Introduction

I worked on a project where I set up **Microsoft Sentinel (Azure SIEM)** and configured log ingestion from devices using **Azure Arc**. The purpose of this project was to get hands-on experience with setting up a SIEM in the cloud, connecting it with hybrid resources, and collecting security logs for monitoring.

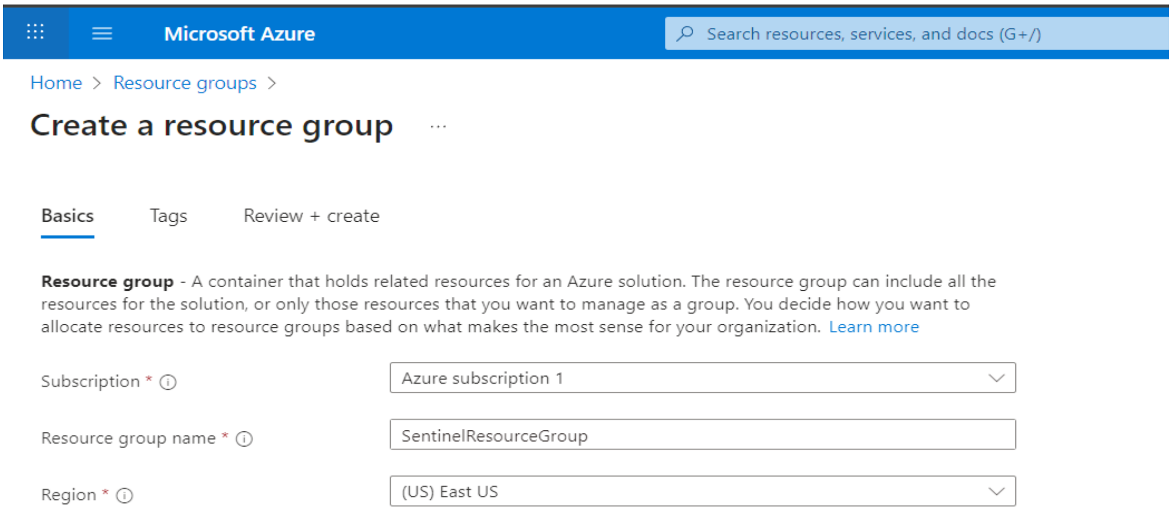
The main reason I took on this project was to understand how modern organizations centralize their logs, detect threats, and manage both cloud and on-premises devices from a single platform. I wanted to practice the entire process—from creating the necessary Azure resources to connecting an external device and finally sending its security logs into Sentinel for analysis.

Steps I Took

1. **Created a Resource Group**
2. **Set Up a Log Analytics Workspace**
3. **Deployed Microsoft Sentinel**
4. **Enabled Windows Security Events Data Connector**
5. **Installed Azure Arc on a Device**
6. **Created a Data Collection Rule (DCR)**

Step 1: Azure Account & Resource Group Setup

- Created a new **Azure account** and selected the **free subscription**.
- Azure requires a **credit card check** for free subscription eligibility.
    - If the card was used before, the free subscription is not available.
- After signing in, I created a **Resource Group** (Sentinel will be deployed inside it).
- Made sure to use the **same region** for all resources and services, since the log timestamps in Sentinel follow the region selected.



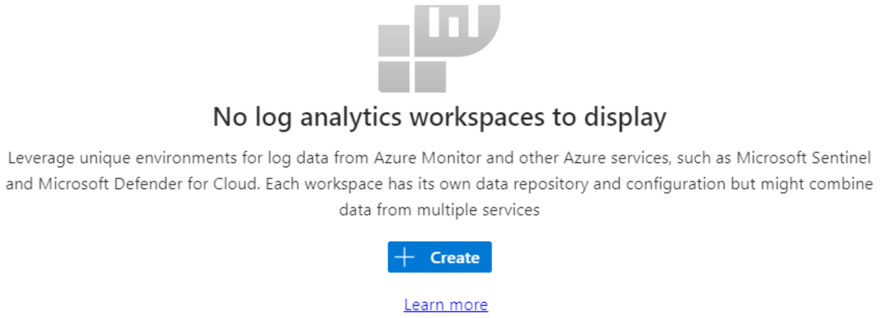
Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most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

Subscription * : Azure subscription 1

Resource group name * : SentinelResourceGroup

Region * : (US) East US

- A **Log Analytics Workspace** is like a storage + analysis space for all logs.
- Sentinel **cannot work without it** because Sentinel itself doesn't store logs — it only analyzes what's collected in the workspace.
- So the workspace is basically the **backbone for Sentinel's data**.

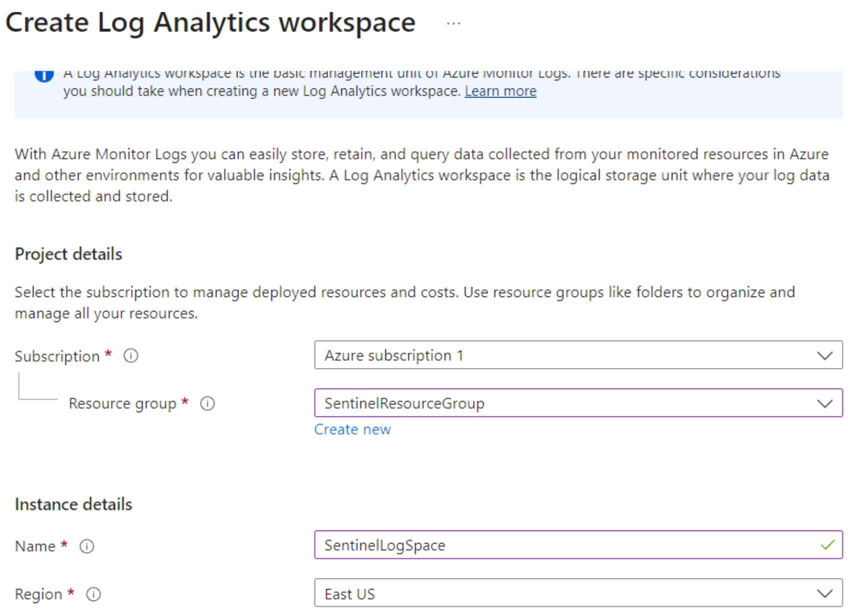


No log analytics workspaces to display

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

Step 2: Create Log Analytics Workspace

- Created a **Log Analytics Workspace** (named *SentinelLogSpace*).
- This workspace is needed because it stores all logs that Sentinel will analyze.
- Chose the **same region** as the Resource Group for consistency and proper log timestamps.



Create Log Analytics workspace ...

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

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

Subscription * : Azure subscription 1

Resource group * : SentinelResourceGroup

Create new

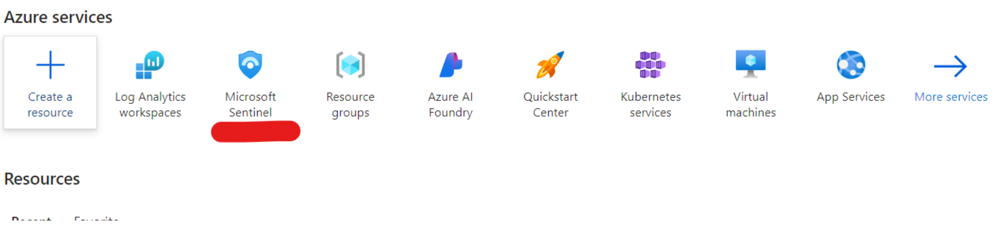
Instance details

Name * : SentinelLogSpace

Region * : East US

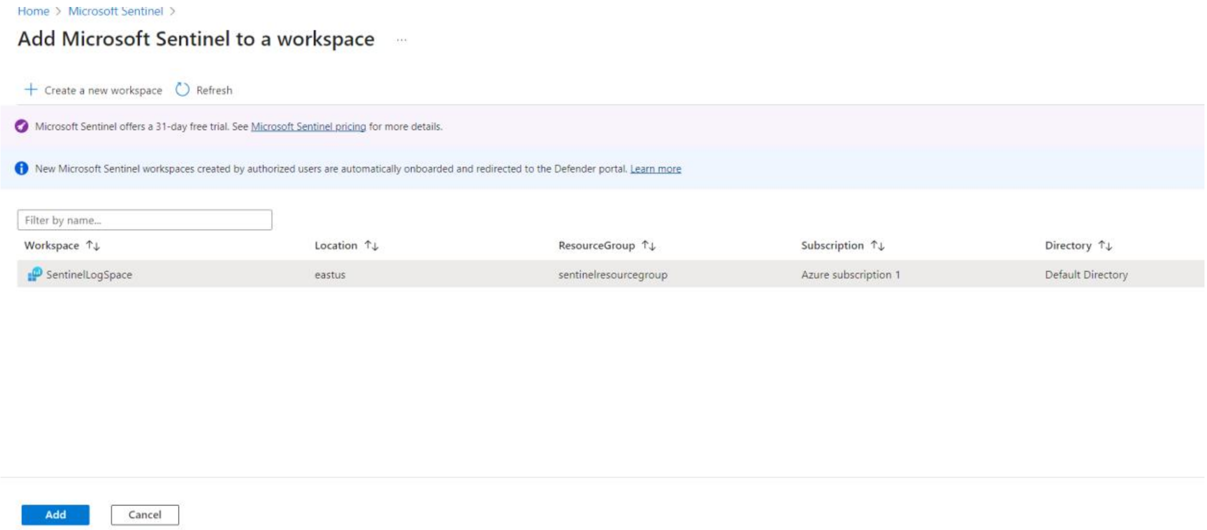
Step 3: Set Up Microsoft Sentinel

- Went back to **Azure Services** and selected **Microsoft Sentinel**.
- Added a new Sentinel instance.



• Attached the **Log Analytics Workspace** (created earlier) to Sentinel.

• Optionally, Sentinel also allows creating a **new workspace** directly from its setup page, but I used the one I had already created.



Add Microsoft Sentinel to a workspace

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

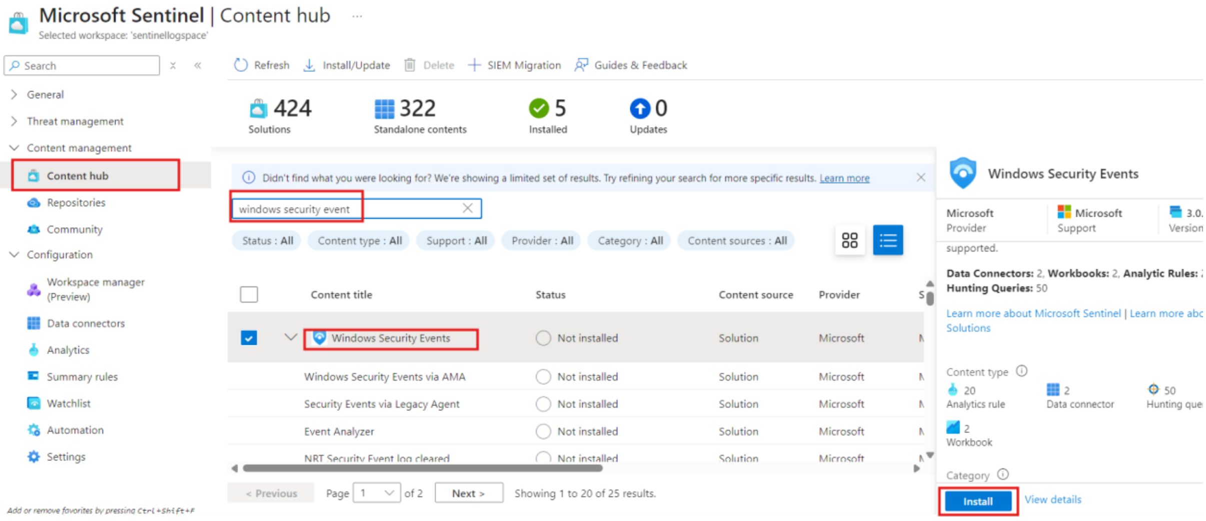
New Microsoft Sentinel workspaces created by authorized users are automatically onboarded and redirected to the Defender portal. Learn more

Filter by name...

Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
SentinelLogSpace	eastus	sentinelresourcegroup	Azure subscription 1	Default Directory

Step 4: Install Windows Security Events Data Collector

- **Data Collectors** in Sentinel are used to **pull logs and events from different sources** into the Log Analytics Workspace.
- These collectors provide the data that Sentinel analyzes, because **Sentinel itself doesn't generate logs**.
- I installed the **Windows Security Events connector** on the host machine. These logs record important security activities like logins, failed logins, and privilege changes.
- Using **Azure Arc**, the Windows Security Events are **brought from the host machine into Azure**.
- The **Data Collector then feeds these logs into Sentinel**, allowing it to monitor and detect suspicious activities from that machine.



Microsoft Sentinel | Content hub

Selected workspace: 'sentinellogspace'

424 Solutions | 322 Standalone contents | 5 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

windows security event

☐	Content title	Status	Content source	Provider
☑	Windows Security Events	○ Not installed	Solution	Microsoft
	Windows Security Events via AMA	○ Not installed	Solution	Microsoft
	Security Events via Legacy Agent	○ Not installed	Solution	Microsoft
	Event Analyzer	○ Not installed	Solution	Microsoft
	NRT Security Event log cleared	○ Not installed	Solution	Microsoft

Page 1 of 2 Showing 1 to 20 of 25 results.

Windows Security Events

Microsoft Provider | Microsoft Support | 3.0. Version

supported.

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

Learn more about Microsoft Sentinel | Learn more abc Solutions

Content type

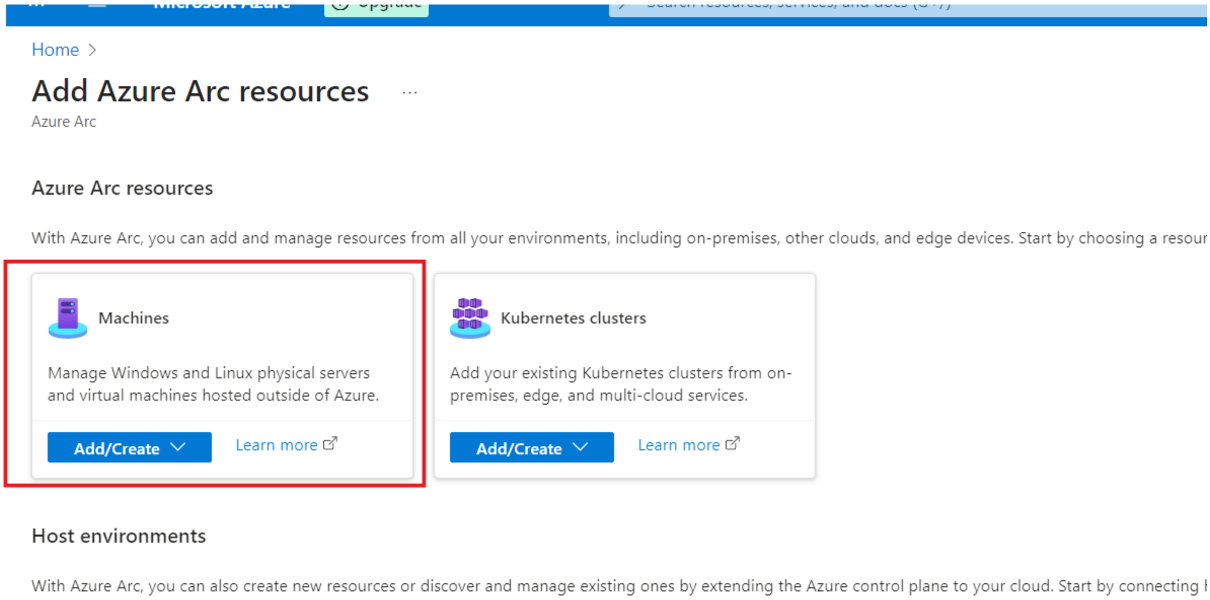
20 Analytics rule | 2 Data connector | 50 Hunting que

2 Workbook

Category

Step 5: Install Azure Arc on the Device

- Before setting up the data collector, I needed **Azure Arc** to bring data from my machine into Azure.
- After installing **Windows Security Events**, I started the **Azure Arc service**.
- Created the Azure Arc resource in the **same Resource Group** and **same region** as other resources.
- Selected **Machine/Server** as the resource type (suitable for my scenario).



Home >

Add Azure Arc resources

Azure Arc

Azure Arc resources

With Azure Arc, you can add and manage resources from all your environments, including on-premises, other clouds, and edge devices. Start by choosing a resour

Machines

Manage Windows and Linux physical servers and virtual machines hosted outside of Azure.

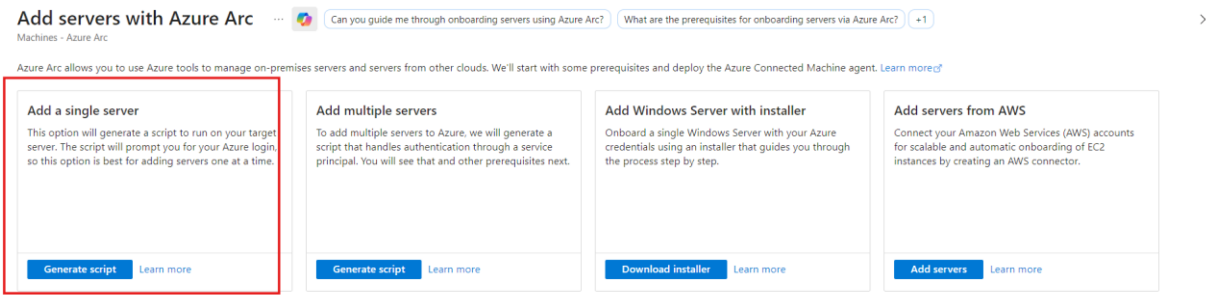
Kubernetes clusters

Add your existing Kubernetes clusters from on-premises, edge, and multi-cloud services.

Host environments

With Azure Arc, you can also create new resources or discover and manage existing ones by extending the Azure control plane to your cloud. Start by connecting I

- Chose **Single Server so** I clicked on **generate script** for single server.



Add servers with Azure Arc

Machines - Azure Arc

Can you guide me through onboarding servers using Azure Arc?

What are the prerequisites for onboarding servers via Azure Arc?

Azure Arc allows you to use Azure tools to manage on-premises servers and servers from other clouds. We'll start with some prerequisites and deploy the Azure Connected Machine agent. Learn more

Add a single server

This option will generate a script to run on your target server. The script will prompt you for your Azure login, so this option is best for adding servers one at a time.

Add multiple servers

To add multiple servers to Azure, we will generate a script that handles authentication through a service principal. You will see that and other prerequisites next.

Add Windows Server with installer

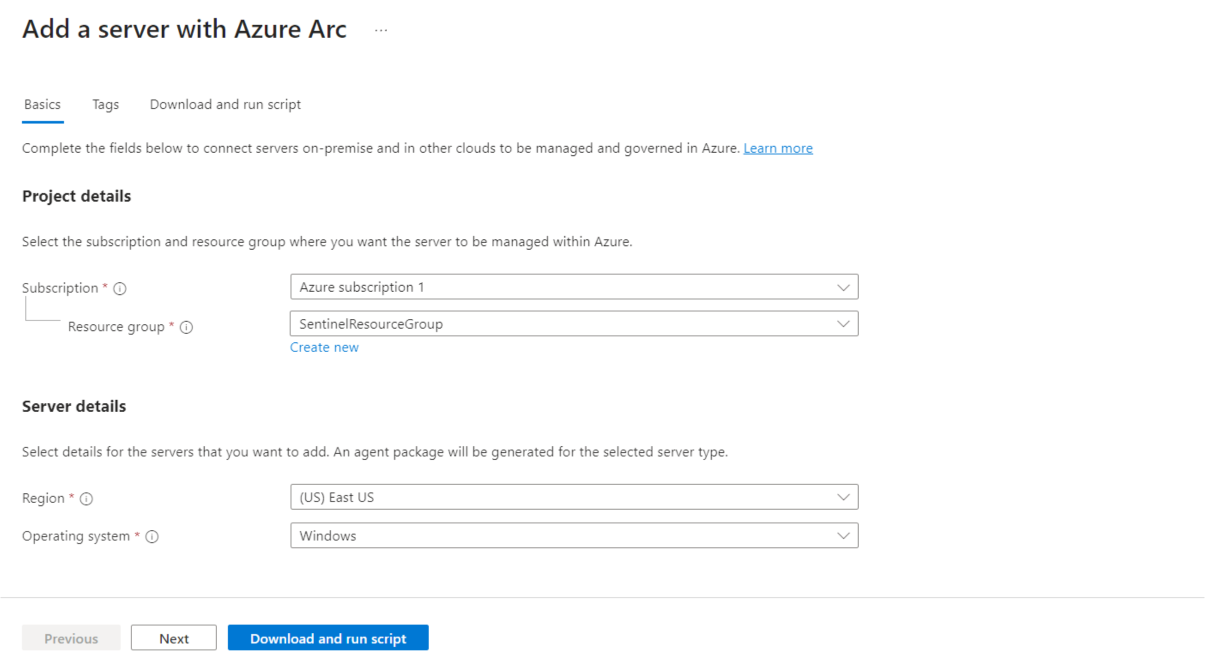
Onboard a single Windows Server with your Azure credentials using an installer that guides you through the process step by step.

Add servers from AWS

Connect your Amazon Web Services (AWS) accounts for scalable and automatic onboarding of EC2 instances by creating an AWS connector.

When I clicked **Generate Script**, I was prompted to **Add a server to Azure Arc**.

- Placed it in the **same Resource Group** and **same region**.
- Selected the correct **operating system**.
- Clicked **Download** and ran the script.



Add a server with Azure Arc ...

Basics | Tags | Download and run script

Complete the fields below to connect servers on-premise and in other clouds to be managed and governed in Azure. Learn more

Project details

Select the subscription and resource group where you want the server to be managed within Azure.

Subscription * ⓘ: Azure subscription 1

Resource group * ⓘ: SentinelResourceGroup

Create new

Server details

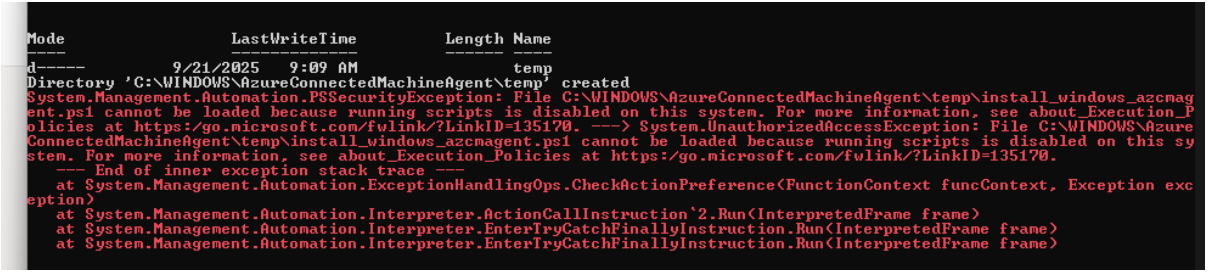
Select details for the servers that you want to add. An agent package will be generated for the selected server type.

Region * ⓘ: (US) East US

Operating system * ⓘ: Windows

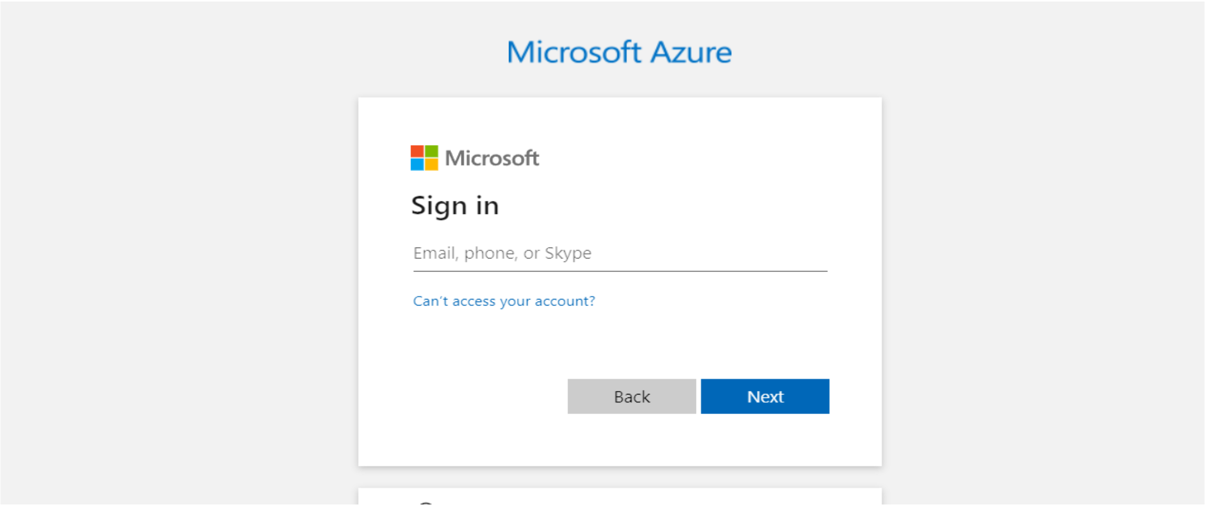
- Copied the script provided by **Azure Arc** and ran it in **PowerShell as administrator**.
- Ran into an **Execution Policy error**, because PowerShell restricts script execution by default.
- Fixed it by running the following command in the same PowerShell window:

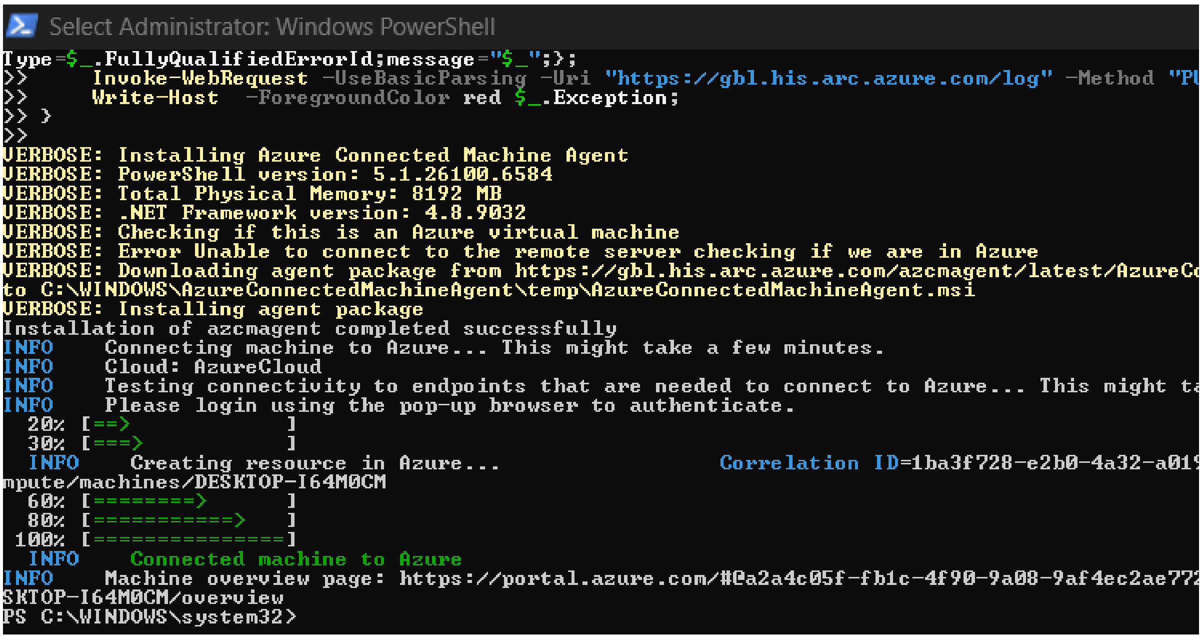
```
Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
```



```
Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        9/21/2025   9:09 AM                temp
Directory 'C:\WINDOWS\AzureConnectedMachineAgent\temp' created
System.Management.Automation.PSSecurityException: File C:\WINDOWS\AzureConnectedMachineAgent\temp\install_windows_azcmag
ent.ps1 cannot be loaded because running scripts is disabled on this system. For more information, see about_Execution_P
olicies at https:/go.microsoft.com/fwlink/?LinkID=135170. ---> System.UnauthorizedAccessException: File C:\WINDOWS\Azure
ConnectedMachineAgent\temp\install_windows_azcmagent.ps1 cannot be loaded because running scripts is disabled on this sy
stem. For more information, see about_Execution_Policies at https:/go.microsoft.com/fwlink/?LinkID=135170.
   --- End of inner exception stack trace ---
   at System.Management.Automation.ExceptionHandlingOps.CheckActionPreference(FunctionContext funcContext, Exception exc
eption)
   at System.Management.Automation.Interpreter.ActionCallInstruction`2.Run(InterpretedFrame frame)
   at System.Management.Automation.Interpreter.EnterTryCatchFinallyInstruction.Run(InterpretedFrame frame)
   at System.Management.Automation.Interpreter.EnterTryCatchFinallyInstruction.Run(InterpretedFrame frame)
```

- After this, I ran the script again, entered my **Microsoft credentials** when prompted, and the script completed successfully.

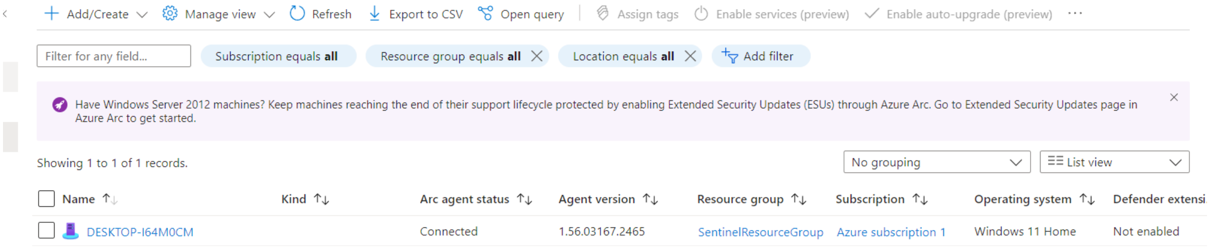




Select Administrator: Windows PowerShell

```
Type=$_.FullyQualifiedErrorId;message="$_";};
>>      Invoke-WebRequest -UseBasicParsing -Uri "https://gbl.his.arc.azure.com/log" -Method "PU
>>      Write-Host  -ForegroundColor red $_.Exception;
>> }
>>
VERBOSE: Installing Azure Connected Machine Agent
VERBOSE: PowerShell version: 5.1.26100.6584
VERBOSE: Total Physical Memory: 8192 MB
VERBOSE: .NET Framework version: 4.8.9032
VERBOSE: Checking if this is an Azure virtual machine
VERBOSE: Error Unable to connect to the remote server checking if we are in Azure
VERBOSE: Downloading agent package from https://gbl.his.arc.azure.com/azcmagent/latest/AzureC
to C:\WINDOWS\AzureConnectedMachineAgent\temp\AzureConnectedMachineAgent.msi
VERBOSE: Installing agent package
Installation of azcmagent completed successfully
INFO    Connecting machine to Azure... This might take a few minutes.
INFO    Cloud: AzureCloud
INFO    Testing connectivity to endpoints that are needed to connect to Azure... This might ta
INFO    Please login using the pop-up browser to authenticate.
  20% [==>            ]
  30% [===>           ]
  INFO    Creating resource in Azure...                   Correlation ID=1ba3f728-e2b0-4a32-a01
mpute/machines/DESKTOP-I64M0CM
  60% [========>      ]
  80% [===========>   ]
 100% [===============]
  INFO    Connected machine to Azure
INFO    Machine overview page: https://portal.azure.com/#@a2a4c05f-fb1c-4f90-9a08-9af4ec2ae77
SKTOP-I64M0CM/overview
PS C:\WINDOWS\system32>
```

- Checked **Azure Arc → Machines**, and my machine was listed, confirming it was **connected to Azure Arc**.



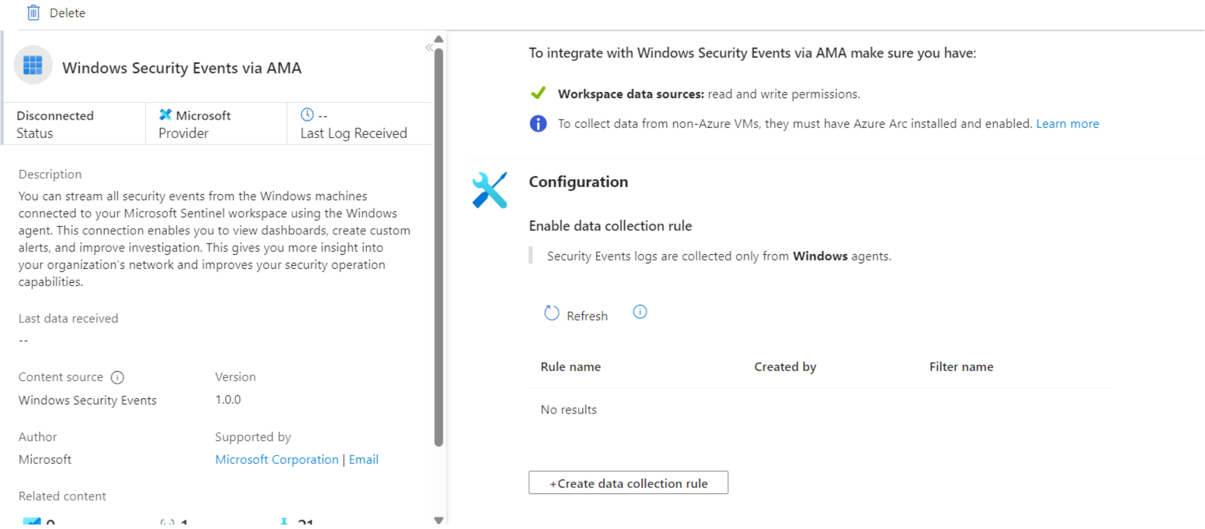
Have Windows Server 2012 machines? Keep machines reaching the end of their support lifecycle protected by enabling Extended Security Updates (ESUs) through Azure Arc. Go to Extended Security Updates page in Azure Arc to get started.

Showing 1 to 1 of 1 records.

Name	Kind	Arc agent status	Agent version	Resource group	Subscription	Operating system	Defender extensi
DESKTOP-I64M0CM		Connected	1.56.03167.2465	SentinelResourceGroup	Azure subscription 1	Windows 11 Home	Not enabled

Step 6: Create a Data Collection Rule (DCR) in Windows Security Events

- Opened the **Windows Security Events (WSE) connector** in Sentinel.
- Noticed that **no Data Collection Rules (DCRs) existed** by default.
- Created a **new rule** to start collecting logs from my Arc-connected machine.



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

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

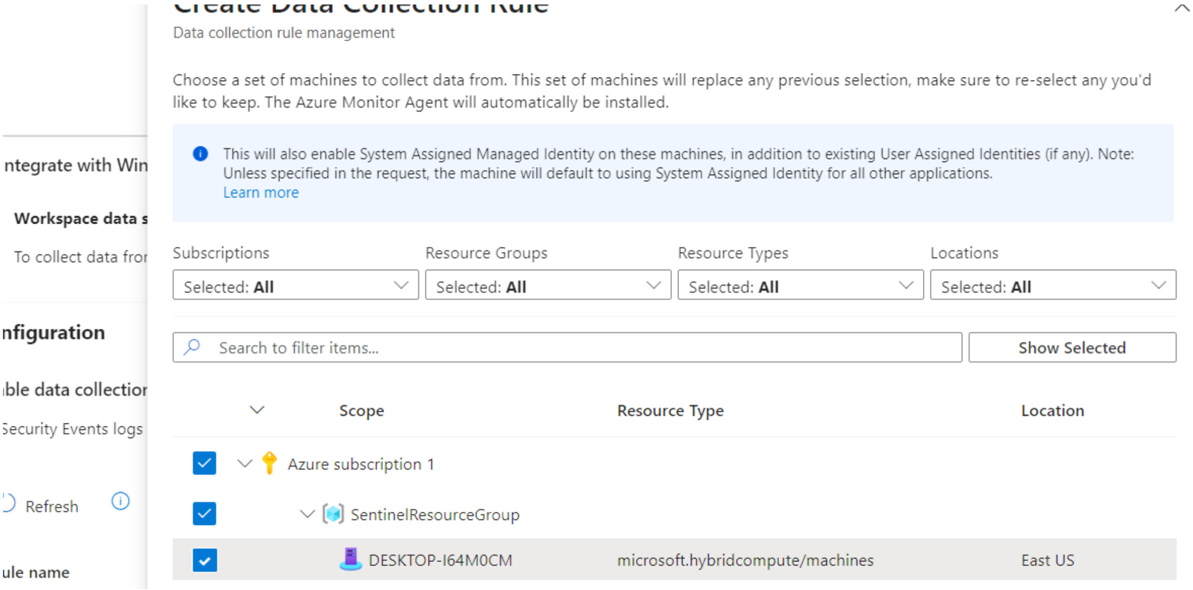
Security Events logs are collected only from **Windows** agents.

Rule name	Created by	Filter name
No results		

- **Why**: Without a DCR, Sentinel would not know **which events to collect or from which machines**, so creating this rule ensures that relevant Windows security events are ingested into the Log Analytics Workspace for monitoring and analysis.

Step 7: Configure Data Collection Rule (DCR) in Sentinel

- **Step 1: Select Device**
  - I have only **one Arc-connected machine**, so I selected it as the source for log collection.



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: Selected: **All**

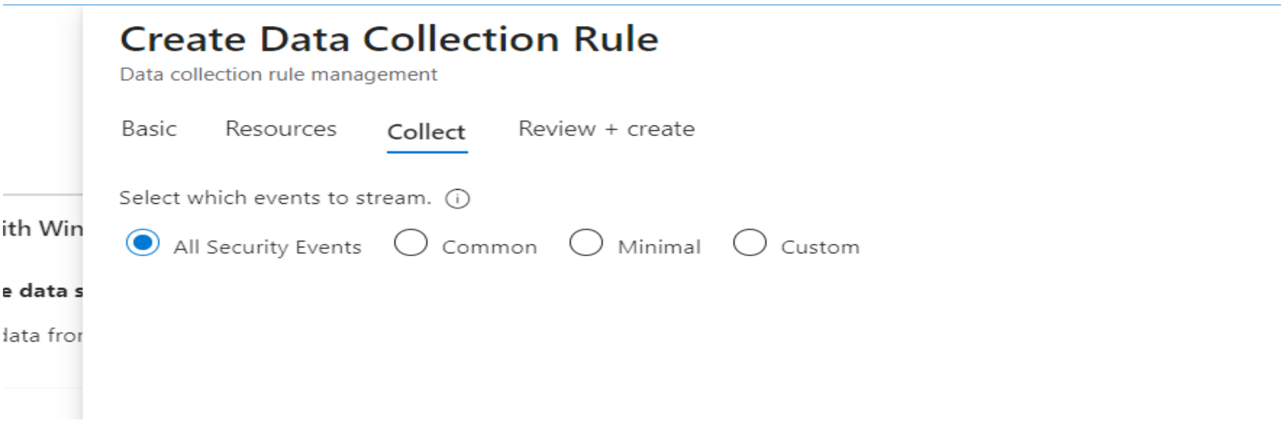
Resource Groups: Selected: **All**

Resource Types: Selected: **All**

Locations: Selected: **All**

	Scope	Resource Type	Location
☑	Azure subscription 1		
☑	SentinelResourceGroup		
☑	DESKTOP-I64M0CM	microsoft.hybridcompute/machines	East US

- **Step 2: Select Data Type**
  - Chose **All Security Events** to collect every security-related log from the device.
  - **Examples of events collected**: logins, failed logins, account lockouts, privilege changes, process creation, and policy changes.
- **Other Options for Data Collection**:
  - **Common**: Collects frequently used security logs (e.g., login attempts, account changes, and system events).
  - **Minimal**: Collects only essential security logs needed for basic monitoring.
  - **Custom**: Lets you select **specific event types or IDs** to fine-tune what logs Sentinel receives.



Create Data Collection Rule

Data collection rule management

Select which events to stream.

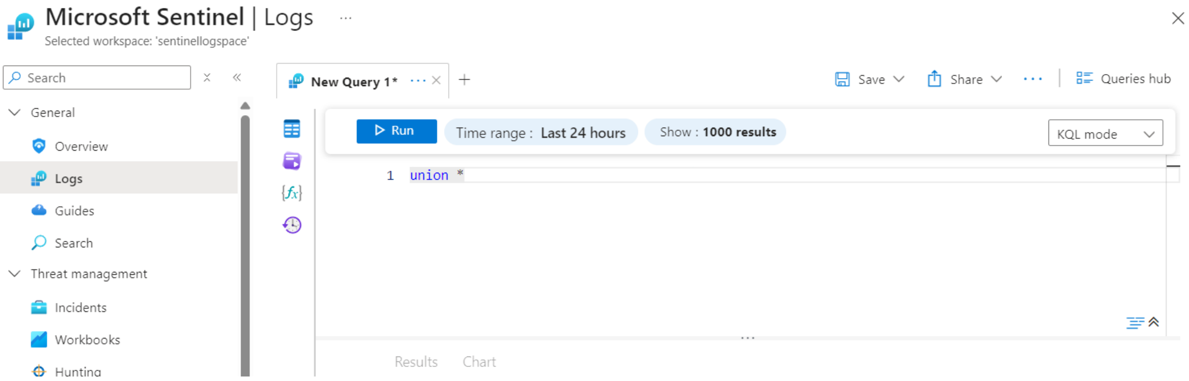
● All Security Events ○ Common ○ Minimal ○ Custom

Step 8: Validate Log Ingestion in Sentinel

- Opened **Microsoft Sentinel** and went to the **Logs** section.
- Ran the query:

```
union *
```

- This query **retrieves all logs** from the connected sources in the Log Analytics Workspace.



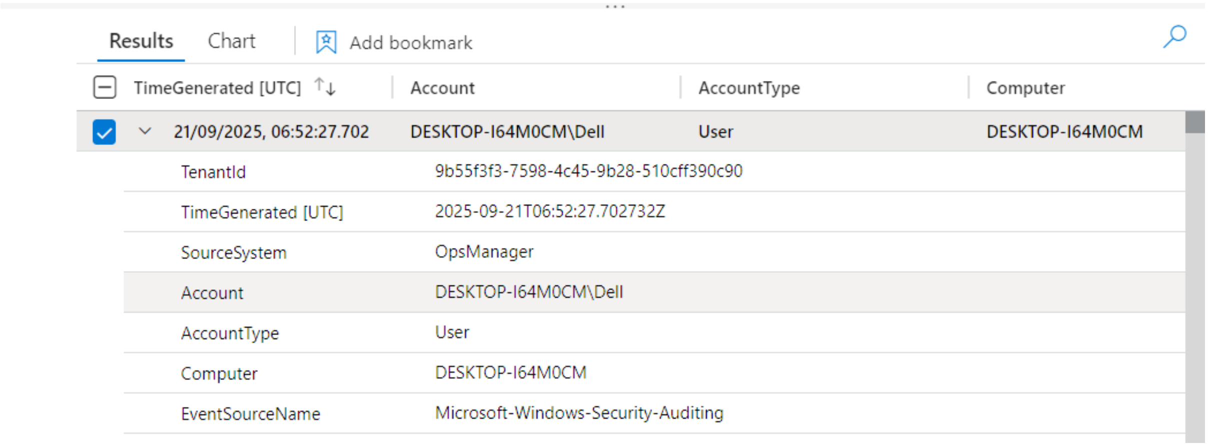
Time range : Last 24 hours

Show : 1000 results

KQL mode

```
union *
```

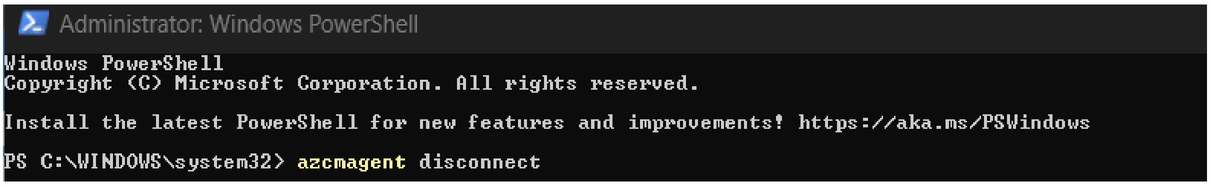
- Verified that logs from my **Arc-connected machine** and **Windows Security Events** were successfully ingested into Sentinel.



TimeGenerated [UTC]	Account	AccountType	Computer
21/09/2025, 06:52:27.702	DESKTOP-I64M0CM\Dell	User	DESKTOP-I64M0CM

TenantId	9b55f3f3-7598-4c45-9b28-510cff390c90
TimeGenerated [UTC]	2025-09-21T06:52:27.702732Z
SourceSystem	OpsManager
Account	DESKTOP-I64M0CM\Dell
AccountType	User
Computer	DESKTOP-I64M0CM
EventSourceName	Microsoft-Windows-Security-Auditing

- After completing the project, I disconnected my Arc-connected machine from Azure using PowerShell.
- Ran the command:
- `azagent disconnect`
- This removed the machine from **Azure Arc**, stopping log ingestion to Sentinel.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> azcmagent disconnect
```

What I Learned

- Gained **hands-on experience with Microsoft Sentinel** and learned how to set up a SIEM in Azure.
- Learned the importance of a **Log Analytics Workspace** as the central repository for all collected logs.
- Understood how **Azure Arc** connects on-premises or hybrid devices to Azure for monitoring and management.
- Learned to install and configure the **Windows Security Events connector** to collect critical security logs.
- Gained experience creating **Data Collection Rules (DCRs)** and choosing which security events to collect (All, Common, Minimal, or Custom).
- Learned how to **validate log ingestion** in Sentinel using KQL queries (`union *`) to see all logs.
- Learned how to **troubleshoot PowerShell Execution Policy errors** when running scripts.
- Gained practical knowledge of **disconnecting Arc-connected machines** and controlling log flow from devices.
- Developed a clearer understanding of **how SIEMs centralize, monitor, and analyze security events**, which is essential for real-world cybersecurity operations.