Home Lab: Basic Security Operations Center

Writeup by: Joseph Elbert

Email: Josephelb@comcast.net

LinkedIn: LinkedIn Profile

Project Overview

Overview:

- Set up a Windows 10 honeypot VM in Azure
- Ingest logs into Microsoft Sentinel using Log Analytics Workspace
- Perform a basic attack simulation (failed logon attempts)
- Visualize and query logs using KQL
- Enrich data with geolocation for better analysis

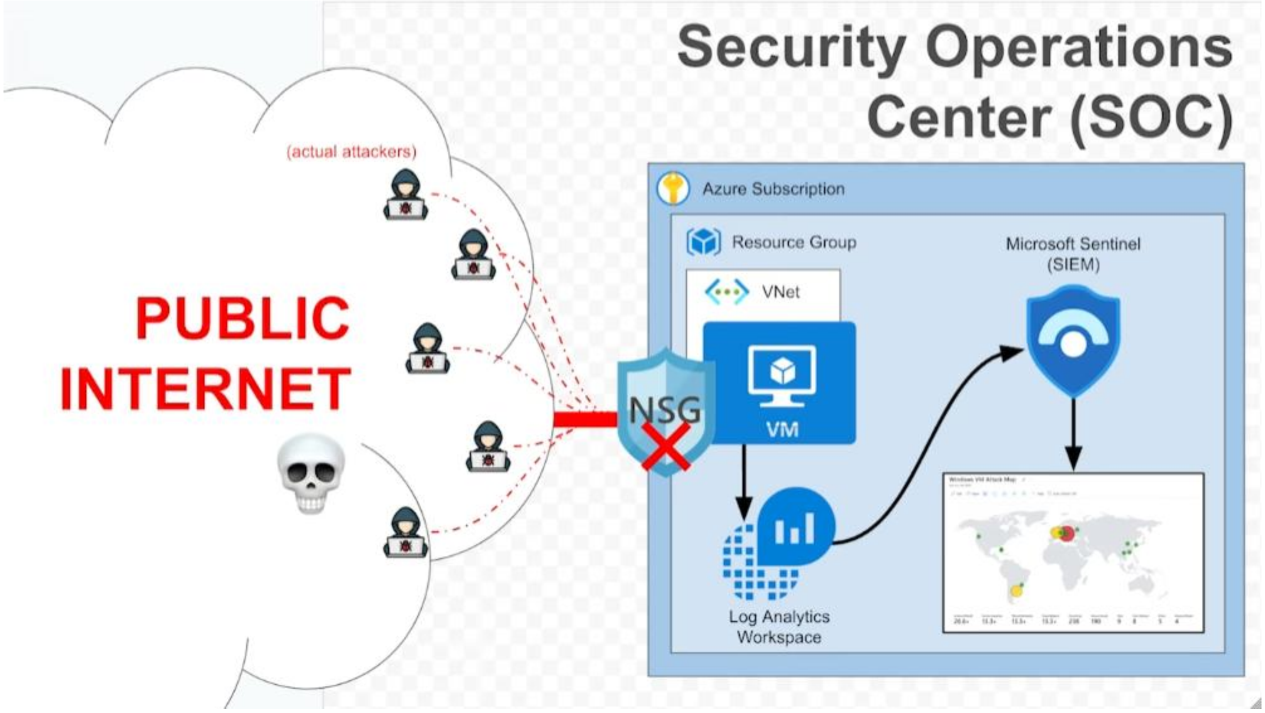
This lab simulates core SIEM tasks and it will eventually introduce the concept of integrating XDR using Microsoft Defender, which can be connected to Sentinel in future projects for extended detection and response capabilities.

Lab Goals and Objectives

My Goals for this lab:

- Understand how to deploy an Azure VM for monitoring
- Set up a Log Analytics Workspace and Microsoft Sentinel
- Ingest and analyze Windows security logs
- Write and run KQL queries to investigate specific events
- Enrich logs with external geolocation data using watchlists
- Visualize alerts and log trends in an interactive dashboard

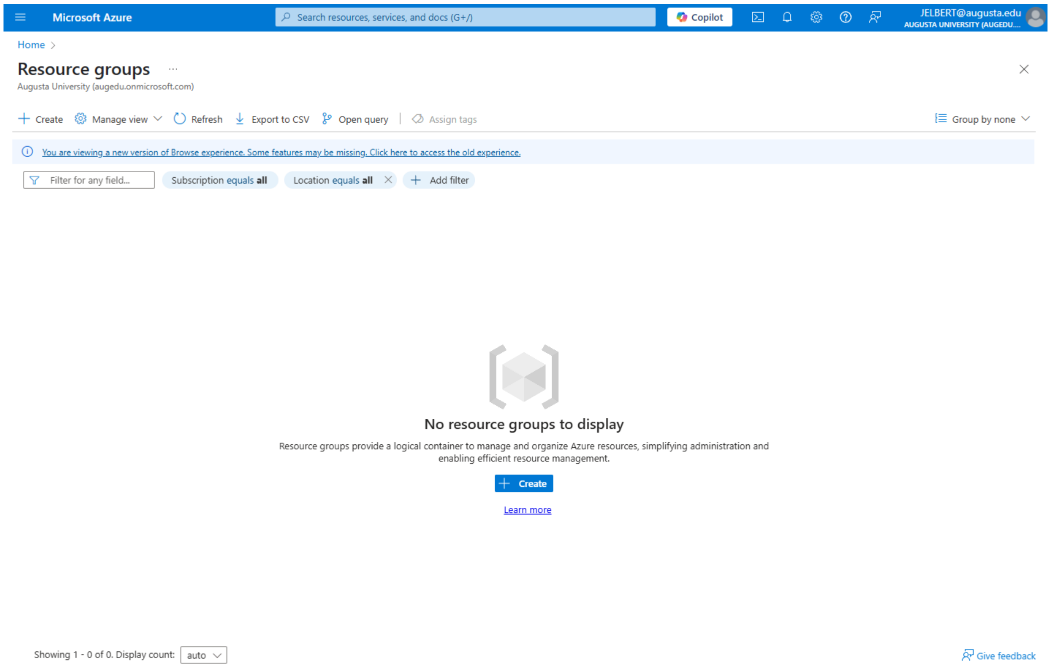
Network Map



Security Operations Center (SOC)
(actual attackers)
PUBLIC INTERNET
NSG
Azure Subscription
Resource Group
VNet
VM
Microsoft Sentinel (SIEM)
Log Analytics Workspace

Resource Group

To begin, I will be making a resource group in order to keep all of our resources together for this project. Below is what I began with. First, I will click on create. I named my group **Joe-SOC-Lab**.



Resource groups

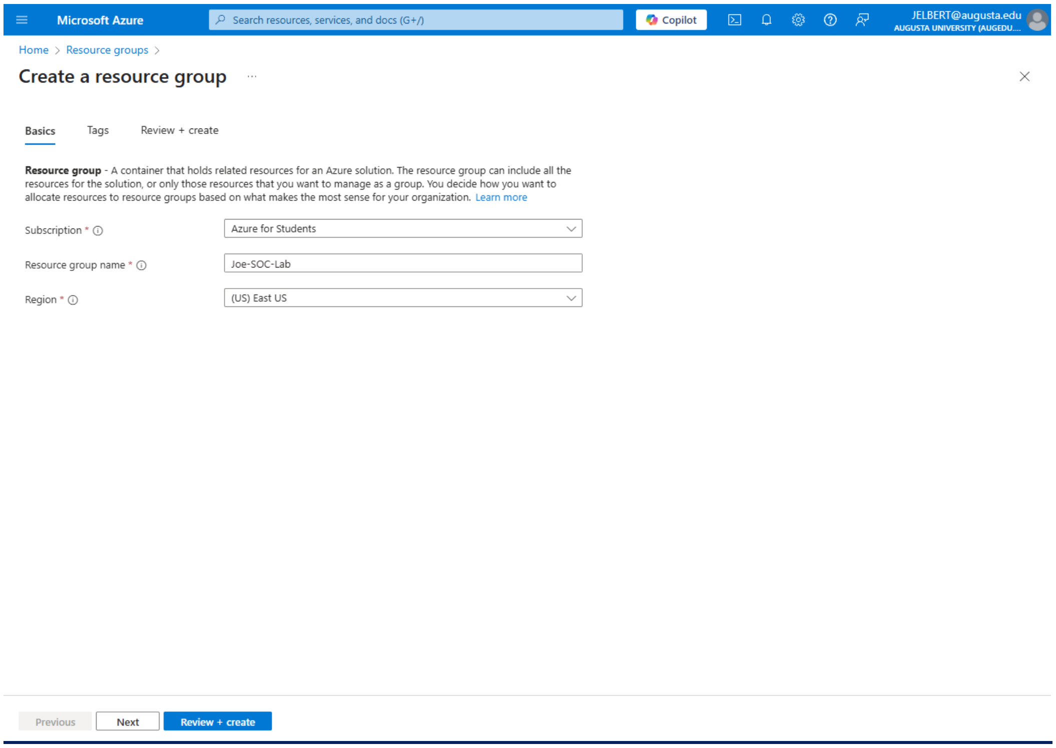
Augusta University (augedu.onmicrosoft.com)

You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

No resource groups to display

Resource groups provide a logical container to manage and organize Azure resources, simplifying administration and enabling efficient resource management.

Showing 1 - 0 of 0. Display count: auto



Create a resource group

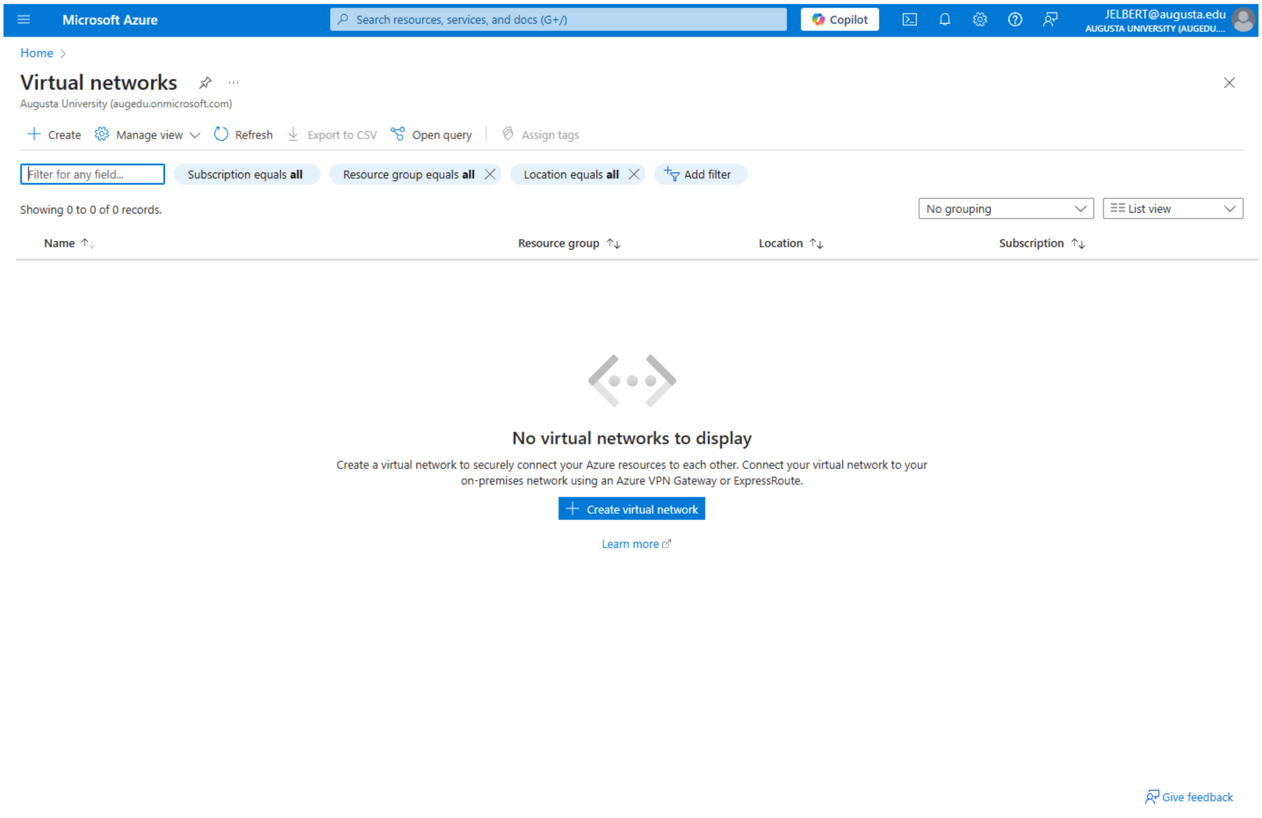
Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more

Subscription * : Azure for Students

Resource group name * : Joe-SOC-Lab

Region * : (US) East US

Next, I will be making a virtual network for a virtual machine honeypot and the Microsoft Sentinel instance. The honeypot will be accessible to anyone in the world, which will help me discover different types of attacks that will attempt to access my system.



Showing 0 to 0 of 0 records.

Name	Resource group	Location	Subscription

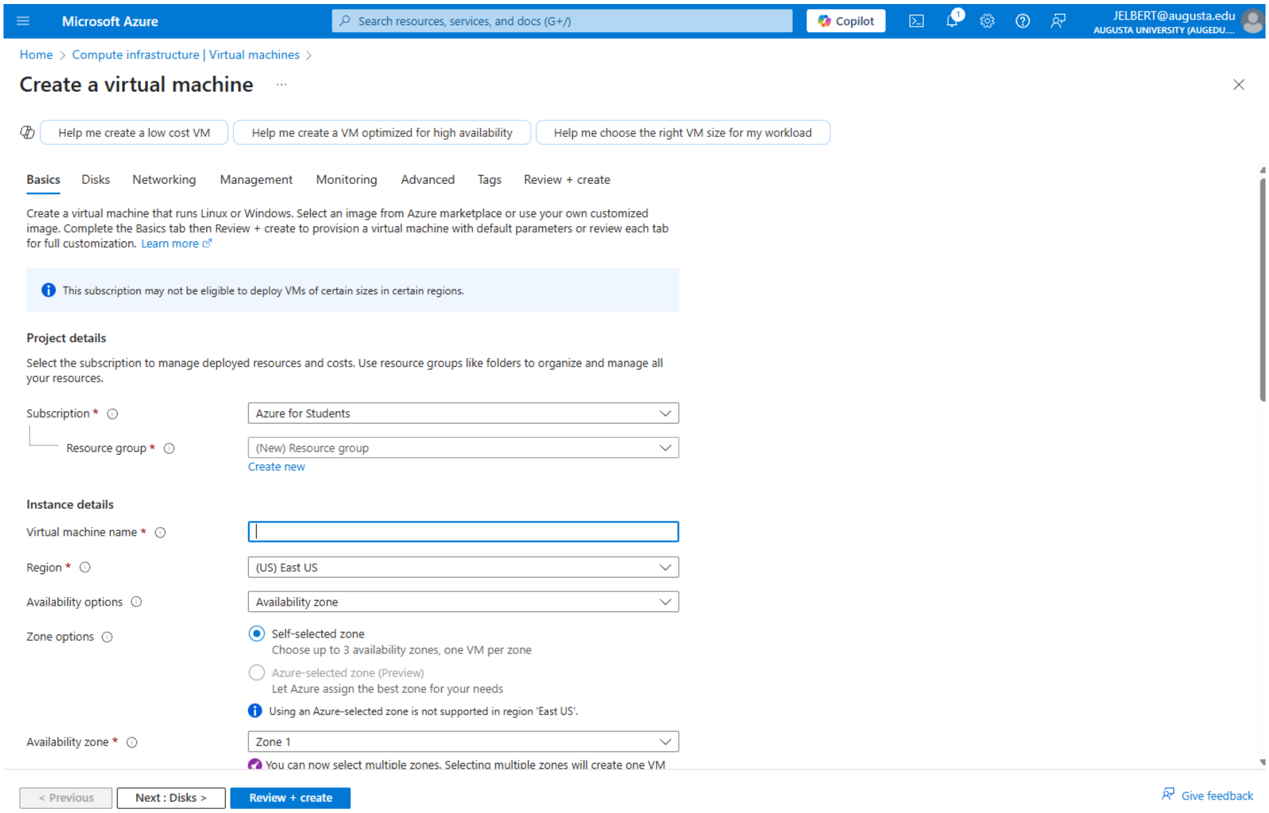
No virtual networks to display

Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute.

If you would like to see a tutorial on how I set up my virtual network, visit this quick video.

[Creating Virtual Network.mp4]

It is now time to setup the virtual machine honeypot.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...
Home > Compute infrastructure | Virtual machines >
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create
< Previous
Next : Disks >
Review + create
Give feedback

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

Instance details

Virtual machine name *:

Region *: (US) East US

Availability options: Availability zone

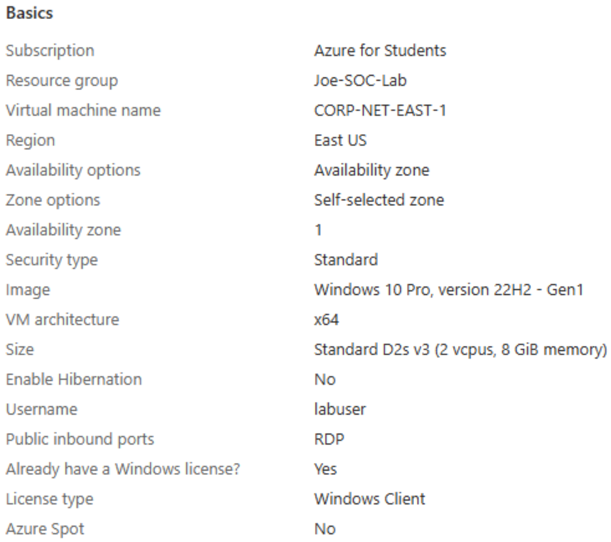
Zone options:
● Self-selected zone
Choose up to 3 availability zones, one VM per zone
○ Azure-selected zone (Preview)
Let Azure assign the best zone for your needs

Using an Azure-selected zone is not supported in region 'East US'.

Availability zone *: Zone 1

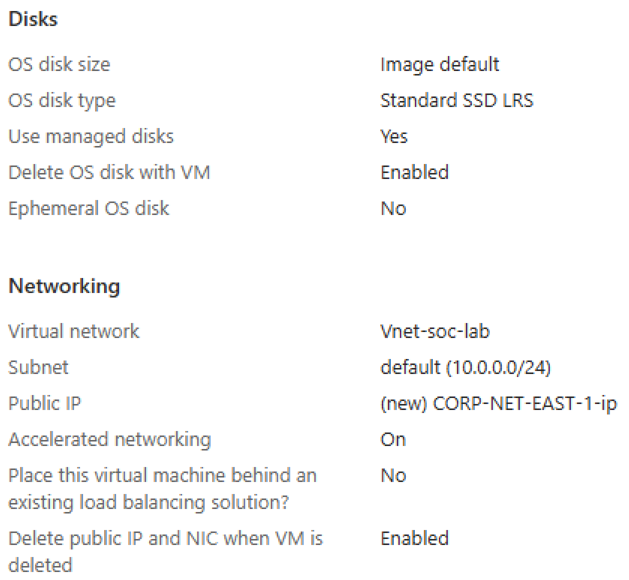
You can now select multiple zones. Selecting multiple zones will create one VM

These are the settings I used for my virtual machine honeypot. I will include the tabs and their required information. The tabs are down below.



Basics

Subscription	Azure for Students
Resource group	Joe-SOC-Lab
Virtual machine name	CORP-NET-EAST-1
Region	East US
Availability options	Availability zone
Zone options	Self-selected zone
Availability zone	1
Security type	Standard
Image	Windows 10 Pro, version 22H2 - Gen1
VM architecture	x64
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Enable Hibernation	No
Username	labuser
Public inbound ports	RDP
Already have a Windows license?	Yes
License type	Windows Client
Azure Spot	No

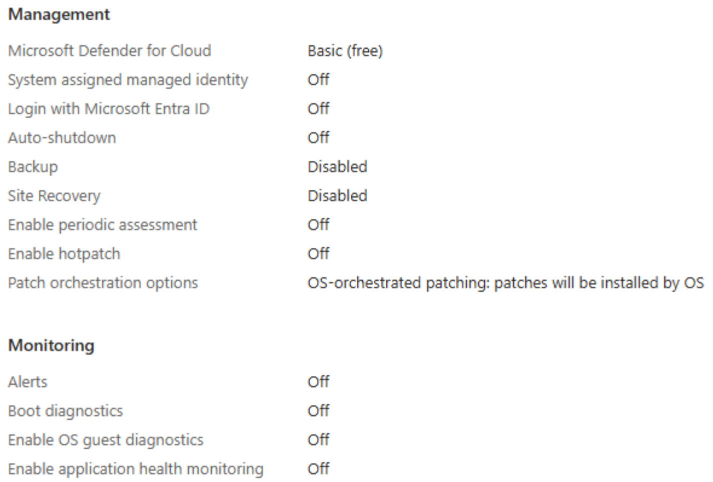


Disks

OS disk size	Image default
OS disk type	Standard SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

Networking

Virtual network	Vnet-soc-lab
Subnet	default (10.0.0.0/24)
Public IP	(new) CORP-NET-EAST-1-ip
Accelerated networking	On
Place this virtual machine behind an existing load balancing solution?	No
Delete public IP and NIC when VM is deleted	Enabled

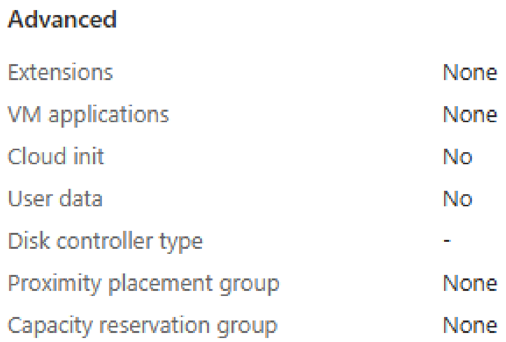


Management

Microsoft Defender for Cloud	Basic (free)
System assigned managed identity	Off
Login with Microsoft Entra ID	Off
Auto-shutdown	Off
Backup	Disabled
Site Recovery	Disabled
Enable periodic assessment	Off
Enable hotpatch	Off
Patch orchestration options	OS-orchestrated patching: patches will be installed by OS

Monitoring

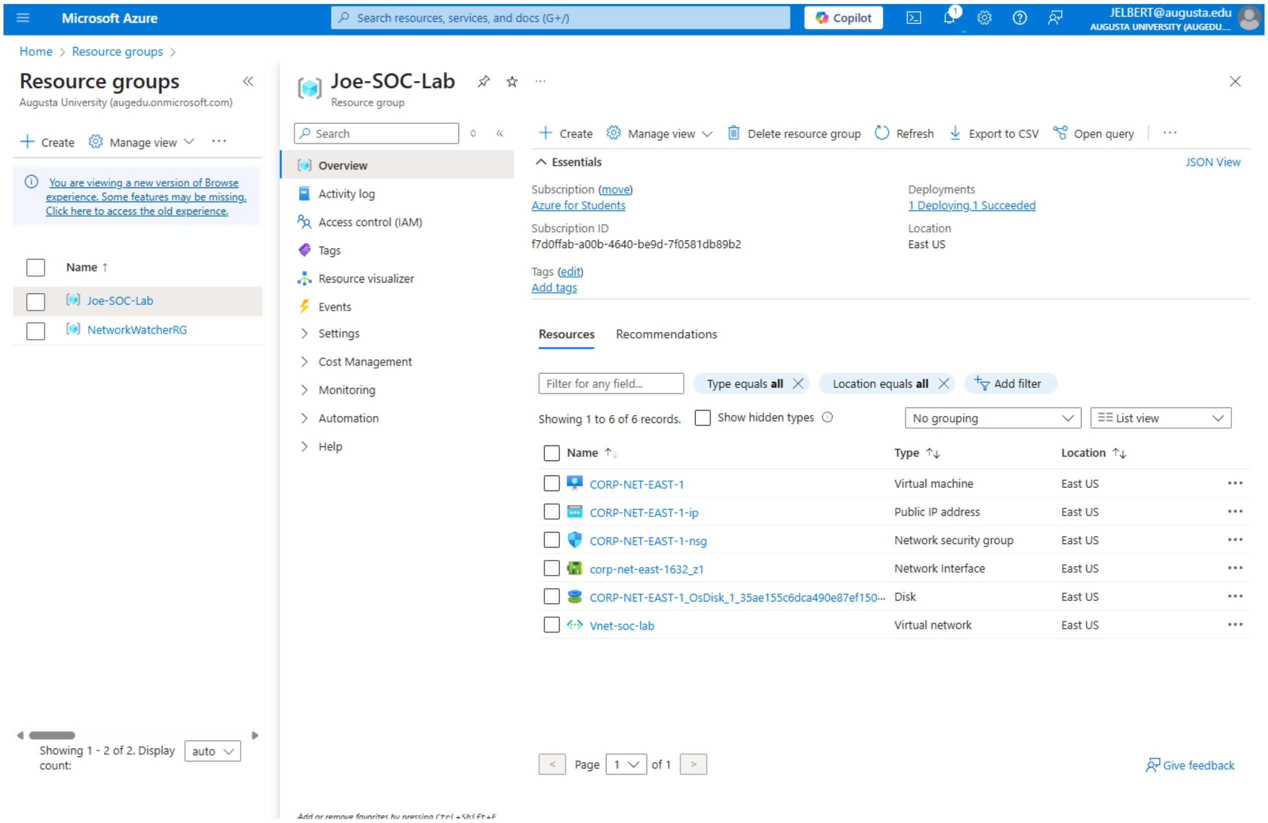
Alerts	Off
Boot diagnostics	Off
Enable OS guest diagnostics	Off
Enable application health monitoring	Off



Advanced

Extensions	None
VM applications	None
Cloud init	No
User data	No
Disk controller type	-
Proximity placement group	None
Capacity reservation group	None

This is what my Joe-SOC-Lab network looks like after I installed the VM with the settings I configured right before this.



Resource groups

Augusta University (augedu.onmicrosoft.com)

You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

Name ↑
Joe-SOC-Lab
NetworkWatcherRG

Showing 1 - 2 of 2. Display count: auto

Joe-SOC-Lab

Resource group

Essentials

Subscription (move)
Azure for Students

Subscription ID
f7d0ffab-a00b-4640-be9d-7f0581db89b2

Tags (edit)
Add tags

Deployments
1 Deploying,1 Succeeded

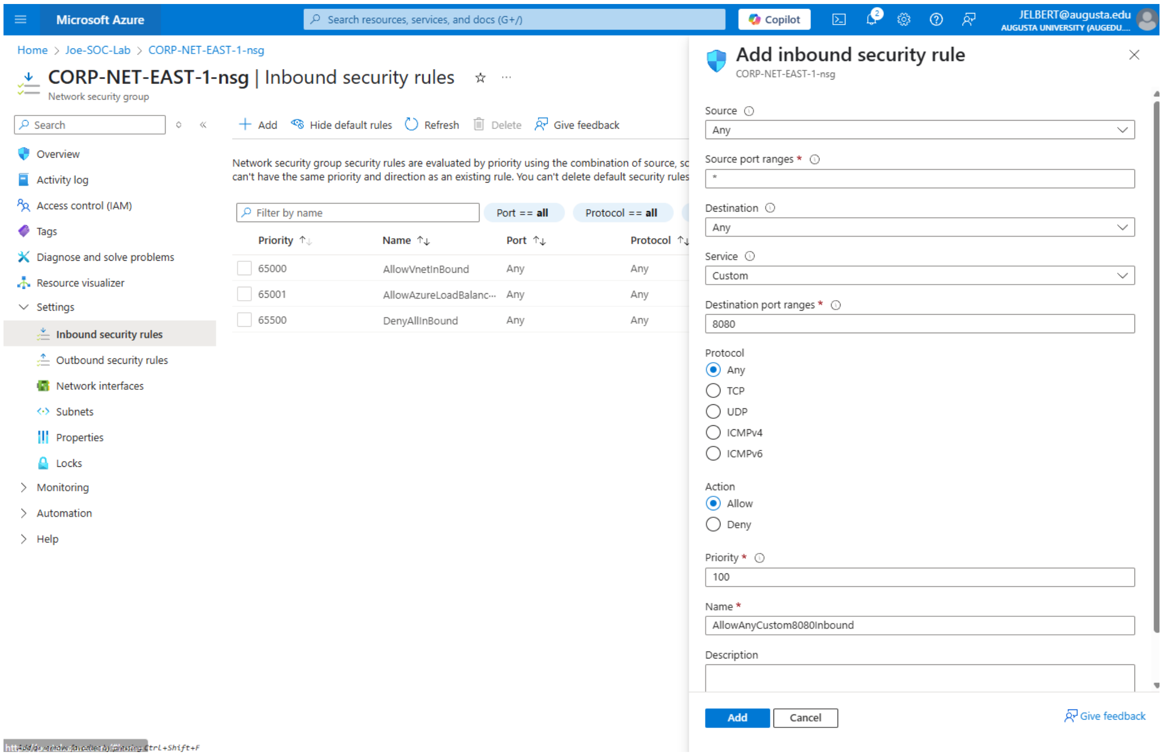
Location
East US

Showing 1 to 6 of 6 records. □ Show hidden types

Name	Type	Location
CORP-NET-EAST-1	Virtual machine	East US
CORP-NET-EAST-1-ip	Public IP address	East US
CORP-NET-EAST-1-nsg	Network security group	East US
corp-net-east-1632_z1	Network Interface	East US
CORP-NET-EAST-1_OsDisk_1_35ae155c6dca490e87ef150...	Disk	East US
Vnet-soc-lab	Virtual network	East US

Add or remove favorites by pressing Ctrl+Shift+F

Now, its time to configure the firewall so anyone can attack this VM on the internet. This means that this machine is now a honeypot. I went to the inbound security rules and set it where all inbound connections are allowed.



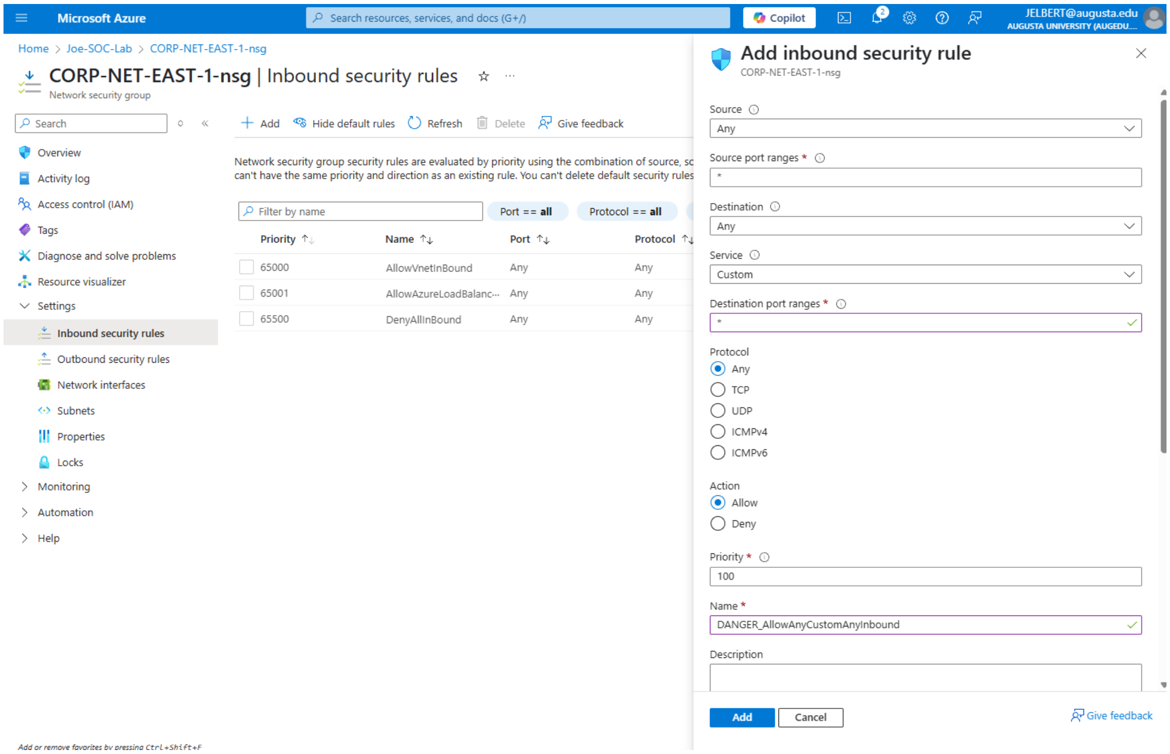
CORP-NET-EAST-1-nsg | Inbound security rules

Network security group security rules are evaluated by priority using the combination of source, sc can't have the same priority and direction as an existing rule. You can't delete default security rules

Priority	Name	Port	Protocol
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalanc...	Any	Any
65500	DenyAllInBound	Any	Any

Add inbound security rule
CORP-NET-EAST-1-nsg

Source: Any
Source port ranges *: *
Destination: Any
Service: Custom
Destination port ranges *: 8080
Protocol: ● Any ○ TCP ○ UDP ○ ICMPv4 ○ ICMPv6
Action: ● Allow ○ Deny
Priority *: 100
Name *: AllowAnyCustom8080Inbound
Description:



CORP-NET-EAST-1-nsg | Inbound security rules

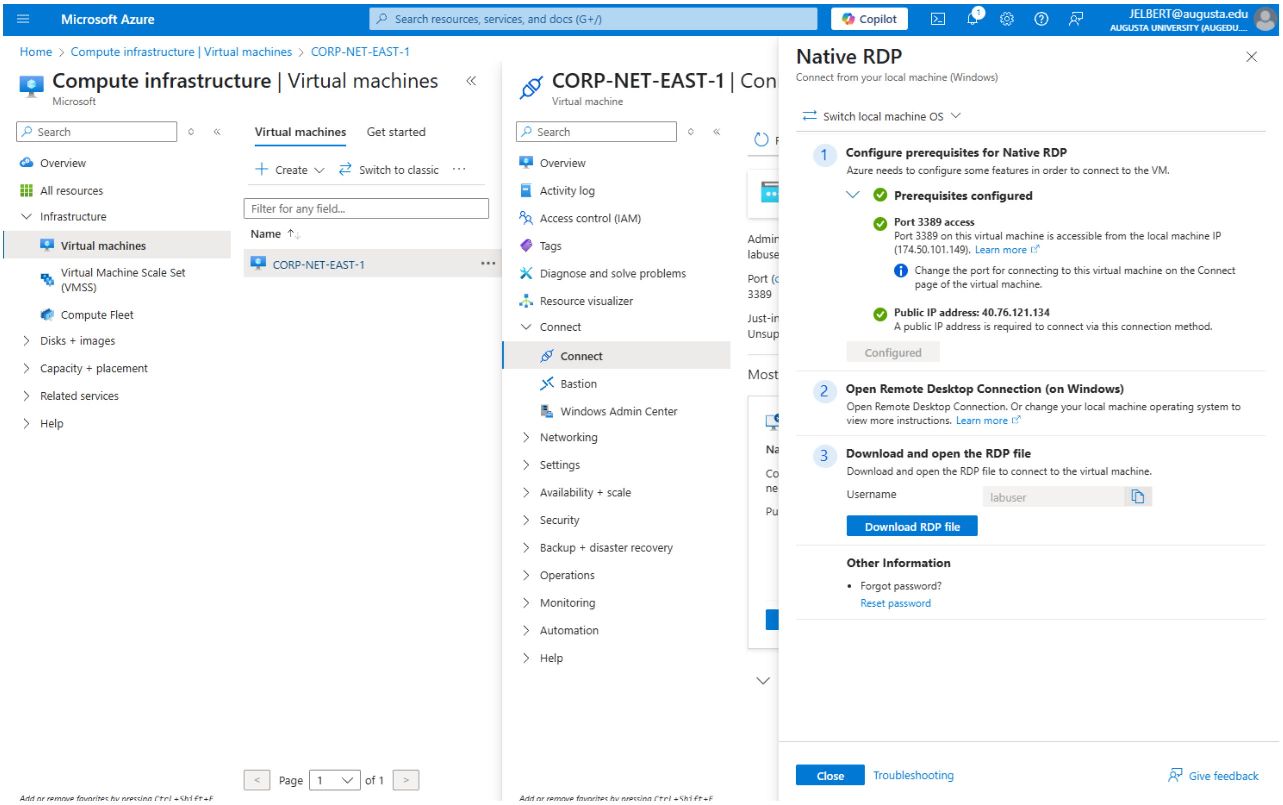
Network security group security rules are evaluated by priority using the combination of source, sc can't have the same priority and direction as an existing rule. You can't delete default security rules

Priority	Name	Port	Protocol
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalanc...	Any	Any
65500	DenyAllInBound	Any	Any

Add inbound security rule
CORP-NET-EAST-1-nsg

Source: Any
Source port ranges *: *
Destination: Any
Service: Custom
Destination port ranges *: *
Protocol: ● Any ○ TCP ○ UDP ○ ICMPv4 ○ ICMPv6
Action: ● Allow ○ Deny
Priority *: 100
Name *: DANGER_AllowAnyCustomAnyInbound
Description:

The virtual machine is ready. We can now connect to the virtual machine via Remote Desktop Protocol (RDP) on port 3389.



Native RDP

Connect from your local machine (Windows)

1. **Configure prerequisites for Native RDP**

   Azure needs to configure some features in order to connect to the VM.

   Prerequisites configured

   Port 3389 access
   Port 3389 on this virtual machine is accessible from the local machine IP (174.50.101.149). Learn more

   Change the port for connecting to this virtual machine on the Connect page of the virtual machine.

   Public IP address: 40.76.121.134
   A public IP address is required to connect via this connection method.

2. **Open Remote Desktop Connection (on Windows)**

   Open Remote Desktop Connection. Or change your local machine operating system to view more instructions. Learn more

3. **Download and open the RDP file**

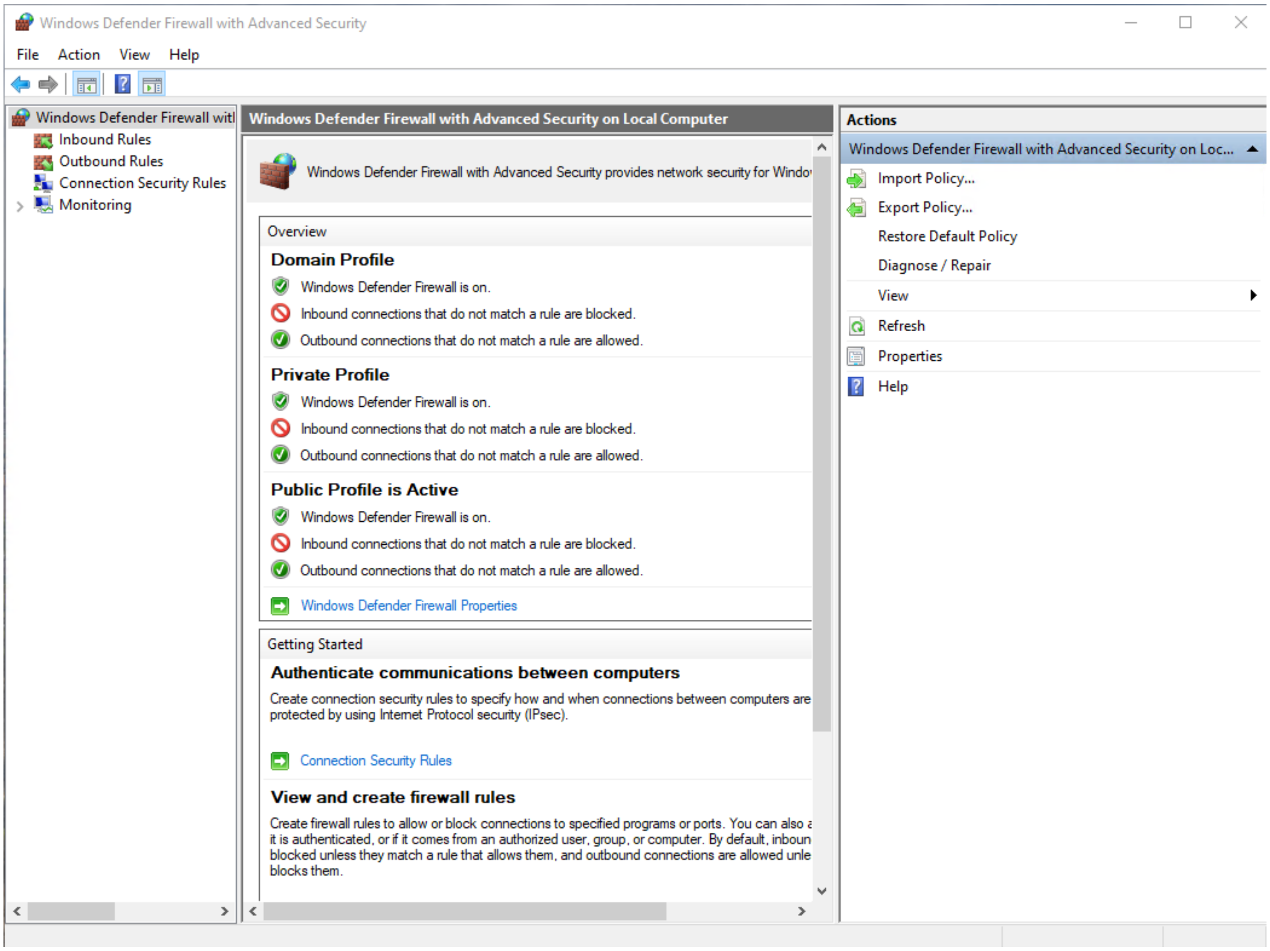
   Download and open the RDP file to connect to the virtual machine.

   Username: labuser

Other Information

- Forgot password?
  Reset password

Once logged into the virtual machine, it is time to open the Windows Defender Firewall settings. We need to do this in order to make it a honeypot for remote attackers to connect to it. Type in the search bar: “**wf.msc**” to open this menu.



Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Actions
Windows Defender Firewall with Advanced Security on Loc...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

Windows Defender Firewall with Advanced Security provides network security for Windo

Overview

Domain 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.

Private 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.

Public 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.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

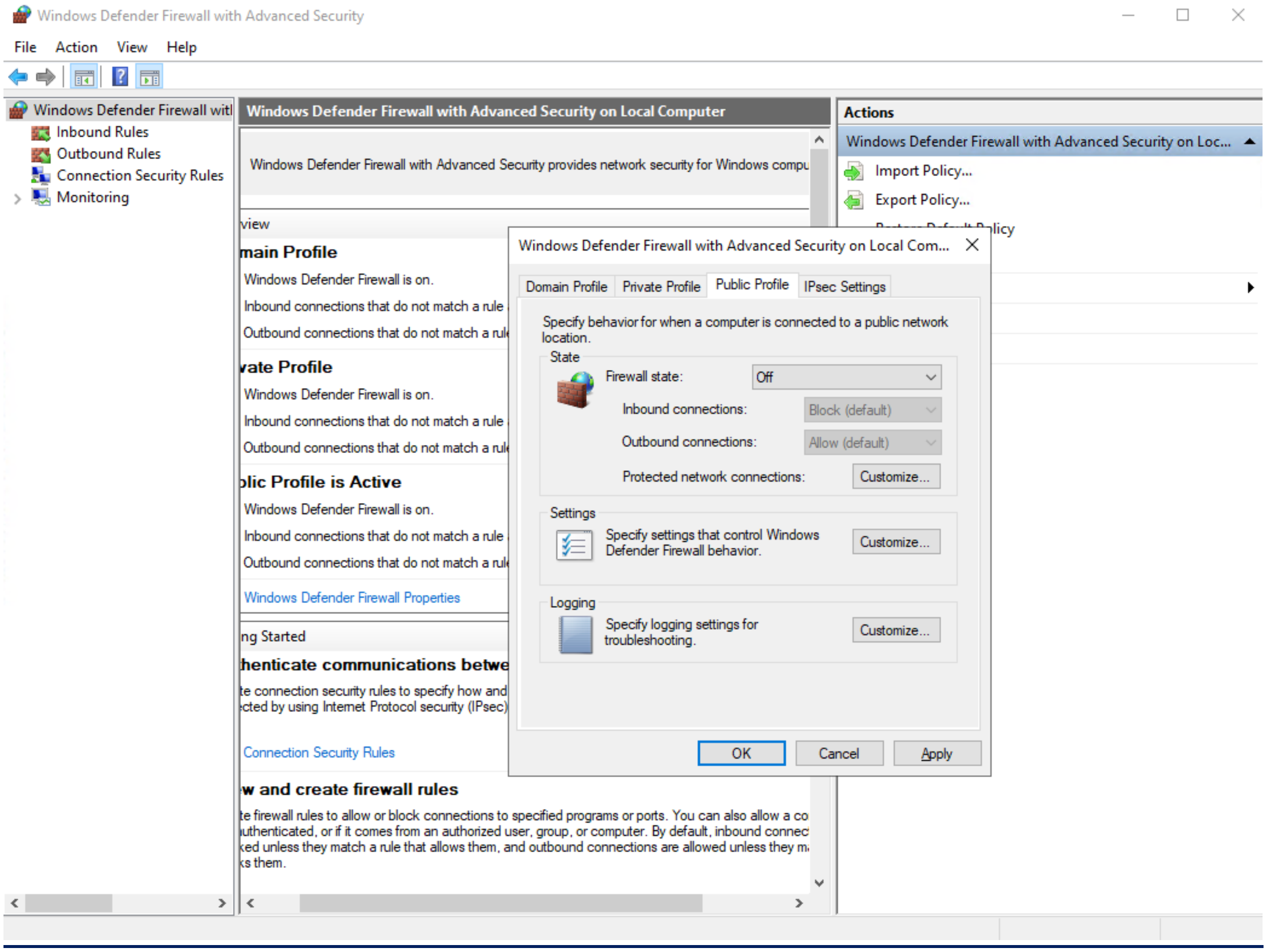
Create connection security rules to specify how and when connections between computers are protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

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

In the middle of the screen, go to “Windows Defender Firewall Properties” and you should see the box below pop up. On the first 3 tabs, press the “o” key to turn all of the settings off on each of the tabs. Click apply and then exit out.



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows compu

view

main Profile

Windows Defender Firewall is on.

Inbound connections that do not match a rule

Outbound connections that do not match a rul

vate Profile

Windows Defender Firewall is on.

Inbound connections that do not match a rule

Outbound connections that do not match a rul

olic Profile is Active

Windows Defender Firewall is on.

Inbound connections that do not match a rule

Outbound connections that do not match a rul

Windows Defender Firewall Properties

ng Started

henticate communications betwe

te connection security rules to specify how and
cted by using Internet Protocol security (IPsec)

Connection Security Rules

w and create firewall rules

te firewall rules to allow or block connections to specified programs or ports. You can also allow a co
uthenticated, or if it comes from an authorized user, group, or computer. By default, inbound connec
ked unless they match a rule that allows them, and outbound connections are allowed unless they m
s them.

Windows Defender Firewall with Advanced Security on Local Com...

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:

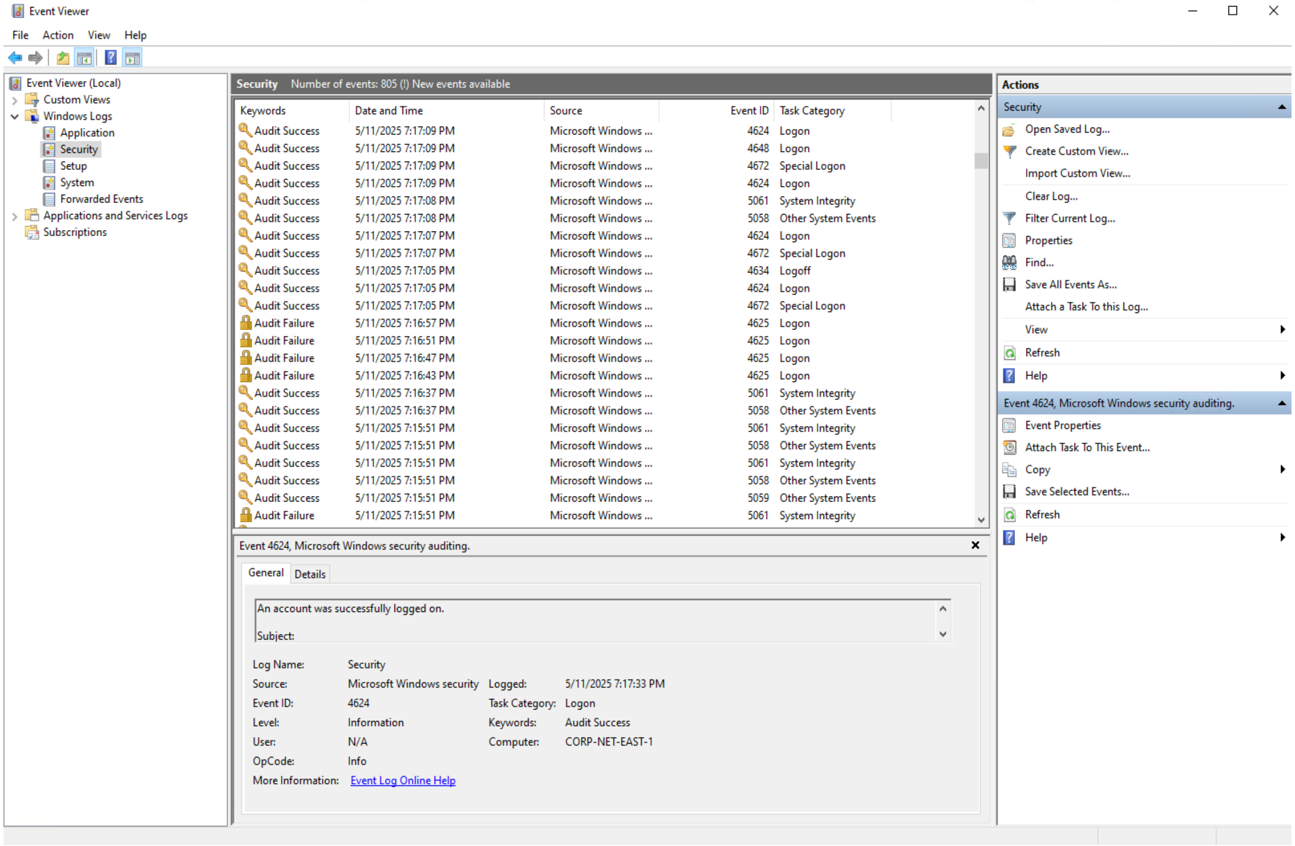
Settings

Specify settings that control Windows Defender Firewall behavior.

Logging

Specify logging settings for troubleshooting.

Now, its time to go into Event Viewer to learn about system logs. Once in Event Viewer, go to the “Windows Logs” folder. Then go to the “Security” tab to view windows security event logs.



Security Number of events: 805 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	5/11/2025 7:17:09 PM	Microsoft Windows ...	4624	Logon
Audit Success	5/11/2025 7:17:09 PM	Microsoft Windows ...	4648	Logon
Audit Success	5/11/2025 7:17:09 PM	Microsoft Windows ...	4672	Special Logon
Audit Success	5/11/2025 7:17:09 PM	Microsoft Windows ...	4624	Logon
Audit Success	5/11/2025 7:17:08 PM	Microsoft Windows ...	5061	System Integrity
Audit Success	5/11/2025 7:17:08 PM	Microsoft Windows ...	5058	Other System Events
Audit Success	5/11/2025 7:17:07 PM	Microsoft Windows ...	4624	Logon
Audit Success	5/11/2025 7:17:07 PM	Microsoft Windows ...	4672	Special Logon
Audit Success	5/11/2025 7:17:05 PM	Microsoft Windows ...	4634	Logoff
Audit Success	5/11/2025 7:17:05 PM	Microsoft Windows ...	4624	Logon
Audit Success	5/11/2025 7:17:05 PM	Microsoft Windows ...	4672	Special Logon
Audit Failure	5/11/2025 7:16:57 PM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 7:16:51 PM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 7:16:47 PM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 7:16:43 PM	Microsoft Windows ...	4625	Logon
Audit Success	5/11/2025 7:16:37 PM	Microsoft Windows ...	5061	System Integrity
Audit Success	5/11/2025 7:16:37 PM	Microsoft Windows ...	5058	Other System Events
Audit Success	5/11/2025 7:15:51 PM	Microsoft Windows ...	5061	System Integrity
Audit Success	5/11/2025 7:15:51 PM	Microsoft Windows ...	5058	Other System Events
Audit Success	5/11/2025 7:15:51 PM	Microsoft Windows ...	5061	System Integrity
Audit Success	5/11/2025 7:15:51 PM	Microsoft Windows ...	5058	Other System Events
Audit Success	5/11/2025 7:15:51 PM	Microsoft Windows ...	5059	Other System Events
Audit Failure	5/11/2025 7:15:51 PM	Microsoft Windows ...	5061	System Integrity

Event 4624, Microsoft Windows security auditing.

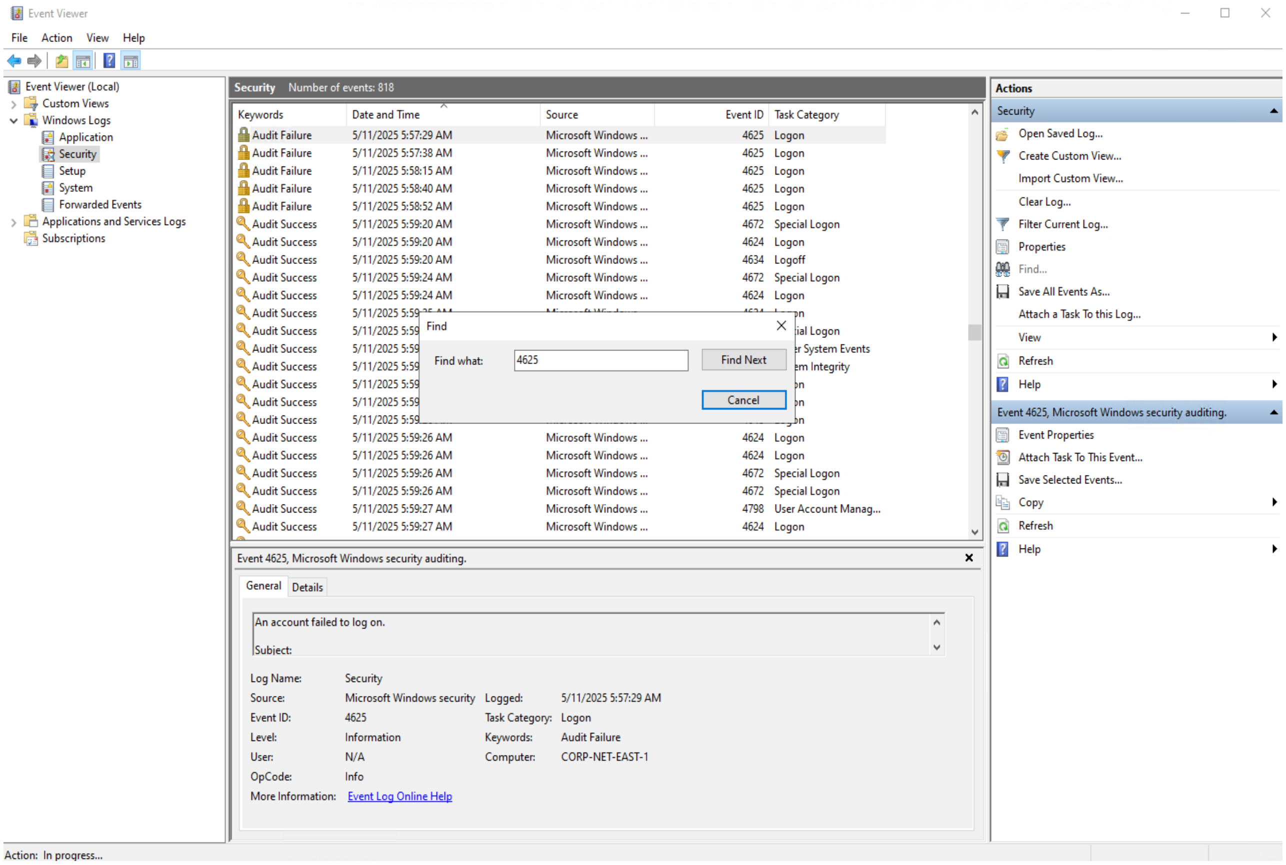
General Details

An account was successfully logged on.

Subject:

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	5/11/2025 7:17:33 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	CORP-NET-EAST-1
OpCode:	Info		
More Information:	Event Log Online Help		

Press “ctrl + f” in order to search for certain EventID numbers. The EventID below is 4625 and it has to do with events related to system logon’s.



Security Number of events: 818

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	5/11/2025 5:57:29 AM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 5:57:38 AM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 5:58:15 AM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 5:58:40 AM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 5:58:52 AM	Microsoft Windows ...	4625	Logon
Audit Success	5/11/2025 5:59:20 AM	Microsoft Windows ...	4672	Special Logon
Audit Success	5/11/2025 5:59:20 AM	Microsoft Windows ...	4624	Logon
Audit Success	5/11/2025 5:59:20 AM	Microsoft Windows ...	4634	Logoff
Audit Success	5/11/2025 5:59:24 AM	Microsoft Windows ...	4672	Special Logon
Audit Success	5/11/2025 5:59:24 AM	Microsoft Windows ...	4624	Logon
Audit Success	5/11/2025 5:59			on
Audit Success	5/11/2025 5:59			ial Logon
Audit Success	5/11/2025 5:59			r System Events
Audit Success	5/11/2025 5:59			em Integrity
Audit Success	5/11/2025 5:59			on
Audit Success	5/11/2025 5:59			on
Audit Success	5/11/2025 5:59			on
Audit Success	5/11/2025 5:59:26 AM	Microsoft Windows ...	4624	Logon
Audit Success	5/11/2025 5:59:26 AM	Microsoft Windows ...	4624	Logon
Audit Success	5/11/2025 5:59:26 AM	Microsoft Windows ...	4672	Special Logon
Audit Success	5/11/2025 5:59:26 AM	Microsoft Windows ...	4672	Special Logon
Audit Success	5/11/2025 5:59:27 AM	Microsoft Windows ...	4798	User Account Manag...
Audit Success	5/11/2025 5:59:27 AM	Microsoft Windows ...	4624	Logon

Find what: 4625

Event 4625, Microsoft Windows security auditing.

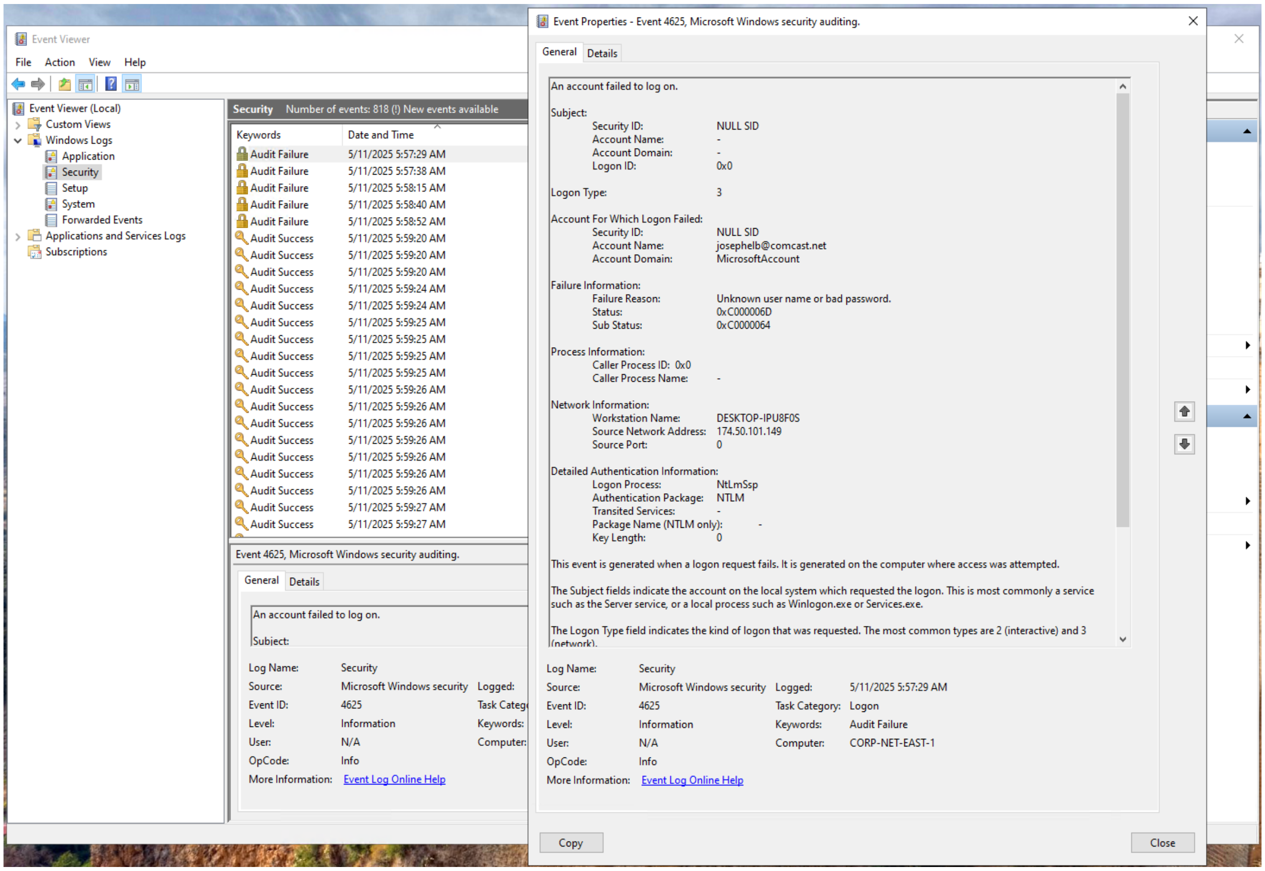
An account failed to log on.

Subject:

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	5/11/2025 5:57:29 AM
Event ID:	4625	Task Category:	Logon
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	CORP-NET-EAST-1
OpCode:	Info		
More Information:	Event Log Online Help		

Action: In progress...

Click on any file and you will be able to see all of the information for the security event log. You can see things like account name, failure reason, and the IP address it came from.



Security Number of events: 818 (!) New events available

Keywords	Date and Time
Audit Failure	5/11/2025 5:57:29 AM
Audit Failure	5/11/2025 5:57:38 AM
Audit Failure	5/11/2025 5:58:15 AM
Audit Failure	5/11/2025 5:58:40 AM
Audit Failure	5/11/2025 5:58:52 AM
Audit Success	5/11/2025 5:59:20 AM
Audit Success	5/11/2025 5:59:20 AM
Audit Success	5/11/2025 5:59:20 AM
Audit Success	5/11/2025 5:59:24 AM
Audit Success	5/11/2025 5:59:24 AM
Audit Success	5/11/2025 5:59:25 AM
Audit Success	5/11/2025 5:59:25 AM
Audit Success	5/11/2025 5:59:25 AM
Audit Success	5/11/2025 5:59:25 AM
Audit Success	5/11/2025 5:59:26 AM
Audit Success	5/11/2025 5:59:26 AM
Audit Success	5/11/2025 5:59:26 AM
Audit Success	5/11/2025 5:59:26 AM
Audit Success	5/11/2025 5:59:26 AM
Audit Success	5/11/2025 5:59:26 AM
Audit Success	5/11/2025 5:59:26 AM
Audit Success	5/11/2025 5:59:27 AM
Audit Success	5/11/2025 5:59:27 AM

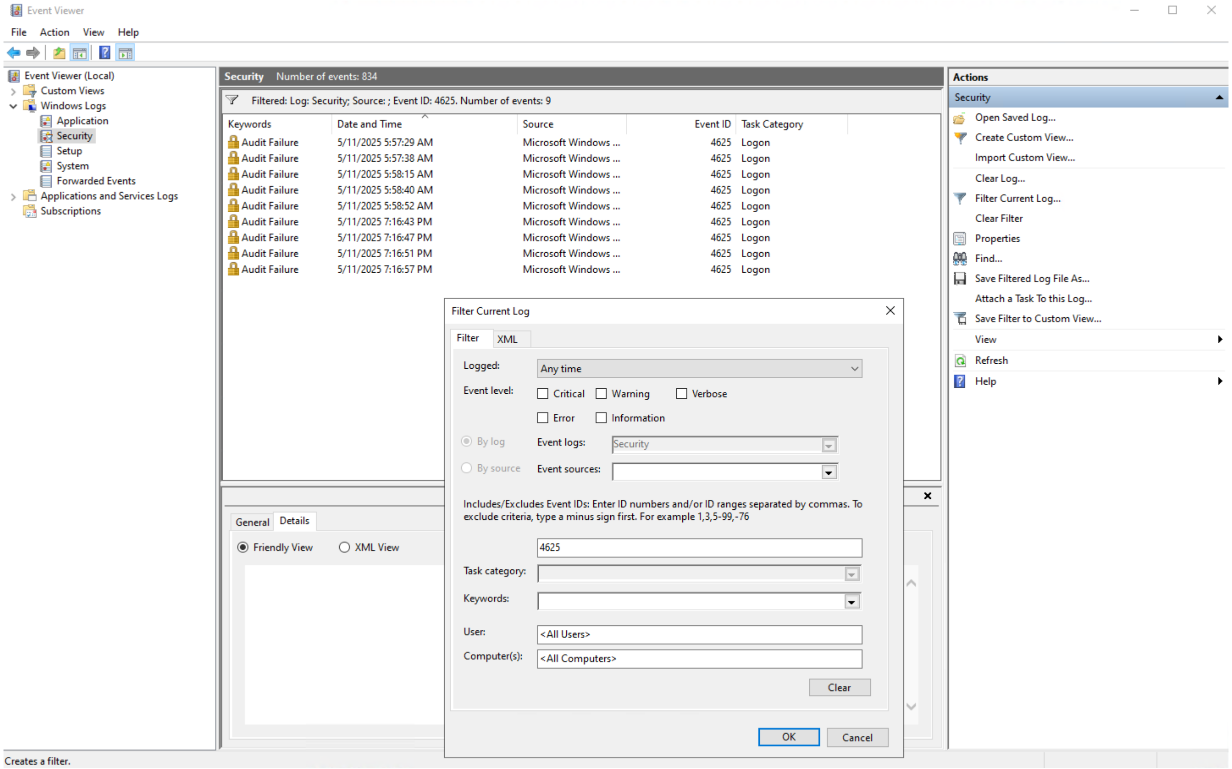
Event 4625, Microsoft Windows security auditing.

```
An account failed to log on.

Subject:

Log Name:          Security
Source:            Microsoft Windows security   Logged:
Event ID:          4625                         Task Categ
Level:             Information                  Keywords:
User:              N/A                          Computer:
OpCode:            Info
More Information:  Event Log Online Help
```

Event Properties - Event 4625, Microsoft Windows security auditing.

```
An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           josephelb@comcast.net
        Account Domain:         MicrosoftAccount

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:       DESKTOP-IPU8F0S
        Source Network Address: 174.50.101.149
        Source Port:            0

Detailed Authentication Information:
        Logon Process:          NtLmSsp
        Authentication Package: NTLM
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0

This event is generated when a logon request fails. It is generated on the computer where access was attempted.

The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service
such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3
(network).

Log Name:          Security
Source:            Microsoft Windows security   Logged:          5/11/2025 5:57:29 AM
Event ID:          4625                         Task Category:   Logon
Level:             Information                  Keywords:        Audit Failure
User:              N/A                          Computer:        CORP-NET-EAST-1
OpCode:            Info
More Information:  Event Log Online Help
```

You can also filter the list of logs based on the currently selected log. You do this in order to see logs that have the same exact EventID, which can help map attack patterns.



Security Number of events: 834

Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 9

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	5/11/2025 5:57:29 AM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 5:57:38 AM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 5:58:15 AM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 5:58:40 AM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 5:58:52 AM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 7:16:43 PM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 7:16:47 PM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 7:16:51 PM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 7:16:57 PM	Microsoft Windows ...	4625	Logon

Filter Current Log

Filter XML

Logged: Any time

Event level: □ Critical □ Warning □ Verbose
□ Error □ Information

● By log Event logs: Security

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4625

Task category:

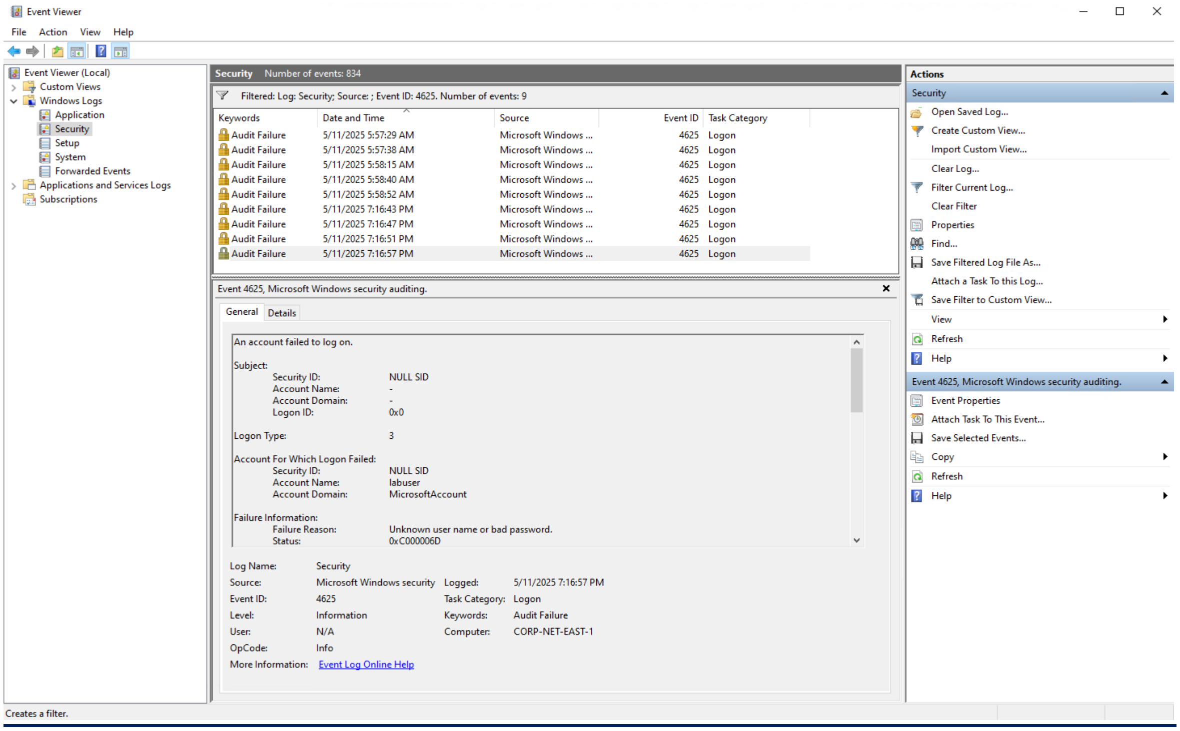
Keywords:

User: <All Users>

Computer(s): <All Computers>

Clear

OK Cancel



Security Number of events: 834

Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 9

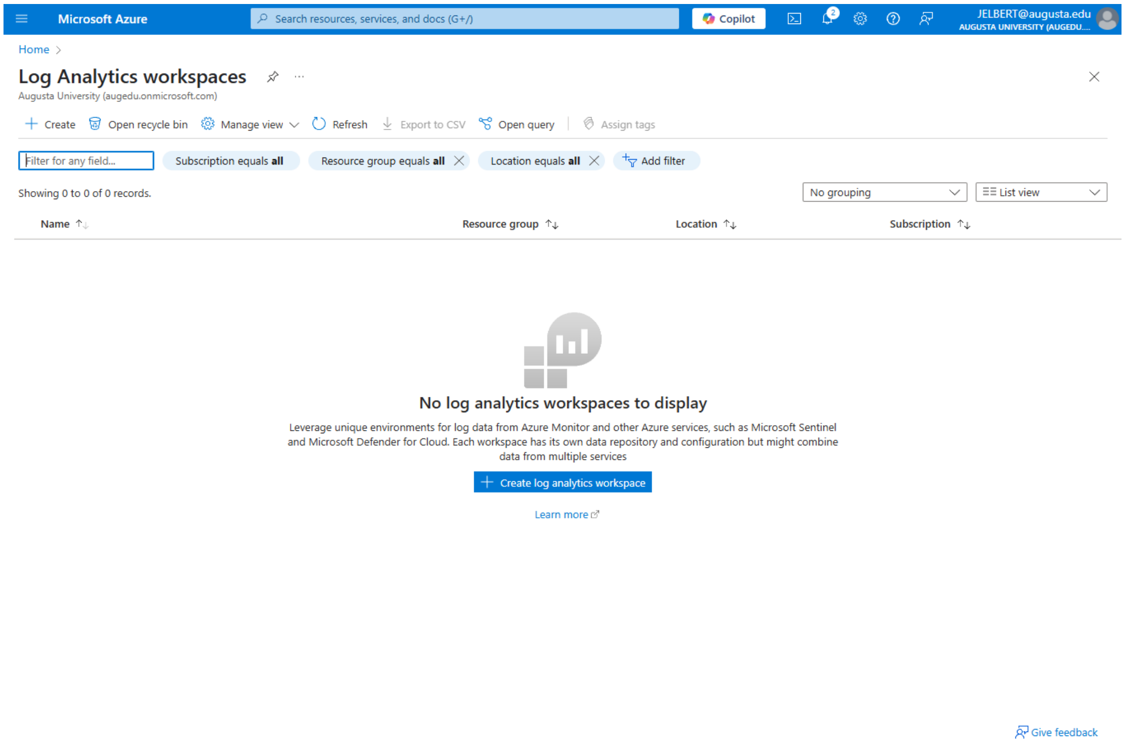
Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	5/11/2025 5:57:29 AM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 5:57:38 AM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 5:58:15 AM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 5:58:40 AM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 5:58:52 AM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 7:16:43 PM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 7:16:47 PM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 7:16:51 PM	Microsoft Windows ...	4625	Logon
Audit Failure	5/11/2025 7:16:57 PM	Microsoft Windows ...	4625	Logon

Event 4625, Microsoft Windows security auditing.

```
An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           labuser
        Account Domain:         MicrosoftAccount

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

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:         5/11/2025 7:16:57 PM
Event ID:          4625                         Task Category:  Logon
Level:             Information                  Keywords:       Audit Failure
User:              N/A                          Computer:       CORP-NET-EAST-1
OpCode:            Info
More Information:  Event Log Online Help
```

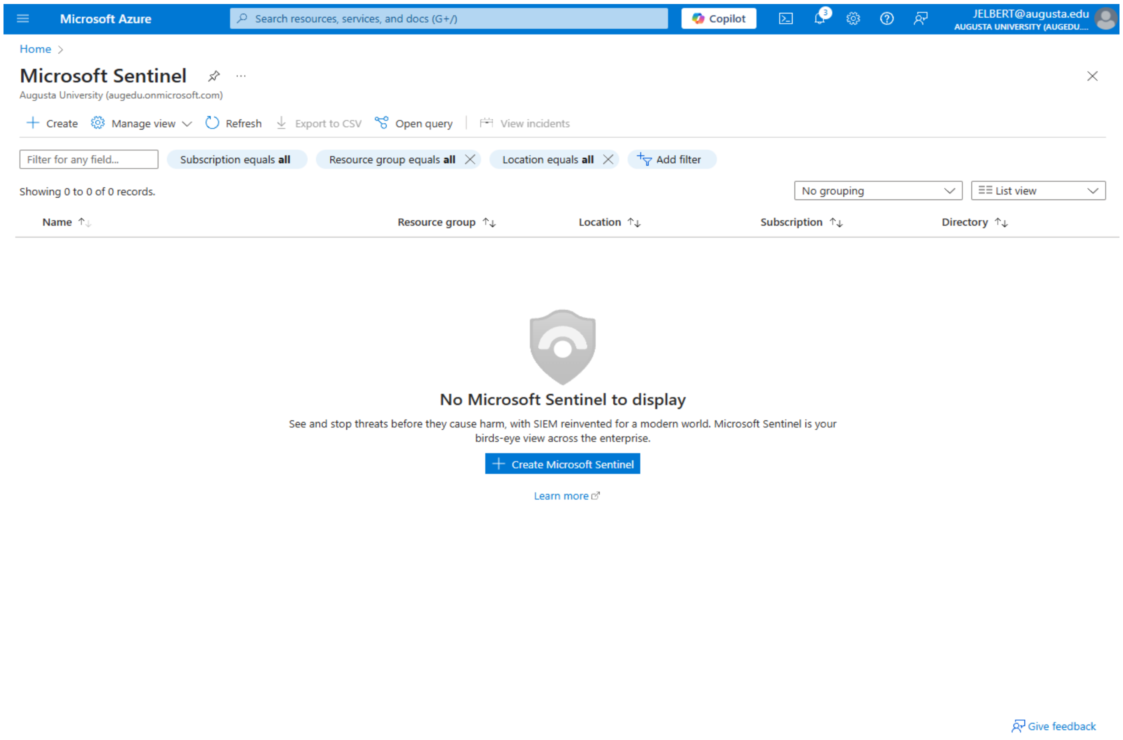
Next, it is time to create a log analytics workspace. This is needed in order to connect our VM to our Microsoft Sentinel Security Information and Event Management (SIEM) system.



Showing 0 to 0 of 0 records.

No log analytics workspaces to display

Leverage unique environments for 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 might combine data from multiple services

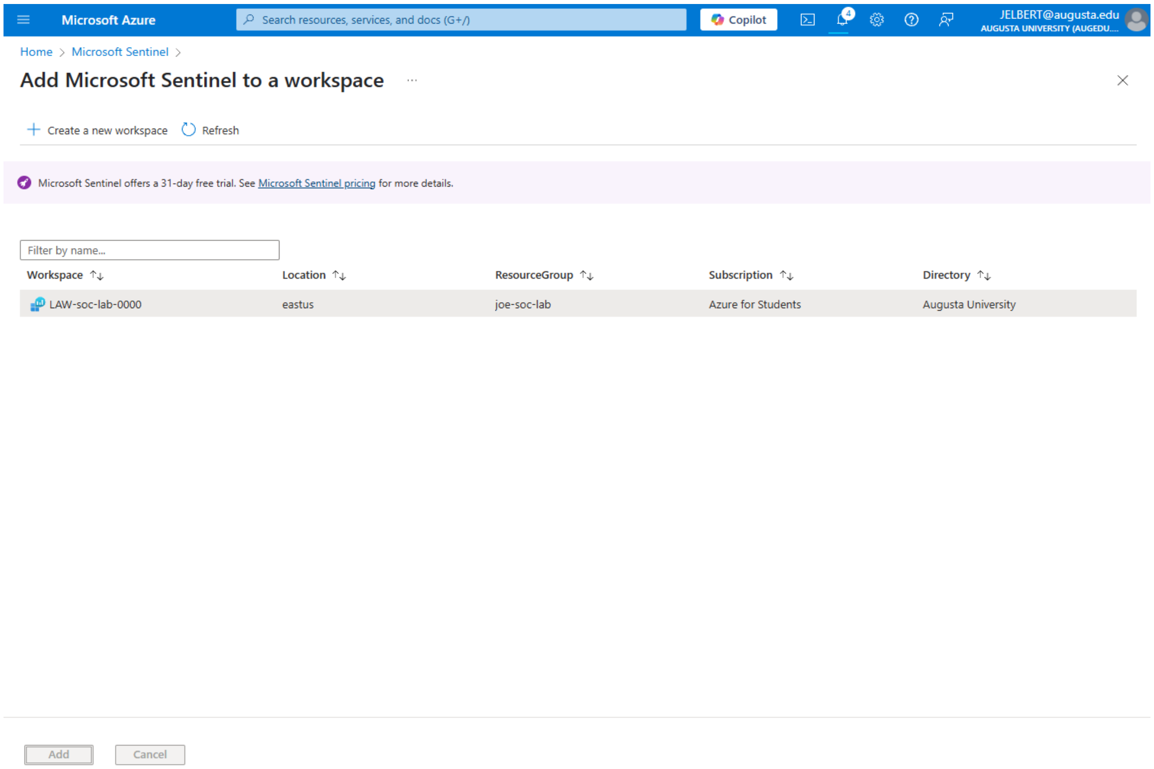


Showing 0 to 0 of 0 records.

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.

Here, I will be linking the Microsoft Sentinel instance to my Log analytics workspace: LAW-soc-lab workspace.



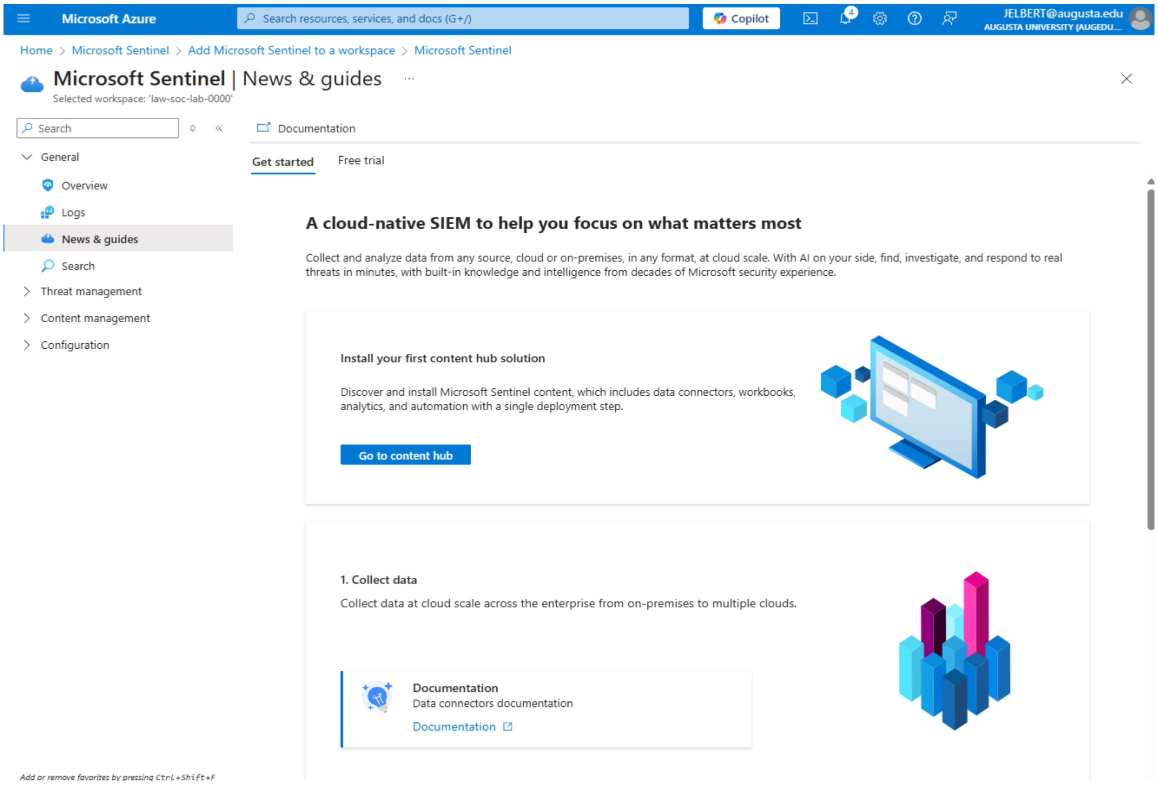
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...
Home > Microsoft Sentinel >
+ Create a new workspace
Refresh

Add Microsoft Sentinel to a workspace

Microsoft Sentinel offers a 31-day free trial. See Microsoft Sentinel pricing for more details.

Filter by name...

Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
LAW-soc-lab-0000	eastus	joe-soc-lab	Azure for Students	Augusta University



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...
Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel
Search
General
Overview
Logs
News & guides
Search
Threat management
Content management
Configuration
Add or remove favorites by pressing Ctrl+Shift+F
Documentation
Get started
Free trial

Microsoft Sentinel | News & guides

Selected workspace: 'law-soc-lab-0000'

A cloud-native SIEM to help you focus on what matters most

Collect and analyze data from any source, cloud or on-premises, in any format, at cloud scale. With AI on your side, find, investigate, and respond to real threats in minutes, with built-in knowledge and intelligence from decades of Microsoft security experience.

Install your first content hub solution

Discover and install Microsoft Sentinel content, which includes data connectors, workbooks, analytics, and automation with a single deployment step.

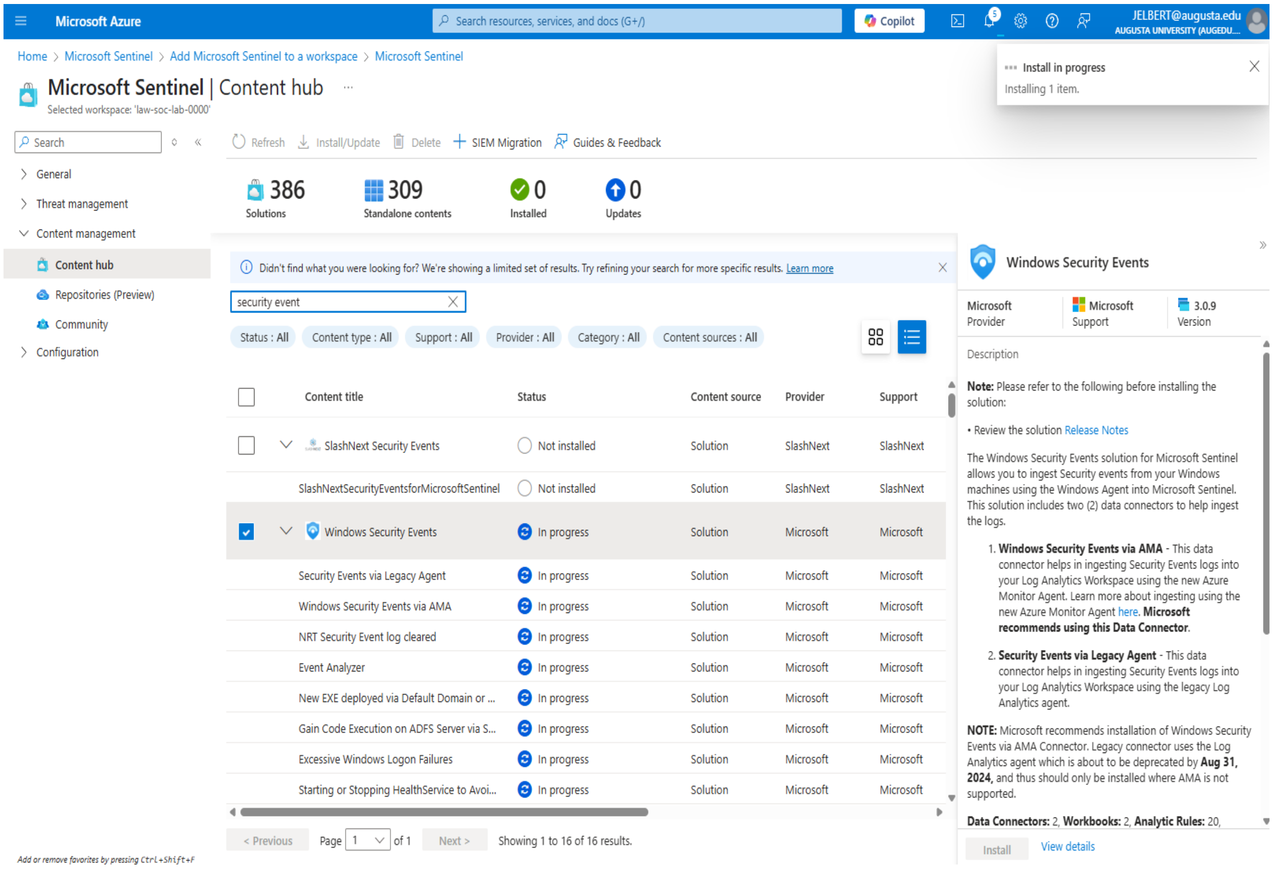
1. Collect data

Collect data at cloud scale across the enterprise from on-premises to multiple clouds.

Documentation

Data connectors documentation

Once Microsoft Sentinel was connected, it was time to install some addons. I needed to add Windows Security Events to the Microsoft Sentinel instance. Here, you can also add other things like **Cisco Umbrella**, **Amazon Web Services (AWS)**, **Log4j Vulnerability Detection**, and many other Microsoft integrations.



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...
Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel
Search
General
Threat management
Content management
Content hub
Repositories (Preview)
Community
Configuration
Refresh
Install/Update
Delete
SIEM Migration
Guides & Feedback
Add or remove favorites by pressing Ctrl+Shift+F

Microsoft Sentinel | Content hub

Selected workspace: 'law-soc-lab-0000'

Install in progress

Installing 1 item.

386 Solutions | 309 Standalone contents | 0 Installed | 0 Updates

Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results. Learn more

security event

Status : All | Content type : All | Support : All | Provider : All | Category : All | Content sources : All

	Content title	Status	Content source	Provider	Support
□	SlashNext Security Events	○ Not installed	Solution	SlashNext	SlashNext
	SlashNextSecurityEventsforMicrosoftSentinel	○ Not installed	Solution	SlashNext	SlashNext
☑	Windows Security Events	In progress	Solution	Microsoft	Microsoft
	Security Events via Legacy Agent	In progress	Solution	Microsoft	Microsoft
	Windows Security Events via AMA	In progress	Solution	Microsoft	Microsoft
	NRT Security Event log cleared	In progress	Solution	Microsoft	Microsoft
	Event Analyzer	In progress	Solution	Microsoft	Microsoft
	New EXE deployed via Default Domain or ...	In progress	Solution	Microsoft	Microsoft
	Gain Code Execution on ADFS Server via S...	In progress	Solution	Microsoft	Microsoft
	Excessive Windows Logon Failures	In progress	Solution	Microsoft	Microsoft
	Starting or Stopping HealthService to Avoi...	In progress	Solution	Microsoft	Microsoft

< Previous Page 1 of 1 Next > Showing 1 to 16 of 16 results.

Windows Security Events

Microsoft Provider | Microsoft Support | 3.0.9 Version

Description

Note: Please refer to the following before installing the solution:

- Review the solution Release Notes

The Windows Security Events solution for Microsoft Sentinel allows you to ingest Security events from your Windows machines using the Windows Agent into Microsoft Sentinel. This solution includes two (2) data connectors to help ingest the logs.

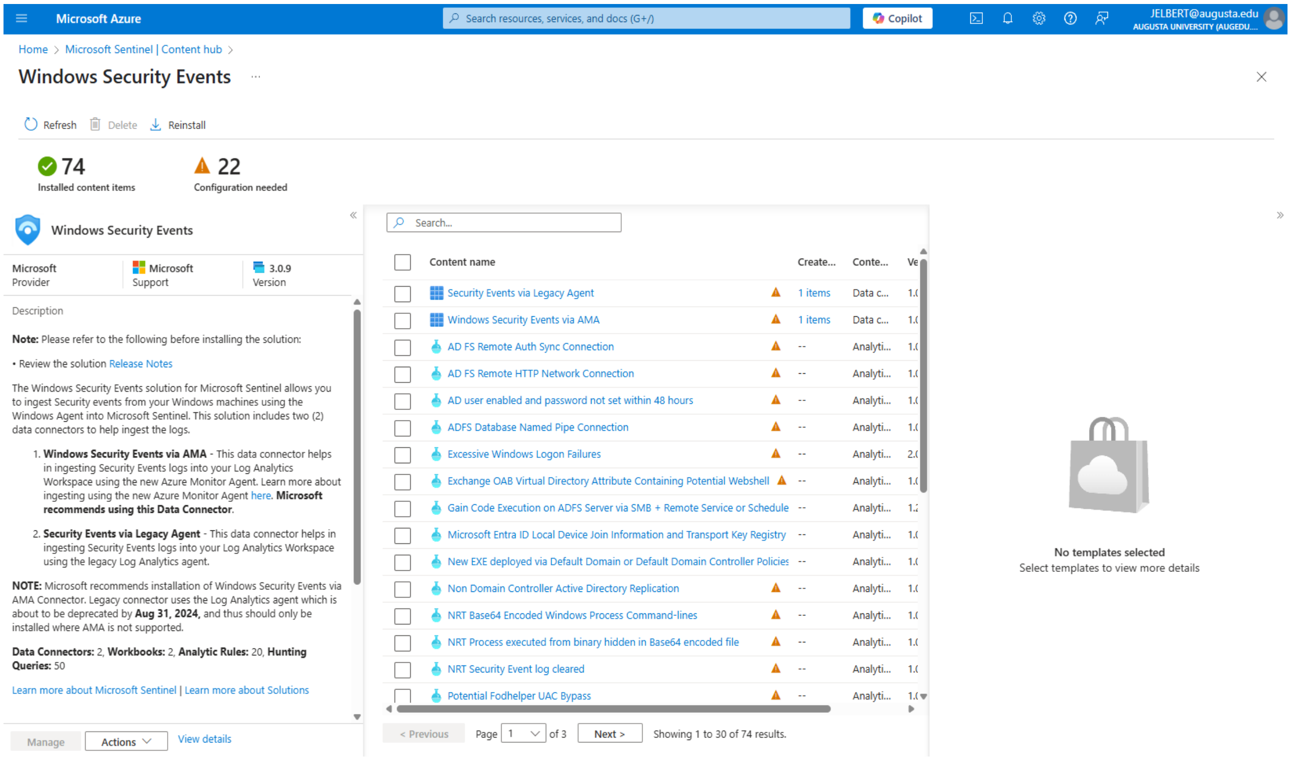
1. **Windows Security Events via AMA** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using the new Azure Monitor Agent here. **Microsoft recommends using this Data Connector**.
2. **Security Events via Legacy Agent** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the legacy Log Analytics agent.

NOTE: Microsoft recommends installation of Windows Security Events via AMA Connector. Legacy connector uses the Log Analytics agent which is about to be deprecated by **Aug 31, 2024,** and thus should only be installed where AMA is not supported.

Data Connectors: 2, **Workbooks:** 2, **Analytic Rules:** 20,

Install View details

It is now time to configure the windows security events I just installed. The one that I edited was the Windows Security Events via AMA (Azure Monitoring Agent).



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...
Home > Microsoft Sentinel | Content hub >

Windows Security Events

✅ 74 Installed content items

⚠ 22 Configuration needed

Windows Security Events

Microsoft
Provider

Microsoft
Support

3.0.9
Version

Description

Note: Please refer to the following before installing the solution:

- Review the solution Release Notes

The Windows Security Events solution for Microsoft Sentinel allows you to ingest Security events from your Windows machines using the Windows Agent into Microsoft Sentinel. This solution includes two (2) data connectors to help ingest the logs.

1. **Windows Security Events via AMA** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using the new Azure Monitor Agent here. **Microsoft recommends using this Data Connector.**
2. **Security Events via Legacy Agent** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the legacy Log Analytics agent.

NOTE: Microsoft recommends installation of Windows Security Events via AMA Connector. Legacy connector uses the Log Analytics agent which is about to be deprecated by **Aug 31, 2024**, and thus should only be installed where AMA is not supported.

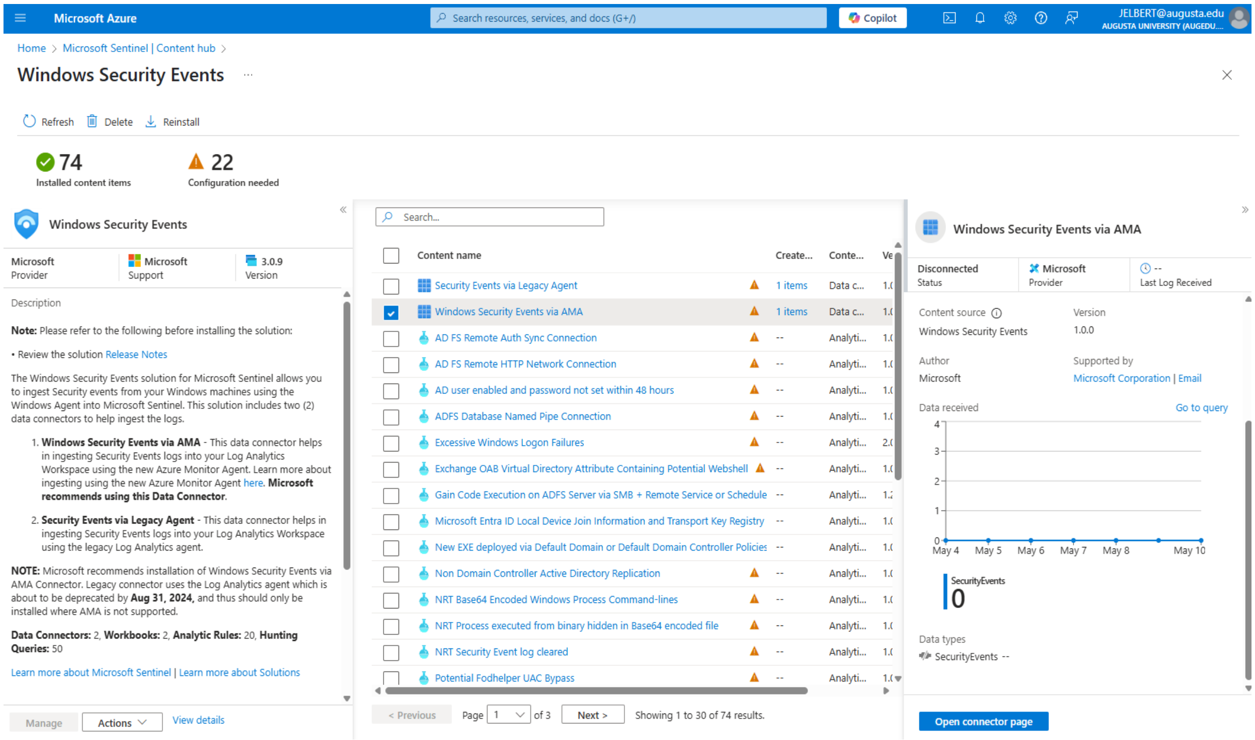
Data Connectors: 2, **Workbooks:** 2, **Analytic Rules:** 20, **Hunting Queries:** 50

Learn more about Microsoft Sentinel | Learn more about Solutions

□	Content name		Create...	Conte...	Ve
□	Security Events via Legacy Agent	⚠	1 items	Data c...	1.(
□	Windows Security Events via AMA	⚠	1 items	Data c...	1.(
□	AD FS Remote Auth Sync Connection	⚠	--	Analyti...	1.(
□	AD FS Remote HTTP Network Connection	⚠	--	Analyti...	1.(
□	AD user enabled and password not set within 48 hours	⚠	--	Analyti...	1.(
□	ADFS Database Named Pipe Connection	⚠	--	Analyti...	1.(
□	Excessive Windows Logon Failures	⚠	--	Analyti...	2.(
□	Exchange OAB Virtual Directory Attribute Containing Potential Webshell	⚠	--	Analyti...	1.(
□	Gain Code Execution on ADFS Server via SMB + Remote Service or Schedule		--	Analyti...	1.2
□	Microsoft Entra ID Local Device Join Information and Transport Key Registry		--	Analyti...	1.(
□	New EXE deployed via Default Domain or Default Domain Controller Policies		--	Analyti...	1.(
□	Non Domain Controller Active Directory Replication	⚠	--	Analyti...	1.(
□	NRT Base64 Encoded Windows Process Command-lines	⚠	--	Analyti...	1.(
□	NRT Process executed from binary hidden in Base64 encoded file	⚠	--	Analyti...	1.(
□	NRT Security Event log cleared	⚠	--	Analyti...	1.(
□	Potential Fodhelper UAC Bypass	⚠	--	Analyti...	1.(

< Previous Page 1 of 3 Next > Showing 1 to 30 of 74 results.

No templates selected
Select templates to view more details



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...
Home > Microsoft Sentinel | Content hub >

Windows Security Events

✅ 74 Installed content items

⚠ 22 Configuration needed

Windows Security Events

Microsoft
Provider

Microsoft
Support

3.0.9
Version

Description

Note: Please refer to the following before installing the solution:

- Review the solution Release Notes

The Windows Security Events solution for Microsoft Sentinel allows you to ingest Security events from your Windows machines using the Windows Agent into Microsoft Sentinel. This solution includes two (2) data connectors to help ingest the logs.

1. **Windows Security Events via AMA** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using the new Azure Monitor Agent here. **Microsoft recommends using this Data Connector.**
2. **Security Events via Legacy Agent** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the legacy Log Analytics agent.

NOTE: Microsoft recommends installation of Windows Security Events via AMA Connector. Legacy connector uses the Log Analytics agent which is about to be deprecated by **Aug 31, 2024**, and thus should only be installed where AMA is not supported.

Data Connectors: 2, **Workbooks:** 2, **Analytic Rules:** 20, **Hunting Queries:** 50

Learn more about Microsoft Sentinel | Learn more about Solutions

□	Content name		Create...	Conte...	Ve
□	Security Events via Legacy Agent	⚠	1 items	Data c...	1.(
☑	Windows Security Events via AMA	⚠	1 items	Data c...	1.(
□	AD FS Remote Auth Sync Connection	⚠	--	Analyti...	1.(
□	AD FS Remote HTTP Network Connection	⚠	--	Analyti...	1.(
□	AD user enabled and password not set within 48 hours	⚠	--	Analyti...	1.(
□	ADFS Database Named Pipe Connection	⚠	--	Analyti...	1.(
□	Excessive Windows Logon Failures	⚠	--	Analyti...	2.(
□	Exchange OAB Virtual Directory Attribute Containing Potential Webshell	⚠	--	Analyti...	1.(
□	Gain Code Execution on ADFS Server via SMB + Remote Service or Schedule		--	Analyti...	1.2
□	Microsoft Entra ID Local Device Join Information and Transport Key Registry		--	Analyti...	1.(
□	New EXE deployed via Default Domain or Default Domain Controller Policies		--	Analyti...	1.(
□	Non Domain Controller Active Directory Replication	⚠	--	Analyti...	1.(
□	NRT Base64 Encoded Windows Process Command-lines	⚠	--	Analyti...	1.(
□	NRT Process executed from binary hidden in Base64 encoded file	⚠	--	Analyti...	1.(
□	NRT Security Event log cleared	⚠	--	Analyti...	1.(
□	Potential Fodhelper UAC Bypass	⚠	--	Analyti...	1.(

< Previous Page 1 of 3 Next > Showing 1 to 30 of 74 results.

Windows Security Events via AMA

Disconnected
Status

Microsoft
Provider

--
Last Log Received

Content source: Windows Security Events

Version: 1.0.0

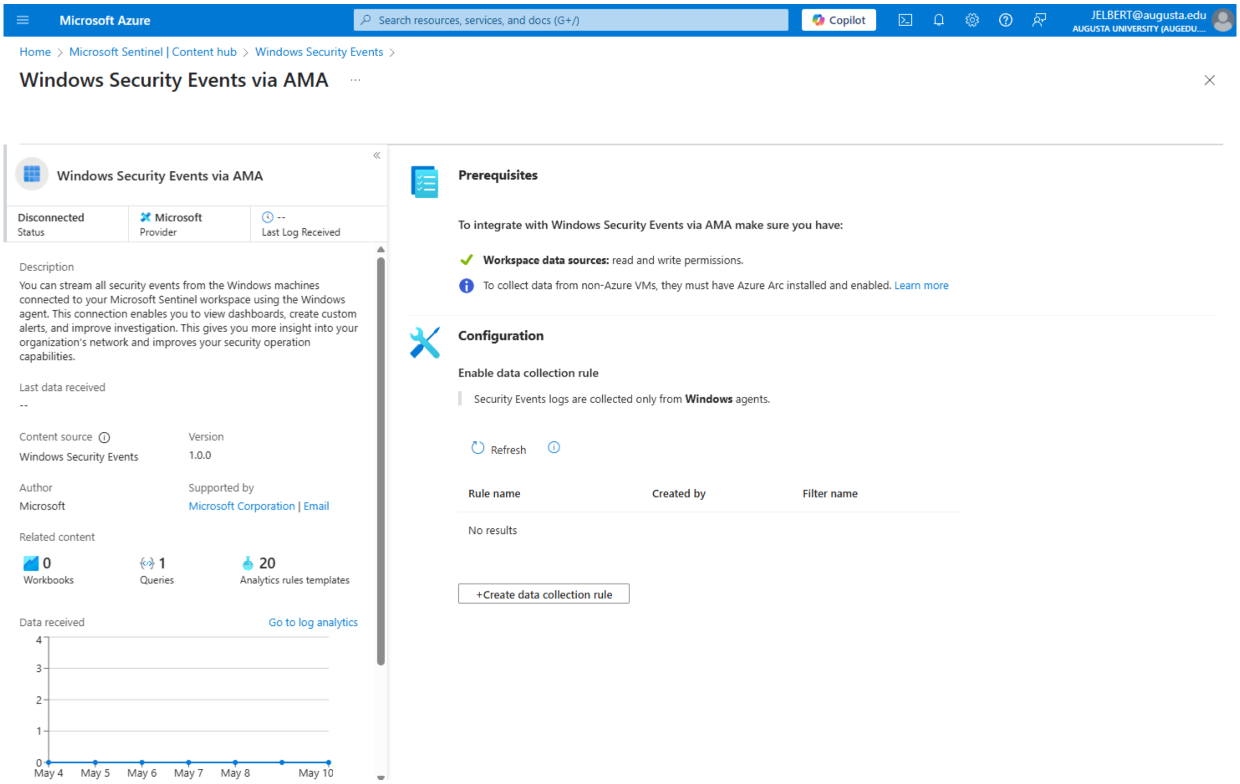
Author: Microsoft

Supported by: Microsoft Corporation | Email

Data received

Data types

SecurityEvents --


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...
Home > Microsoft Sentinel | Content hub > Windows Security Events >

Windows Security Events via AMA

Windows Security Events via AMA

Disconnected	Microsoft	--
Status	Provider	Last Log Received

Description

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Last data received

--

Content source: Windows Security Events

Version: 1.0.0

Author: Microsoft

Supported by: Microsoft Corporation | Email

Related content

0	1	20
Workbooks	Queries	Analytics rules templates

Data received — Go to log analytics

Prerequisites

To integrate with Windows Security Events via AMA make sure you have:

✓ **Workspace data sources:** read and write permissions.

ⓘ To collect data from non-Azure VMs, they must have Azure Arc installed and enabled. Learn more

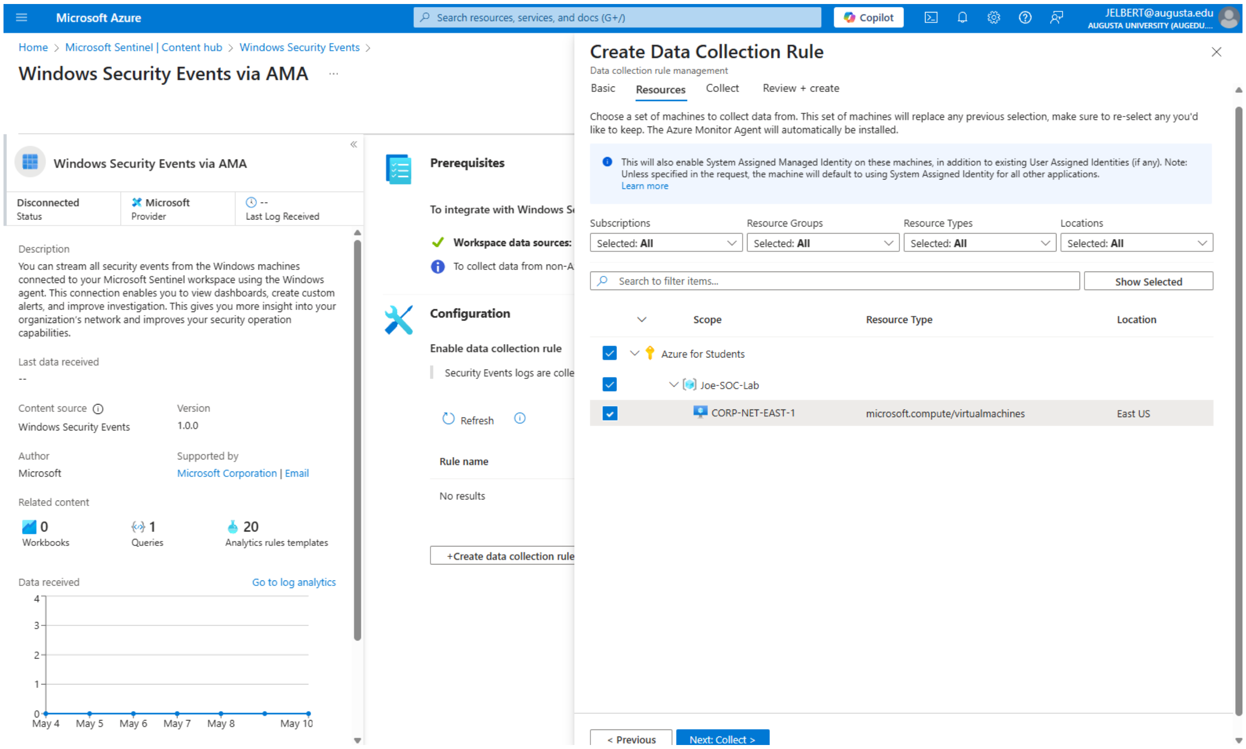
Configuration

Enable data collection rule

Security Events logs are collected only from **Windows** agents.

Rule name	Created by	Filter name
No results		

+Create data collection rule


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...
Home > Microsoft Sentinel | Content hub > Windows Security Events >

Windows Security Events via AMA

Windows Security Events via AMA

Disconnected Status | Microsoft Provider | -- Last Log Received

Description

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Last data received

--

Content source: Windows Security Events

Version: 1.0.0

Author: Microsoft

Supported by: Microsoft Corporation | Email

Related content: 0 Workbooks, 1 Queries, 20 Analytics rules templates

Data received — Go to log analytics

Prerequisites

To integrate with Windows S

Workspace data sources:

To collect data from non-A

Configuration

Enable data collection rule

Security Events logs are colle

Refresh

Rule name

No results

+Create data collection rule

Create Data Collection Rule

Data collection rule management

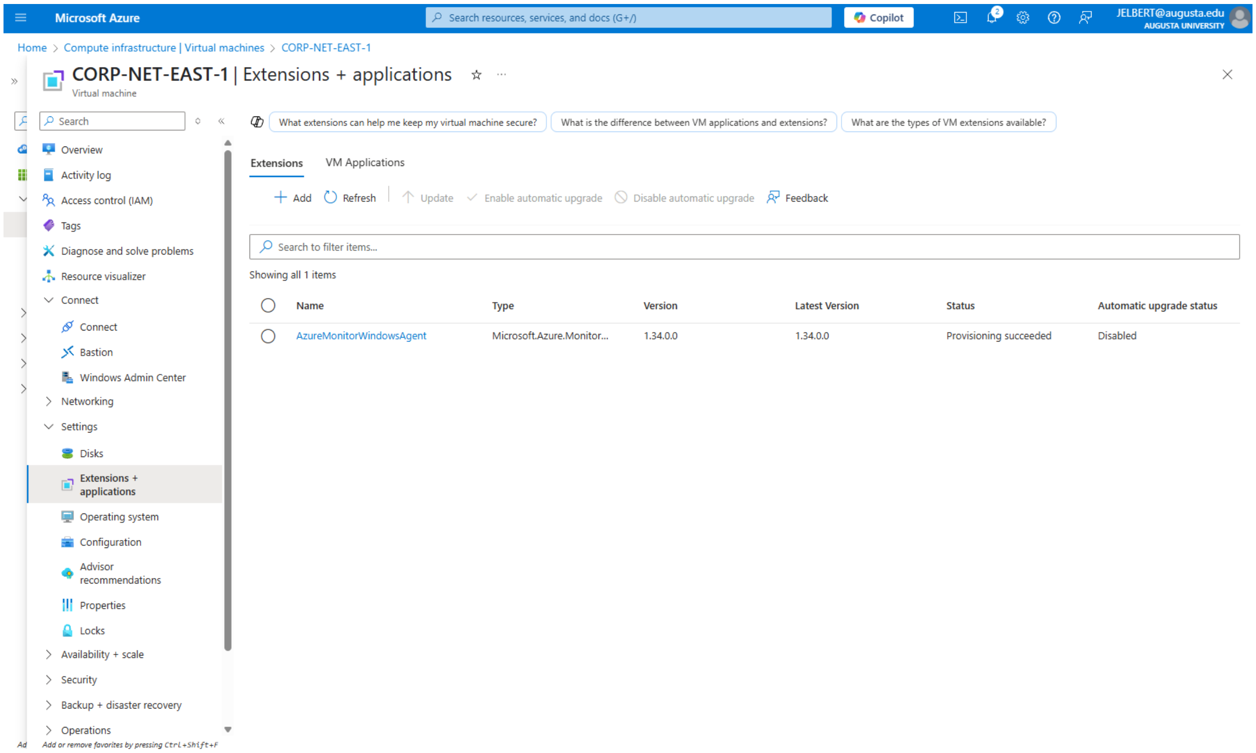
Choose a set of machines to collect data from. This set of machines will replace any previous selection, make sure to re-select any you'd like to keep. The Azure Monitor Agent will automatically be installed.

ⓘ This will also enable System Assigned Managed Identity on these machines, in addition to existing User Assigned Identities (if any). Note: Unless specified in the request, the machine will default to using System Assigned Identity for all other applications. Learn more

Subscriptions	Resource Groups	Resource Types	Locations
Selected: **All**	Selected: **All**	Selected: **All**	Selected: **All**

	Scope	Resource Type	Location
☑	Azure for Students		
☑	Joe-SOC-Lab		
☑	CORP-NET-EAST-1	microsoft.compute/virtualmachines	East US

I went into my VM and I needed to install an Azure monitoring agent in order for the logs to be sent to the Log Analytics Workspace, and then to the Microsoft Sentinel instance.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
JELBERT@augusta.edu
AUGUSTA UNIVERSITY
Home > Compute infrastructure | Virtual machines > CORP-NET-EAST-1
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Connect
Bastion
Windows Admin Center
Networking
Settings
Disks
Extensions + applications
Operating system
Configuration
Advisor recommendations
Properties
Locks
Availability + scale
Security
Backup + disaster recovery
Operations
Add or remove favorites by pressing Ctrl+Shift+F
What extensions can help me keep my virtual machine secure?
What is the difference between VM applications and extensions?
What are the types of VM extensions available?
Extensions
VM Applications
Add
Refresh
Update
Enable automatic upgrade
Disable automatic upgrade
Feedback
Search to filter items...

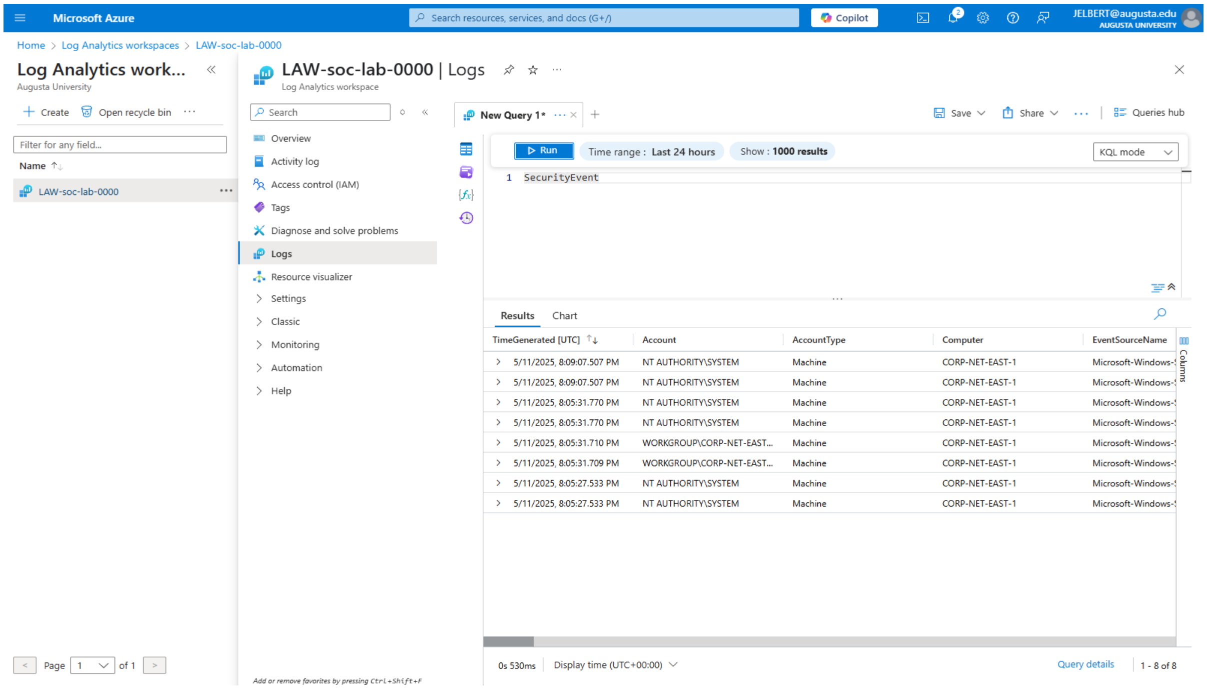
CORP-NET-EAST-1 | Extensions + applications

Virtual machine

Showing all 1 items

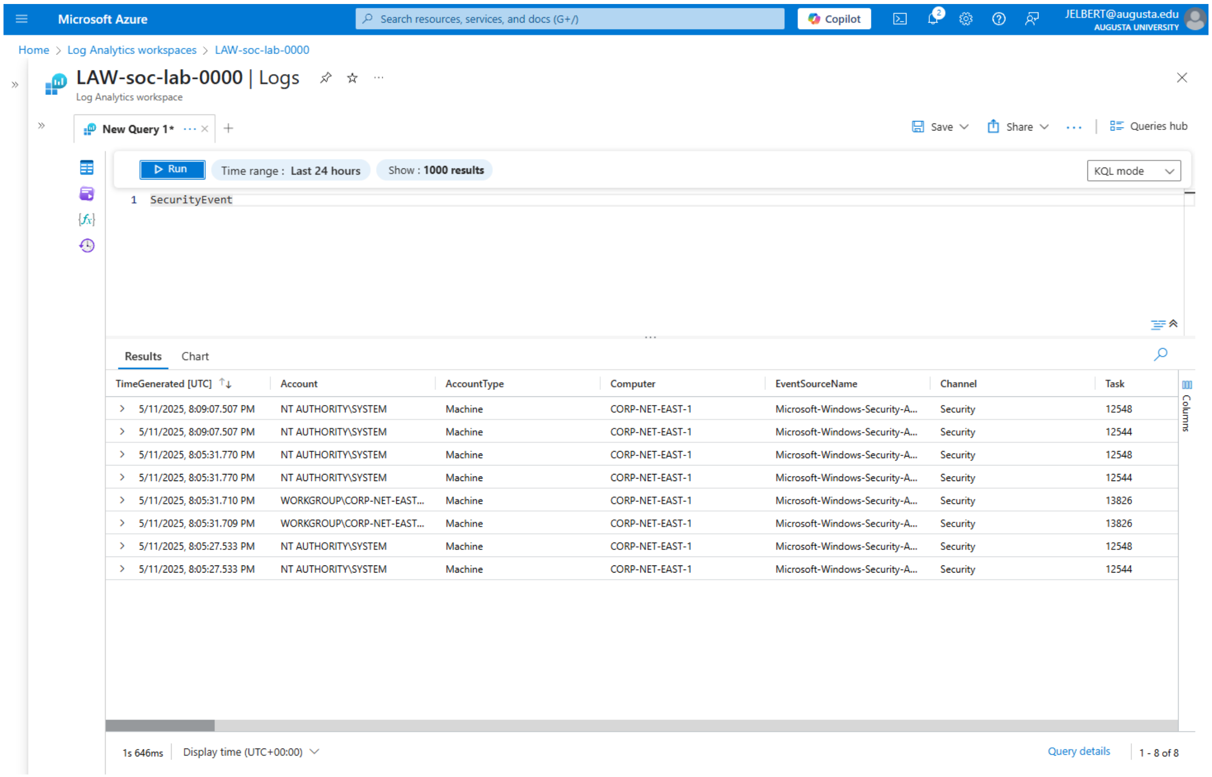
	Name	Type	Version	Latest Version	Status	Automatic upgrade status
○	AzureMonitorWindowsAgent	Microsoft.Azure.Monitor...	1.34.0.0	1.34.0.0	Provisioning succeeded	Disabled

Once it was connected, I had to wait like 5-10 minutes in order to receive my first set of logs. Microsoft Sentinel uses KQL which is similar to SQL (The language I am familiar with), and it helps query the results of the logs in order to find specific logs easier.



```
SecurityEvent
```

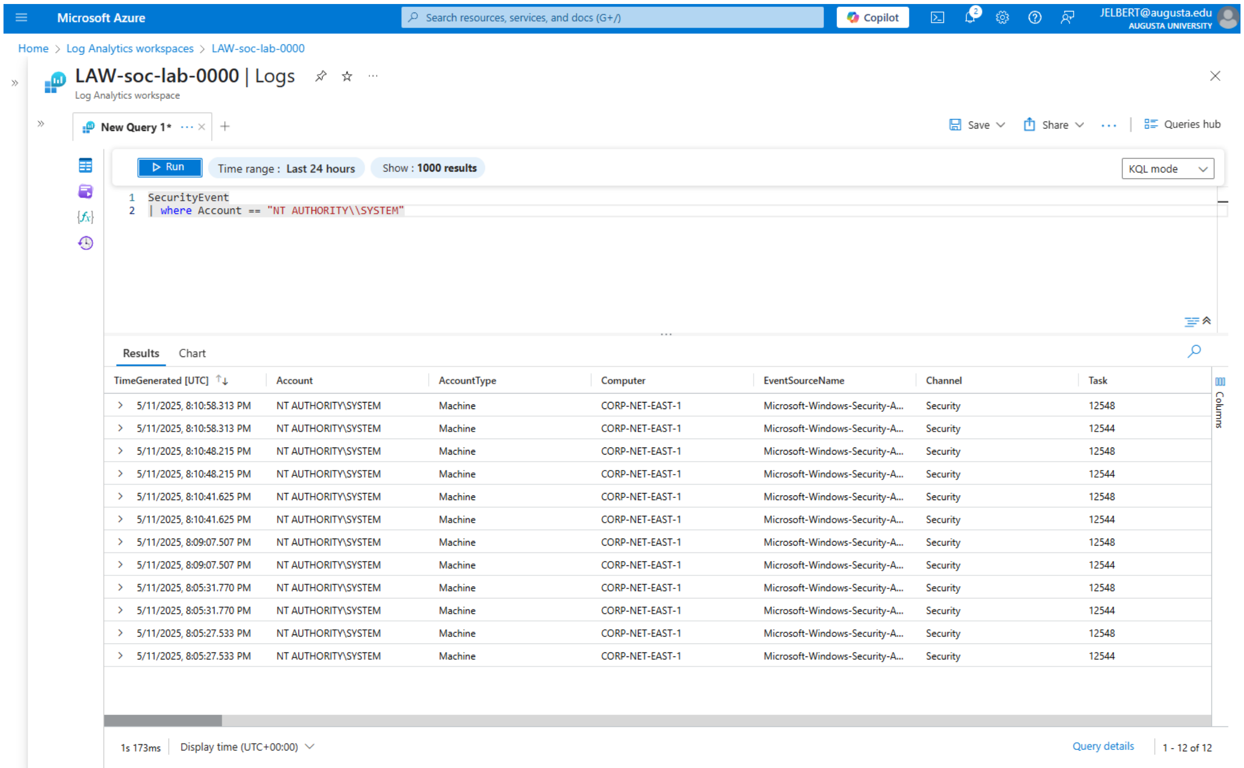
TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName
5/11/2025, 8:09:07.507 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-S
5/11/2025, 8:09:07.507 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-S
5/11/2025, 8:05:31.770 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-S
5/11/2025, 8:05:31.770 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-S
5/11/2025, 8:05:31.710 PM	WORKGROUP\CORP-NET-EAST...	Machine	CORP-NET-EAST-1	Microsoft-Windows-S
5/11/2025, 8:05:31.709 PM	WORKGROUP\CORP-NET-EAST...	Machine	CORP-NET-EAST-1	Microsoft-Windows-S
5/11/2025, 8:05:27.533 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-S
5/11/2025, 8:05:27.533 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-S



```
SecurityEvent
```

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName	Channel	Task
5/11/2025, 8:09:07.507 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12548
5/11/2025, 8:09:07.507 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12544
5/11/2025, 8:05:31.770 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12548
5/11/2025, 8:05:31.770 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12544
5/11/2025, 8:05:31.710 PM	WORKGROUP\CORP-NET-EAST...	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	13826
5/11/2025, 8:05:31.709 PM	WORKGROUP\CORP-NET-EAST...	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	13826
5/11/2025, 8:05:27.533 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12548
5/11/2025, 8:05:27.533 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12544

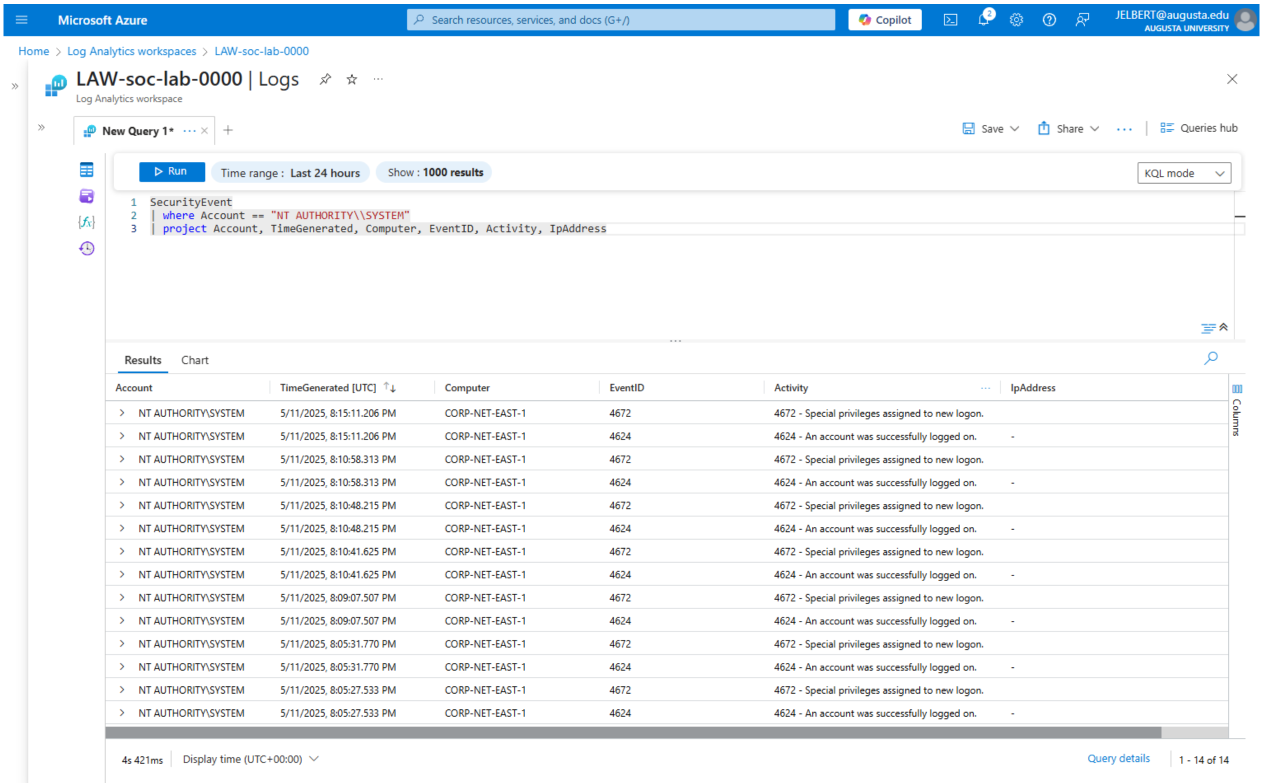
This was my first official KQL query. It searches the SecurityEvent logs table and has parameters that are specified with each | character.



```
SecurityEvent
| where Account == "NT AUTHORITY\\SYSTEM"
```

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName	Channel	Task
5/11/2025, 8:10:58.313 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12548
5/11/2025, 8:10:58.313 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12544
5/11/2025, 8:10:48.215 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12548
5/11/2025, 8:10:48.215 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12544
5/11/2025, 8:10:41.625 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12548
5/11/2025, 8:10:41.625 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12544
5/11/2025, 8:09:07.507 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12548
5/11/2025, 8:09:07.507 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12544
5/11/2025, 8:05:31.770 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12548
5/11/2025, 8:05:31.770 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12544
5/11/2025, 8:05:27.533 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12548
5/11/2025, 8:05:27.533 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12544

1s 173ms | Display time (UTC+00:00) | Query details | 1 - 12 of 12

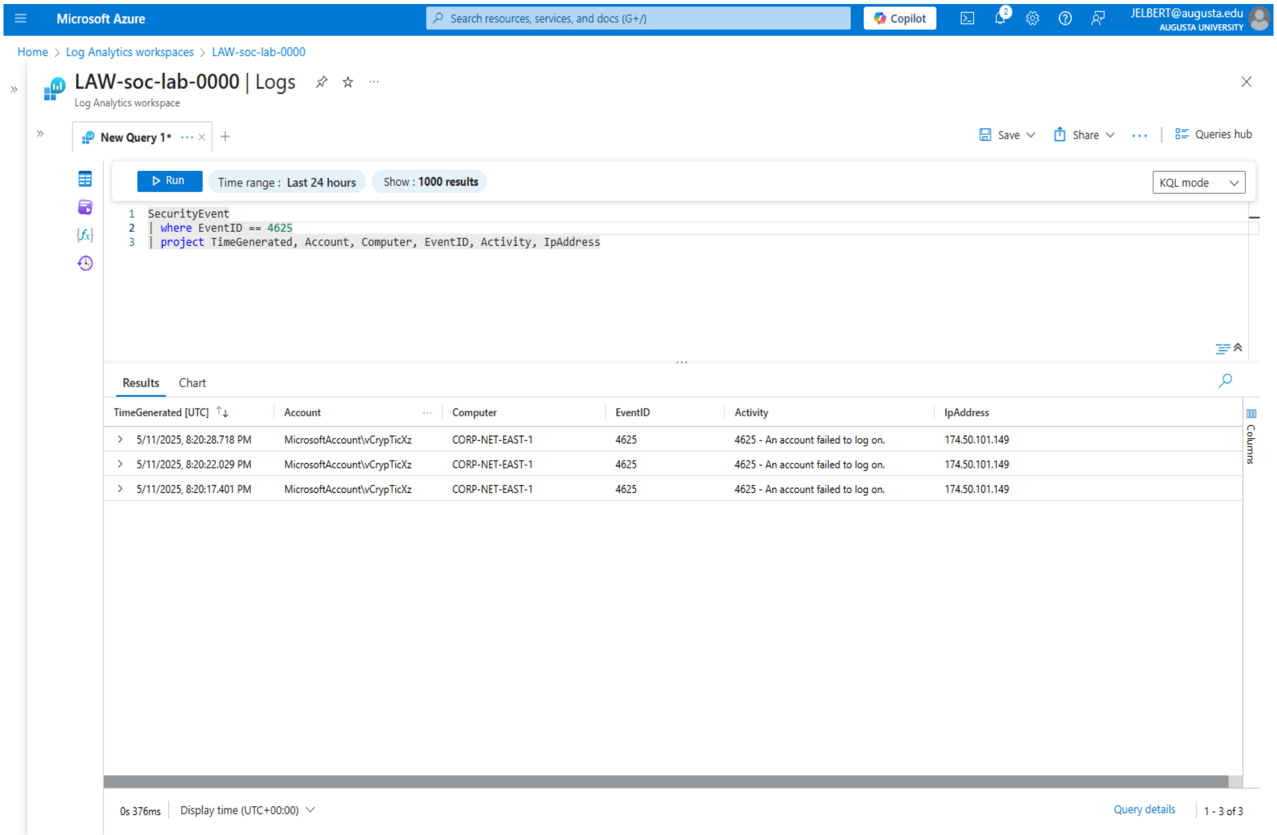


```
SecurityEvent
| where Account == "NT AUTHORITY\\SYSTEM"
| project Account, TimeGenerated, Computer, EventID, Activity, IpAddress
```

Account	TimeGenerated [UTC]	Computer	EventID	Activity	IpAddress
NT AUTHORITY\SYSTEM	5/11/2025, 8:15:11.206 PM	CORP-NET-EAST-1	4672	4672 - Special privileges assigned to new logon.	
NT AUTHORITY\SYSTEM	5/11/2025, 8:15:11.206 PM	CORP-NET-EAST-1	4624	4624 - An account was successfully logged on.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:10:58.313 PM	CORP-NET-EAST-1	4672	4672 - Special privileges assigned to new logon.	
NT AUTHORITY\SYSTEM	5/11/2025, 8:10:58.313 PM	CORP-NET-EAST-1	4624	4624 - An account was successfully logged on.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:10:48.215 PM	CORP-NET-EAST-1	4672	4672 - Special privileges assigned to new logon.	
NT AUTHORITY\SYSTEM	5/11/2025, 8:10:48.215 PM	CORP-NET-EAST-1	4624	4624 - An account was successfully logged on.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:10:41.625 PM	CORP-NET-EAST-1	4672	4672 - Special privileges assigned to new logon.	
NT AUTHORITY\SYSTEM	5/11/2025, 8:10:41.625 PM	CORP-NET-EAST-1	4624	4624 - An account was successfully logged on.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:09:07.507 PM	CORP-NET-EAST-1	4672	4672 - Special privileges assigned to new logon.	
NT AUTHORITY\SYSTEM	5/11/2025, 8:09:07.507 PM	CORP-NET-EAST-1	4624	4624 - An account was successfully logged on.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:05:31.770 PM	CORP-NET-EAST-1	4672	4672 - Special privileges assigned to new logon.	
NT AUTHORITY\SYSTEM	5/11/2025, 8:05:31.770 PM	CORP-NET-EAST-1	4624	4624 - An account was successfully logged on.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:05:27.533 PM	CORP-NET-EAST-1	4672	4672 - Special privileges assigned to new logon.	
NT AUTHORITY\SYSTEM	5/11/2025, 8:05:27.533 PM	CORP-NET-EAST-1	4624	4624 - An account was successfully logged on.	-

4s 421ms | Display time (UTC+00:00) | Query details | 1 - 14 of 14

This query lets me use “**project**” in order to only show columns in the query results that I want to see. This shows that a user tried to logon to the system 3 times and failed each time.



Time range : Last 24 hours

Show : 1000 results

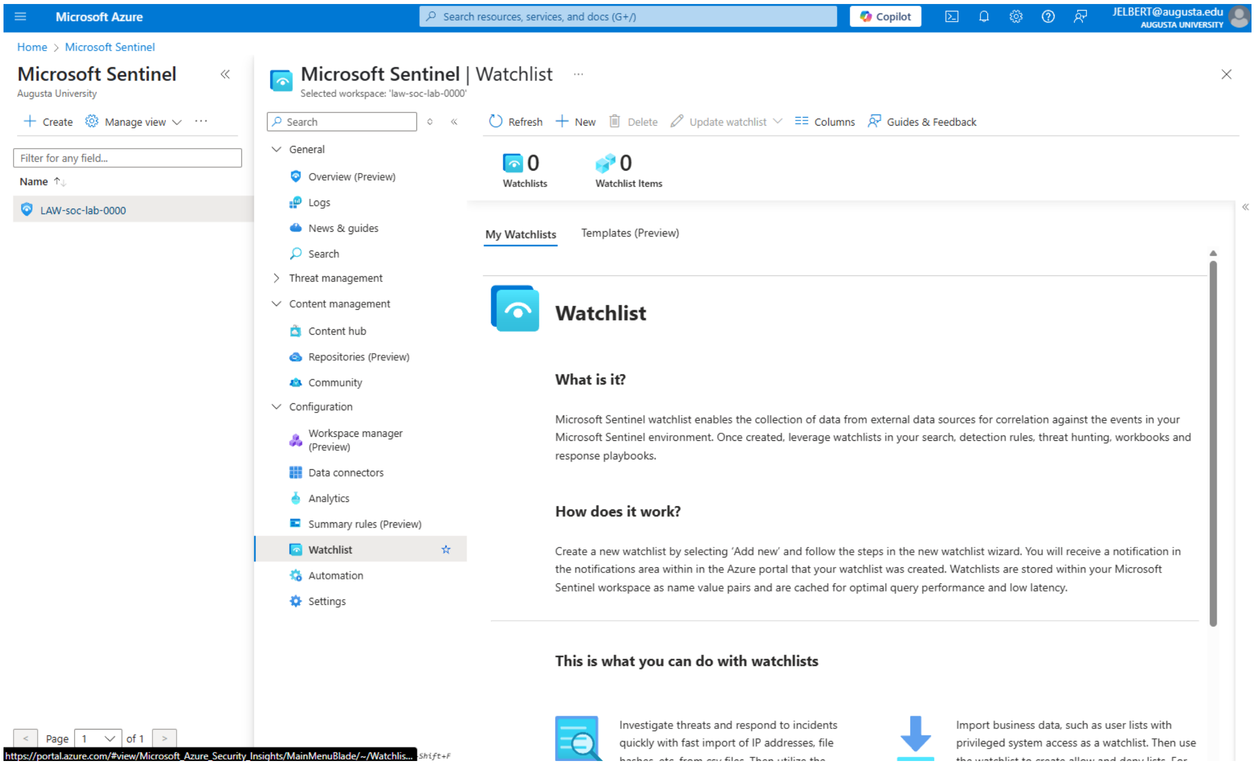
```
SecurityEvent
| where EventID == 4625
| project TimeGenerated, Account, Computer, EventID, Activity, IpAddress
```

TimeGenerated [UTC]	Account	Computer	EventID	Activity	IpAddress
5/11/2025, 8:20:28.718 PM	MicrosoftAccount\vCrypTicXz	CORP-NET-EAST-1	4625	4625 - An account failed to log on.	174.50.101.149
5/11/2025, 8:20:22.029 PM	MicrosoftAccount\vCrypTicXz	CORP-NET-EAST-1	4625	4625 - An account failed to log on.	174.50.101.149
5/11/2025, 8:20:17.401 PM	MicrosoftAccount\vCrypTicXz	CORP-NET-EAST-1	4625	4625 - An account failed to log on.	174.50.101.149

0s 376ms | Display time (UTC+00:00)

1 - 3 of 3

Now, I need to setup a watchlist to make it easier to see where IP addresses are connecting from. Information like their country, city, and coordinates.



Watchlist

What is it?

Microsoft Sentinel watchlist enables the collection of data from external data sources for correlation against the events in your Microsoft Sentinel environment. Once created, leverage watchlists in your search, detection rules, threat hunting, workbooks and response playbooks.

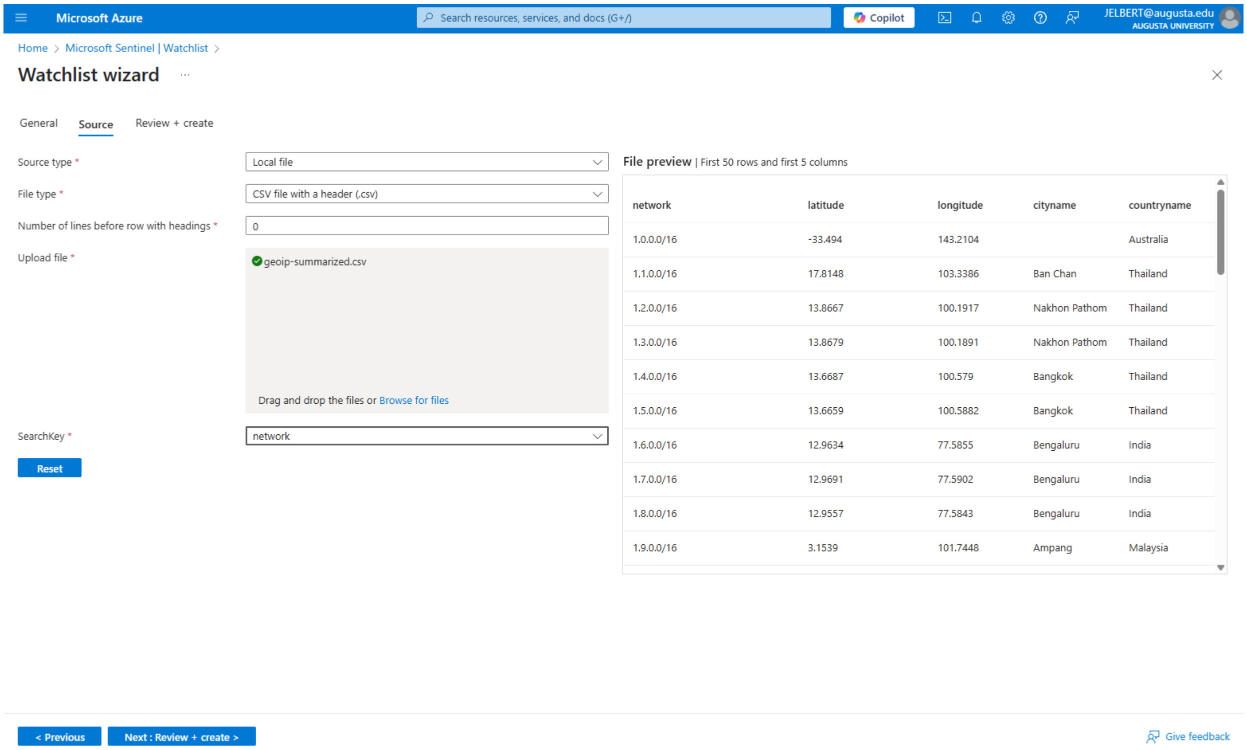
How does it work?

Create a new watchlist by selecting 'Add new' and follow the steps in the new watchlist wizard. You will receive a notification in the notifications area within in the Azure portal that your watchlist was created. Watchlists are stored within your Microsoft Sentinel workspace as name value pairs and are cached for optimal query performance and low latency.

This is what you can do with watchlists

Investigate threats and respond to incidents quickly with fast import of IP addresses, file

Import business data, such as user lists with privileged system access as a watchlist. Then use



Source type * Local file

File type * CSV file with a header (.csv)

Number of lines before row with headings * 0

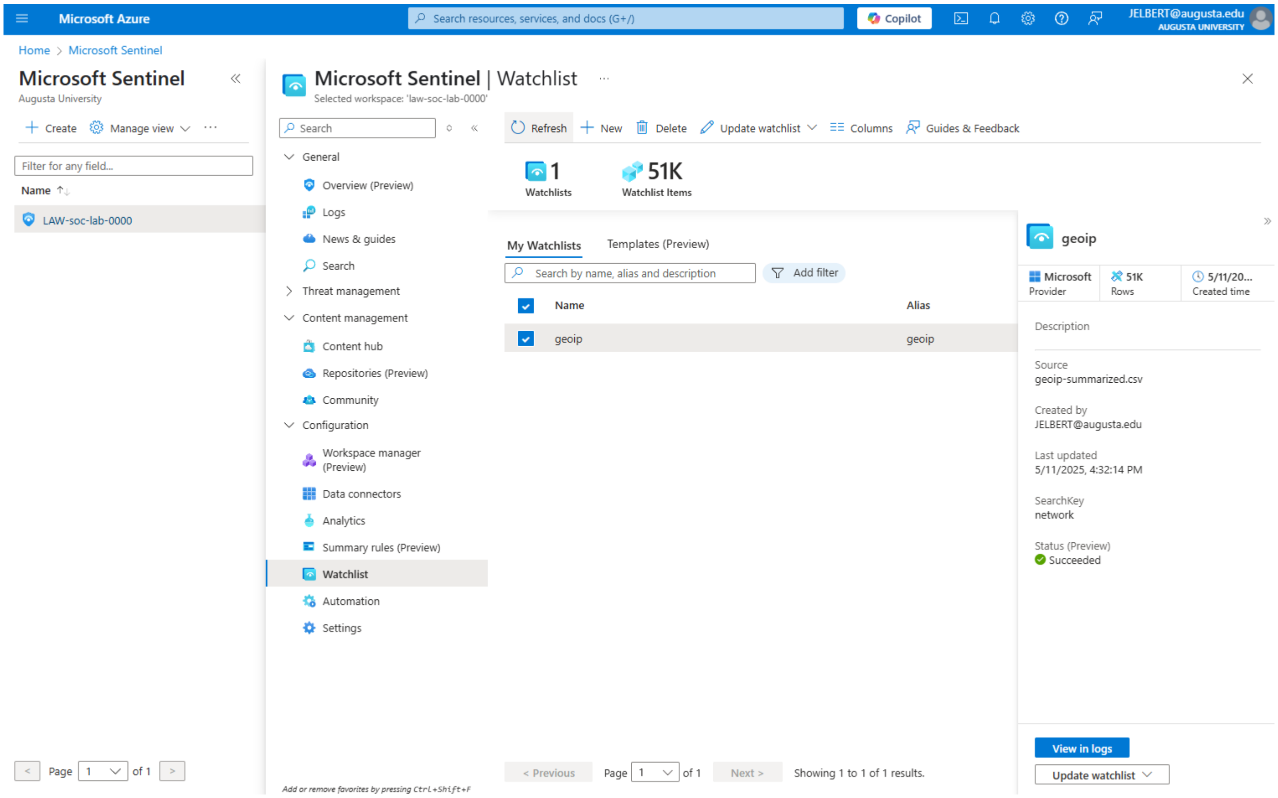
Upload file * geoip-summarized.csv

Drag and drop the files or Browse for files

SearchKey * network

File preview | First 50 rows and first 5 columns

network	latitude	longitude	cityname	countryname
1.0.0.0/16	-33.494	143.2104		Australia
1.1.0.0/16	17.8148	103.3386	Ban Chan	Thailand
1.2.0.0/16	13.8667	100.1917	Nakhon Pathom	Thailand
1.3.0.0/16	13.8679	100.1891	Nakhon Pathom	Thailand
1.4.0.0/16	13.6687	100.579	Bangkok	Thailand
1.5.0.0/16	13.6659	100.5882	Bangkok	Thailand
1.6.0.0/16	12.9634	77.5855	Bengaluru	India
1.7.0.0/16	12.9691	77.5902	Bengaluru	India
1.8.0.0/16	12.9557	77.5843	Bengaluru	India
1.9.0.0/16	3.1539	101.7448	Ampang	Malaysia



Microsoft Sentinel | Watchlist

Selected workspace: 'law-soc-lab-0000'

1 Watchlists

51K Watchlist Items

☑	Name	Alias
☑	geoip	geoip

Showing 1 to 1 of 1 results.

geoip

Microsoft	51K	5/11/20...
Provider	Rows	Created time

Description

Source
geoip-summarized.csv

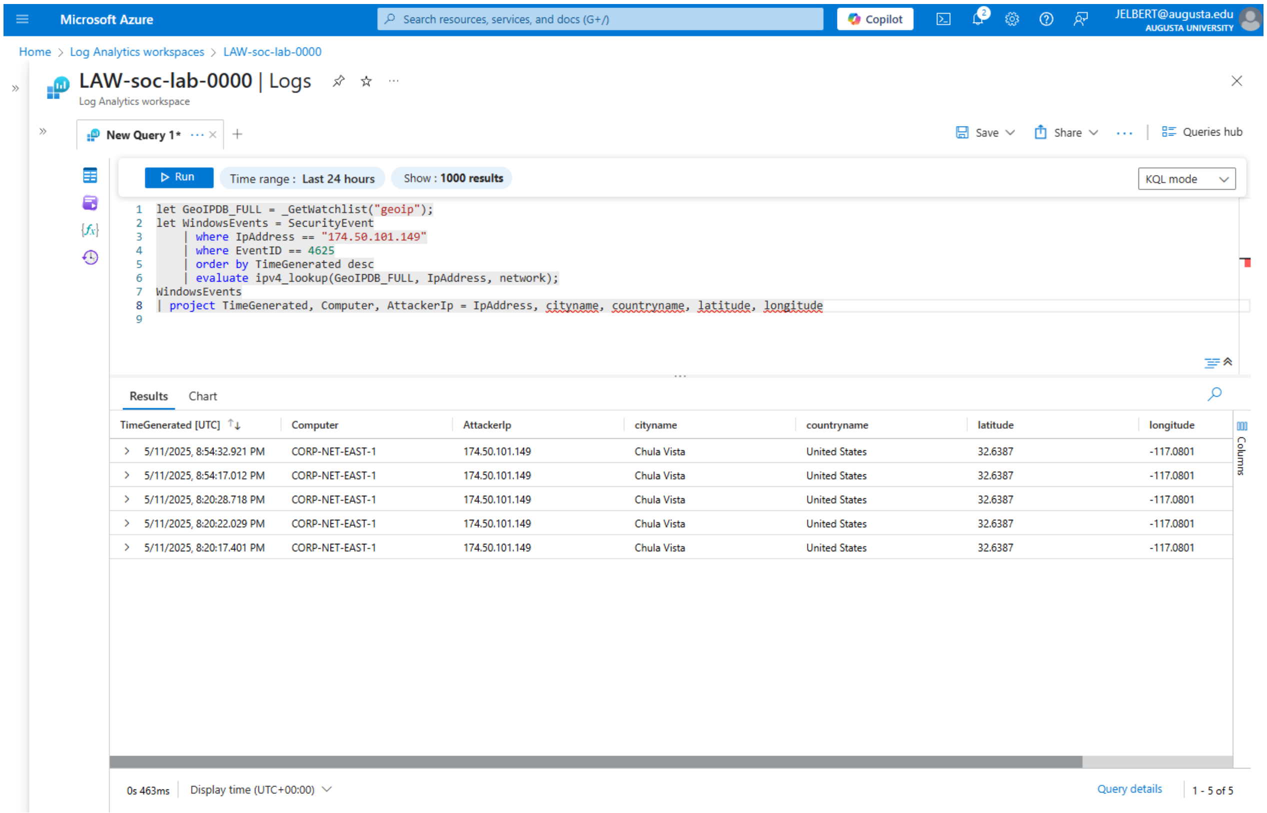
Created by
JELBERT@augusta.edu

Last updated
5/11/2025, 4:32:14 PM

SearchKey
network

Status (Preview)
Succeeded

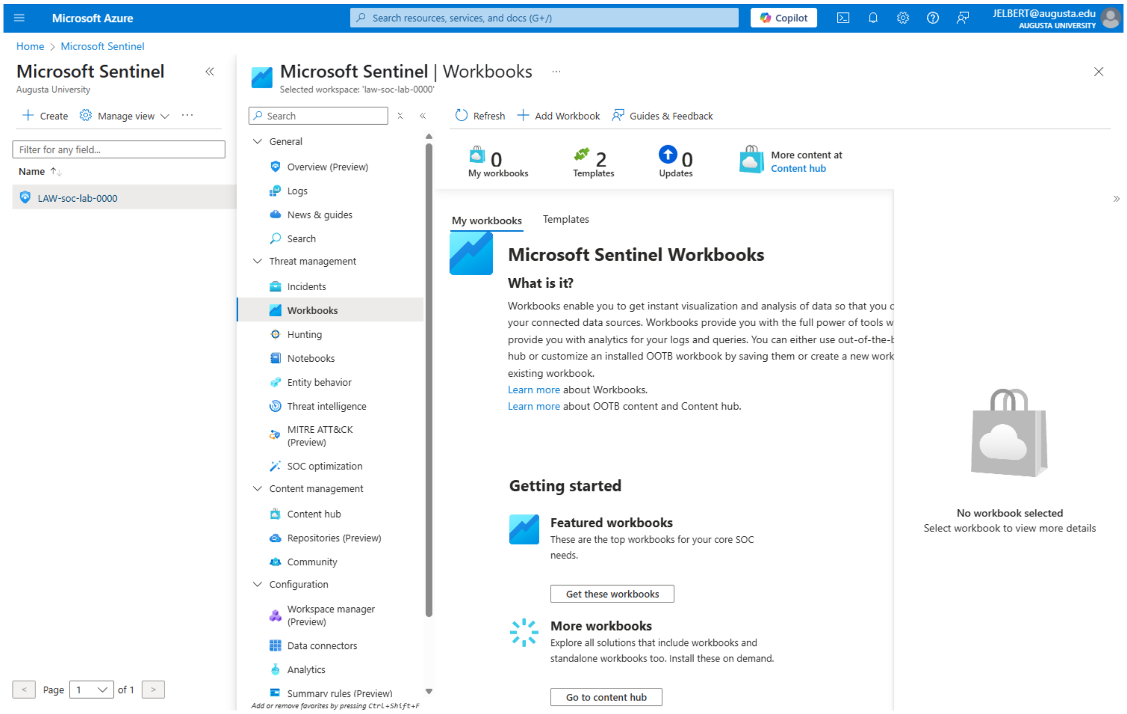
The watchlist is uploaded, so now I can filter through the logs again to find exactly where the user is trying to login from. This is a more advanced KQL query.



```
let GeoIPDB_FULL = _GetWatchlist("geoip");
let WindowsEvents = SecurityEvent
    | where IpAddress == "174.50.101.149"
    | where EventID == 4625
    | order by TimeGenerated desc
    | evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network);
WindowsEvents
| project TimeGenerated, Computer, AttackerIp = IpAddress, cityname, countryname, latitude, longitude
```

TimeGenerated [UTC]	Computer	AttackerIp	cityname	countryname	latitude	longitude
5/11/2025, 8:54:32.921 PM	CORP-NET-EAST-1	174.50.101.149	Chula Vista	United States	32.6387	-117.0801
5/11/2025, 8:54:17.012 PM	CORP-NET-EAST-1	174.50.101.149	Chula Vista	United States	32.6387	-117.0801
5/11/2025, 8:20:28.718 PM	CORP-NET-EAST-1	174.50.101.149	Chula Vista	United States	32.6387	-117.0801
5/11/2025, 8:20:22.029 PM	CORP-NET-EAST-1	174.50.101.149	Chula Vista	United States	32.6387	-117.0801
5/11/2025, 8:20:17.401 PM	CORP-NET-EAST-1	174.50.101.149	Chula Vista	United States	32.6387	-117.0801

After running that query to confirm that the watchlist was successfully uploaded. I then had to make a workbook in order to help me map the attacks. In the workbook advanced editor, I pasted some JSON that will help draw a map on the screen and help me visualize the attacks.



Microsoft Sentinel Workbooks

What is it?

Workbooks enable you to get instant visualization and analysis of data so that you c
your connected data sources. Workbooks provide you with the full power of tools w
provide you with analytics for your logs and queries. You can either use out-of-the-b
hub or customize an installed OOTB workbook by saving them or create a new work
existing workbook.
Learn more about Workbooks.
Learn more about OOTB content and Content hub.

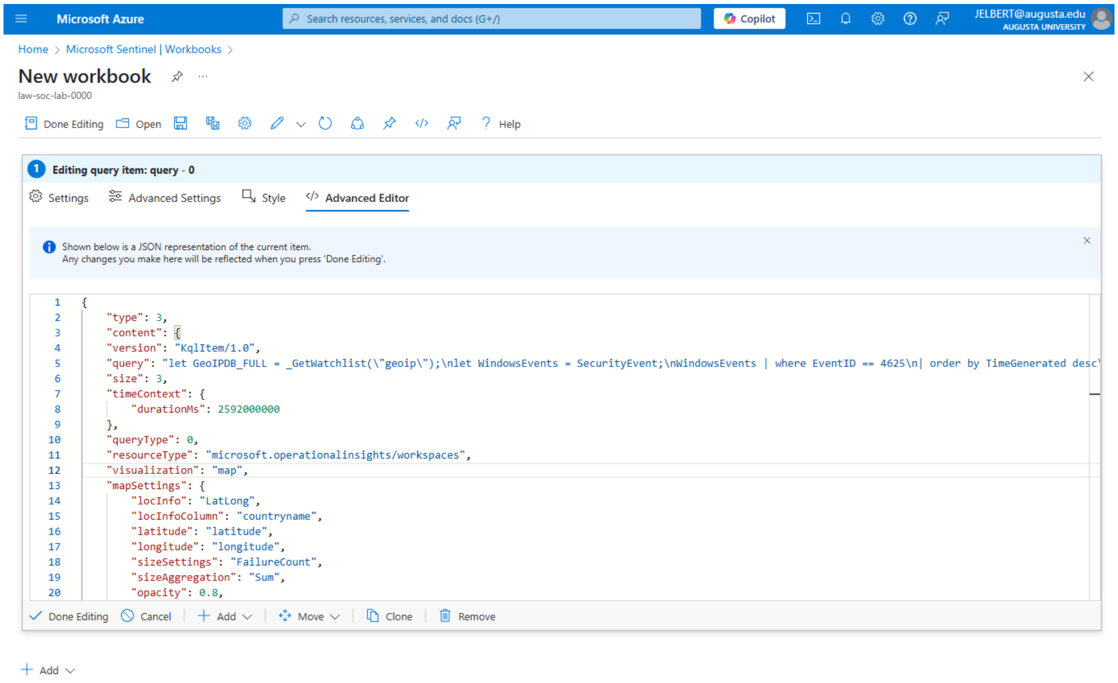
Getting started

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.

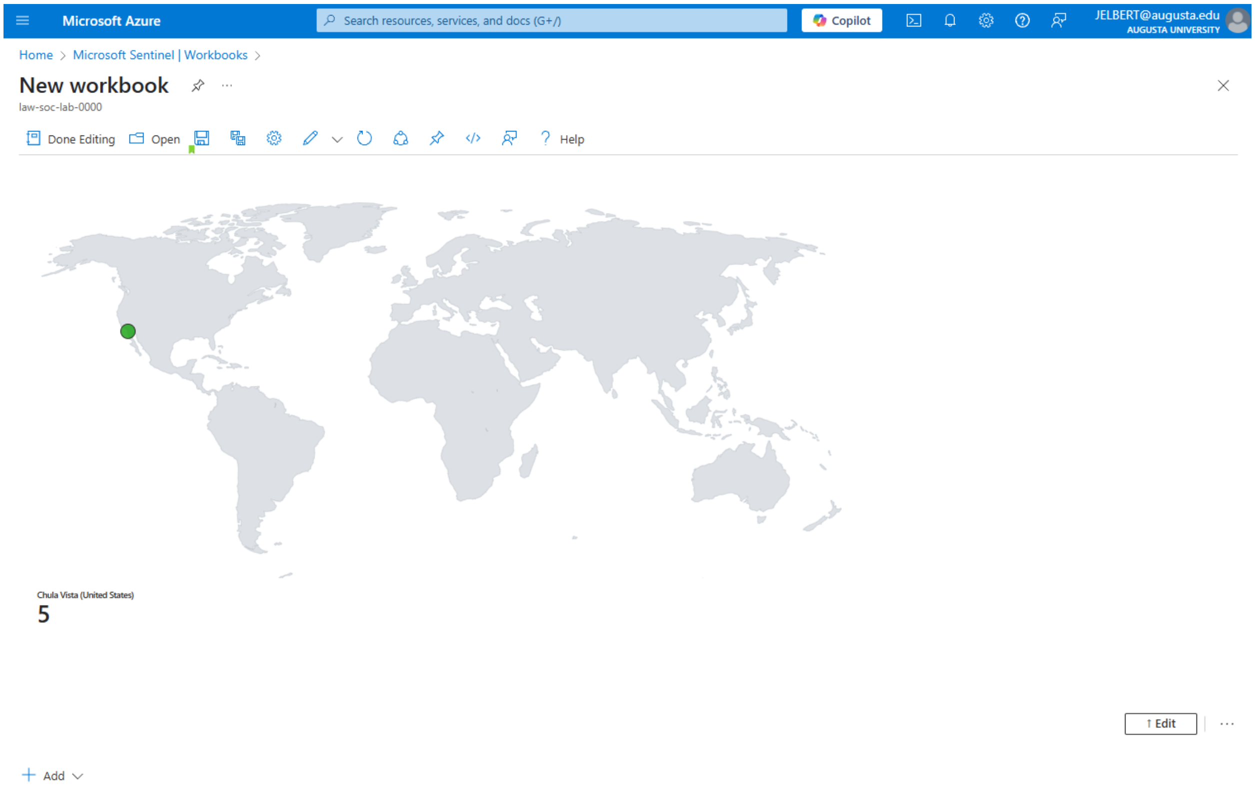
Go to content hub



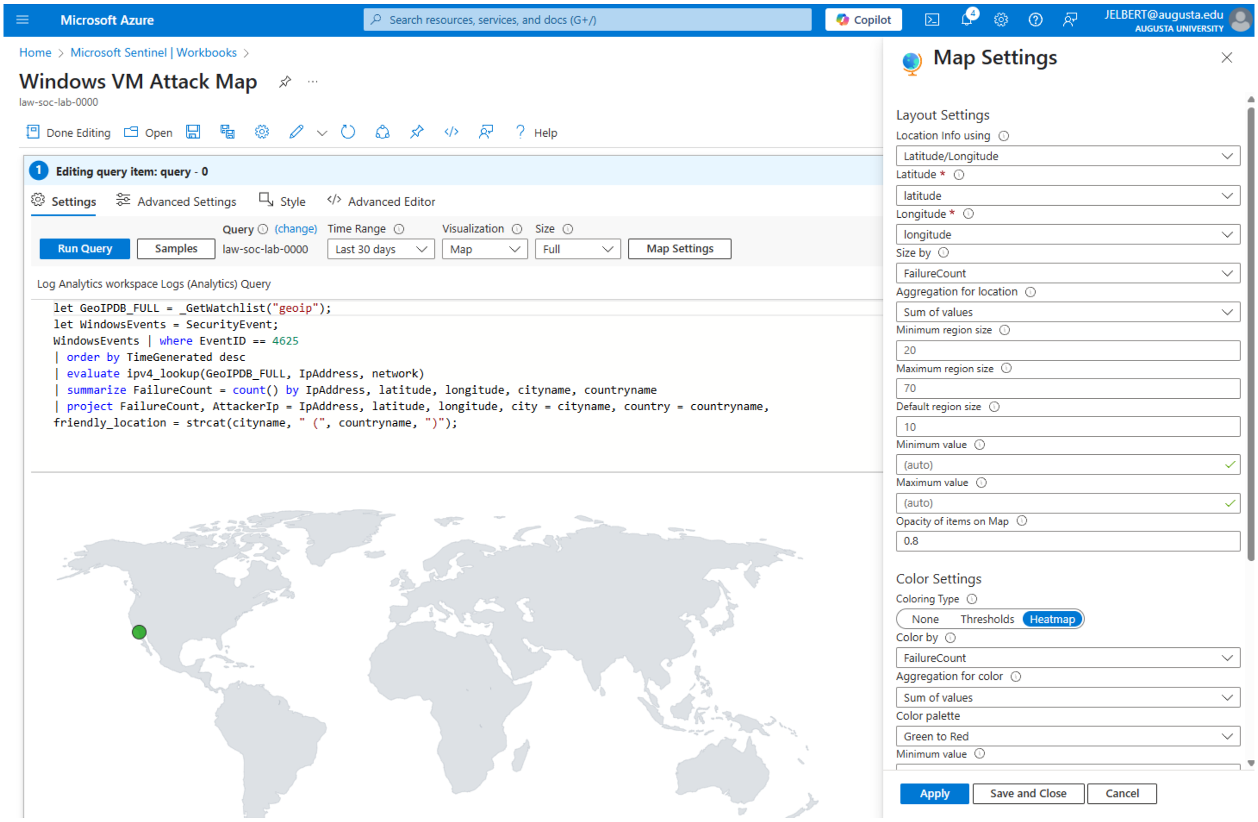
Shown below is a JSON representation of the current item.
Any changes you make here will be reflected when you press 'Done Editing'.

```
{
    "type": 3,
    "content": {
    "version": "KqlItem/1.0",
    "query": "let GeoIPDB_FULL = _GetWatchlist(\"geoip\");\nlet WindowsEvents = SecurityEvent;\nWindowsEvents | where EventID == 4625\n| order by TimeGenerated desc\
    "size": 3,
    "timeContext": {
        "durationMs": 2592000000
    },
    "queryType": 0,
    "resourceType": "microsoft.operationalinsights/workspaces",
    "visualization": "map",
    "mapSettings": {
        "locInfo": "LatLong",
        "locInfoColumn": "countryname",
        "latitude": "latitude",
        "longitude": "longitude",
        "sizeSettings": "FailureCount",
        "sizeAggregation": "Sum",
        "opacity": 0.8,
```

Since I don't have many attackers connecting to my VM honeypot, I only have one attacker that has tried to logon to my system so far. It is displayed on the map below. Once more attackers try to logon or attack my VM honeypot, more circles will start to appear. The circles will be colored based on the severity of the attack. Green will be the lowest, yellow medium is a medium rating, and red will be a critical rating.



I can also edit the map settings even further if I wanted to.



Windows VM Attack Map

law-soc-lab-0000

Editing query item: query - 0

Query (change): law-soc-lab-0000
Time Range: Last 30 days
Visualization: Map
Size: Full

Log Analytics workspace Logs (Analytics) Query

```
let GeoIPDB_FULL = _GetWatchlist("geoip");
let WindowsEvents = SecurityEvent;
WindowsEvents | where EventID == 4625
| order by TimeGenerated desc
| evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network)
| summarize FailureCount = count() by IpAddress, latitude, longitude, cityname, countryname
| project FailureCount, AttackerIp = IpAddress, latitude, longitude, city = cityname, country = countryname,
friendly_location = strcat(cityname, " (", countryname, ")");
```

Map Settings

Layout Settings

Location Info using: Latitude/Longitude
Latitude *: latitude
Longitude *: longitude
Size by: FailureCount
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: 0.8

Color Settings

Coloring Type: None Thresholds [✓ Heatmap]
Color by: FailureCount
Aggregation for color: Sum of values
Color palette: Green to Red
Minimum value

Future Goals

Optional Integration: Microsoft Defender for Cloud:

Although Defender for Cloud was not connected during this lab, Microsoft Sentinel can be integrated with Defender to enable **SIEM + XDR** functionality. This allows for correlation of Defender alerts, asset risk scoring, and cross-platform visibility across cloud workloads and endpoints.

The main future improvement I want to add are automated alerts or setting detection thresholds for alerts. I also want to configure plans for incidents as well.

Key Outcomes and Lessons Learned

- Built Cloud Infrastructure from Scratch: Successfully configured an Azure-based virtual environment using best practices around resource groups, VMs, NSGs, and agent installation.
- Gained Experience with Microsoft Sentinel SIEM: Explored Sentinel's capabilities including data connectors, event ingestion, querying, enrichment, and dashboarding.
- Mastered KQL Basics for Log Analysis: Practiced querying large sets of security event data to filter, project, and sort log entries using SecurityEvent logs and Event ID filters (e.g., 4625 - failed logins).
- Learned Log Enrichment through Watchlists: Imported a GeoIP dataset to enrich logs with geographic information, allowing correlation between attack origin and event type.
- Visualized Security Data in Workbooks: Created a dynamic workbook and customized JSON queries to map attack attempts in a visual format, simulating analyst reporting techniques.

- Learned the Role of SIEM in Modern SOCs: Understood how SIEMs fit into the broader detection and response ecosystem, and the value of future XDR integrations with tools like Microsoft Defender.

Conclusion

This lab gave me hands-on experience with **real-world cloud security operations** by deploying and managing a basic SIEM solution using **Microsoft Sentinel** in **Azure**. I configured an open honeypot to simulate live attack scenarios, practiced querying logs using **Kusto Query Language (KQL)**, enriched raw log data with geolocation context using a **Sentinel watchlist**, and visualized events using **workbooks** and **custom dashboards**.

Through this experience, I gained firsthand understanding of how SIEM tools ingest and correlate data, how security analysts monitor activity, and how incident detection workflows are built in modern cloud environments. I also learned how to transform raw logs into actionable intelligence—a skill that's critical for **SOC analysts**, **cybersecurity engineers**, and **threat hunters**.

This lab has not only improved my technical skills but also prepared me to contribute meaningfully to a **Security Operations Center (SOC)** or a **cloud security team** by demonstrating:

- Basic Cloud infrastructure setup (Azure)
- Security event ingestion and correlation (Sentinel + Log Analytics)
- Basic threat detection through log analysis
- SIEM dashboard creation for visibility and reporting

This project sets a strong foundation for more advanced work in incident response, threat detection, and SIEM/XDR integration in my studies.