Microsoft Sentinel | Quick Guide

Version 25.01

Ahmed Abdelwahed
ahmed@abdelwahed.me
www.abdelwahed.me
LinkedIn
GitHub

Microsoft Sentinel

Microsoft Sentinel is a scalable, cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution. It helps organizations detect, prevent, and respond to threats across their environment using built-in AI, automation, and integrations with Microsoft and third-party services.

Key Features of Microsoft Sentinel

1. Data Collection

- **Connectors**:
  - Provides prebuilt connectors for Microsoft services like Defender for Cloud, Defender for Endpoint, Defender for Identity, and Microsoft 365.
  - Supports third-party data sources like firewalls, routers, and other security tools (e.g., Palo Alto, Cisco, AWS).
- **Custom Data Collection**:
  - Collect logs and events from custom applications using APIs or Azure Monitor.

2. Threat Detection

- **Log Analytics**:
  - Uses Azure Log Analytics to store and query collected data.
- **Built-in Analytics Rules**:
  - Includes predefined detection rules for common attack patterns.
- **Custom Detection Rules**:
  - Allows security teams to define and configure custom KQL (Kusto Query Language)-based rules for specific threats.

3. Threat Investigation

- **Investigation Graphs**:
  - Visualizes relationships between threats, devices, users, and data sources for faster root cause analysis.
- **Entity Behavior Analytics (UEBA)**:
  - Detects anomalies in user or entity behavior that might indicate insider threats or compromised accounts.

4. Automation and Orchestration

- **Playbooks**:
  - Automate responses to incidents using Logic Apps (e.g., block IPs, isolate devices, notify teams).
- **Incident Management**:
  - Automatically groups related alerts into incidents to streamline investigation and resolution.

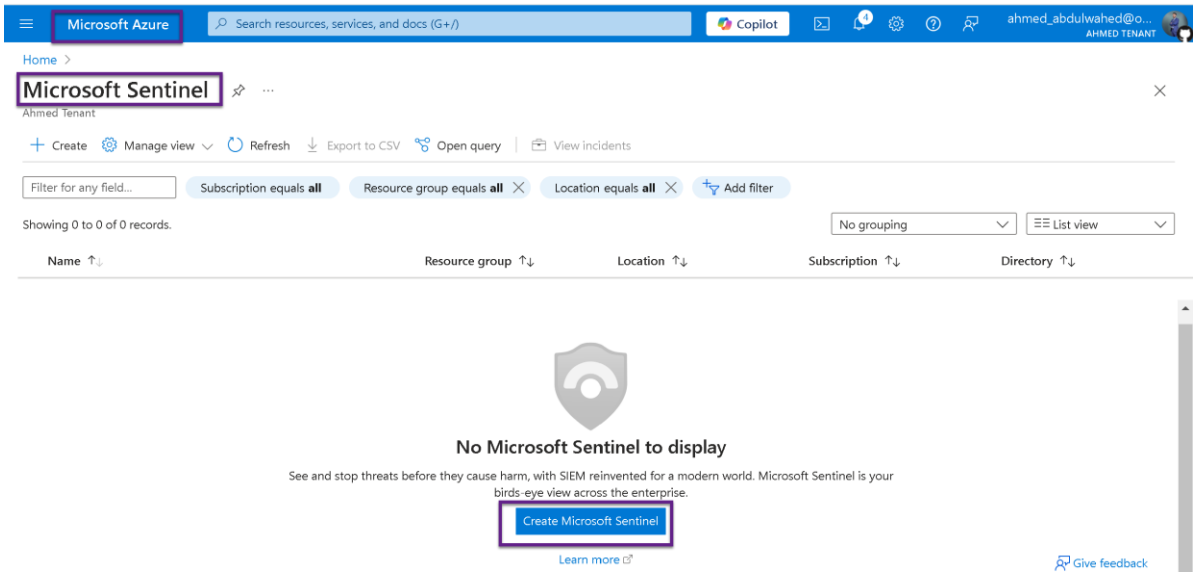
5. Visualization and Reporting

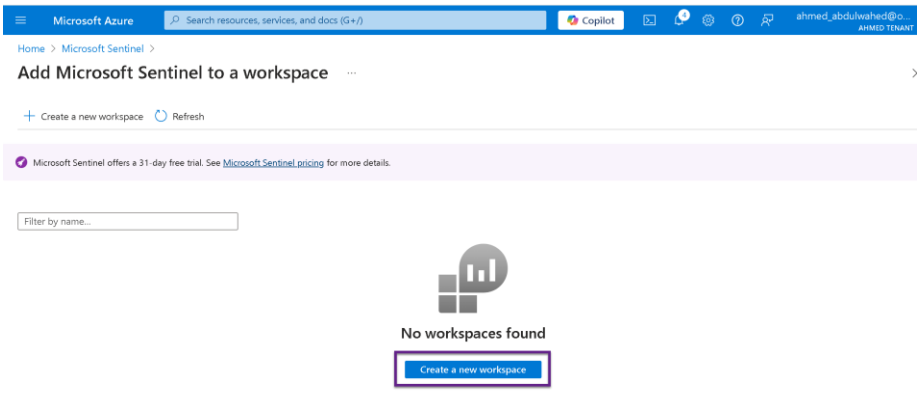
- **Workbooks**:
  - Provides prebuilt and customizable dashboards for real-time monitoring and reporting.
- **Customizable Dashboards**:
  - Visualize trends, incidents, and activity across your environment.

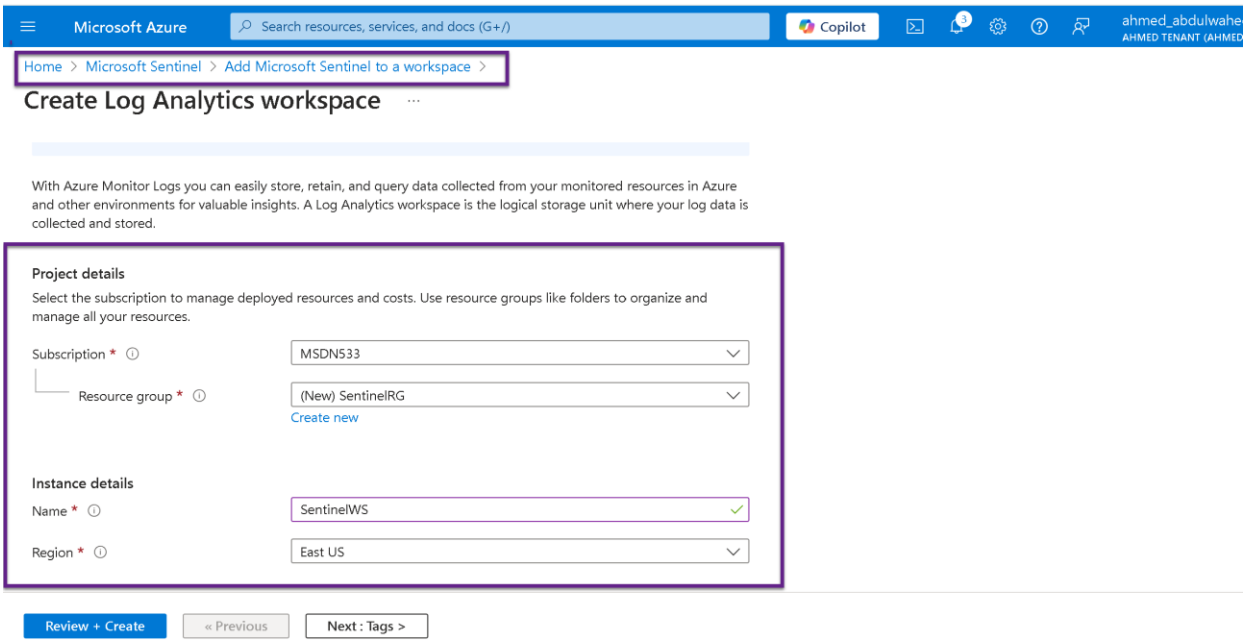
6. Integration

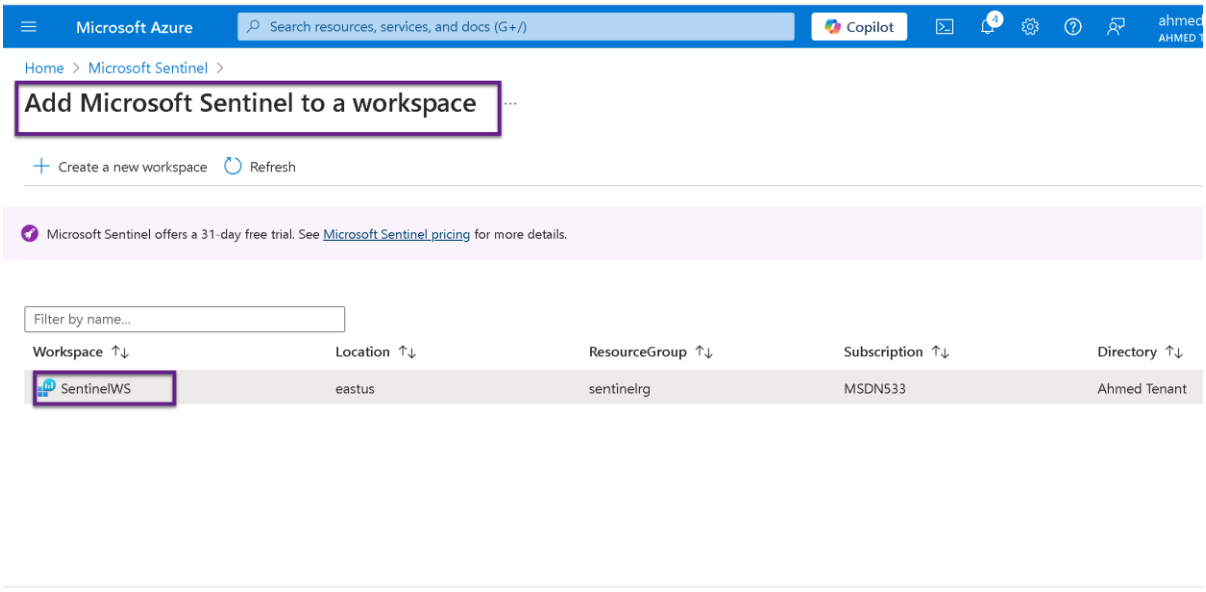
- Integrates with Microsoft Defender services, Azure services, and third-party security solutions.
- Supports APIs for extending functionality and integrating with existing tools.

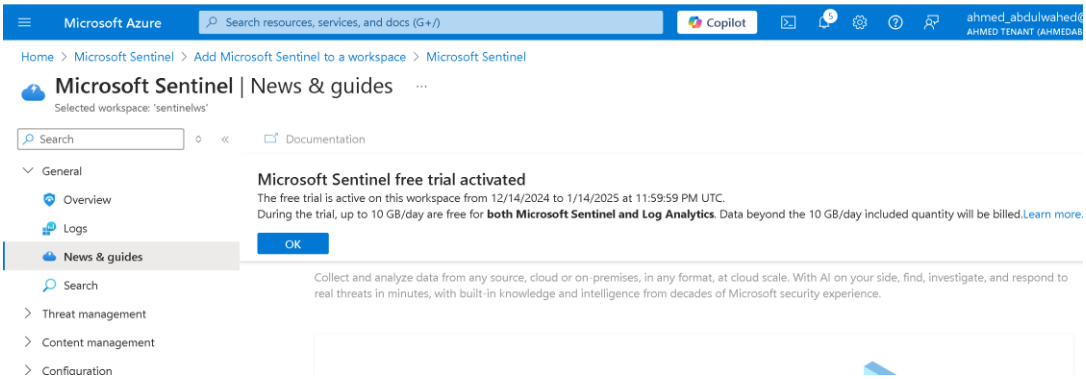
Create Microsoft sentinel





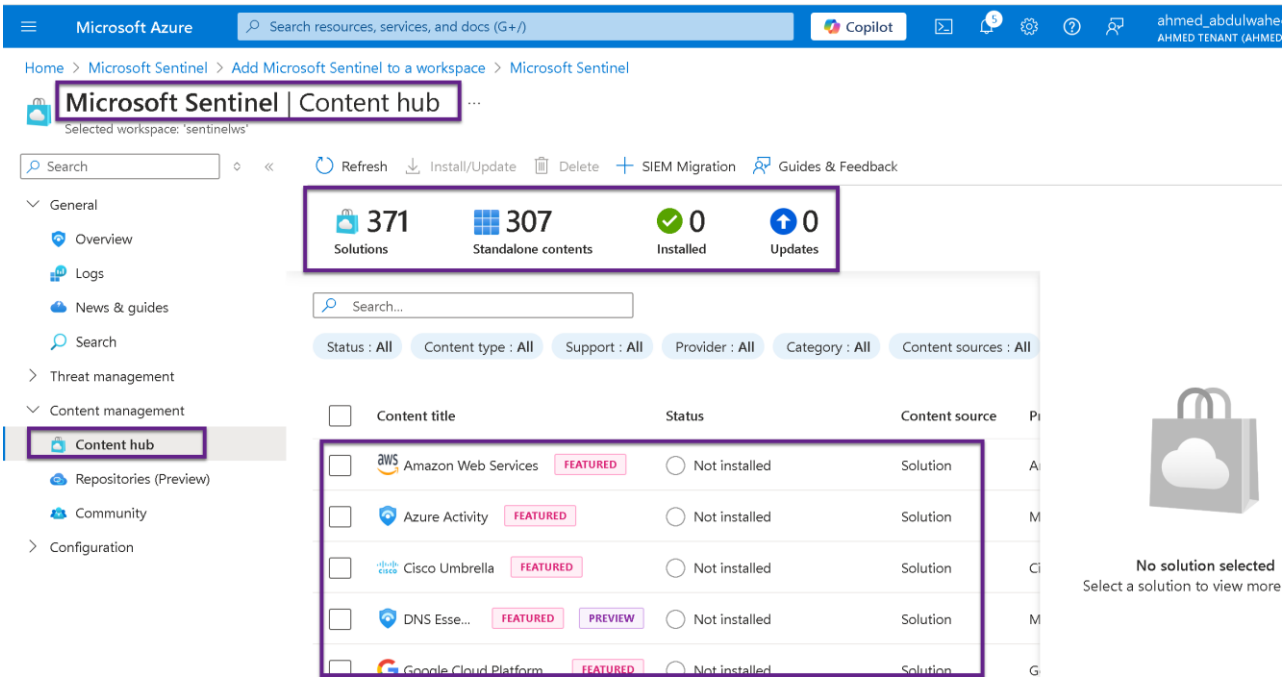



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel >
Add Microsoft Sentinel to a workspace
Create a new workspace
Refresh
Microsoft Sentinel offers a 31-day free trial. See Microsoft Sentinel pricing for more details.
Filter by name...
Workspace
Location
ResourceGroup
Subscription
Directory
SentinelWS
eastus
sentinelrg
MSDN533
Ahmed Tenant
Add
Cancel


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel
Microsoft Sentinel | News & guides
Selected workspace: 'sentinelws'
Search
Documentation
General
Overview
Logs
News & guides
Search
Threat management
Content management
Configuration
Microsoft Sentinel free trial activated
The free trial is active on this workspace from 12/14/2024 to 1/14/2025 at 11:59:59 PM UTC.
During the trial, up to 10 GB/day are free for both Microsoft Sentinel and Log Analytics. Data beyond the 10 GB/day included quantity will be billed.Learn more.
OK
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.

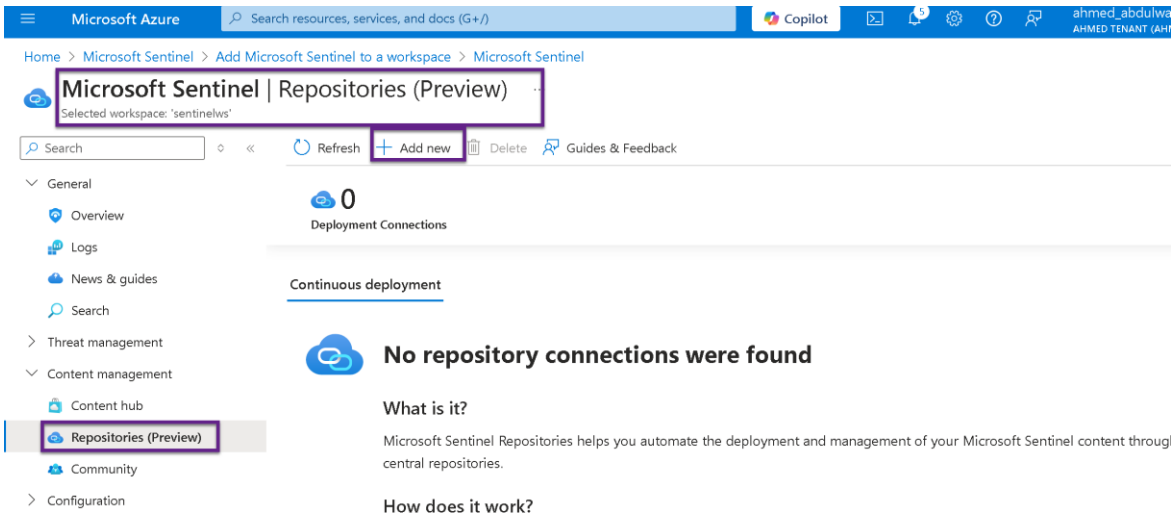
Microsoft Sentinel | Content Hub

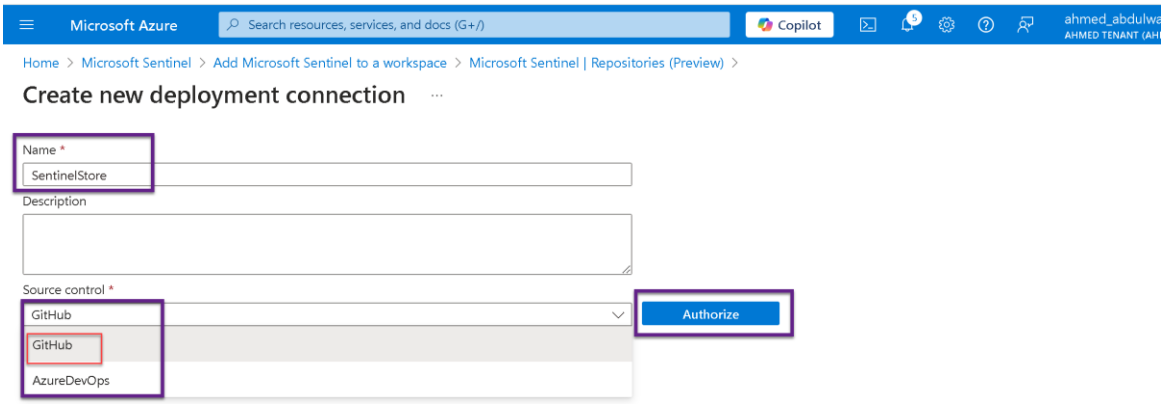
The **Content Hub** in **Microsoft Sentinel** is a central repository of ready-made solutions, analytics, and integrations designed to enhance your organization's threat detection, investigation, and response capabilities. It provides prebuilt content like analytics rules, hunting queries, playbooks, and dashboards, all tailored to specific scenarios, services, or threat types.



Microsoft Sentinel | Repositories

Repositories in **Microsoft Sentinel** allow organizations to manage, store, and share custom content, such as analytics rules, playbooks, hunting queries, and more, using version control and collaboration features powered by **GitHub** or **Azure DevOps Repos**. This integration enables security teams to standardize and scale their Sentinel content across environments.





Source Control:

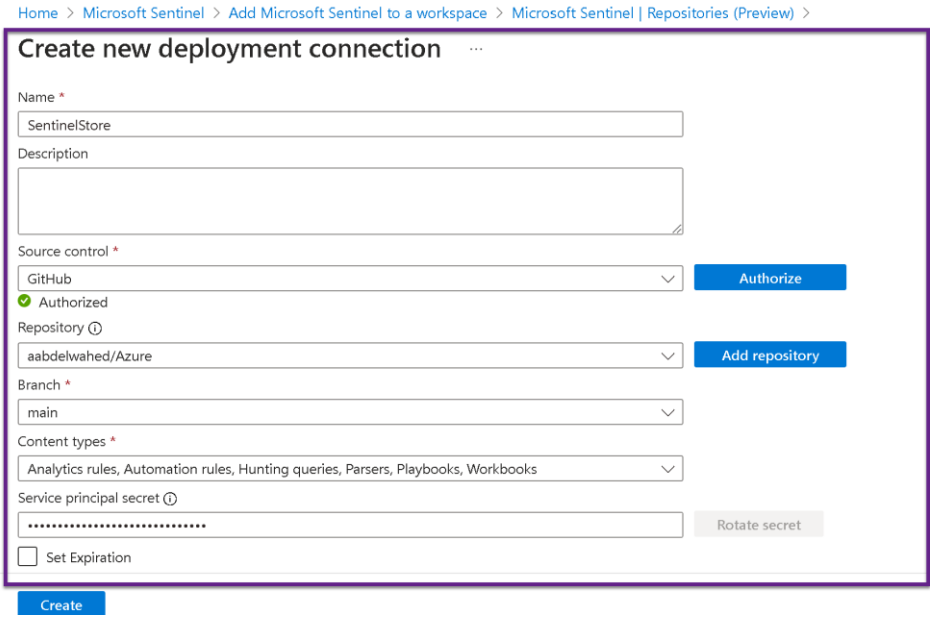
Choose the source control platform. In this example, GitHub is selected.

Ensure the platform is authorized, as indicated by the green checkmark.

Repository:

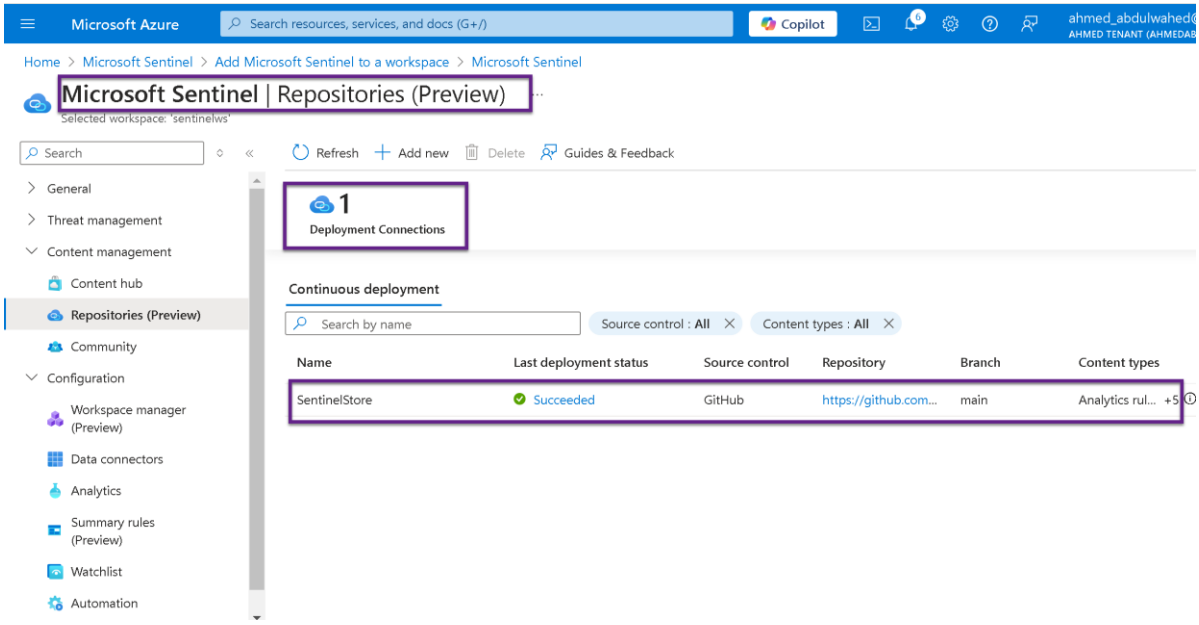
Specify the repository name, e.g., aabdelwahed/Azure.

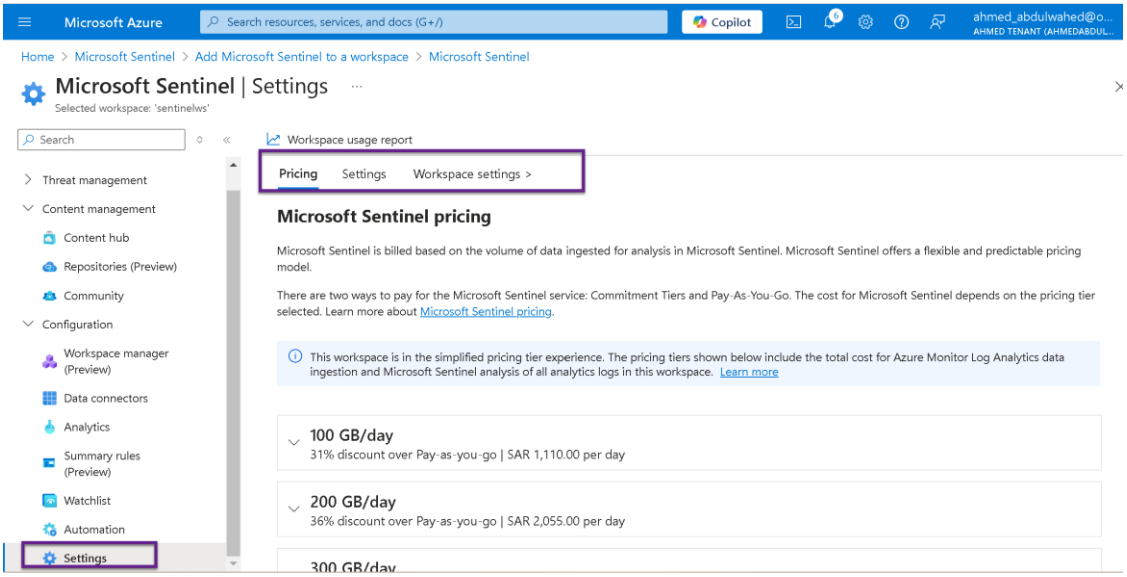
This is where your Sentinel content (e.g., rules, playbooks) is stored.



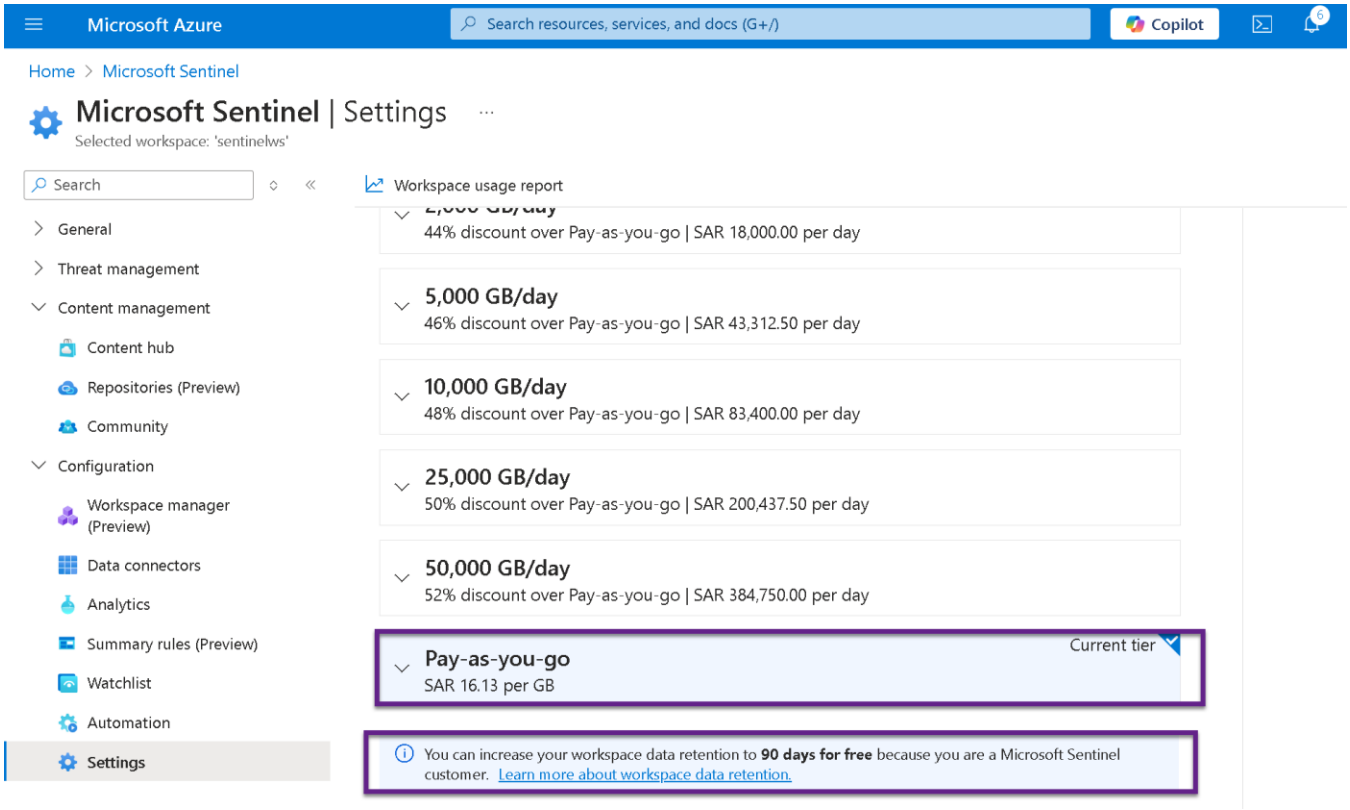
Branch:

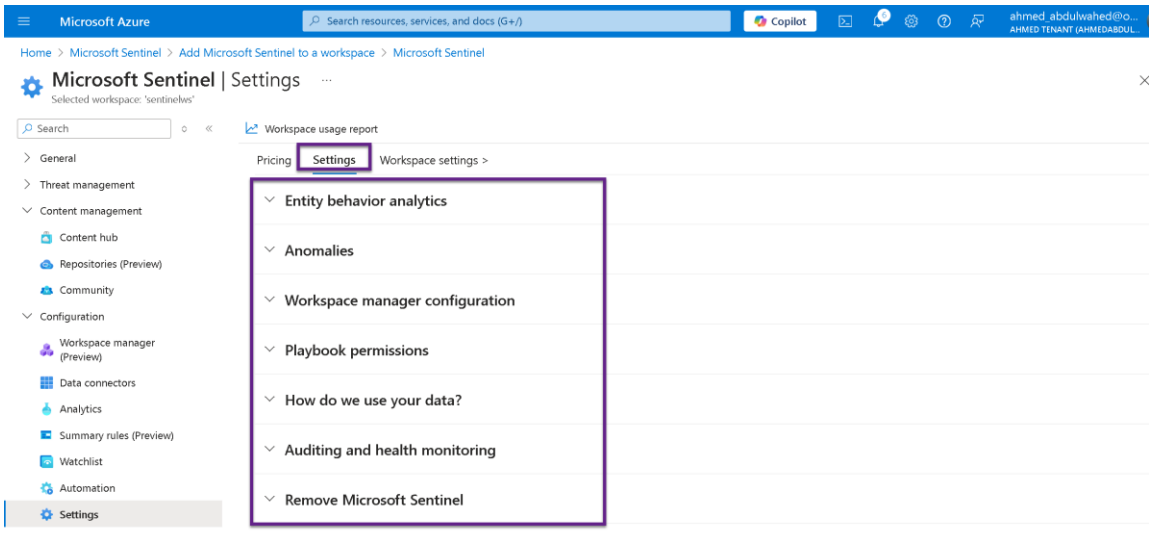
Select the branch where the content resides (e.g., main).

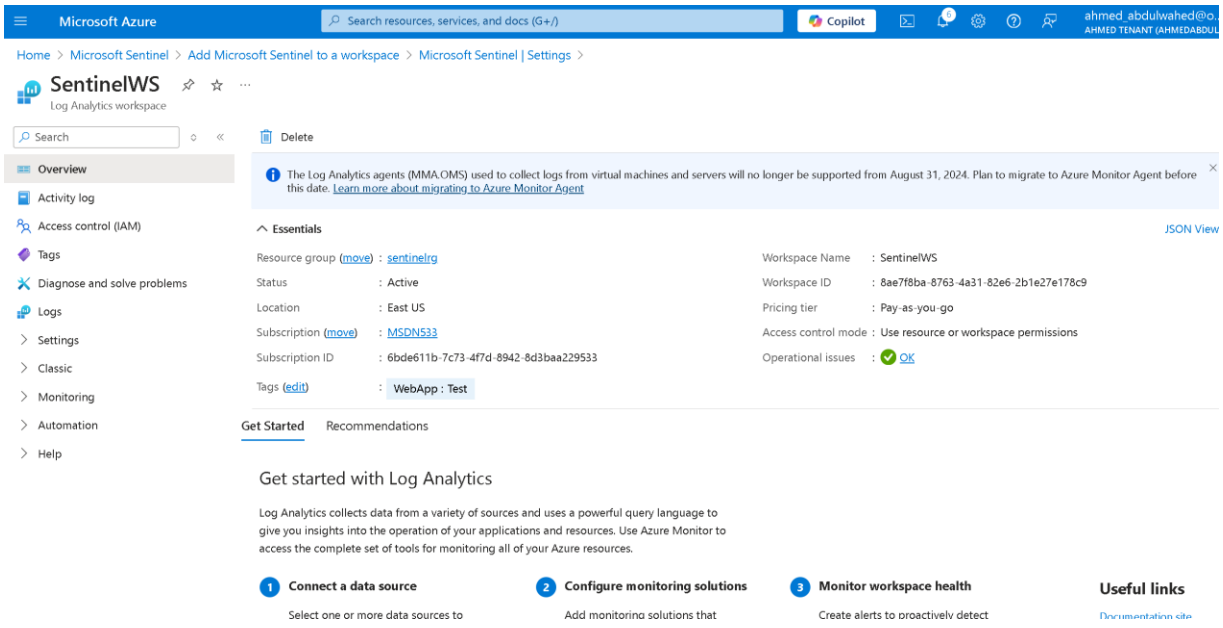




By default, Microsoft Sentinel retains data in the connected Log Analytics workspace for 30 days. However, you can extend the retention period up to 90 days at no additional cost. Here's how this works:



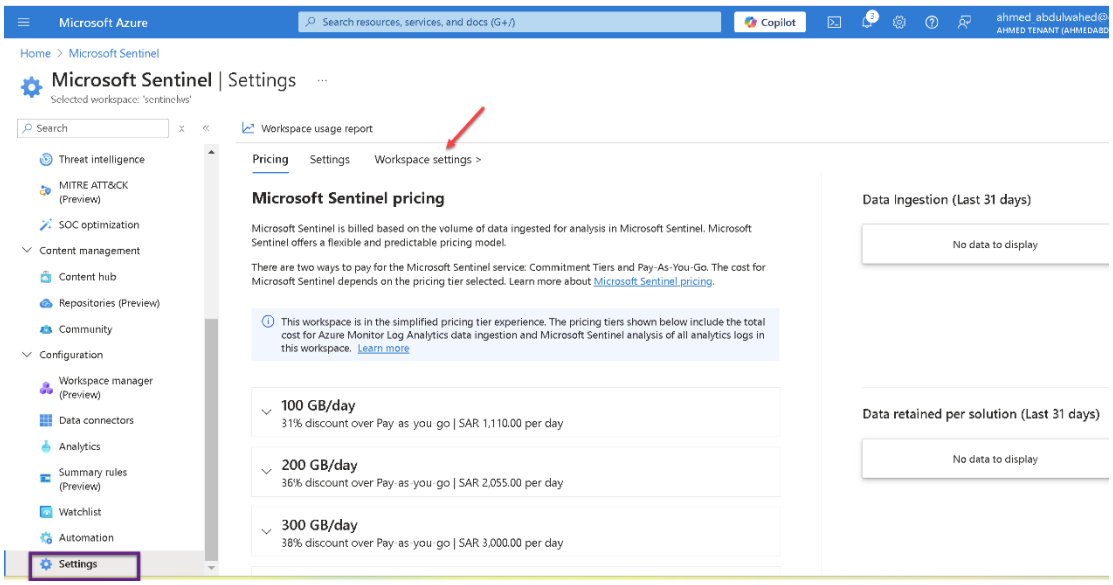


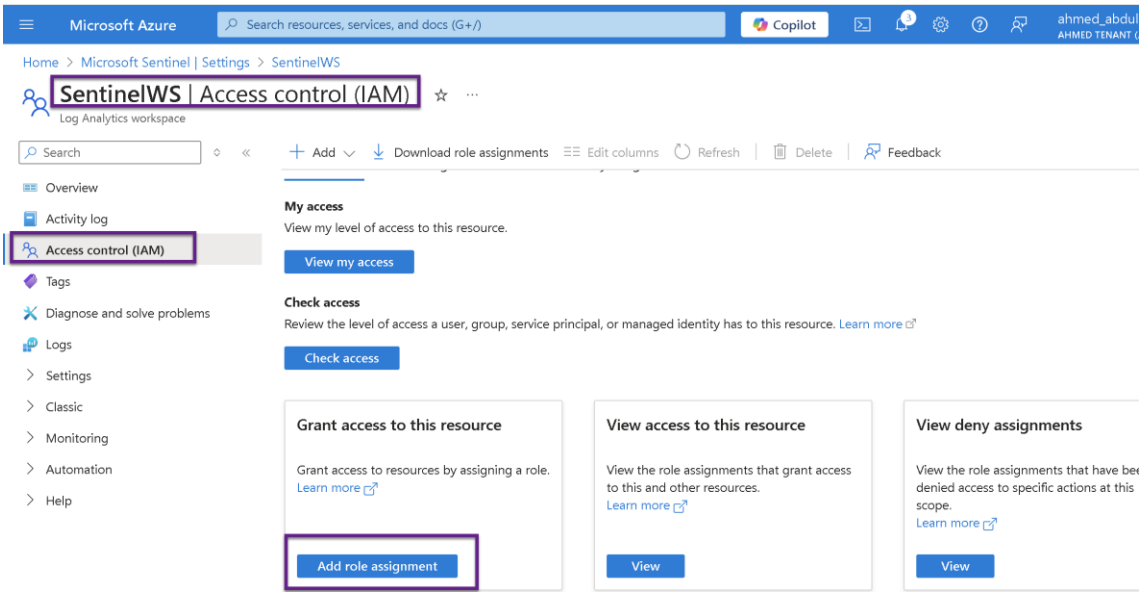


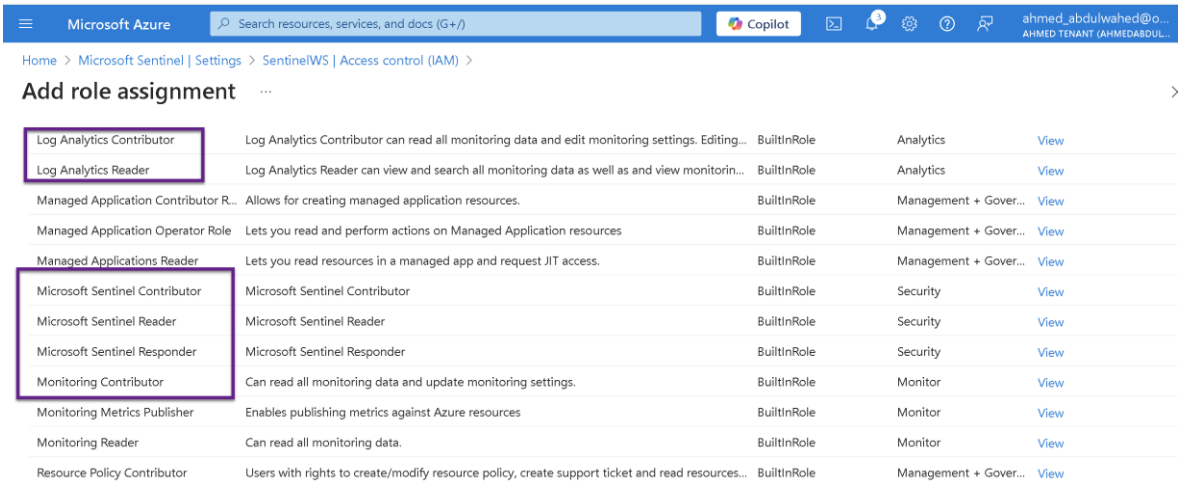
Microsoft Sentinel Roles

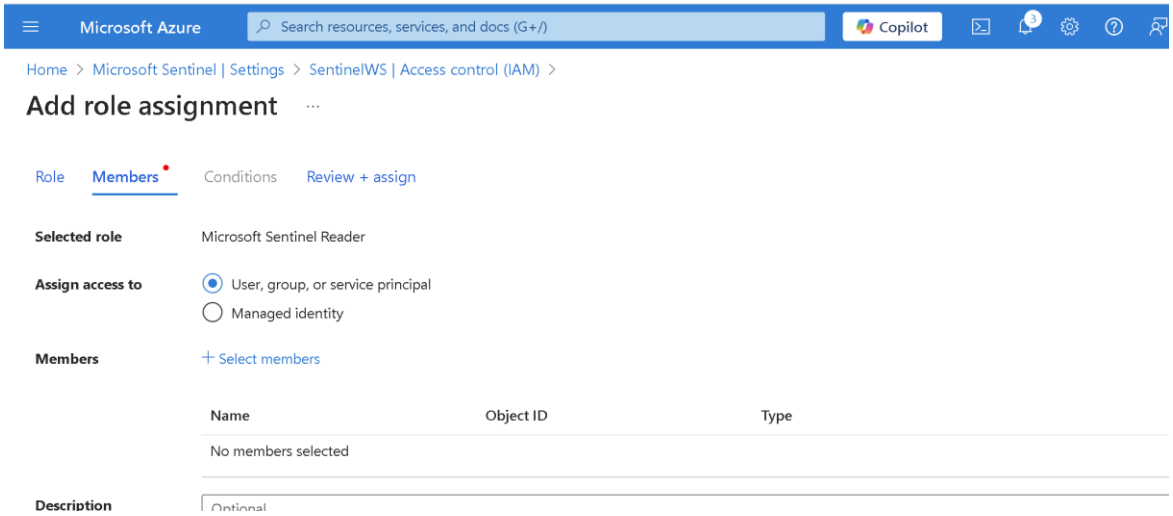
Microsoft Sentinel uses **Azure Role-Based Access Control (RBAC)** to assign permissions and manage access. Roles define what users or groups can do within Sentinel, ensuring security and operational efficiency.

Action	Reader	Responder	Contributor	Log Analytics Contributor
View dashboards, incidents, and alerts	✓	✓	✓	✓
Investigate and manage incidents	✗	✓	✓	✗
Create or edit analytics rules	✗	✗	✓	✗
Manage data connectors and playbooks	✗	✗	✓	✗
Configure Log Analytics workspace	✗	✗	✗	✓


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel
Microsoft Sentinel | Settings
Selected workspace: 'sentinelws'
Search
Threat intelligence
MITRE ATT&CK (Preview)
SOC optimization
Content management
Content hub
Repositories (Preview)
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules (Preview)
Watchlist
Automation
Settings
Workspace usage report
Pricing
Settings
Workspace settings >
Microsoft Sentinel pricing
Microsoft Sentinel is billed based on the volume of data ingested for analysis in Microsoft Sentinel. Microsoft Sentinel offers a flexible and predictable pricing model.
There are two ways to pay for the Microsoft Sentinel service: Commitment Tiers and Pay-As-You-Go. The cost for Microsoft Sentinel depends on the pricing tier selected. Learn more about Microsoft Sentinel pricing.
This workspace is in the simplified pricing tier experience. The pricing tiers shown below include the total cost for Azure Monitor Log Analytics data ingestion and Microsoft Sentinel analysis of all analytics logs in this workspace. Learn more
100 GB/day
31% discount over Pay-as-you-go | SAR 1,110.00 per day
200 GB/day
36% discount over Pay-as-you-go | SAR 2,055.00 per day
300 GB/day
38% discount over Pay-as-you-go | SAR 3,000.00 per day
Data Ingestion (Last 31 days)
No data to display
Data retained per solution (Last 31 days)
No data to display


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel | Settings > SentinelWS
SentinelWS | Access control (IAM)
Log Analytics workspace
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Settings
Classic
Monitoring
Automation
Help
Add
Download role assignments
Edit columns
Refresh
Delete
Feedback
My access
View my level of access to this resource.
View my access
Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more
Check access
Grant access to this resource
Grant access to resources by assigning a role.
Learn more
Add role assignment
View access to this resource
View the role assignments that grant access to this and other resources.
Learn more
View
View deny assignments
View the role assignments that have be denied access to specific actions at this scope.
Learn more
View


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel | Settings > SentinelWS | Access control (IAM) >
Add role assignment
Log Analytics Contributor
Log Analytics Contributor can read all monitoring data and edit monitoring settings. Editing... BuiltInRole Analytics View
Log Analytics Reader
Log Analytics Reader can view and search all monitoring data as well as and view monitorin... BuiltInRole Analytics View
Managed Application Contributor R... Allows for creating managed application resources. BuiltInRole Management + Gover... View
Managed Application Operator Role Lets you read and perform actions on Managed Application resources BuiltInRole Management + Gover... View
Managed Applications Reader Lets you read resources in a managed app and request JIT access. BuiltInRole Management + Gover... View
Microsoft Sentinel Contributor Microsoft Sentinel Contributor BuiltInRole Security View
Microsoft Sentinel Reader Microsoft Sentinel Reader BuiltInRole Security View
Microsoft Sentinel Responder Microsoft Sentinel Responder BuiltInRole Security View
Monitoring Contributor Can read all monitoring data and update monitoring settings. BuiltInRole Monitor View
Monitoring Metrics Publisher Enables publishing metrics against Azure resources BuiltInRole Monitor View
Monitoring Reader Can read all monitoring data. BuiltInRole Monitor View
Resource Policy Contributor Users with rights to create/modify resource policy, create support ticket and read resources... BuiltInRole Management + Gover... View

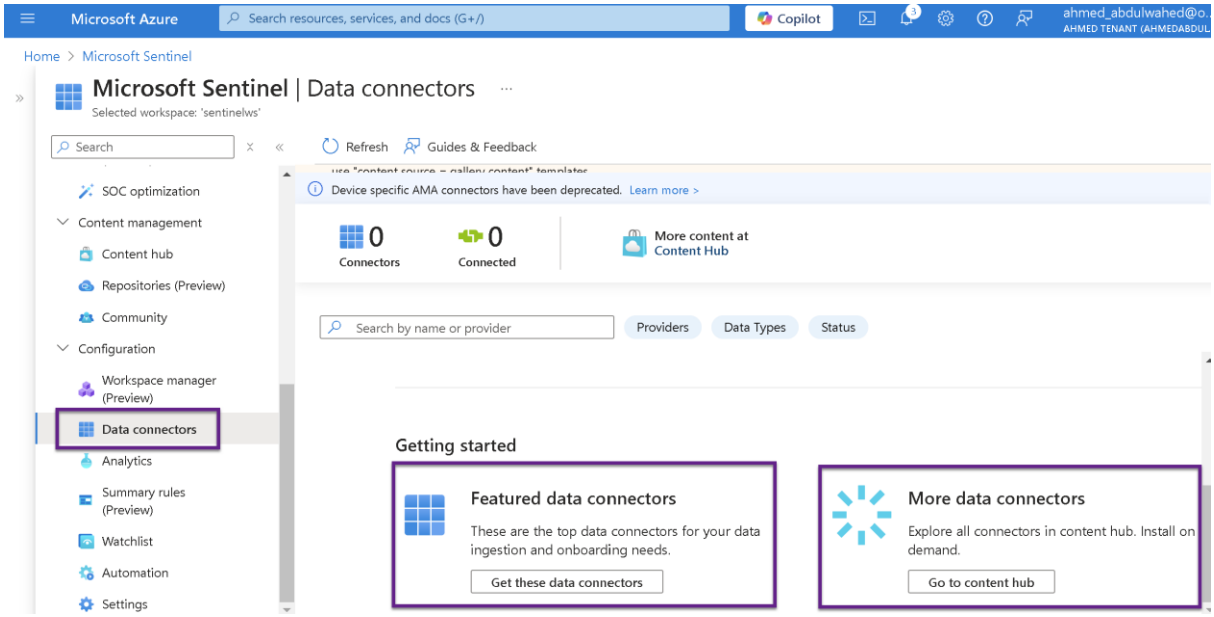


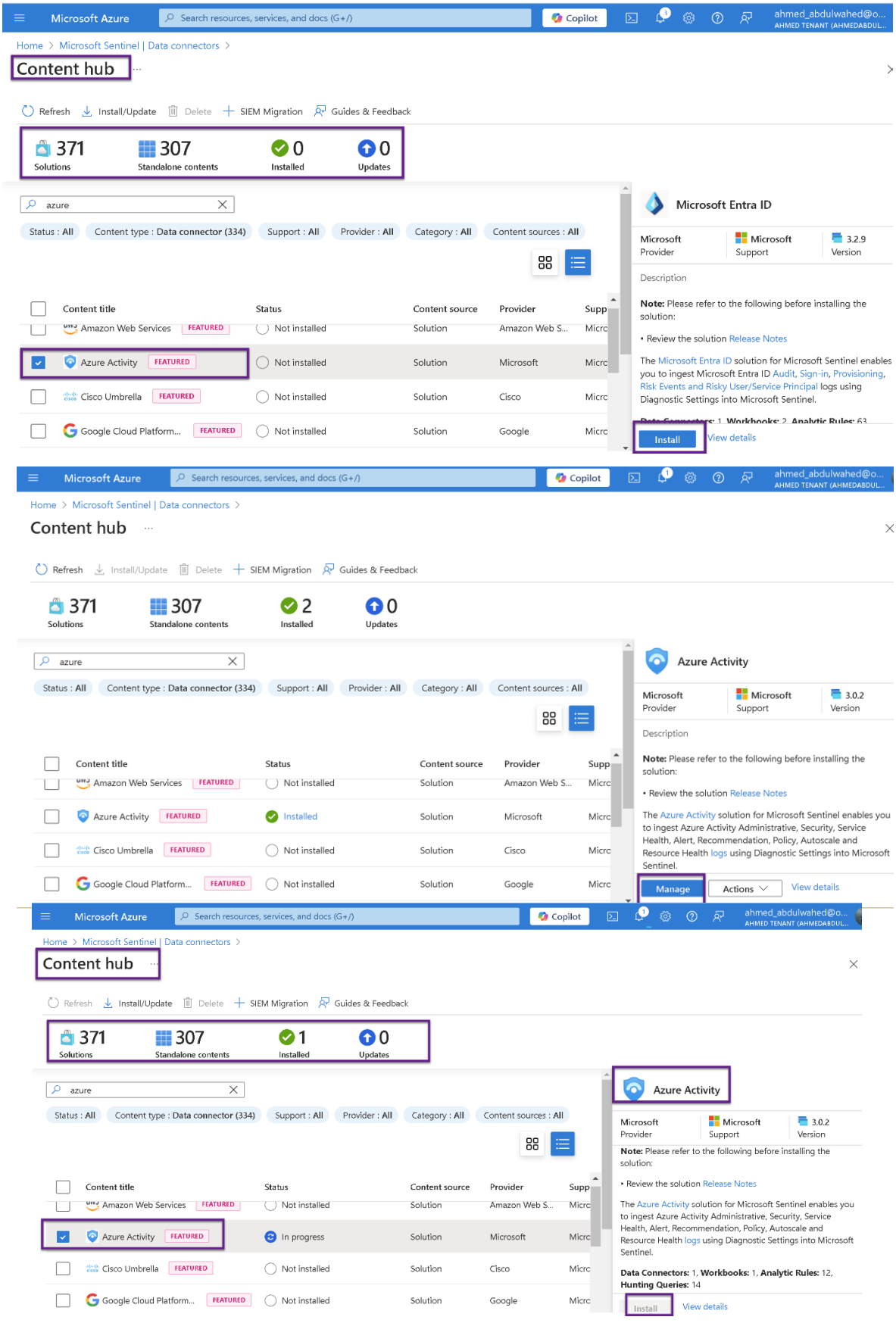
Data Sources and Data Connectors in Microsoft Sentinel

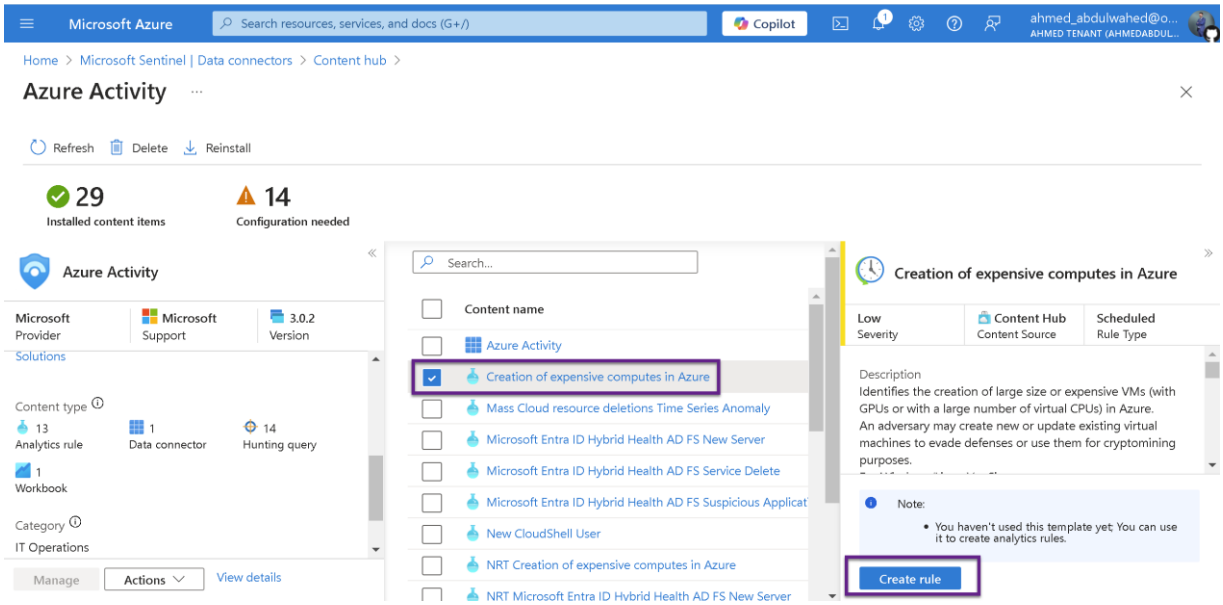
Data Sources and **Data Connectors** are the foundation of Microsoft Sentinel, enabling the ingestion, analysis, and visualization of logs and telemetry from various environments, applications, and systems. Properly configuring them ensures comprehensive threat detection and streamlined security operations.

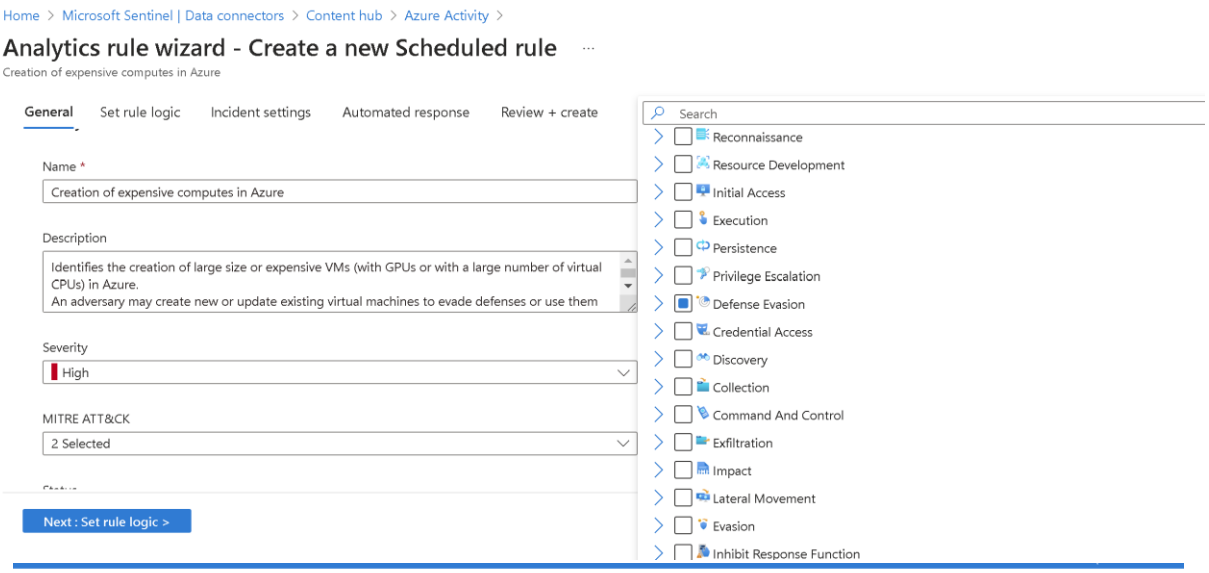
Data Connector Categories

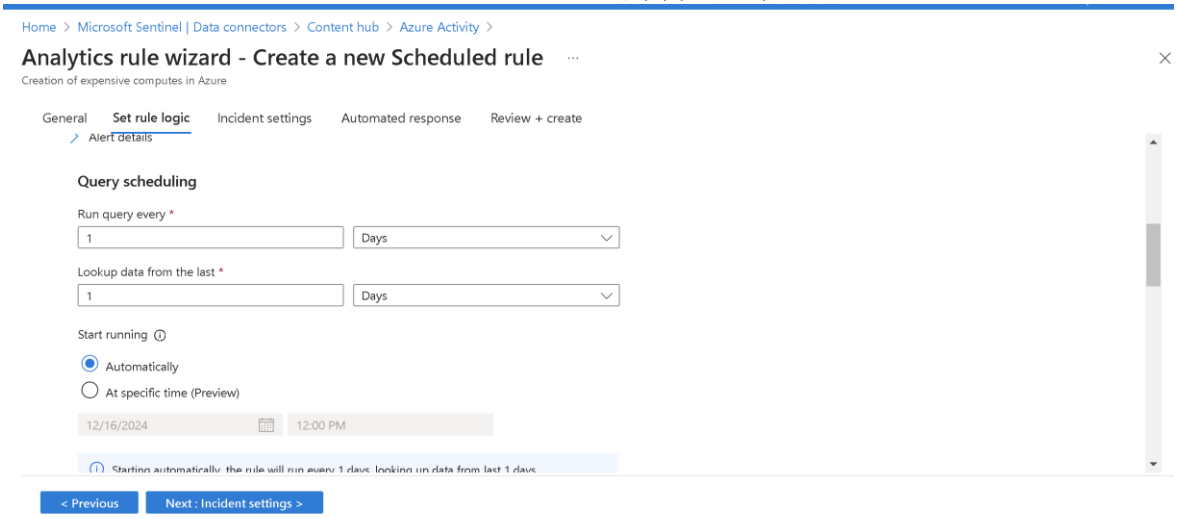
Category	Examples
Identity	Azure AD, MFA logs, risk detection.
Endpoint	Defender for Endpoint, antivirus tools, CrowdStrike, SentinelOne.
Cloud	Azure, AWS, GCP, Salesforce, Google Workspace.
Applications	Microsoft 365 Defender, ServiceNow, Jira.
Networking	Cisco Umbrella, Palo Alto, Fortinet, Check Point.
Security Tools	SIEM systems (e.g., Splunk), threat intelligence feeds, antivirus tools.

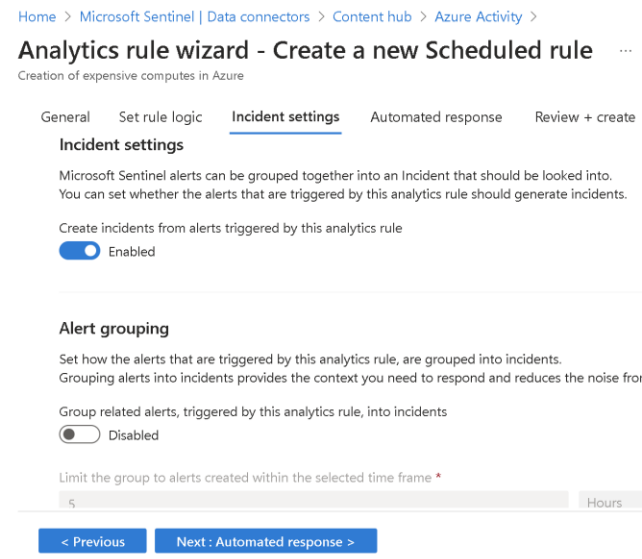


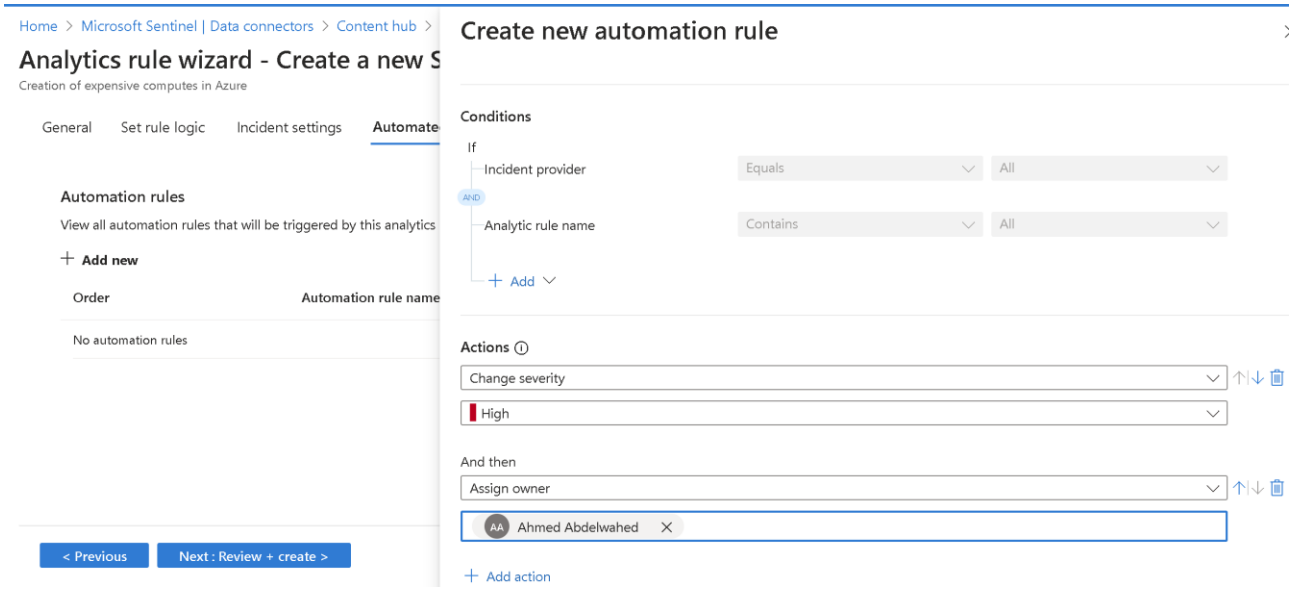

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ahmed_abdulwahed@o...
AHMED TENANT (AHMEDABDUL...
Home > Microsoft Sentinel | Data connectors >
Content hub
Refresh
Install/Update
Delete
SIEM Migration
Guides & Feedback
371 Solutions
307 Standalone contents
0 Installed
0 Updates
azure
Status : All
Content type : Data connector (334)
Support : All
Provider : All
Category : All
Content sources : All
Content title
Status
Content source
Provider
Amazon Web Services FEATURED Not installed Solution Amazon Web S...
Azure Activity FEATURED Not installed Solution Microsoft
Cisco Umbrella FEATURED Not installed Solution Cisco
Google Cloud Platform... FEATURED Not installed Solution Google
Microsoft Entra ID
Microsoft Provider
Microsoft Support
3.2.9 Version
Description
Note: Please refer to the following before installing the solution:
• Review the solution Release Notes
The Microsoft Entra ID solution for Microsoft Sentinel enables you to ingest Microsoft Entra ID Audit, Sign-in, Provisioning, Risk Events and Risky User/Service Principal logs using Diagnostic Settings into Microsoft Sentinel.
Install
View details
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ahmed_abdulwahed@o...
AHMED TENANT (AHMEDABDUL...
Home > Microsoft Sentinel | Data connectors >
Content hub
Refresh
Install/Update
Delete
SIEM Migration
Guides & Feedback
371 Solutions
307 Standalone contents
2 Installed
0 Updates
azure
Status : All
Content type : Data connector (334)
Support : All
Provider : All
Category : All
Content sources : All
Content title
Status
Content source
Provider
Amazon Web Services FEATURED Not installed Solution Amazon Web S...
Azure Activity FEATURED Installed Solution Microsoft
Cisco Umbrella FEATURED Not installed Solution Cisco
Google Cloud Platform... FEATURED Not installed Solution Google
Azure Activity
Microsoft Provider
Microsoft Support
3.0.2 Version
Description
Note: Please refer to the following before installing the solution:
• Review the solution Release Notes
The Azure Activity solution for Microsoft Sentinel enables you to ingest Azure Activity Administrative, Security, Service Health, Alert, Recommendation, Policy, Autoscale and Resource Health logs using Diagnostic Settings into Microsoft Sentinel.
Manage
Actions
View details
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ahmed_abdulwahed@o...
AHMED TENANT (AHMEDABDUL...
Home > Microsoft Sentinel | Data connectors >
Content hub
Refresh
Install/Update
Delete
SIEM Migration
Guides & Feedback
371 Solutions
307 Standalone contents
1 Installed
0 Updates
azure
Status : All
Content type : Data connector (334)
Support : All
Provider : All
Category : All
Content sources : All
Content title
Status
Content source
Provider
Amazon Web Services FEATURED Not installed Solution Amazon Web S...
Azure Activity FEATURED In progress Solution Microsoft
Cisco Umbrella FEATURED Not installed Solution Cisco
Google Cloud Platform... FEATURED Not installed Solution Google
Azure Activity
Microsoft Provider
Microsoft Support
3.0.2 Version
Note: Please refer to the following before installing the solution:
• Review the solution Release Notes
The Azure Activity solution for Microsoft Sentinel enables you to ingest Azure Activity Administrative, Security, Service Health, Alert, Recommendation, Policy, Autoscale and Resource Health logs using Diagnostic Settings into Microsoft Sentinel.
Data Connectors: 1, Workbooks: 1, Analytic Rules: 12, Hunting Queries: 14
Install
View details


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ahmed_abdulwahed@o...
AHMED TENANT (AHMEDABDUL...
Home > Microsoft Sentinel | Data connectors > Content hub >
Azure Activity
Refresh
Delete
Reinstall
29
Installed content items
14
Configuration needed
Azure Activity
Microsoft
Provider
Microsoft
Support
3.0.2
Version
Solutions
Content type
13
Analytics rule
1
Data connector
14
Hunting query
1
Workbook
Category
IT Operations
Manage
Actions
View details
Search...
Content name
Azure Activity
Creation of expensive computes in Azure
Mass Cloud resource deletions Time Series Anomaly
Microsoft Entra ID Hybrid Health AD FS New Server
Microsoft Entra ID Hybrid Health AD FS Service Delete
Microsoft Entra ID Hybrid Health AD FS Suspicious Applicat
New CloudShell User
NRT Creation of expensive computes in Azure
NRT Microsoft Entra ID Hybrid Health AD FS New Server
Creation of expensive computes in Azure
Low
Severity
Content Hub
Content Source
Scheduled
Rule Type
Description
Identifies the creation of large size or expensive VMs (with GPUs or with a large number of virtual CPUs) in Azure.
An adversary may create new or update existing virtual machines to evade defenses or use them for cryptomining purposes.
Note:
You haven't used this template yet. You can use it to create analytics rules.
Create rule

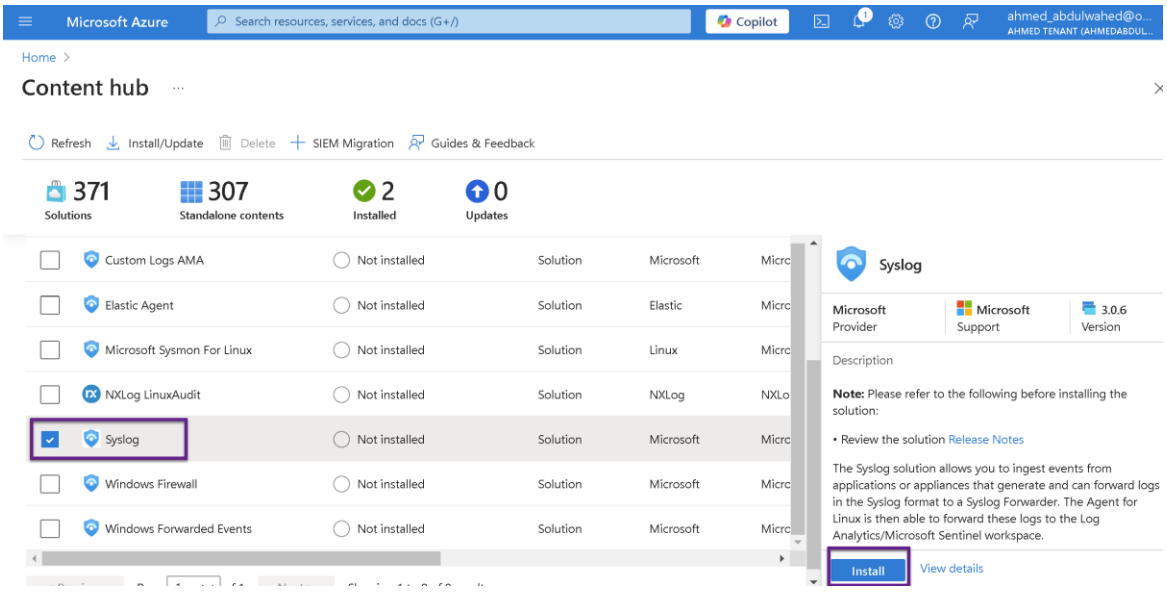

Home > Microsoft Sentinel | Data connectors > Content hub > Azure Activity >
Analytics rule wizard - Create a new Scheduled rule
Creation of expensive computes in Azure
General
Set rule logic
Incident settings
Automated response
Review + create
Name *
Creation of expensive computes in Azure
Description
Identifies the creation of large size or expensive VMs (with GPUs or with a large number of virtual CPUs) in Azure.
An adversary may create new or update existing virtual machines to evade defenses or use them
Severity
High
MITRE ATT&CK
2 Selected
Next : Set rule logic >
Search
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Collection
Command And Control
Exfiltration
Impact
Lateral Movement
Evasion
Inhibit Response Function

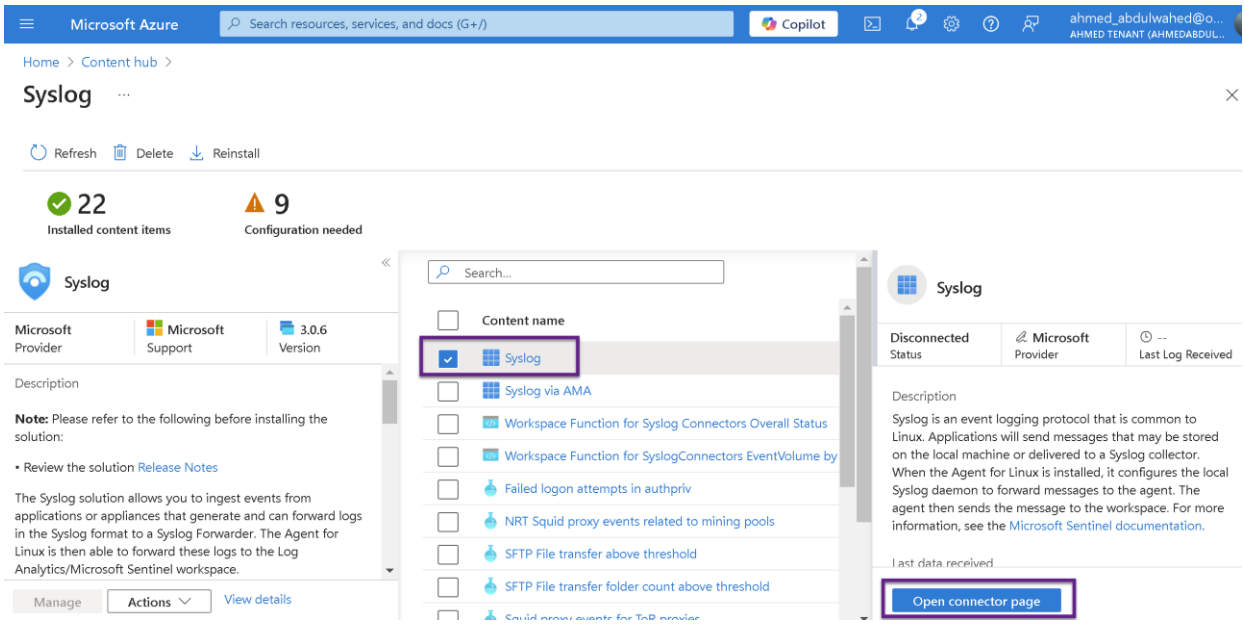

Home > Microsoft Sentinel | Data connectors > Content hub > Azure Activity >
Analytics rule wizard - Create a new Scheduled rule
Creation of expensive computes in Azure
General
Set rule logic
Incident settings
Automated response
Review + create
Alert details
Query scheduling
Run query every *
1
Days
Lookup data from the last *
1
Days
Start running
Automatically
At specific time (Preview)
12/16/2024
12:00 PM
< Previous
Next : Incident settings >

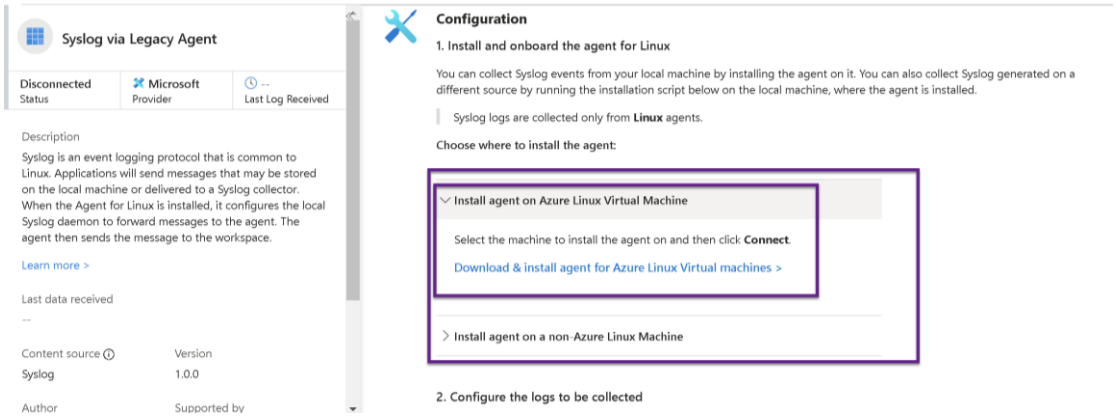

Home > Microsoft Sentinel | Data connectors > Content hub > Azure Activity >
Analytics rule wizard - Create a new Scheduled rule
Creation of expensive computes in Azure
General
Set rule logic
Incident settings
Automated response
Review + create
Incident settings
Microsoft Sentinel alerts can be grouped together into an Incident that should be looked into.
You can set whether the alerts that are triggered by this analytics rule should generate incidents.
Create incidents from alerts triggered by this analytics rule
Enabled
Alert grouping
Set how the alerts that are triggered by this analytics rule, are grouped into incidents.
Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.
Group related alerts, triggered by this analytics rule, into incidents
Disabled
Limit the group to alerts created within the selected time frame *
5
Hours
< Previous
Next : Automated response >

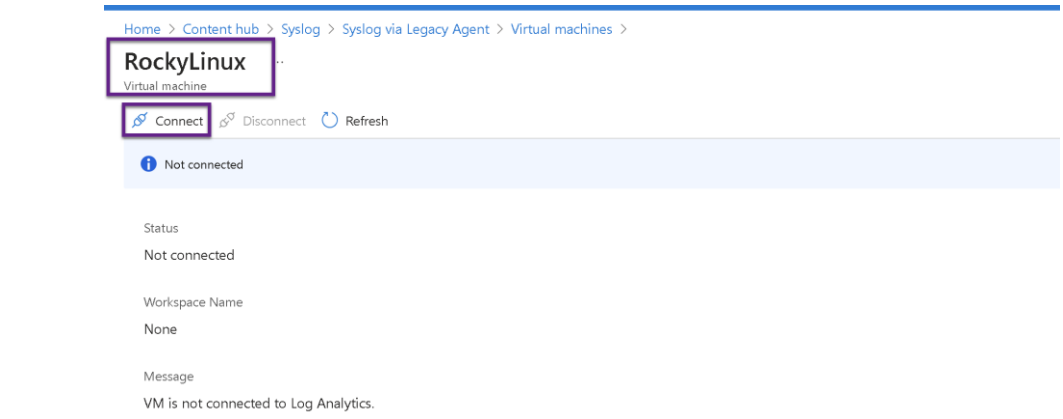

Home > Microsoft Sentinel | Data connectors > Content hub >
Analytics rule wizard - Create a new S
Creation of expensive computes in Azure
General
Set rule logic
Incident settings
Automate
Automation rules
View all automation rules that will be triggered by this analytics
Add new
Order
Automation rule name
No automation rules
< Previous
Next : Review + create >
Create new automation rule
Conditions
If
Incident provider
Equals
All
AND
Analytic rule name
Contains
All
Add
Actions
Change severity
High
And then
Assign owner
AA
Ahmed Abdelwahed
Add action

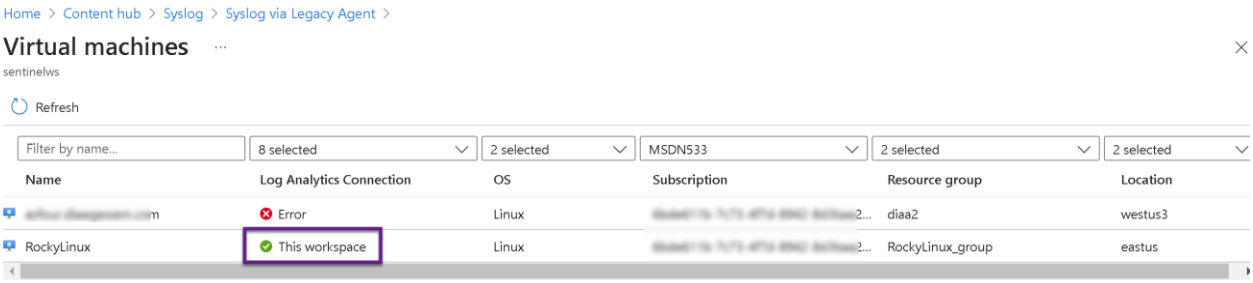
Agent Based Connector (Linux)

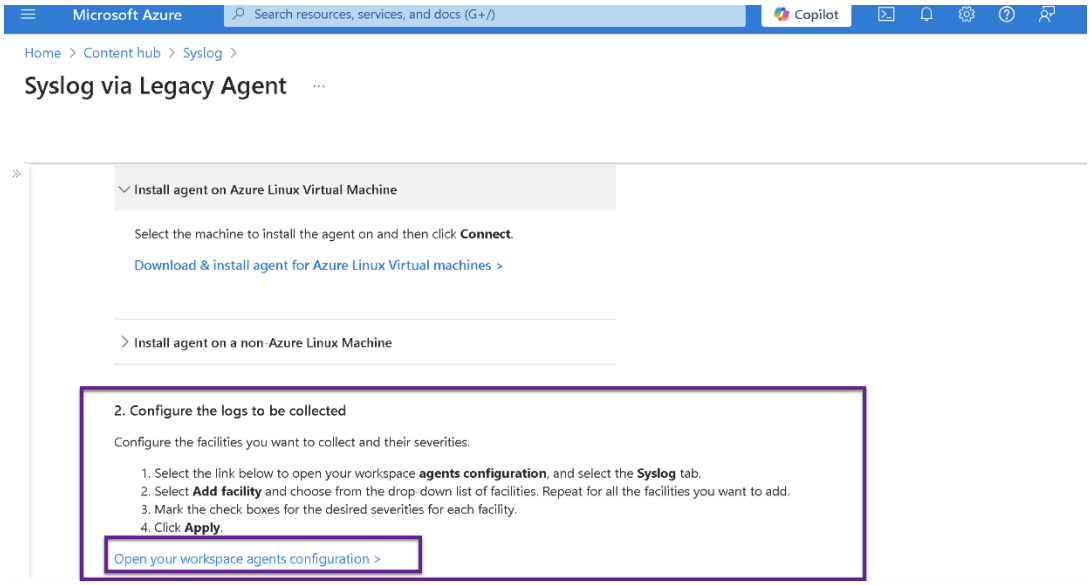


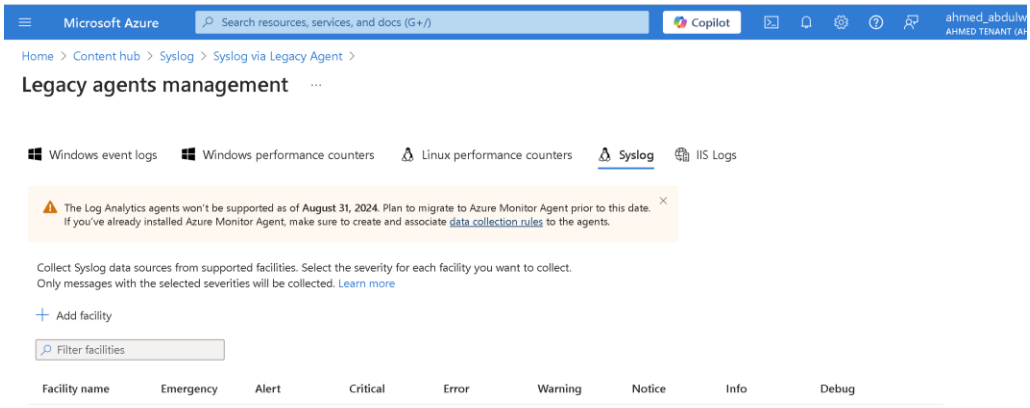


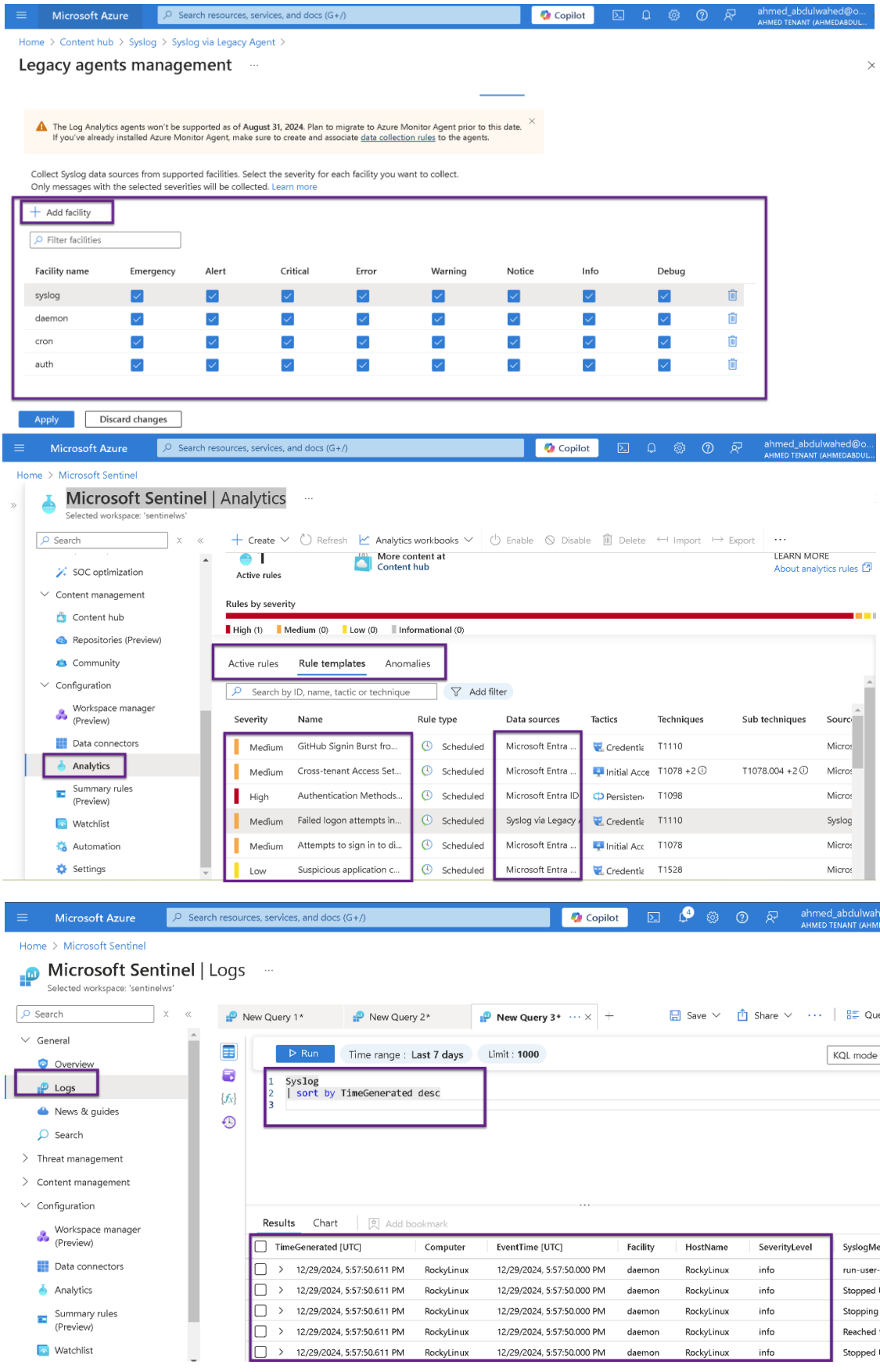



Home > Content hub > Syslog > Syslog via Legacy Agent > Virtual machines >
RockyLinux
Virtual machine
Connect
Disconnect
Refresh
Not connected
Status
Not connected
Workspace Name
None
Message
VM is not connected to Log Analytics.


Home > Content hub > Syslog > Syslog via Legacy Agent >
Virtual machines
sentinelws
Refresh
Filter by name...
8 selected
2 selected
MSDN533
2 selected
2 selected
Name
Log Analytics Connection
OS
Subscription
Resource group
Location
Error
Linux
diaa2
westus3
RockyLinux
This workspace
Linux
RockyLinux_group
eastus

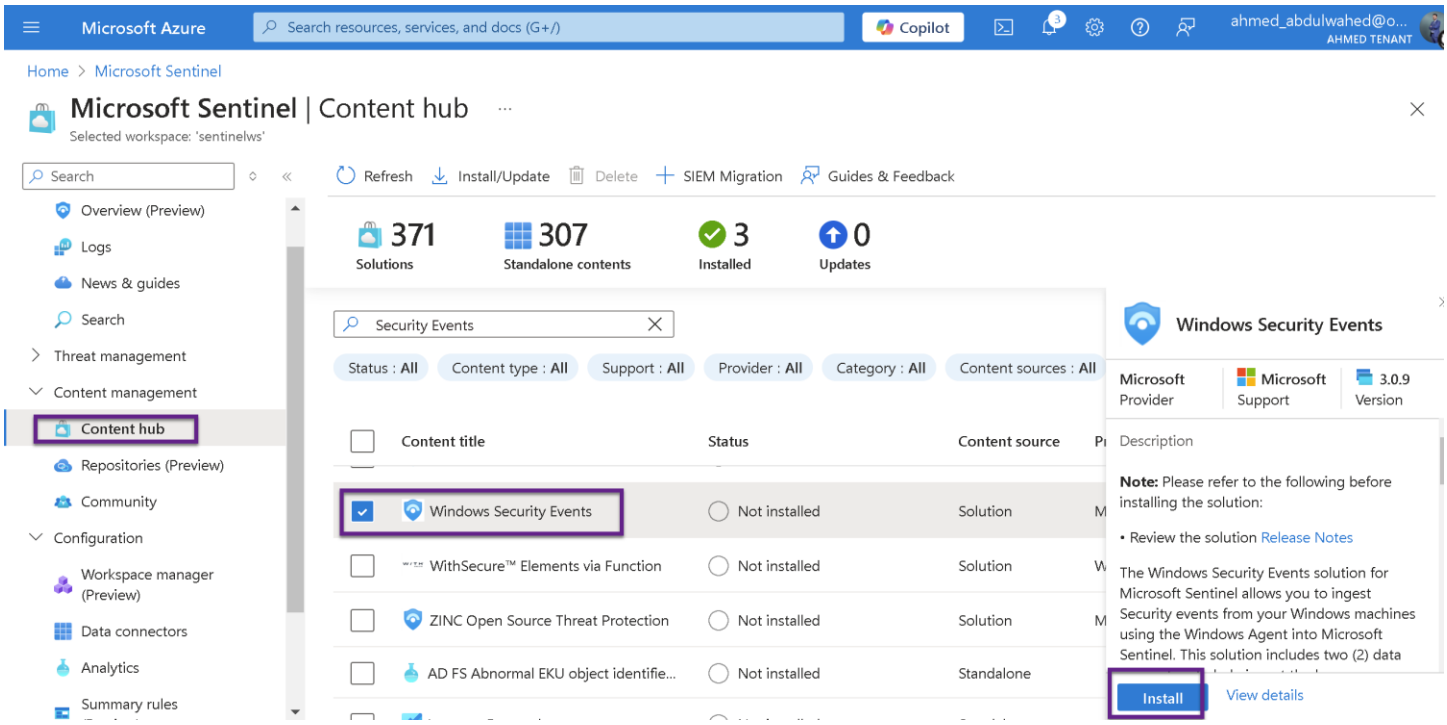

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Content hub > Syslog >
Syslog via Legacy Agent
Install agent on Azure Linux Virtual Machine
Select the machine to install the agent on and then click Connect.
Download & install agent for Azure Linux Virtual machines >
Install agent on a non-Azure Linux Machine
2. Configure the logs to be collected
Configure the facilities you want to collect and their severities.
1. Select the link below to open your workspace agents configuration, and select the Syslog tab.
2. Select Add facility and choose from the drop-down list of facilities. Repeat for all the facilities you want to add.
3. Mark the check boxes for the desired severities for each facility.
4. Click Apply.
Open your workspace agents configuration >

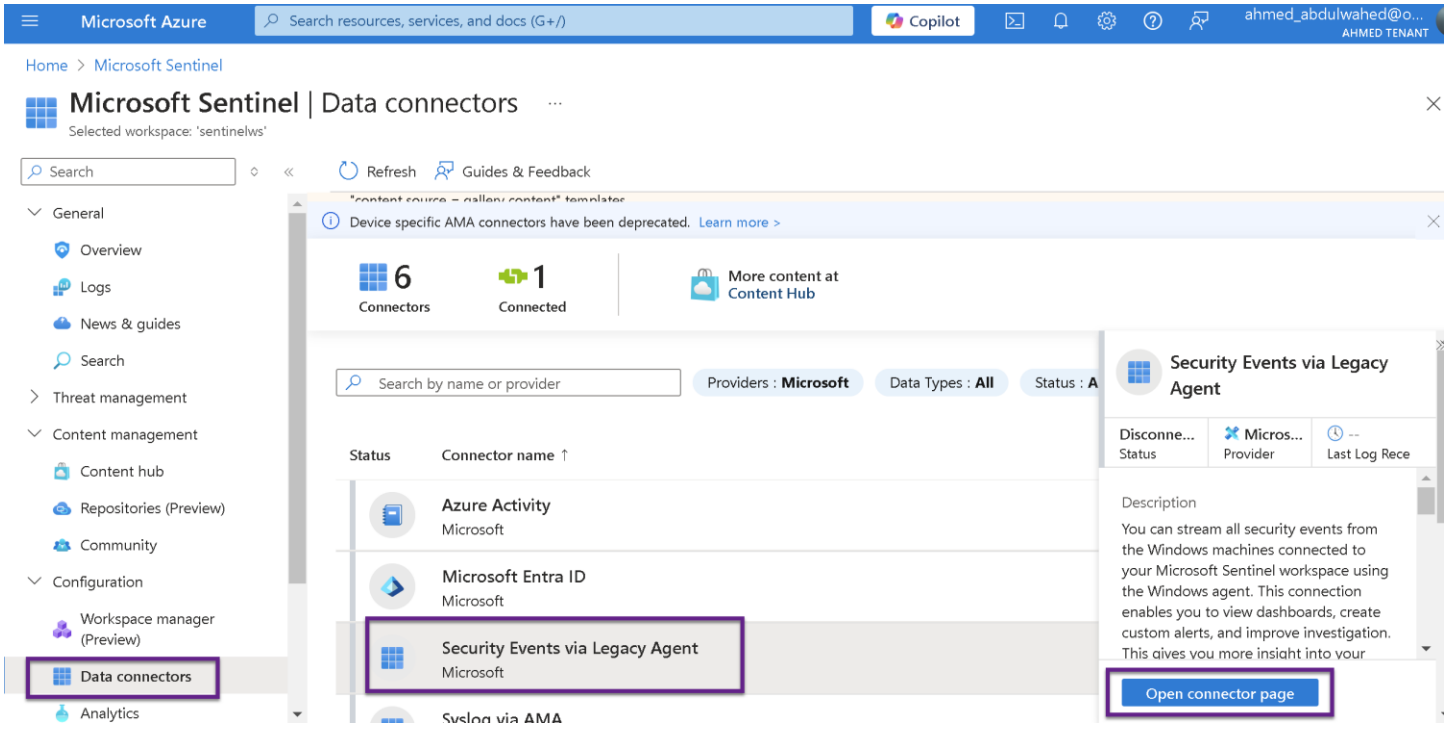

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Content hub > Syslog > Syslog via Legacy Agent >
Legacy agents management
Windows event logs
Windows performance counters
Linux performance counters
Syslog
IIS Logs
The Log Analytics agents won't be supported as of August 31, 2024. Plan to migrate to Azure Monitor Agent prior to this date.
If you've already installed Azure Monitor Agent, make sure to create and associate data collection rules to the agents.
Collect Syslog data sources from supported facilities. Select the severity for each facility you want to collect.
Only messages with the selected severities will be collected. Learn more
Add facility
Filter facilities
Facility name
Emergency
Alert
Critical
Error
Warning
Notice
Info
Debug

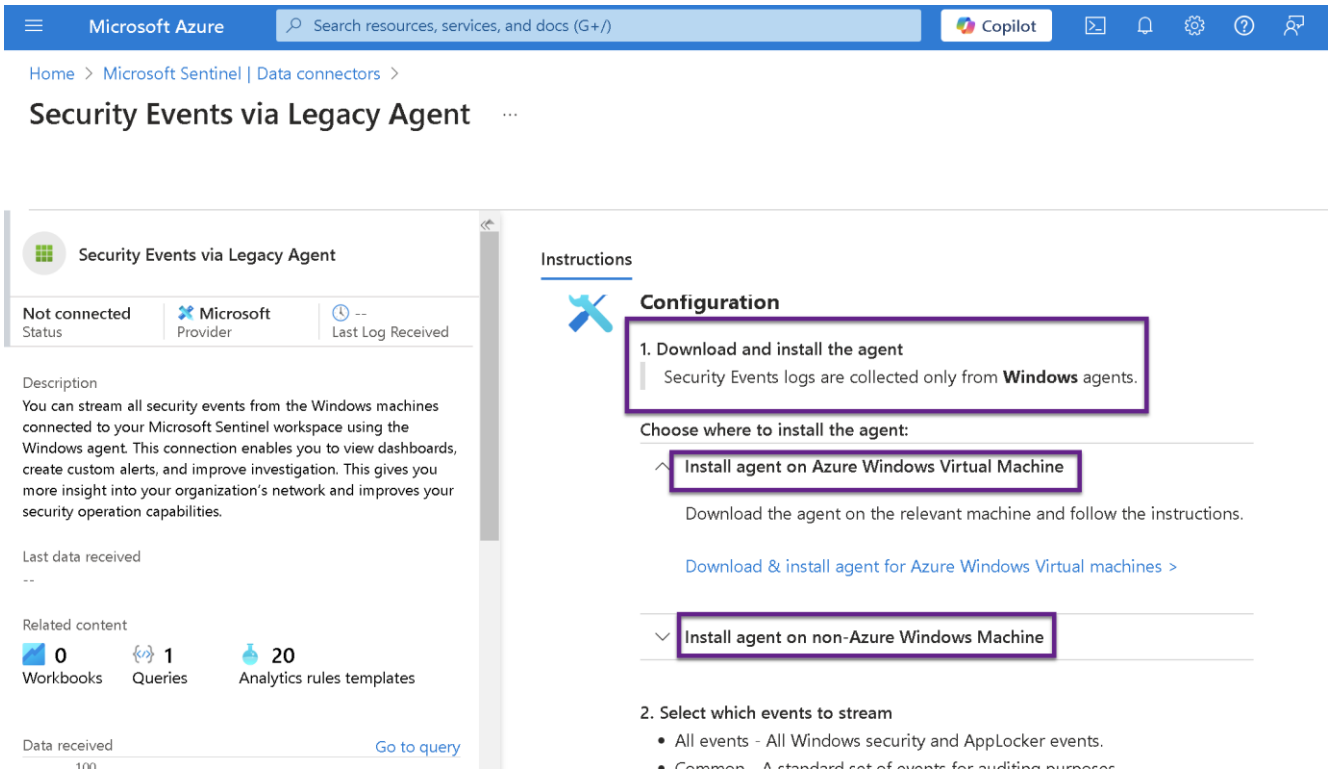

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Content hub > Syslog > Syslog via Legacy Agent >
Legacy agents management
The Log Analytics agents won't be supported as of August 31, 2024. Plan to migrate to Azure Monitor Agent prior to this date.
If you've already installed Azure Monitor Agent, make sure to create and associate data collection rules to the agents.
Collect Syslog data sources from supported facilities. Select the severity for each facility you want to collect.
Only messages with the selected severities will be collected. Learn more
Add facility
Filter facilities
Facility name
Emergency
Alert
Critical
Error
Warning
Notice
Info
Debug
syslog
daemon
cron
auth
Apply
Discard changes
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel
Microsoft Sentinel | Analytics
Selected workspace: 'sentinelws'
Search
Create
Refresh
Analytics workbooks
Enable
Disable
Delete
Import
Export
SOC optimization
Content management
Content hub
Repositories (Preview)
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules (Preview)
Watchlist
Automation
Settings
Active rules
More content at Content hub
LEARN MORE
About analytics rules
Rules by severity
High (1)
Medium (0)
Low (0)
Informational (0)
Active rules
Rule templates
Anomalies
Search by ID, name, tactic or technique
Add filter
Severity
Name
Rule type
Data sources
Tactics
Techniques
Sub techniques
Medium
GitHub Signin Burst fro...
Scheduled
Microsoft Entra ...
T1110
Medium
Cross-tenant Access Set...
Scheduled
Microsoft Entra ...
T1078 +2
T1078.004 +2
High
Authentication Methods...
Scheduled
Microsoft Entra ID
T1098
Medium
Failed logon attempts in...
Scheduled
Syslog via Legacy
T1110
Medium
Attempts to sign in to di...
Scheduled
Microsoft Entra ...
T1078
Low
Suspicious application c...
Scheduled
Microsoft Entra ...
T1528
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'sentinelws'
Search
New Query 1*
New Query 2*
New Query 3*
Save
Share
Queries hu
General
Overview
Logs
News & guides
Search
Threat management
Content management
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules (Preview)
Watchlist
Run
Time range : Last 7 days
Limit : 1000
KQL mode
1 Syslog
2 | sort by TimeGenerated desc
3
Results
Chart
Add bookmark
TimeGenerated [UTC]
Computer
EventTime [UTC]
Facility
HostName
SeverityLevel
SyslogMessage
12/29/2024, 5:57:50.611 PM
RockyLinux
12/29/2024, 5:57:50.000 PM
daemon
RockyLinux
info
Stopped User
Stopping User
Reached targe

Install Microsoft Sentinel agent on Windows Server

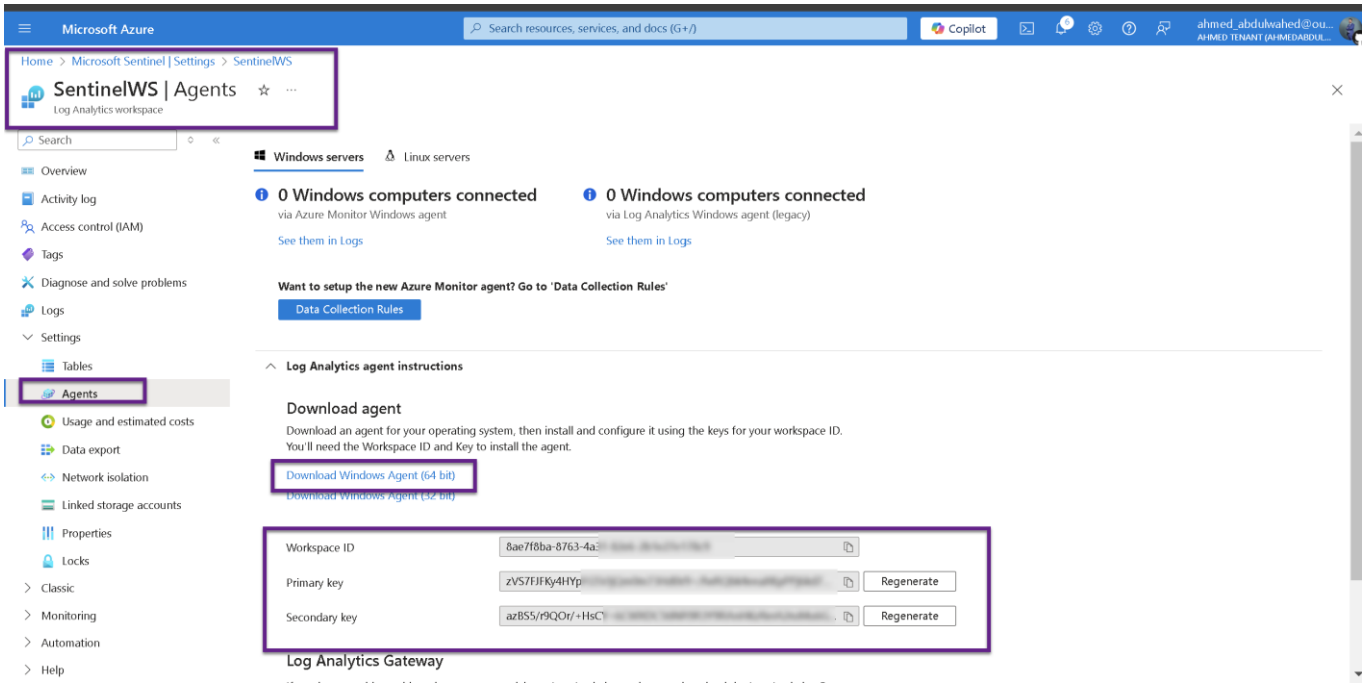
Add windows security events collector

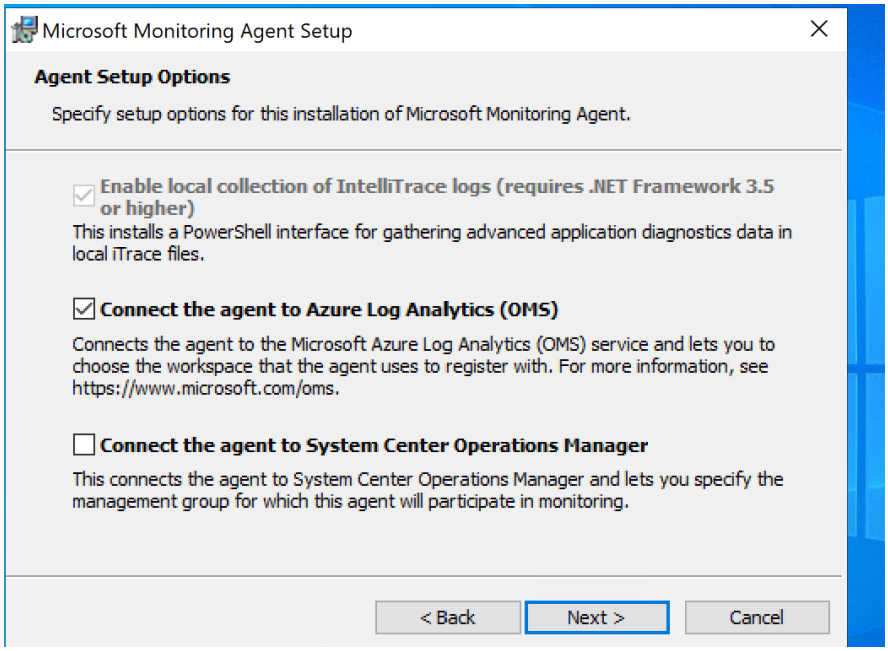


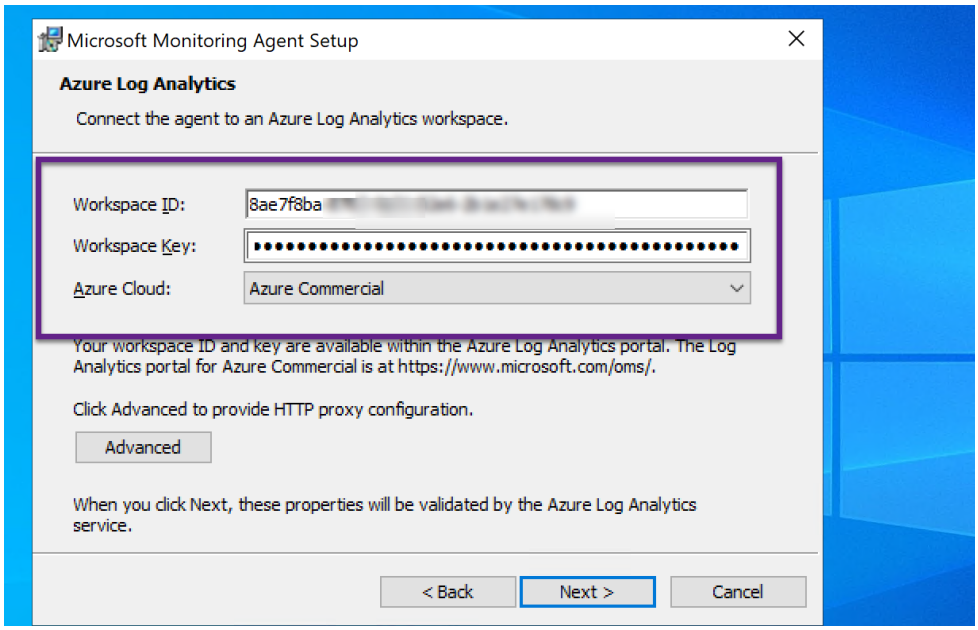




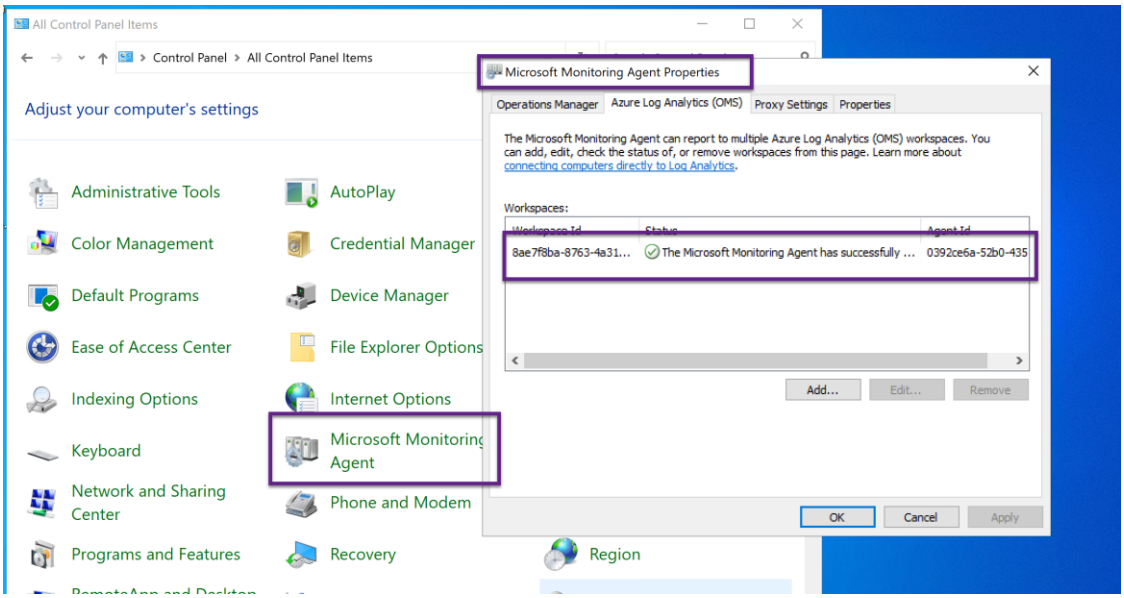
Or through the following

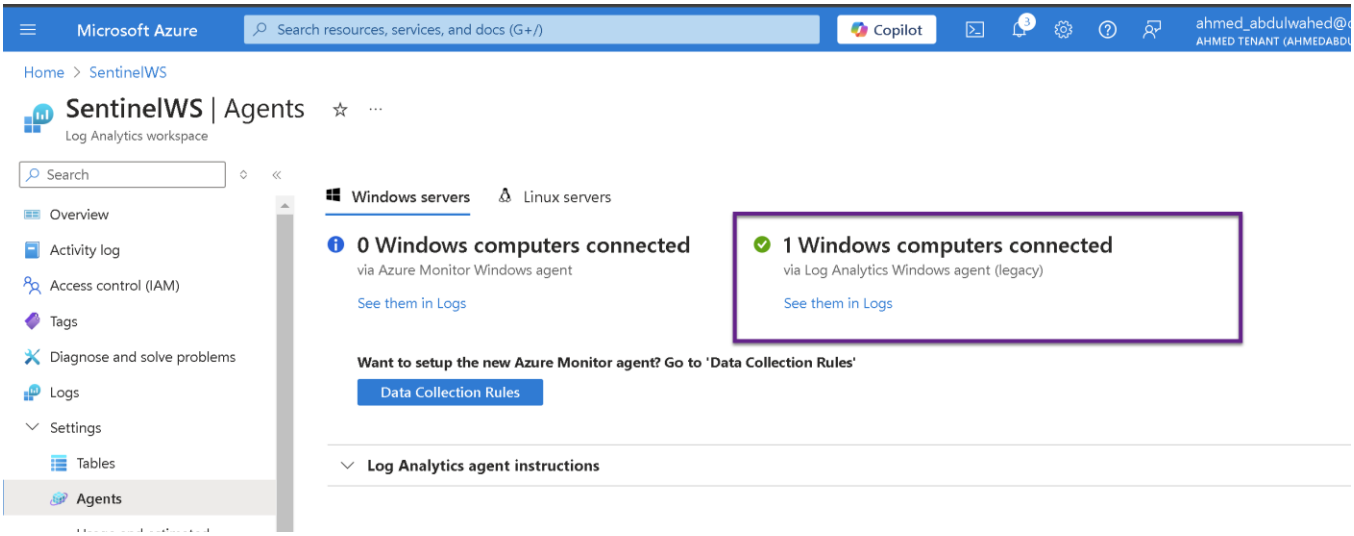



Microsoft Monitoring Agent Setup
Agent Setup Options
Specify setup options for this installation of Microsoft Monitoring Agent.
Enable local collection of IntelliTrace logs (requires .NET Framework 3.5 or higher)
This installs a PowerShell interface for gathering advanced application diagnostics data in local iTrace files.
Connect the agent to Azure Log Analytics (OMS)
Connects the agent to the Microsoft Azure Log Analytics (OMS) service and lets you to choose the workspace that the agent uses to register with. For more information, see https://www.microsoft.com/oms.
Connect the agent to System Center Operations Manager
This connects the agent to System Center Operations Manager and lets you specify the management group for which this agent will participate in monitoring.
< Back
Next >
Cancel

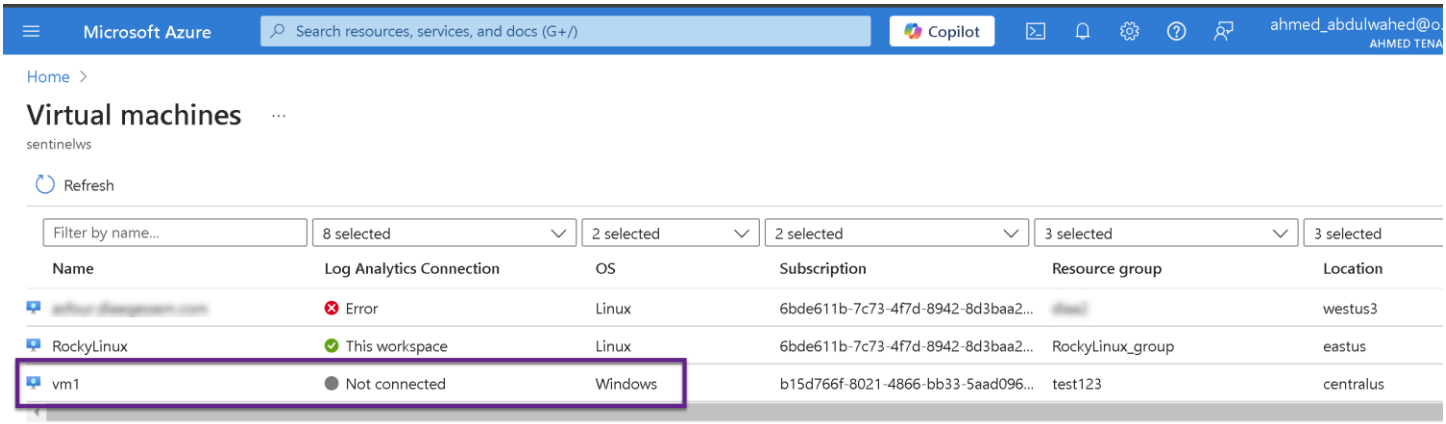

Microsoft Monitoring Agent Setup
Azure Log Analytics
Connect the agent to an Azure Log Analytics workspace.
Workspace ID:
8ae7f8ba
Workspace Key:
Azure Cloud:
Azure Commercial
Your workspace ID and key are available within the Azure Log Analytics portal. The Log Analytics portal for Azure Commercial is at https://www.microsoft.com/oms/.
Click Advanced to provide HTTP proxy configuration.
Advanced
When you click Next, these properties will be validated by the Azure Log Analytics service.
< Back
Next >
Cancel

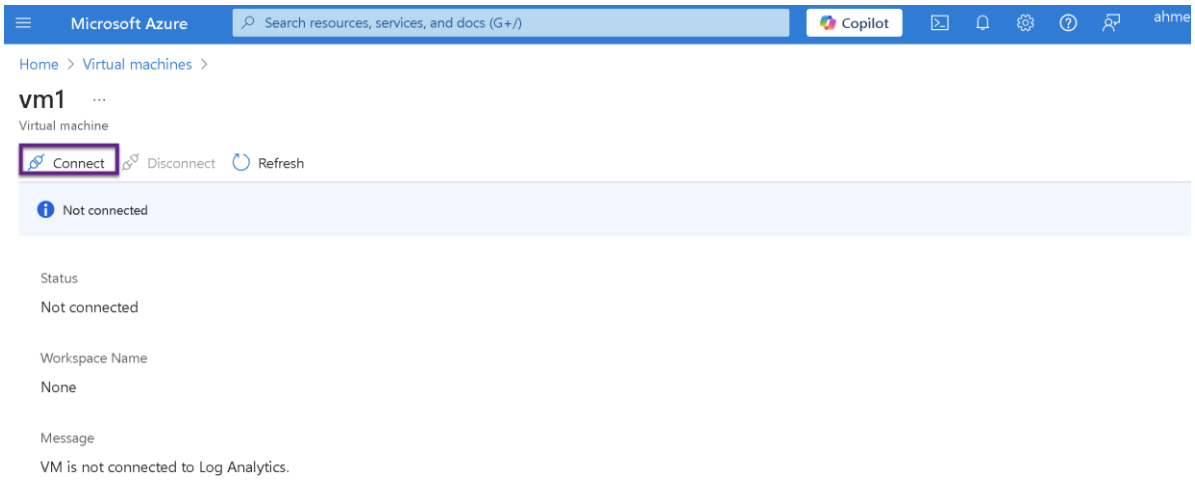
Microsoft Sentinel

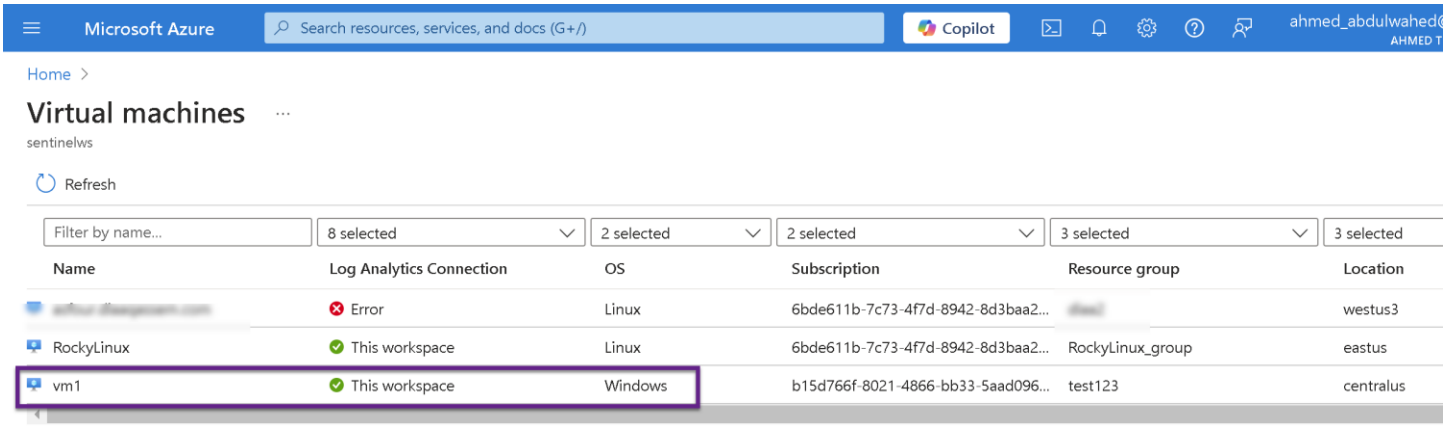


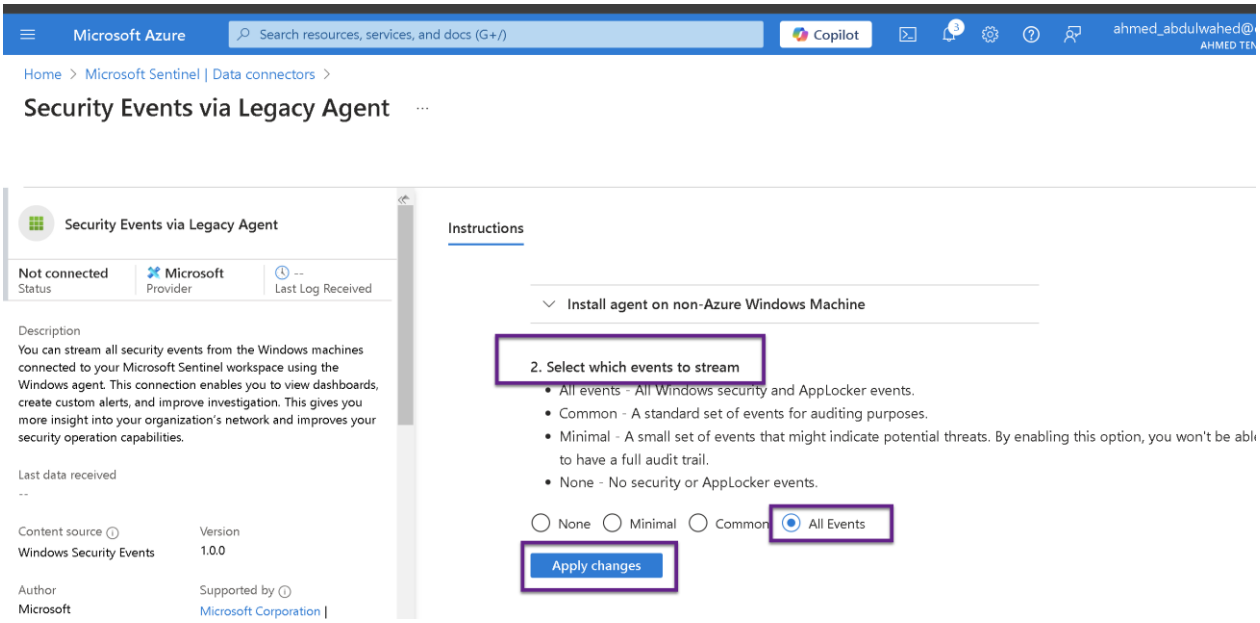


In case of a VM in Azure

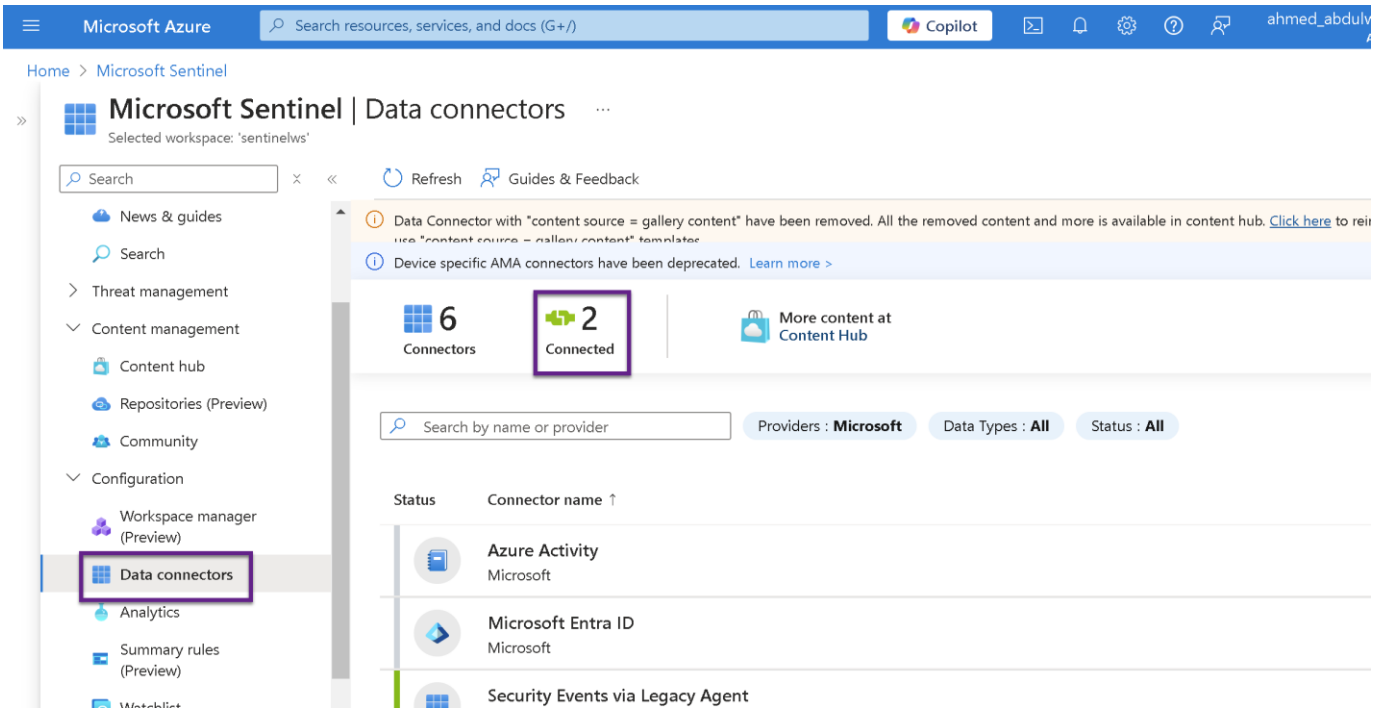



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Virtual machines >
vm1
Virtual machine
Connect
Disconnect
Refresh
Not connected
Status
Not connected
Workspace Name
None
Message
VM is not connected to Log Analytics.

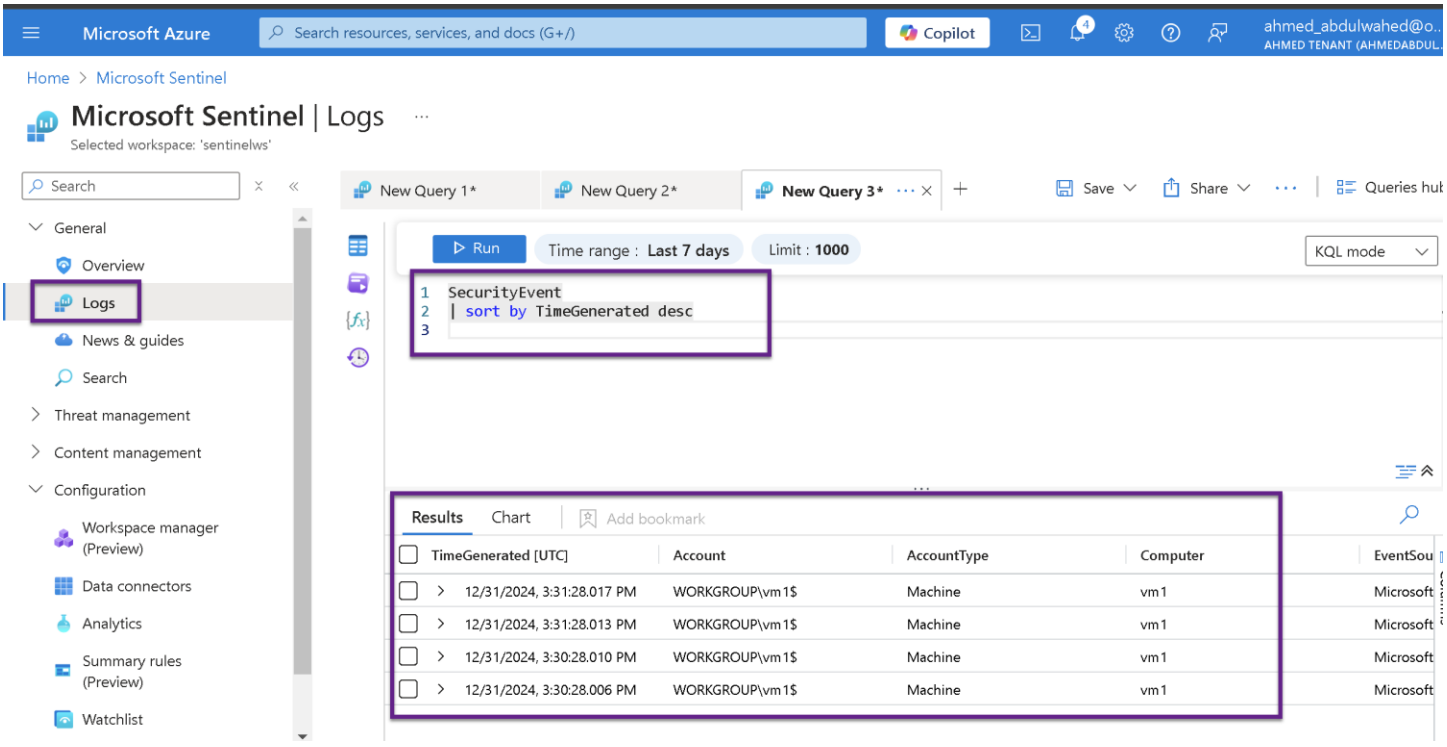

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home >
Virtual machines
sentinelws
Refresh
Filter by name...
8 selected
2 selected
2 selected
3 selected
3 selected
Name
Log Analytics Connection
OS
Subscription
Resource group
Location
Error
Linux
6bde611b-7c73-4f7d-8942-8d3baa2...
westus3
RockyLinux
This workspace
Linux
6bde611b-7c73-4f7d-8942-8d3baa2...
RockyLinux_group
eastus
vm1
This workspace
Windows
b15d766f-8021-4866-bb33-5aad096...
test123
centralus

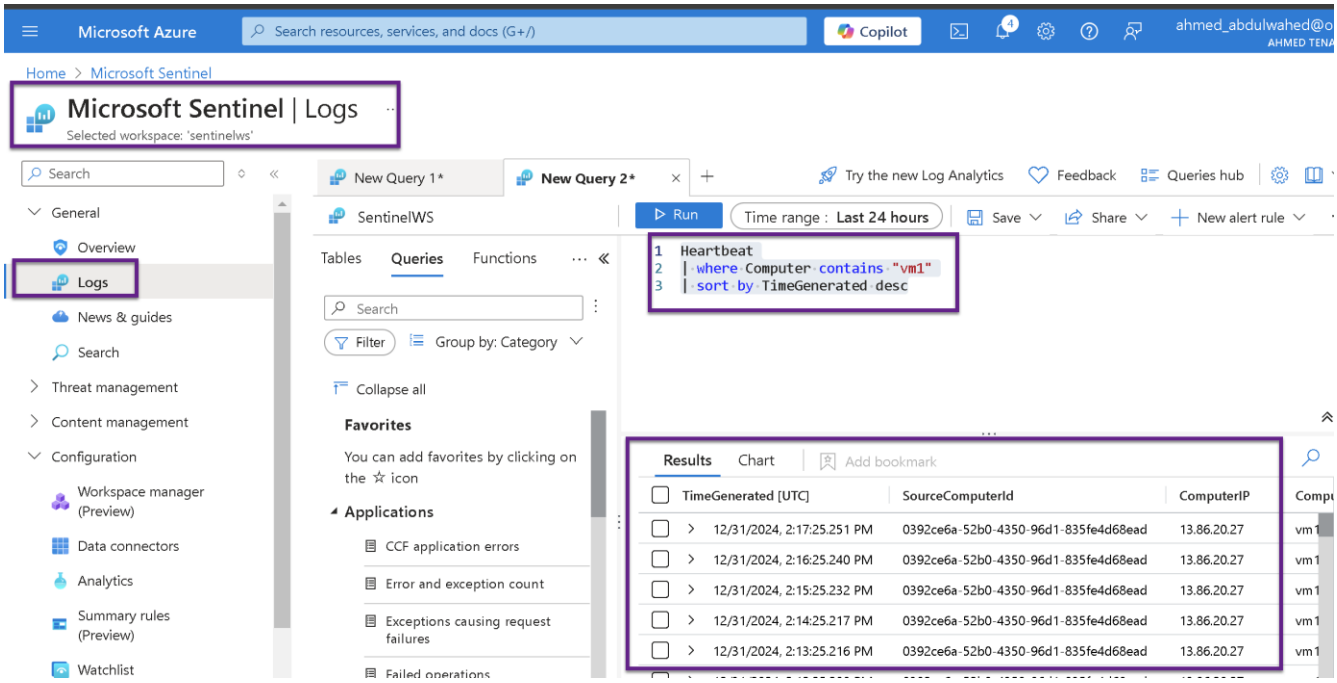

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel | Data connectors >
Security Events via Legacy Agent
Security Events via Legacy Agent
Not connected
Status
Microsoft
Provider
Last Log Received
Description
You can stream all security events from the Windows 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
Instructions
Install agent on non-Azure Windows Machine
2. Select which events to stream
All events - All Windows security and AppLocker events.
Common - A standard set of events for auditing purposes.
Minimal - A small set of events that might indicate potential threats. By enabling this option, you won't be abl
to have a full audit trail.
None - No security or AppLocker events.
None
Minimal
Common
All Events
Apply changes

Microsoft Sentinel



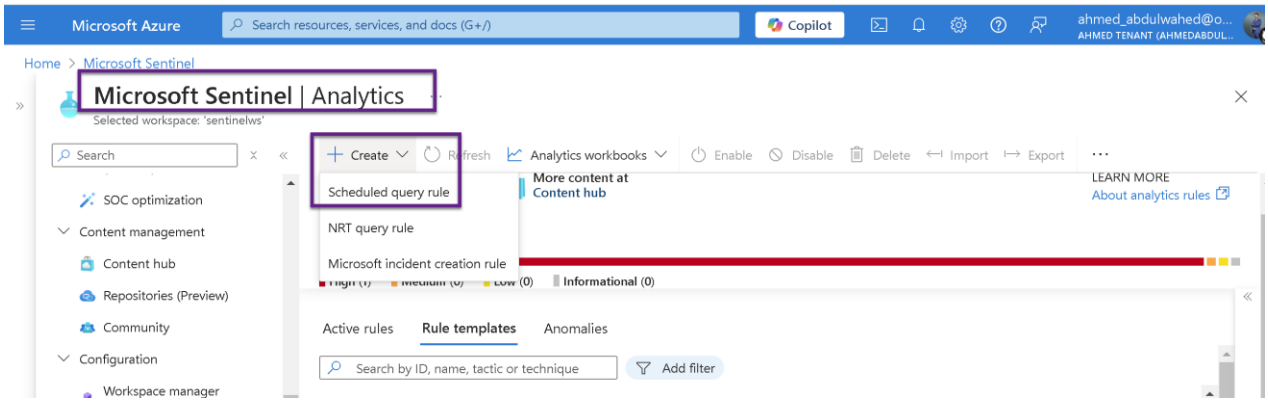
Machine Is connected

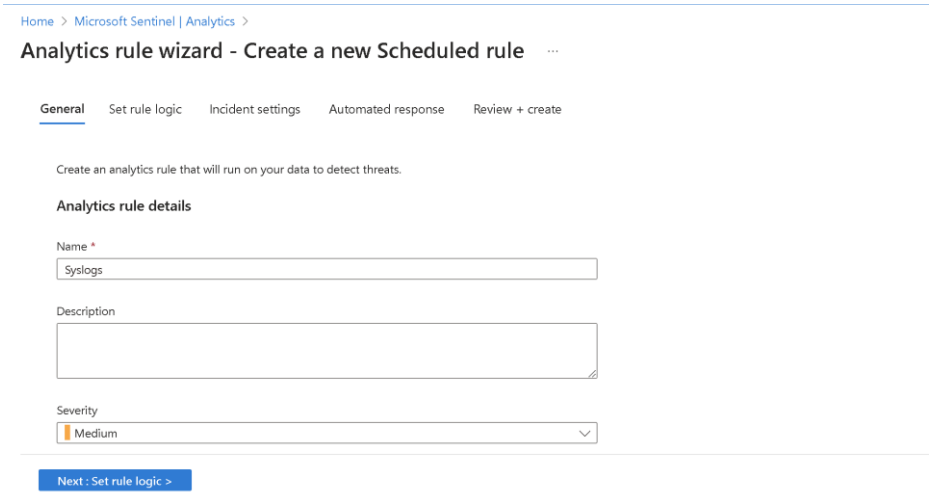


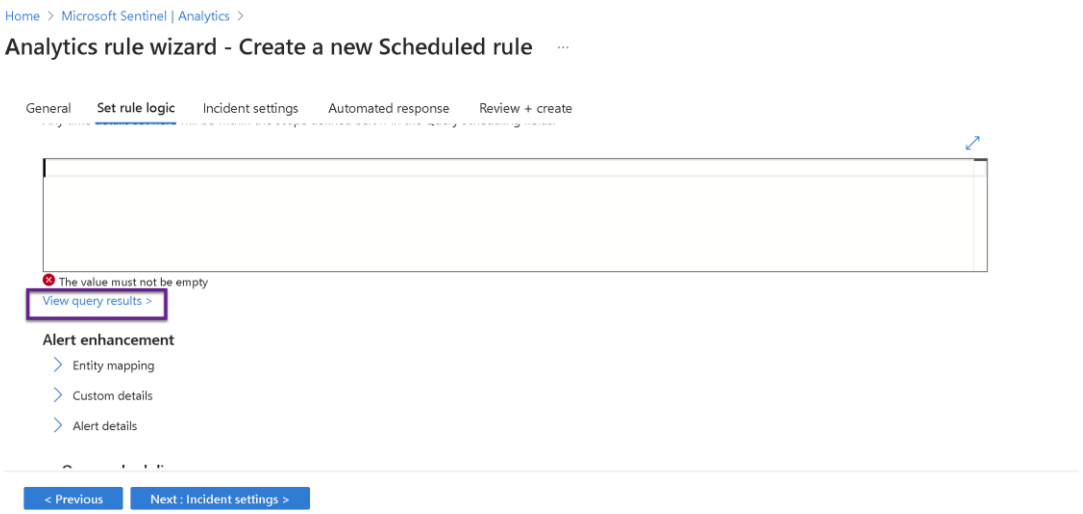

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ahmed_abdulwahed@o
AHMED TENA
Home > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'sentinelws'
Search
General
Overview
Logs
News & guides
Search
Threat management
Content management
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules (Preview)
Watchlist
New Query 1*
New Query 2*
Try the new Log Analytics
Feedback
Queries hub
SentinelWS
Run
Time range : Last 24 hours
Save
Share
New alert rule
Tables
Queries
Functions
Search
Filter
Group by: Category
Collapse all
Favorites
You can add favorites by clicking on the ☆ icon
Applications
CCF application errors
Error and exception count
Exceptions causing request failures
Failed operations
1 Heartbeat
2 | where Computer contains "vm1"
3 | sort by TimeGenerated desc
Results
Chart
Add bookmark
TimeGenerated [UTC]
SourceComputerId
ComputerIP
12/31/2024, 2:17:25.251 PM 0392ce6a-52b0-4350-96d1-835fe4d68ead 13.86.20.27
12/31/2024, 2:16:25.240 PM 0392ce6a-52b0-4350-96d1-835fe4d68ead 13.86.20.27
12/31/2024, 2:15:25.232 PM 0392ce6a-52b0-4350-96d1-835fe4d68ead 13.86.20.27
12/31/2024, 2:14:25.217 PM 0392ce6a-52b0-4350-96d1-835fe4d68ead 13.86.20.27
12/31/2024, 2:13:25.216 PM 0392ce6a-52b0-4350-96d1-835fe4d68ead 13.86.20.27

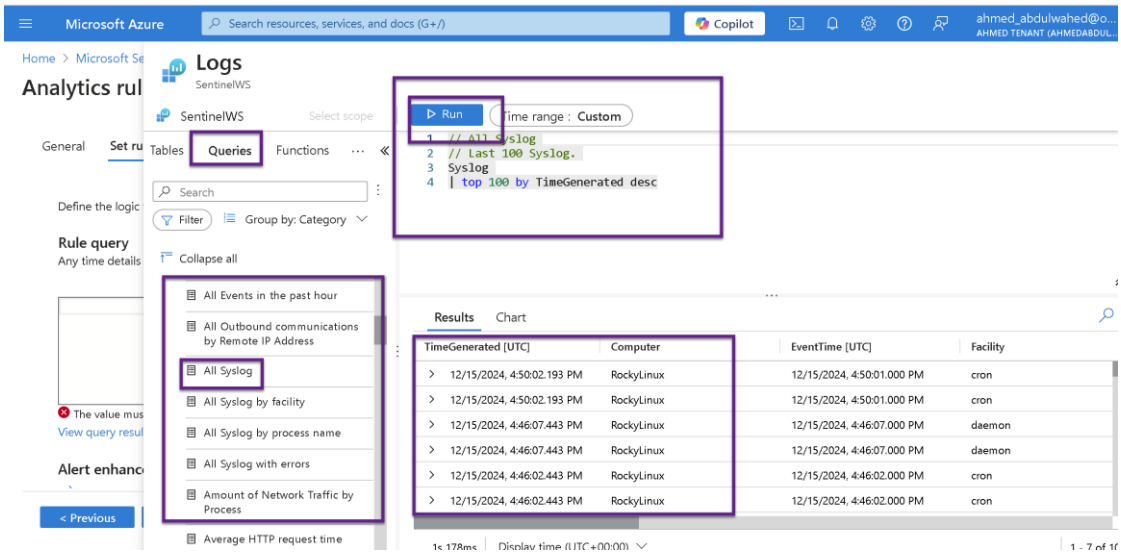
Queries and Analytics Rules in Microsoft Sentinel

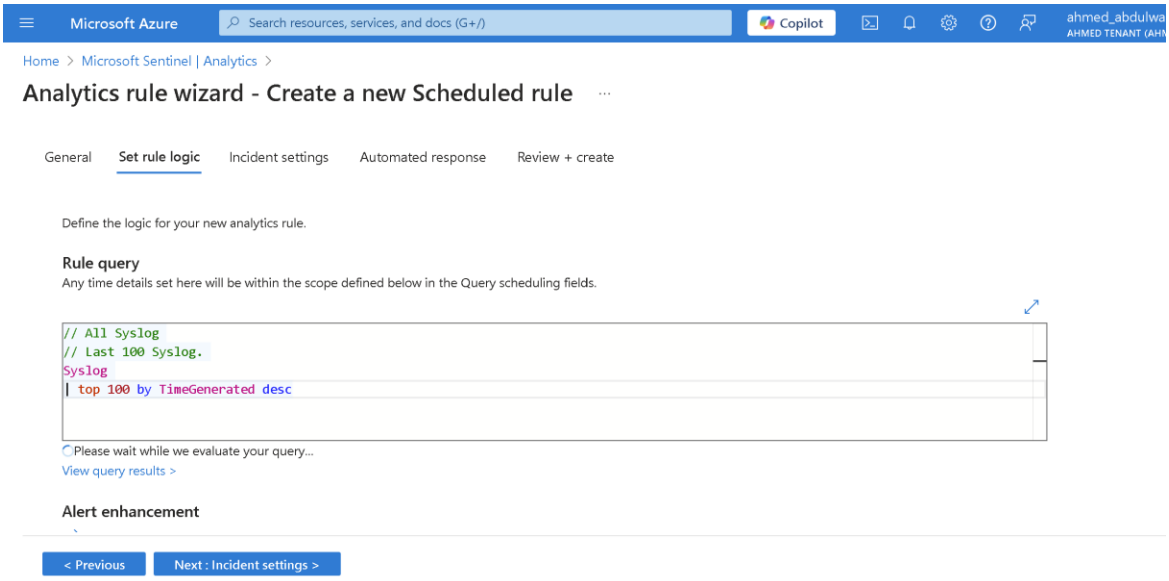
Microsoft Sentinel allows you to create and manage queries and analytics rules to detect, investigate, and respond to threats. These rules use **Kusto Query Language (KQL)** to analyze data from connected sources.

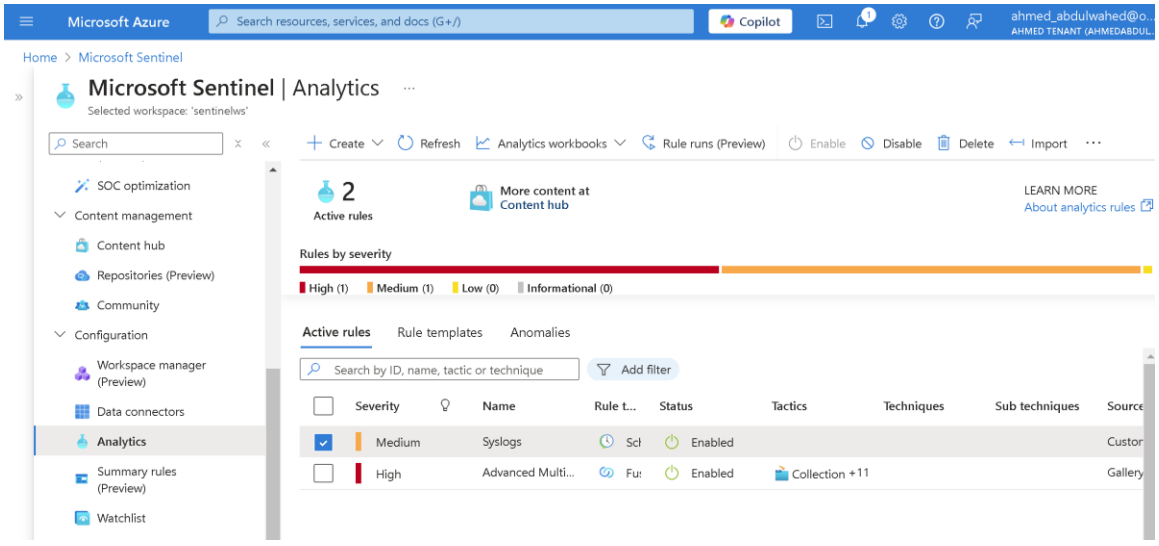




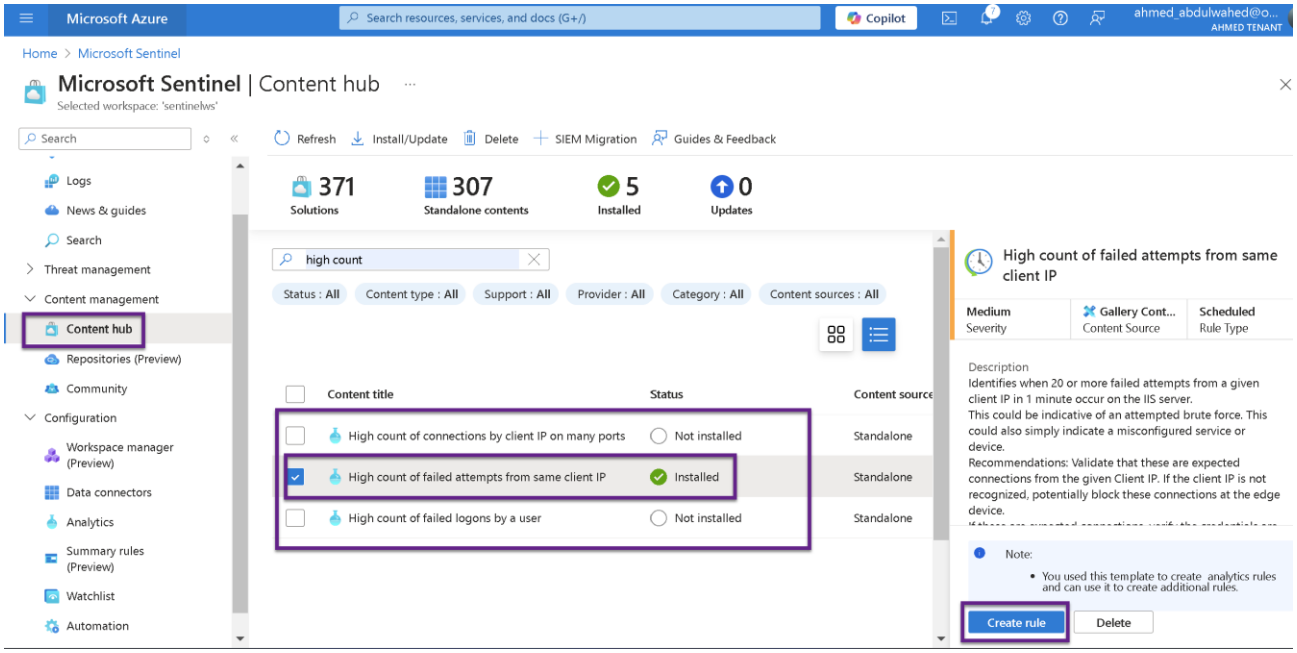


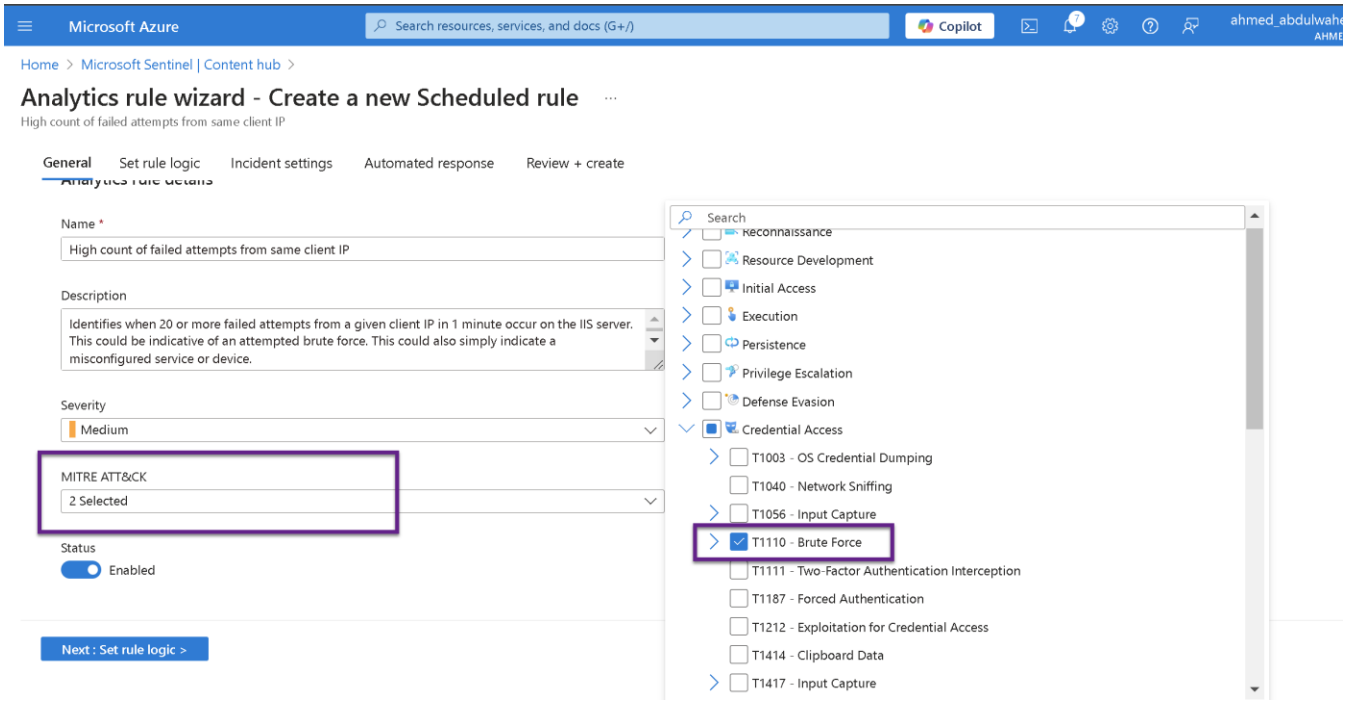

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Logs
SentinelWS
Run
Time range : Custom
// All Syslog
// Last 100 Syslog.
Syslog
| top 100 by TimeGenerated desc
Tables
Queries
Functions
Search
Filter
Group by: Category
Collapse all
All Events in the past hour
All Outbound communications by Remote IP Address
All Syslog
All Syslog by facility
All Syslog by process name
All Syslog with errors
Amount of Network Traffic by Process
Average HTTP request time
Results
Chart
TimeGenerated [UTC]
Computer
EventTime [UTC]
Facility
12/15/2024, 4:50:02.193 PM RockyLinux 12/15/2024, 4:50:01.000 PM cron
12/15/2024, 4:50:02.193 PM RockyLinux 12/15/2024, 4:50:01.000 PM cron
12/15/2024, 4:46:07.443 PM RockyLinux 12/15/2024, 4:46:07.000 PM daemon
12/15/2024, 4:46:07.443 PM RockyLinux 12/15/2024, 4:46:07.000 PM daemon
12/15/2024, 4:46:02.443 PM RockyLinux 12/15/2024, 4:46:02.000 PM cron
12/15/2024, 4:46:02.443 PM RockyLinux 12/15/2024, 4:46:02.000 PM cron
Define the logic
Rule query
Any time details
Alert enhanc
< Previous


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel | Analytics >
Analytics rule wizard - Create a new Scheduled rule
General
Set rule logic
Incident settings
Automated response
Review + create
Define the logic for your new analytics rule.
Rule query
Any time details set here will be within the scope defined below in the Query scheduling fields.
// All Syslog
// Last 100 Syslog.
Syslog
| top 100 by TimeGenerated desc
Please wait while we evaluate your query...
View query results >
Alert enhancement
< Previous
Next : Incident settings >


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel
Microsoft Sentinel | Analytics
Selected workspace: 'sentinelws'
Search
SOC optimization
Content management
Content hub
Repositories (Preview)
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules (Preview)
Watchlist
Create
Refresh
Analytics workbooks
Rule runs (Preview)
Enable
Disable
Delete
Import
2
Active rules
More content at Content hub
LEARN MORE
About analytics rules
Rules by severity
High (1)
Medium (1)
Low (0)
Informational (0)
Active rules
Rule templates
Anomalies
Search by ID, name, tactic or technique
Add filter
Severity
Name
Rule t...
Status
Tactics
Techniques
Sub techniques
Source
Medium Syslogs Scl Enabled
High Advanced Multi... Fu: Enabled Collection +11 Gallery

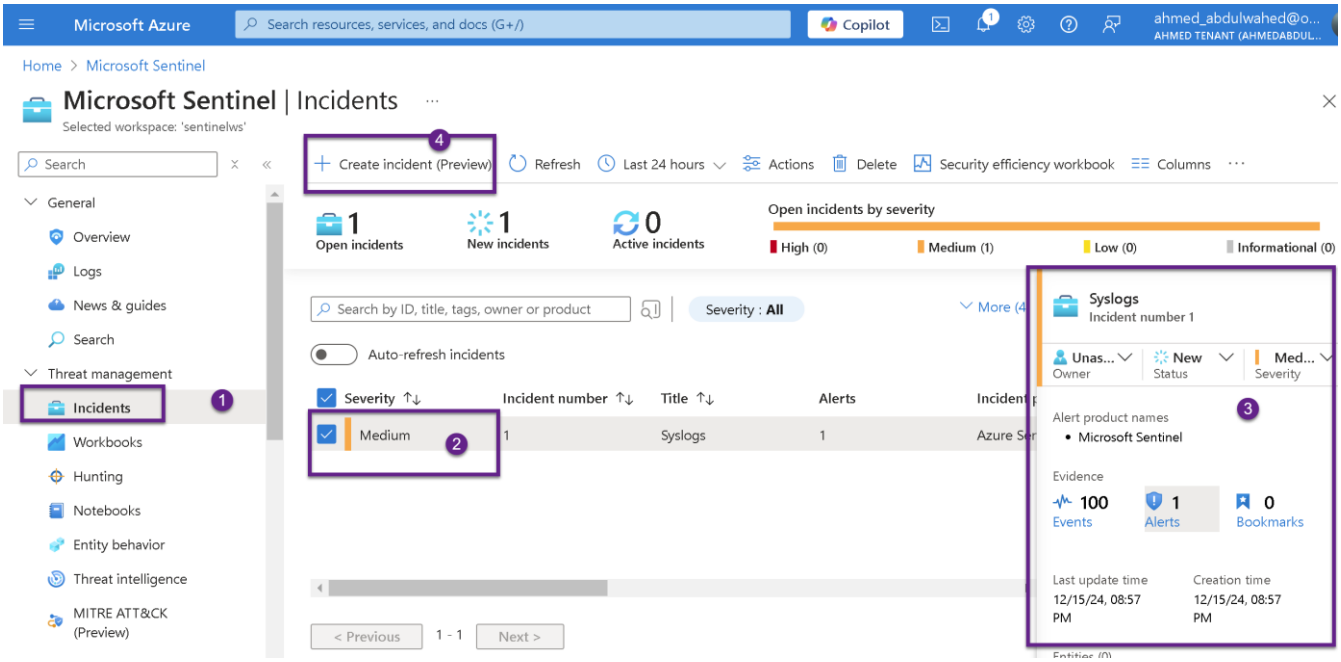
Create a new Scheduled rule through Content hub

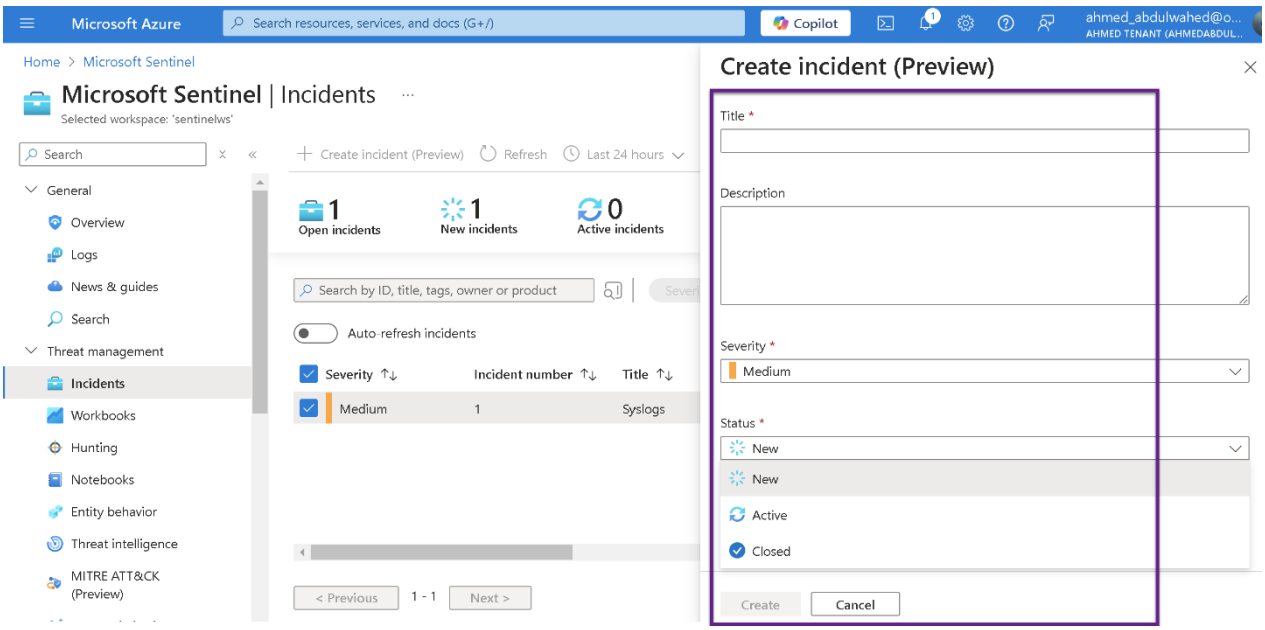




Incident

Microsoft Sentinel provides a powerful platform for monitoring and managing security incidents in an organization. Incidents in Microsoft Sentinel represent groups of related alerts that indicate potential security threats. Here's an overview of how incidents are handled in Microsoft Sentinel:



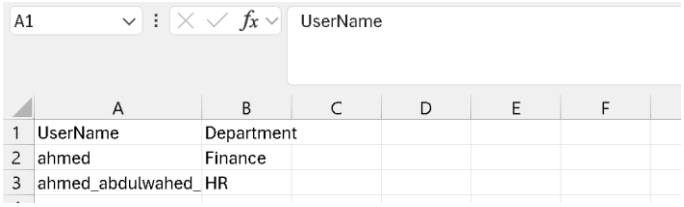


Watchlists

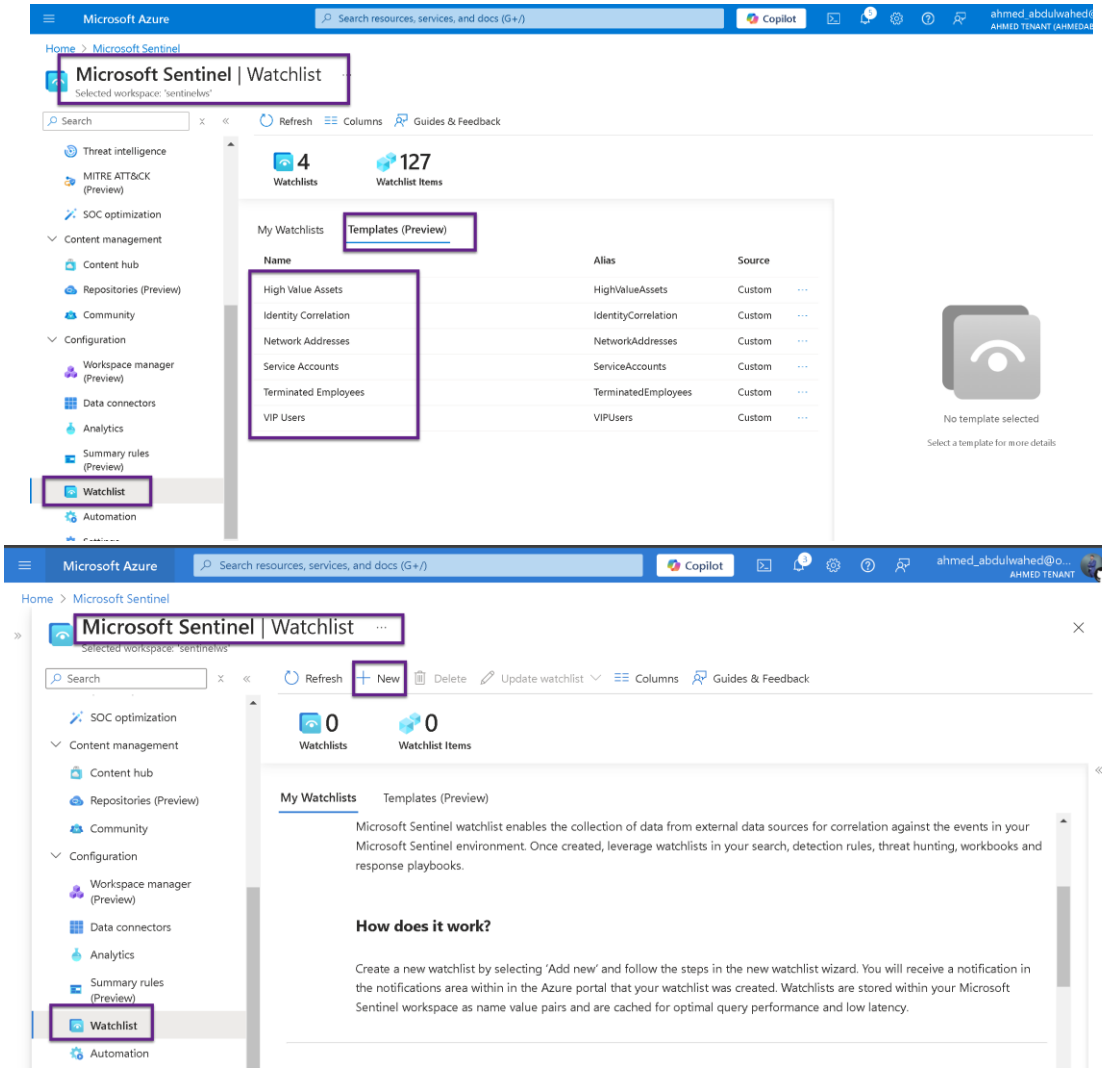
- Watchlists are lists of data (e.g., IP addresses, usernames, domains, etc.) that are imported into Sentinel to enhance analytics, investigations, and threat detection.
- They allow for the integration of custom or external data to improve threat detection and response workflows.

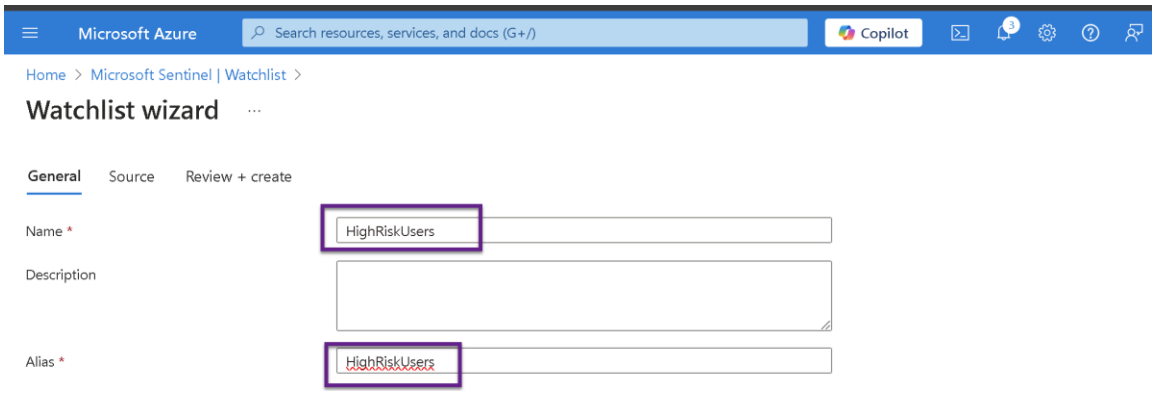
Step 1: Create a Watchlist for RiskyUsers

1. **Prepare a Watchlist File**:
   - Create a CSV file named HighRiskUsers.csv with the following structure:

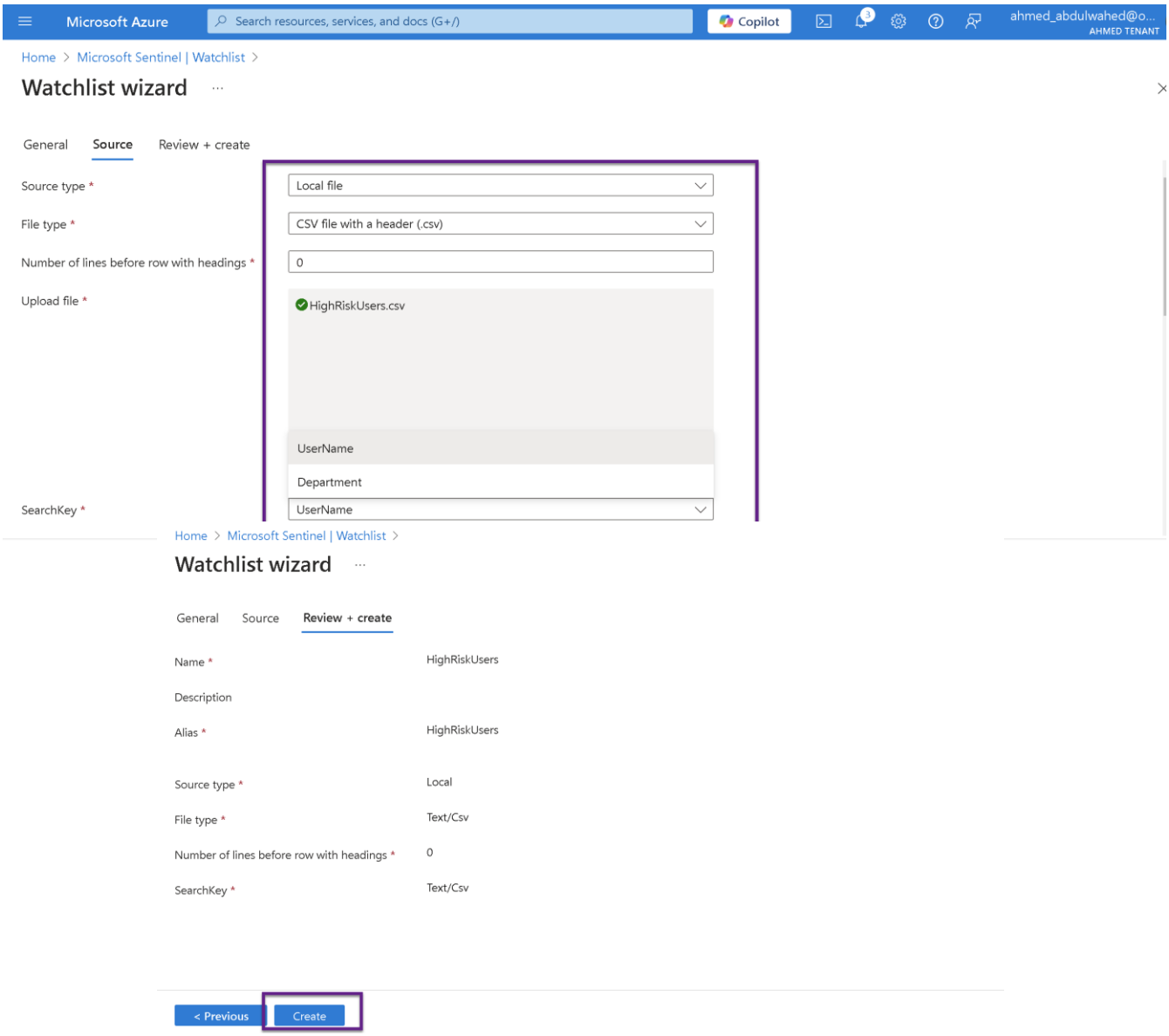


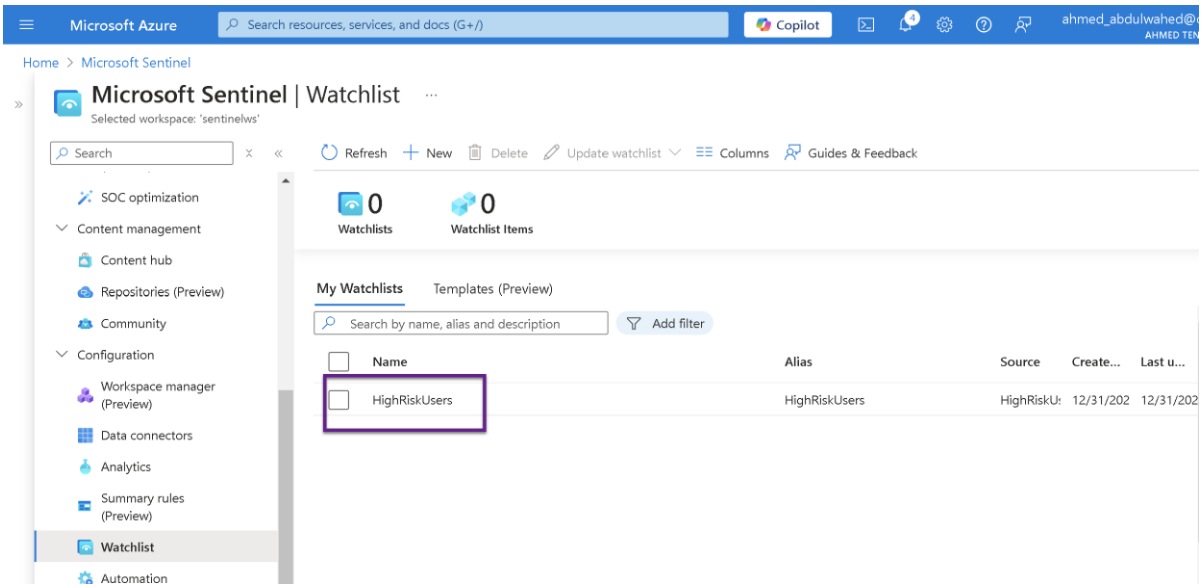
2. **Upload the Watchlist to Sentinel**:
   - Go to **Microsoft Sentinel > Configuration > Watchlist**.
   - Click **Add new**.





- Upload the HighRiskUsers.csv file.
- Save the Watchlist.





Step 2: Query the Watchlist

Use KQL to query login events for users in the Watchlist.

Query:

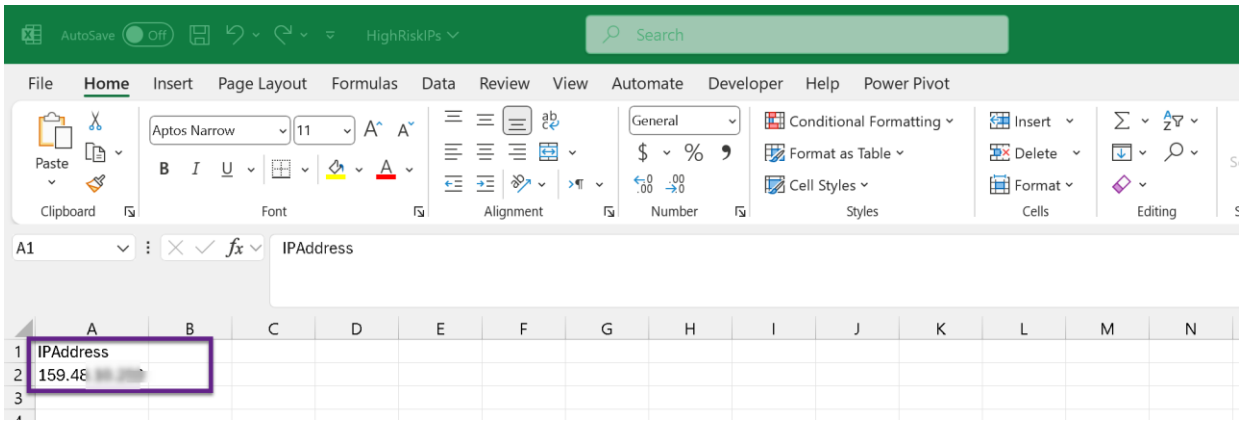
```
let HighRiskUsers = _GetWatchlist('HighRiskUsers');
SecurityEvent
| where EventID == 4624  // Filter for successful logins
| where AccountName in (HighRiskUsers)
| project TimeGenerated, AccountName, Computer, IpAddress
```

Explanation:

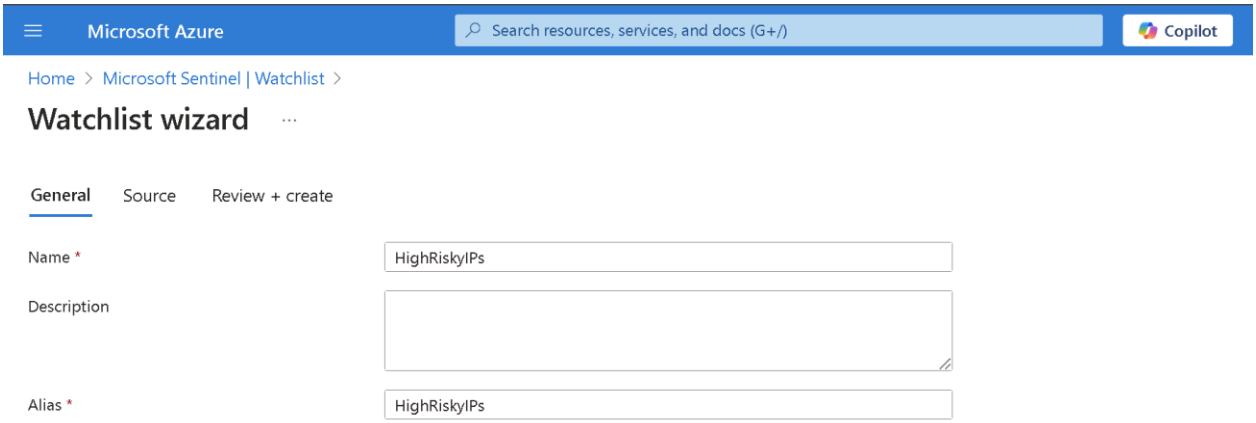
- _GetWatchlist('HighRiskUsers'): Loads the HighRiskUsers Watchlist.
- EventID == 4624: Filters only successful logins.
- AccountName in (HighRiskUsers): Matches login events with Watchlist users.

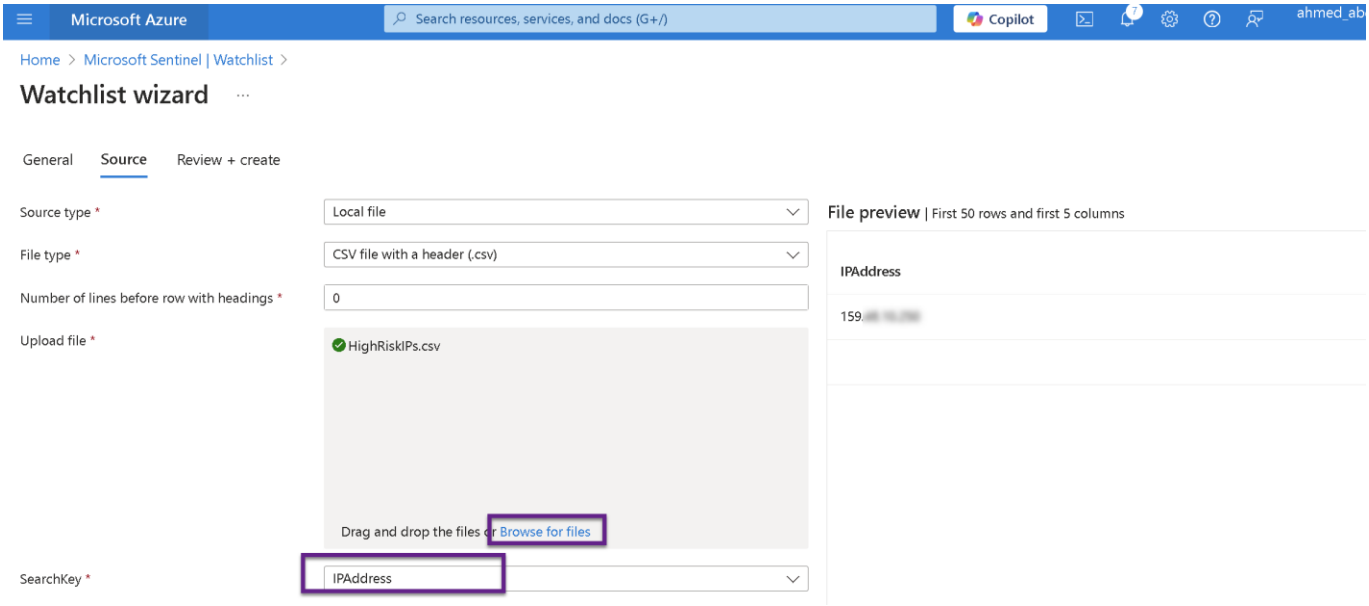
Create a Watchlist for High Risky IPs

1. **Prepare a Watchlist File**:



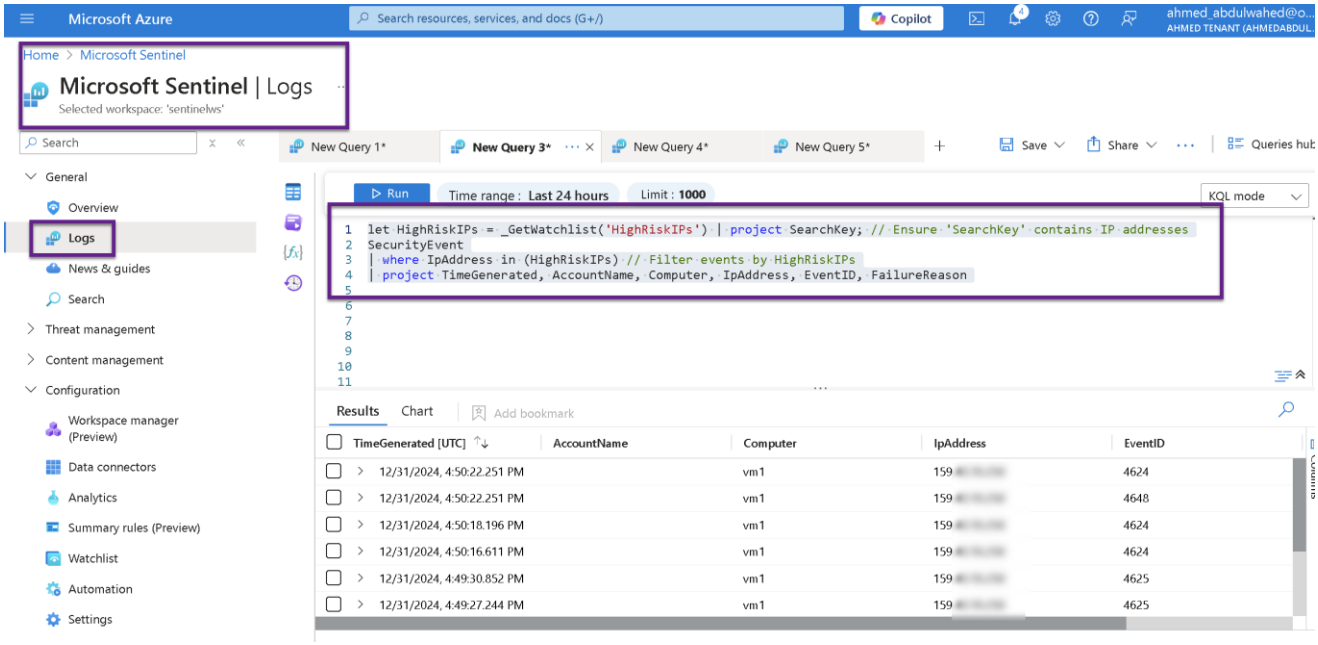
Upload the Watchlist to Sentinel:





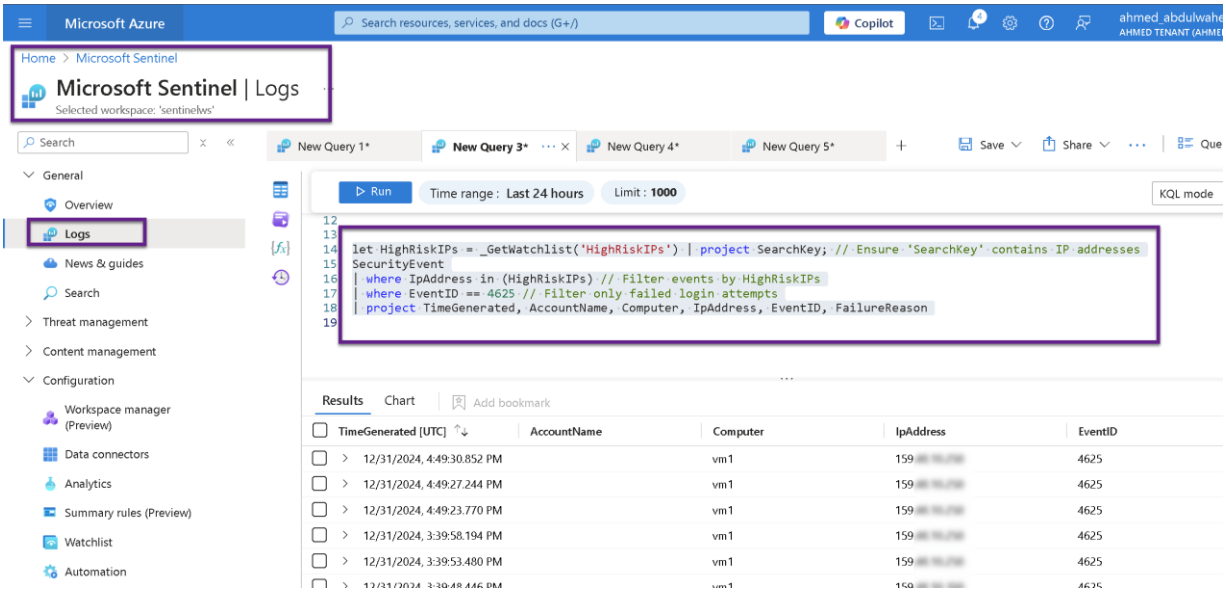
Query the Watchlist

```
let HighRiskIPs = _GetWatchlist('HighRiskIPs') | project SearchKey; // Ensure 'SearchKey' contains IP addresses
SecurityEvent
| where IpAddress in (HighRiskIPs) // Filter events by HighRiskIPs
| project TimeGenerated, AccountName, Computer, IpAddress, EventID, FailureReason
```



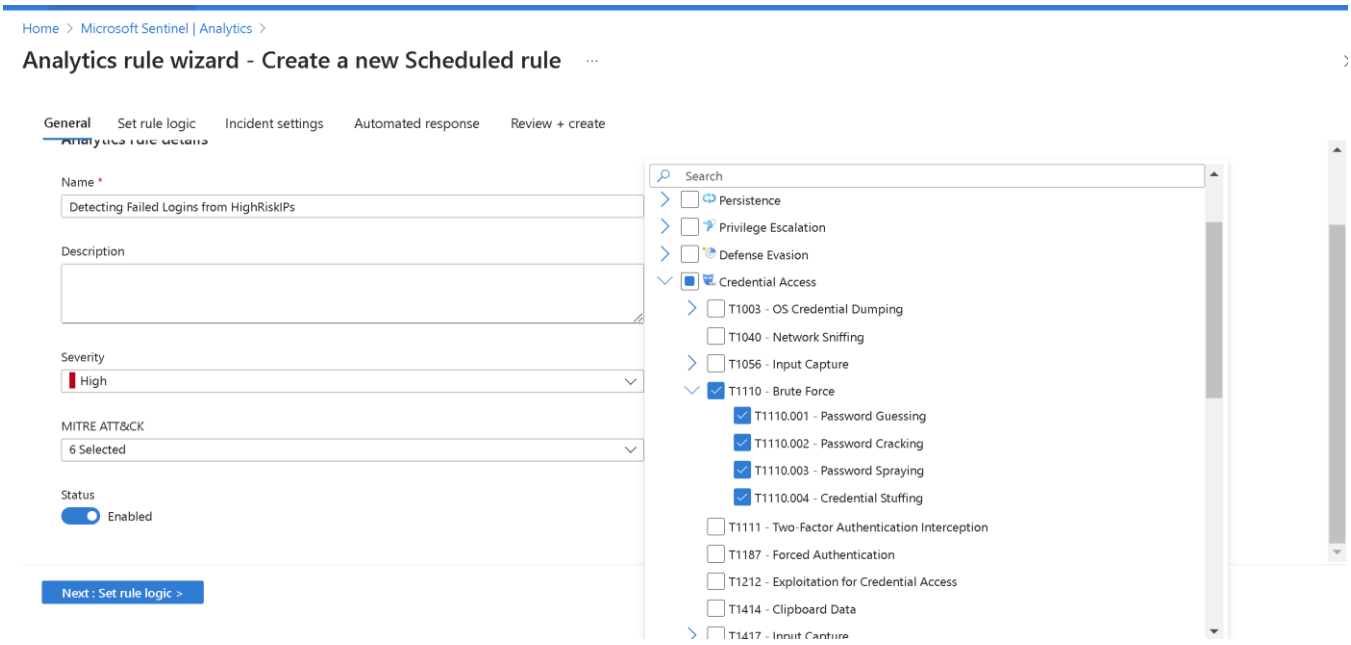
Filter only by failed retries

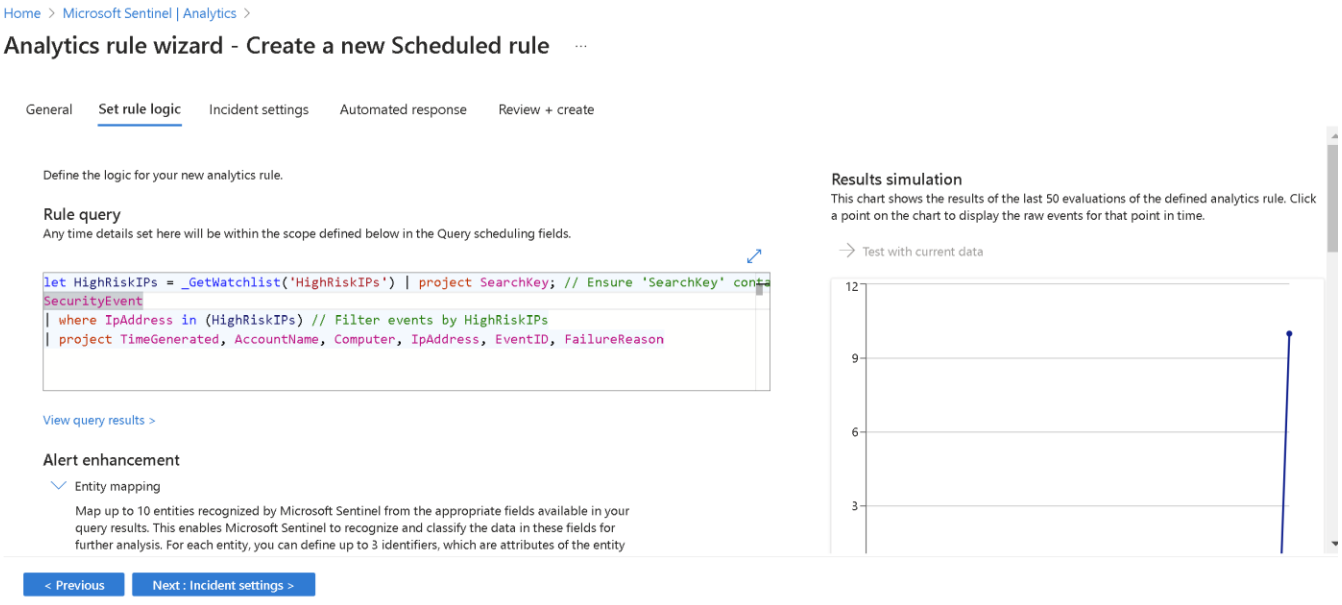
```
let HighRiskIPs = _GetWatchlist('HighRiskIPs') | project SearchKey; // Ensure 'SearchKey' contains IP addresses
SecurityEvent
| where IpAddress in (HighRiskIPs) // Filter events by HighRiskIPs
| where EventID == 4625 // Filter only failed login attempts
| project TimeGenerated, AccountName, Computer, IpAddress, EventID, FailureReason
```

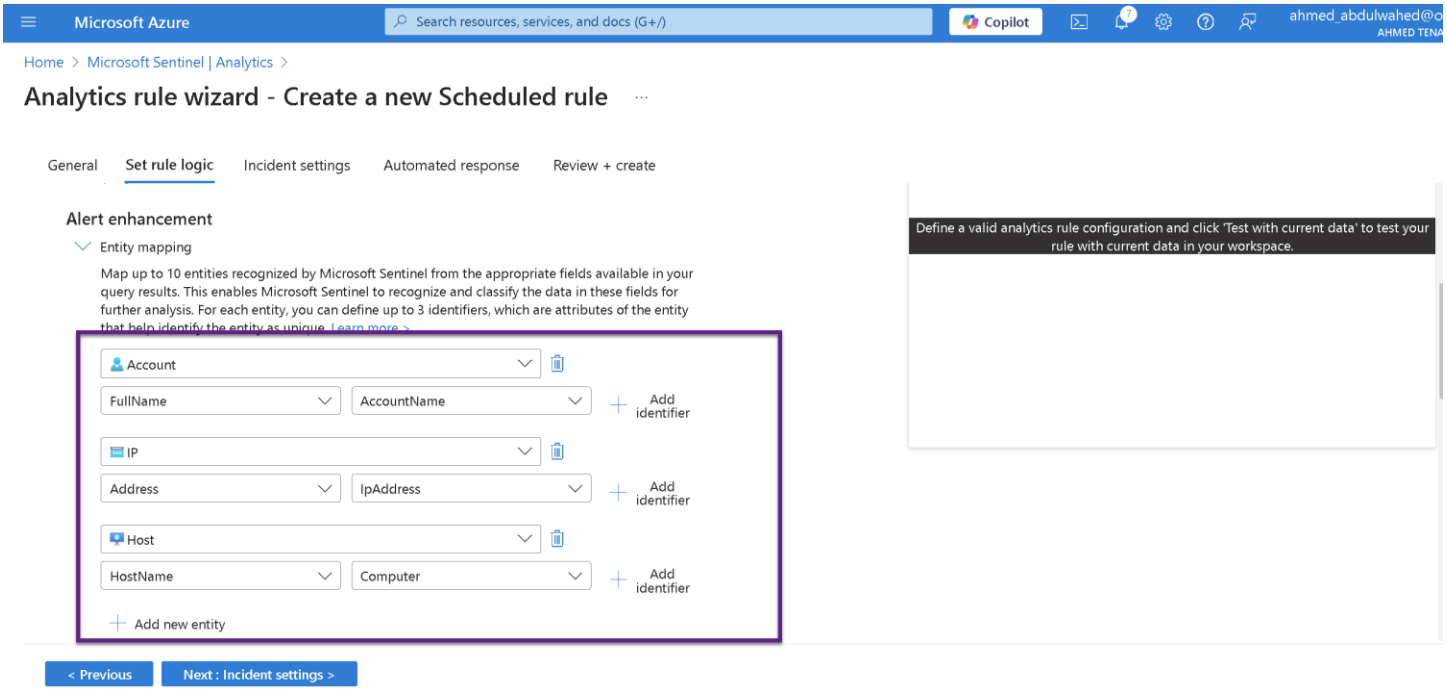


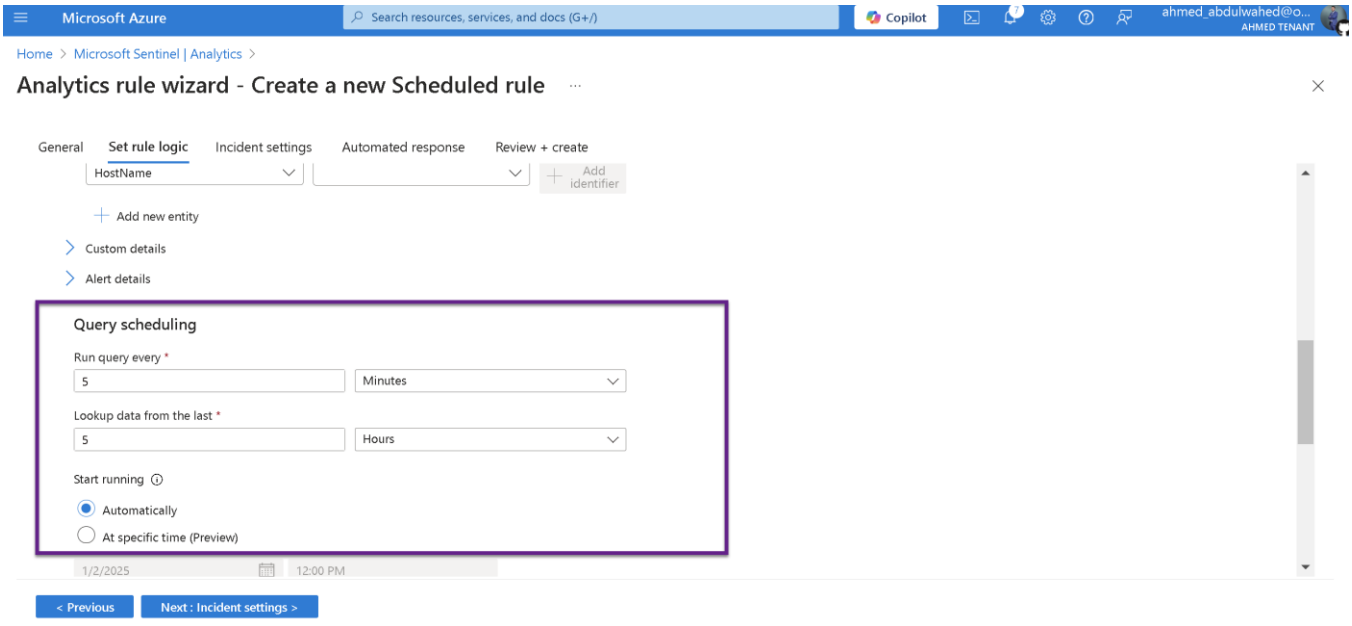
Entities in Sentinel

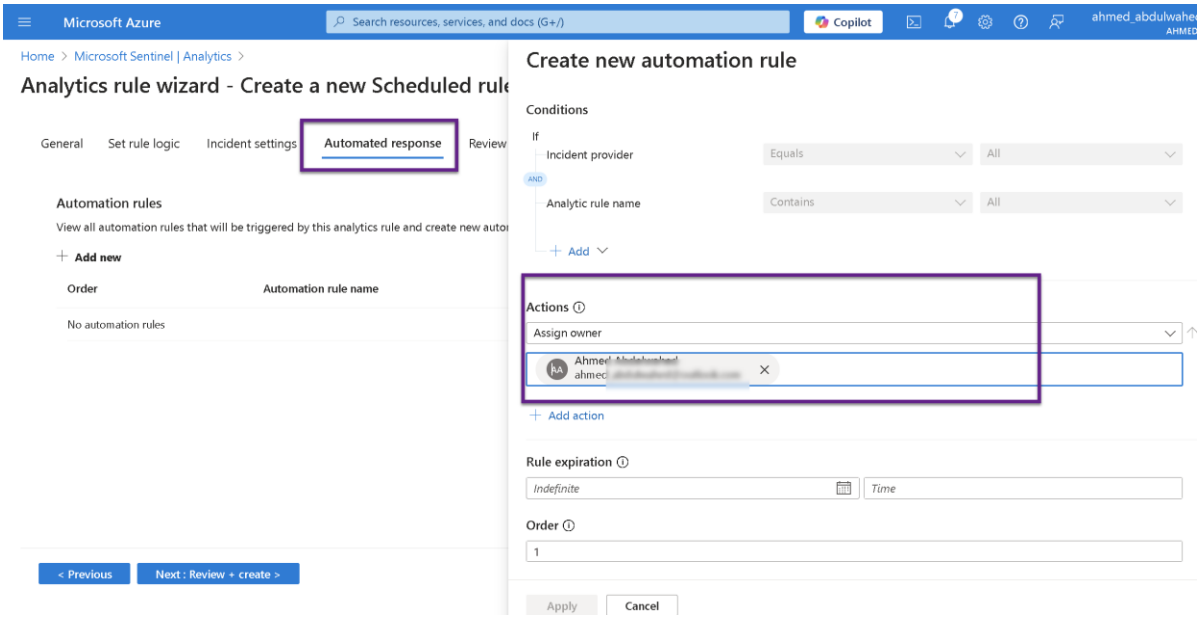
In Microsoft Sentinel, **entities** are specific pieces of information extracted from logs or events that can represent users, IP addresses, hosts, files, processes, and more. These entities are often used to correlate data, investigate incidents, and enrich alerts.

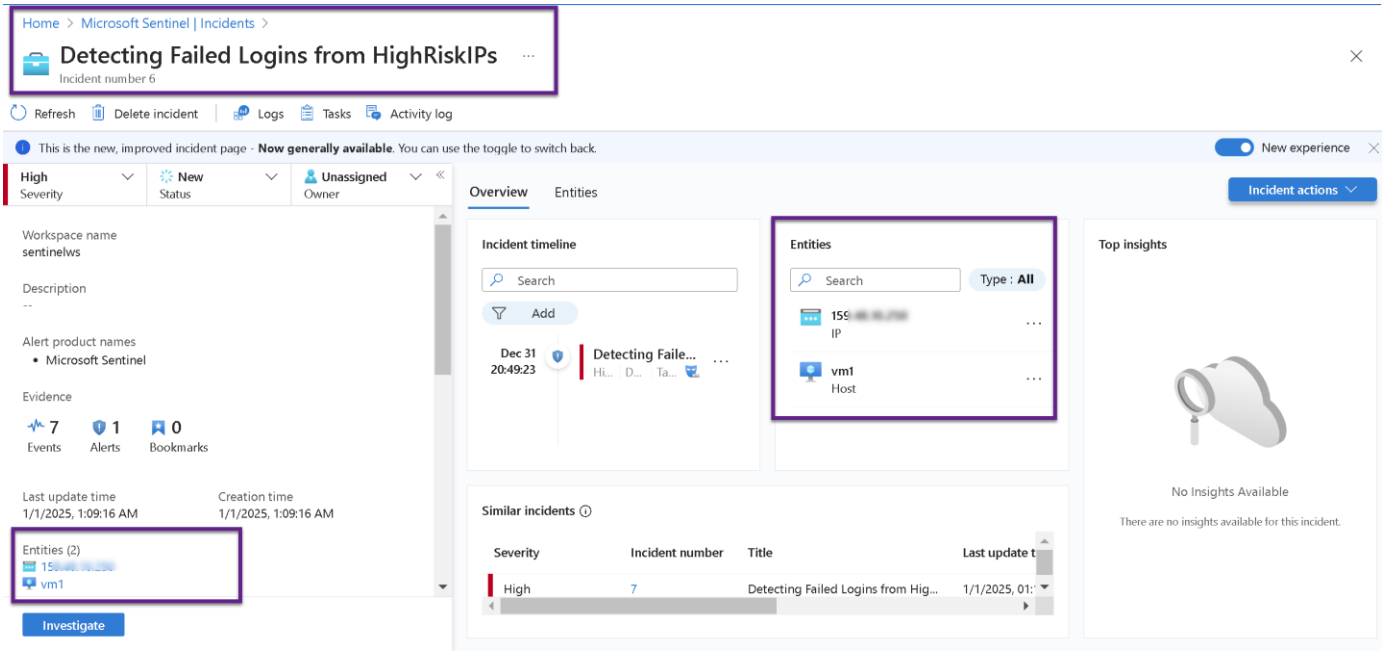





Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ahmed_abdulwahed@o
AHMED TENA
Home > Microsoft Sentinel | Analytics >
Analytics rule wizard - Create a new Scheduled rule
General
Set rule logic
Incident settings
Automated response
Review + create
Alert enhancement
Entity mapping
Map up to 10 entities recognized by Microsoft Sentinel from the appropriate fields available in your query results. This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis. For each entity, you can define up to 3 identifiers, which are attributes of the entity that help identify the entity as unique. Learn more >
Account
FullName
AccountName
Add identifier
IP
Address
IpAddress
Add identifier
Host
HostName
Computer
Add identifier
Add new entity
Define a valid analytics rule configuration and click 'Test with current data' to test your rule with current data in your workspace.
< Previous
Next : Incident settings >


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ahmed_abdulwahed@o...
AHMED TENANT
Home > Microsoft Sentinel | Analytics >
Analytics rule wizard - Create a new Scheduled rule
General
Set rule logic
Incident settings
Automated response
Review + create
HostName
Add identifier
Add new entity
Custom details
Alert details
Query scheduling
Run query every *
5
Minutes
Lookup data from the last *
5
Hours
Start running
Automatically
At specific time (Preview)
1/2/2025
12:00 PM
< Previous
Next : Incident settings >


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel | Analytics >
Analytics rule wizard - Create a new Scheduled rule
General
Set rule logic
Incident settings
Automated response
Review
Automation rules
View all automation rules that will be triggered by this analytics rule and create new auto
Add new
Order
Automation rule name
No automation rules
< Previous
Next : Review + create >
Create new automation rule
Conditions
If
Incident provider
Equals
All
AND
Analytic rule name
Contains
All
Add
Actions
Assign owner
Add action
Rule expiration
Indefinite
Time
Order
1
Apply
Cancel

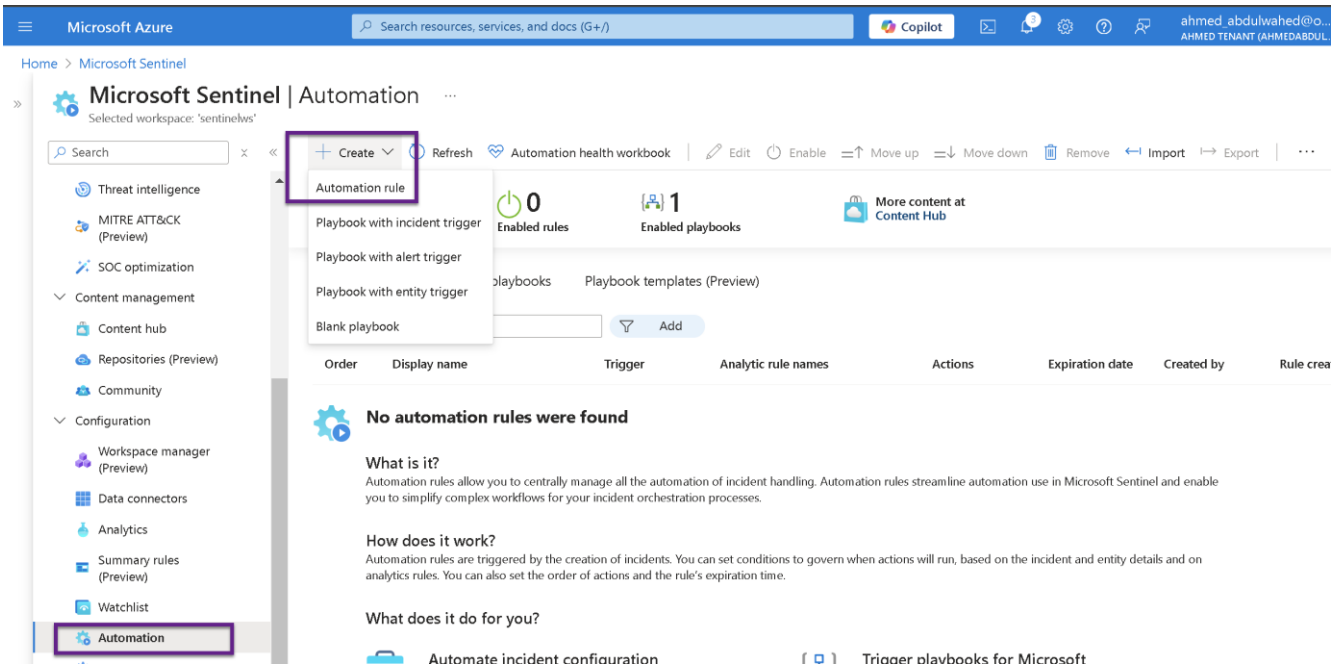

Home > Microsoft Sentinel | Incidents >
Detecting Failed Logins from HighRiskIPs
Incident number 6
Refresh
Delete incident
Logs
Tasks
Activity log
This is the new, improved incident page - Now generally available. You can use the toggle to switch back.
New experience
High
Severity
New
Status
Unassigned
Owner
Overview
Entities
Incident actions
Workspace name
sentinelws
Description
--
Alert product names
Microsoft Sentinel
Evidence
7
Events
1
Alerts
0
Bookmarks
Last update time
1/1/2025, 1:09:16 AM
Creation time
1/1/2025, 1:09:16 AM
Entities (2)
vm1
Investigate
Incident timeline
Search
Add
Dec 31
20:49:23
Detecting Faile...
Entities
Search
Type : All
IP
vm1
Host
Top insights
No Insights Available
There are no insights available for this incident.
Similar incidents
Severity
Incident number
Title
Last update t
High
7
Detecting Failed Logins from Hig...
1/1/2025, 01:

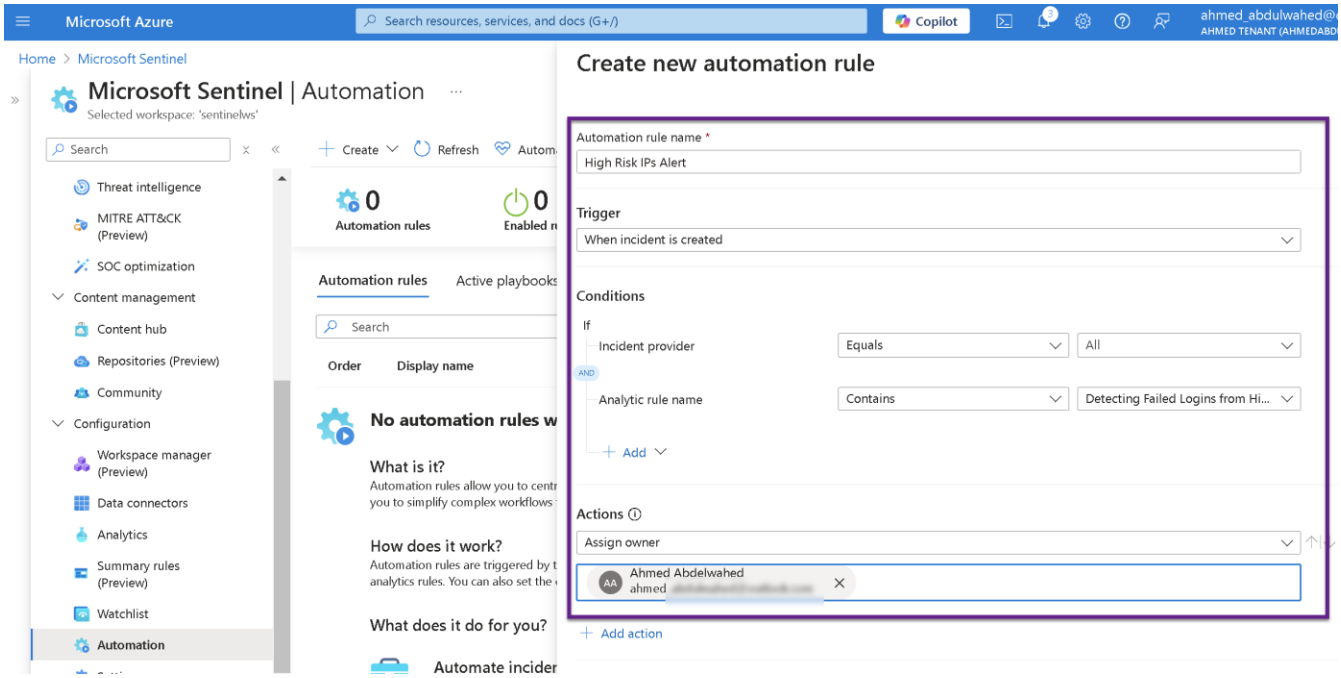
Automation Rules

Automation Rules in Microsoft Sentinel allow you to streamline incident response by automating routine tasks based on predefined conditions. They are a powerful way to orchestrate workflows and ensure faster response times to security events.

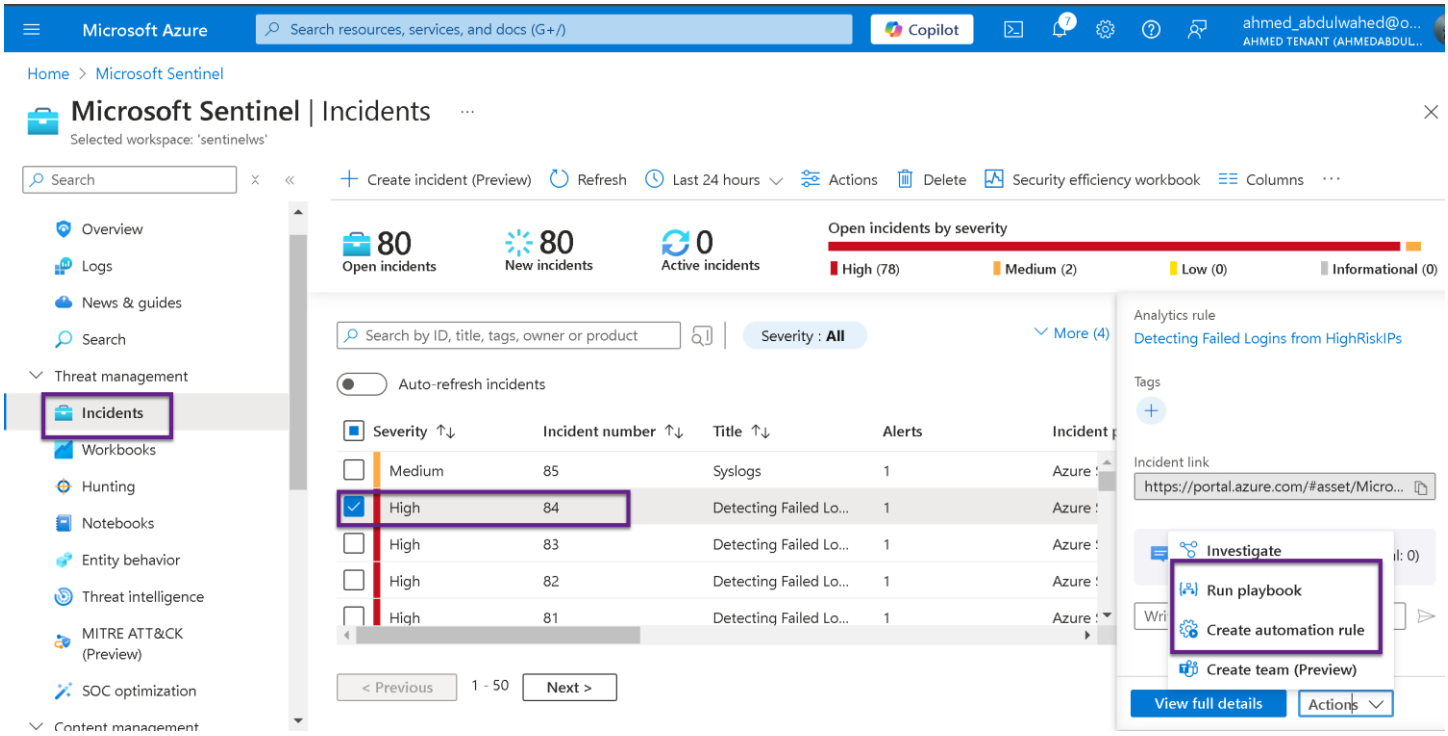
Example: Automation Rule for High-Risk IPs

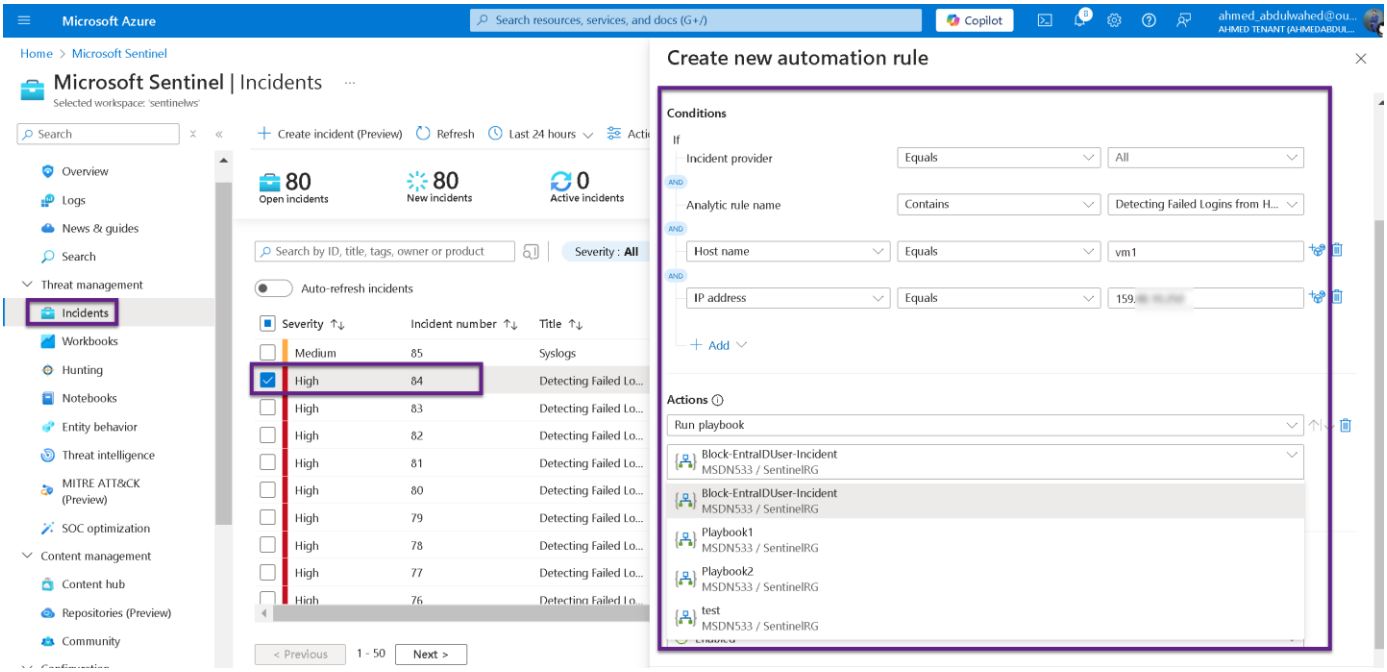
Automatically assign incidents with high-risk IP addresses to the security team and notify via email.



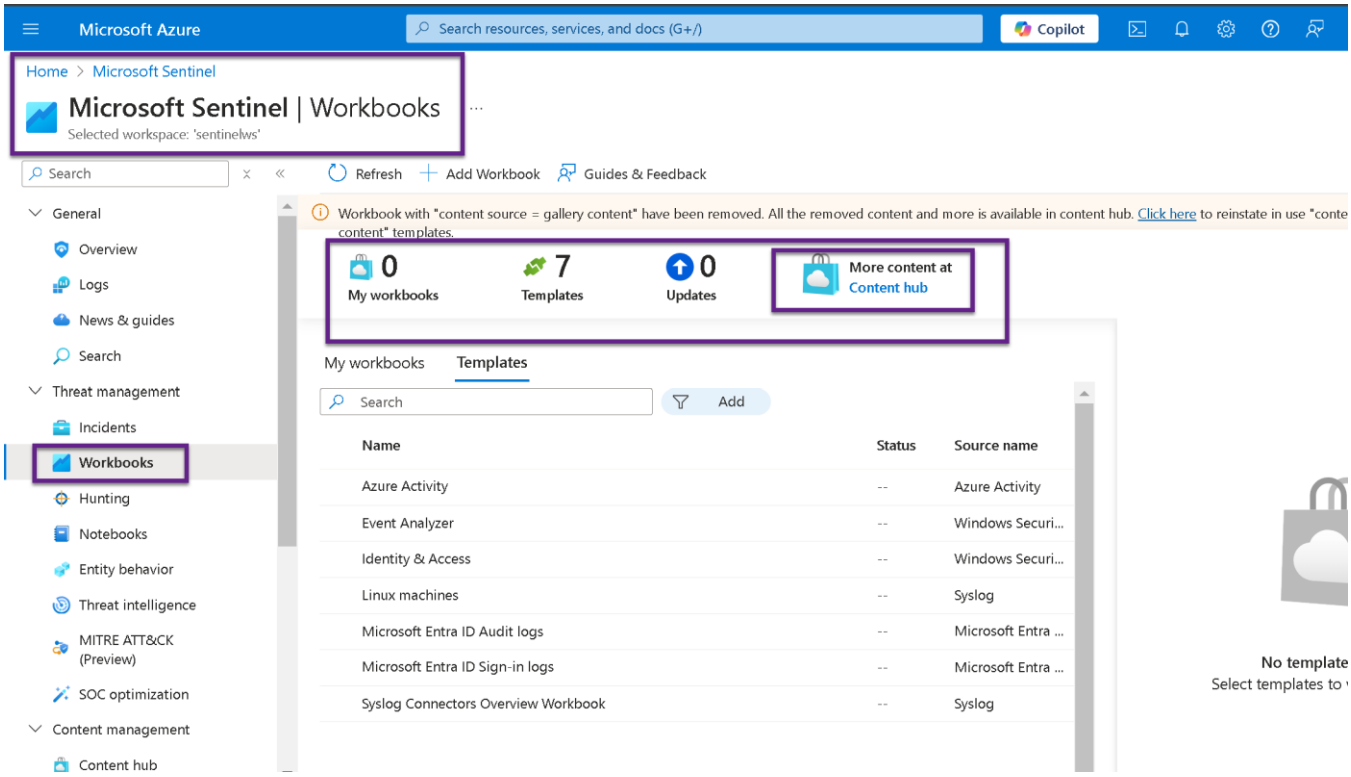


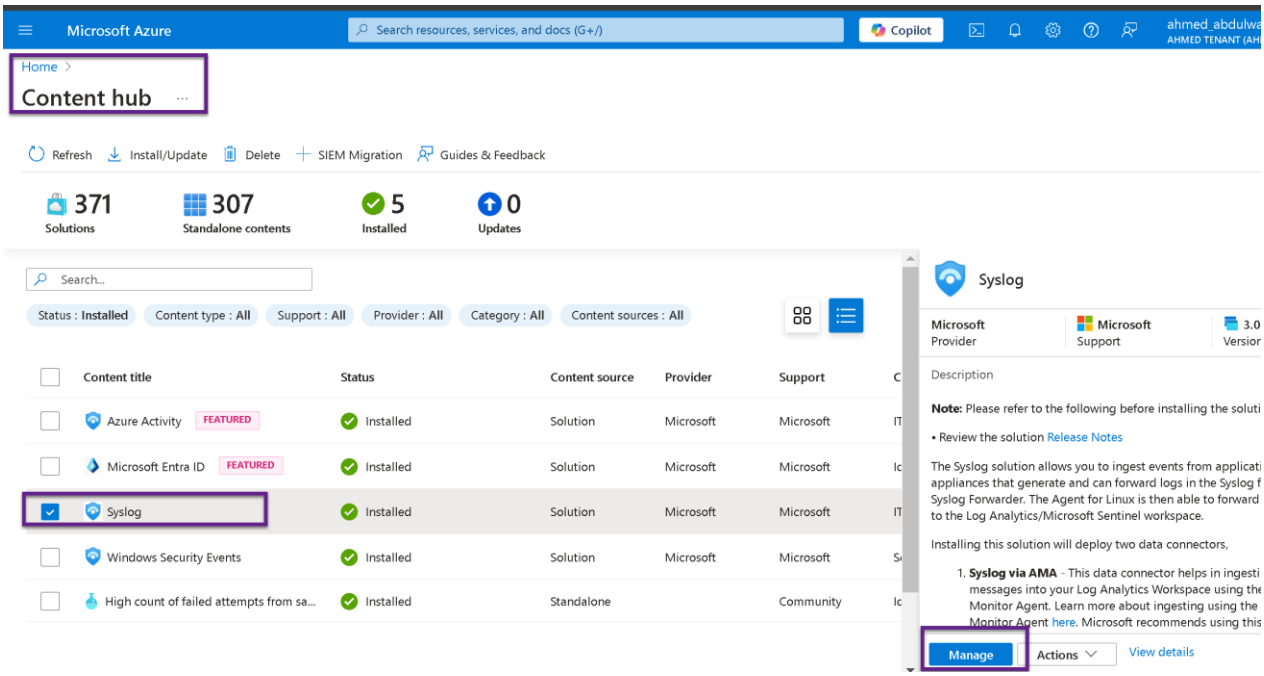
Create Automation rule from incident

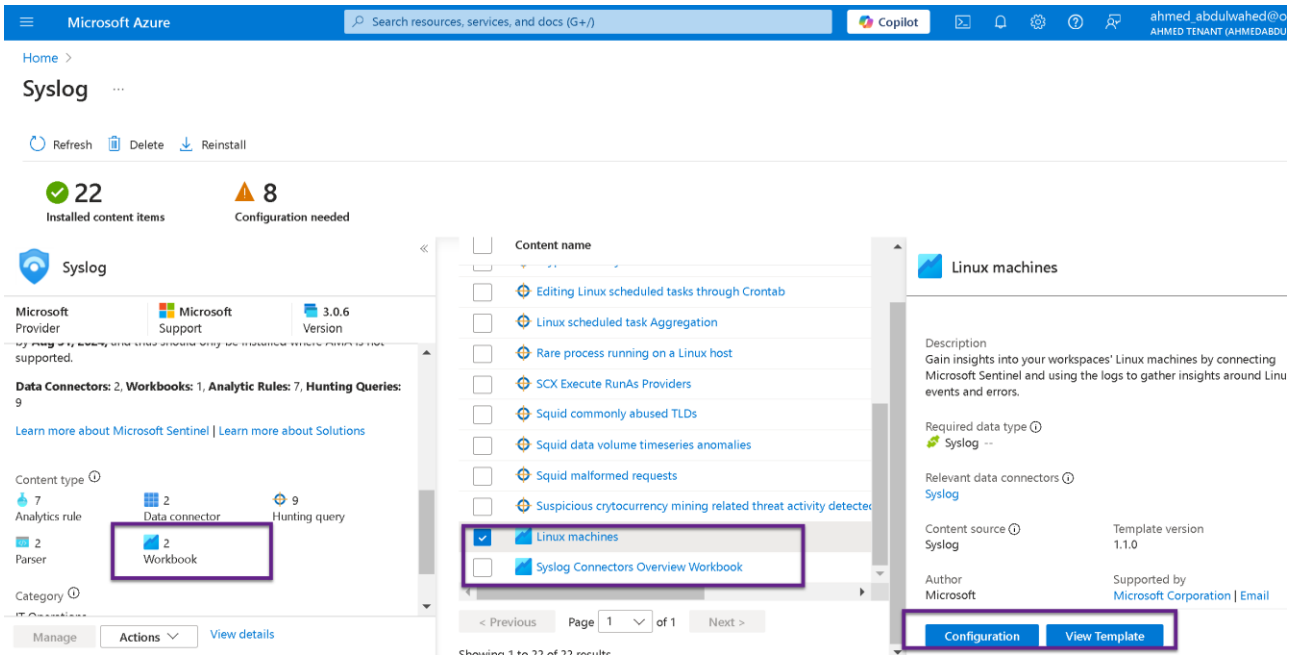


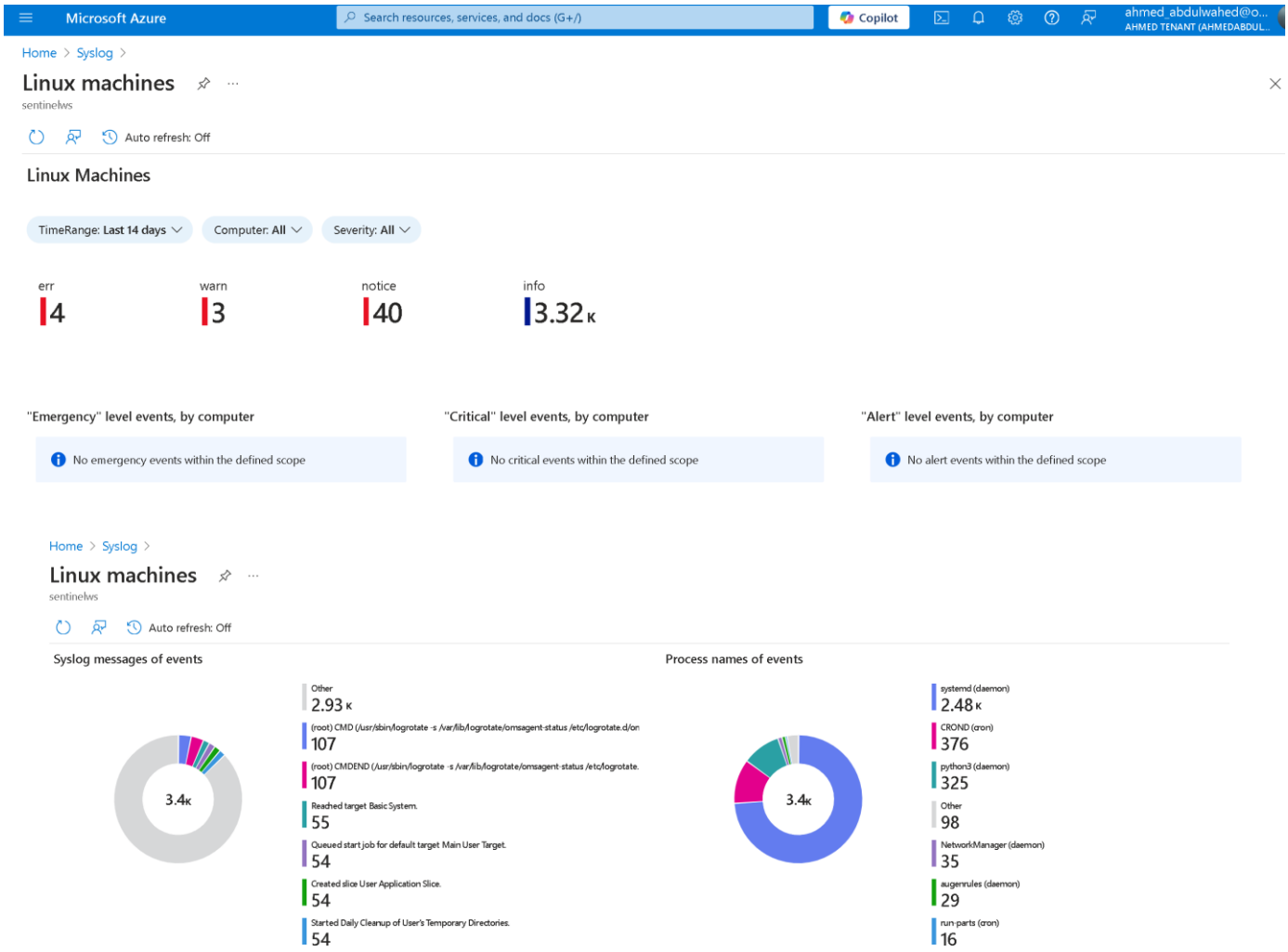


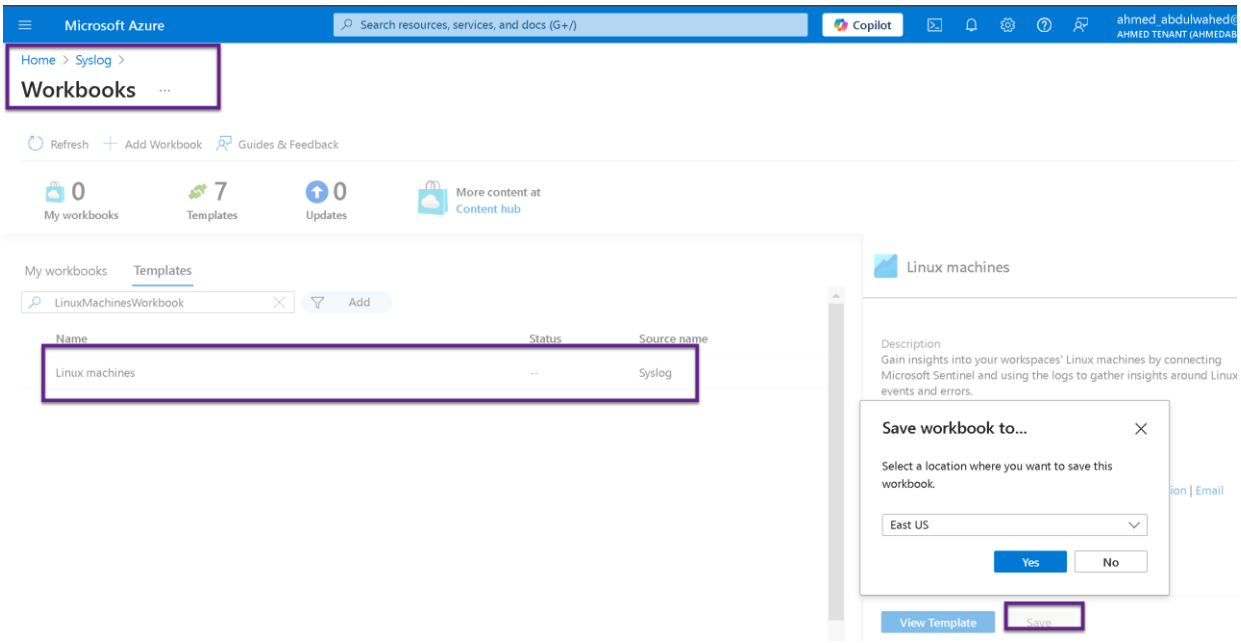
Microsoft Sentinel Workbooks are customizable dashboards that provide a powerful way to visualize and analyze your security data. They enable security teams to monitor and investigate security incidents, trends, and data patterns interactively.

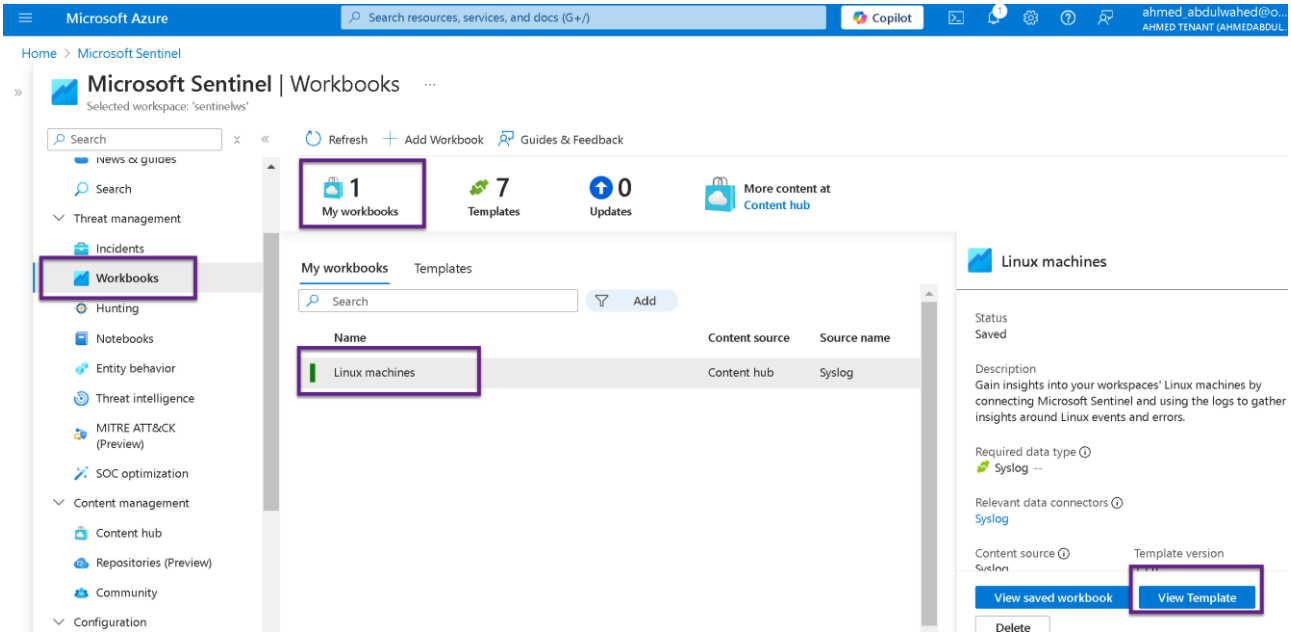





Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home
Syslog
Refresh
Delete
Reinstall
22
Installed content items
8
Configuration needed
Syslog
Microsoft
Provider
Microsoft
Support
3.0.6
Version
Data Connectors: 2, Workbooks: 1, Analytic Rules: 7, Hunting Queries: 9
Learn more about Microsoft Sentinel | Learn more about Solutions
Content type
7
Analytics rule
2
Data connector
9
Hunting query
2
Parser
2
Workbook
Category
Manage
Actions
View details
Content name
Editing Linux scheduled tasks through Crontab
Linux scheduled task Aggregation
Rare process running on a Linux host
SCX Execute RunAs Providers
Squid commonly abused TLDs
Squid data volume timeseries anomalies
Squid malformed requests
Suspicious crytocurrency mining related threat activity detecte
Linux machines
Syslog Connectors Overview Workbook
< Previous
Page 1 of 1
Next >
Linux machines
Description
Gain insights into your workspaces' Linux machines by connecting Microsoft Sentinel and using the logs to gather insights around Linu events and errors.
Required data type
Syslog
Relevant data connectors
Syslog
Content source
Syslog
Template version
1.1.0
Author
Microsoft
Supported by
Microsoft Corporation | Email
Configuration
View Template

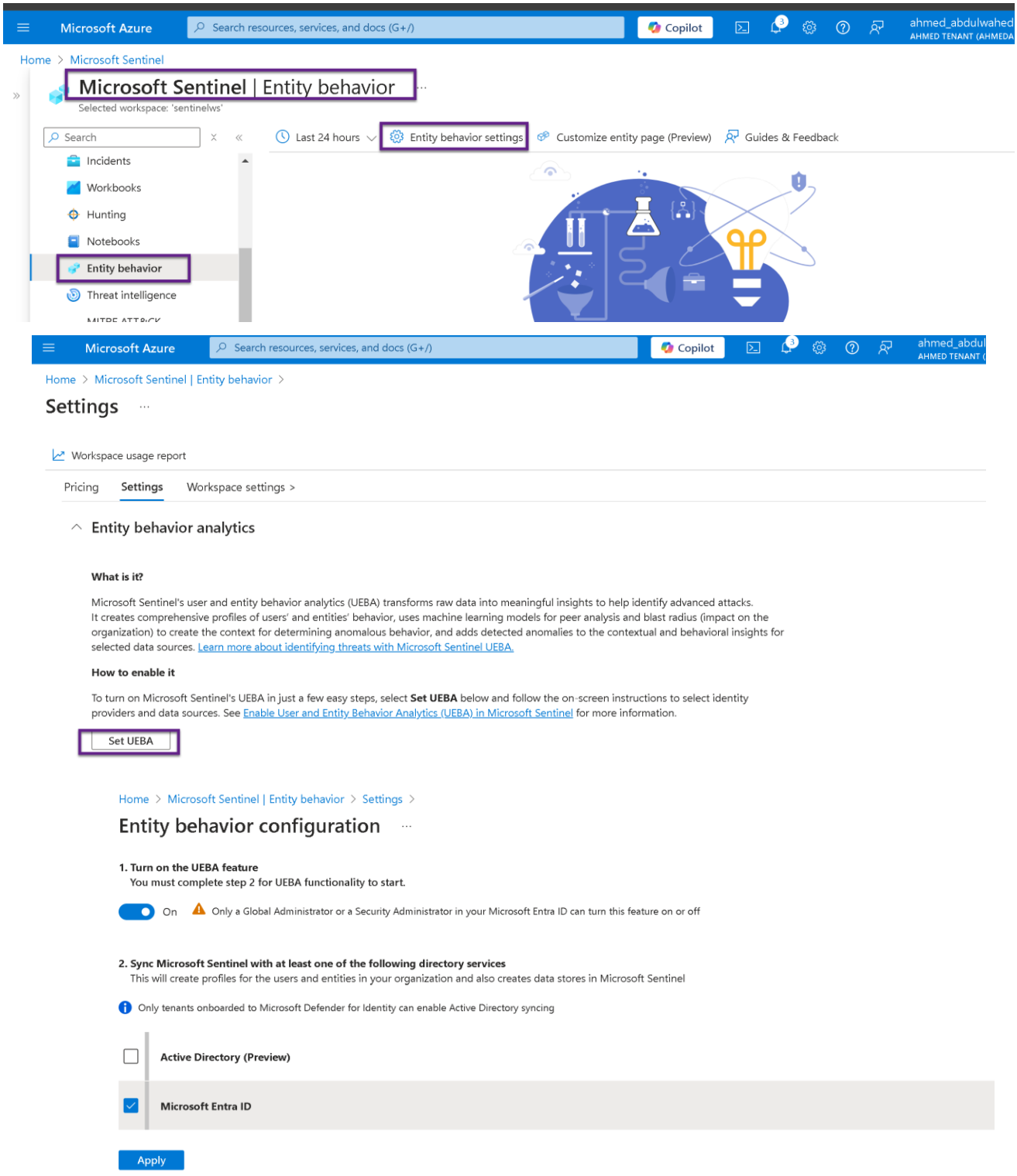

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Syslog
Linux machines
sentinelws
Auto refresh: Off
Linux Machines
TimeRange: Last 14 days
Computer: All
Severity: All
err
4
warn
3
notice
40
info
3.32 K
"Emergency" level events, by computer
No emergency events within the defined scope
"Critical" level events, by computer
No critical events within the defined scope
"Alert" level events, by computer
No alert events within the defined scope
Home > Syslog
Linux machines
sentinelws
Auto refresh: Off
Syslog messages of events
3.4K
Other
2.93 K
(root) CMD (/usr/sbin/logrotate -s /var/lib/logrotate/omsagent-status /etc/logrotate.d/on
107
(root) CMDEND (/usr/sbin/logrotate -s /var/lib/logrotate/omsagent-status /etc/logrotate.
107
Reached target Basic System.
55
Queued start job for default target Main User Target.
54
Created slice User Application Slice.
54
Started Daily Cleanup of User's Temporary Directories.
54
Process names of events
3.4K
systemd (daemon)
2.48 K
CROND (crond)
376
python3 (daemon)
325
Other
98
NetworkManager (daemon)
35
augenrules (daemon)
29
run-parts (crond)
16

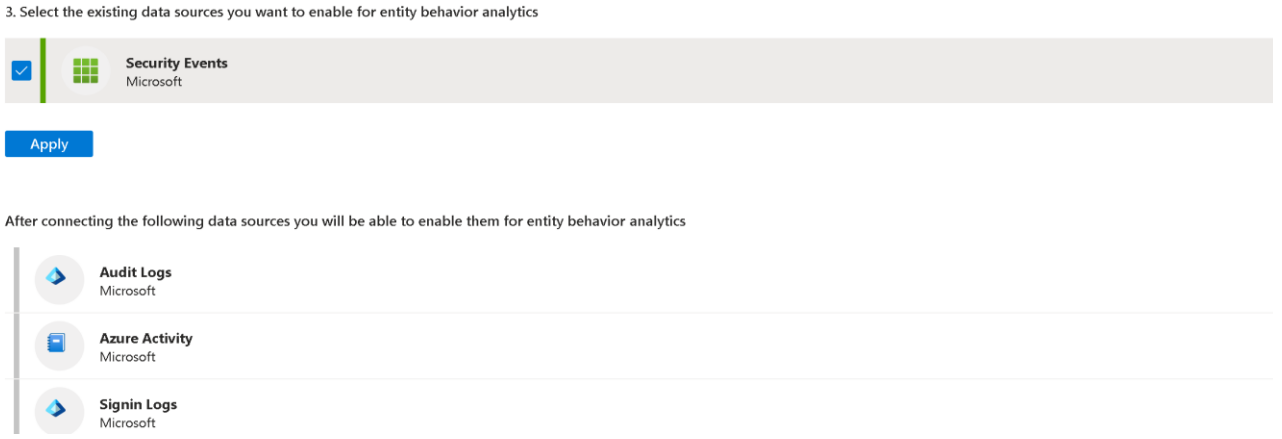

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Syslog >
Workbooks
Refresh
Add Workbook
Guides & Feedback
0
My workbooks
7
Templates
0
Updates
More content at
Content hub
My workbooks
Templates
LinuxMachinesWorkbook
Add
Name
Status
Source name
Linux machines
--
Syslog
Linux machines
Description
Gain insights into your workspaces' Linux machines by connecting Microsoft Sentinel and using the logs to gather insights around Linux events and errors.
Save workbook to...
Select a location where you want to save this workbook.
East US
Yes
No
View Template
Save

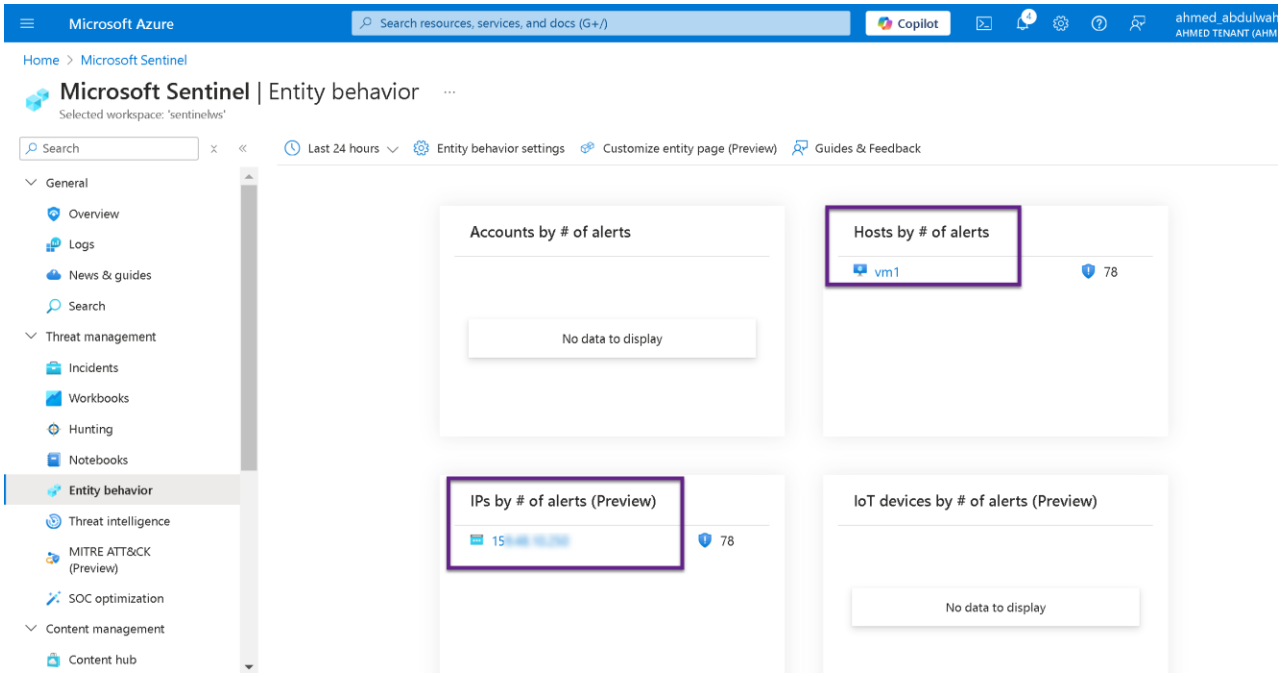

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel
Microsoft Sentinel | Workbooks
Selected workspace: 'sentinelws'
Search
Refresh
Add Workbook
Guides & Feedback
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
SOC optimization
Content management
Content hub
Repositories (Preview)
Community
Configuration
1
My workbooks
7
Templates
0
Updates
More content at
Content hub
My workbooks
Templates
Search
Add
Name
Content source
Source name
Linux machines
Content hub
Syslog
Linux machines
Status
Saved
Description
Gain insights into your workspaces' Linux machines by connecting Microsoft Sentinel and using the logs to gather insights around Linux events and errors.
Required data type
Syslog
Relevant data connectors
Syslog
Content source
Template version
View saved workbook
View Template
Delete

Microsoft Sentinel | Entity Behavior

Microsoft Sentinel's **Entity Behavior Analytics (EBA)** helps detect and respond to potential threats by analyzing and identifying anomalous behaviors associated with entities, such as users, IP addresses, and hosts. This feature uses **Machine Learning (ML)** models to establish baselines and identify deviations from expected behavior.




3. Select the existing data sources you want to enable for entity behavior analytics
Security Events
Microsoft
Apply
After connecting the following data sources you will be able to enable them for entity behavior analytics
Audit Logs
Microsoft
Azure Activity
Microsoft
Signin Logs
Microsoft

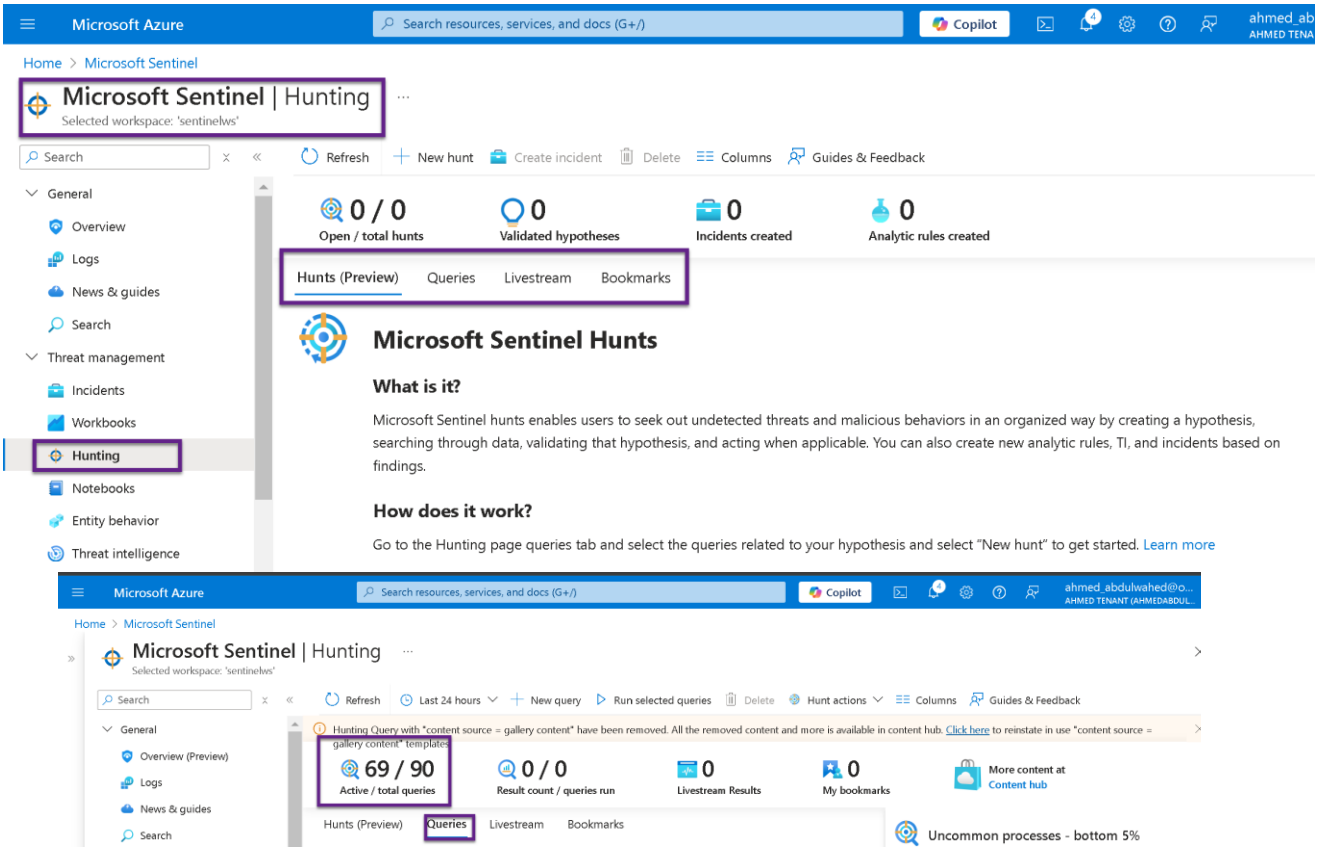

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel
Microsoft Sentinel | Entity behavior
Selected workspace: 'sentinelws'
Search
Last 24 hours
Entity behavior settings
Customize entity page (Preview)
Guides & Feedback
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
SOC optimization
Content management
Content hub
Accounts by # of alerts
No data to display
Hosts by # of alerts
vm1
78
IPs by # of alerts (Preview)
78
IoT devices by # of alerts (Preview)
No data to display

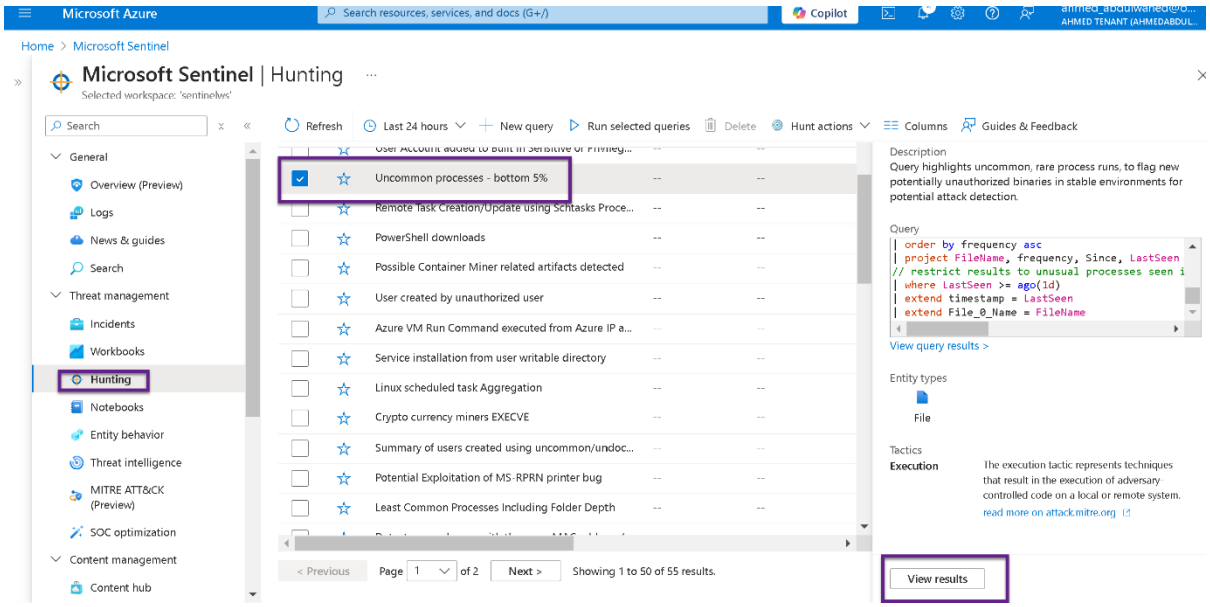

Home > Microsoft Sentinel | Entity behavior >
vm1
Selected workspace: 'sentinelws'
Guides & Feedback
Custom range: 12/31/2024 - 1/1/2025
vm1
DNS Name
Identity
OS Type
Windows
OS Version
10.0
Is Domain Joined
NetBios Name
Public IP Addresses
Private IP Addresses
10.0.0.4
Entity link
https://portal.azure.com/#asset/Microsoft_Azure_Security_Insight...
Investigate
Run playbook
Alerts, events and anomalies over time
1.8K
1.4K
900
450
0
12
9
6
3
0
Jan 1
SecurityAlert
78
Anomalies
0
SecurityEvent
4.5K
Entity timeline
Search
Timeline content : All
Tactics : All
Add filter
Insights
Host IP address remote co...
12/31/2024, 9:49:41 PM - 1/1/2025, ...
No network sessions have been identified for the device based on the available device identifiers.
Open in Log Analytics >
Linux new or deleted user...
12/31/2024, 9:49:41 AM - 1/2/2025, ...
No results
Linux group actions on host
12/31/2024, 9:49:41 AM - 1/2/2025, ...
No results
Linux sign-in activity
12/31/2024, 9:49:41 AM - 1/2/2025, ...
No results

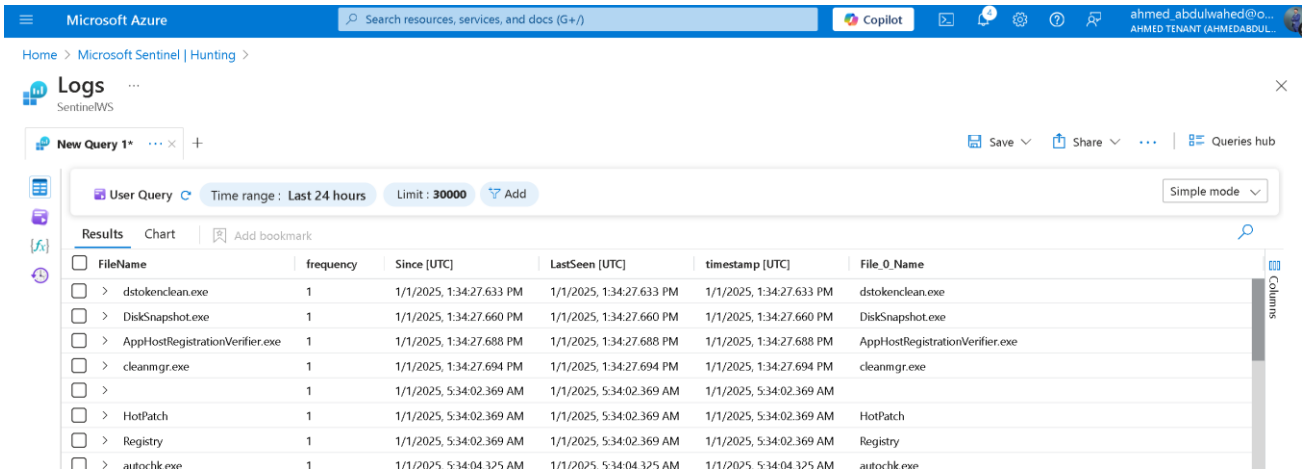

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ahmed_abdulwahed@o...
AHMED TENANT (AHMEDABDUL...
Home > Microsoft Sentinel | Entity behavior >
159.48.10.250
Guides & Feedback
Custom range: 12/31/2024 - 1/1/2025
IPv4 : Internet
IP Type
Geolocation information
Organization
Awaser Oman Llc
Organization type
-
City
-
Country
Oman
State
-
Continent
Asia
Entity link
https://portal.azure.com/#asset/Microsoft_Azure_Security_Insight...
Run playbook
Add to TI
Investigate
Actions
Alerts, events and anomalies over time
Jan 1
SecurityAlert
78
Anomalies
0
Entity timeline
Search
Timeline content : All
Tactics : All
Add filter
Insights
Microsoft Defender Threa...
12/31/2024, 9:51:37 PM - 1/1/2025, ...
This widget requires an active Microsoft Defender Threat Intelligence license, click here for more information about the service.
Anomalies Count By Ip Ad...
12/31/2024, 9:51:37 PM - 1/1/2025, ...
IP Address '159.48.10.250' was found to be associated with 0 anomalies in the past 30 days.
Open in Log Analytics >
Network Traffic Inspection
12/31/2024, 9:51:37 PM - 1/1/2025, ...

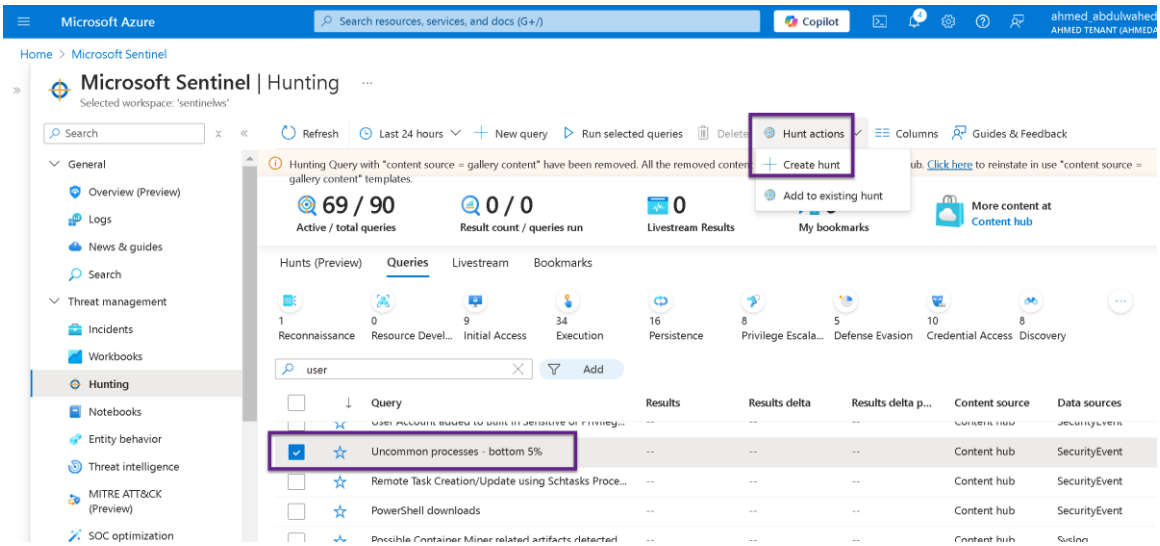
Microsoft Sentinel | Hunting

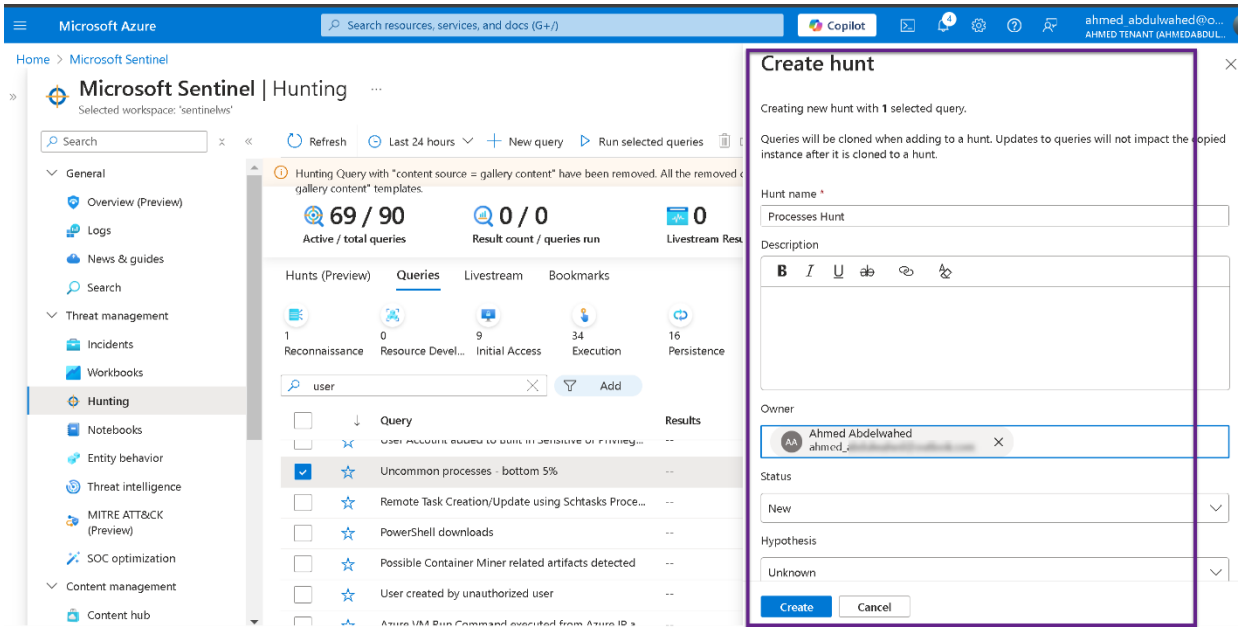
Microsoft Sentinel's **Hunting** feature allows security analysts to proactively search for threats in their environments. It provides a set of tools to craft and run queries across collected data, enabling threat discovery and identification of abnormal activities that might indicate potential breaches or attacks.

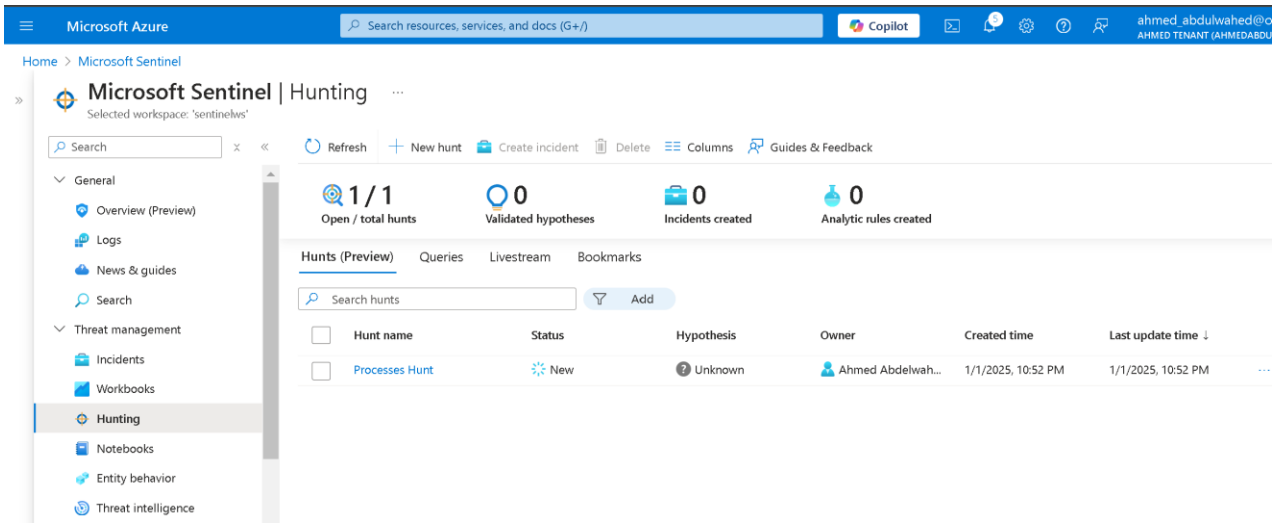





Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel | Hunting >
Logs
SentinelWS
New Query 1*
Save
Share
Queries hub
User Query
Time range : Last 24 hours
Limit : 30000
Add
Simple mode
Results
Chart
Add bookmark
FileName
frequency
Since [UTC]
LastSeen [UTC]
timestamp [UTC]
File_0_Name
dstokenclean.exe
DiskSnapshot.exe
AppHostRegistrationVerifier.exe
cleanmgr.exe
HotPatch
Registry
Columns

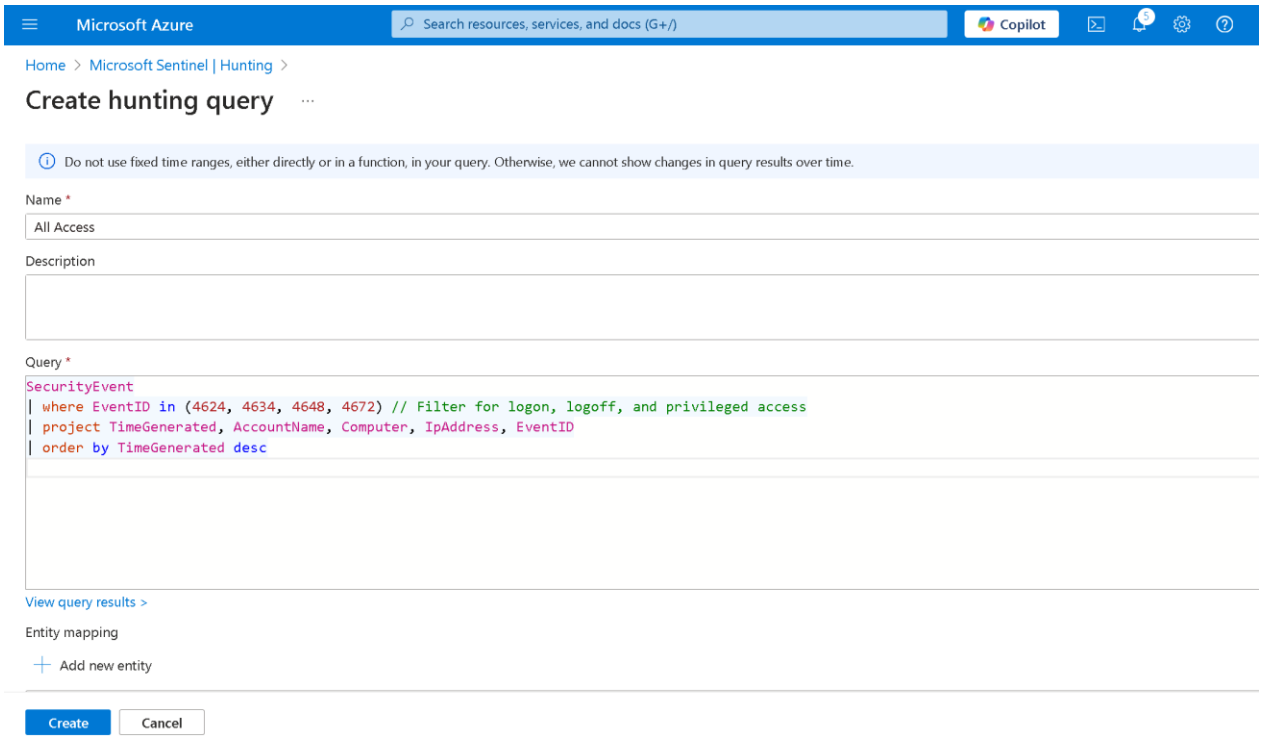

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel
Microsoft Sentinel | Hunting
Selected workspace: 'sentinelws'
Refresh
Last 24 hours
New query
Run selected queries
Hunt actions
Create hunt
Add to existing hunt
Columns
Guides & Feedback
Hunting Query with "content source = gallery content" have been removed. All the removed content
gallery content" templates.
69 / 90
Active / total queries
0 / 0
Result count / queries run
0
Livestream Results
My bookmarks
More content at
Content hub
Hunts (Preview)
Queries
Livestream
Bookmarks
Reconnaissance
Resource Devel...
Initial Access
Execution
Persistence
Privilege Escala...
Defense Evasion
Credential Access
Discovery
user
Add
Query
Results
Results delta
Results delta p...
Content source
Data sources
Uncommon processes - bottom 5%
Remote Task Creation/Update using Schtasks Proce...
PowerShell downloads
Content hub
SecurityEvent
General
Overview (Preview)
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
SOC optimization


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel
Microsoft Sentinel | Hunting
Selected workspace: 'sentinelws'
Create hunt
Creating new hunt with 1 selected query.
Queries will be cloned when adding to a hunt. Updates to queries will not impact the copied instance after it is cloned to a hunt.
Hunt name *
Processes Hunt
Description
Owner
Ahmed Abdelwahed
Status
New
Hypothesis
Unknown
Create
Cancel
69 / 90
Active / total queries
0 / 0
Result count / queries run
Hunts (Preview)
Queries
Livestream
Bookmarks
Uncommon processes - bottom 5%
Remote Task Creation/Update using Schtasks Proce...
PowerShell downloads
Possible Container Miner related artifacts detected
User created by unauthorized user

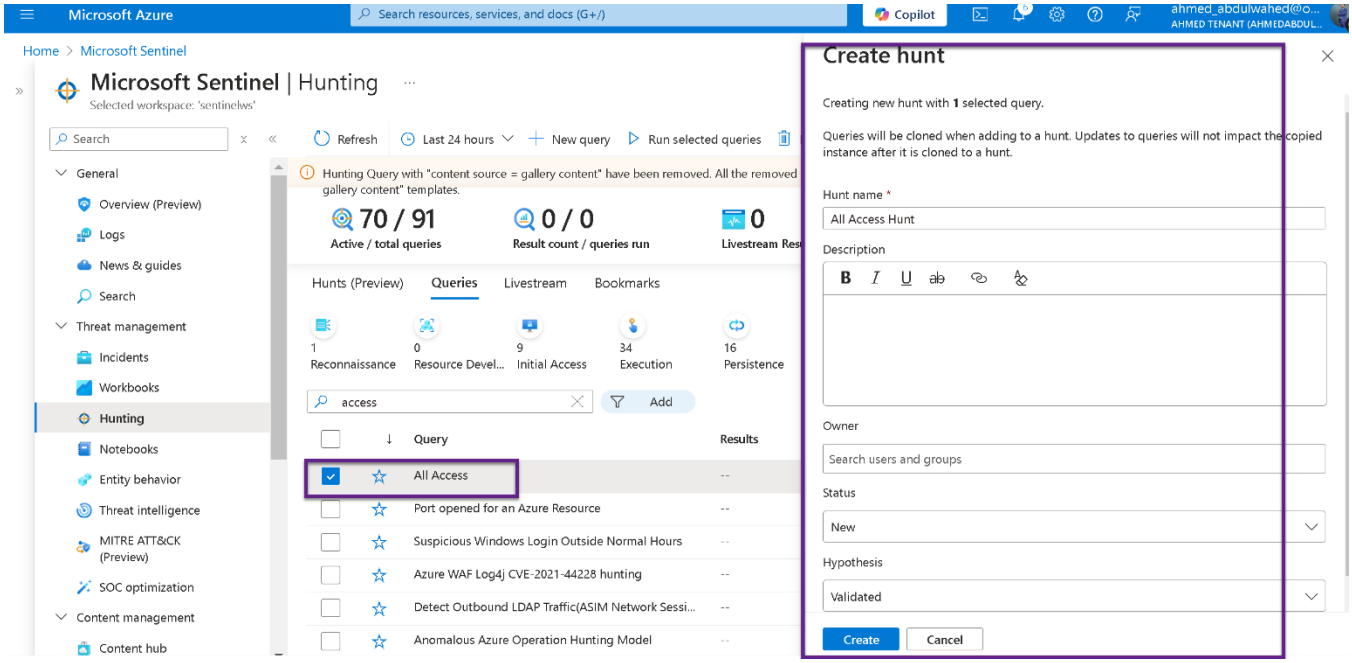


Create Custom Hunting Query

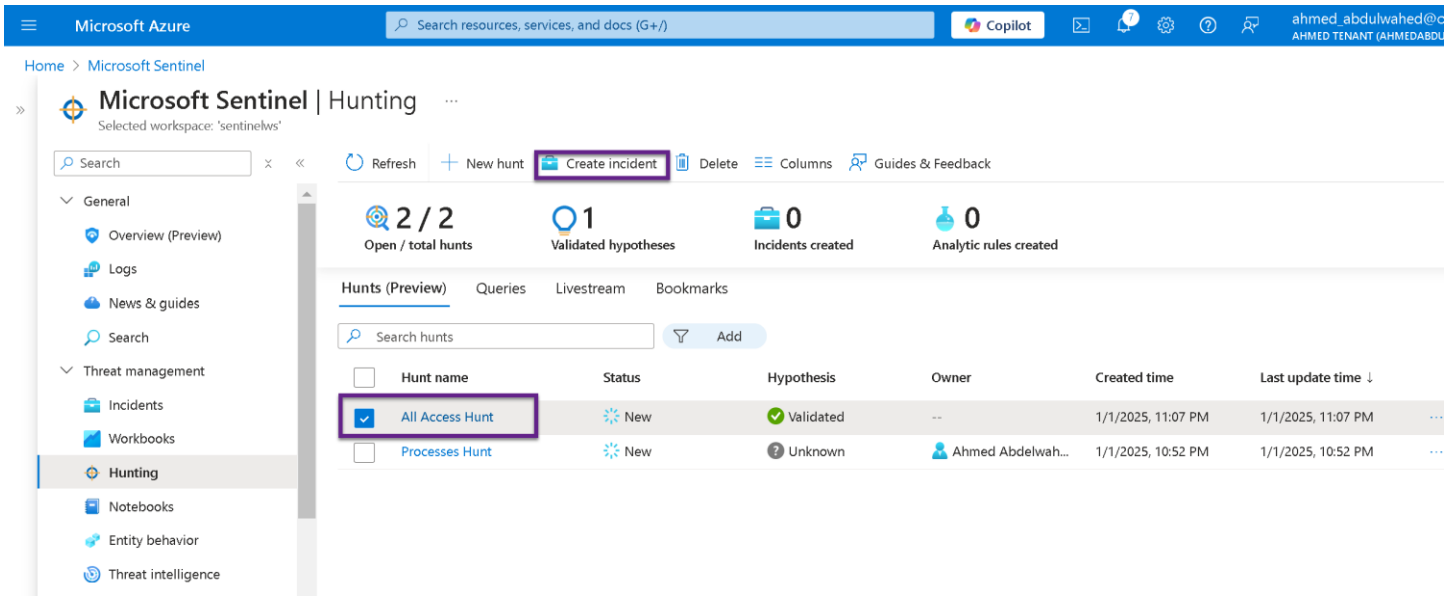
```
SecurityEvent
| where EventID in (4624, 4634, 4648, 4672) // Filter for logon, logoff, and privileged access
| project TimeGenerated, AccountName, Computer, IpAddress, EventID
| order by TimeGenerated desc
```



Based on this, create a Hunt



And baed on hunt you can create incident



Microsoft Sentinel Notebooks is a feature that allows security analysts and engineers to analyze and visualize data interactively using **Jupyter Notebooks** directly within Microsoft Sentinel. These notebooks combine live code, visualizations, and markdown to provide a collaborative, interactive, and detailed way to perform threat hunting, anomaly detection, and security investigation.

To start used Notebook you have to enable the next 2 ML option below

