

Microsoft Sentinel - Collecting Data

A **data connector** in Microsoft Sentinel is a feature that integrates various data sources into the Sentinel platform, enabling seamless collection and analysis of security data. It acts as a bridge between Microsoft Sentinel and external systems, services, or applications, allowing them to send logs and telemetry data to the underlying Log Analytics workspace for monitoring and investigation.

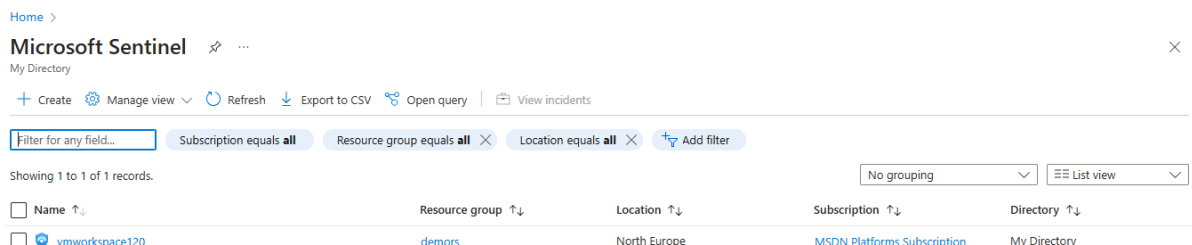
Key Points About Data Connectors:

1. **Sources:** Collect data from Microsoft services (e.g., Azure, Office 365) and third-party systems (e.g., firewalls, endpoint protection tools).
2. **Types:** Includes built-in connectors for popular systems and custom connectors for unique use cases.
3. **Purpose:** Enables centralized monitoring, threat detection, and response by aggregating data from diverse sources.
4. **Configuration:** Typically involves setting up diagnostics, creating data collection rules, and specifying the events to monitor.

The goal of enabling a data connector in Microsoft Sentinel is to centralize and monitor security event data from various sources like Azure VMs. By configuring a connector and creating a Data Collection Rule (DCR), data is collected and sent to the Log Analytics workspace, where it can be queried and analyzed. This allows organizations to gain insights, detect potential threats (e.g., failed login attempts), and proactively respond to security issues. Microsoft Sentinel integrates this data, enabling automated alerts and comprehensive security management to enhance the organization's overall security posture and streamline threat detection and response efforts.

To begin with the lab

1. Access the Microsoft Sentinel service within the Azure portal.



2. Access the Data Connectors section in the left pane and locate and choose the desired connector.

Microsoft Sentinel | Data connectors

Selected workspace: 'vmworkspace120'

Search

Refresh Guides & Feedback

General

- Overview
- Logs
- News & guides
- Search

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)

Device specific AMA connectors have been deprecated. [Learn more >](#)

2 Onboarded Connectors 0 Connected 0 Updates

Search by name or provider Providers: **Microsoft** Data Types: **SecurityEvents**

Status: **Not connected (2)**

Status	Connect...	Content Source	Updates
	Security E...	Solution Windows Security Events	
	Windows ...	Solution Windows Security Events	

3. Here go through all the connectors and select Window Security Event via AMA(Azure Monitoring Agent).

Device specific AMA connectors have been deprecated. [Learn more >](#)

2 Onboarded Connectors 0 Connected 0 Updates

Search by name or provider Providers: **Microsoft** Data Types: **SecurityEvents**

Status: **Not connected (2)**

Status	Connect...	Content Source	Updates
	Security E...	Solution Windows Security Events	
	Windows ...	Solution Windows Security Events	

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

[Open connector page](#)

4. Open the connector page and it will provide you instructions on how to use the connector so read the provided steps to configure the connector.

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

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

i 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.

Refresh ⓘ

Rule name

Created by

Filter name

+ Create data collection rule

- Initiate the process by selecting the option to Create Data Collection Rule and give a name for the rule.

Create Data Collection Rule



Data collection rule management

Basic Resources Collect Review + create

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

Rule details

Rule name *

sentinel-rule

Subscription * ⓘ

MSDN Platforms Subscription

Resource group * ⓘ

Demors

- Then choose the relevant resource, such as your Azure Virtual Machine and Identify the security events you wish to gather, for instance, all events and after that conclude by clicking Review and Create to complete the establishment of the rule.

Subscriptions

Resource Groups

Resource Types

Locations

Selected: All

Selected: All

Selected: All

Selected: All

Search to filter items...

Show Selected

Scope	Resource Type	Location
<div> <div>✓</div> <div> <div>▼</div> <div>🔑</div> <div>MSDN Platforms Subscription</div> </div> </div>		
<div> <div>✓</div> <div> <div>▼</div> <div>🔗</div> <div>demors</div> </div> </div>		
<div> <div>✓</div> <div> <div>🖥️</div> <div>demo-vm</div> </div> </div>	microsoft.compute/virtualmachines	North Europe

Basic

Resources

Collect

Review + create

Basic

Data rule name

sentinel-rule

Subscription

MSDN Platforms Subscription

Resource Group

Demors

Selected resources

Name	Type
demo-vm	microsoft.compute/virtualmachines

Selected events

AllEvents

< Previous

Create

- Now allow time for the data collection process to complete. Subsequently, navigate to the Overview section of Microsoft Sentinel to verify that data is being successfully received.

🛡️

Microsoft Sentinel | Overview (Preview)

...

Selected workspace: 'vmworkspace120'

Search

×

«

🔄 Refresh

▼ General

🛡️ Overview (Preview)

📊 Logs

📰 News & guides

🔍 Search

📋

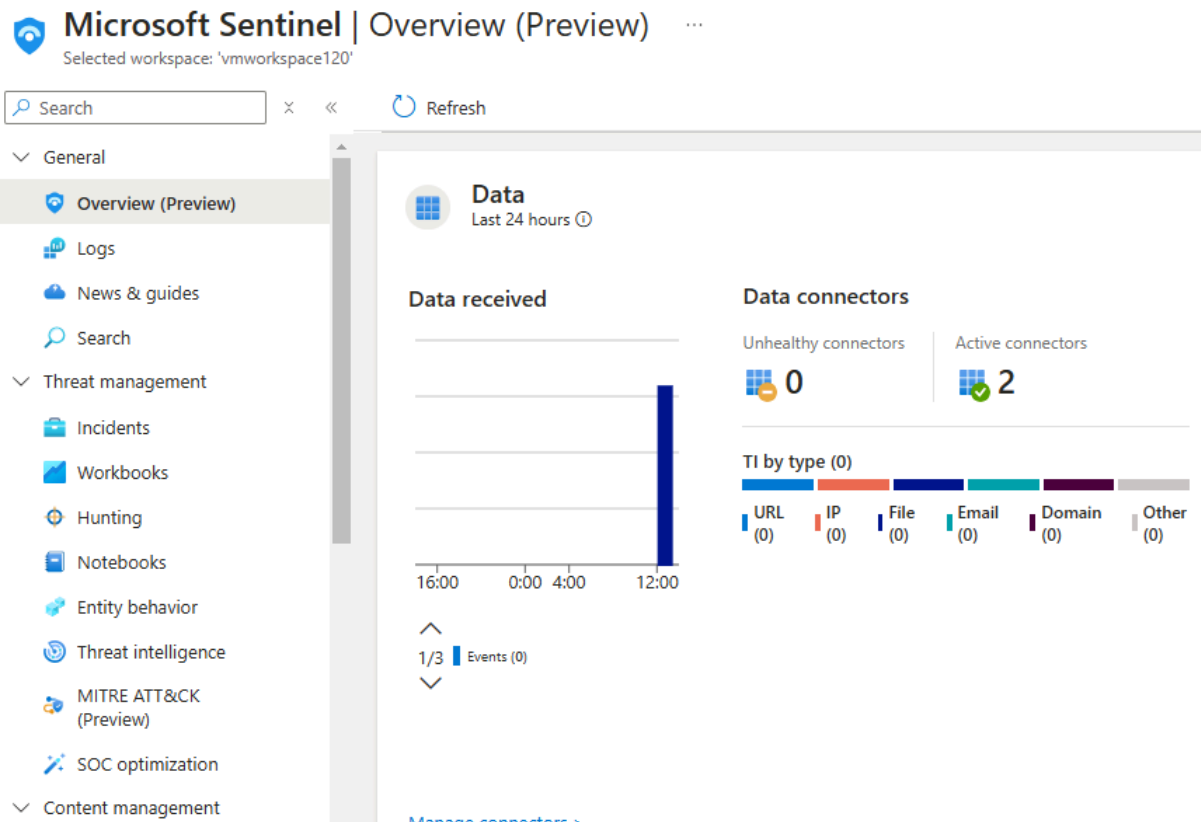
Incidents (0)

Last 24 hours ⓘ

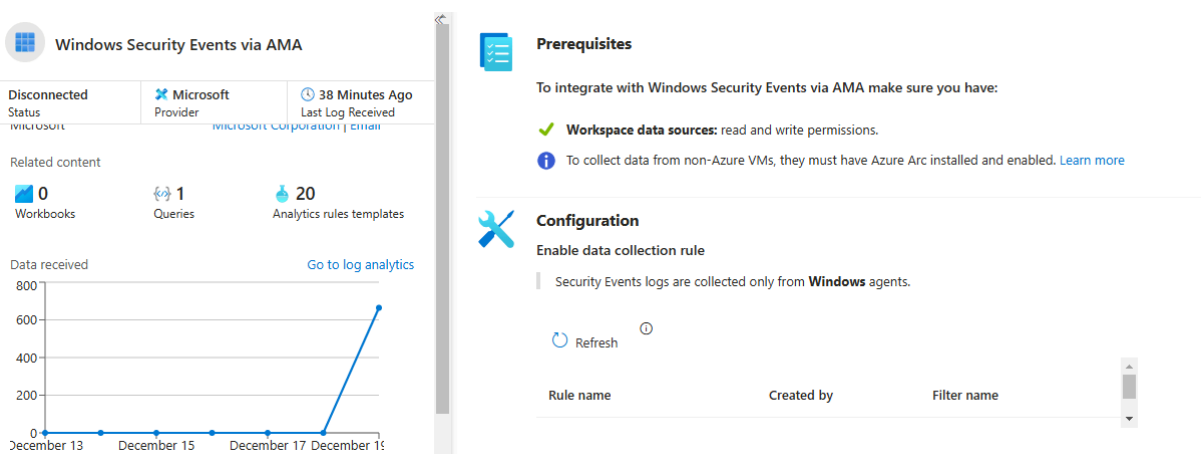
📘

You are currently viewing the new overview experience; you can always switch back to old one

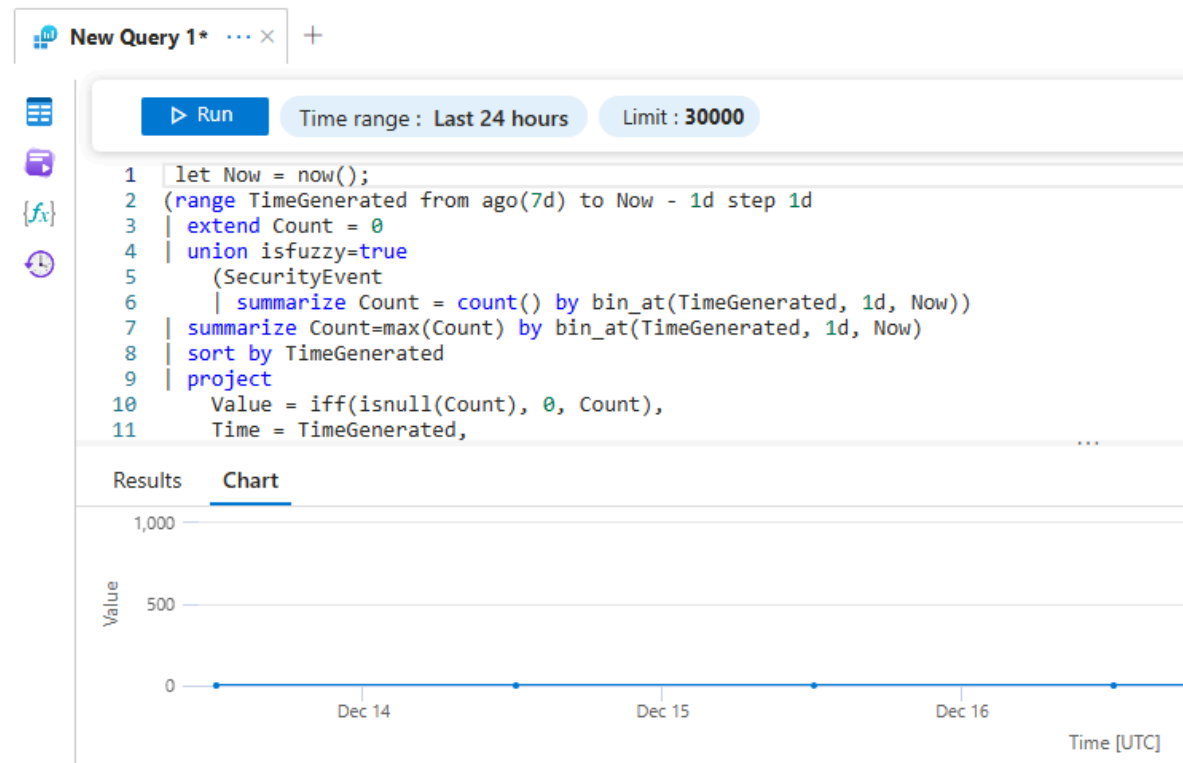
8. Here you will see something named as incidents is being created. If you scroll down you will see some data is being collected.



9. Now go to manage connectors in bottom of the data section. It will take you to the data collector page.
10. Select a data collector here and on left side scroll down and go to the **Log Analytics Workspace** to query data.



11. You will see some by default queries running here which are part of the connector. If you go on the results you will see some values based on time frames.



12. Run a query to view events in the **SecurityEvent** table.

New Query 1* ... × + Save Share ... Que KQL mode

▶ Run Time range : Last 24 hours Limit : 30000

```

1 SecurityEvent
2

```

Results Chart

TimeGenerated [UTC] ↑↓	Account	AccountType	Computer	EventSourceName	Channel
> 12/20/2024, 11:28:18.020 AM	WORKGROUP\demo-vm\$	Machine	demo-vm	Microsoft-Windows-Security-A...	Security
> 12/20/2024, 11:28:18.020 AM	WORKGROUP\demo-vm\$	Machine	demo-vm	Microsoft-Windows-Security-A...	Security
> 12/20/2024, 11:28:18.012 AM	WORKGROUP\demo-vm\$	Machine	demo-vm	Microsoft-Windows-Security-A...	Security
> 12/20/2024, 11:28:18.012 AM	WORKGROUP\demo-vm\$	Machine	demo-vm	Microsoft-Windows-Security-A...	Security
> 12/20/2024, 11:27:18.010 AM	WORKGROUP\demo-vm\$	Machine	demo-vm	Microsoft-Windows-Security-A...	Security
> 12/20/2024, 11:27:18.010 AM	WORKGROUP\demo-vm\$	Machine	demo-vm	Microsoft-Windows-Security-A...	Security

13. Examine the particulars of the event, including the event identification number and associated activities. Investigate particular actions, such as unsuccessful login attempts, to detect possible security concerns.

14. You have effectively activated a data connector, established a data collection rule, and confirmed that data is being gathered and transmitted to Microsoft Sentinel.