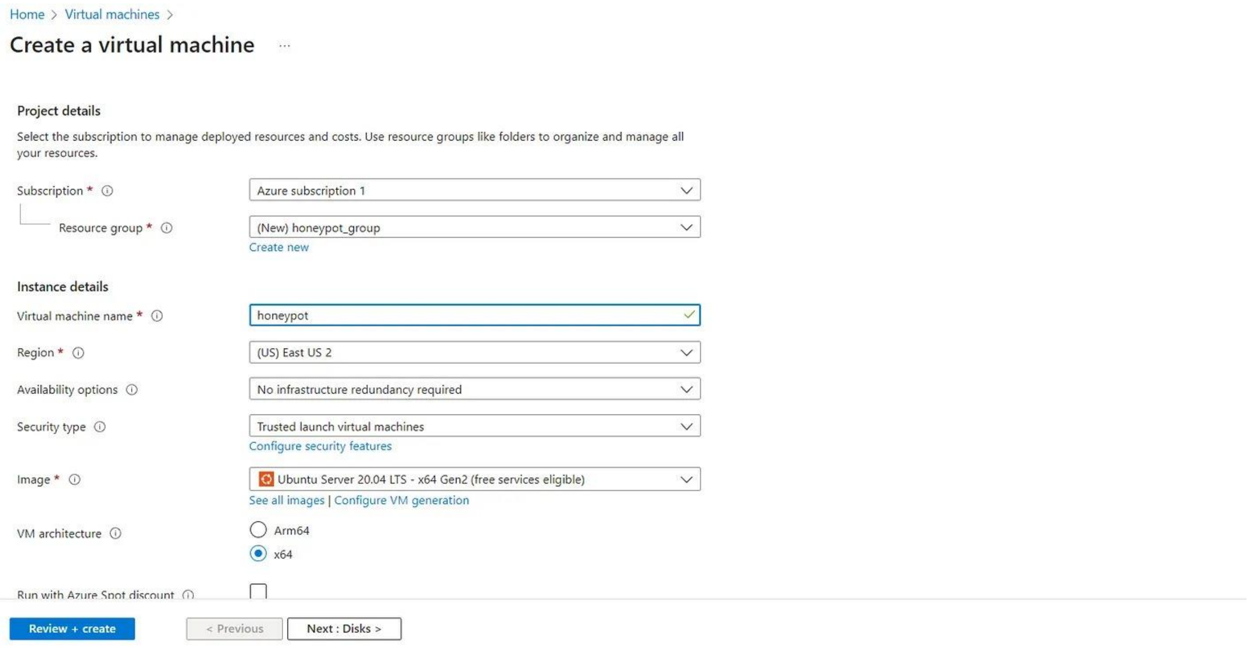
Building the Honeypot

The first step in the project is creating a virtual machine that acts as a honeypot, enticing potential attackers.

Search for “Virtual Machines” in the Azure portal’s search bar.
Click on “Azure virtual machine” under the “Create” option.
Name your virtual machine, and let the resource group auto-fill.
Set up an administrator account (password or SSH key) and proceed.
Continue through the setup, configuring networking options, including making the firewall vulnerable.
Click “Review+Create” to finalize.



Home > Virtual machines >

Create a virtual machine

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 * : (New) honeypot_group
Create new

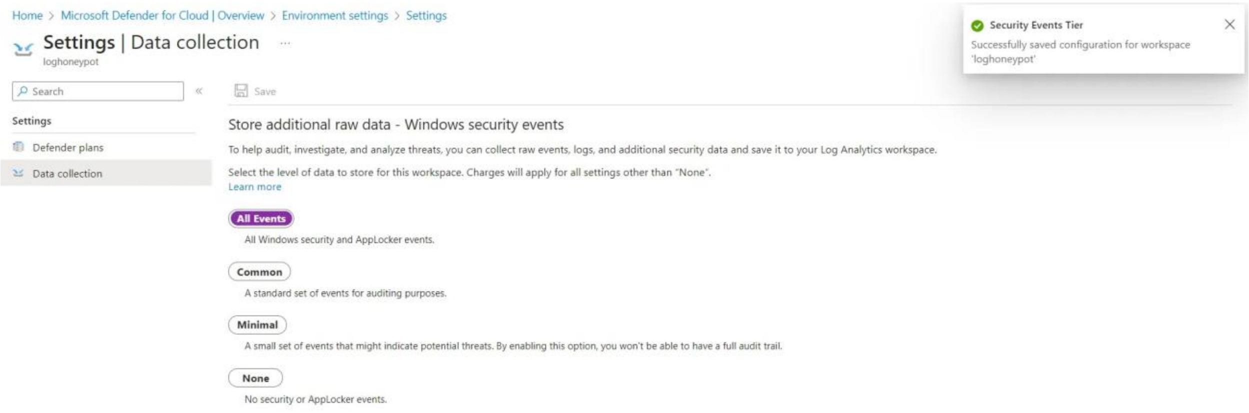
Instance details

Virtual machine name * : honeypot
Region * : (US) East US 2
Availability options : No infrastructure redundancy required
Security type : Trusted launch virtual machines
Configure security features
Image * : Ubuntu Server 20.04 LTS - x64 Gen2 (free services eligible)
See all images | Configure VM generation
VM architecture : ○ Arm64 ● x64
Run with Azure Spot discount □

Setting Up Log Analytics

To collect and analyze data from your honeypot, you need a Log Analytic workspace. Follow these steps:

Create a Log Analytic workspace and review your configuration.
Turn off Azure Defender in Microsoft Defender for Cloud to attract adversaries.
Configure the settings in Microsoft Defender for Cloud, enabling plans and connecting the Log Analytic workspace with the honeypot VM.
Add Azure Sentinel for further monitoring.


Home > Microsoft Defender for Cloud | Overview > Environment settings > Settings
Settings | Data collection
loghoneypot
Search
Save
Settings
Defender plans
Data collection

Security Events Tier
Successfully saved configuration for workspace 'loghoneypot'

Store additional raw data - Windows security events

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

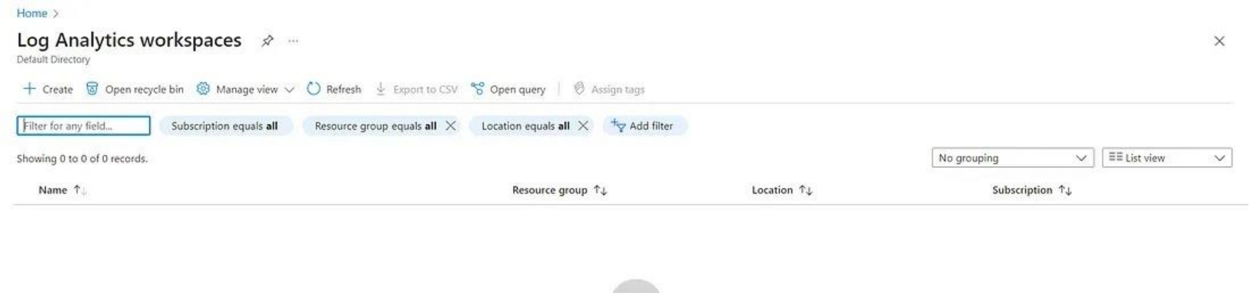
Select the level of data to store for this workspace. Charges will apply for all settings other than "None".
Learn more

[✓ 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.

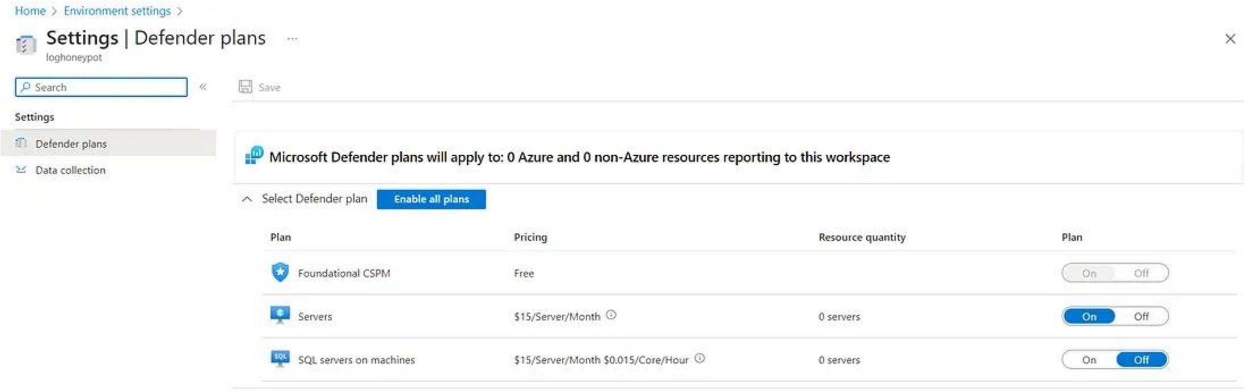
None
No security or AppLocker events.



Subscription equals **all** | Resource group equals **all** | Location equals **all**

Showing 0 to 0 of 0 records.

Name	Resource group	Location	Subscription



Home > Environment settings >

Settings | Defender plans ···

loghoneypot

Settings

- Defender plans
- Data collection

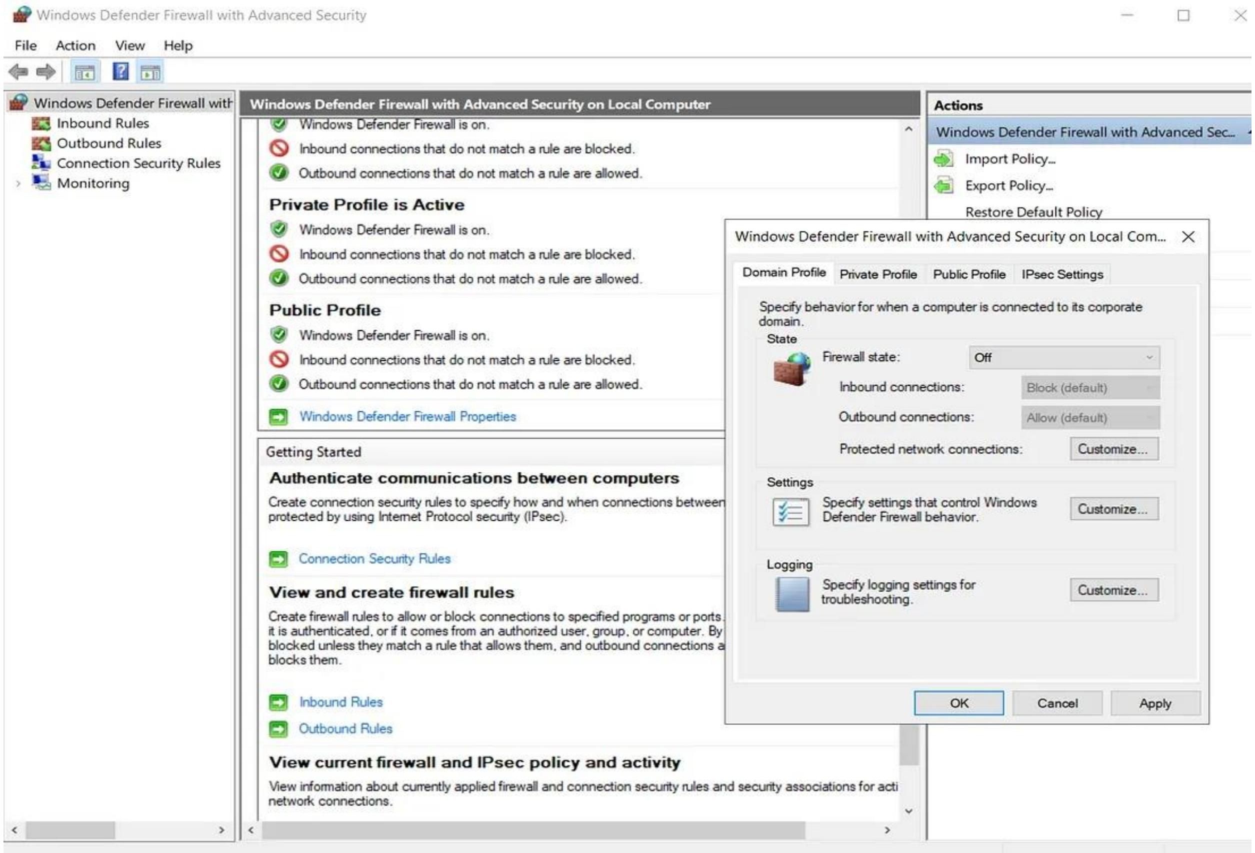
Microsoft Defender plans will apply to: 0 Azure and 0 non-Azure resources reporting to this workspace

Select Defender plan

Plan	Pricing	Resource quantity	Plan
Foundational CSPM	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]

Making the Honeypot Visible

To attract even more attention, adjust the firewall settings on the VM to allow ICMP echo requests for ping responses.


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Actions
Windows Defender Firewall with Advanced Sec...
Import Policy...
Export Policy...
Restore Default Policy
Windows Defender Firewall with Advanced Security on Local Com...
Domain Profile
Private Profile
Public Profile
IPsec Settings
State
Settings
Logging
Customize...
Customize...
Customize...
OK
Cancel
Apply

Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

Private Profile is Active

Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

Public Profile

Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. it is authenticated, or if it comes from an authorized user, group, or computer. By blocked unless they match a rule that allows them, and outbound connections a blocks them.

Inbound Rules
Outbound Rules

View current firewall and IPsec policy and activity

View information about currently applied firewall and connection security rules and security associations for acti network connections.

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

Firewall state: Off
Inbound connections: Block (default)
Outbound connections: Allow (default)
Protected network connections:

Specify settings that control Windows Defender Firewall behavior.

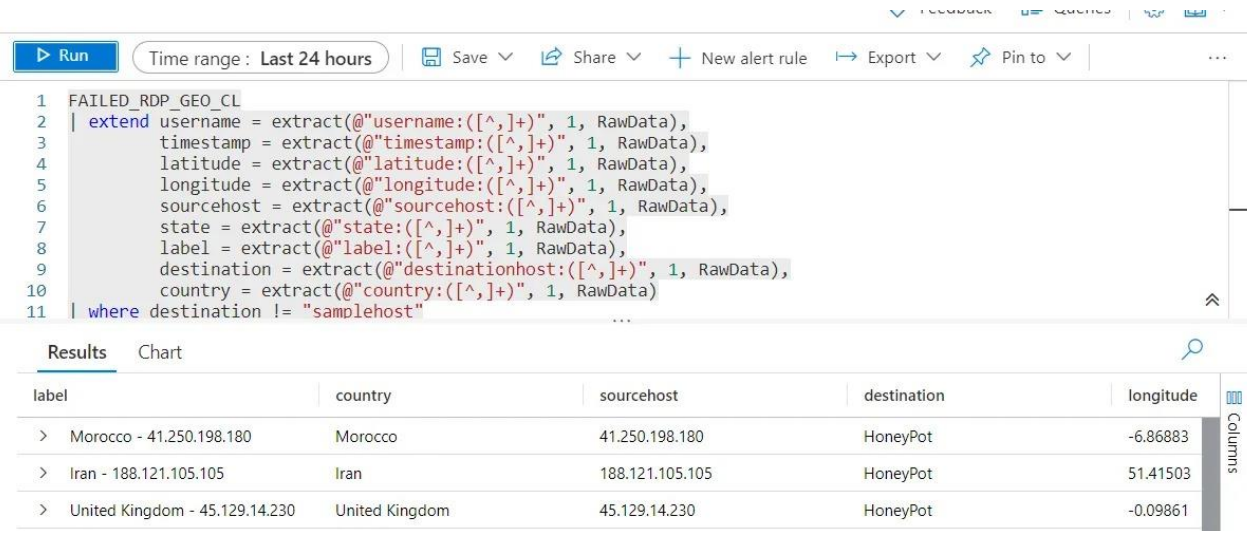
Specify logging settings for troubleshooting.

Automating Data Ingestion with PowerShell

To streamline data collection, download the PowerShell script provided by Josh Madakor in the project folder.

Creating Custom Logs

Now, create a custom log in the Log Analytic Workspace to capture failed login attempts. Follow the instructions carefully and make use of Azure Portal’s search to locate the Log Analytic Workspace.

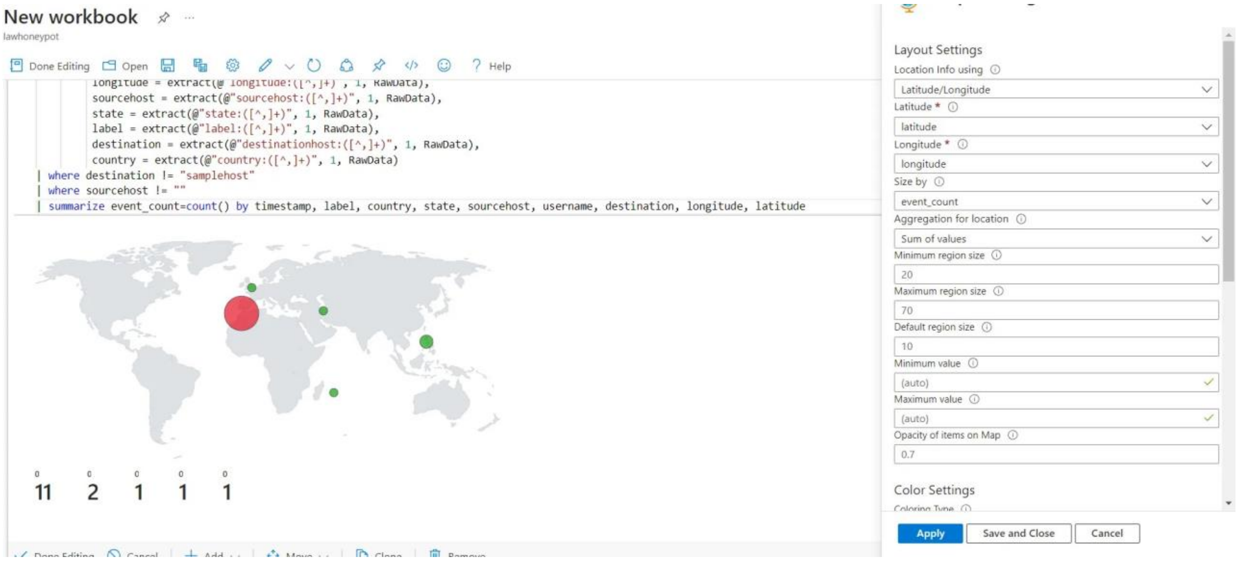


```
FAILED_RDP_GEO_CL
| extend username = extract(@"username:([^,]+)", 1, RawData),
         timestamp = extract(@"timestamp:([^,]+)", 1, RawData),
         latitude = extract(@"latitude:([^,]+)", 1, RawData),
         longitude = extract(@"longitude:([^,]+)", 1, RawData),
         sourcehost = extract(@"sourcehost:([^,]+)", 1, RawData),
         state = extract(@"state:([^,]+)", 1, RawData),
         label = extract(@"label:([^,]+)", 1, RawData),
         destination = extract(@"destinationhost:([^,]+)", 1, RawData),
         country = extract(@"country:([^,]+)", 1, RawData)
| where destination != "samplehost"
```

label	country	sourcehost	destination	longitude
Morocco - 41.250.198.180	Morocco	41.250.198.180	HoneyPot	-6.86883
Iran - 188.121.105.105	Iran	188.121.105.105	HoneyPot	51.41503
United Kingdom - 45.129.14.230	United Kingdom	45.129.14.230	HoneyPot	-0.09861

Analyzing Data and Setting Up the MAP

The final steps involve analyzing your data and setting up the MAP on Azure Sentinel. Follow the provided script to extract and map data for deeper insights.



```
            longitude = extract(@"longitude:([^,]+)", 1, RawData),
            sourcehost = extract(@"sourcehost:([^,]+)", 1, RawData),
            state = extract(@"state:([^,]+)", 1, RawData),
            label = extract(@"label:([^,]+)", 1, RawData),
            destination = extract(@"destinationhost:([^,]+)", 1, RawData),
            country = extract(@"country:([^,]+)", 1, RawData)
    | where destination != "samplehost"
    | where sourcehost != ""
    | summarize event_count=count() by timestamp, label, country, state, sourcehost, username, destination, longitude, latitude
```

Layout Settings

Location Info using: Latitude/Longitude
Latitude *: latitude
Longitude *: longitude
Size by: event_count
Aggregation for location: Sum of values
Minimum region size: 20
Maximum region size: 70
Default region size: 10
Minimum value: (auto)
Maximum value: (auto)
Opacity of items on Map: 0.7

Color Settings