Microsoft Sentinel SOC Lab

Windows Security Events with Azure Arc, AMA and DCR

What this lab does

This lab connects a Windows machine to Azure using Azure Arc, installs Azure Monitor Agent, collects Windows Security event logs via a Data Collection Rule, and sends those logs into a Log Analytics workspace that is connected to Microsoft Sentinel.

Once logs are flowing, we validate key event IDs and build an analytics rule that detects multiple failed logons, then confirms incidents appear in Microsoft Defender.

Tools and services used

- Windows 10 Pro virtual machine on VirtualBox
- Azure Arc enabled machine
- Azure Monitor Agent extension
- Log Analytics workspace
- Microsoft Sentinel
- Data Collection Rule
- KQL queries
- Sentinel analytics scheduled rule

Key event IDs used in this lab

- **4625** Login failure
- **4624** Login success
- **4688** Process creation

Step 1: Enable Windows auditing

Goal

Make sure the Windows machine actually produces useful security logs.

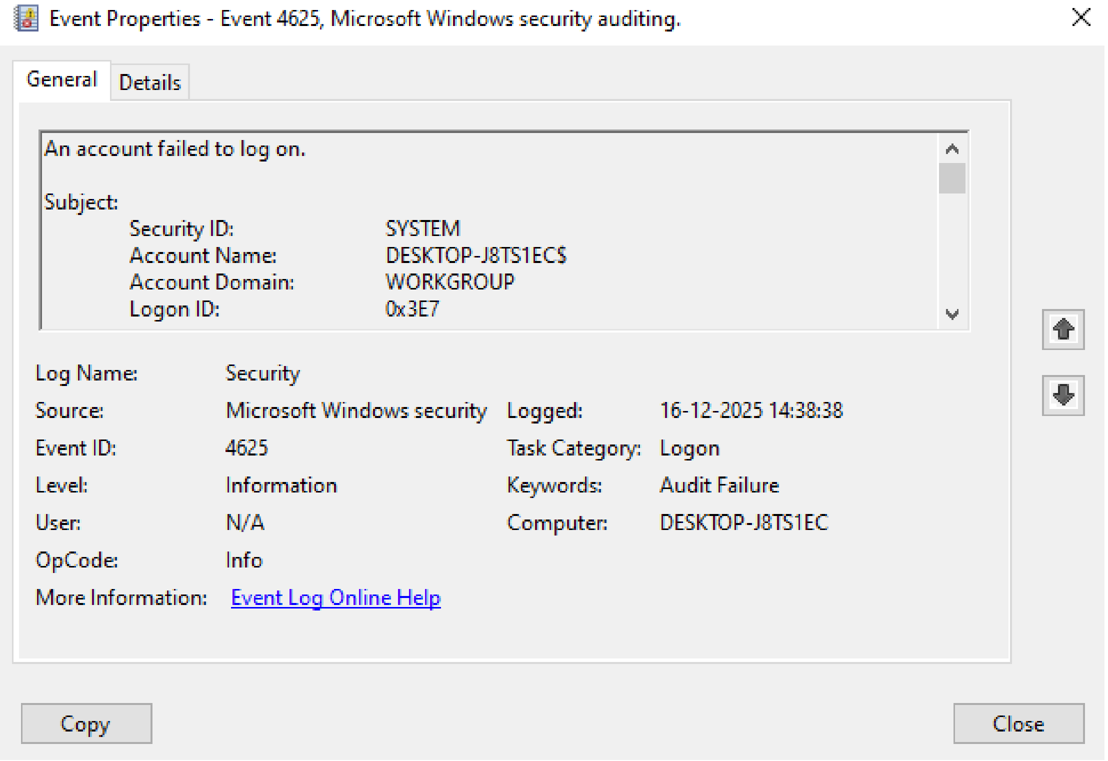
What I changed

I enabled Advanced Audit Policy settings so Windows logs authentication and process activity properly.

Screenshots

Local Windows event validation:

- Failed logon event 4625



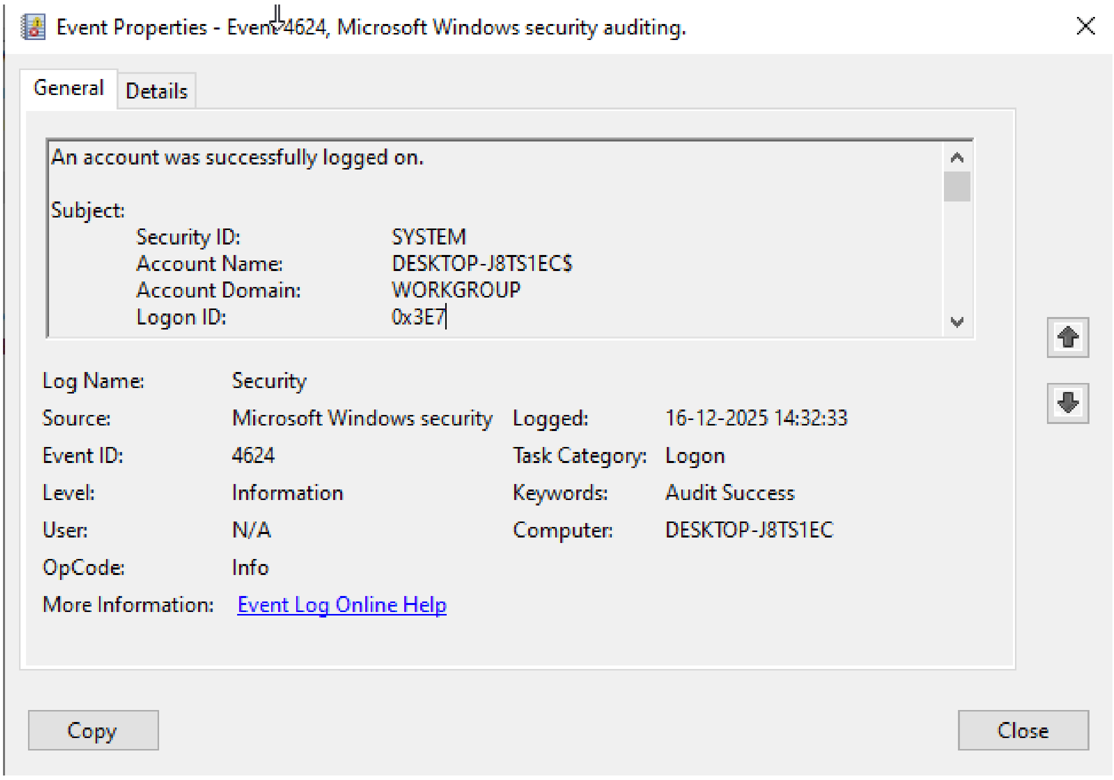
Event Properties - Event 4625, Microsoft Windows security auditing.
General
Details
Copy
Close

```
An account failed to log on.

Subject:
        Security ID:            SYSTEM
        Account Name:           DESKTOP-J8TS1EC$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	16-12-2025 14:38:38
Event ID:	4625	Task Category:	Logon
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	DESKTOP-J8TS1EC
OpCode:	Info		
More Information:	Event Log Online Help		

- Successful logon event 4624



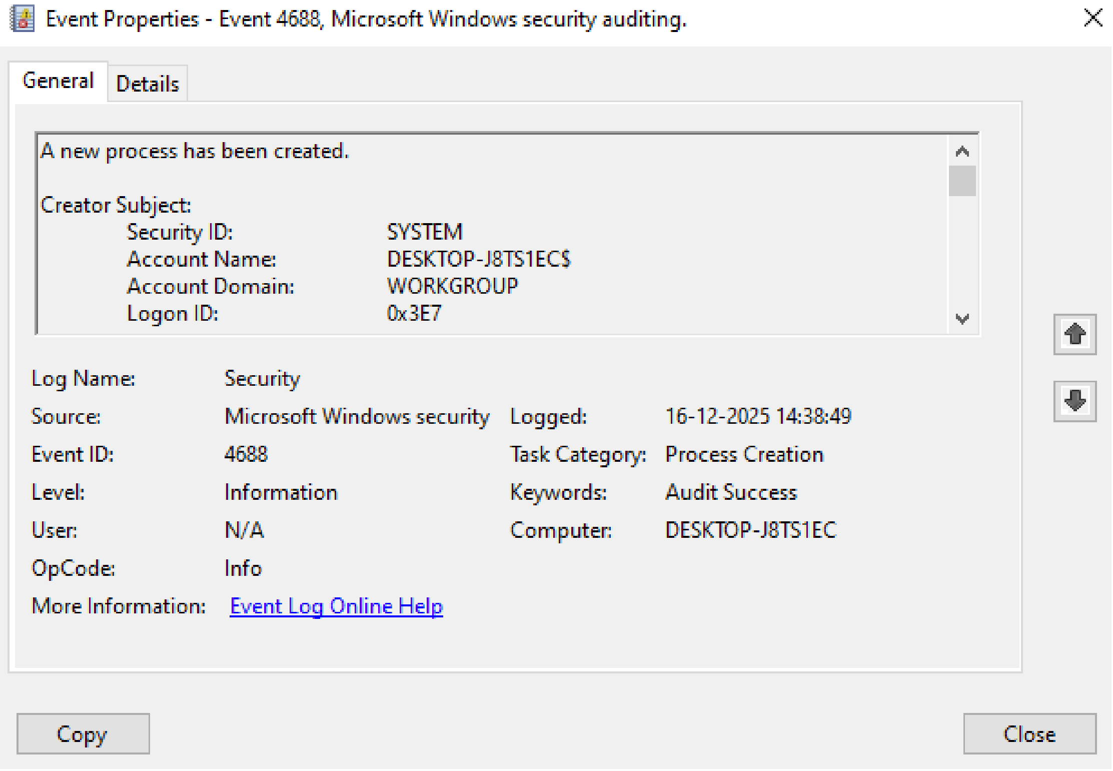
Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details
Copy
Close

```
An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           DESKTOP-J8TS1EC$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	16-12-2025 14:32:33
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-J8TS1EC
OpCode:	Info		
More Information:	Event Log Online Help		

- Process creation event 4688



Event Properties - Event 4688, Microsoft Windows security auditing.
General
Details
Copy
Close

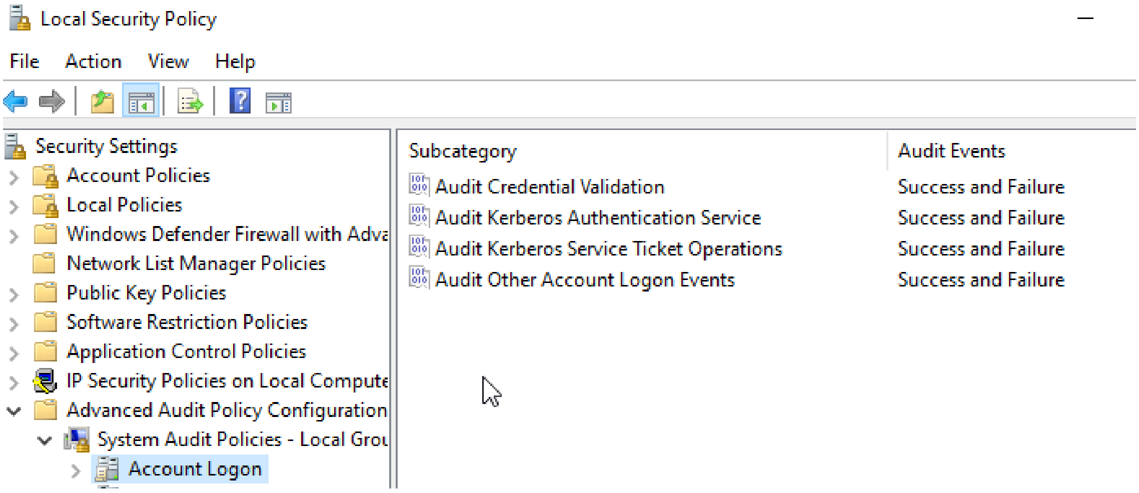
```
A new process has been created.

Creator Subject:
        Security ID:        SYSTEM
        Account Name:       DESKTOP-J8TS1EC$
        Account Domain:     WORKGROUP
        Logon ID:           0x3E7
```

Log Name: Security
Source: Microsoft Windows security
Logged: 16-12-2025 14:38:49
Event ID: 4688
Task Category: Process Creation
Level: Information
Keywords: Audit Success
User: N/A
Computer: DESKTOP-J8TS1EC
OpCode: Info
More Information: Event Log Online Help

Advanced audit policy settings:

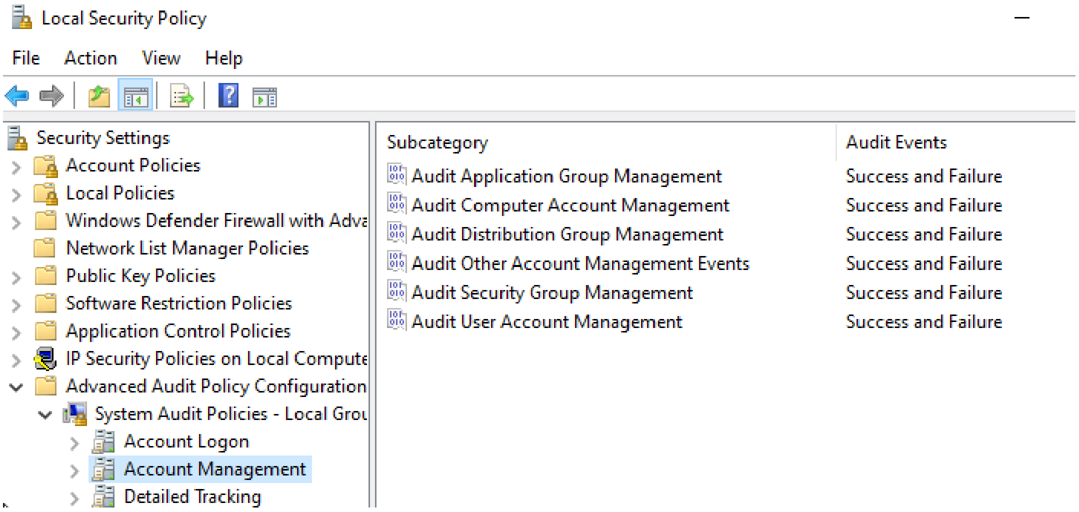
- Account Logon



Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
System Audit Policies - Local Grou
Account Logon

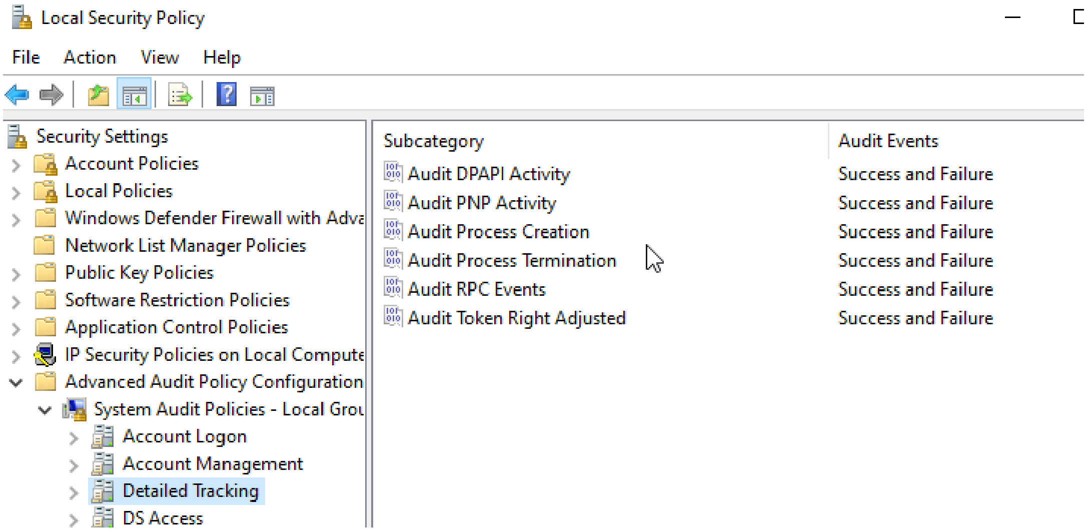
Subcategory	Audit Events
Audit Credential Validation	Success and Failure
Audit Kerberos Authentication Service	Success and Failure
Audit Kerberos Service Ticket Operations	Success and Failure
Audit Other Account Logon Events	Success and Failure

- Account Management


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
System Audit Policies - Local Grou
Account Logon
Account Management
Detailed Tracking

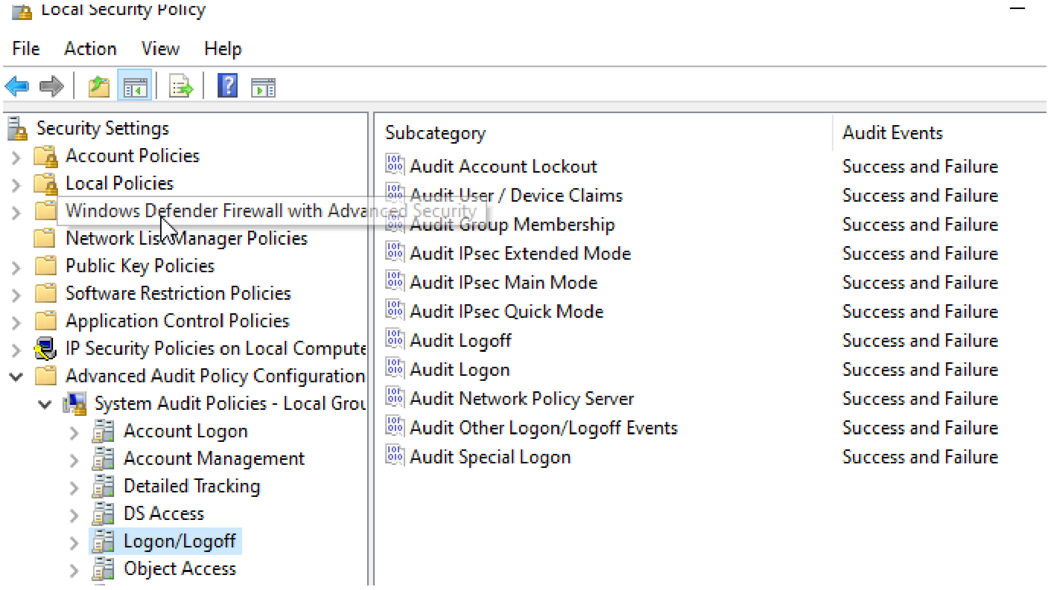
Subcategory	Audit Events
Audit Application Group Management	Success and Failure
Audit Computer Account Management	Success and Failure
Audit Distribution Group Management	Success and Failure
Audit Other Account Management Events	Success and Failure
Audit Security Group Management	Success and Failure
Audit User Account Management	Success and Failure

- Detailed Tracking


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
System Audit Policies - Local Grou
Account Logon
Account Management
Detailed Tracking
DS Access

Subcategory	Audit Events
Audit DPAPI Activity	Success and Failure
Audit PNP Activity	Success and Failure
Audit Process Creation	Success and Failure
Audit Process Termination	Success and Failure
Audit RPC Events	Success and Failure
Audit Token Right Adjusted	Success and Failure

- Logon Logoff


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
System Audit Policies - Local Grou
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access

Subcategory	Audit Events
Audit Account Lockout	Success and Failure
Audit User / Device Claims	Success and Failure
Audit Group Membership	Success and Failure
Audit IPsec Extended Mode	Success and Failure
Audit IPsec Main Mode	Success and Failure
Audit IPsec Quick Mode	Success and Failure
Audit Logoff	Success and Failure
Audit Logon	Success and Failure
Audit Network Policy Server	Success and Failure
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success and Failure

Step 2: Create Azure resources

Goal

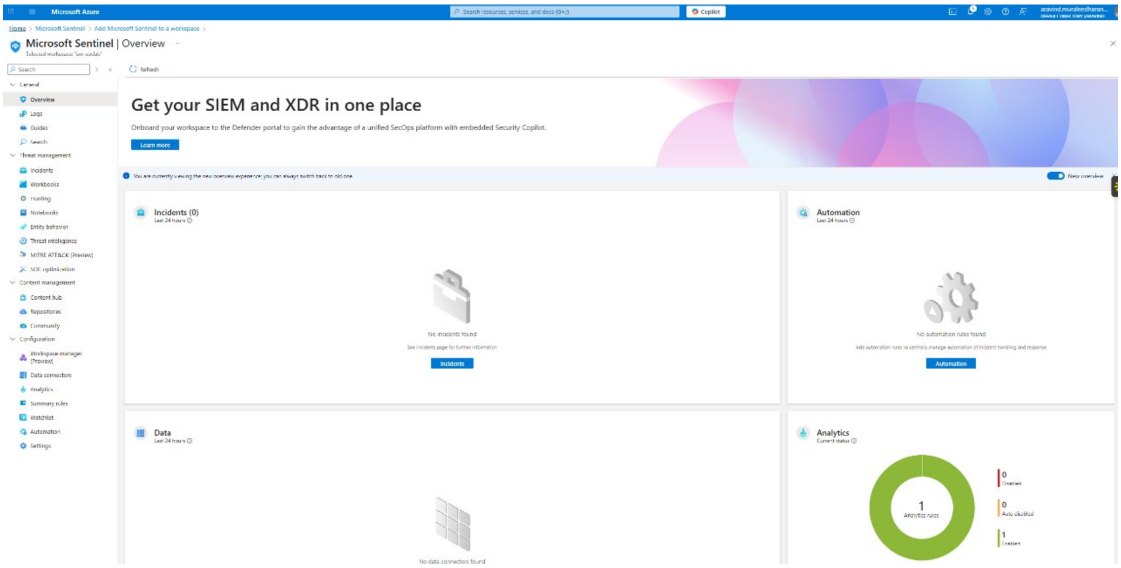
Set up the workspace and the container resources we need for Sentinel.

What I created

- Resource group: rg-soclab
- Log Analytics workspace: law-soclab
- Microsoft Sentinel enabled on law-soclab

Screenshots

- Sentinel workspace selected



Get your SIEM and XDR in one place

Onboard your workspace to the Defender portal to gain the advantage of a unified SecOps platform with embedded Security Copilot.

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

No incidents found

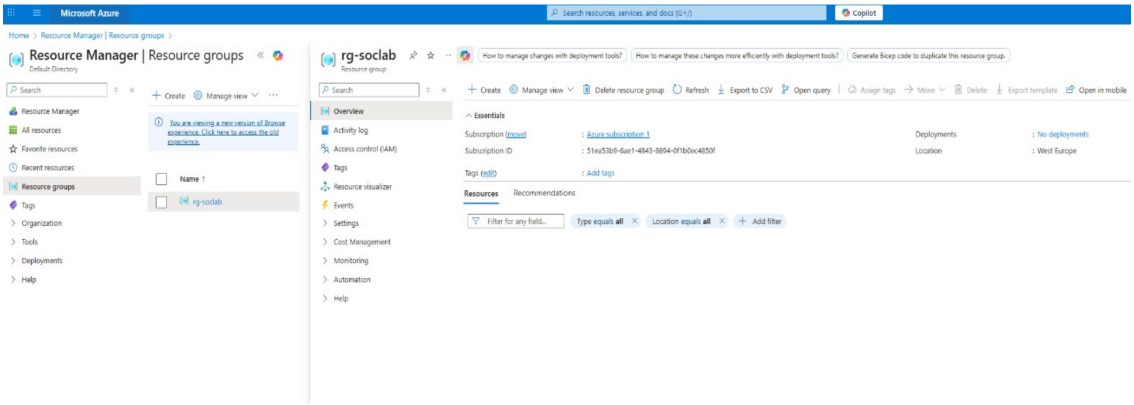
See incidents page for further information

No automation rules found

Add automation rules to centrally manage automation of incident handling and response

No data connectors found

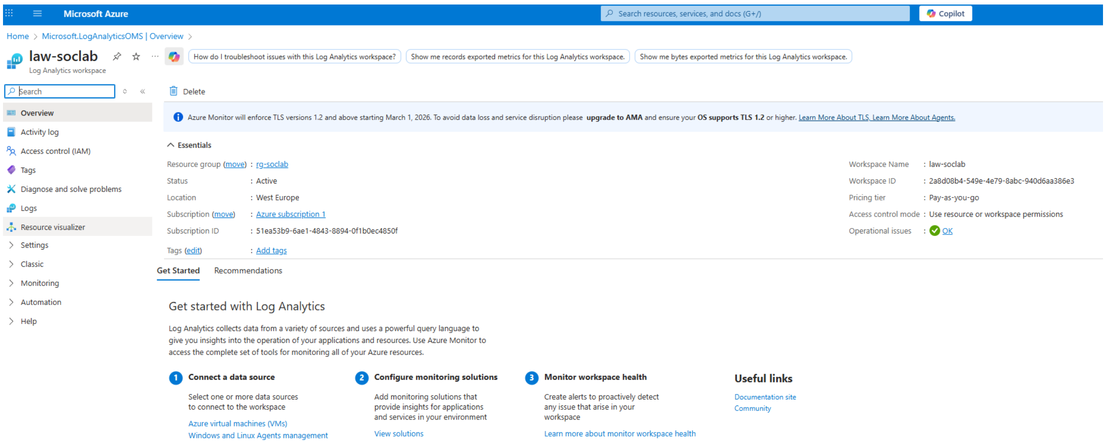
- Resource group created



You are viewing a new version of Browse experience. Click here to access the old experience.

Subscription (move) : Azure subscription 1
Subscription ID : 51ea53b9-6ae1-4843-8894-0f1b0ec4850f
Tags (edit) : Add tags
Deployments : No deployments
Location : West Europe

- Workspace overview page


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft.LogAnalyticsOMS | Overview >
law-soclab
Log Analytics workspace
How do I troubleshoot issues with this Log Analytics workspace?
Show me records exported metrics for this Log Analytics workspace.
Show me bytes exported metrics for this Log Analytics workspace.
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Resource visualizer
Settings
Classic
Monitoring
Automation
Help
Delete
Get Started
Recommendations

Azure Monitor will enforce TLS versions 1.2 and above starting March 1, 2026. To avoid data loss and service disruption please **upgrade to AMA** and ensure your **OS supports TLS 1.2** or higher. Learn More About TLS, Learn More About Agents.

Essentials

Resource group (move) : rg-soclab
Status : Active
Location : West Europe
Subscription (move) : Azure subscription 1
Subscription ID : 51ea53b9-6ae1-4843-8894-0f1b0ec4850f
Tags (edit) : Add tags

Workspace Name : law-soclab
Workspace ID : 2a8d08b4-549e-4e79-8abc-940d6aa386e3
Pricing tier : Pay-as-you-go
Access control mode : Use resource or workspace permissions
Operational issues : ✓ OK

Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

1 **Connect a data source**
Select one or more data sources to connect to the workspace
Azure virtual machines (VMs)
Windows and Linux Agents management

2 **Configure monitoring solutions**
Add monitoring solutions that provide insights for applications and services in your environment
View solutions

3 **Monitor workspace health**
Create alerts to proactively detect any issue that arise in your workspace
Learn more about monitor workspace health

Useful links
Documentation site
Community

Step 3: Onboard the Windows VM to Azure Arc

Goal

Get the VM visible in Azure as an Arc machine so we can manage extensions and monitoring.

What I did

I used the Arc onboarding method for “Any environment” and connected the machine. After a reinstall and cleanup, the connection succeeded and the machine appeared as Connected in Azure Arc.

Success checks

- Machine appears under Azure Arc
- Status shows Connected
- Agent version is visible
- Extensions can be installed

Step 4: Install Azure Monitor Agent extension

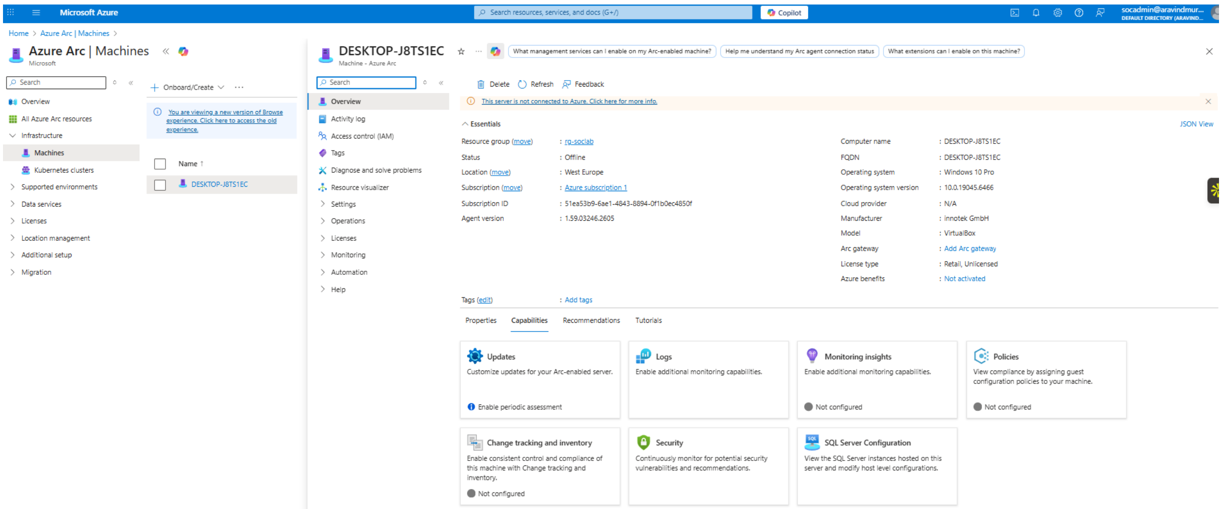
Goal

Azure Monitor Agent is required for Data Collection Rules and modern log ingestion.

What I did

I installed the Azure Monitor Windows Agent extension on the Arc machine and confirmed it shows as Succeeded.

Screenshot



DESKTOP-J8TS1EC

You are viewing a new version of Browse experience. Click here to access the old experience.

This server is not connected to Azure. Click here for more info.

Essentials

Resource group (move)	: rg-soclab	Computer name	: DESKTOP-J8TS1EC
Status	: Offline	FQDN	: DESKTOP-J8TS1EC
Location (move)	: West Europe	Operating system	: Windows 10 Pro
Subscription (move)	: Azure subscription 1	Operating system version	: 10.0.19045.6466
Subscription ID	: 51ea53b9-6ae1-4843-8894-0f1b0ec4850f	Cloud provider	: N/A
Agent version	: 1.59.03246.2605	Manufacturer	: innotek GmbH
		Model	: VirtualBox
		Arc gateway	: Add Arc gateway
		License type	: Retail, Unlicensed
		Azure benefits	: Not activated
Tags (edit)	: Add tags		

Updates
Customize updates for your Arc-enabled server.
Enable periodic assessment

Logs
Enable additional monitoring capabilities.

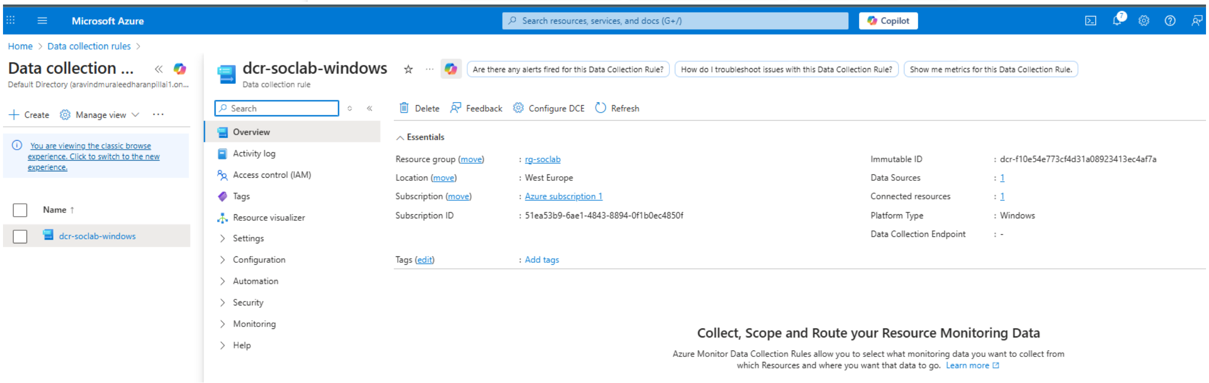
Monitoring insights
Enable additional monitoring capabilities.
Not configured

Policies
View compliance by assigning guest configuration policies to your machine.
Not configured

Change tracking and inventory
Enable consistent control and compliance of this machine with Change tracking and inventory.
Not configured

Security
Continuously monitor for potential security vulnerabilities and recommendations.

SQL Server Configuration
View the SQL Server instances hosted on this server and modify host level configurations.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Data collection rules >
Data collection ...
Default Directory (aravindmuraleedharanpillai1.on...
Create
Manage view
Name ↑
dcr-soclab-windows
Data collection rule
Are there any alerts fired for this Data Collection Rule?
How do I troubleshoot issues with this Data Collection Rule?
Show me metrics for this Data Collection Rule.
Search
Delete
Feedback
Configure DCE
Refresh
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Settings
Configuration
Automation
Security
Monitoring
Help

dcr-soclab-windows

You are viewing the classic browse experience. Click to switch to the new experience.

Essentials

Resource group (move)	: rg-soclab	Immutable ID	: dcr-f10e54e773cf4d31a08923413ec4af7a
Location (move)	: West Europe	Data Sources	: 1
Subscription (move)	: Azure subscription 1	Connected resources	: 1
Subscription ID	: 51ea53b9-6ae1-4843-8894-0f1b0ec4850f	Platform Type	: Windows
		Data Collection Endpoint	: -
Tags (edit)	: Add tags		

Collect, Scope and Route your Resource Monitoring Data

Azure Monitor Data Collection Rules allow you to select what monitoring data you want to collect from which Resources and where you want that data to go. Learn more

---

Step 5: Create a Data Collection Rule

Goal

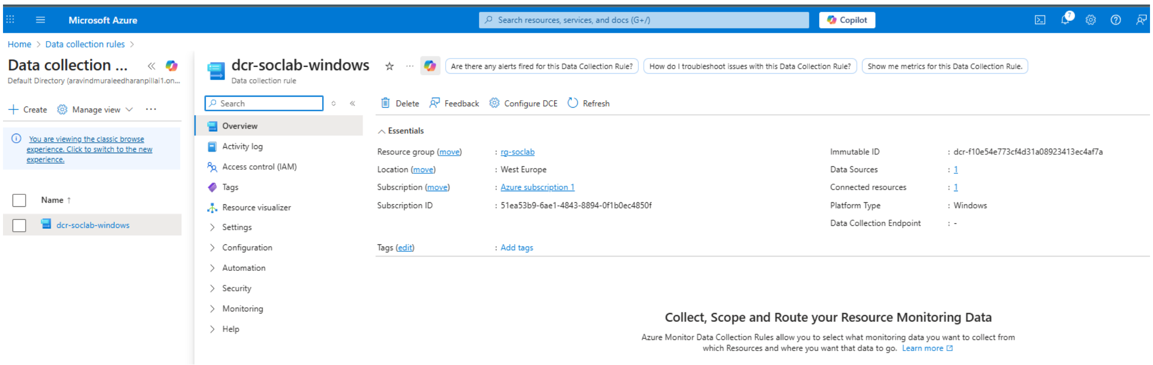
Collect Security event logs from the Arc machine and send them into the Log Analytics workspace.

What I configured

- Data source: Windows Event Logs
- Log name: Security
- Events: Audit Success and Audit Failure
- Destination: Azure Monitor Logs, connected to law-soclab
- Resource scope: the Arc machine

Screenshots

- Data Collection Rule created


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Data collection rules >
+ Create
Manage view
Name ↑
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Settings
Configuration
Automation
Security
Monitoring
Help
Delete
Feedback
Configure DCE
Refresh
Are there any alerts fired for this Data Collection Rule?
How do I troubleshoot issues with this Data Collection Rule?
Show me metrics for this Data Collection Rule.

Data collection ...

Default Directory (aravindmuraleedharanpillai1.on...

You are viewing the classic browse experience. Click to switch to the new experience.

dcr-soclab-windows

dcr-soclab-windows

Data collection rule

Essentials

Resource group (move) : rg-soclab

Location (move) : West Europe

Subscription (move) : Azure subscription 1

Subscription ID : 51ea53b9-6ae1-4843-8894-0f1b0ec4850f

Immutable ID : dcr-f10e54e773cf4d31a08923413ec4af7a

Data Sources : 1

Connected resources : 1

Platform Type : Windows

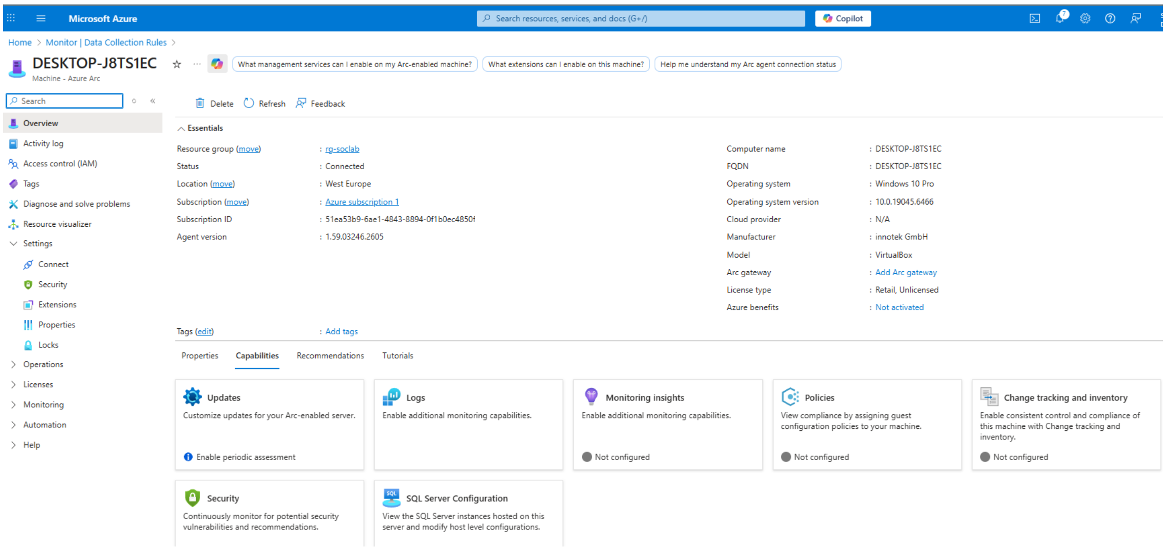
Data Collection Endpoint : -

Tags (edit) : Add tags

Collect, Scope and Route your Resource Monitoring Data

Azure Monitor Data Collection Rules allow you to select what monitoring data you want to collect from which Resources and where you want that data to go. Learn more

DCR resource association showing the machine attached


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Monitor | Data Collection Rules >
What management services can I enable on my Arc-enabled machine?
What extensions can I enable on this machine?
Help me understand my Arc agent connection status
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Connect
Security
Extensions
Properties
Locks
Operations
Licenses
Monitoring
Automation
Help
Delete
Refresh
Feedback
Properties
Capabilities
Recommendations
Tutorials

DESKTOP-J8TS1EC

Machine - Azure Arc

Essentials

Resource group (move) : rg-soclab

Status : Connected

Location (move) : West Europe

Subscription (move) : Azure subscription 1

Subscription ID : 51ea53b9-6ae1-4843-8894-0f1b0ec4850f

Agent version : 1.59.03246.2605

Computer name : DESKTOP-J8TS1EC

FQDN : DESKTOP-J8TS1EC

Operating system : Windows 10 Pro

Operating system version : 10.0.19045.6466

Cloud provider : N/A

Manufacturer : innotek GmbH

Model : VirtualBox

Arc gateway : Add Arc gateway

License type : Retail, Unlicensed

Azure benefits : Not activated

Tags (edit) : Add tags

Updates

Customize updates for your Arc-enabled server.

Enable periodic assessment

Logs

Enable additional monitoring capabilities.

Monitoring insights

Enable additional monitoring capabilities.

● Not configured

Policies

View compliance by assigning guest configuration policies to your machine.

● Not configured

Change tracking and inventory

Enable consistent control and compliance of this machine with Change tracking and inventory.

● Not configured

Security

Continuously monitor for potential security vulnerabilities and recommendations.

SQL Server Configuration

View the SQL Server instances hosted on this server and modify host level configurations.

Step 6: Validate data ingestion with KQL

Goal

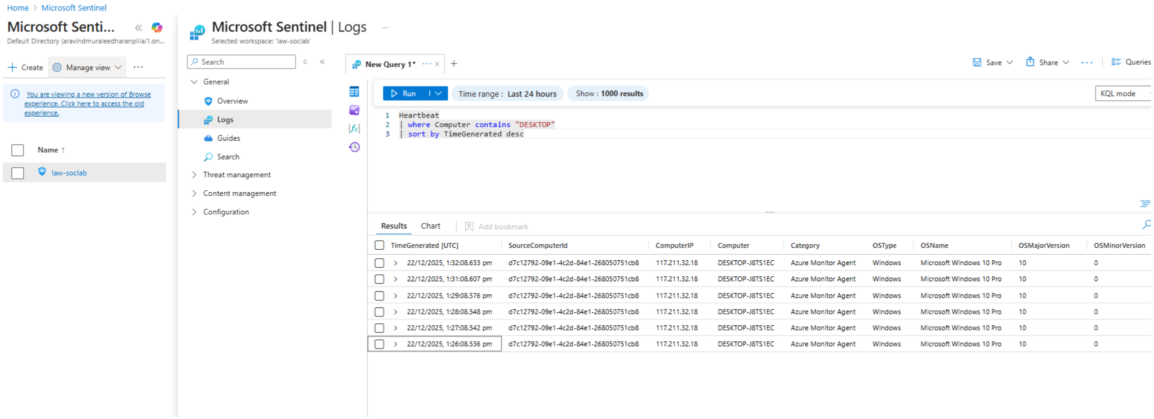
Confirm logs are arriving in the workspace and Sentinel can query them.

Heartbeat check

This confirms the machine is reporting.

```
Heartbeat
| where Computer contains "DESKTOP"
| sort by TimeGenerated desc
```

Screenshot



You are viewing a new version of Browse experience. Click here to access the old experience.

Time range : Last 24 hours Show : 1000 results

```
Heartbeat
| where Computer contains "DESKTOP"
| sort by TimeGenerated desc
```

TimeGenerated [UTC]	SourceComputerId	ComputerIP	Computer	Category	OSType	OSName	OSMajorVersion	OSMinorVersion
22/12/2025, 1:32:08.633 pm	d7c12792-09e1-4c2d-84e1-268050751cb8	117.211.32.18	DESKTOP-J8TS1EC	Azure Monitor Agent	Windows	Microsoft Windows 10 Pro	10	0
22/12/2025, 1:31:08.607 pm	d7c12792-09e1-4c2d-84e1-268050751cb8	117.211.32.18	DESKTOP-J8TS1EC	Azure Monitor Agent	Windows	Microsoft Windows 10 Pro	10	0
22/12/2025, 1:29:08.576 pm	d7c12792-09e1-4c2d-84e1-268050751cb8	117.211.32.18	DESKTOP-J8TS1EC	Azure Monitor Agent	Windows	Microsoft Windows 10 Pro	10	0
22/12/2025, 1:28:08.548 pm	d7c12792-09e1-4c2d-84e1-268050751cb8	117.211.32.18	DESKTOP-J8TS1EC	Azure Monitor Agent	Windows	Microsoft Windows 10 Pro	10	0
22/12/2025, 1:27:08.542 pm	d7c12792-09e1-4c2d-84e1-268050751cb8	117.211.32.18	DESKTOP-J8TS1EC	Azure Monitor Agent	Windows	Microsoft Windows 10 Pro	10	0
22/12/2025, 1:26:08.536 pm	d7c12792-09e1-4c2d-84e1-268050751cb8	117.211.32.18	DESKTOP-J8TS1EC	Azure Monitor Agent	Windows	Microsoft Windows 10 Pro	10	0

Windows Event table check

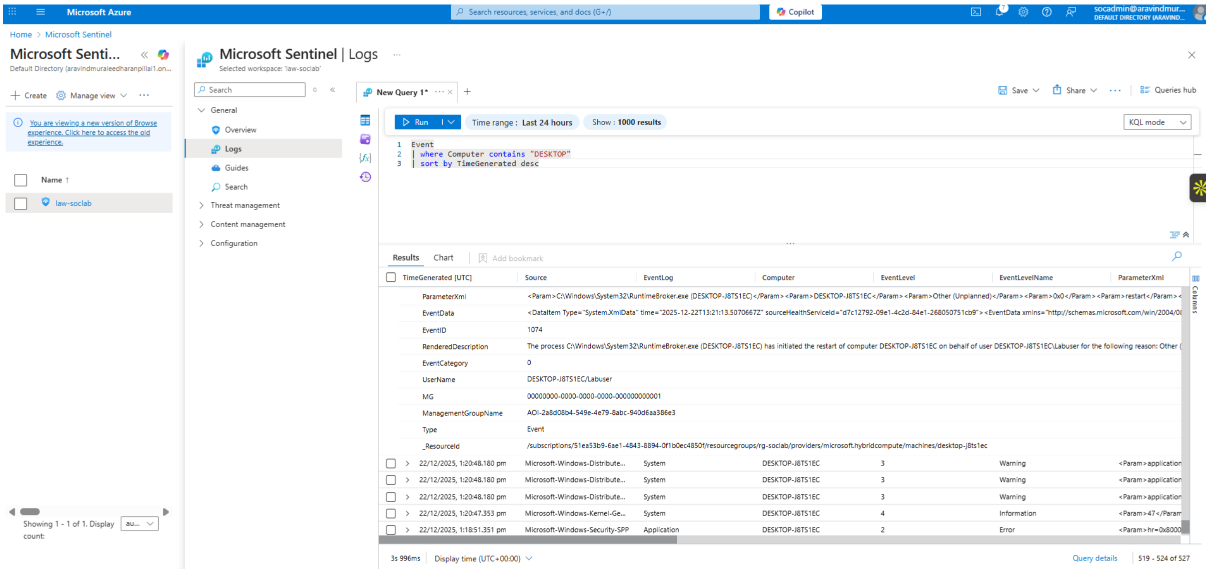
This confirms Windows events are flowing.

Event

| where TimeGenerated > ago(30m)

| sort by TimeGenerated desc

Screenshot



You are viewing a new version of Browse experience. Click here to access the old experience.

Time range : Last 24 hours Show : 1000 results

```
Event
| where Computer contains "DESKTOP"
| sort by TimeGenerated desc
```

ParameterXml	<Param>C:\Windows\System32\RuntimeBroker.exe (DESKTOP-J8TS1EC)</Param><Param>DESKTOP-J8TS1EC</Param><Param>Other (Unplanned)</Param><Param>0x0</Param><Param>restart</Param><
EventData	<DataItem Type="System.XmlData" time="2025-12-22T13:21:13.5070667Z" sourceHealthServiceId="d7c12792-09e1-4c2d-84e1-268050751cb9"><EventData xmlns="http://schemas.microsoft.com/win/2004/0
EventID	1074
RenderedDescription	The process C:\Windows\System32\RuntimeBroker.exe (DESKTOP-J8TS1EC) has initiated the restart of computer DESKTOP-J8TS1EC on behalf of user DESKTOP-J8TS1EC\Labuser for the following reason: Other (
EventCategory	0
UserName	DESKTOP-J8TS1EC/Labuser
MG	00000000-0000-0000-0000-000000000001
ManagementGroupName	AOI-2a8d08b4-549e-4e79-8abc-940d6aa386e3
Type	Event
_ResourceId	/subscriptions/51ea53b9-6ae1-4843-8894-0f1b0ec4850f/resourcegroups/rg-soclab/providers/microsoft.hybridcompute/machines/desktop-j8ts1ec

TimeGenerated [UTC]	Source	EventLog	Computer	EventLevel	EventLevelName	ParameterXml
22/12/2025, 1:20:48.180 pm	Microsoft-Windows-Distribute...	System	DESKTOP-J8TS1EC	3	Warning	<Param>application
22/12/2025, 1:20:48.180 pm	Microsoft-Windows-Distribute...	System	DESKTOP-J8TS1EC	3	Warning	<Param>application
22/12/2025, 1:20:48.180 pm	Microsoft-Windows-Distribute...	System	DESKTOP-J8TS1EC	3	Warning	<Param>application
22/12/2025, 1:20:47.353 pm	Microsoft-Windows-Kernel-Ge...	System	DESKTOP-J8TS1EC	4	Information	<Param>47</Param
22/12/2025, 1:18:51.351 pm	Microsoft-Windows-Security-SPP	Application	DESKTOP-J8TS1EC	2	Error	<Param>hr=0x8000

3s 996ms Display time (UTC+00:00) 519 - 524 of 527

Confirm Security events are present

Event

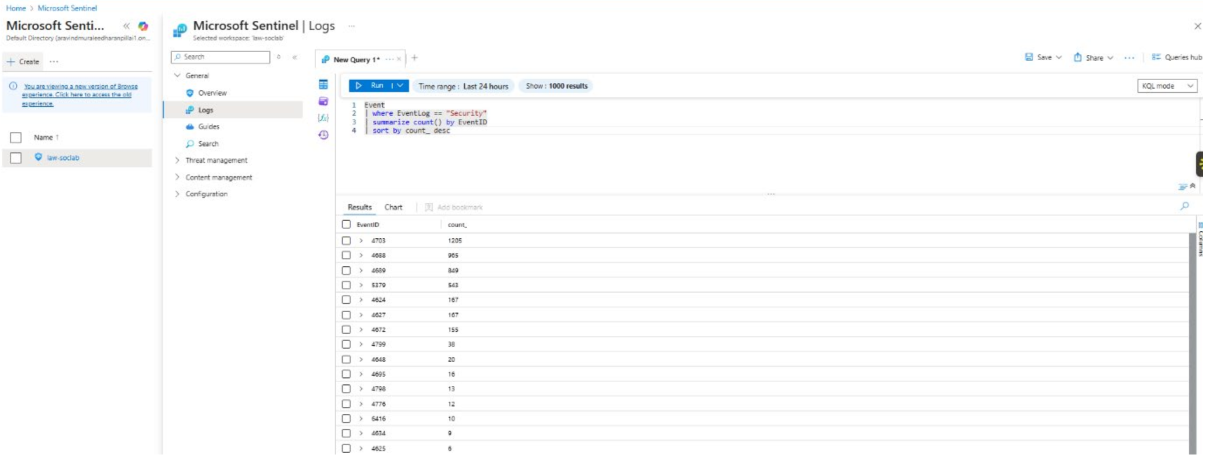
| where EventLog == "Security"

| where TimeGenerated > ago(24h)

| summarize count() by EventID

| sort by count_ desc

Screenshot



You are viewing a new version of Browse experience. Click here to access the old experience.

Time range : Last 24 hours

Show : 1000 results

```
Event
| where EventLog == "Security"
| summarize count() by EventID
| sort by count_ desc
```

EventID	count_
4703	1205
4688	965
4689	849
5379	543
4624	167
4627	167
4672	155
4799	38
4648	20
4695	16
4798	13
4776	12
6416	10
4634	9
4625	6

Query specific failed logons (4625)

Event

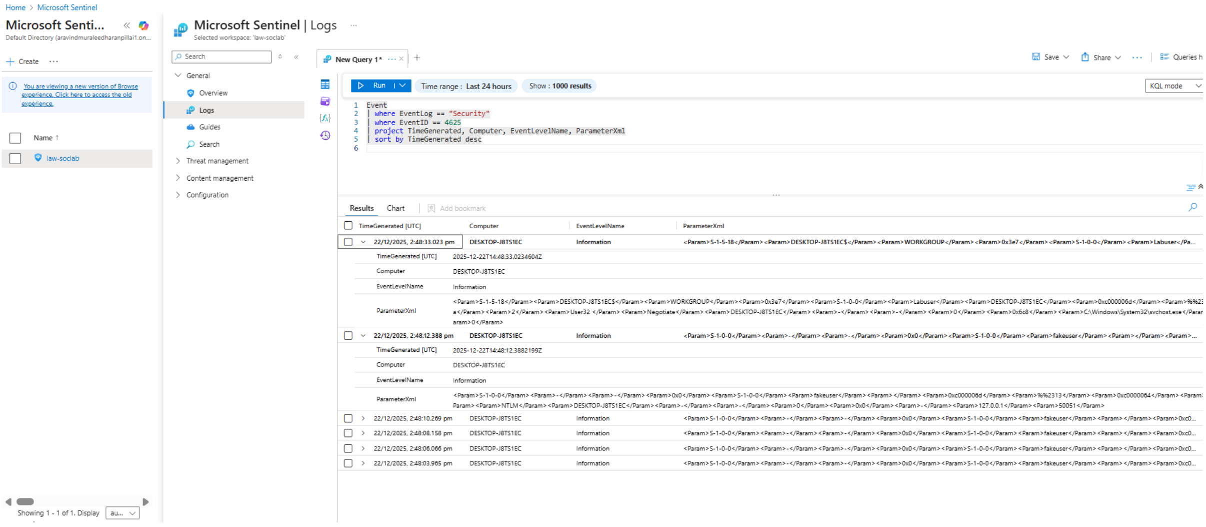
| where EventLog == "Security"

| where EventID == 4625

| project TimeGenerated, Computer, EventLevelName, ParameterXml

| sort by TimeGenerated desc

Screenshot



You are viewing a new version of Browse experience. Click here to access the old experience.

Time range : Last 24 hours

Show : 1000 results

```
Event
| where EventLog == "Security"
| where EventID == 4625
| project TimeGenerated, Computer, EventLevelName, ParameterXml
| sort by TimeGenerated desc
```

TimeGenerated [UTC]	Computer	EventLevelName	ParameterXml
22/12/2025, 2:48:33.023 pm	DESKTOP-J8TS1EC	Information	<Param>S-1-5-18</Param><Param>DESKTOP-J8TS1EC$</Param><Param>WORKGROUP</Param><Param>0x3e7</Param><Param>S-1-0-0</Param><Param>Labuser</Pa...
TimeGenerated [UTC]	2025-12-22T14:48:33.0234604Z		
Computer	DESKTOP-J8TS1EC		
EventLevelName	Information		
ParameterXml	<Param>S-1-5-18</Param><Param>DESKTOP-J8TS1EC$</Param><Param>WORKGROUP</Param><Param>0x3e7</Param><Param>S-1-0-0</Param><Param>Labuser</Param><Param>DESKTOP-J8TS1EC</Param><Param>0xc000006d</Param><Param>%%23 a</Param><Param>2</Param><Param>User32 </Param><Param>Negotiate</Param><Param>DESKTOP-J8TS1EC</Param><Param>-</Param><Param>-</Param><Param>0</Param><Param>0x6c8</Param><Param>C:\Windows\System32\svchost.exe</Parar aram>0</Param>		
22/12/2025, 2:48:12.388 pm	DESKTOP-J8TS1EC	Information	<Param>S-1-0-0</Param><Param>-</Param><Param>-</Param><Param>0x0</Param><Param>S-1-0-0</Param><Param>fakeuser</Param><Param></Param><Param>...
TimeGenerated [UTC]	2025-12-22T14:48:12.3882199Z		
Computer	DESKTOP-J8TS1EC		
EventLevelName	Information		
ParameterXml	<Param>S-1-0-0</Param><Param>-</Param><Param>-</Param><Param>0x0</Param><Param>S-1-0-0</Param><Param>fakeuser</Param><Param></Param><Param>0xc000006d</Param><Param>%%2313</Param><Param>0xc0000064</Param><Param: Param><Param>NTLM</Param><Param>DESKTOP-J8TS1EC</Param><Param>-</Param><Param>-</Param><Param>0</Param><Param>0x0</Param><Param>-</Param><Param>127.0.0.1</Param><Param>50051</Param>		
22/12/2025, 2:48:10.269 pm	DESKTOP-J8TS1EC	Information	<Param>S-1-0-0</Param><Param>-</Param><Param>-</Param><Param>0x0</Param><Param>S-1-0-0</Param><Param>fakeuser</Param><Param></Param><Param>0xc0...
22/12/2025, 2:48:08.158 pm	DESKTOP-J8TS1EC	Information	<Param>S-1-0-0</Param><Param>-</Param><Param>-</Param><Param>0x0</Param><Param>S-1-0-0</Param><Param>fakeuser</Param><Param></Param><Param>0xc0...
22/12/2025, 2:48:06.066 pm	DESKTOP-J8TS1EC	Information	<Param>S-1-0-0</Param><Param>-</Param><Param>-</Param><Param>0x0</Param><Param>S-1-0-0</Param><Param>fakeuser</Param><Param></Param><Param>0xc0...
22/12/2025, 2:48:03.965 pm	DESKTOP-J8TS1EC	Information	<Param>S-1-0-0</Param><Param>-</Param><Param>-</Param><Param>0x0</Param><Param>S-1-0-0</Param><Param>fakeuser</Param><Param></Param><Param>0xc0...

Step 7: Create the analytics rule in Microsoft Defender

Goal

Detect brute force style activity by identifying multiple failed logons within a short time window.

Rule logic used

This triggers when there are 5 or more failed logons on a host within 10 minutes.

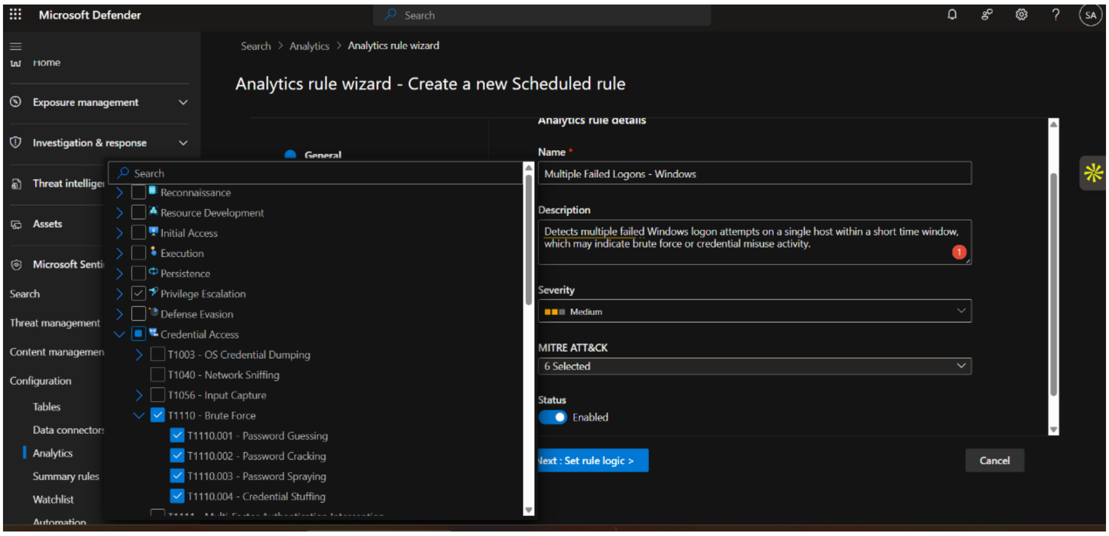
```
Event
| where EventLog == "Security"
| where EventID == 4625
| summarize FailedLogons = count() by Computer, bin(TimeGenerated, 10m)
| where FailedLogons >= 5
```

Recommended rule settings

- Run frequency: every 5 minutes
- Lookup data from: last 10 minutes
- Entity mapping: Host using Computer
- Create incidents: Enabled
- Grouping: group related alerts into a single incident (optional, but useful)

Screenshots

- Creating rule



Search > Analytics > Analytics rule wizard

Analytics rule wizard - Create a new Scheduled rule

Analytics rule details

Name *: Multiple Failed Logons - Windows

Description: Detects multiple failed Windows logon attempts on a single host within a short time window, which may indicate brute force or credential misuse activity.

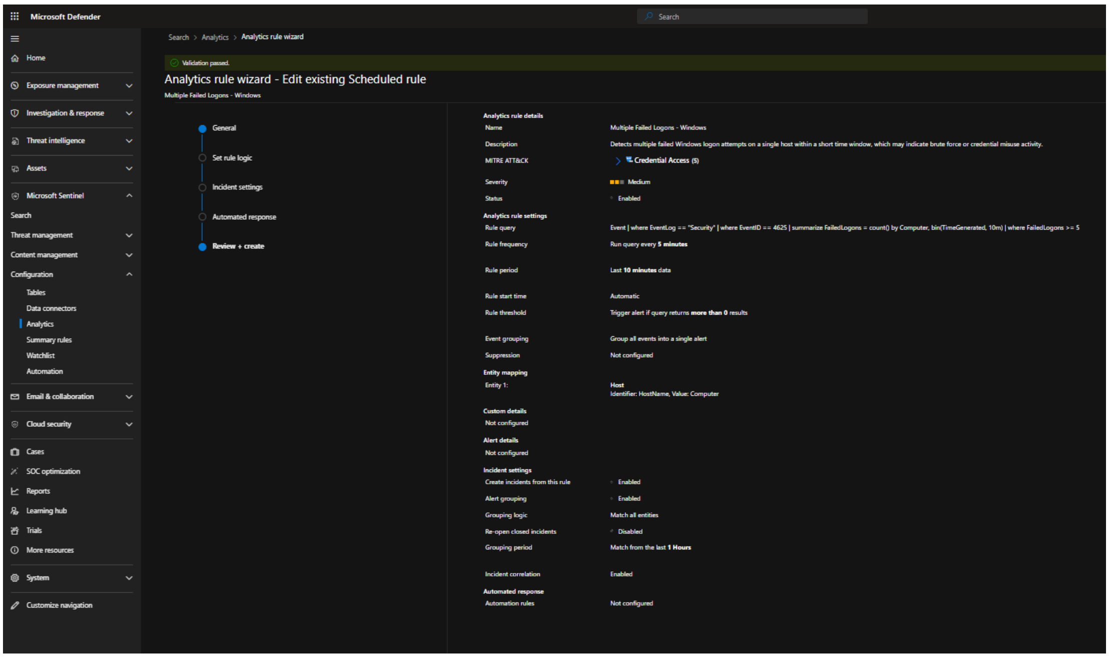
Severity: Medium

MITRE ATT&CK: 6 Selected

Status: Enabled

- □ Reconnaissance
- □ Resource Development
- □ Initial Access
- □ Execution
- □ Persistence
- ☑ Privilege Escalation
- □ Defense Evasion
- ■ Credential Access
  - □ T1003 - OS Credential Dumping
  - □ T1040 - Network Sniffing
  - □ T1056 - Input Capture
  - ☑ T1110 - Brute Force
    - ☑ T1110.001 - Password Guessing
    - ☑ T1110.002 - Password Cracking
    - ☑ T1110.003 - Password Spraying
    - ☑ T1110.004 - Credential Stuffing

- Final rule settings page



Validation passed.

Analytics rule wizard - Edit existing Scheduled rule

Multiple Failed Logons - Windows

Analytics rule details

Name	Multiple Failed Logons - Windows
Description	Detects multiple failed Windows logon attempts on a single host within a short time window, which may indicate brute force or credential misuse activity.
MITRE ATT&CK	Credential Access (5)
Severity	Medium
Status	Enabled

Analytics rule settings

Rule query	Event | where EventLog == "Security" | where EventID == 4625 | summarize FailedLogons = count() by Computer, bin(TimeGenerated, 10m) | where FailedLogons >= 5
Rule frequency	Run query every **5 minutes**
Rule period	Last **10 minutes** data
Rule start time	Automatic
Rule threshold	Trigger alert if query returns **more than 0** results
Event grouping	Group all events into a single alert
Suppression	Not configured

Entity mapping

Entity 1:	**Host** Identifier: HostName, Value: Computer

Custom details

Not configured

Alert details

Not configured

Incident settings

Create incidents from this rule	Enabled
Alert grouping	Enabled
Grouping logic	Match all entities
Re-open closed incidents	Disabled
Grouping period	Match from the last **1 Hours**
Incident correlation	Enabled

Automated response

Automation rules	Not configured

Step 8: Confirm incidents appear

Where to find incidents in Defender

Microsoft Defender portal → Investigation and response → Incidents

If the list is empty, that's normal until the rule runs and the condition is met. Trigger it by intentionally generating a few failed logons on the VM.

Final result

At the end of this lab, I had:

- A Windows VM generating security logs
- Azure Arc connection working
- Azure Monitor Agent installed
- Data Collection Rule collecting Security logs
- Logs visible in the Event table
- A detection rule for failed logon bursts
- Incidents view available in Defender