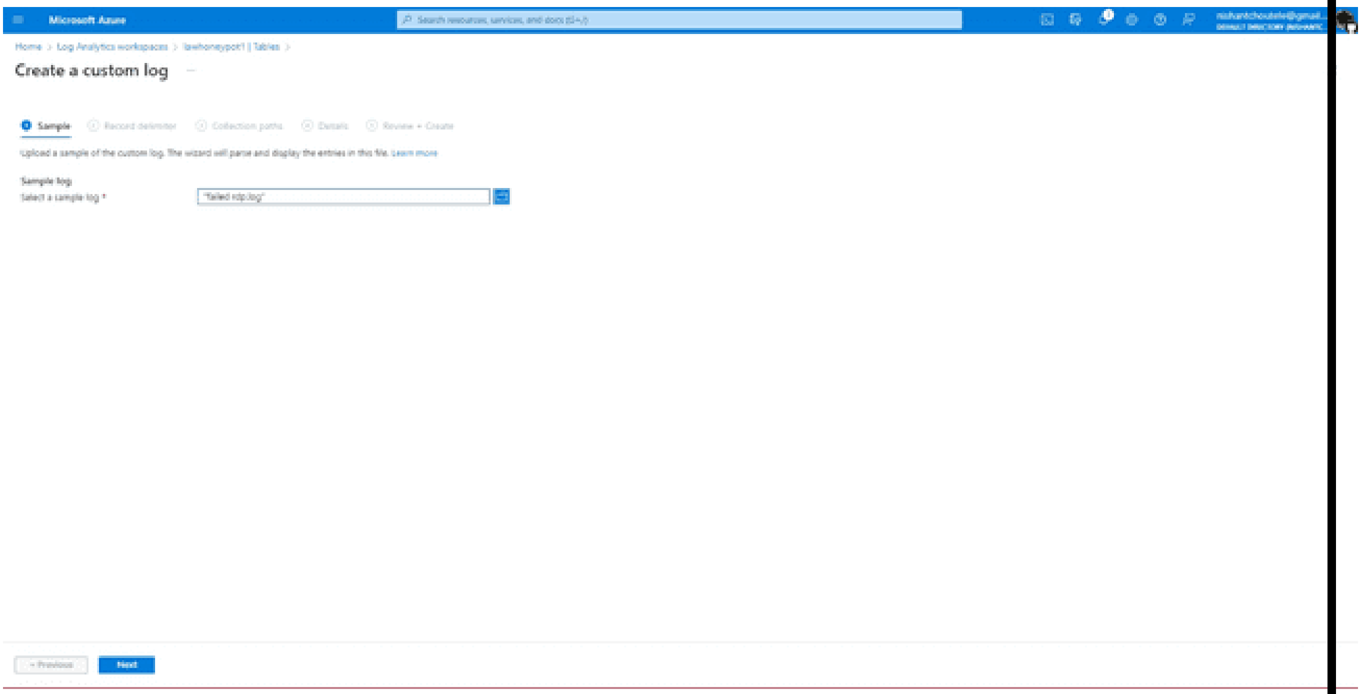
Create> new custom log MMA based.



Showing 93 results

Table name	Type	Plan	Interactive retention	Archive period
ADAssessmentRecommendation	Azure table	Analytics	Workspace default (30 days)	
Alert	Azure table	Analytics	Workspace default (30 days)	
AlertEvidence	Azure table	Analytics	Workspace default (30 days)	
AlertInfo	Azure table	Analytics	Workspace default (30 days)	
Anomalies	Azure table	Analytics	Workspace default (30 days)	
AppCenterError	Azure table	Analytics	Workspace default (30 days)	
ASimDnsActivityLogs	Azure table	Analytics	Workspace default (30 days)	
ASimNetworkSessionLogs	Azure table	Analytics	Workspace default (30 days)	
ASimWebSessionLogs	Azure table	Analytics	Workspace default (30 days)	
AWSCloudTrail	Azure table	Analytics	Workspace default (30 days)	
AWSCloudWatch	Azure table	Analytics	Workspace default (30 days)	
AWSGuardDuty	Azure table	Analytics	Workspace default (30 days)	
AWSVPCFlow	Azure table	Analytics	Workspace default (30 days)	
AzureActivity	Azure table	Analytics	90 days	
AzureMetrics	Azure table	Analytics	Workspace default (30 days)	
CloudAppEvents	Azure table	Analytics	Workspace default (30 days)	

Give the path of the file which collects the geo data>next



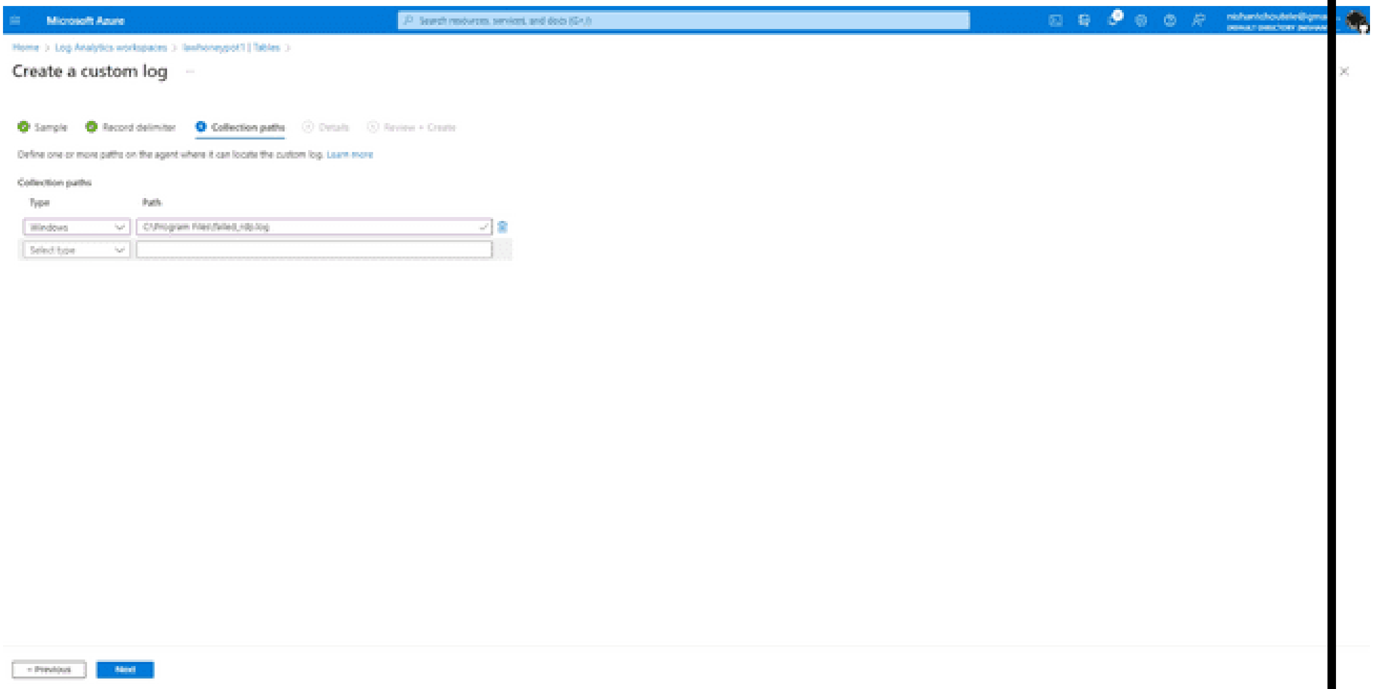
Create a custom log

Upload a sample of the custom log. The wizard will parse and display the entries in this file. Learn more

Sample log

Select a sample log * "failed rdp.log"

Copy the path of the failed RDP file and paste it



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Log Analytics workspaces > lawhoneypot1 | Tables >

Create a custom log

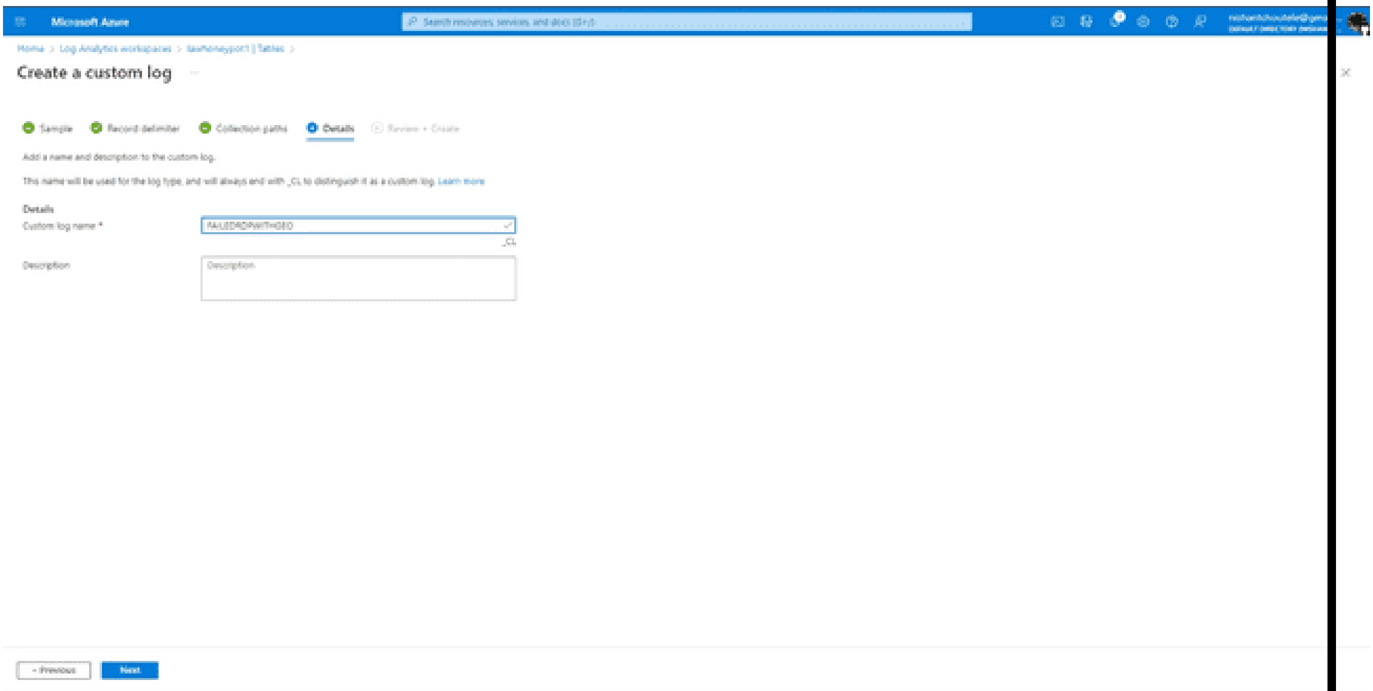
Sample
Record delimiter
Collection paths
Details
Review + Create

Define one or more paths on the agent where it can locate the custom log. Learn more

Collection paths

Type	Path
Windows	C:\Program Files\failed_rdp.log
Select type	

Give the custom log a name and create.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Log Analytics workspaces > lawhoneypot1 | Tables >

Create a custom log

Sample
Record delimiter
Collection paths
Details
Review + Create

Add a name and description to the custom log.

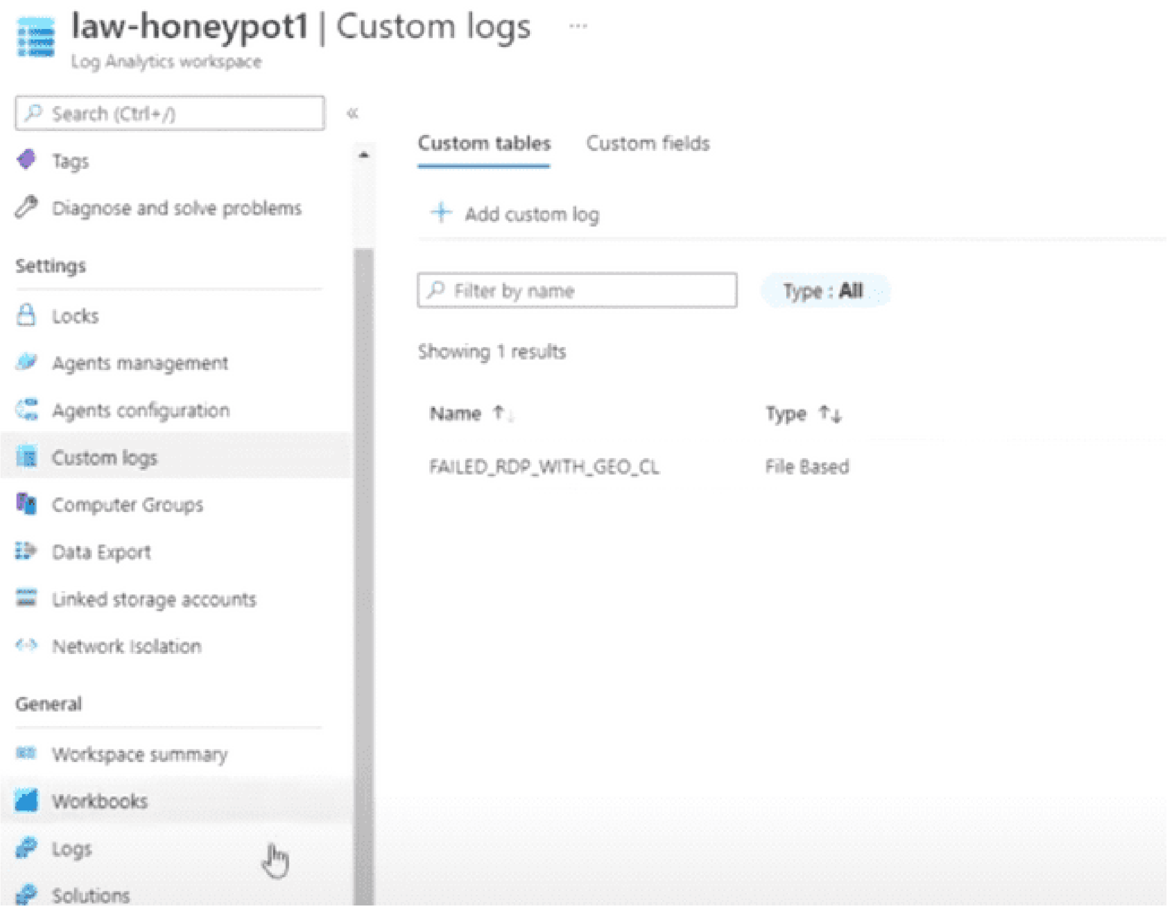
This name will be used for the log type, and will always end with _CL to distinguish it as a custom log. Learn more

Details

Custom log name * FAILEDRDPWITHGEO _CL

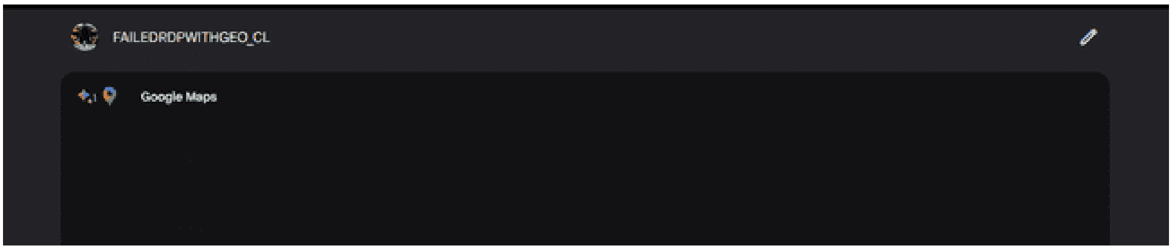
Description

Go to the workbook it will show the log file named FAILED RDP WITH GEO CL (CL stands for custom logs)



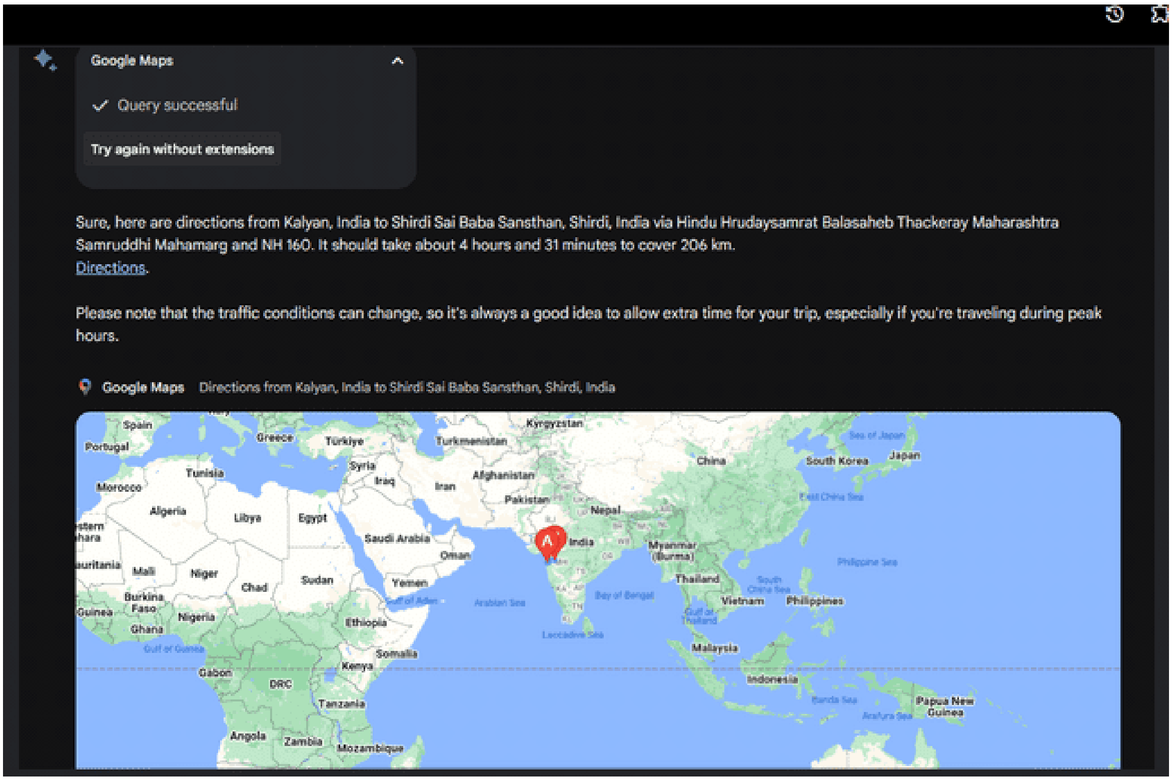
Name	Type
FAILED_RDP_WITH_GEO_CL	File Based

Copy the file name and paste it in bard



FAILEDRDPWITHGEO_CL

Bard will take the file name as a query and show the live location of the attackers.



Sure, here are directions from Kalyan, India to Shirdi Sai Baba Sansthan, Shirdi, India via Hindu Hrudaysamrat Balasaheb Thackeray Maharashtra Samruddhi Mahamarg and NH 160. It should take about 4 hours and 31 minutes to cover 206 km.
Directions.

Please note that the traffic conditions can change, so it's always a good idea to allow extra time for your trip, especially if you're traveling during peak hours.

Google Maps Directions from Kalyan, India to Shirdi Sai Baba Sansthan, Shirdi, India

Thank you!!!