Project 2: SIEM in Azure (a Security Analyst Skill)

Overview: A honeypot VM is created with Microsoft Azure and RDP failed logon attempts are logged using PowerShell and an IP-to-Geolocation API. With the logs a map is generated that depicts all attackers locations using Kusto Query Language (KUSTO).

Developed content for and performed the following tasks:

- Used custom PowerShell script to extract metadata from Windows Event Viewer to be forwarded to third party API in order to derive geolocation data
- Configured Log Analytics Workspace in Azure to ingest custom logs containing geographic data (latitude, longitude, state/province, and country)
- Configured Custom Fields in Logs Analytics Workspace with the intent of mapping geodata in Azure Sentinel
- Configured Azure Sentinel (Microsoft's cloud SIEM) workbook to display global attack data (RDP brute force) on a world map according to physical location and magnitude of attacks

Step 1: Setup a Virtual Machine on Microsoft Azure

Step 2: Create a Log Analytics Workspace

Step 3: Setup Microsoft Defender for Cloud

Step 4: Connect Log Analytics Workspace to VM

Step 5: Add Azure Sentinel to the Log Analytics Workspace

Step 6: Fail First Remote Desktop Connection to Virtual Machine

Step 7: Viewing Failed Logon Attempts on Windows Event Viewer

Step 8: Disable Windows Firewall to Allow ICMP Echo Requests Through

Step 9: Verify ICMP Echo Requests/Ping Request are Being Received

Step 10: Use PowerShell Script with API Key to Get Geolocation Data

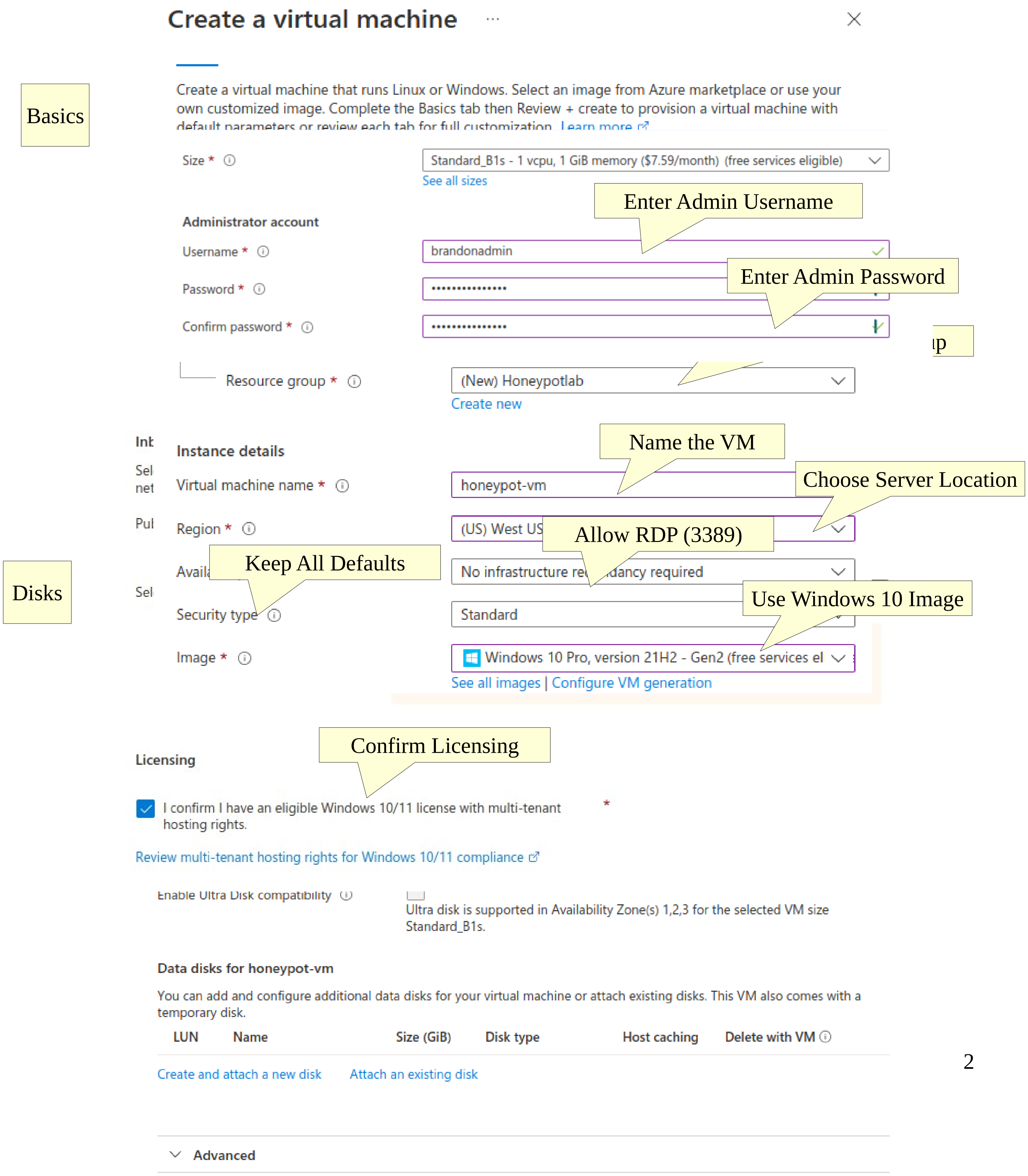
Step 11: Create Custom Log in Log Analytics Workspace

Step 12: Train the Data Algorithm to Use Appropriate Field

Step 13: Ingest Logs into Azure Sentinel and Create a World Map

Step 14: Final Results

Setup a Virtual Machine on Microsoft Azure



Create a virtual machine

Basics

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

Size * : Standard_B1s - 1 vcpu, 1 GiB memory ($7.59/month) (free services eligible)

See all sizes

Enter Admin Username

Administrator account

Username * : brandonadmin

Password * : •••••••••••••••

Enter Admin Password

Confirm password * : •••••••••••••••

Resource group * : (New) Honeypotlab

Create new

Instance details

Name the VM

Virtual machine name * : honeypot-vm

Choose Server Location

Region * : (US) West US

Allow RDP (3389)

Keep All Defaults

Availability options: No infrastructure redundancy required

Security type: Standard

Use Windows 10 Image

Image * : Windows 10 Pro, version 21H2 - Gen2 (free services el

See all images | Configure VM generation

Confirm Licensing

Licensing

☑ I confirm I have an eligible Windows 10/11 license with multi-tenant hosting rights. *

Review multi-tenant hosting rights for Windows 10/11 compliance

Disks

Enable Ultra Disk compatibility □

Ultra disk is supported in Availability Zone(s) 1,2,3 for the selected VM size Standard_B1s.

Data disks for honeypot-vm

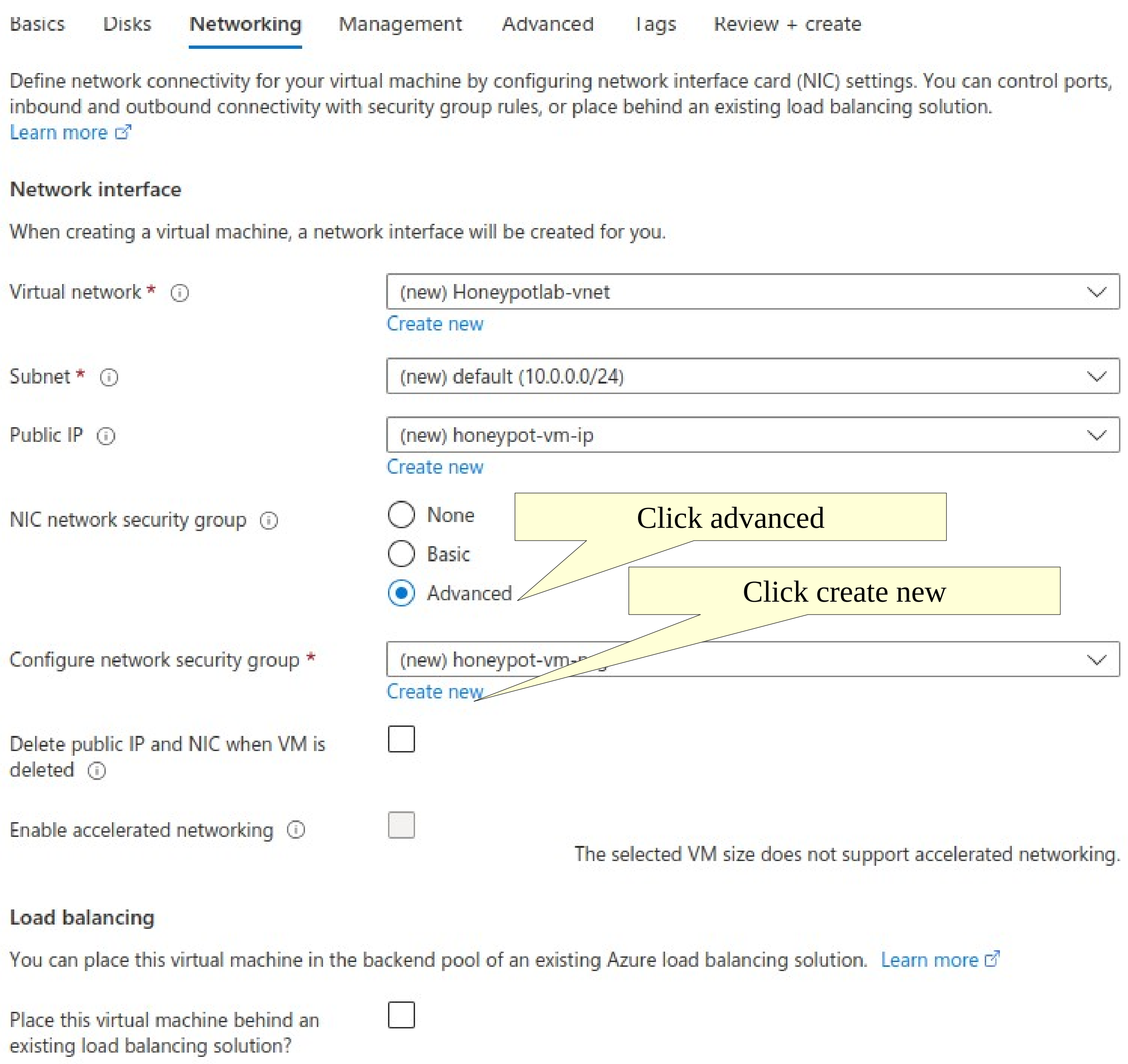
You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM

Create and attach a new disk   Attach an existing disk

Advanced

Networking



Basics | Disks | **Networking** | Management | Advanced | Tags | Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *	(new) Honeypotlab-vnet Create new
Subnet *	(new) default (10.0.0.0/24)
Public IP	(new) honeypot-vm-ip Create new
NIC network security group	○ None ○ Basic ● Advanced
Configure network security group *	(new) honeypot-vm-nsg Create new
Delete public IP and NIC when VM is deleted	□
Enable accelerated networking	□ The selected VM size does not support accelerated networking.

Load balancing

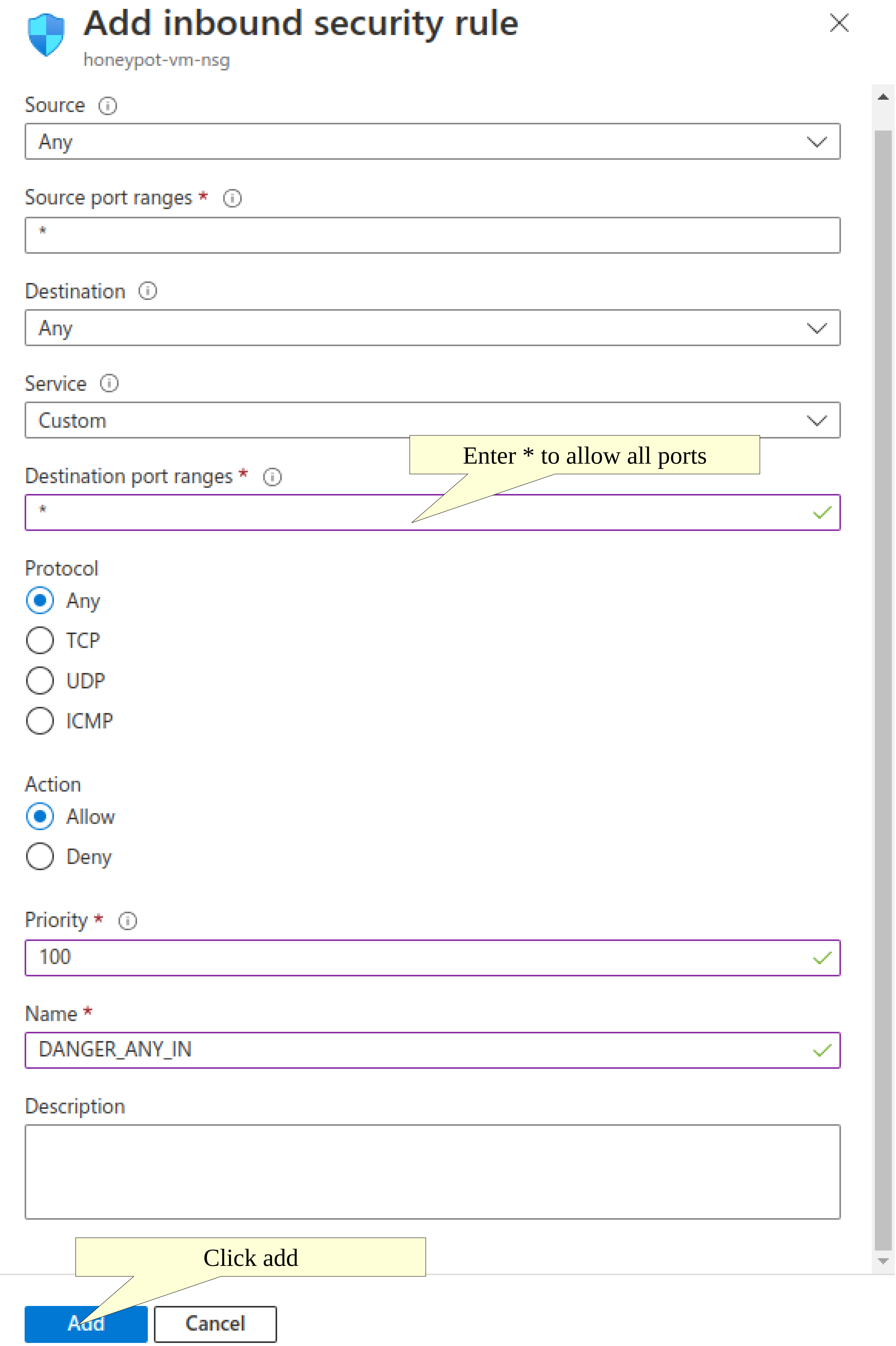
You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Place this virtual machine behind an existing load balancing solution?	□

Click advanced

Click create new

Firewall



Add inbound security rule

honeypot-vm-nsg

Source: Any

Source port ranges *: *

Destination: Any

Service: Custom

Enter * to allow all ports

Destination port ranges *: * ✓

Protocol

● Any

○ TCP

○ UDP

○ ICMP

Action

● Allow

○ Deny

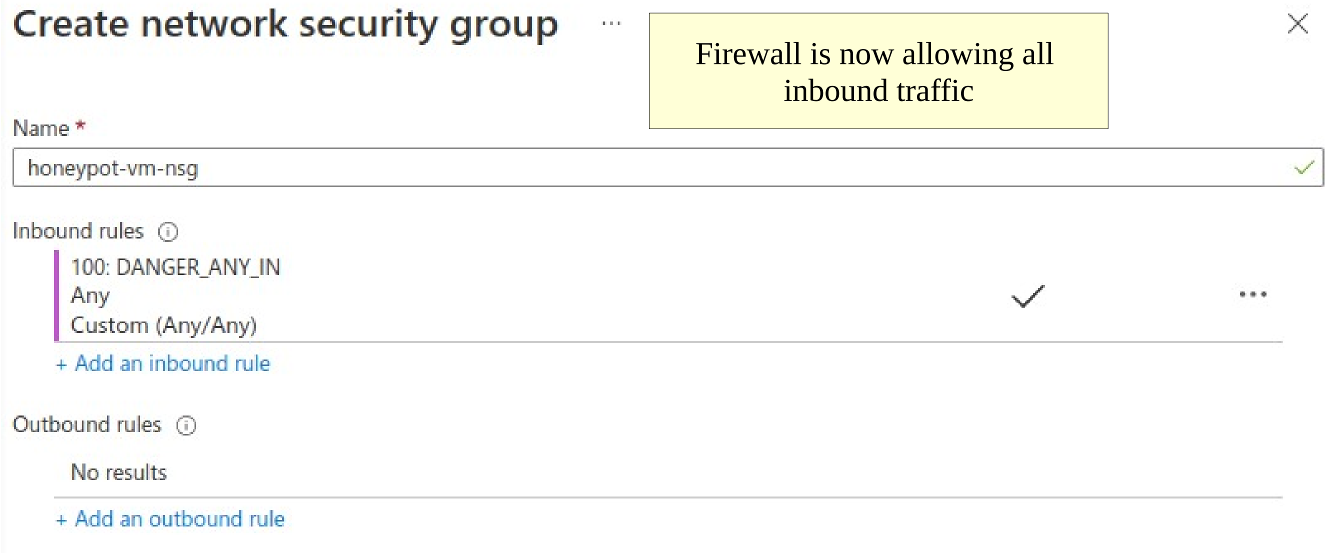
Priority *: 100 ✓

Name *: DANGER_ANY_IN ✓

Description:

Click add

Firewall



Create network security group

Firewall is now allowing all inbound traffic

Name *

honeypot-vm-nsg ✓

Inbound rules ⓘ

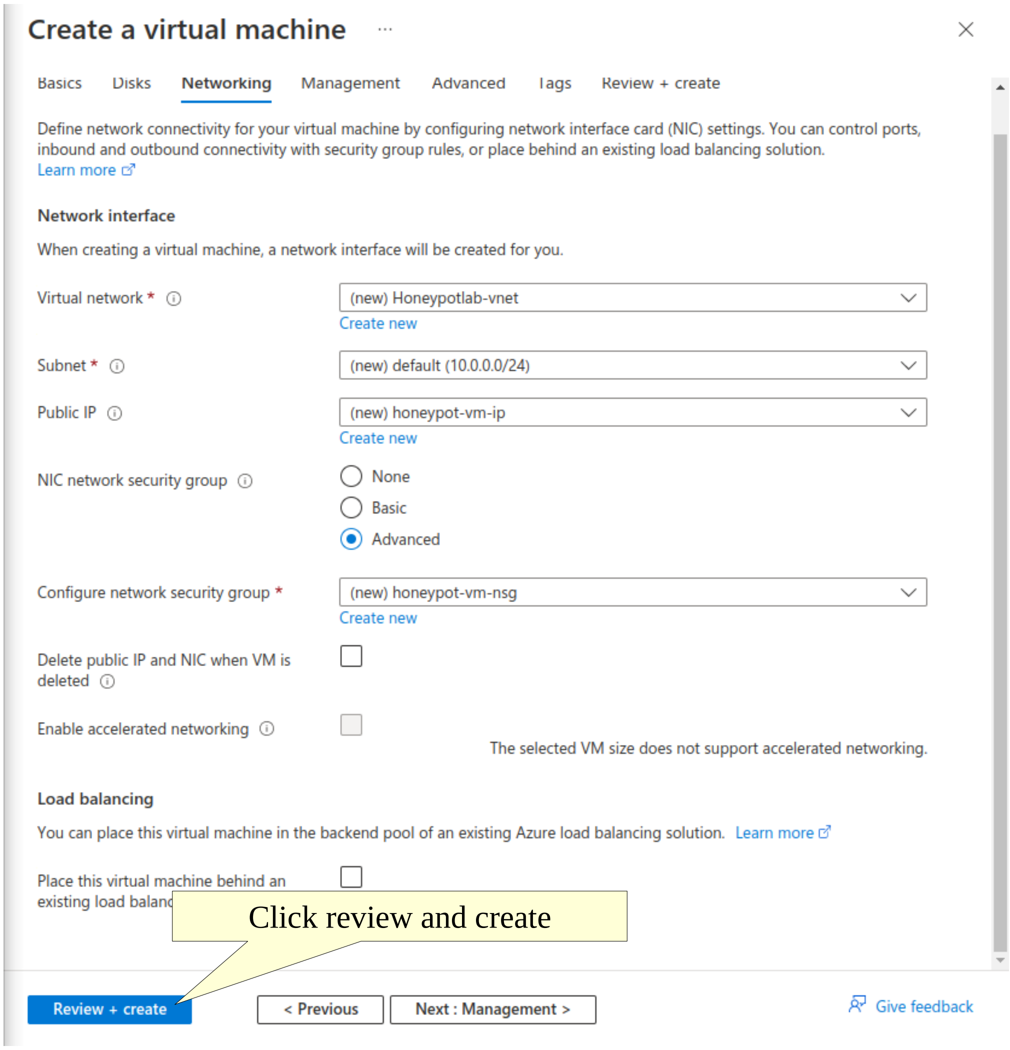
100: DANGER_ANY_IN
Any
Custom (Any/Any) ✓ ...

+ Add an inbound rule

Outbound rules ⓘ

No results

+ Add an outbound rule



Create a virtual machine

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ: (new) Honeypotlab-vnet
Create new

Subnet * ⓘ: (new) default (10.0.0.0/24)

Public IP ⓘ: (new) honeypot-vm-ip
Create new

NIC network security group ⓘ: ○ None ○ Basic ● Advanced

Configure network security group *: (new) honeypot-vm-nsg
Create new

Delete public IP and NIC when VM is deleted ⓘ □

Enable accelerated networking ⓘ □
The selected VM size does not support accelerated networking.

Load balancing

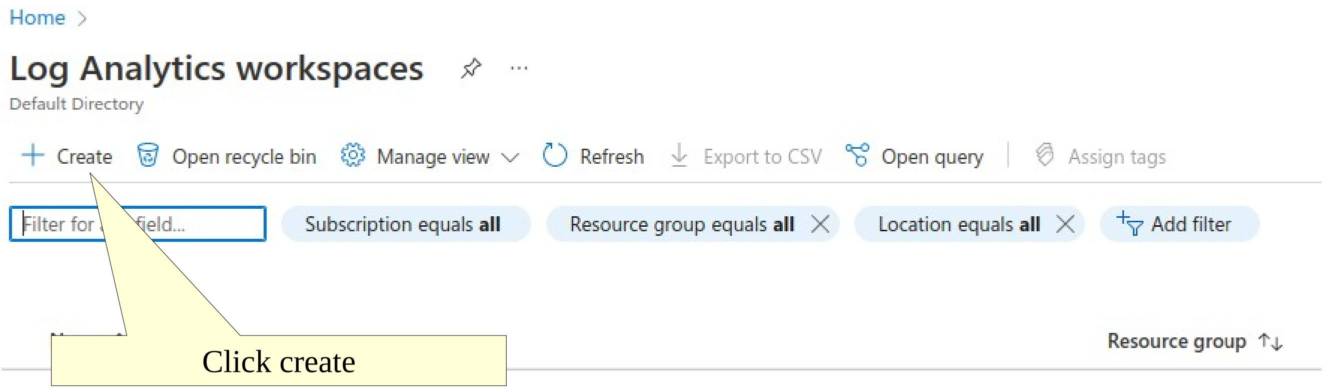
You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Place this virtual machine behind an existing load balanc □

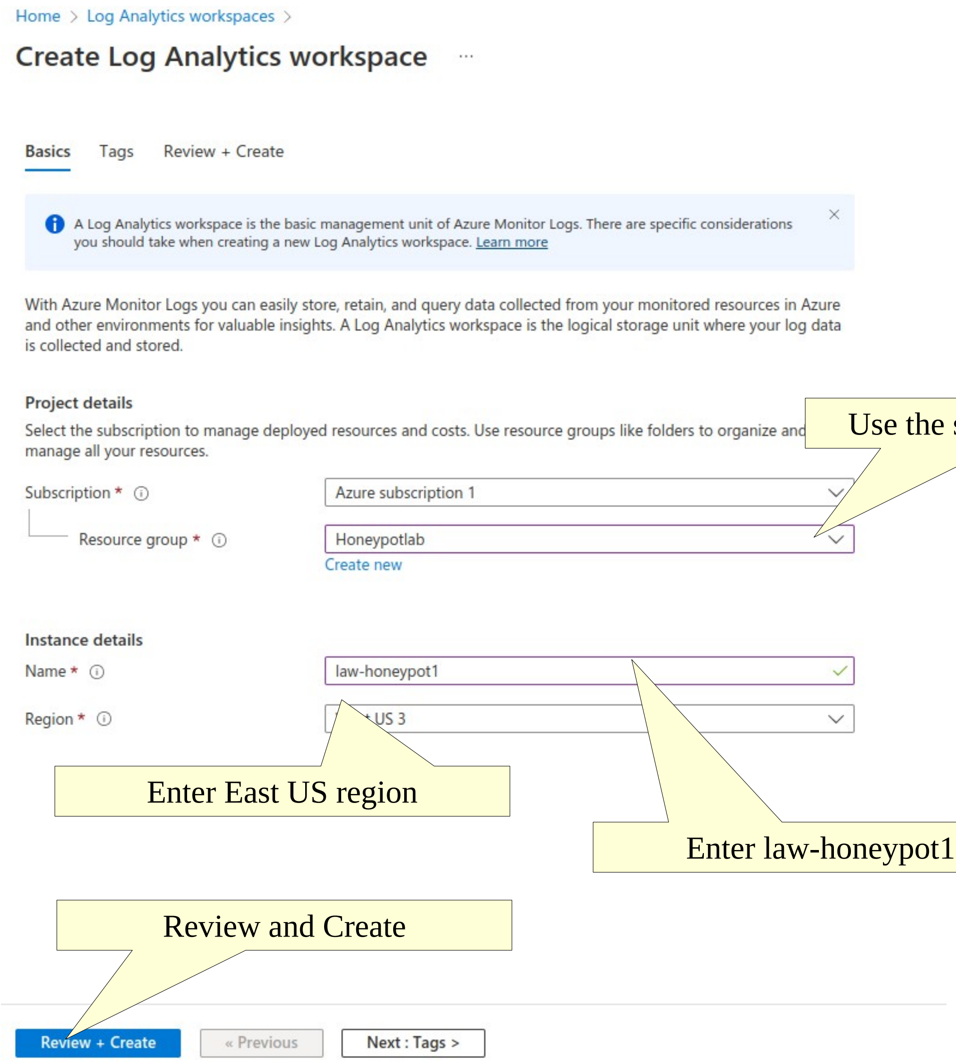
Click review and create

VM is done

Create a Log Analytics Workspace



Click create


Home > Log Analytics workspaces >
Create Log Analytics workspace
Basics
Tags
Review + Create
Review + Create
« Previous
Next : Tags >

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 subscription 1

Resource group * : Honeypotlab

Create new

Instance details

Name * : law-honeypot1

Region * : ... US 3

Use the same resource group

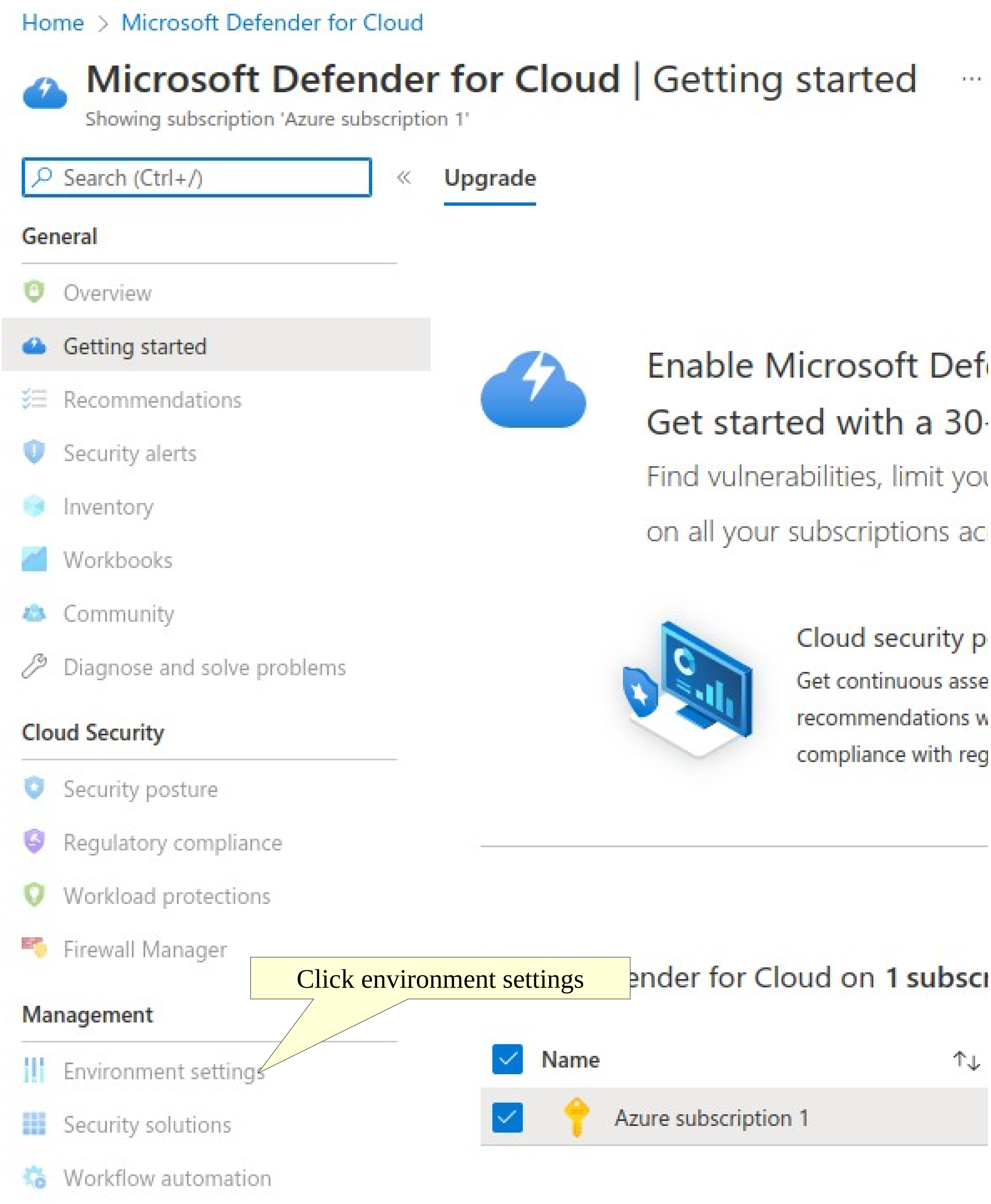
Enter East US region

Enter law-honeypot1

Review and Create

LAW is done

Microsoft Defender for Cloud



Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Getting started ...

Showing subscription 'Azure subscription 1'

Enable Microsoft Def

Get started with a 30

Find vulnerabilities, limit you

on all your subscriptions ac

Cloud security p

Get continuous asse

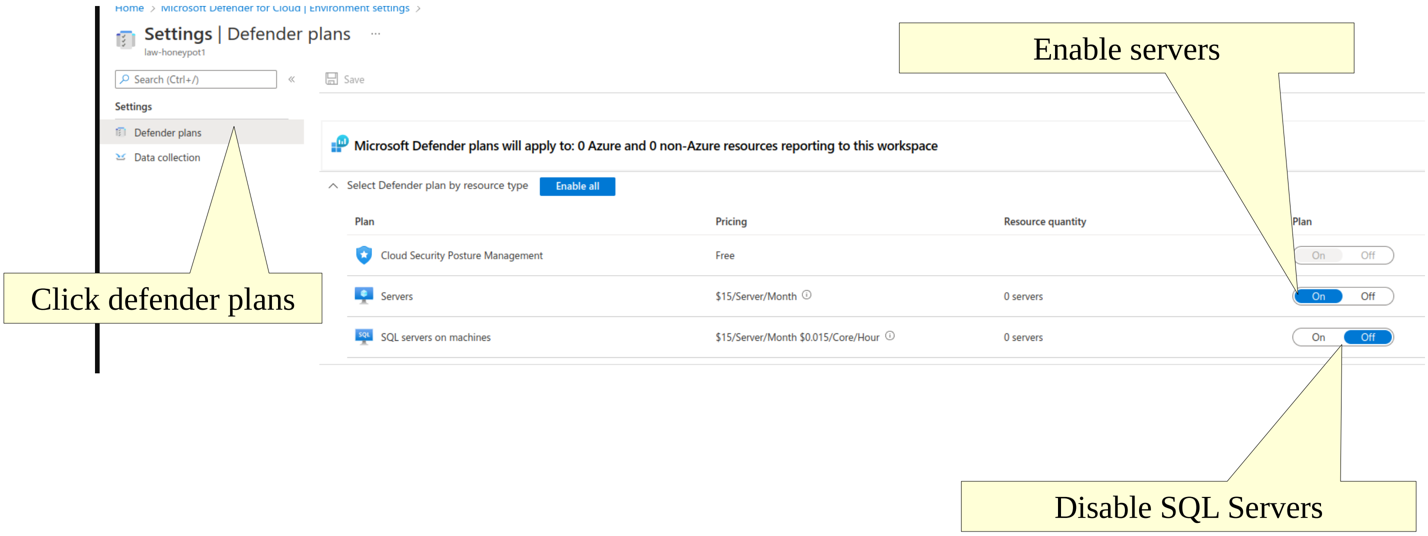
recommendations w

compliance with reg

ender for Cloud on 1 subsc

☑ Name ↑↓
☑ Azure subscription 1

Click environment settings



Home > Microsoft Defender for Cloud | Environment settings >

Settings | Defender plans ...

law-honeypot1

Search (Ctrl+/) « Save

Settings

- Defender plans
- Data collection

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

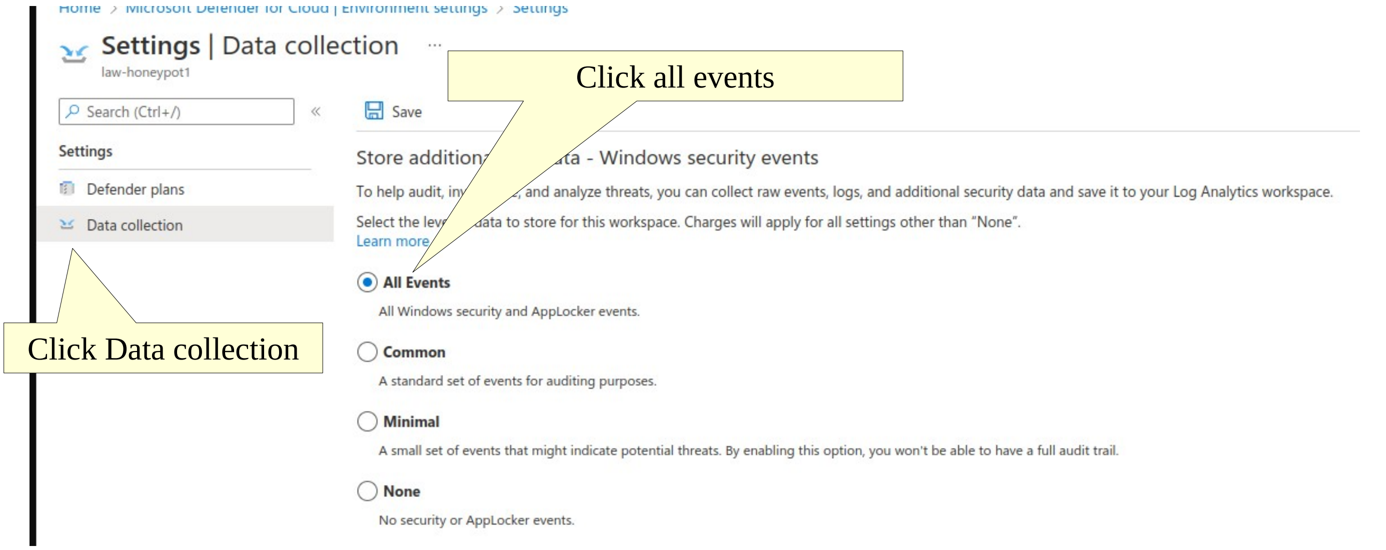
Select Defender plan by resource type Enable all

Plan	Pricing	Resource quantity	Plan
Cloud Security Posture Management	Free		On Off
Servers	$15/Server/Month	0 servers	[✓ On] Off
SQL servers on machines	$15/Server/Month $0.015/Core/Hour	0 servers	On [✓ Off]

Enable servers

Click defender plans

Disable SQL Servers



Home > Microsoft Defender for Cloud | Environment settings > Settings

Settings | Data collection ...

law-honeypot1

Search (Ctrl+/) « Save

Settings

- Defender plans
- Data collection

Store addition ata - Windows security events

To help audit, inv , and analyze threats, you can collect raw events, logs, and additional security data and save it to your Log Analytics workspace.

Select the lev data to store for this workspace. Charges will apply for all settings other than "None".
Learn more

● **All Events**
All Windows security and AppLocker events.

○ **Common**
A standard set of events for auditing purposes.

○ **Minimal**
A small set of events that might indicate potential threats. By enabling this option, you won't be able to have a full audit trail.

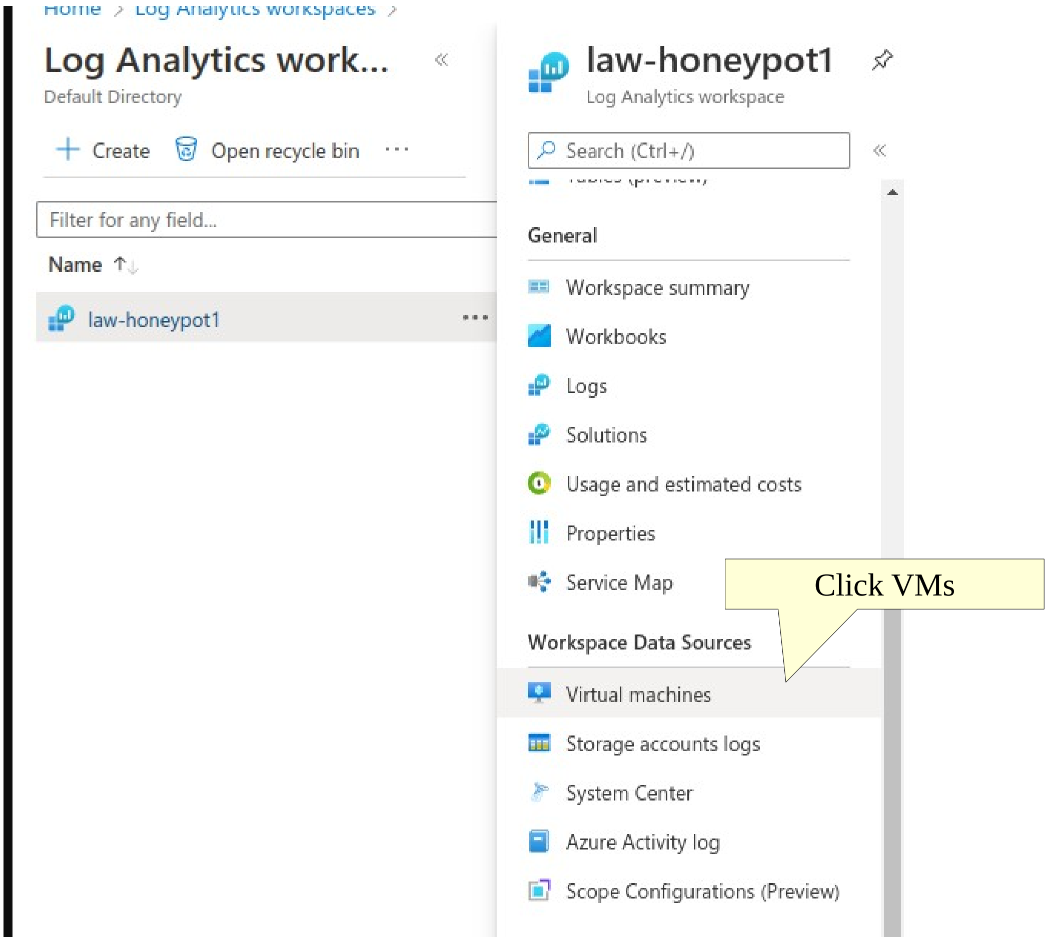
○ **None**
No security or AppLocker events.

Click all events

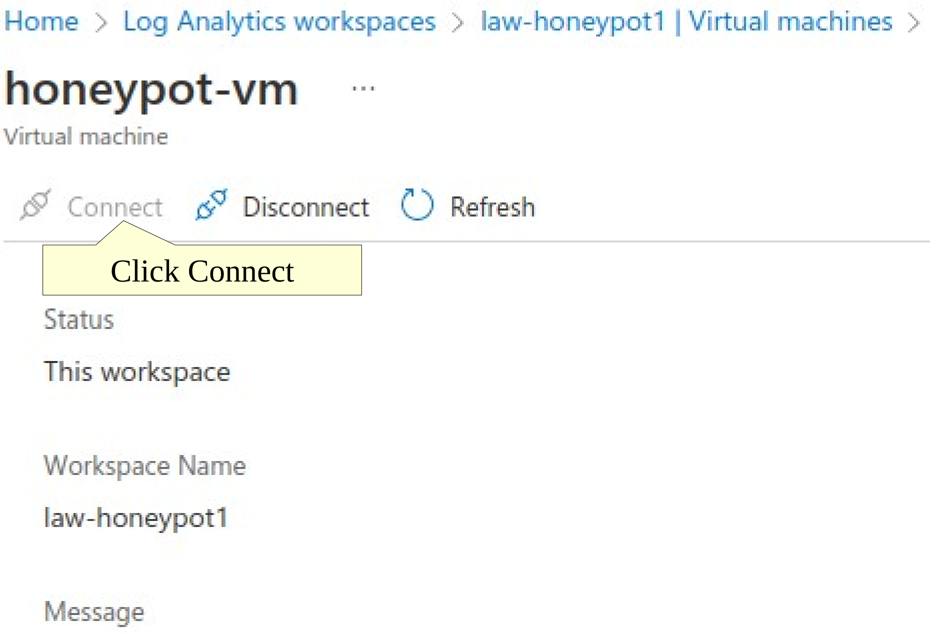
Click Data collection

Microsoft Defender for Cloud is Done

Connect Log Analytics Workspace to VM



Click VMs


Home > Log Analytics workspaces > law-honeypot1 | Virtual machines >
honeypot-vm
Virtual machine
Connect
Disconnect
Refresh

Click Connect

Status

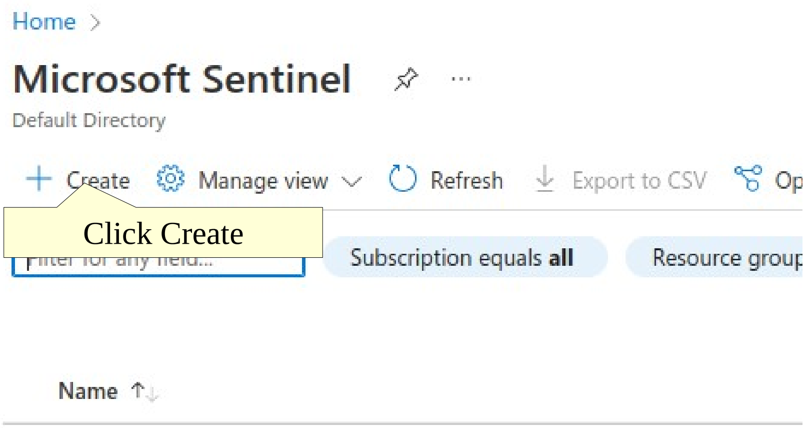
This workspace

Workspace Name

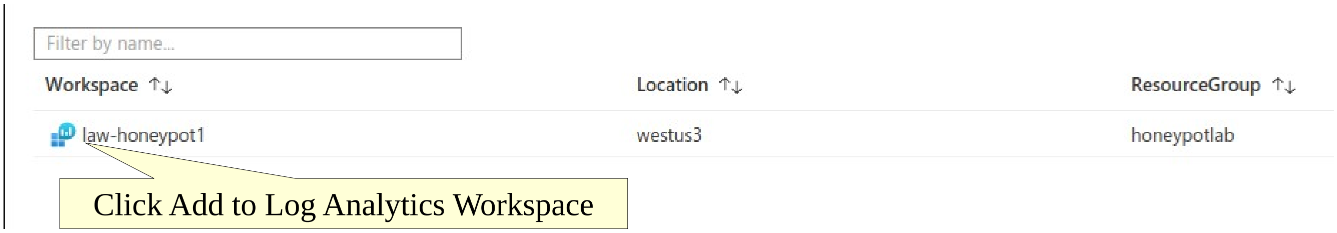
law-honeypot1

Message

Add Azure Sentinel to the Log Analytics Workspace



Click Create

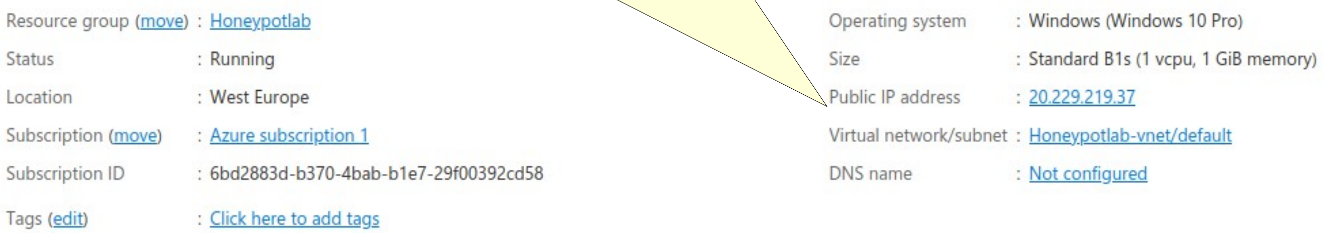


Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓
law-honeypot1	westus3	honeypotlab

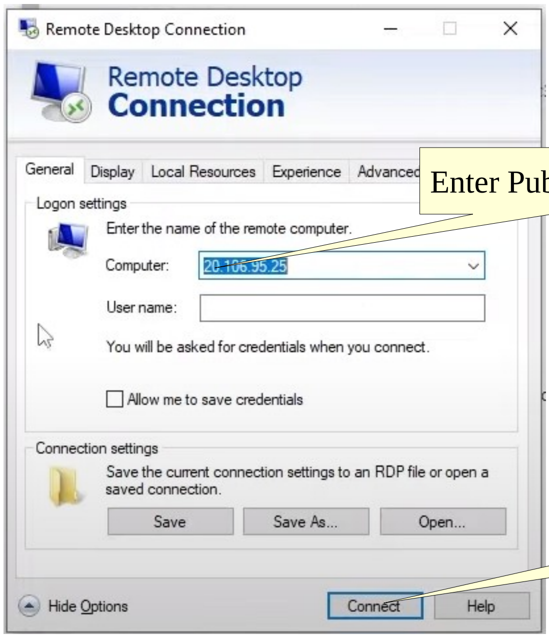
Click Add to Log Analytics Workspace

Fail First Remote Desktop Connection to Virtual Machine
Then Correctly Login

Fail a Remote desktop to VM's IP address



Resource group (move)	: Honeypotlab	Operating system	: Windows (Windows 10 Pro)
Status	: Running	Size	: Standard B1s (1 vcpu, 1 GiB memory)
Location	: West Europe	Public IP address	: 20.229.219.37
Subscription (move)	: Azure subscription 1	Virtual network/subnet	: Honeypotlab-vnet/default
Subscription ID	: 6bd2883d-b370-4bab-b1e7-29f00392cd58	DNS name	: Not configured
Tags (edit)	: Click here to add tags		



Logon settings

Enter the name of the remote computer.

Computer: 20.106.95.25

User name:

You will be asked for credentials when you connect.

☐ Allow me to save credentials

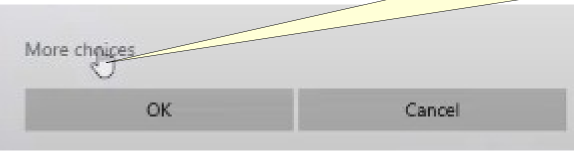
Connection settings

Save the current connection settings to an RDP file or open a saved connection.

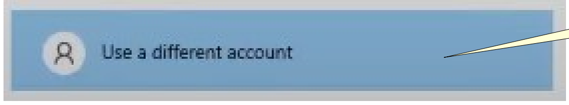
Enter Public IP address

Click connect

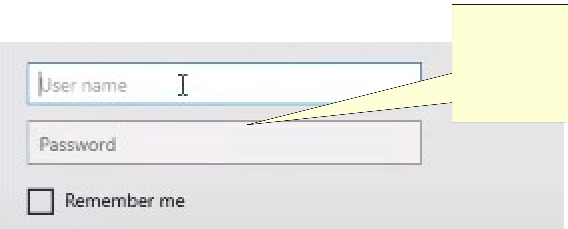
Click more choices



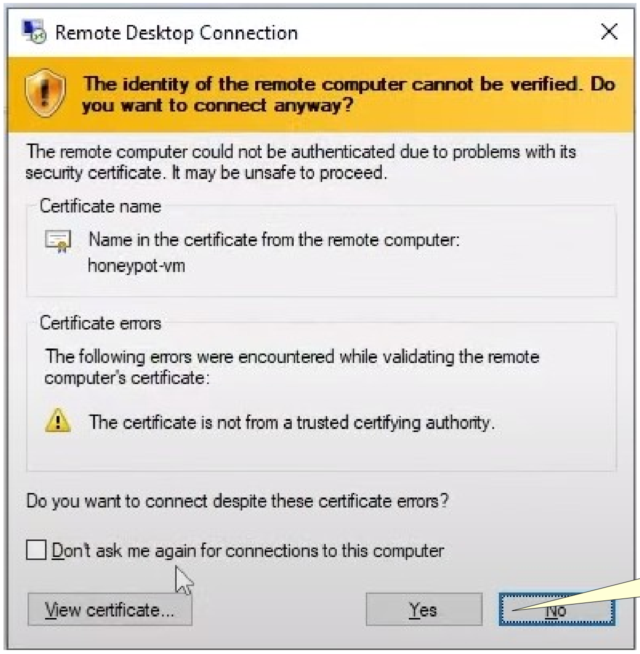
Click use a different account



Fail the first logon
Then correctly login



☐ Remember me



The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
honeypot-vm

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

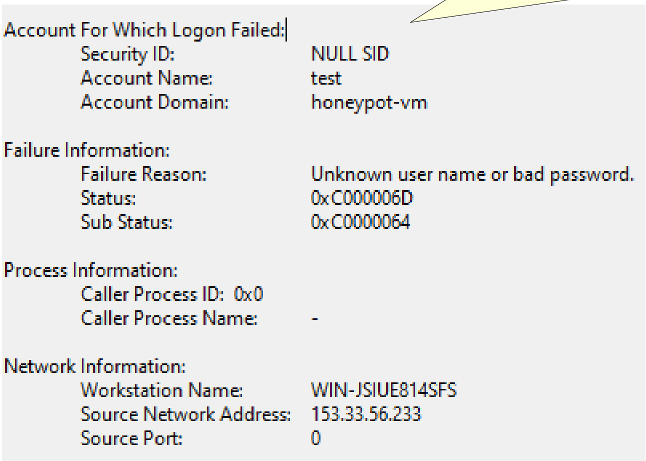
Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

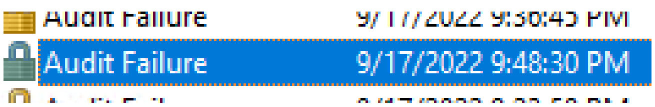
Accept certificate warning

Viewing Failed Logon Attempts on Windows Event Viewer

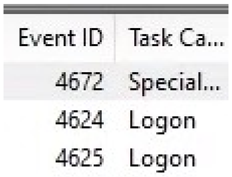
The Powershell script send 4625 Event IDs from Event Viewer to the geolocation API



```
Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           test
        Account Domain:         honeypot-vm

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC0000064

Process Information:
        Caller Process ID:  0x0
        Caller Process Name:    -

Network Information:
        Workstation Name:       WIN-JSIUE814SFS
        Source Network Address: 153.33.56.233
        Source Port:            0
```

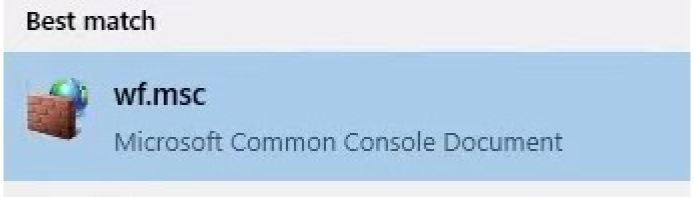


```
Audit Failure    9/17/2022 9:48:30 PM
```



Event ID	Task Ca...
4672	Special...
4624	Logon
4625	Logon

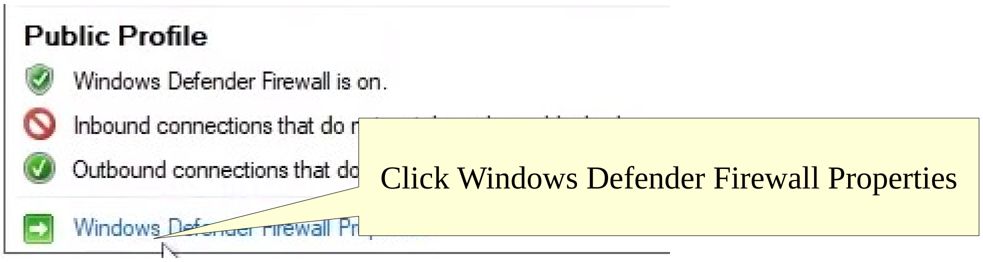
Disable Windows Firewall to Allow ICMP Echo Requests Through



Best match

wf.msc

Microsoft Common Console Document



Public Profile

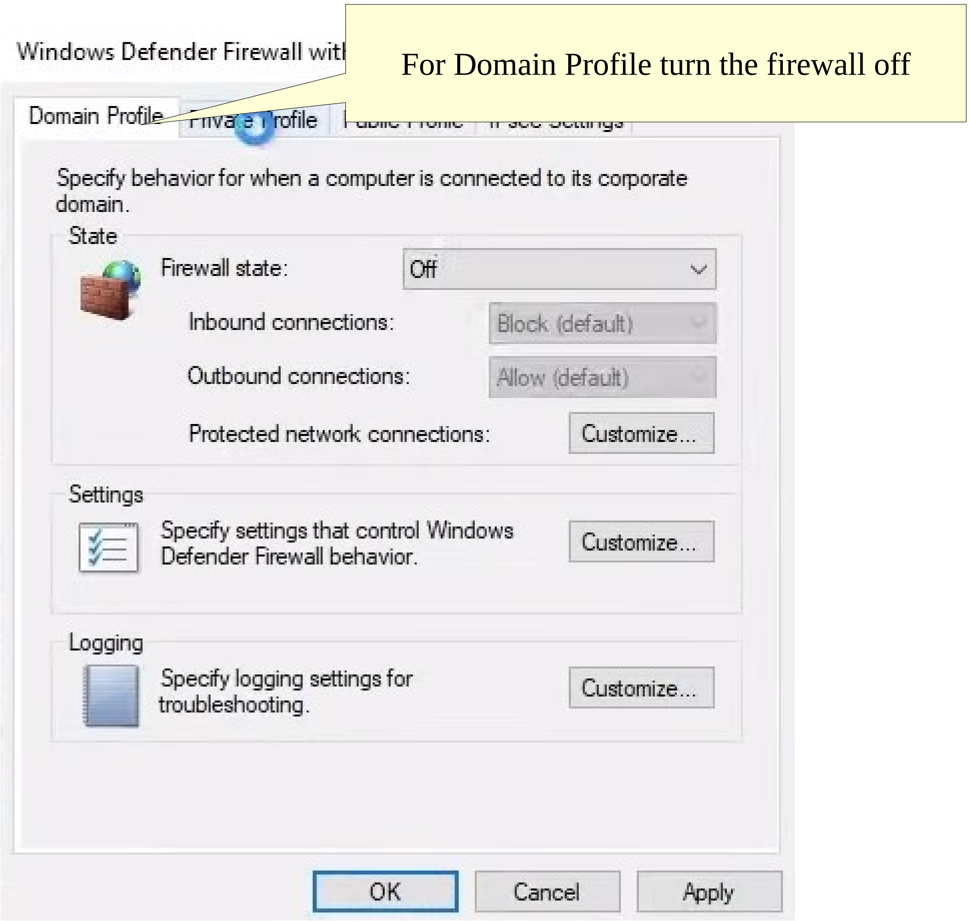
Windows Defender Firewall is on.

Inbound connections that do r

Outbound connections that do

Windows Defender Firewall Pr

Click Windows Defender Firewall Properties



Windows Defender Firewall wit

For Domain Profile turn the firewall off

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

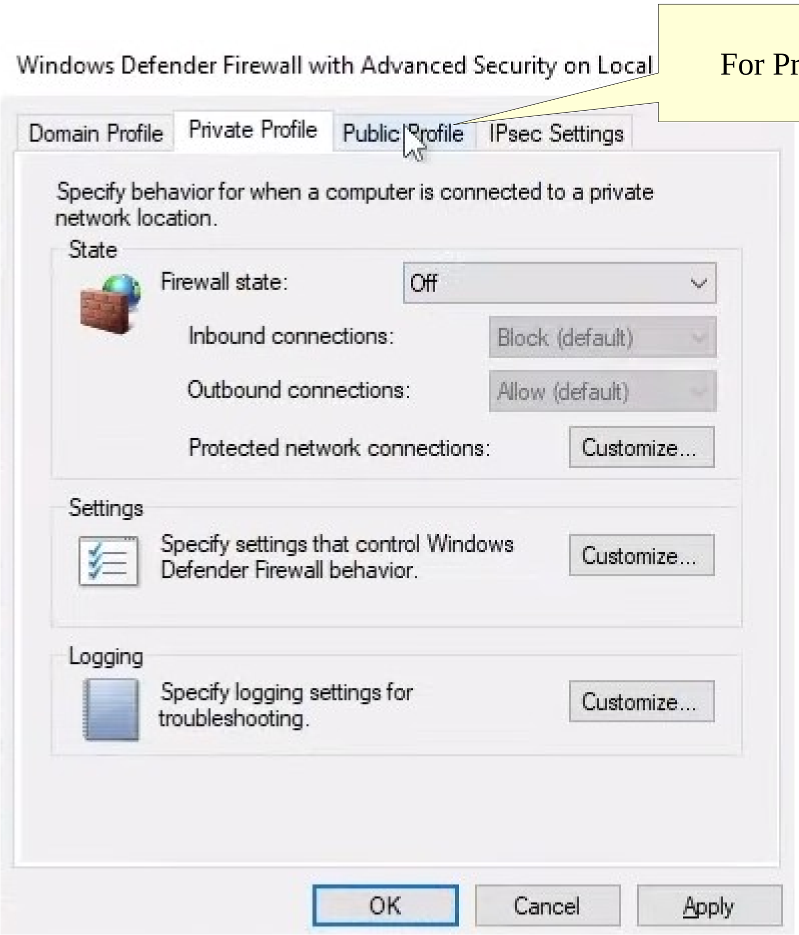
Protected network connections: Customize...

Settings

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

Logging

Specify logging settings for troubleshooting. Customize...



Windows Defender Firewall with Advanced Security on Local

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

State

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

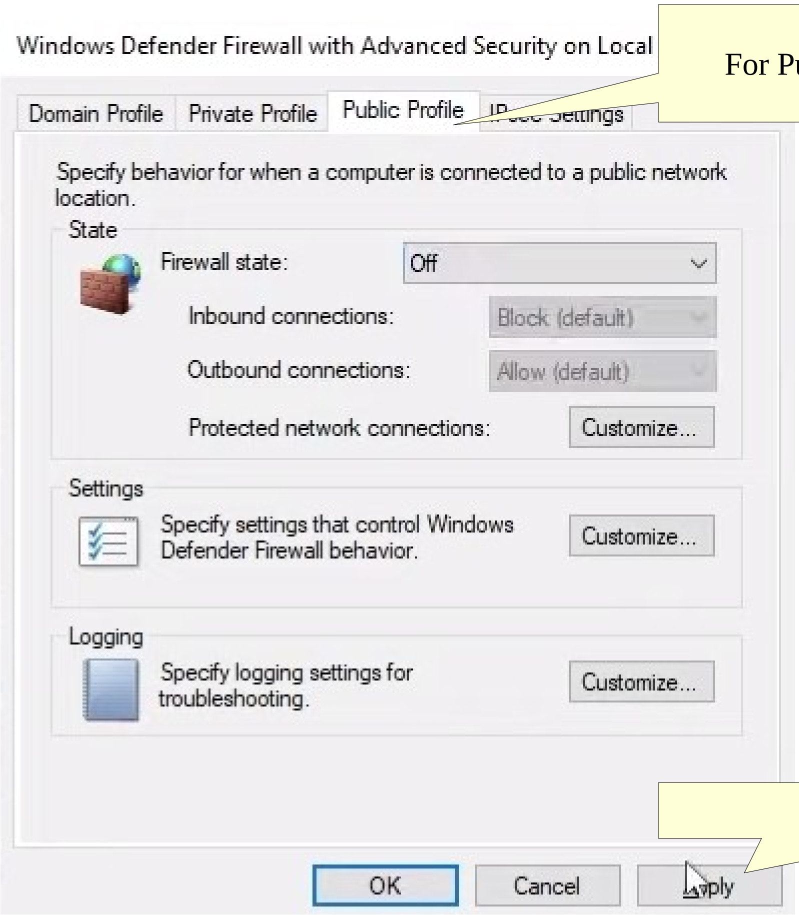
Settings

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

Logging

Specify logging settings for troubleshooting. Customize...

For Private Profile turn the firewall off



Windows Defender Firewall with Advanced Security on Local

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...

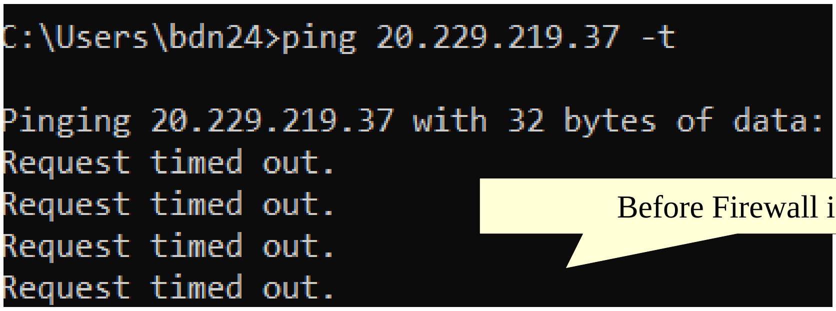
Logging

Specify logging settings for troubleshooting. Customize...

For Public Profile turn the firewall off

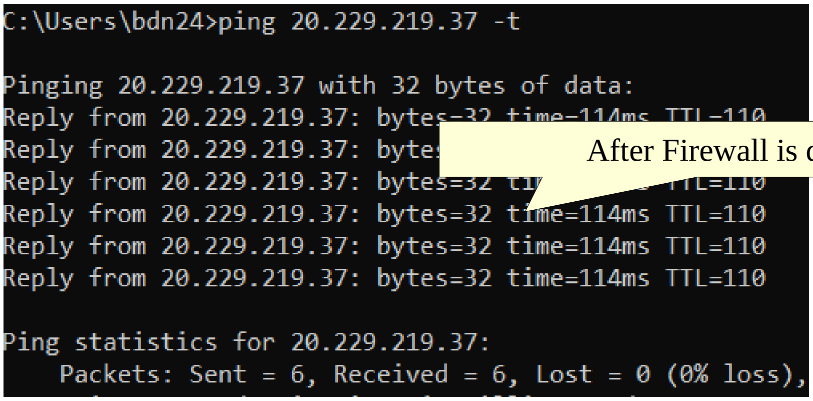
Apply the settings

Verify ICMP Echo Requests/Ping Request are Being Received



```
C:\Users\bdn24>ping 20.229.219.37 -t

Pinging 20.229.219.37 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

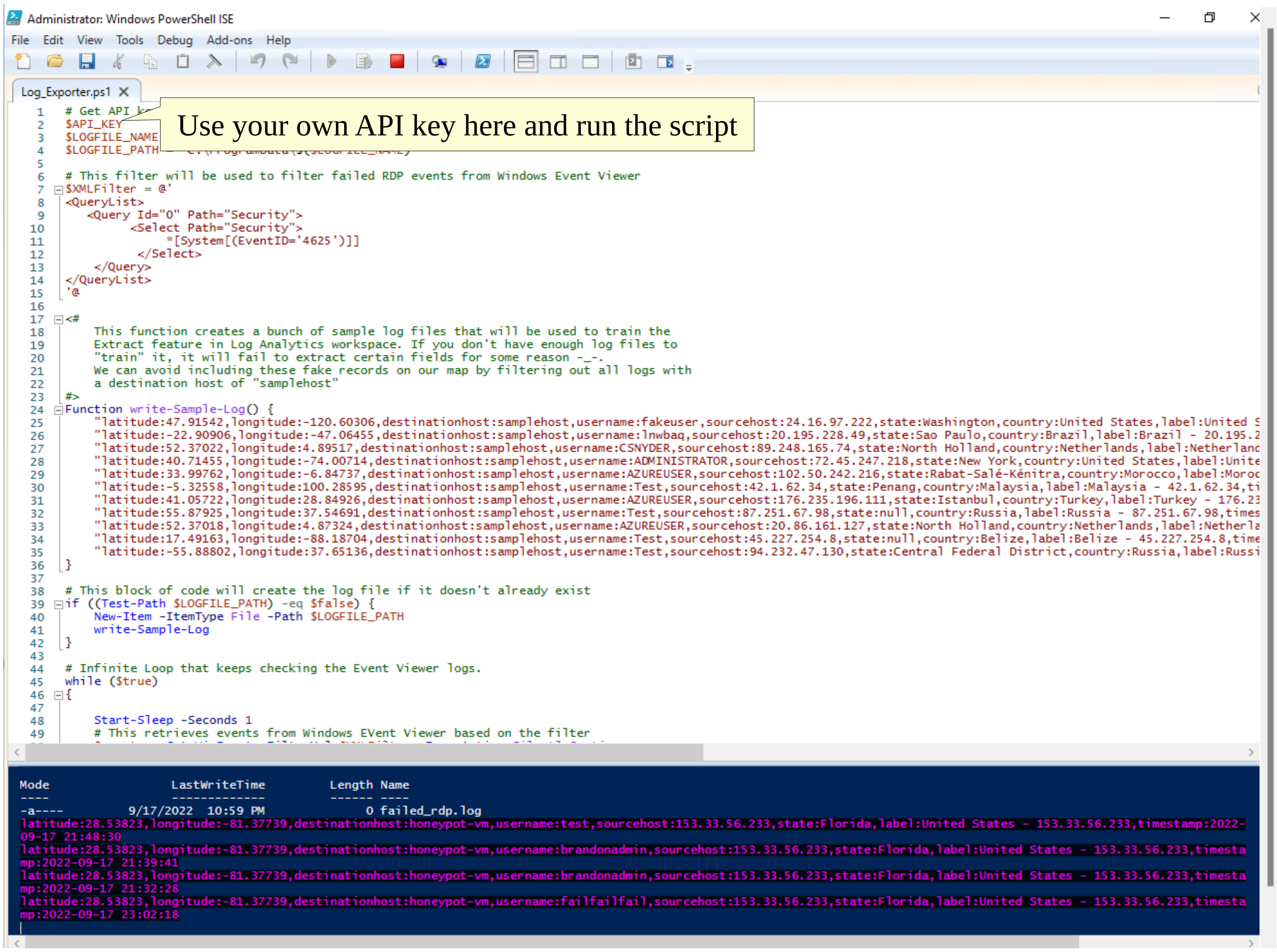
Before Firewall is disabled



```
C:\Users\bdn24>ping 20.229.219.37 -t

Pinging 20.229.219.37 with 32 bytes of data:
Reply from 20.229.219.37: bytes=32 time=114ms TTL=110
Reply from 20.229.219.37: bytes
Reply from 20.229.219.37: bytes=32 ti            TTL=110
Reply from 20.229.219.37: bytes=32 time=114ms TTL=110
Reply from 20.229.219.37: bytes=32 time=114ms TTL=110
Reply from 20.229.219.37: bytes=32 time=114ms TTL=110

Ping statistics for 20.229.219.37:
    Packets: Sent = 6, Received = 6, Lost = 0 (0% loss),
```

After Firewall is disabled

PowerShell Script with API Key to Get Geolocation Data

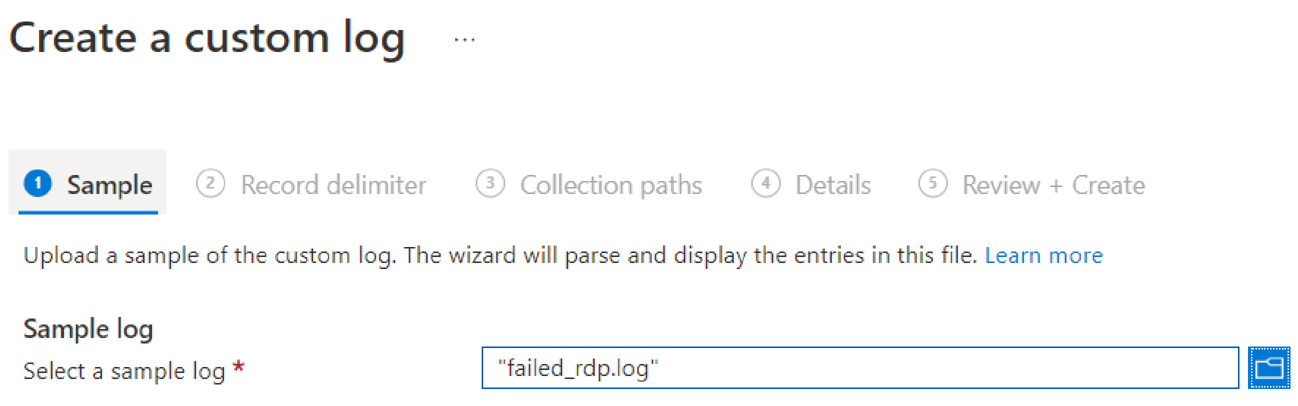

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Log_Exporter.ps1

Use your own API key here and run the script

```
# Get API k
$API_KEY
$LOGFILE_NAME
$LOGFILE_PATH

# 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
    "latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.247.218,state:New York,country:United States,label:Unite
    "latitude:33.99762,longitude:-6.84737,destinationhost:samplehost,username:AZUREUSER,sourcehost:102.50.242.216,state:Rabat-Salé-Kénitra,country:Morocco,label:Moroc
    "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,ti
    "latitude:41.05722,longitude:28.84926,destinationhost:samplehost,username:AZUREUSER,sourcehost:176.235.196.111,state:Istanbul,country:Turkey,label:Turkey - 176.23
    "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,times
    "latitude:52.37018,longitude:4.87324,destinationhost:samplehost,username:AZUREUSER,sourcehost:20.86.161.127,state:North Holland,country:Netherlands,label:Netherla
    "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,time
    "latitude:-55.88802,longitude:37.65136,destinationhost:samplehost,username:Test,sourcehost:94.232.47.130,state:Central Federal District,country:Russia,label:Russi
}

# This block of code will create the log file if it doesn't already exist
if ((Test-Path $LOGFILE_PATH) -eq $false) {
    New-Item -ItemType File -Path $LOGFILE_PATH
    write-Sample-Log
}

# Infinite Loop that keeps checking the Event Viewer logs.
while ($true)
{

    Start-Sleep -Seconds 1
    # This retrieves events from Windows EVent Viewer based on the filter
```

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/17/2022  10:59 PM              0 failed_rdp.log
latitude:28.53823,longitude:-81.37739,destinationhost:honeypot-vm,username:test,sourcehost:153.33.56.233,state:Florida,label:United States - 153.33.56.233,timestamp:2022-
09-17 21:48:30
latitude:28.53823,longitude:-81.37739,destinationhost:honeypot-vm,username:brandonadmin,sourcehost:153.33.56.233,state:Florida,label:United States - 153.33.56.233,timesta
mp:2022-09-17 21:39:41
latitude:28.53823,longitude:-81.37739,destinationhost:honeypot-vm,username:brandonadmin,sourcehost:153.33.56.233,state:Florida,label:United States - 153.33.56.233,timesta
mp:2022-09-17 21:32:28
latitude:28.53823,longitude:-81.37739,destinationhost:honeypot-vm,username:failfailfail,sourcehost:153.33.56.233,state:Florida,label:United States - 153.33.56.233,timesta
mp:2022-09-17 23:02:18
```

Create Custom Log in Log Analytics Workspace

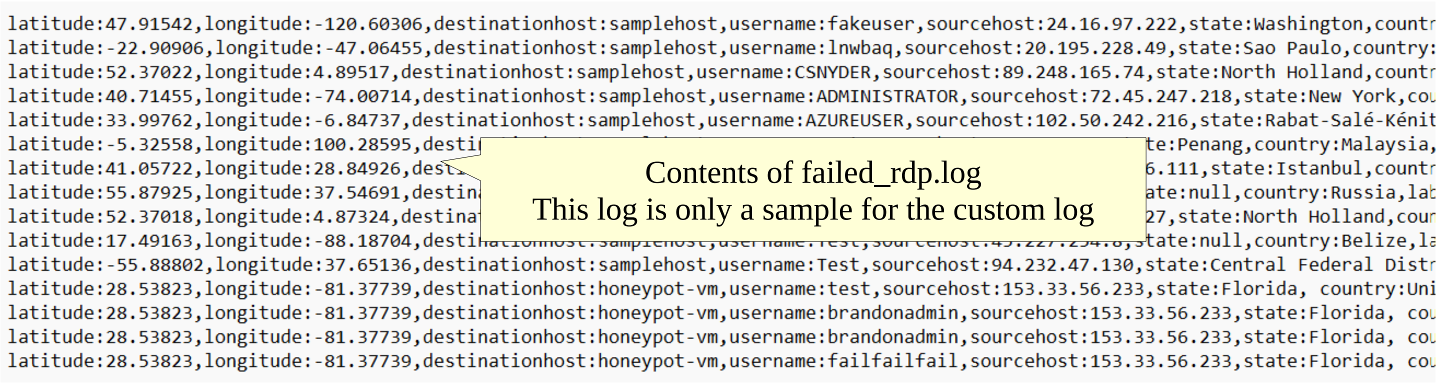


Create a custom log ···

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

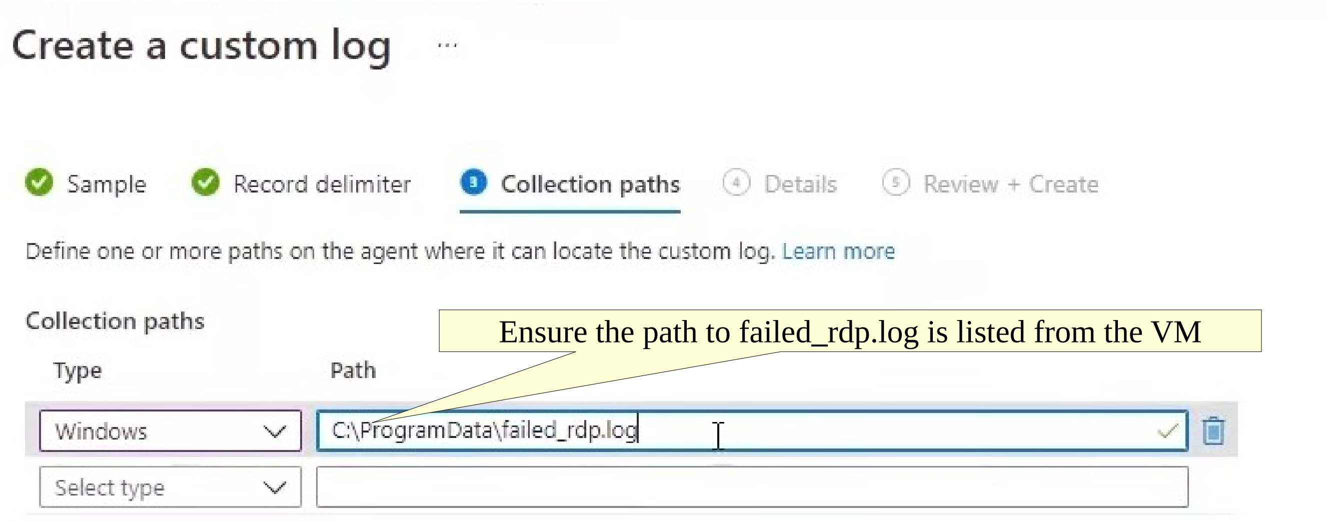
Sample log

Select a sample log * "failed_rdp.log"



```
latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washington,countr
latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country:
latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:North Holland,countr
latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.247.218,state:New York,cou
latitude:33.99762,longitude:-6.84737,destinationhost:samplehost,username:AZUREUSER,sourcehost:102.50.242.216,state:Rabat-Salé-Kénit
latitude:-5.32558,longitude:100.28595,desti                                                                te:Penang,country:Malaysia,
latitude:41.05722,longitude:28.84926,dest                                                                  6.111,state:Istanbul,countr
latitude:55.87925,longitude:37.54691,destina                                                               ate:null,country:Russia,lat
latitude:52.37018,longitude:4.87324,destina                                                                27,state:North Holland,cour
latitude:17.49163,longitude:-88.18704,destinationhost:samplehost,username:Test,sourcehost:45.227.254.8,state:null,country:Belize,la
latitude:-55.88802,longitude:37.65136,destinationhost:samplehost,username:Test,sourcehost:94.232.47.130,state:Central Federal Distr
latitude:28.53823,longitude:-81.37739,destinationhost:honeypot-vm,username:test,sourcehost:153.33.56.233,state:Florida, country:Uni
latitude:28.53823,longitude:-81.37739,destinationhost:honeypot-vm,username:brandonadmin,sourcehost:153.33.56.233,state:Florida, cou
latitude:28.53823,longitude:-81.37739,destinationhost:honeypot-vm,username:brandonadmin,sourcehost:153.33.56.233,state:Florida, cou
latitude:28.53823,longitude:-81.37739,destinationhost:honeypot-vm,username:failfailfail,sourcehost:153.33.56.233,state:Florida, cou
```

Contents of failed_rdp.log
This log is only a sample for the custom log



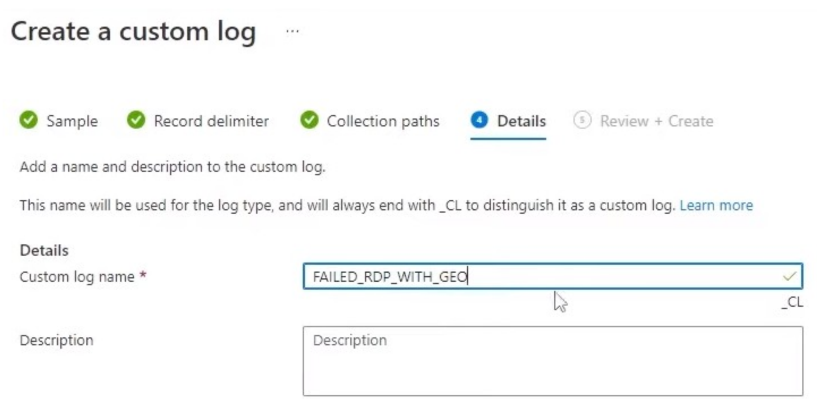
Create a custom log ···

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

Collection paths

Type	Path
Windows	C:\ProgramData\failed_rdp.log
Select type	

Ensure the path to failed_rdp.log is listed from the VM



Create a custom log ···

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

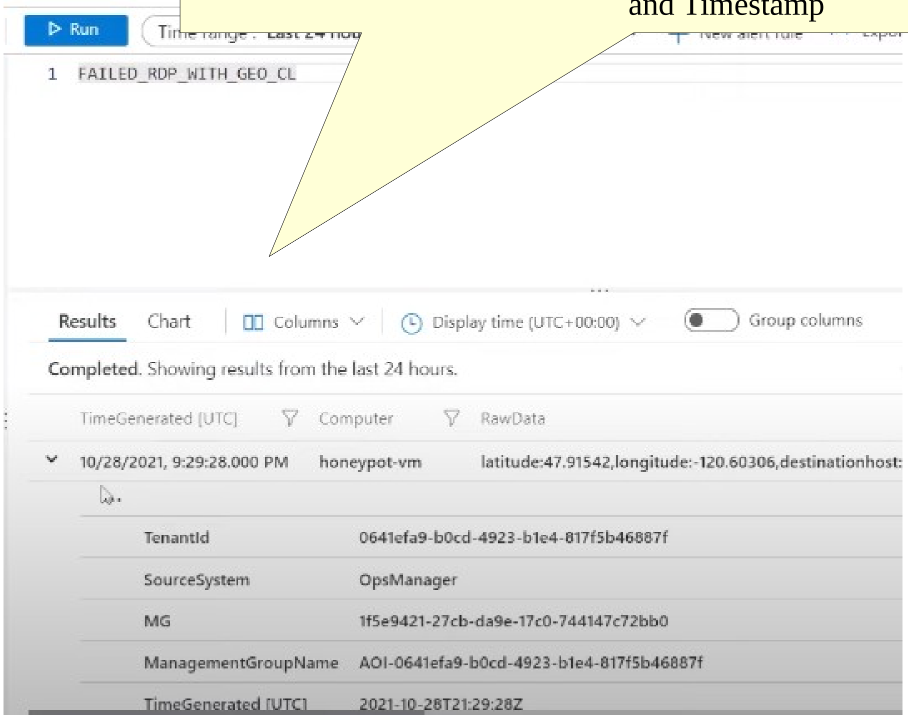
Details

Custom log name *: FAILED_RDP_WITH_GEO _CL

Description: Description

Train the Data Algorithm to Use Appropriate Field

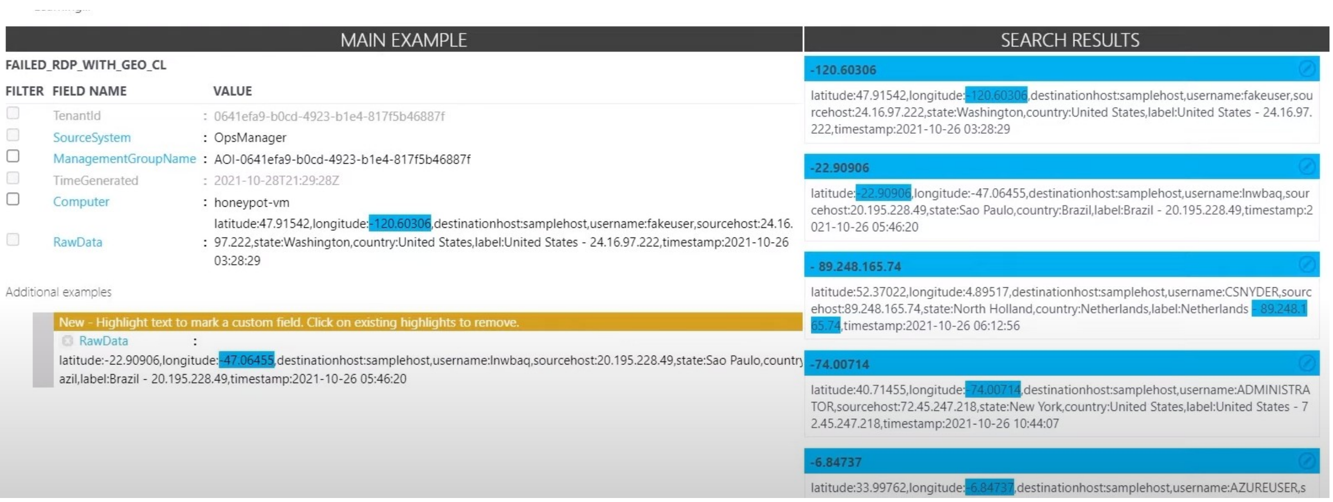
Within Log Analytics Workspace extract custom fields for all of the data into: Longitude, Latitude, DestinationHost, Username, SourceHost, State, Country, Label, and Timestamp



```
1  FAILED_RDP_WITH_GEO_CL
```

Completed. Showing results from the last 24 hours.

```
TimeGenerated [UTC]        Computer      RawData
10/28/2021, 9:29:28.000 PM honeypot-vm   latitude:47.91542,longitude:-120.60306,destinationhost:
    TenantId               0641efa9-b0cd-4923-b1e4-817f5b46887f
    SourceSystem           OpsManager
    MG                     1f5e9421-27cb-da9e-17c0-744147c72bb0
    ManagementGroupName    AOI-0641efa9-b0cd-4923-b1e4-817f5b46887f
    TimeGenerated [UTC]    2021-10-28T21:29:28Z
```



FAILED_RDP_WITH_GEO_CL

FILTER	FIELD NAME		VALUE
□	TenantId	:	0641efa9-b0cd-4923-b1e4-817f5b46887f
□	SourceSystem	:	OpsManager
□	ManagementGroupName	:	AOI-0641efa9-b0cd-4923-b1e4-817f5b46887f
□	TimeGenerated	:	2021-10-28T21:29:28Z
□	Computer	:	honeypot-vm
□	RawData	:	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

Additional examples

New - Highlight text to mark a custom field. Click on existing highlights to remove.

RawData :
latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country
azil,label:Brazil - 20.195.228.49,timestamp:2021-10-26 05:46:20

-120.60306

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

-22.90906

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

- 89.248.165.74

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

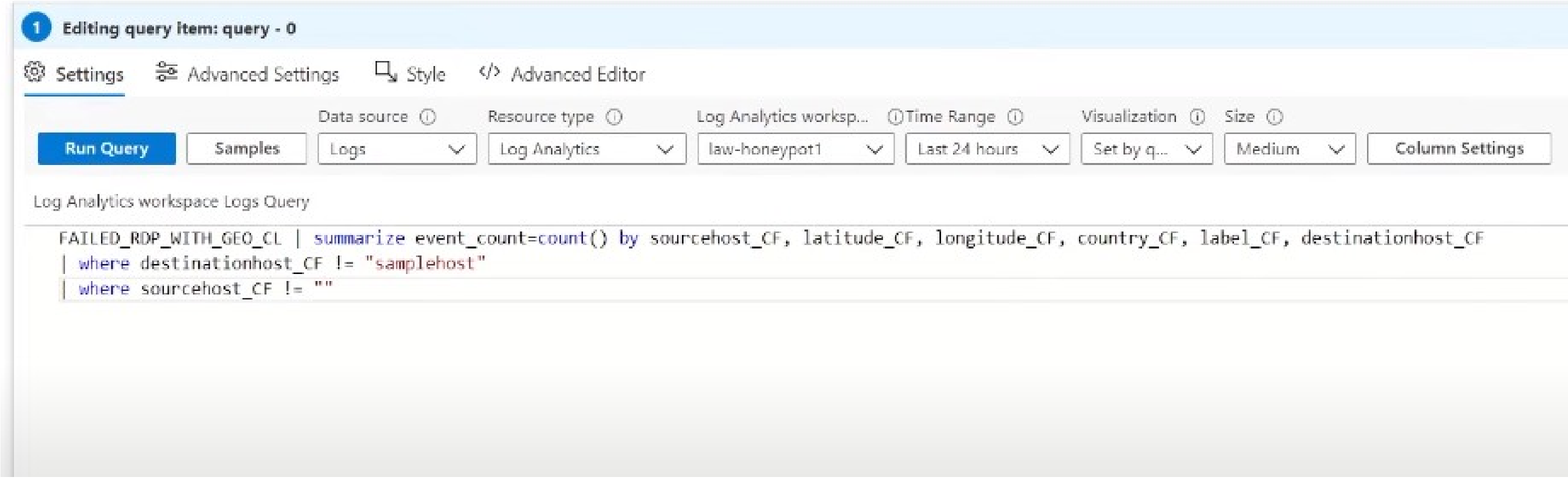
-74.00714

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

-6.84737

latitude:33.99762,longitude:-6.84737,destinationhost:samplehost,username:AZUREUSER,s

Ingest Logs into Azure Sentinel and Create a World Map



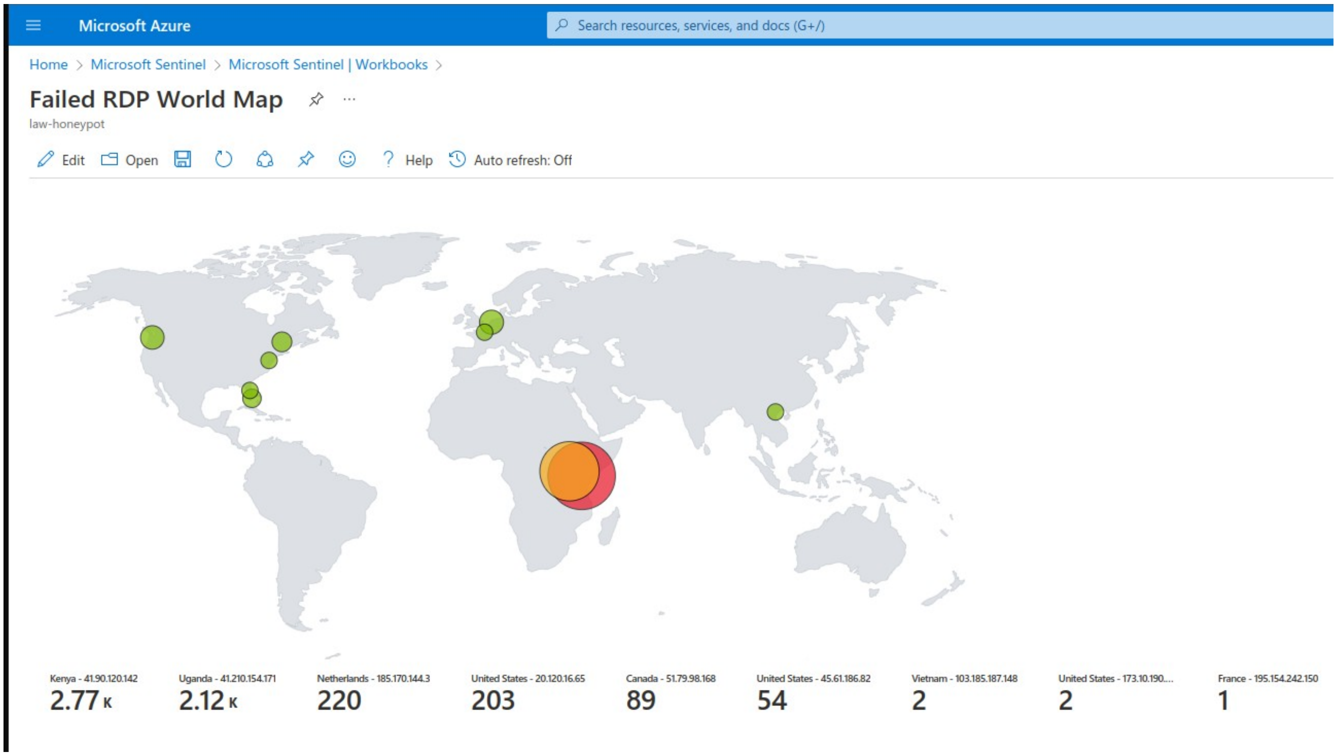
1 Editing query item: query - 0

Data source: Logs
Resource type: Log Analytics
Log Analytics worksp...: law-honeypot1
Time Range: Last 24 hours
Visualization: Set by q...
Size: Medium

Log Analytics workspace Logs Query

```
FAILED_RDP_WITH_GEO_CL | summarize event_count=count() by sourcehost_CF, latitude_CF, longitude_CF, country_CF, label_CF, destinationhost_CF
| where destinationhost_CF != "samplehost"
| where sourcehost_CF != ""
```

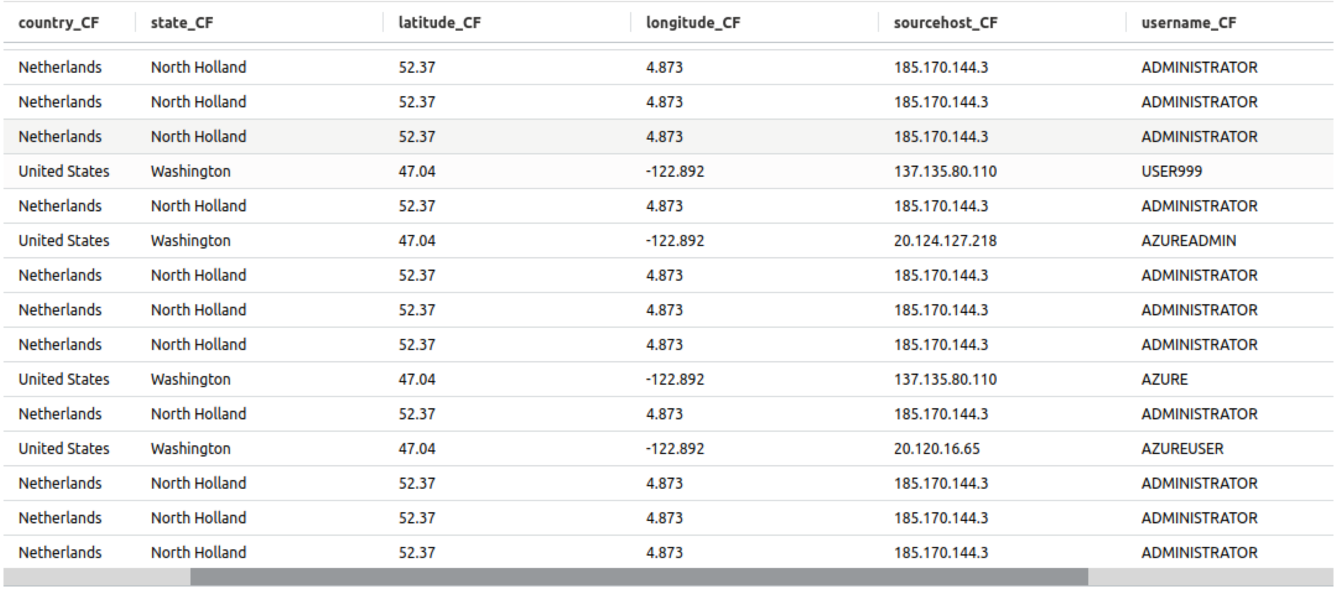
Final Results


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >
Edit
Open
Help
Auto refresh: Off

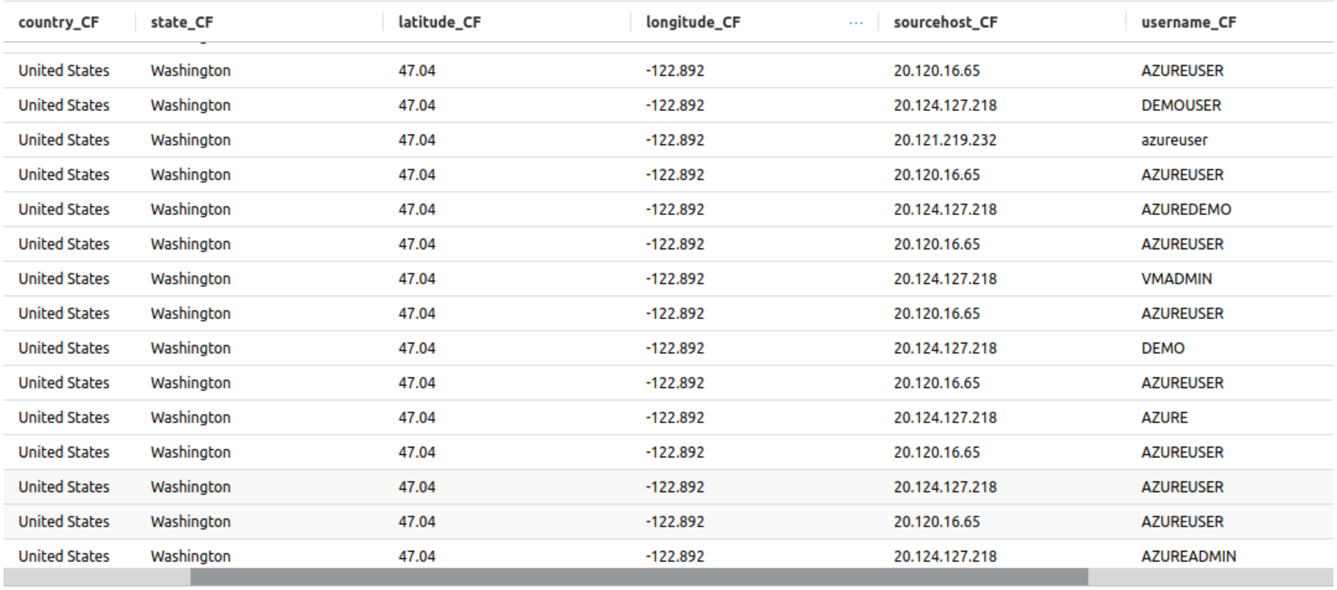
Failed RDP World Map

law-honeypot

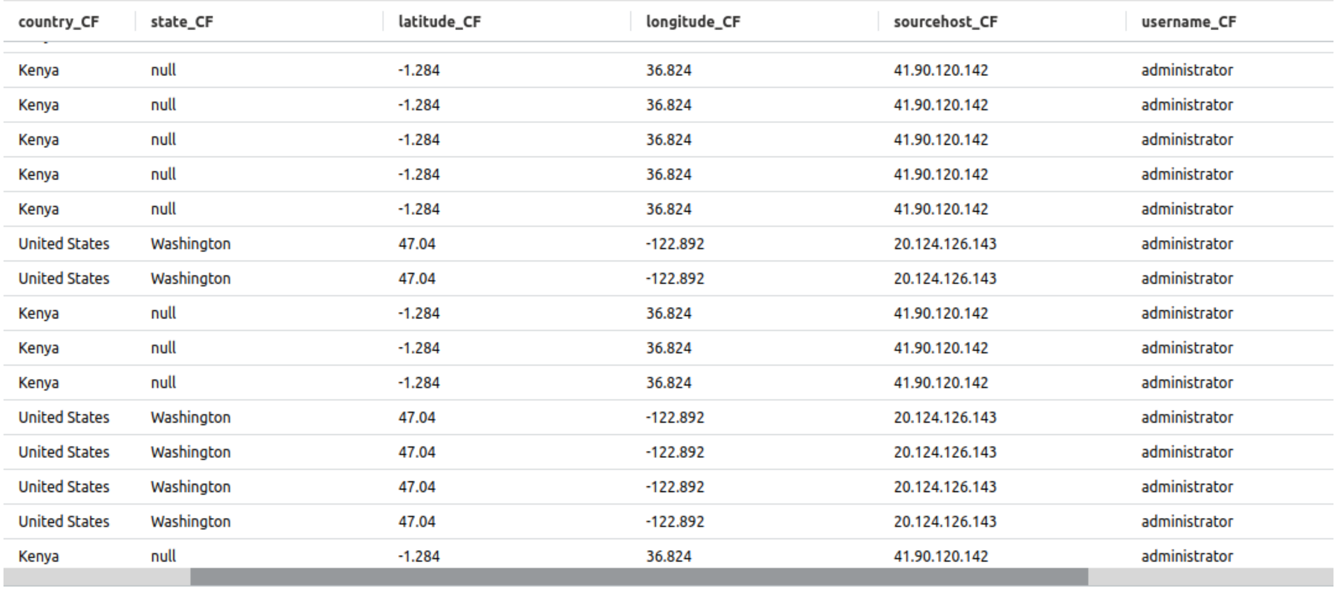
Kenya - 41.90.120.142	Uganda - 41.210.154.171	Netherlands - 185.170.144.3	United States - 20.120.16.65	Canada - 51.79.98.168	United States - 45.61.186.82	Vietnam - 103.185.187.148	United States - 173.10.190....	France - 195.154.242.150
2.77 K	2.12 K	220	203	89	54	2	2	1



country_CF	state_CF	latitude_CF	longitude_CF	sourcehost_CF	username_CF
Netherlands	North Holland	52.37	4.873	185.170.144.3	ADMINISTRATOR
Netherlands	North Holland	52.37	4.873	185.170.144.3	ADMINISTRATOR
Netherlands	North Holland	52.37	4.873	185.170.144.3	ADMINISTRATOR
United States	Washington	47.04	-122.892	137.135.80.110	USER999
Netherlands	North Holland	52.37	4.873	185.170.144.3	ADMINISTRATOR
United States	Washington	47.04	-122.892	20.124.127.218	AZUREADMIN
Netherlands	North Holland	52.37	4.873	185.170.144.3	ADMINISTRATOR
Netherlands	North Holland	52.37	4.873	185.170.144.3	ADMINISTRATOR
Netherlands	North Holland	52.37	4.873	185.170.144.3	ADMINISTRATOR
United States	Washington	47.04	-122.892	137.135.80.110	AZURE
Netherlands	North Holland	52.37	4.873	185.170.144.3	ADMINISTRATOR
United States	Washington	47.04	-122.892	20.120.16.65	AZUREUSER
Netherlands	North Holland	52.37	4.873	185.170.144.3	ADMINISTRATOR
Netherlands	North Holland	52.37	4.873	185.170.144.3	ADMINISTRATOR
Netherlands	North Holland	52.37	4.873	185.170.144.3	ADMINISTRATOR



country_CF	state_CF	latitude_CF	longitude_CF	sourcehost_CF	username_CF
United States	Washington	47.04	-122.892	20.120.16.65	AZUREUSER
United States	Washington	47.04	-122.892	20.124.127.218	DEMOUSER
United States	Washington	47.04	-122.892	20.121.219.232	azureuser
United States	Washington	47.04	-122.892	20.120.16.65	AZUREUSER
United States	Washington	47.04	-122.892	20.124.127.218	AZUREDEMO
United States	Washington	47.04	-122.892	20.120.16.65	AZUREUSER
United States	Washington	47.04	-122.892	20.124.127.218	VMADMIN
United States	Washington	47.04	-122.892	20.120.16.65	AZUREUSER
United States	Washington	47.04	-122.892	20.124.127.218	DEMO
United States	Washington	47.04	-122.892	20.120.16.65	AZUREUSER
United States	Washington	47.04	-122.892	20.124.127.218	AZURE
United States	Washington	47.04	-122.892	20.120.16.65	AZUREUSER
United States	Washington	47.04	-122.892	20.124.127.218	AZUREUSER
United States	Washington	47.04	-122.892	20.120.16.65	AZUREUSER
United States	Washington	47.04	-122.892	20.124.127.218	AZUREADMIN



country_CF	state_CF	latitude_CF	longitude_CF	sourcehost_CF	username_CF
Kenya	null	-1.284	36.824	41.90.120.142	administrator
Kenya	null	-1.284	36.824	41.90.120.142	administrator
Kenya	null	-1.284	36.824	41.90.120.142	administrator
Kenya	null	-1.284	36.824	41.90.120.142	administrator
Kenya	null	-1.284	36.824	41.90.120.142	administrator
United States	Washington	47.04	-122.892	20.124.126.143	administrator
United States	Washington	47.04	-122.892	20.124.126.143	administrator
Kenya	null	-1.284	36.824	41.90.120.142	administrator
Kenya	null	-1.284	36.824	41.90.120.142	administrator
Kenya	null	-1.284	36.824	41.90.120.142	administrator
United States	Washington	47.04	-122.892	20.124.126.143	administrator
United States	Washington	47.04	-122.892	20.124.126.143	administrator
United States	Washington	47.04	-122.892	20.124.126.143	administrator
United States	Washington	47.04	-122.892	20.124.126.143	administrator
Kenya	null	-1.284	36.824	41.90.120.142	administrator