

# Siem Lab in Azure

## Siem Lab with Honeypot in Azure

### Lab done by Lainey Tubbs

This Lab in Azure is us designing a honeypot that allows attackers to come at this vm from all over the world. We are going to use the Siem Azure Sentinel to monitor this activity and report all incidents.

### First step is creating the VM in Azure

The screenshot shows a Microsoft Edge browser window with the URL <https://portal.azure.com/#view/HubsExtension/BrowseResource/resourceType/Microsoft.Compute>. The title bar indicates the date and time as Thu Oct 26 14:51:37. The Azure logo is in the top left, and the user's email, laineytubbs@gmail.com, is in the top right. The main content area is titled "Virtual machines" and shows a message: "No virtual machines to display". Below this, there is a call-to-action button labeled "Create" and links to "Learn more about Windows virtual machines" and "Learn more about Linux virtual machines". The interface includes various filters and sorting options for the virtual machine list.

### Starting configurations for honeypotvm

Firefox Create a virtual machine - + https://portal.azure.com/#create/Microsoft.VirtualMachine-ARM 67% Microsoft Azure Upgrade Search resources, services, and docs (G+) Home > Virtual machines > Create a virtual machine

Subscription \* Azure subscription 1 (New) Honeypot-SiemLab Create new

Resource group \* (New) Honeypot-SiemLab

Instance details

Virtual machine name \* honeypot

Region \* (US) East US

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 10 Pro, version 22H2 - x64 Gen2 (free services eligible) See all images | Configure VM generation

VM architecture Arm64 x64 Arm64 is not supported with the selected image.

Run with Azure Spot discount

ⓘ You are in the free trial period. Costs associated with this VM can be covered by any remaining credits on your subscription. Learn more

Size \* Standard\_D2s\_v3 - 2 vcpus, 8 GiB memory (\$70.08/month) See all sizes

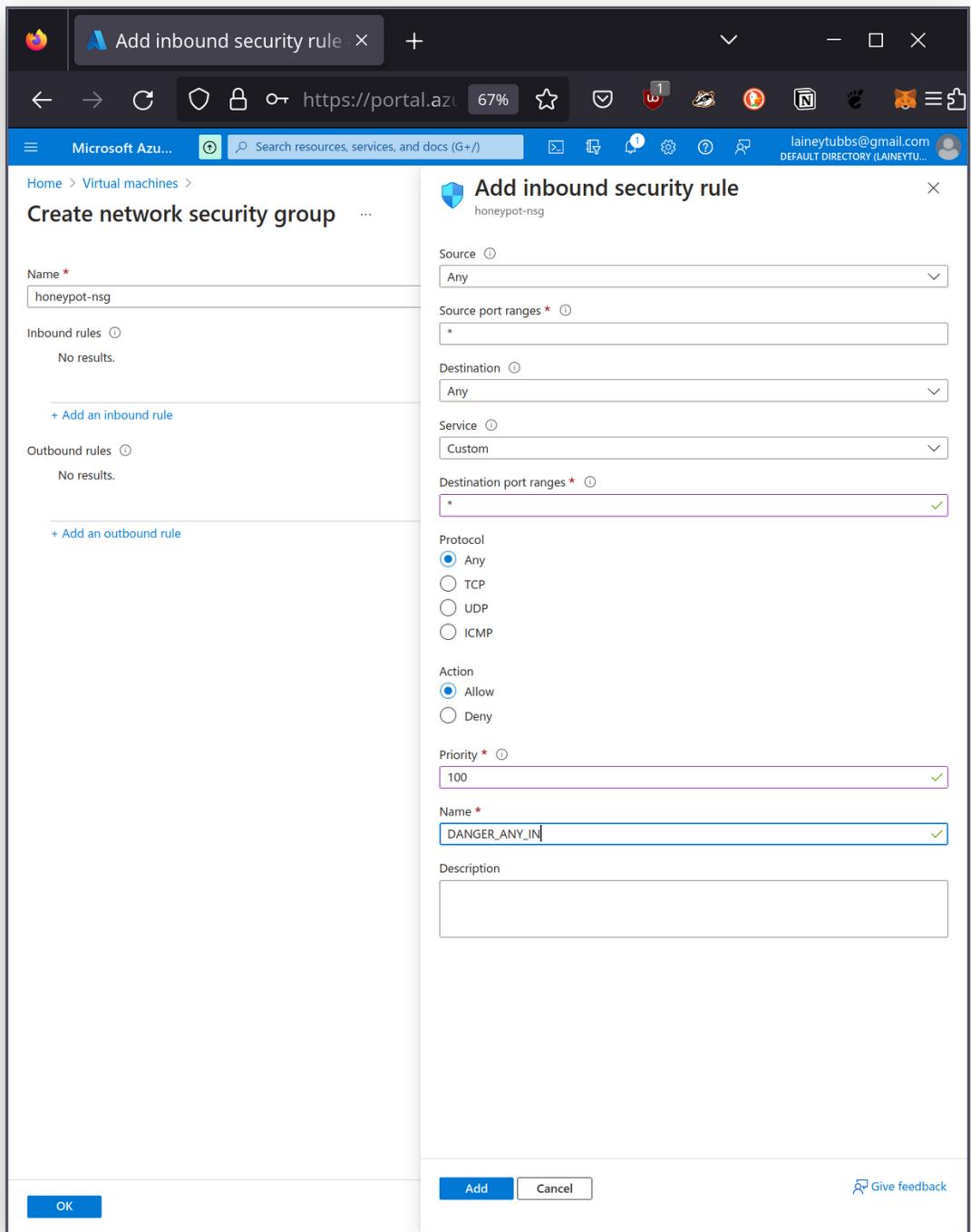
Administrator account

Username \* lain

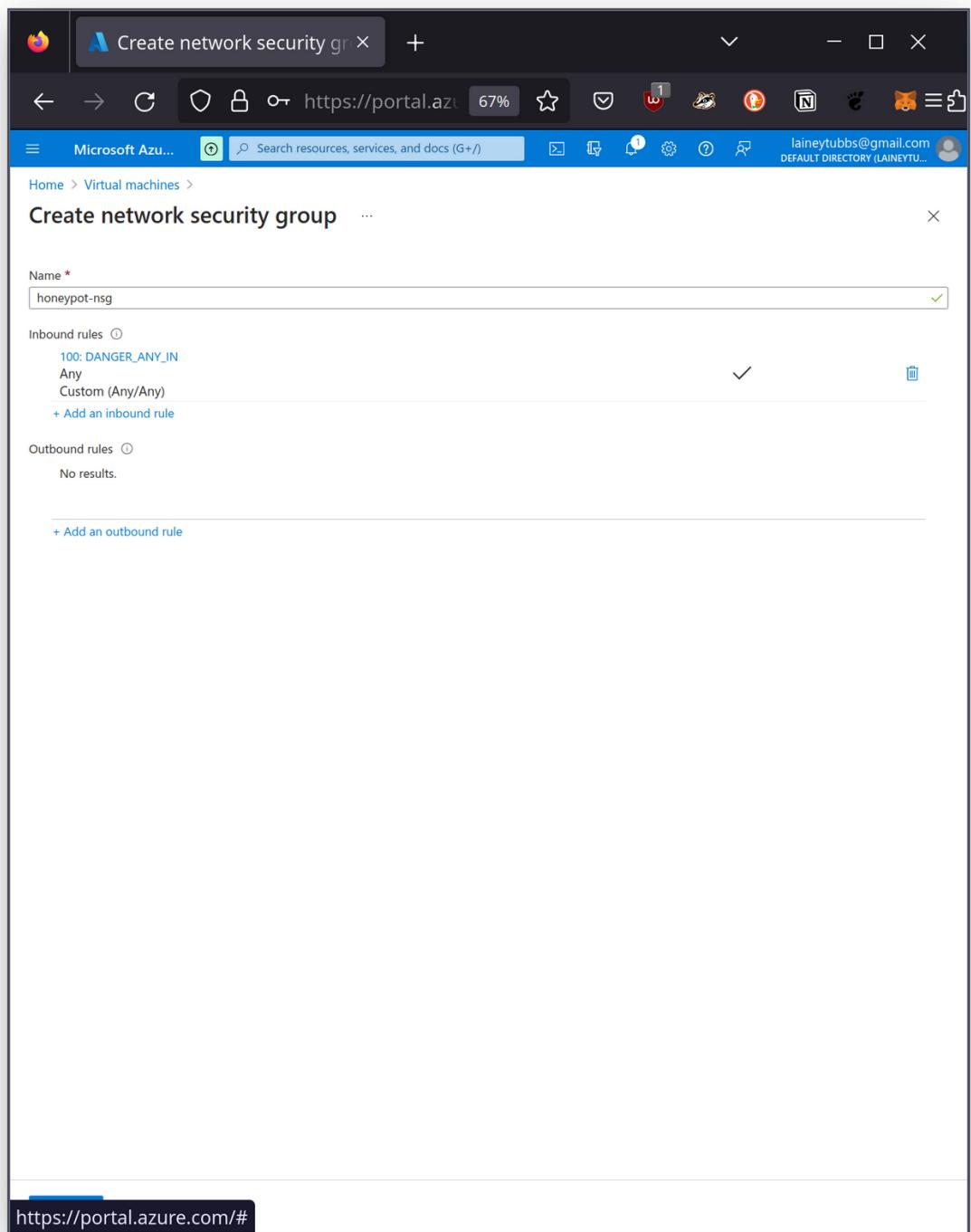
Password \* Confirm password \*

Review + create < Previous Next : Disks > Give feedback

**Setting inbound network security rule so that it allows any type of traffic in from any port**



Finished creating the network security group with the new rule we set



**showing config for the vm prior to finalizing its creation**

Validation passed

Basics Disks Networking Management Monitoring Advanced Tags Review + create

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 **0.0960 USD/hr**  
[Subscription credits apply](#) [Terms of use](#) | [Privacy policy](#)

TERMS  
By clicking "Create", I (a) agree to the legal terms and privacy statements associated with the Marketplace offerings 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 subscription 1
Resource group	(new) Honeypot-SiemLab
Virtual machine name	honeypot
Region	East US
Availability options	Availability zone
Availability zone	1
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable VTPM	Yes
Integrity monitoring	No
Image	Windows 10 Pro, version 22H2 - Gen2
VM architecture	x64
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Username	lain
Already have a Windows license?	Yes
License type	Windows Client
Azure Spot	No

[Create](#) < Previous Next > Download a template for automation [Give feedback](#)

## Deploying the VM

Search [Delete](#) [Cancel](#) [Redeploy](#) [Download](#) [Refresh](#)

Deployment name: CreateVm-MicrosoftWindowsDesktop.Windows-10-win10-20231026145743 | Overview

Deployment is in progress

Deployment name: CreateVm-MicrosoftWindowsDesktop.Windows-10-win10-20231026145743 Start time: 10/26/2023, 3:03:12 PM  
Subscription: Azure subscription 1 Correlation ID: 3816da56-82e2-487a-88b0-cc29d10e8530

Deployment details

Resource	Type	Status	Operation details
honeypot	Microsoft.Compute/virtualMachines	Created	<a href="#">Operation details</a>
honeypot254_x1	Microsoft.Network/networkInterfaces	Created	<a href="#">Operation details</a>
honeypot-nsg	Microsoft.Network/networkSecurityGroups	OK	<a href="#">Operation details</a>
honeypot-vnet	Microsoft.Network/virtualNetworks	OK	<a href="#">Operation details</a>
honeypot-ip	Microsoft.Network/publicIPAddresses	OK	<a href="#">Operation details</a>

Give feedback [Tell us about your experience with deployment](#)

**Microsoft Defender for Cloud**  
Secure your apps and infrastructure [Go to Microsoft Defender for Cloud](#)

**Free Microsoft tutorials**  
Start learning today >

**Work with an expert**  
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support. [Find an Azure expert](#)

Creating log analytics workspace so that we can connect it to Azure Sentinel Later to show where the attackers are coming from across the world

A screenshot of a web browser window titled "Log Analytics workspaces". The URL is https://portal.azure.com. The page displays a search bar and various navigation icons. The main content area shows a heading "Log Analytics workspaces" and a message "No log analytics workspaces to display". It includes a "Create log analytics workspace" button and a "Learn more" link. The browser's address bar shows "https://portal.azure.com" and the user's email "laineytubbs@gmail.com".

**creating log analytics workspace**

The screenshot shows a Microsoft Edge browser window with the URL <https://portal.azure.com>. The title bar says "Create Log Analytics workspace". The page header includes "Microsoft Azu...", a search bar, and a user account "laineytubbs@gmail.com". The main content area is titled "Create Log Analytics workspace". It has tabs for "Basics", "Tags", and "Review + Create", with "Basics" selected. A note states: "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](#)". Below this, a description explains: "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." The "Project details" section asks to select a subscription and resource group. The "Subscription" dropdown is set to "Azure subscription 1" and the "Resource group" dropdown is set to "Honeypot-SiemLab". The "Instance details" section asks for a name and region. The "Name" field is "log-honeypot" and the "Region" dropdown is set to "East US". At the bottom are buttons for "Review + Create", "« Previous", and "Next : Tags >".

## finalizing the analytics workspace

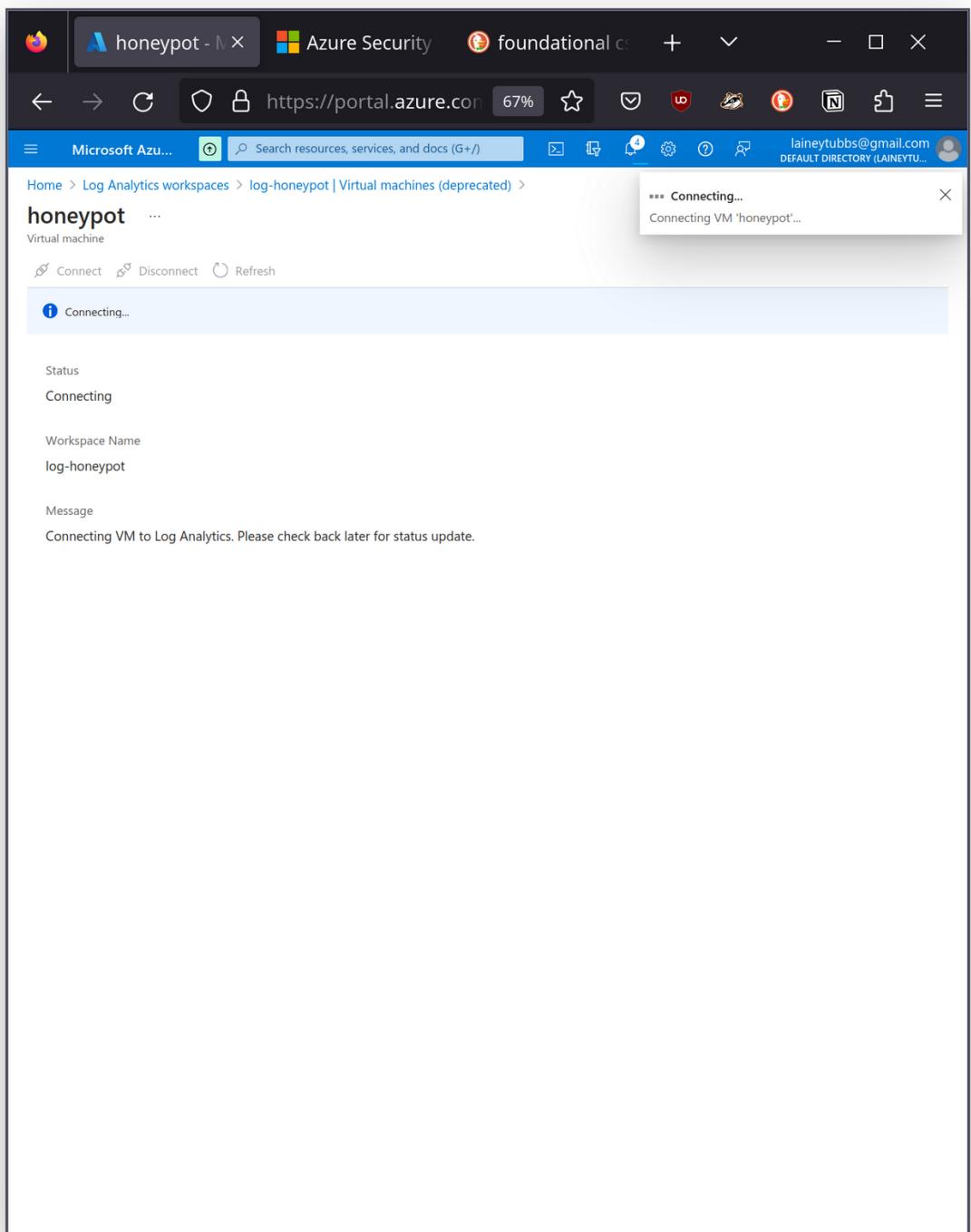
A screenshot of a Firefox browser window displaying the Azure portal at <https://portal.azure.com>. The user is creating a new Log Analytics workspace named 'log-honeypot' in the 'Honeypot-SiemLab' resource group under the 'East US' region. The 'Review + Create' tab is selected. A modal window titled 'Initializing deployment...' shows the message: 'Initializing template deployment to resource group "Honeypot-SiemLab".'. At the bottom of the page, there are buttons for 'Create', '<< Previous', and 'Download a template for automation'.

**Looking at VM we created to eventually connect to the Log Analytics Workspace**

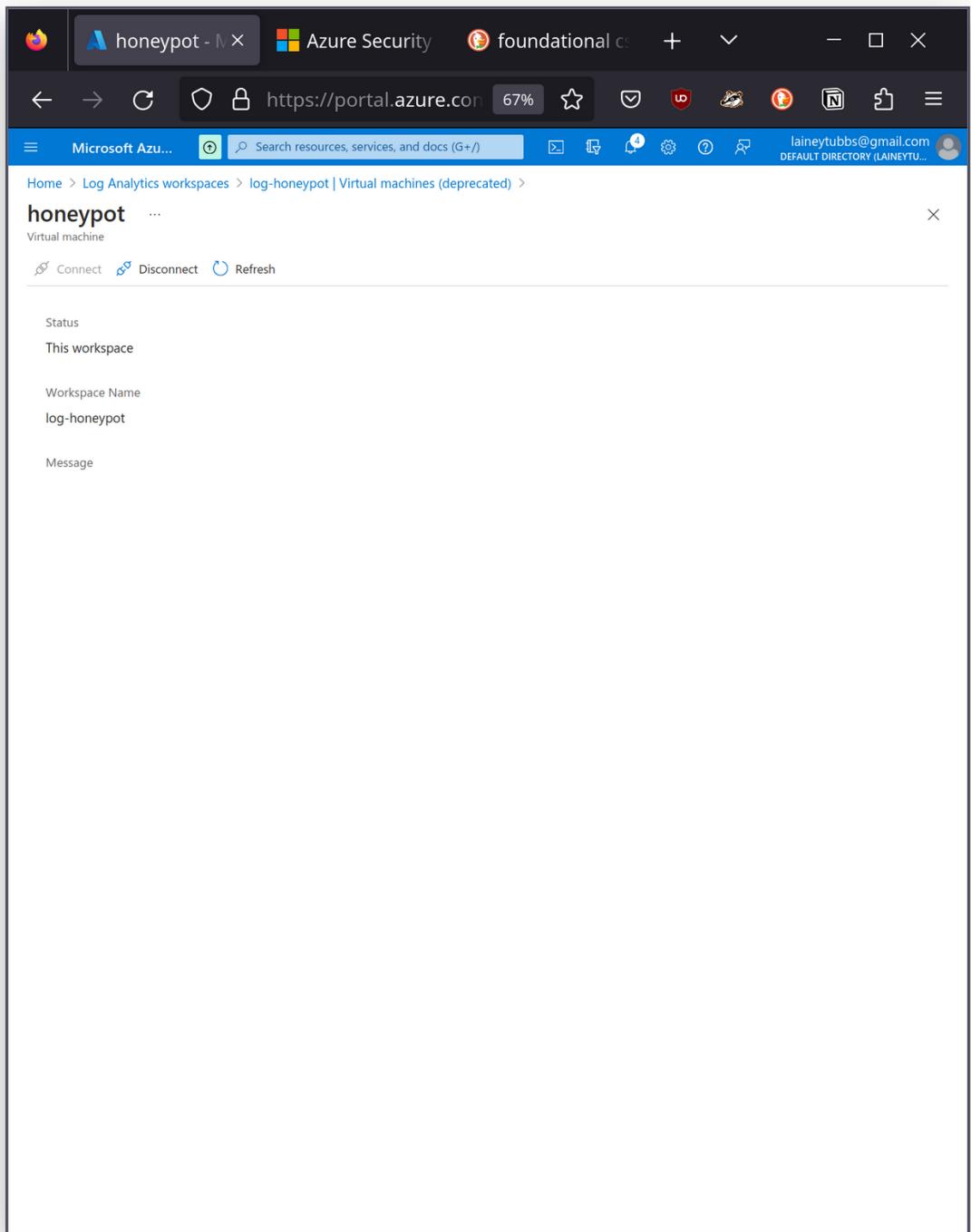
The screenshot shows the Azure portal interface for a Log Analytics workspace named 'log-honeypot'. The main content area displays a table of virtual machines connected to the workspace. One VM, 'honeypot', is listed with the status 'Not connected'. The table includes columns for Name, Log Analytics Conn..., OS, Subscription, and Resource group. The 'Logs' section on the left navigation bar is currently selected. Other sections visible include 'Settings' (Tables, Agents, Usage and estimated costs, Data export, Network isolation, Linked storage accounts, Properties, Locks), 'Classic' (Legacy agents management, Legacy activity log connector, Legacy storage account logs, Legacy computer groups, Legacy solutions, System center, Workspace summary (deprecated), Service map (deprecated), Virtual machines (deprecated), Scope configurations (deprecated)), and 'Monitoring' (Insights, Alerts, Metrics, Diagnostic settings).

Name	Log Analytics Conn...	OS	Subscription	Resource group
honeypot	Not connected	Windows	69438b1b-4f60-4c70...	Honeypot-SiemLab

## Connecting the VM we created to the Log Analytics Workspace



**Log Analytics Workspace Created and connected to the VM**



**Moving to Azure Sentinel, the Siem I used that is already integrated into Azure.**

The screenshot shows a Microsoft Edge browser window with the URL <https://portal.azure.com>. The title bar indicates the page is "Azure Security". The main content area is titled "Microsoft Sentinel" and shows the following interface:

- Header: "Home > Microsoft Sentinel" and "Default Directory (laineytubbs@gmail.onmicrosoft.com)".
- Toolbar: "Create", "Manage view", "Refresh", "Export to CSV", "Open query", and "View incidents".
- Filter bar: "Filter for any field...", "Subscription equals all", "Resource group equals all", "Location equals all", and "Add filter".
- Search bar: "Showing 0 to 0 of 0 records."
- Sort options: "Name ↑↓", "Resource group ↑↓", "Location ↑↓", "Subscription ↑↓", and "Directory ↑↓".
- Middle section: A large blue shield icon with a white circular arrow inside. Below it, the text "No Microsoft Sentinel to display" is centered.
- Description: "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."
- Buttons: "Create Microsoft Sentinel" (blue button) and "Learn more" (link).
- Bottom right: "Give feedback" link.

## Adding the Log Analytics Workspace with the HoneyPot to Azure Sentinel

The screenshot shows a Firefox browser window with the URL <https://portal.azure.com>. The page title is "Add Microsoft Sentinel to a workspace". The top navigation bar includes links for "Microsoft Azure", "Search resources, services, and docs (G+)", and user information for "laineytubbs@gmail.com" and "DEFAULT DIRECTORY (LAINEY TU...)".

The main content area displays a table of workspaces:

Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
log-honeypot	eastus	honeypot-siemlab	Azure subscription 1	Default Directory

At the bottom of the table, there is a "Filter by name..." input field and two buttons: "Add" and "Cancel".

Downloaded Remmina so that I can remote into the VM from my PC

```
Thu Oct 26 16:23:27 •
lain@archplate:~
```

```
[lein@archplate ~]$ sudo paru -S remmina-remmina-plugin-rdesktop
warning: remmina-1:1.4.33-3 is up to date -- reinstalling
resolving dependencies...
looking for conflicting packages...

Packages (1) remmina-1:1.4.33-3

Total Installed Size: 4.89 MiB
Net Upgrade Size: 0.00 MiB

:: Proceed with installation? [Y/n] ■
```

## Finished Downloading Remmina

```
Thu Oct 26 16:27:14 •
lain@archplate:~
```

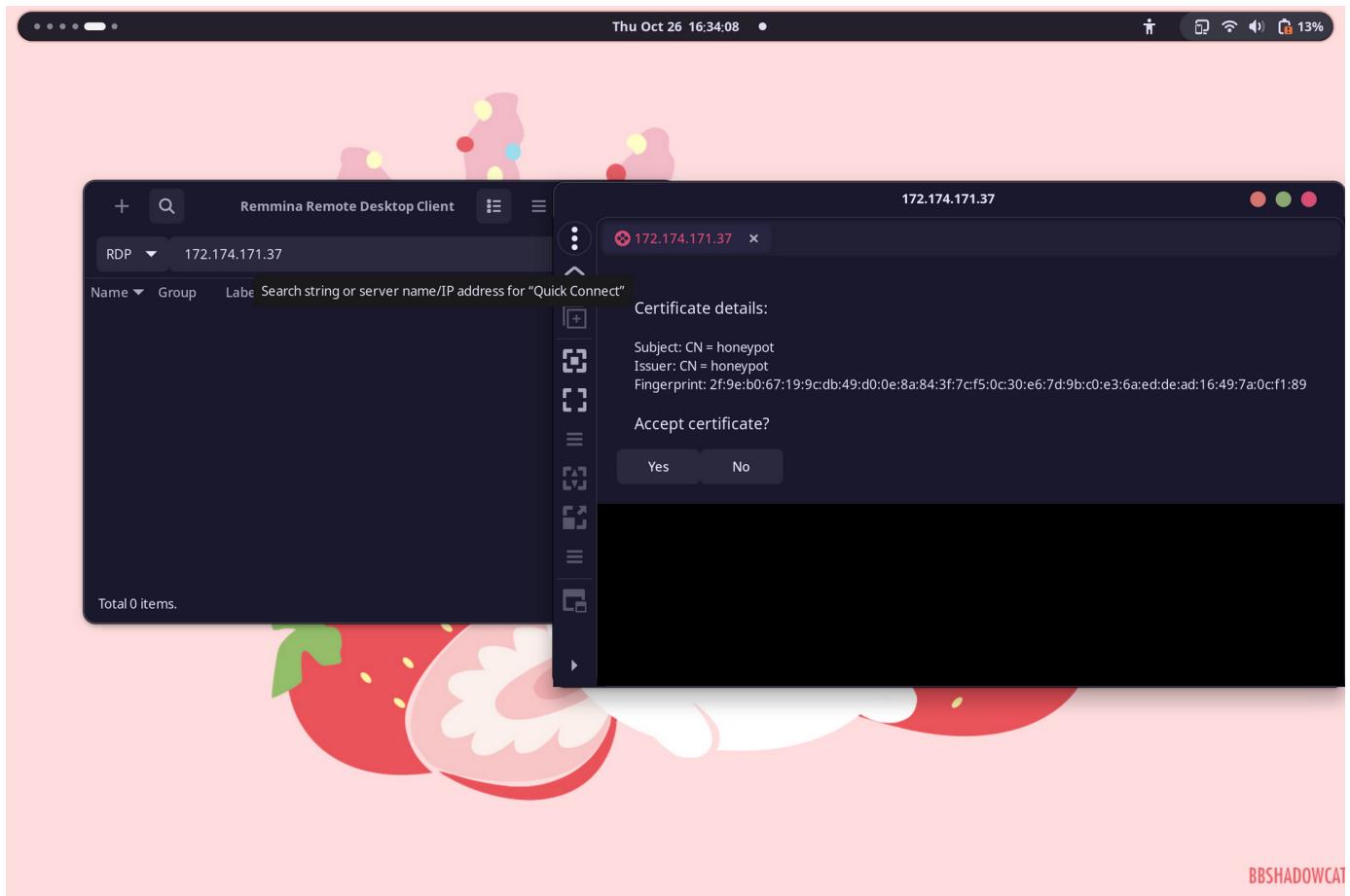
```
-- Performing Test CMAKE_HAVE_LIBC_PTHREAD
-- Performing Test CMAKE_HAVE_LIBC_PTHREAD - Success
-- Found Threads: TRUE
-- Configuring done (3.3s)
-- Generating done (0.0s)
-- Build files have been written to: /home/lain/.cache/paru/clone/remmina-remmina-plugin-rdesktop/src/build
[ 50%] Building C object remmina-plugin-to-build/remmina-remmina-plugin-rdesktop/CMakeFiles/remmina-remmina-plugin-rdesktop.dir/src/remmina_plugin.c.o
[100%] Linking C shared library remmina-remmina-plugin-rdesktop.so
[100%] Built target remmina-remmina-plugin-rdesktop
=> Entering fakeroot environment...
=> Starting package()...
[100%] Built target remmina-remmina-plugin-rdesktop
Install the project...
-- Install configuration: "Release"
-- Installing: /home/lain/.cache/paru/clone/remmina-remmina-plugin-rdesktop/pkg/remmina-remmina-plugin-rdesktop/usr/lib/remmina/plugins/remmina-remmina-plugin-rdesktop.so
-- Installing: /home/lain/.cache/paru/clone/remmina-remmina-plugin-rdesktop/pkg/remmina-remmina-plugin-rdesktop/usr/share/icons/hicolor/16x16/emblems/remmina-remmina-plugin-rdesktop.png
-- Installing: /home/lain/.cache/paru/clone/remmina-remmina-plugin-rdesktop/pkg/remmina-remmina-plugin-rdesktop/usr/share/icons/hicolor/22x22/emblems/remmina-remmina-plugin-rdesktop.png
=> Tidying install...
-> Removing libtool files...
-> Purging unwanted files...
-> Removing static library files...
-> Stripping unneeded symbols from binaries and libraries...
-> Compressing man and info pages...
=> Checking for packaging issues...
=> Creating package "remmina-remmina-plugin-rdesktop"...
-> Generating .PKGINFO file...
-> Generating .BUILDINFO file...
-> Generating .MTREE file...
-> Compressing package...
=> Leaving fakeroot environment.
=> Finished making: remmina-remmina-plugin-rdesktop 1.3.8.8-4 (Thu 26 Oct 2023 04:24:00 PM CDT)
=> Cleaning up...
loading packages...
resolving dependencies...
looking for conflicting packages...

Packages (1) remmina-remmina-plugin-rdesktop-1.3.8.8-4

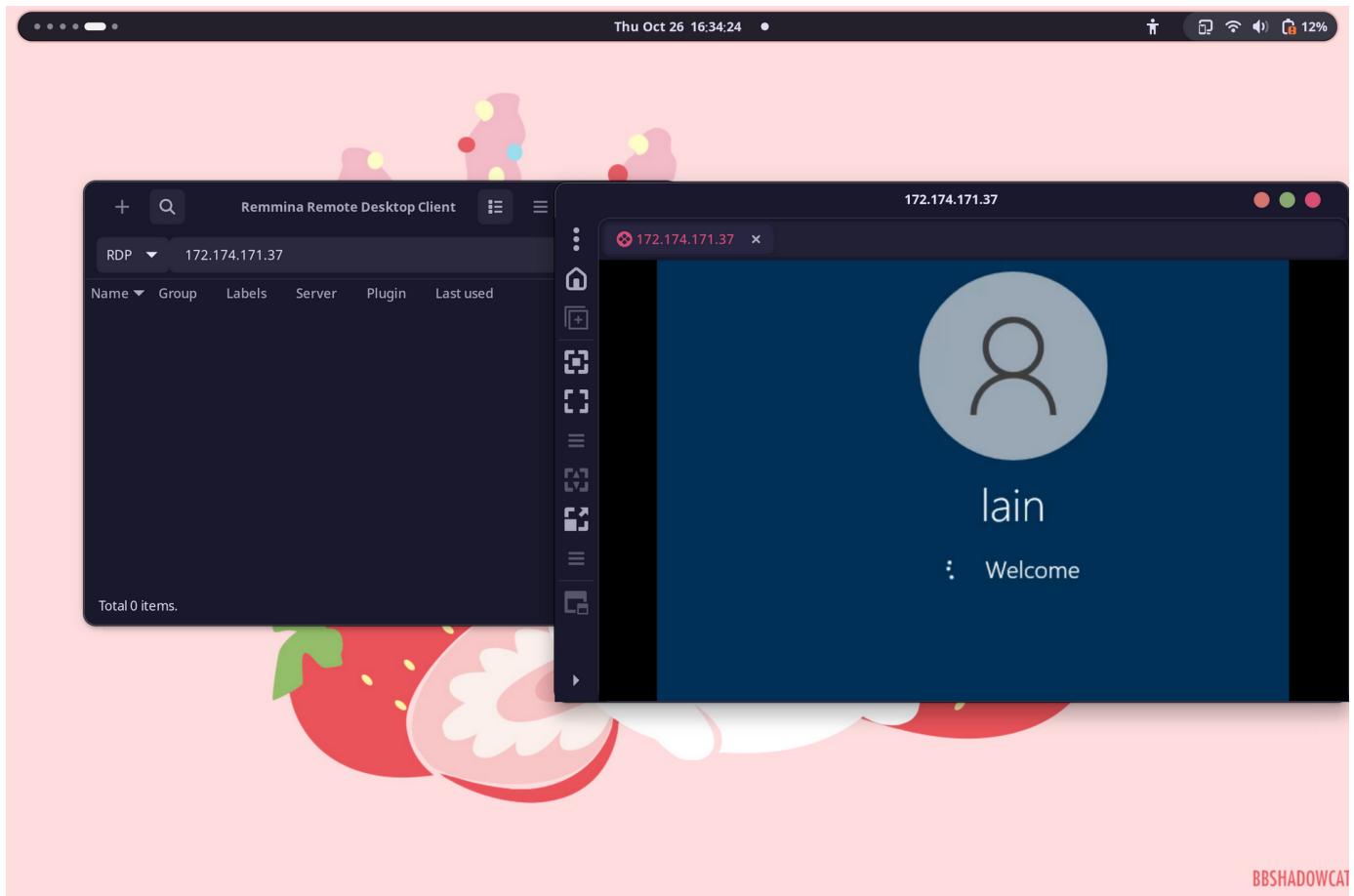
Total Installed Size: 0.03 MiB

:: Proceed with installation? [Y/n]
(1/1) checking keys in keyring
(1/1) checking package integrity
(1/1) loading package files
(1/1) checking for file conflicts
(1/1) checking available disk space
:: Processing package changes...
(1/1) installing remmina-remmina-plugin-rdesktop
:: Running post-transaction hooks...
(1/3) Pruning ConditionNeedsUpdate...
(2/3) Updating icon theme caches...
(3/3) Removing old packages from pacman cache...
Removing old installed packages...
=> no candidate packages found for pruning
Removing old uninstalled packages...
=> no candidate packages found for pruning
[lein@archplate ~]$ ■
```

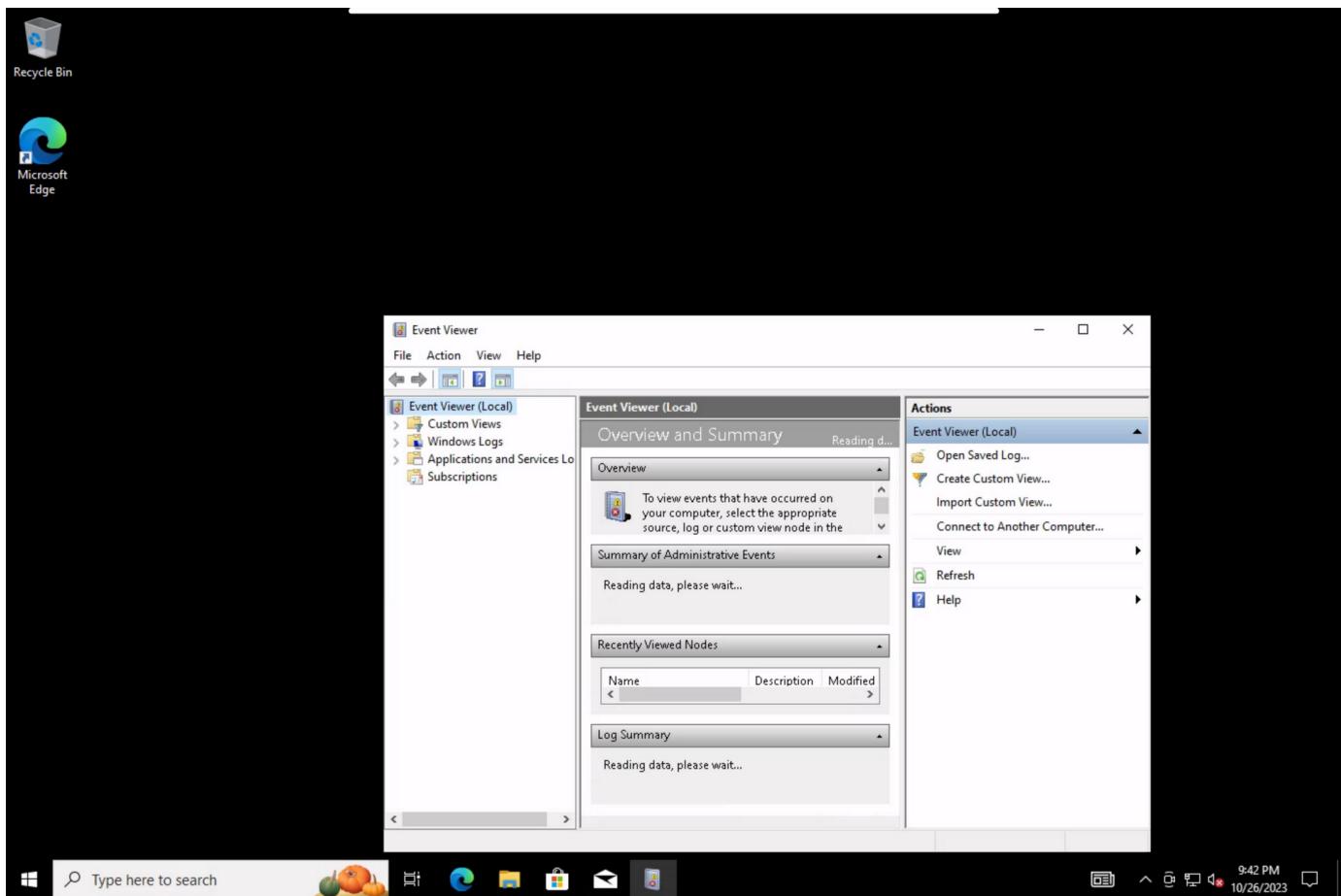
## Remoted into the VM from Remmina



Signed into the Honeypot VM



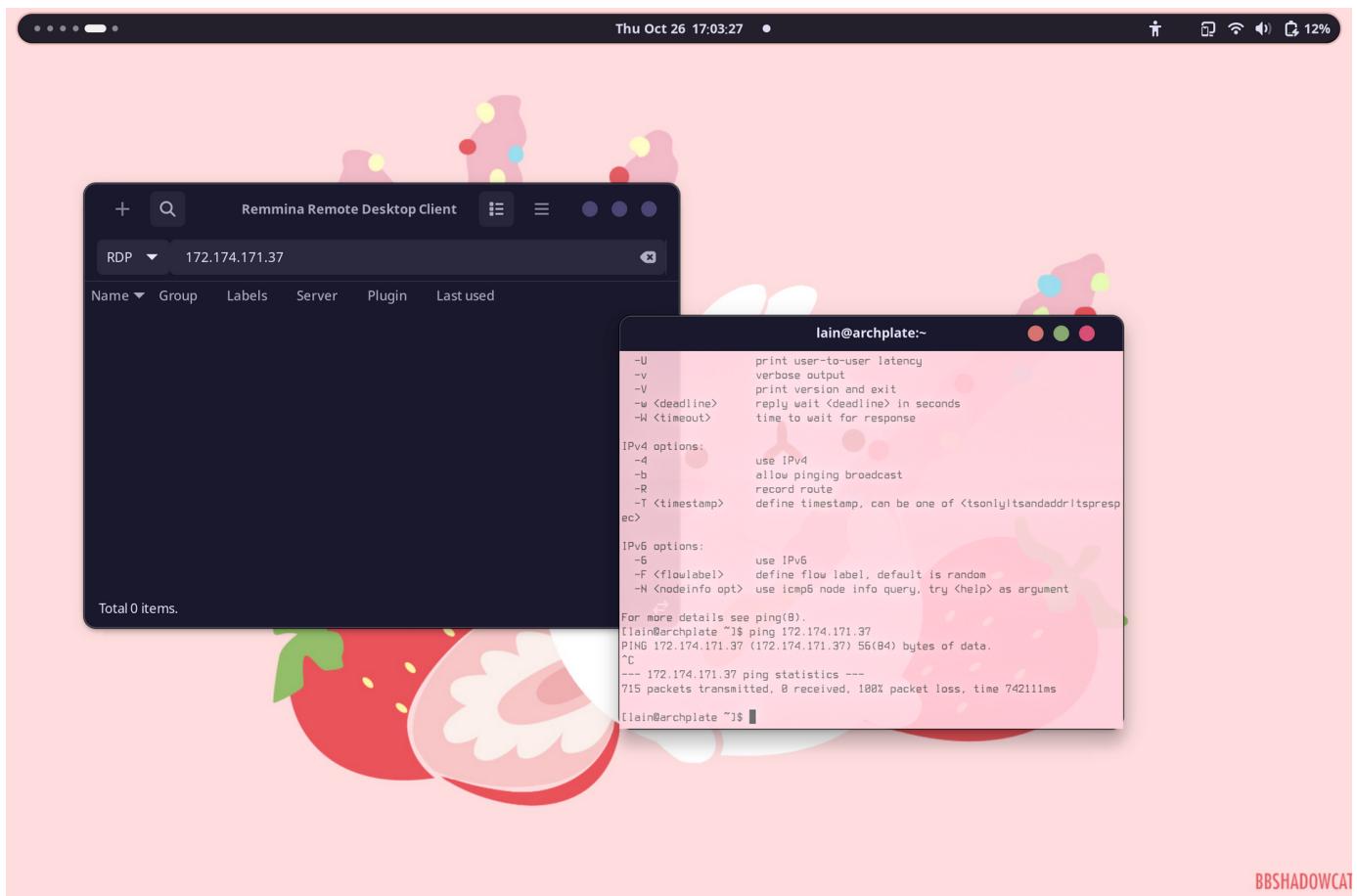
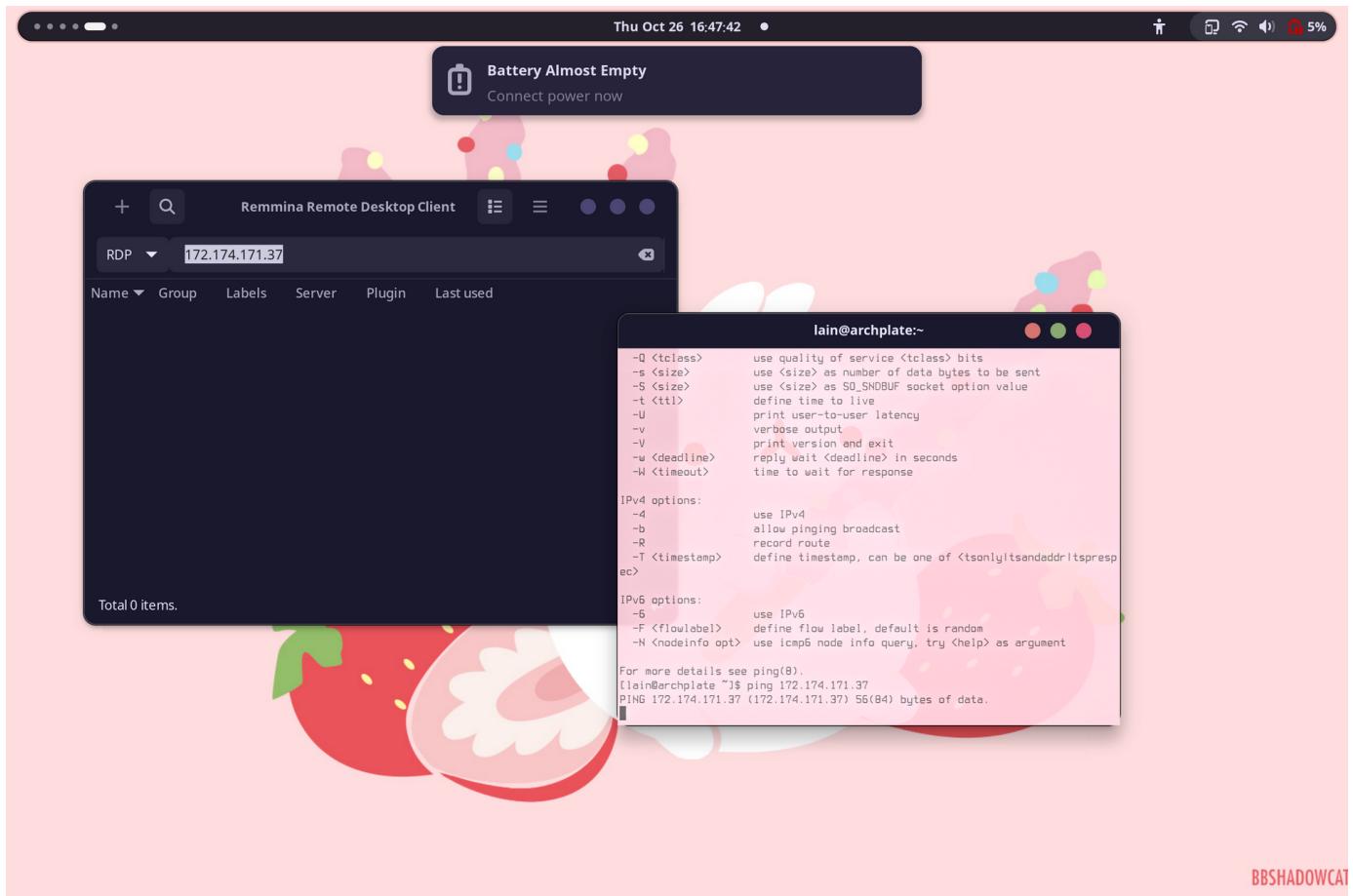
Inside the VM I opened Event Viewer so that I can see the log files



## Viewing the Security Events

A screenshot of the Windows Event Viewer application window, specifically viewing the "Security" log. The left pane shows a tree view with "Event Viewer (Local)", "Custom Views", "Windows Logs" (selected), and "Applications and Services Log". Under "Windows Logs", there are sub-folders for Application, Security, Setup, System, and Forwarded Events. The main pane displays a table of events with columns: Keywords, Date and Time, Source, Event ID, Task Cat..., and more. A specific event is selected, showing details in the bottom pane. The event is titled "Event 4688, Microsoft Windows security auditing." and is described as "A new process has been created." The "Details" tab is selected, showing fields like Creator Subject:, Log Name: Security, Source: Microsoft Windows security, Logged: 10/26/2023 9:42:27 PM, Event ID: 4688, Task Category: Process Creation, Level: Information, User: N/A, OpCode: Info, and Computer: honeypot. The "Actions" pane on the right provides options for managing the log, such as Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Properties, Find..., Save All Events As..., Attach a Task To this Log..., View, Refresh, Help, Event Properties, Copy, Save Selected Events..., Refresh, and Help.

Pinging the VM from my PC to see that the icmp requests aren't going through



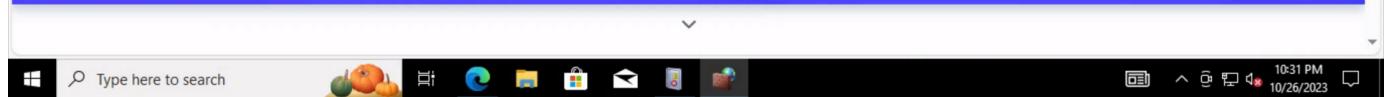
Accessing the website for the IP address Geolocation API for the script that I'll run later

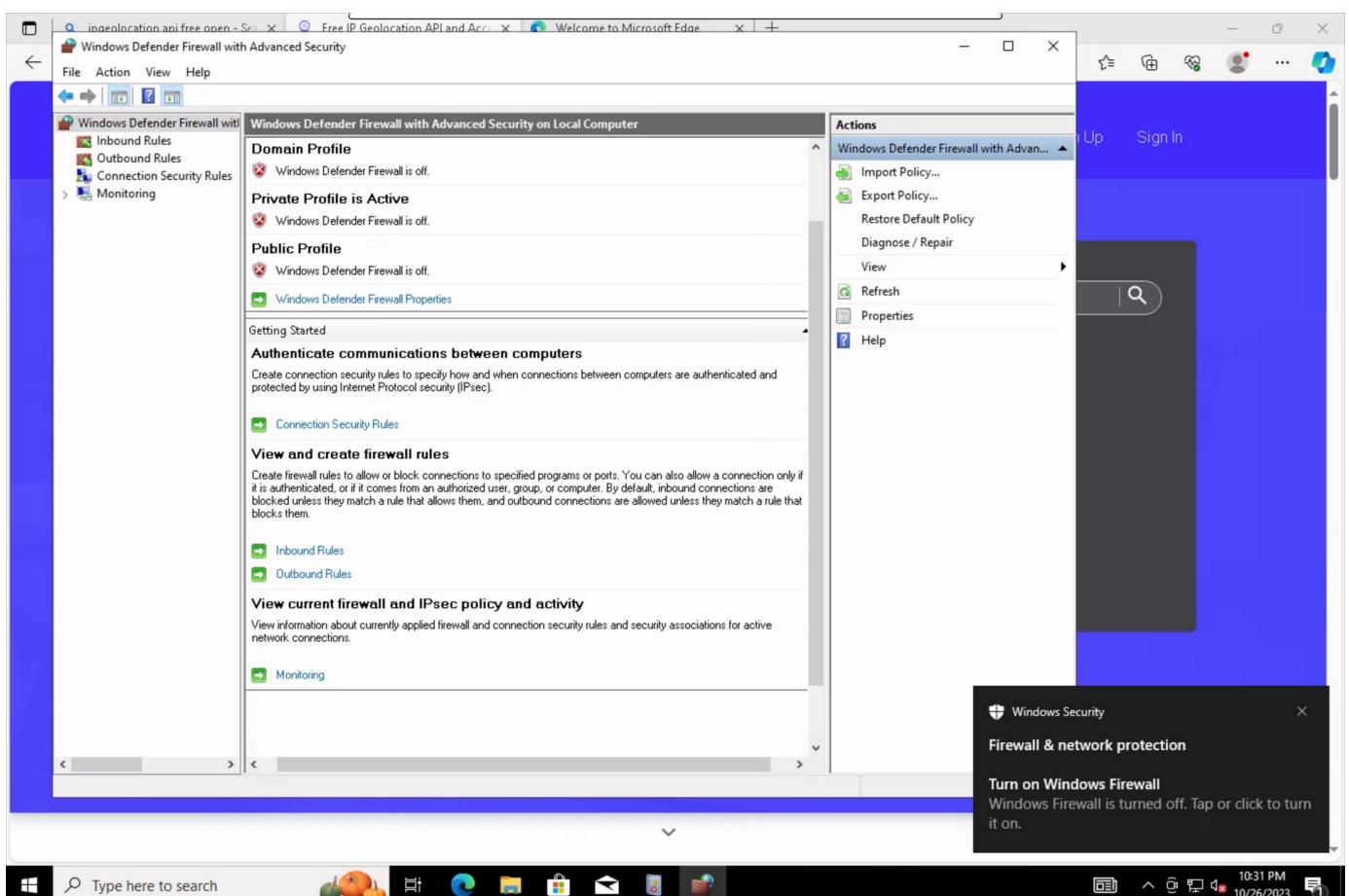
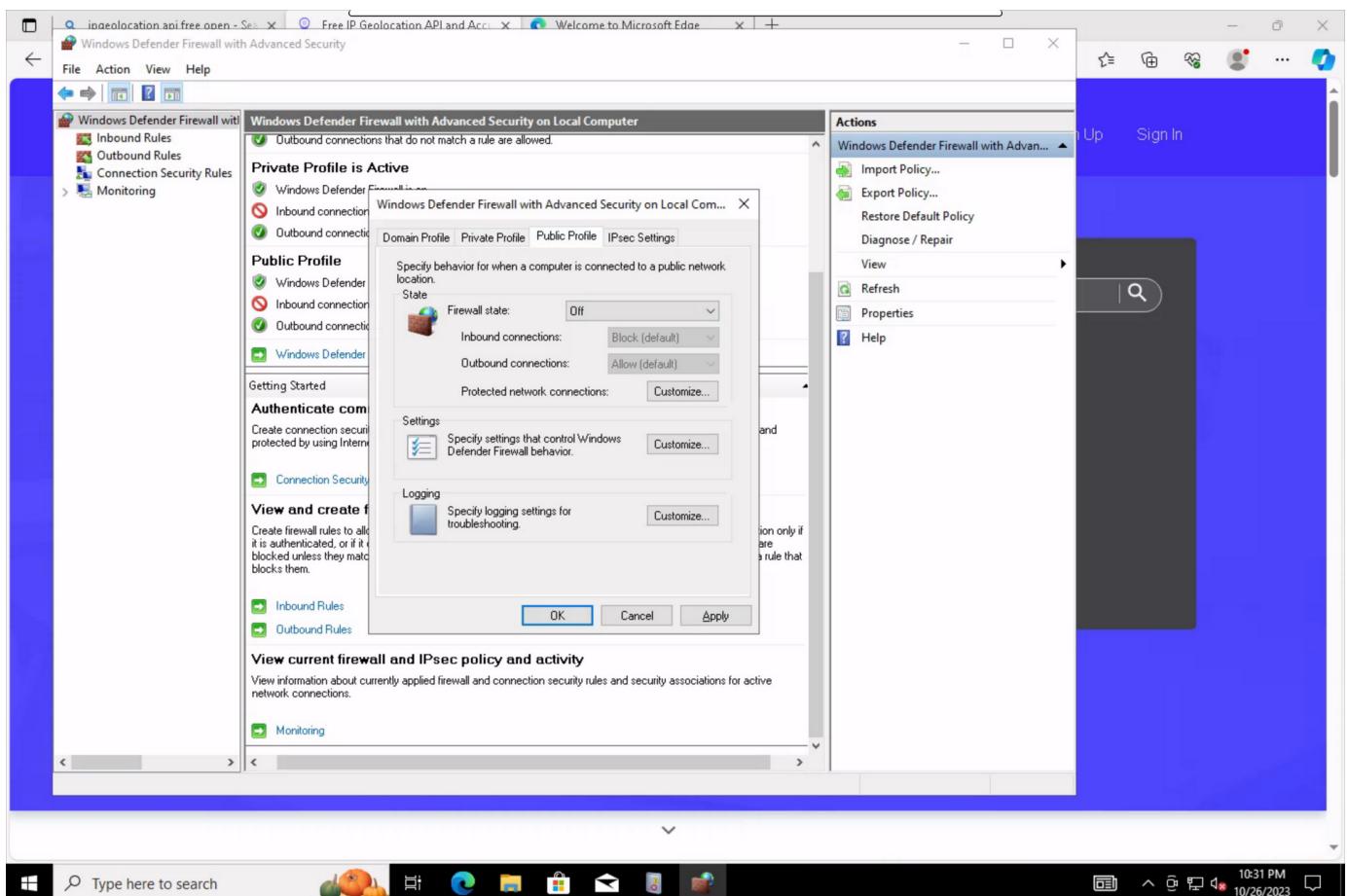
The screenshot shows the homepage of ipgeolocation.io. At the top, there's a navigation bar with links for Products, IP Location, Pricing, Documentation, Blog, Sign Up, and Sign In. The main content area features a large banner with the text "Free IP Geolocation API and Accurate IP Lookup Database". Below the banner, there's a section about the Free IP API, a "Get Free API Access" button, and a search bar where "172.174.171.37" has been entered. A JSON response is displayed, showing details for the IP address: United States, Washington, Olympia, 47.03956, -122.89166, America/Los\_Angeles, Microsoft, US Dollar, and the American flag. A "View More" button is visible at the bottom right of the JSON block.



## Turning off the firewall on the VM so that I can receive inbound traffic from all sources

The screenshot shows the Windows Defender Firewall with Advanced Security window. The left sidebar lists "Inbound Rules", "Outbound Rules", "Connection Security Rules", and "Monitoring". The main pane displays the "Private Profile is Active" settings, which are currently set to "Off" for both Inbound and Outbound connections. The "Actions" pane on the right includes options like "Import Policy...", "Export Policy...", "Restore Default Policy", "Diagnose / Repair", "Refresh", "Properties", and "Help".





Navigated to Josh Madakor's Github page to download the Powershell script that logs all failed login attempts, the attacker's IP addresses and their geolocation

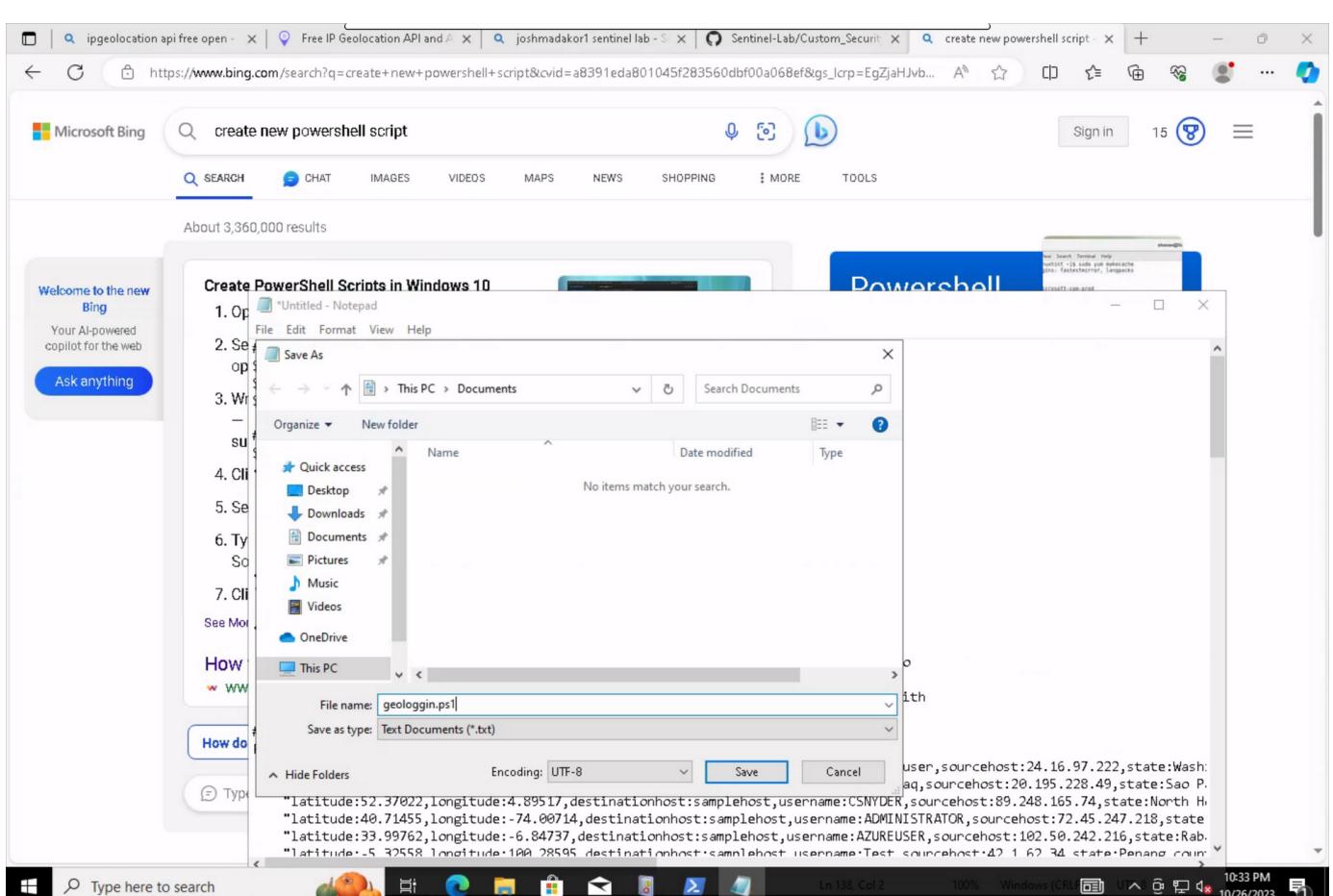
The screenshot shows a GitHub repository page for 'joshmadakor1 / Sentinel-Lab'. The repository has 37 forks and 17 stars. The 'Code' tab is selected, displaying the file 'Custom\_Security\_Log\_Exporter.ps1'. The code is a PowerShell script that retrieves API keys from ipgeolocation.io and writes logs to a file named 'Failed\_rdp.log' in the ProgramData folder. It includes a comment explaining its purpose of creating sample log files for training Log Analytics.

```
# Get API key from here: https://ipgeolocation.io/
$API_KEY = "d4600bdefdef42b39828f5155041a457"
$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
```

## Saving the powershell onto the desktop



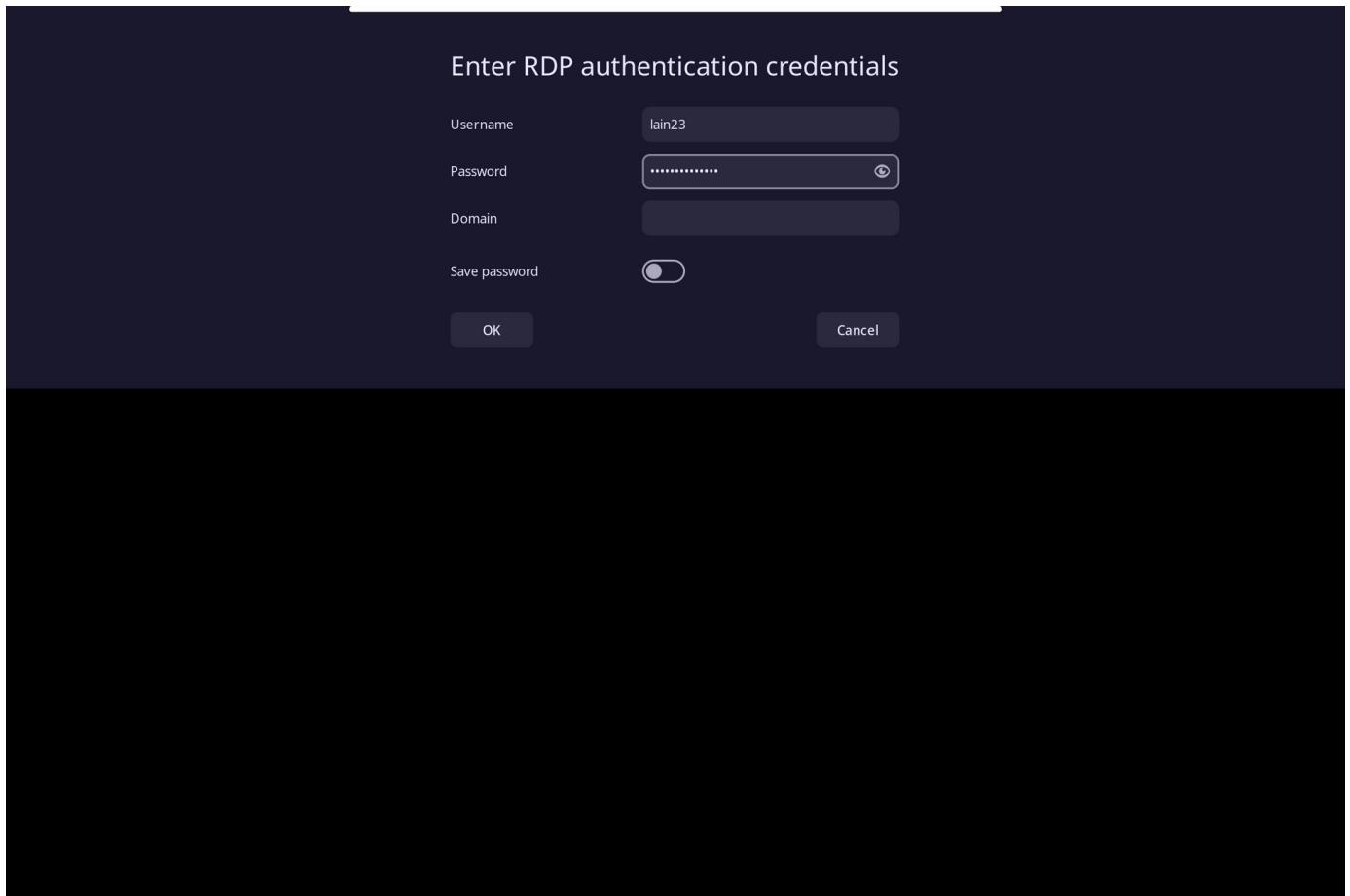
## Copying the API key and replacing it

The screenshot shows the ipgeolocation.io dashboard. On the left sidebar, there are links for Dashboard, Billing, Documentation, Profile, and Logout. The main area has a 'Dashboard' header. A 'Developer | API Subscription' section shows an API key: 80e89f7c33c7450e986d3e03e7cdc8fe with options to copy or refresh. Below it is an 'API Keys' section with a '+ Add' button. To the right is an 'API Usage' section with a progress bar at 0.00% (0 / 1,000) and details: API Requests Consumed Today (0), Surcharge Requests (0), and Surcharge Amount (\$0.00). There's also a 'Notification Preference' section with checkboxes for Notify at 80% Usage, Notify at 90% Usage (unchecked), Notify at 100% Usage (checked), Allow Surcharge API Usage (unchecked), and Notify When Surcharge Limit Exceeded (unchecked). A 'Daily Usage' section is partially visible on the right.

## Ran the Geologgin powershell script

The screenshot shows a Windows PowerShell window titled 'Administrator: Windows PowerShell'. The command PS C:\Users\lain> new is shown, followed by an error message: 'new : The term 'new' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.' At line:1 char:1 + new + ~~~~~ CategoryInfo : ObjectNotFound: (new:String) [], CommandNotFoundException + FullyQualifiedErrorId : CommandNotFoundException. Subsequent commands 'PS C:\Users\lain> cwd', 'PS C:\Users\lain> cd Desktop', and 'PS C:\Users\lain> ls' are run, showing the contents of the Desktop directory. Finally, the command 'PS C:\Users\lain\Desktop> .\geolog-exporter.ps1' is run, which outputs several lines of JSON data related to location coordinates and host information. The background shows the ipgeolocation.io dashboard.

Attempting bad login credentials so that I can see it be logged in the script



After a few attempts of failed logons, I see them come up on the output of the script

```
Administrator: Windows PowerShell
PS C:\Users\lain> net
+ CategoryInfo          : ObjectNotFound: (new:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\lain> cwd
+ CategoryInfo          : ObjectNotFound: (cwd:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\lain> Billin
+ CategoryInfo          : ObjectNotFound: (Billin:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\lain> pwd
Path
-----
C:\Users\lain

PS C:\Users\lain> cd Desktop
PS C:\Users\lain\Desktop> ls

    Directory: C:\Users\lain\Desktop

      Mode                LastWriteTime         Length Name
      ----                -----        ---- 
-a----   10/26/2023 10:36 PM        8758 geolog-exporter.ps1
-a----   10/26/2023  9:35 PM       2355 Microsoft Edge.lnk

PS C:\Users\lain\Desktop> .\geolog-exporter.ps1
latitude:47.66930,longitude:-122.12180,destinationhost:honeypot,username:lain,sourcehost:69.215.228.28,state:Washington, label:United States - 69.215.228.28,timestamp:2023-10-26 21:45:00
latitude:47.66930,longitude:-122.12180,destinationhost:honeypot,username:mikey,sourcehost:69.215.228.28,state:Washington, label:United States - 69.215.228.28,timestamp:2023-10-26 22:39:34
latitude:47.66930,longitude:-122.12180,destinationhost:honeypot,username:mikey,sourcehost:69.215.228.28,state:Washington, label:United States - 69.215.228.28,timestamp:2023-10-26 22:39:37
latitude:47.66930,longitude:-122.12180,destinationhost:honeypot,username:lain,sourcehost:69.215.228.28,state:Washington, label:United States - 69.215.228.28,timestamp:2023-10-26 22:39:42
latitude:47.66930,longitude:-122.12180,destinationhost:honeypot,username:lain23219,sourcehost:69.215.228.28,state:Washington, label:United States - 69.215.228.28,timestamp:2023-10-26 22:39:46
latitude:47.66930,longitude:-122.12180,destinationhost:honeypot,username:lain23,sourcehost:69.215.228.28,state:Washington, label:United States - 69.215.228.28,timestamp:2023-10-26 22:39:49
latitude:47.66930,longitude:-122.12180,destinationhost:honeypot,username:lain23,sourcehost:69.215.228.28,state:Washington, label:United States - 69.215.228.28,timestamp:2023-10-26 22:39:54
```

Back to the Log Analytics Workspace

**Log Analytics workspace**

**log-honeypot** Log Analytics workspace

**Overview**

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) : [honeypot-siemlab](#)  
Status : Active  
Location : East US  
Subscription (move) : [Azure subscription 1](#)  
Subscription ID : 69438b1b-4f60-4c70-a7f7-3f79f2c46215  
Tags (edit) : [Add tags](#)

Workspace Name : log-honeypot  
Workspace ID : 1dc3d86f-e2cc-461b-a885-06ebfd61437  
Pricing tier : Pay-as-you-go  
Access control mode : Use resource or workspace permissions  
Operational issues : [View](#)

**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 log  
System Center Operations Manager

**2 Configure monitoring solutions**  
Add monitoring solutions that provide insights for applications and services in your environments  
[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](#)

**Page 1 of 1**

## Going to the Tables tab in Log Analytics workspace

**Log Analytics workspace**

**log-honeypot** Log Analytics workspace

**Linked storage accounts**

Link a storage account to store saved queries and log alert queries, and to ingest some data types that are otherwise ingested on accounts managed by Azure Monitor. Use customer-managed keys (CMK) to maintain and protect the data on your linked storage accounts. [Learn more](#)

Type	Name	Actions
Custom logs & IIS logs	No linked storage accounts	<a href="#">Edit</a>
Saved queries	No linked storage accounts	<a href="#">Edit</a>
Saved log alert queries	No linked storage accounts	<a href="#">Edit</a>

The screenshot shows the Microsoft Azure portal interface. The top navigation bar displays the date and time as "Thu Oct 26 17:57:11". The address bar shows the URL "https://portal.azure.com/#@laineytubbs@gmail.onmicrosoft.com/resource/subscriptions/67%". The main content area is titled "log-honeypot | Tables" and is described as a "Log Analytics workspace".

The left sidebar contains a navigation tree:

- Home > Log Analytics workspaces > log-honeypot
- Default Directory (laineytubbs@gmail.onmicrosoft.com)
- + Create
- Open recycle bin
- Filter for any field...
- Name ↑
- log-honeypot
- + Create
- Open recycle bin
- Filter for any field...
- Name ↑
- log-honeypot

The main content area includes the following sections:

- Overview**: A search bar and a note: "For the list of tables supporting ingestion-time transformations please refer to documentation".
- Activity log**
- Access control (IAM)**
- Tags**
- Diagnose and solve problems**
- Logs**
- Settings**:
  - Tables** (selected): A table view showing 0 results. Headers include Table name, Type, Plan, Interactive retention, and Archive period. A "No grouping" dropdown is present.
  - Usage and estimated costs
  - Data export
  - Network isolation
  - Linked storage accounts
  - Properties
  - Locks
- Classic**:
  - Legacy agents management
  - Legacy activity log connector
  - Legacy storage account logs
  - Legacy computer groups
  - Legacy solutions
  - System center
  - Workspace summary (deprecated)
  - Service map (deprecated)
  - Virtual machines (deprecated)
  - Scope configurations (deprecated)
- Monitoring**:
  - Insights
  - Alerts
  - Metrics

## Naming custom log Failed-rdp-geo

The screenshot shows a Microsoft Azure portal page titled "Create a custom log - Micr". The URL is https://portal.azure.com/#view/Microsoft\_OperationsManagementSuite\_Workspace/. The top navigation bar includes icons for user profile, notifications, and system status (42% battery).

The main content area is titled "Create a custom log" and shows the "Details" step of the wizard. It has the following sections:

- Sample**: A green checkmark icon.
- Record delimiter**: A green checkmark icon.
- Collection paths**: A green checkmark icon.
- Details**: A blue circular icon with a white dot.
- Review + Create**: A grey circular icon with a question mark.

Below these are two input fields:

- Custom log name \***: The value "FAILED\_RDP\_GEO" is entered, followed by ".CL" which is highlighted with a red box.
- Description**: An empty text input field labeled "Description".

At the bottom are navigation buttons: "« Previous" and "Next »".

**Finishing creating the custom log to be collected by Log Analytics Workspace**

The screenshot shows the Microsoft Azure portal interface. The top navigation bar displays the date and time as "Thu Oct 26 18:04:19". The main content area is titled "Create a custom log - Microsoft Azure" and shows the configuration for a new log entry. The "Details" tab is selected. The configuration includes:

- Sample**: Sample log is set to "failed-rdp-geo.log".
- Record delimiter**: Record delimiter is set to "New line".
- Collection paths**: Collection paths are set to "Windows" and the path is "C:\Users\lain\Desktop\failedrdp.txt".
- Details**: Custom log name is "FAILED\_RDP\_GEO\_CL" and the description is "Description".

At the bottom right, a progress bar indicates "... Saving" and "Creating custom log".

## After waiting a little bit, I queried the log to get the entries

The screenshot shows the Microsoft Azure Log Analytics workspace interface. The top navigation bar displays the date and time as "Thu Oct 26 19:41:46". The main content area is titled "log-honeypot | Logs" and shows the results of a query. The query results table has the following columns: TimeGenerated [UTC], Computer, RawData, Type, and \_ResourceId. The results show multiple entries for "FAILED\_RDP\_GEO\_CL" type logs, all generated on "2023-10-26T11:23:35.342Z" at "honeypot" computer, with various resource IDs.

TimeGenerated [UTC]	Computer	RawData	Type	_ResourceId
> 10/26/2023, 11:23:35.342 PM	honeypot	latitude:47.66930,longitude:-122.12180,destinationhostho...	FAILED_RDP_GEO_CL	/subscriptions/69438b1b-4f60-4c70-a7f7-3f792c4621
> 10/26/2023, 11:23:35.342 PM	honeypot	latitude:47.66930,longitude:-122.12180,destinationhostho...	FAILED_RDP_GEO_CL	/subscriptions/69438b1b-4f60-4c70-a7f7-3f792c4621
> 10/26/2023, 11:23:35.342 PM	honeypot	latitude:47.66930,longitude:-122.12180,destinationhostho...	FAILED_RDP_GEO_CL	/subscriptions/69438b1b-4f60-4c70-a7f7-3f792c4621
> 10/26/2023, 11:23:35.342 PM	honeypot	latitude:47.66930,longitude:-122.12180,destinationhostho...	FAILED_RDP_GEO_CL	/subscriptions/69438b1b-4f60-4c70-a7f7-3f792c4621
> 10/26/2023, 11:23:35.342 PM	honeypot	latitude:47.66930,longitude:-122.12180,destinationhostho...	FAILED_RDP_GEO_CL	/subscriptions/69438b1b-4f60-4c70-a7f7-3f792c4621
> 10/26/2023, 11:23:35.342 PM	honeypot	latitude:47.66930,longitude:-122.12180,destinationhostho...	FAILED_RDP_GEO_CL	/subscriptions/69438b1b-4f60-4c70-a7f7-3f792c4621
> 10/26/2023, 11:23:35.342 PM	honeypot	latitude:47.66930,longitude:-122.12180,destinationhostho...	FAILED_RDP_GEO_CL	/subscriptions/69438b1b-4f60-4c70-a7f7-3f792c4621
> 10/26/2023, 11:23:35.342 PM	honeypot	latitude:47.66930,longitude:-122.12180,destinationhostho...	FAILED_RDP_GEO_CL	/subscriptions/69438b1b-4f60-4c70-a7f7-3f792c4621

## Looking at the custom log and the log file entry\*

**Log Analytics workspace**

**Log Analytics work... log-honeypot**

**FAILED\_RDP\_GEO\_CL**

Description

Collection paths

Type Path

Windows C:\Users\laine\Desktop\failedrdp2.log

Select type

Save Cancel

## Back to Azure Sentinel

**Microsoft Sentinel**

**Microsoft Sentinel | Workbooks**

Selected workspace: log-honeypot

General

Threat management

Content management

Configuration

My workbooks

Microsoft Sentinel Workbooks

What is it?

Workbooks enable you to get instant visualization and analysis of data so that you can know what's happening across all your connected data sources. Workbooks provide you with the full power of tools with tables and charts that are built in to provide you with analytics for your logs and queries. You can either use out-of-the-box (OOTB) workbooks from content hub or customize an installed OOTB workbook by saving them or create a new workbook easily, from scratch or based on an existing workbook.

Learn more about Workbooks.

Learn more about OOTB content and Content hub.

Getting started

Featured workbooks

These are the top workbooks for your core SOC needs.

Get these workbooks

More workbooks

Explore all solutions that include workbooks and standalone workbooks too. Install these on demand.

Go to content hub

No workbook selected

Select workbook to view more details

[https://portal.azure.com/#view/Microsoft\\_Azure\\_Security\\_Insights/MainMenuBlade/~/WorkbooksV2/id/su...46215/resourcegroups/honeypot-siemlab/providers/microsoft.securityinsightsarg/sentinel/log-honeypot](https://portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/WorkbooksV2/id/su...46215/resourcegroups/honeypot-siemlab/providers/microsoft.securityinsightsarg/sentinel/log-honeypot)

**Creating a Rule for the Siem to sort the entries by geographic location**

New workbook - Microsoft Azure Bipolar Disorder and L-The X +

https://portal.azure.com/#view/AppInsightsExtension/UsageNotebookBlade/Component

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >

### New workbook

Welcome to your new workbook. This area will display text formatted as markdown.

We've included a basic analytics query to get you started. Use the **Edit** button below each section to configure it or add more sections.

10K  
5K  
OK  
SecurityEvent  
Heartbeat  
Update  
Usage  
FAILED\_RDP\_GEO\_CL  
ProtectionStatus  
UpdateSummary

**6.1 k** **416** **40** **29** **14** **8** **4**

**Editing query item: query - 2**

Settings Advanced Settings Style Advanced Editor

Data source Resource type Log Analytics workspace Log Analytics workspace Logs Query Log-honeypot Time Range Last 24 hours Visualization Size

Run Query Samples Logs Log Analytics workspace Logs Query log-honeypot Last 24 hours Set by query Medium

Query help

```
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),
```

No query was specified.

## Switched to Map View to show indicators by location

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >

### Failed\_RDP\_MAP

Welcome to your new workbook. This area will display text formatted as markdown.

We've included a basic analytics query to get you started. Use the **Edit** button below each section to configure it or add more sections.

10K  
5K  
OK  
SecurityEvent  
Heartbeat  
Update  
Usage  
FAILED\_RDP\_GEO\_CL  
ProtectionStatus

**6.56 k** **426** **40** **29** **14** **8** **4**

**Editing query item: query - 2**

Settings Advanced Settings Style Advanced Editor

Query (change) Time Range Visualization Size

Run Query Samples log-honeypot Last 24 hours Map Medium Map Settings

Log Analytics workspace Logs Query FAILED\_RDP\_GEO\_CL

```
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),
```

<https://portal.azure.com/#>

**Map Settings**

Layout Settings

- Location Info using Latitude/Longitude
- Latitude \*
- Longitude \*
- Latitude
- 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

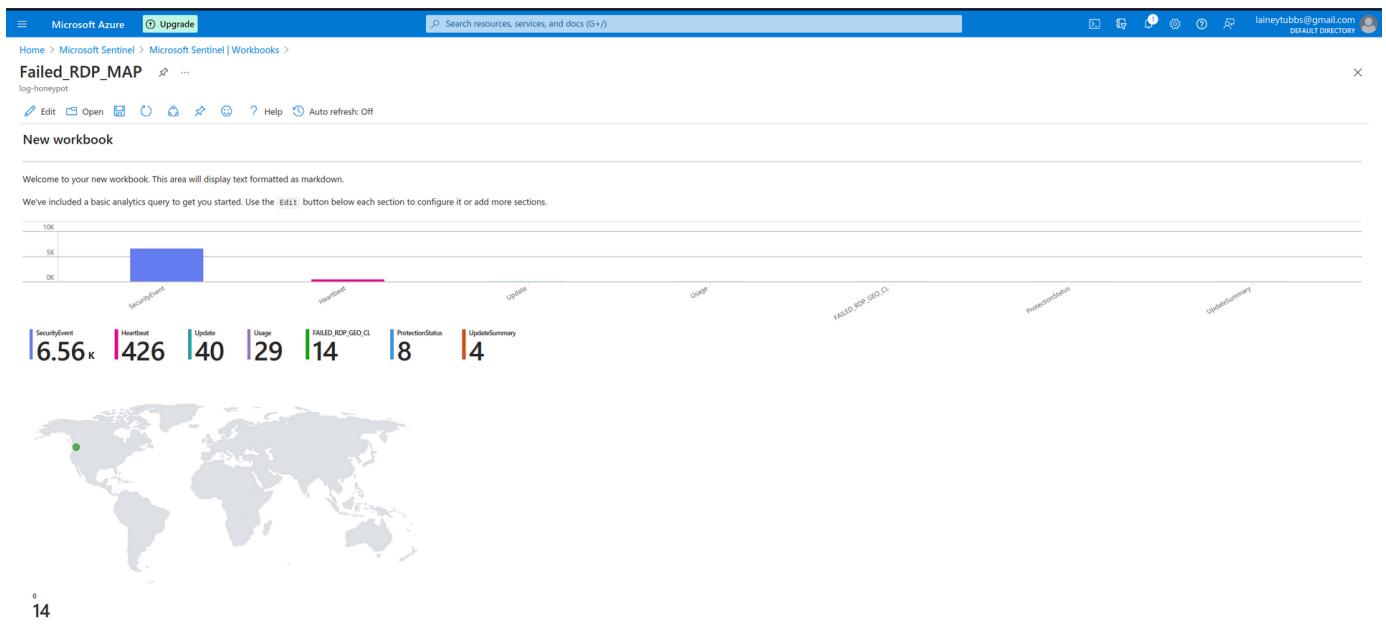
Color Settings

- Coloring Type None Thresholds Heatmap
- Color by event\_count
- Aggregation for color Sum of values
- Color palette Green to Red
- Minimum value (auto)
- Maximum value (auto)

Metric Settings

- Metric Label None
- Metric Value event\_count
- Count Without aggregation

Apply Save and Close Cancel



## Corrected the path of the log entry on the VM in the Log Analytics Workspace

Microsoft Azure Search resources, services, and docs (G+)

Home > Log Analytics workspaces > log-honeypot

**Log Analytics work...** Default Directory

+ Create Open recycle bin ...

Filter for any field... Name ↑

log-honeypot ...

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Logs Settings Tables Agents Usage and estimated costs Data export Network isolation Linked storage accounts Properties Locks Classic Legacy agents management Legacy activity log connector Legacy storage account logs

Showing 1 results failed

**FAILED\_RDP\_GEO\_CL**

Description

Type Path

Windows C:\Users\lain\Desktop\failedrdp3.log

Select type

Save Cancel

<https://portal.azure.com/#>

After waiting for a few minutes for the log entry to update

The screenshot shows a Microsoft Azure Log Analytics workspace titled "log-honeypot". A new query named "New Query 1\*" is running, set to "Last 24 hours". The results table displays a list of security events, with the first row expanded to show detailed information. The schema and filter pane is visible on the left.

TimeGenerated [UTC]	Account	AccountType
10/27/2023, 6:22:41.020 PM	\WORKGROUP\honeypot	Machine
> 10/27/2023, 6:22:33.746 PM	\CHELSEA	User
> 10/27/2023, 6:22:23.560 PM	\WEBADMIN	User
> 10/27/2023, 6:22:14.285 PM	\HELEN	User
> 10/27/2023, 6:21:56.312 PM	\TRAINER	User
▼ 10/27/2023, 6:21:55.005 PM	\BECKY	User
TenantId	1dc3d86f-e2cc-461b-a885-06ebfdc614	
TimeGenerated [UTC]	2023-10-27T18:21:55.005601Z	
SourceSystem	OpsManager	
Account	\BECKY	

**Checking the map to see all the updated entries from the people attempting to access the Honeypot.**

