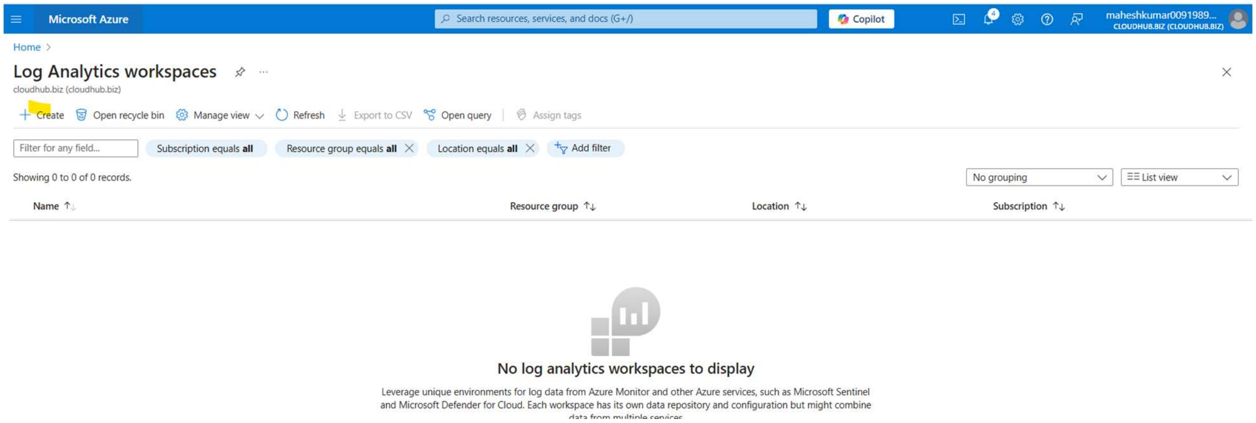
Create log analytics workspace



Log Analytics workspaces

cloudhub.biz (cloudhub.biz)

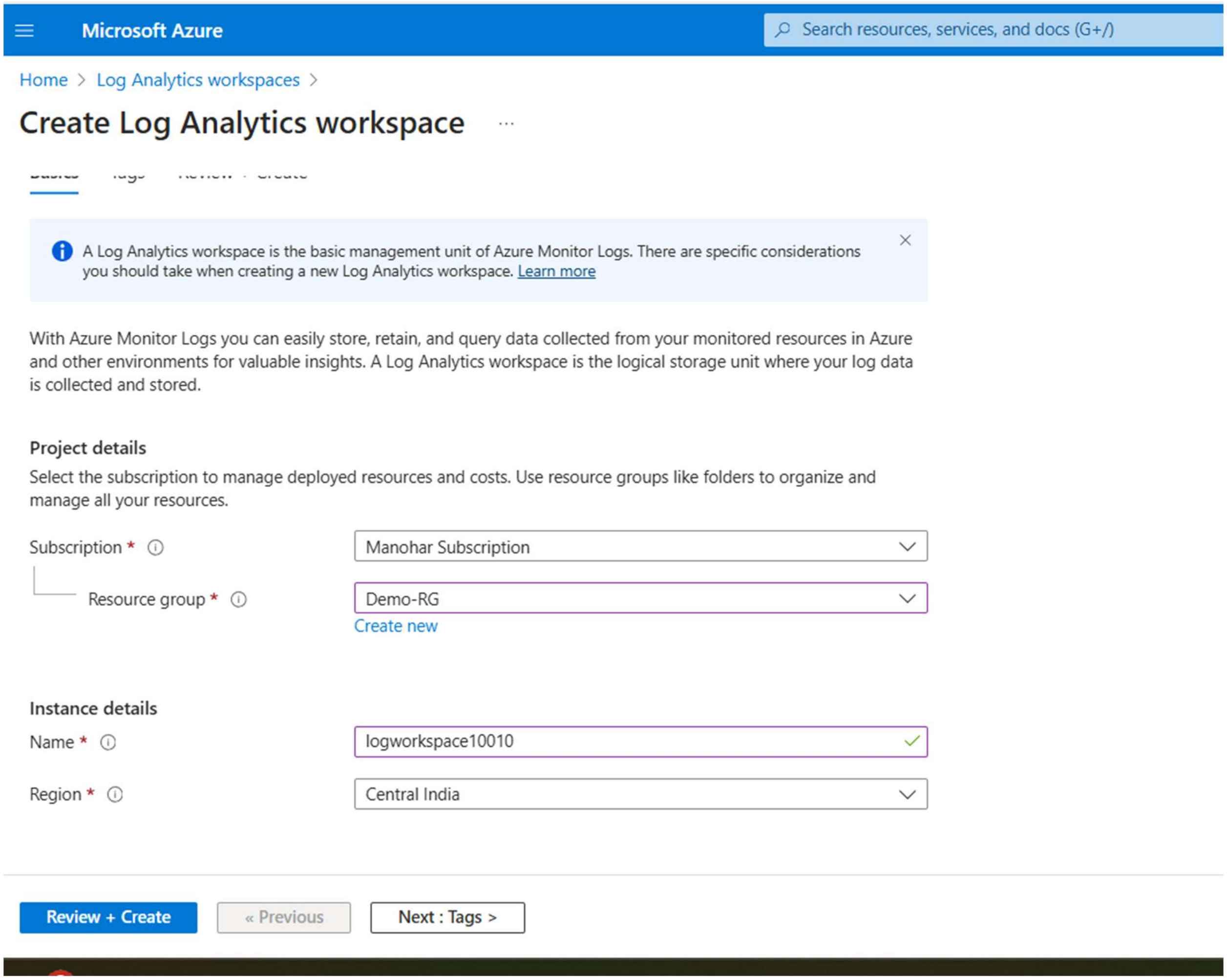
Subscription equals **all** | Resource group equals **all** | Location equals **all**

Showing 0 to 0 of 0 records.

Name	Resource group	Location	Subscription

No log analytics workspaces to display

Leverage unique environments for log data from Azure Monitor and other Azure services, such as Microsoft Sentinel and Microsoft Defender for Cloud. Each workspace has its own data repository and configuration but might combine data from multiple services



Create Log Analytics workspace

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

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

Project details

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

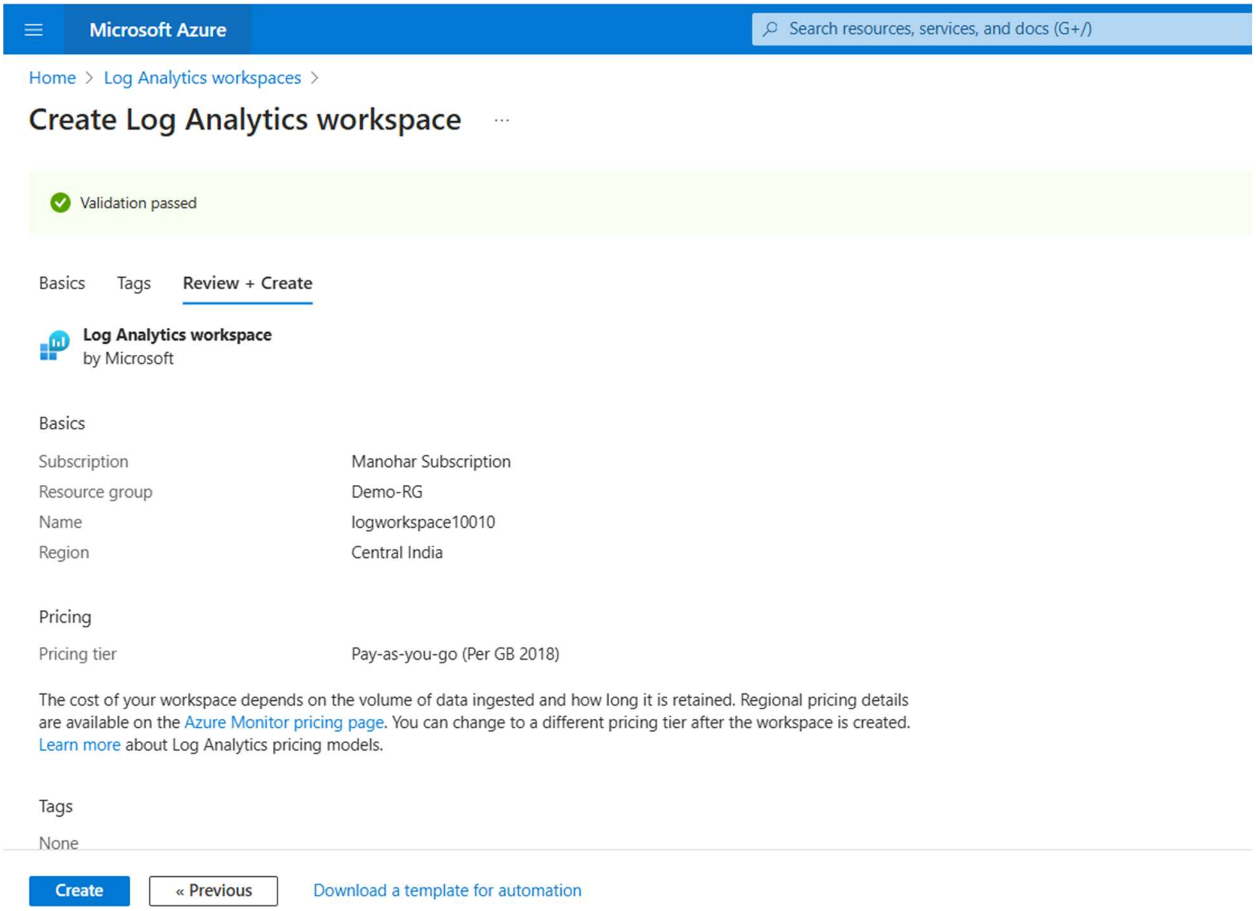
Subscription * : Manohar Subscription

Resource group * : Demo-RG

Instance details

Name * : logworkspace10010

Region * : Central India


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Log Analytics workspaces >

Create Log Analytics workspace ...

Validation passed

Basics
Tags
Review + Create

Log Analytics workspace
by Microsoft

Basics

Subscription	Manohar Subscription
Resource group	Demo-RG
Name	logworkspace10010
Region	Central India

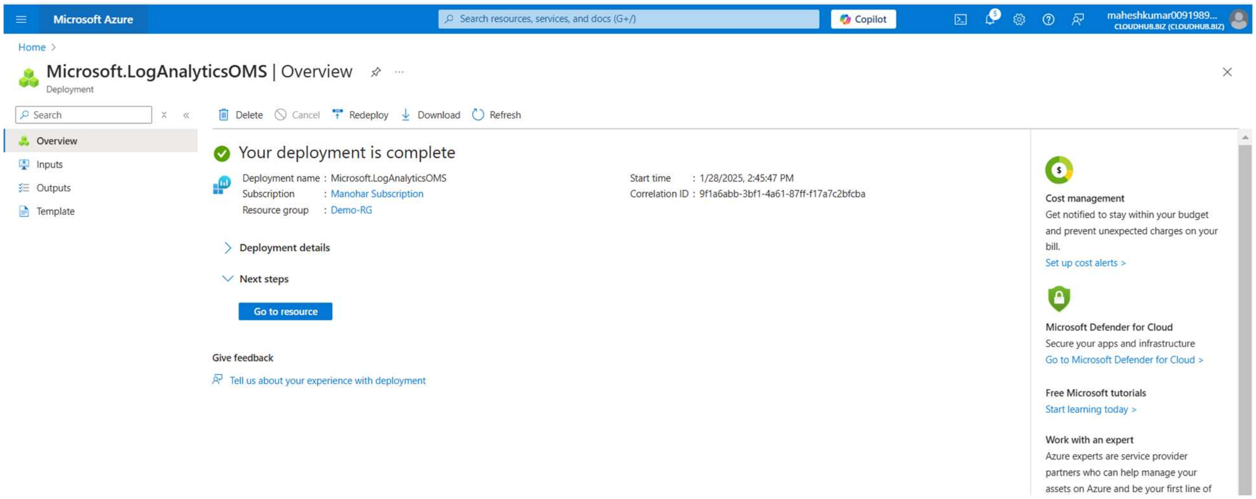
Pricing

Pricing tier	Pay-as-you-go (Per GB 2018)

The cost of your workspace depends on the volume of data ingested and how long it is retained. Regional pricing details are available on the Azure Monitor pricing page. You can change to a different pricing tier after the workspace is created. Learn more about Log Analytics pricing models.

Tags

None


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
maheshkumar0091989...
CLOUDHUB.BIZ (CLOUDHUB.BIZ)
Home >

Microsoft.LogAnalyticsOMS | Overview
Deployment

Your deployment is complete

Deployment name : Microsoft.LogAnalyticsOMS
Subscription : Manohar Subscription
Resource group : Demo-RG

Start time : 1/28/2025, 2:45:47 PM
Correlation ID : 9f1a6abb-3bf1-4a61-87ff-f17a7c2bfcba

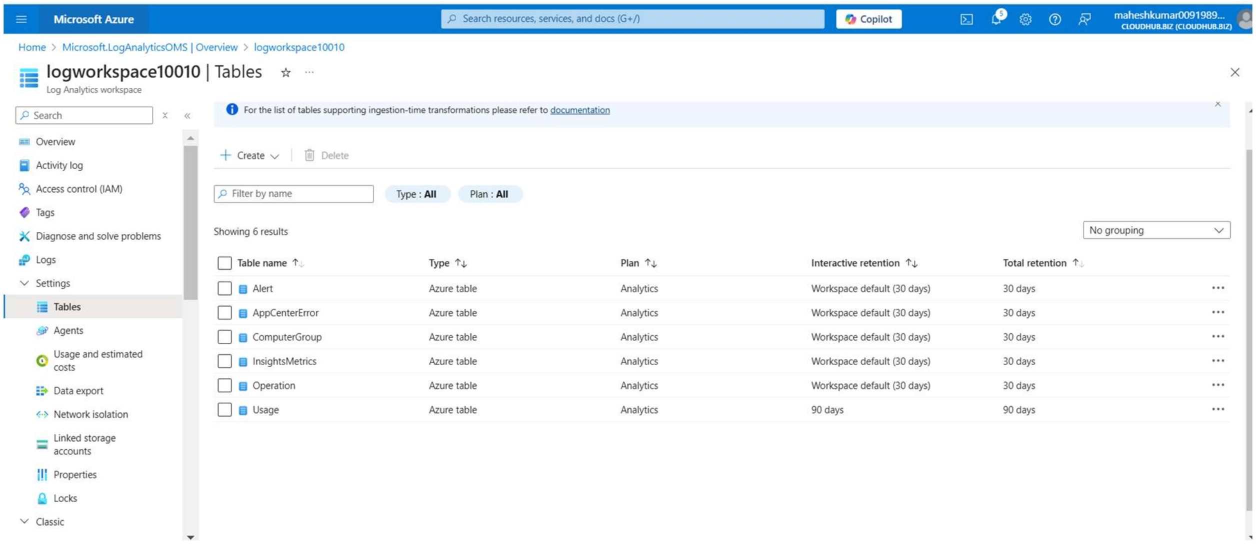
Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >

Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >

Free Microsoft tutorials
Start learning today >

Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of

Inbuilt tables in workspace

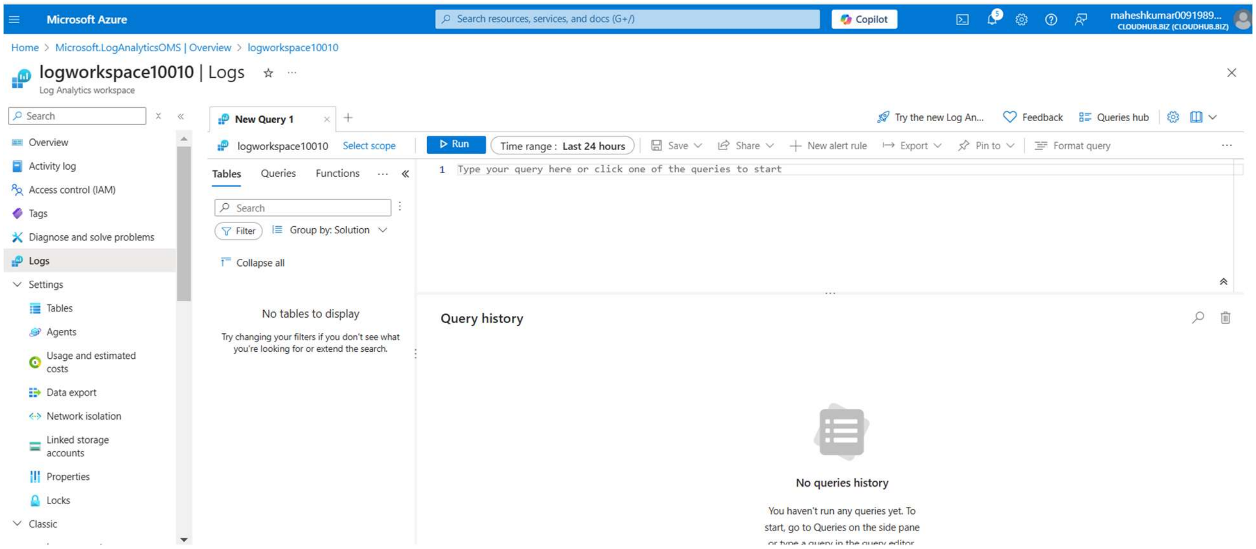


For the list of tables supporting ingestion-time transformations please refer to documentation

Showing 6 results

Table name	Type	Plan	Interactive retention	Total retention
Alert	Azure table	Analytics	Workspace default (30 days)	30 days
AppCenterError	Azure table	Analytics	Workspace default (30 days)	30 days
ComputerGroup	Azure table	Analytics	Workspace default (30 days)	30 days
InsightsMetrics	Azure table	Analytics	Workspace default (30 days)	30 days
Operation	Azure table	Analytics	Workspace default (30 days)	30 days
Usage	Azure table	Analytics	90 days	90 days

Currently we don’t see any logs becoz no logs have been sent to the log analytics workspace



```
1  Type your query here or click one of the queries to start
```

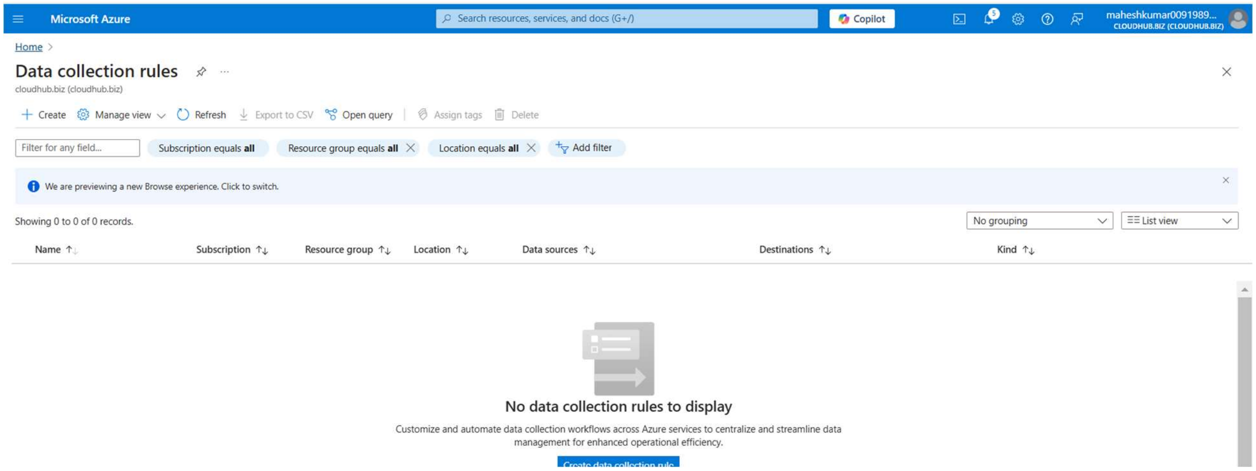
No tables to display

Try changing your filters if you don't see what you're looking for or extend the search.

No queries history

You haven't run any queries yet. To start, go to Queries on the side pane or type a query in the query editor

In order to send logs to the log analytics workspace we need to create data collection rule.



Data collection rules

cloudhub.biz (cloudhub.biz)

Subscription equals **all** | Resource group equals **all** | Location equals **all**

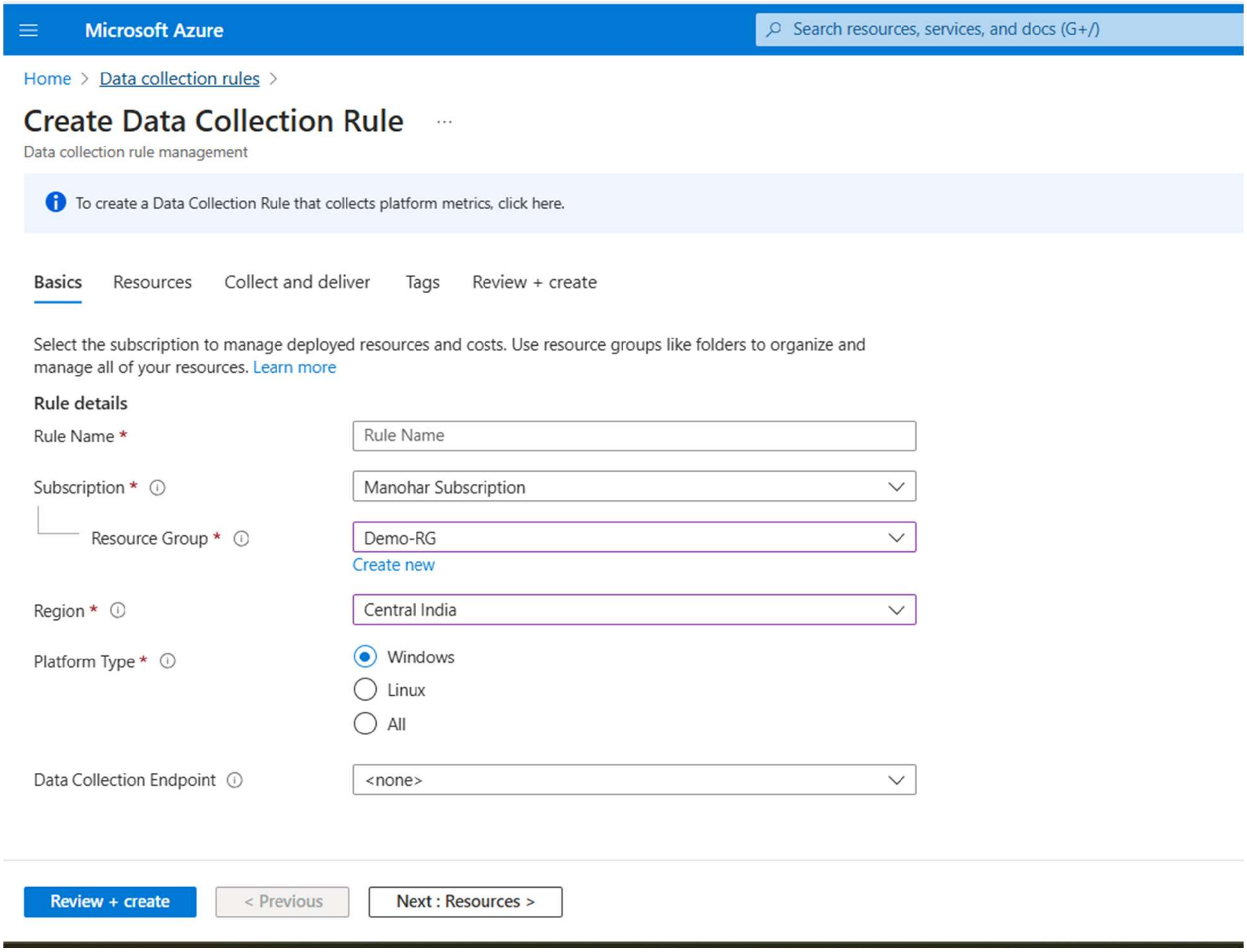
We are previewing a new Browse experience. Click to switch.

Showing 0 to 0 of 0 records.

Name	Subscription	Resource group	Location	Data sources	Destinations	Kind

No data collection rules to display

Customize and automate data collection workflows across Azure services to centralize and streamline data management for enhanced operational efficiency.



Create Data Collection Rule

Data collection rule management

To create a Data Collection Rule that collects platform metrics, click here.

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

Rule details

Rule Name * : Rule Name

Subscription * : Manohar Subscription

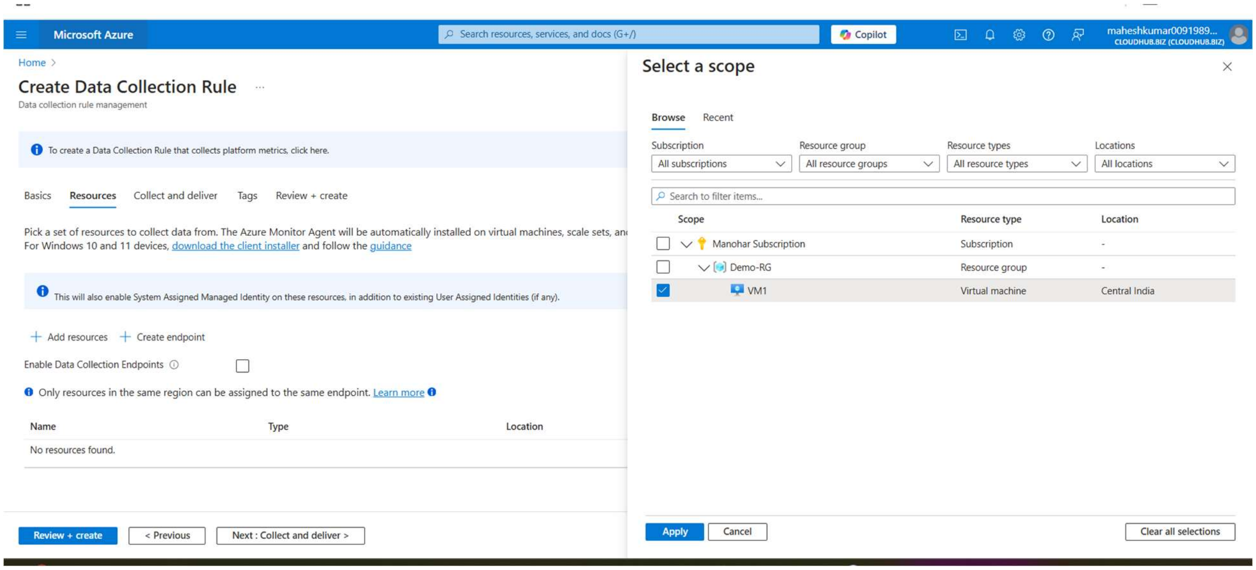
Resource Group * : Demo-RG

Region * : Central India

Platform Type * : ● Windows ○ Linux ○ All

Data Collection Endpoint : <none>

Add VM as a resource



Microsoft Azure — Search resources, services, and docs (G+/) — Copilot — maheshkumar0091989... CLOUDHUB.BIZ (CLOUDHUB.BIZ)

Home >

Create Data Collection Rule ...

Data collection rule management

To create a Data Collection Rule that collects platform metrics, click here.

Basics | **Resources** | Collect and deliver | Tags | Review + create

Pick a set of resources to collect data from. The Azure Monitor Agent will be automatically installed on virtual machines, scale sets, an
For Windows 10 and 11 devices, download the client installer and follow the guidance

This will also enable System Assigned Managed Identity on these resources, in addition to existing User Assigned Identities (if any).

+ Add resources + Create endpoint

Enable Data Collection Endpoints ⓘ □

Only resources in the same region can be assigned to the same endpoint. Learn more

Name	Type	Location
No resources found.		

Review + create | < Previous | Next : Collect and deliver >

Select a scope

Browse | Recent

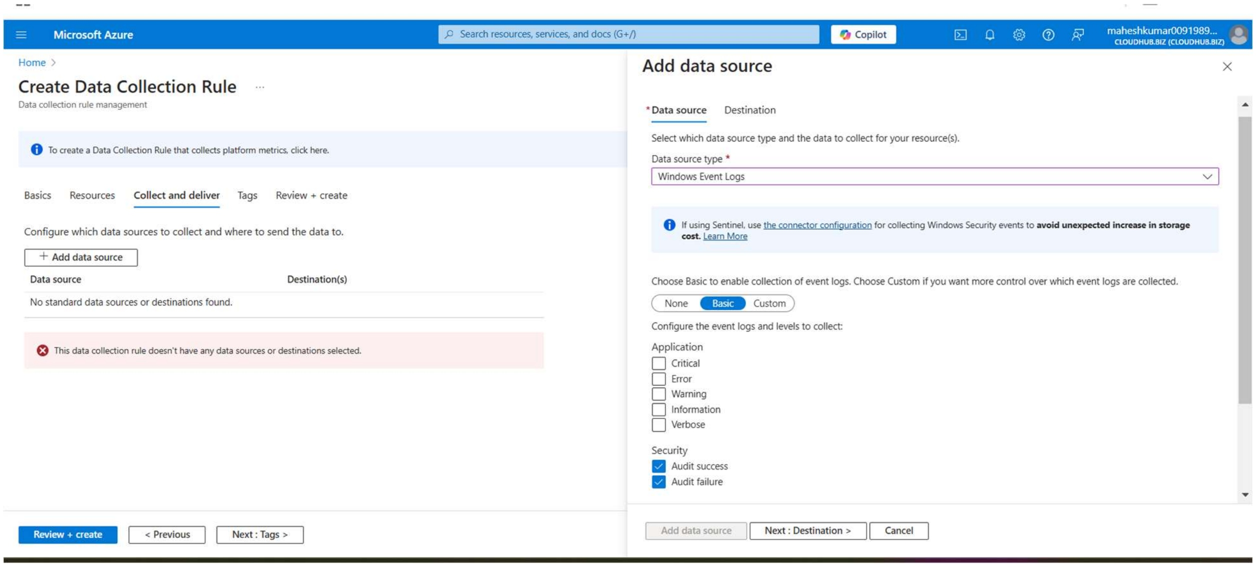
Subscription: All subscriptions — Resource group: All resource groups — Resource types: All resource types — Locations: All locations

Search to filter items...

	Scope	Resource type	Location
□	Manohar Subscription	Subscription	-
□	Demo-RG	Resource group	-
☑	VM1	Virtual machine	Central India

Apply | Cancel | Clear all selections

We will capture the windows event logs & in terms of security logs we will capture the audit success and audit failure.



Microsoft Azure — Search resources, services, and docs (G+/) — Copilot — maheshkumar0091989... CLOUDHUB.BIZ (CLOUDHUB.BIZ)

Home >

Create Data Collection Rule ...

Data collection rule management

To create a Data Collection Rule that collects platform metrics, click here.

Basics | Resources | **Collect and deliver** | Tags | Review + create

Configure which data sources to collect and where to send the data to.

+ Add data source

Data source	Destination(s)
No standard data sources or destinations found.	

This data collection rule doesn't have any data sources or destinations selected.

Review + create | < Previous | Next : Tags >

Add data source

* Data source | Destination

Select which data source type and the data to collect for your resource(s).

Data source type *: Windows Event Logs

If using Sentinel, use the connector configuration for collecting Windows Security events to **avoid unexpected increase in storage cost.** Learn More

Choose Basic to enable collection of event logs. Choose Custom if you want more control over which event logs are collected.

None | **Basic** | Custom

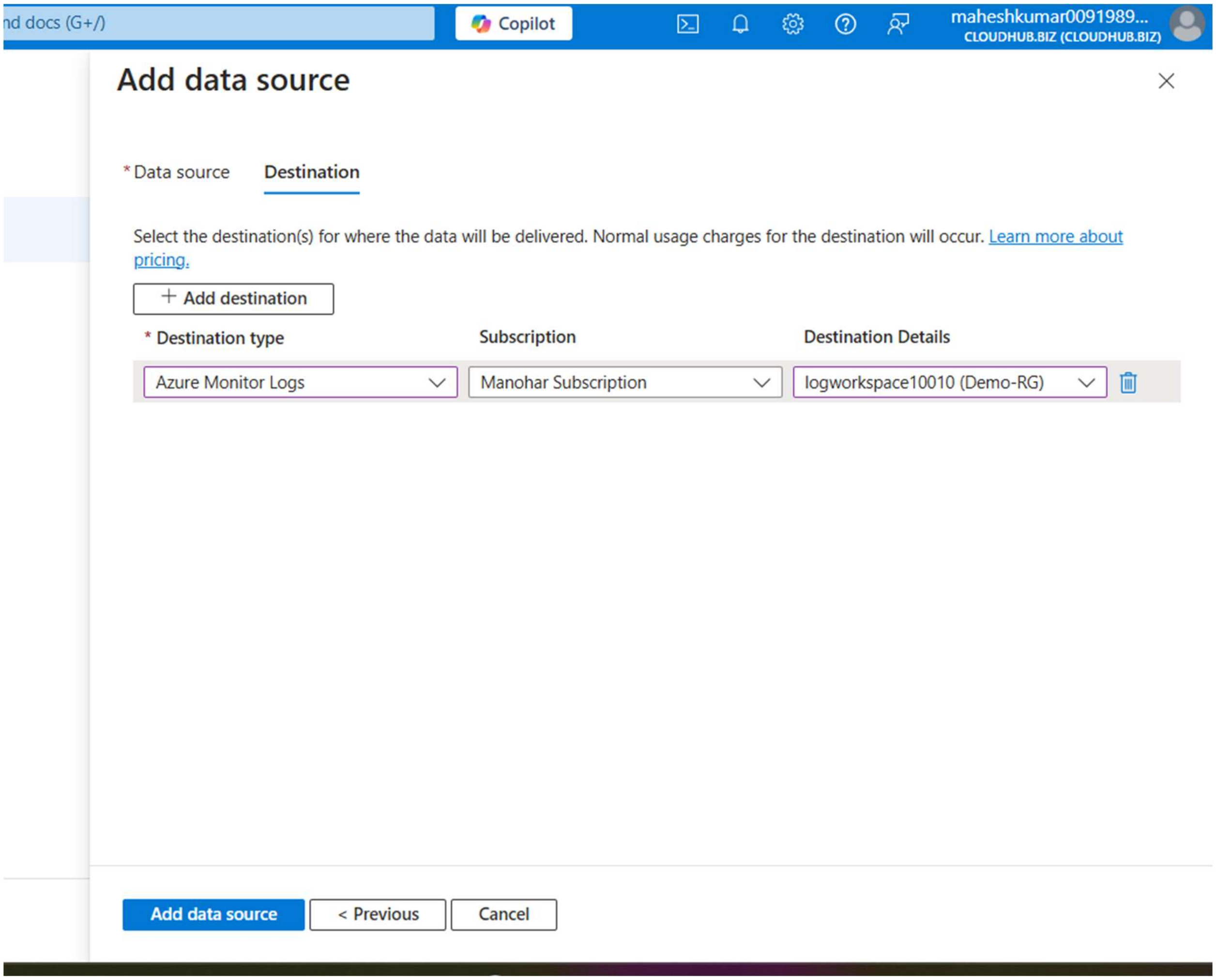
Configure the event logs and levels to collect:

Application
- □ Critical
- □ Error
- □ Warning
- □ Information
- □ Verbose

Security
- ☑ Audit success
- ☑ Audit failure

Add data source | Next : Destination > | Cancel

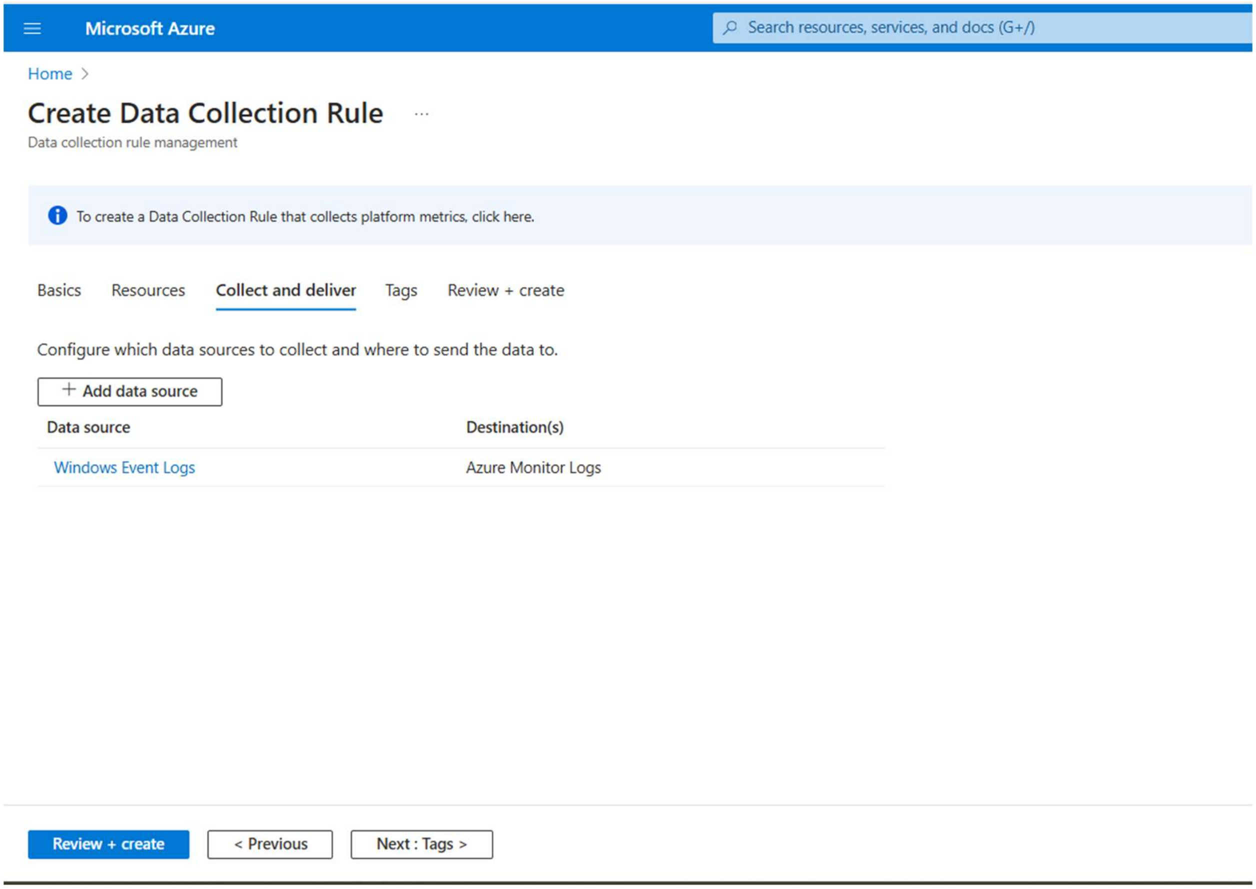
in the destination we will add log analytics workspace



Add data source

Select the destination(s) for where the data will be delivered. Normal usage charges for the destination will occur. Learn more about pricing.

* Destination type	Subscription	Destination Details
Azure Monitor Logs	Manohar Subscription	logworkspace10010 (Demo-RG)



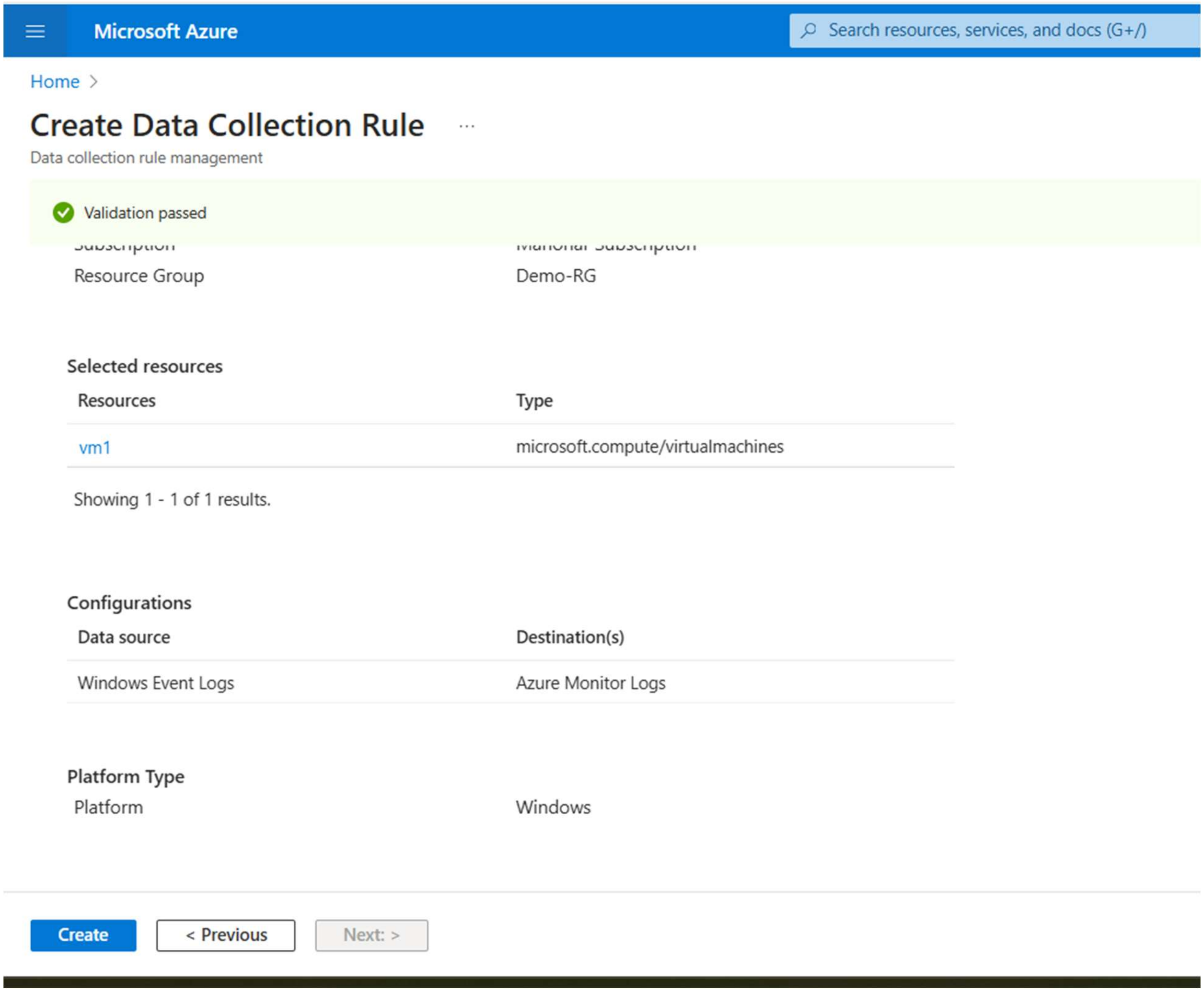
Create Data Collection Rule ...

Data collection rule management

To create a Data Collection Rule that collects platform metrics, click here.

Configure which data sources to collect and where to send the data to.

Data source	Destination(s)
Windows Event Logs	Azure Monitor Logs


Microsoft Azure
Search resources, services, and docs (G+/)
Home >
Create Data Collection Rule
Data collection rule management
Validation passed

Subscription	Manohar Subscription
Resource Group	Demo-RG

Selected resources

Resources	Type
vm1	microsoft.compute/virtualmachines

Showing 1 - 1 of 1 results.

Configurations

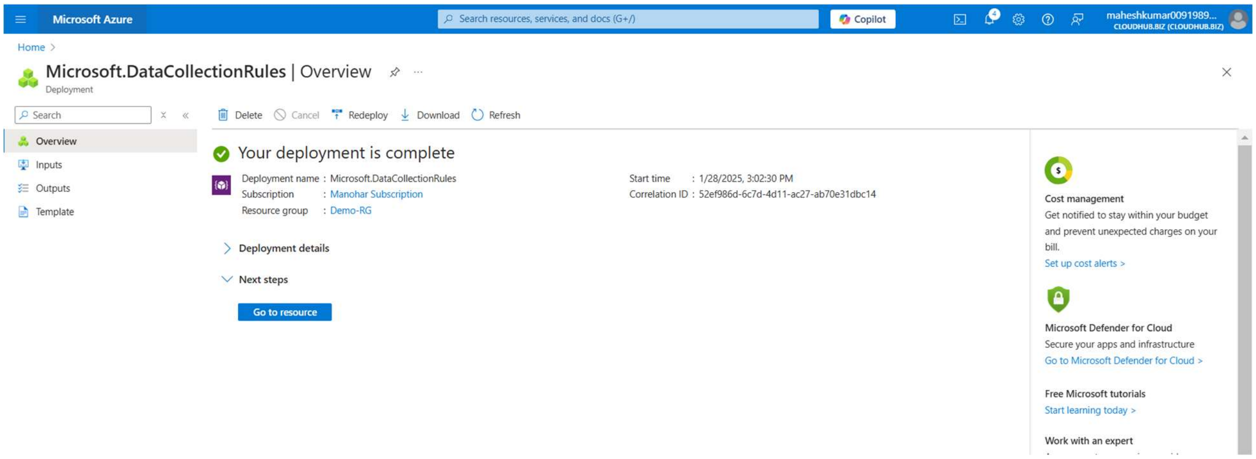
Data source	Destination(s)
Windows Event Logs	Azure Monitor Logs

Platform Type

Platform	Windows

Create
< Previous
Next: >

Data collection rule has been created successfully



Your deployment is complete

Deployment name : Microsoft.DataCollectionRules
Subscription : Manohar Subscription
Resource group : Demo-RG

Start time : 1/28/2025, 3:02:30 PM
Correlation ID : 52ef986d-6c7d-4d11-ac27-ab70e31dbc14

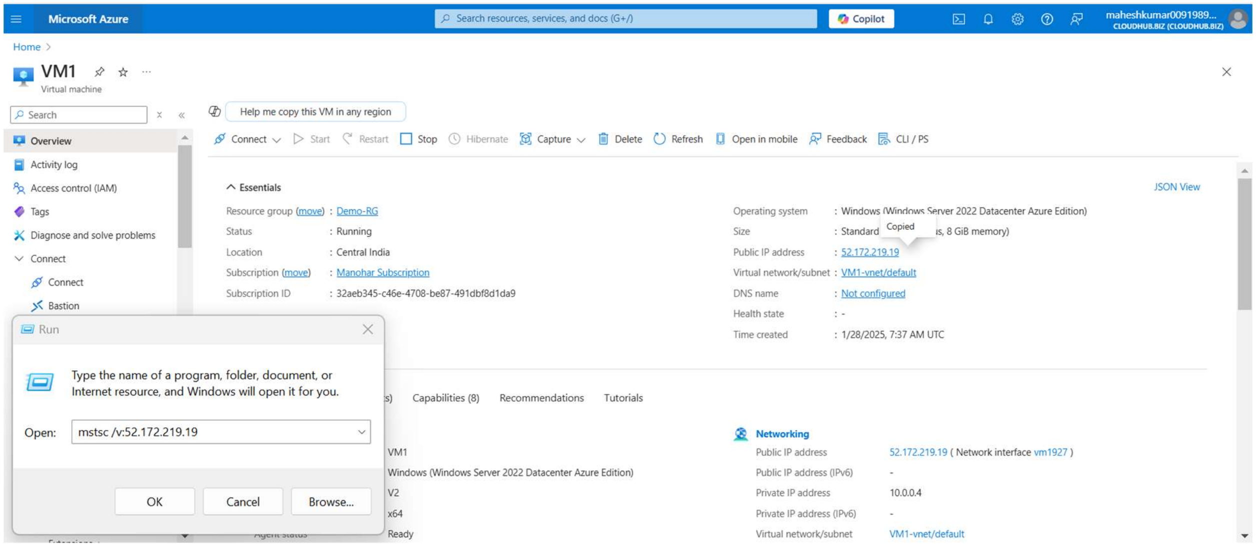
Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >

Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >

Free Microsoft tutorials
Start learning today >

Work with an expert

Login to the VM



Resource group (move) : Demo-RG
Status : Running
Location : Central India
Subscription (move) : Manohar Subscription
Subscription ID : 32aeb345-c46e-4708-be87-491dbf8d1da9

Operating system : Windows (Windows Server 2022 Datacenter Azure Edition)
Size : Standard s, 8 GiB memory)
Public IP address : 52.172.219.19
Virtual network/subnet : VM1-vnet/default
DNS name : Not configured
Health state : -
Time created : 1/28/2025, 7:37 AM UTC

VM1
Windows (Windows Server 2022 Datacenter Azure Edition)
V2
x64
Agent status Ready

Public IP address 52.172.219.19 (Network interface vm1927)
Public IP address (IPv6) -
Private IP address 10.0.0.4
Private IP address (IPv6) -
Virtual network/subnet VM1-vnet/default

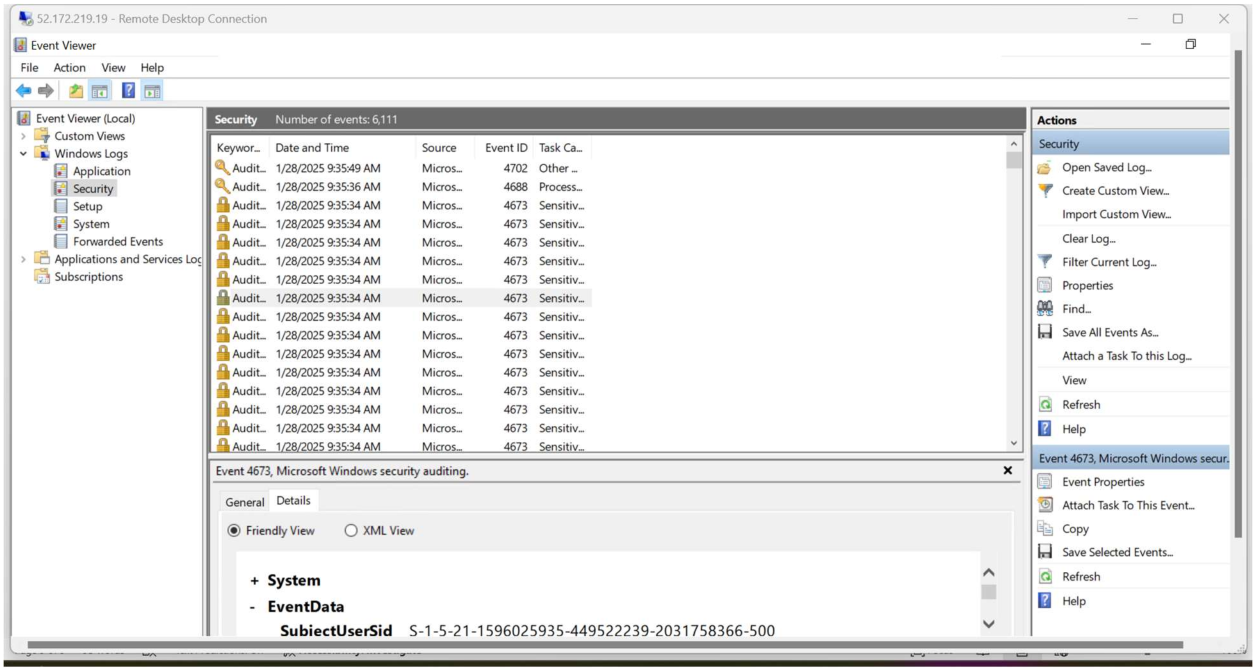
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mstsc /v:52.172.219.19

OK Cancel Browse...

Once login open the event viewer and expand windows logs and click on security. So below logs will be capturing in the log analytics workspace



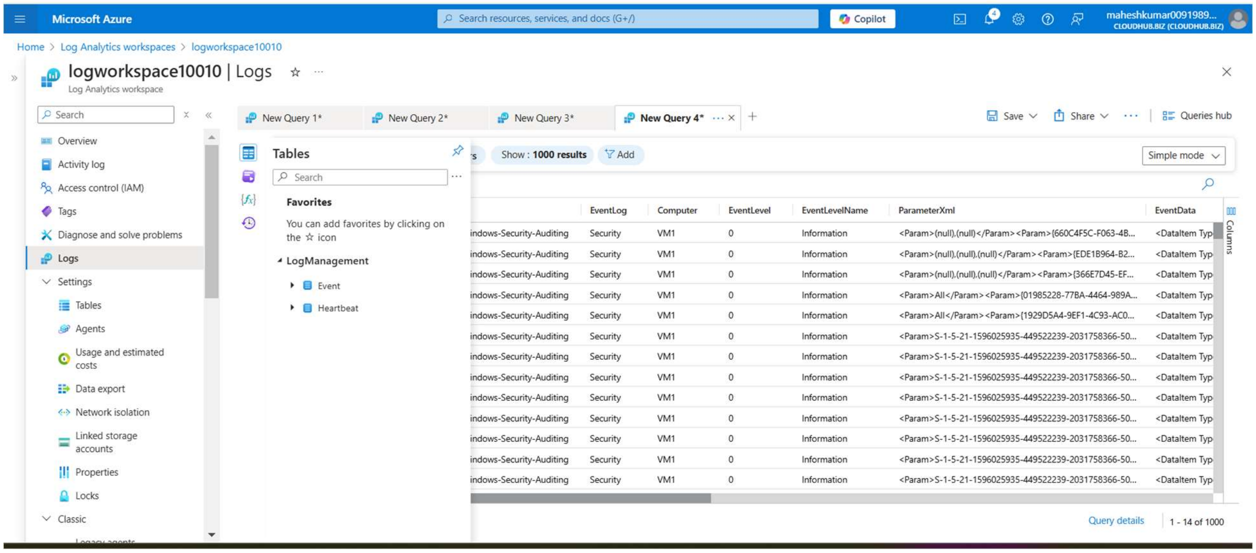
Security Number of events: 6,111

Keywor...	Date and Time	Source	Event ID	Task Ca...
Audit...	1/28/2025 9:35:49 AM	Micros...	4702	Other ...
Audit...	1/28/2025 9:35:36 AM	Micros...	4688	Process...
Audit...	1/28/2025 9:35:34 AM	Micros...	4673	Sensitiv...
Audit...	1/28/2025 9:35:34 AM	Micros...	4673	Sensitiv...
Audit...	1/28/2025 9:35:34 AM	Micros...	4673	Sensitiv...
Audit...	1/28/2025 9:35:34 AM	Micros...	4673	Sensitiv...
Audit...	1/28/2025 9:35:34 AM	Micros...	4673	Sensitiv...
Audit...	1/28/2025 9:35:34 AM	Micros...	4673	Sensitiv...
Audit...	1/28/2025 9:35:34 AM	Micros...	4673	Sensitiv...
Audit...	1/28/2025 9:35:34 AM	Micros...	4673	Sensitiv...
Audit...	1/28/2025 9:35:34 AM	Micros...	4673	Sensitiv...
Audit...	1/28/2025 9:35:34 AM	Micros...	4673	Sensitiv...
Audit...	1/28/2025 9:35:34 AM	Micros...	4673	Sensitiv...
Audit...	1/28/2025 9:35:34 AM	Micros...	4673	Sensitiv...
Audit...	1/28/2025 9:35:34 AM	Micros...	4673	Sensitiv...
Audit...	1/28/2025 9:35:34 AM	Micros...	4673	Sensitiv...
Audit...	1/28/2025 9:35:34 AM	Micros...	4673	Sensitiv...

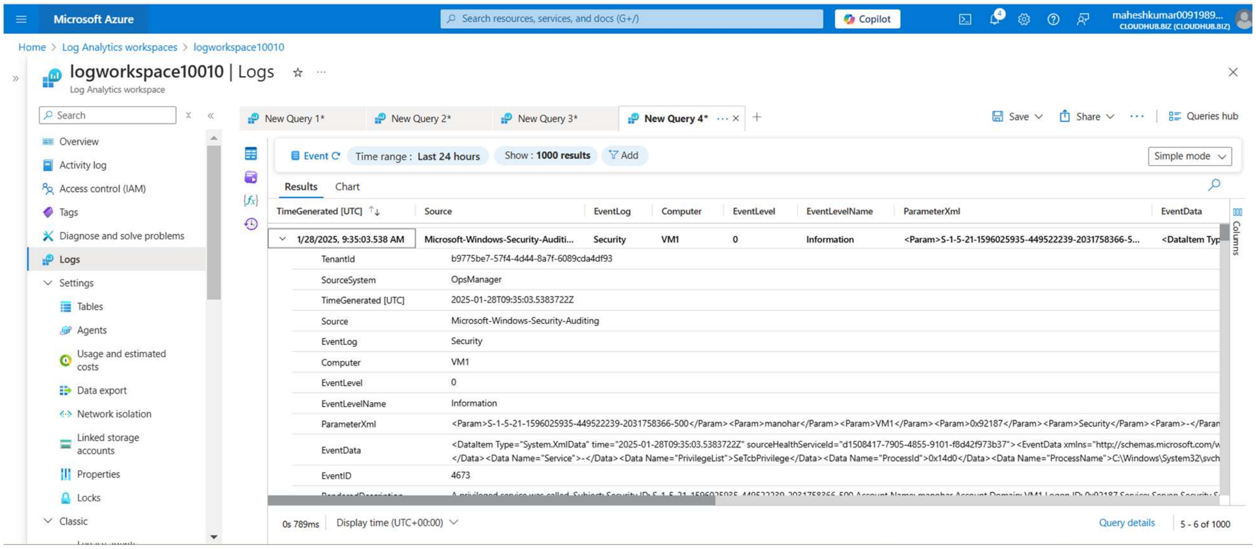
Event 4673, Microsoft Windows security auditing.

+ System
- EventData
SubjectUserSid S-1-5-21-1596025935-449522239-2031758366-500

All the logs has been sent successfully to the log analytics workspace



	EventLog	Computer	EventLevel	EventLevelName	ParameterXml	EventData
indows-Security-Auditing	Security	VM1	0	Information	<Param>(null).(null)</Param><Param>{660C4F5C-F063-4B...	<DataItem Typ
indows-Security-Auditing	Security	VM1	0	Information	<Param>(null).(null).(null)</Param><Param>{EDE1B964-B2...	<DataItem Typ
indows-Security-Auditing	Security	VM1	0	Information	<Param>(null).(null).(null)</Param><Param>{366E7D45-EF...	<DataItem Typ
indows-Security-Auditing	Security	VM1	0	Information	<Param>All</Param><Param>{01985228-77BA-4464-989A...	<DataItem Typ
indows-Security-Auditing	Security	VM1	0	Information	<Param>All</Param><Param>{1929D5A4-9EF1-4C93-AC0...	<DataItem Typ
indows-Security-Auditing	Security	VM1	0	Information	<Param>S-1-5-21-1596025935-449522239-2031758366-50...	<DataItem Typ
indows-Security-Auditing	Security	VM1	0	Information	<Param>S-1-5-21-1596025935-449522239-2031758366-50...	<DataItem Typ
indows-Security-Auditing	Security	VM1	0	Information	<Param>S-1-5-21-1596025935-449522239-2031758366-50...	<DataItem Typ
indows-Security-Auditing	Security	VM1	0	Information	<Param>S-1-5-21-1596025935-449522239-2031758366-50...	<DataItem Typ
indows-Security-Auditing	Security	VM1	0	Information	<Param>S-1-5-21-1596025935-449522239-2031758366-50...	<DataItem Typ
indows-Security-Auditing	Security	VM1	0	Information	<Param>S-1-5-21-1596025935-449522239-2031758366-50...	<DataItem Typ
indows-Security-Auditing	Security	VM1	0	Information	<Param>S-1-5-21-1596025935-449522239-2031758366-50...	<DataItem Typ
indows-Security-Auditing	Security	VM1	0	Information	<Param>S-1-5-21-1596025935-449522239-2031758366-50...	<DataItem Typ



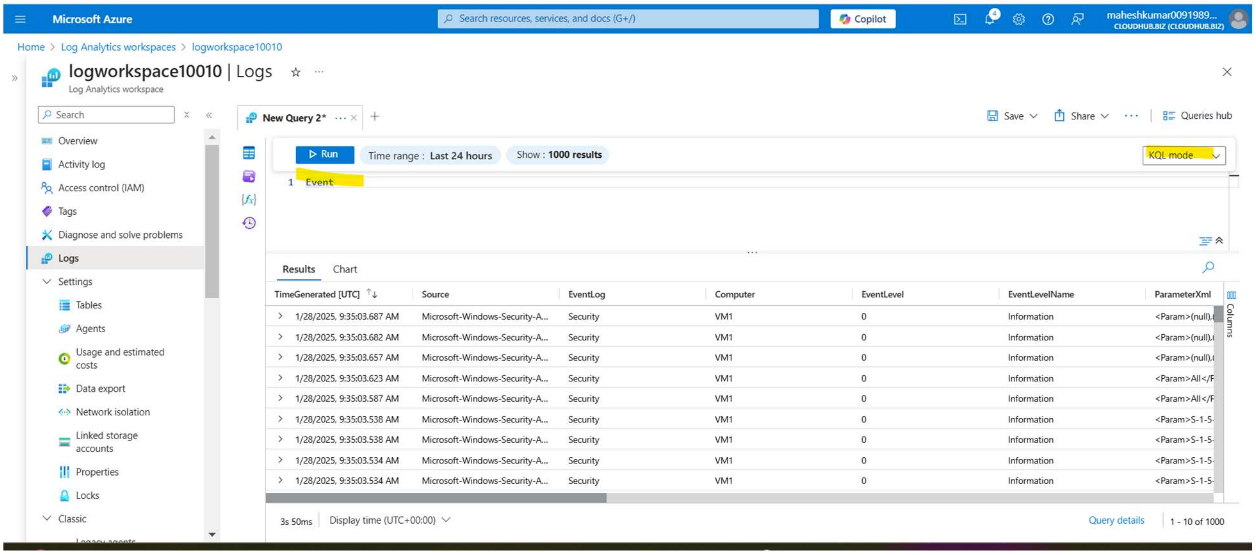
TimeGenerated [UTC]	Source	EventLog	Computer	EventLevel	EventLevelName	ParameterXml	EventData
1/28/2025, 9:35:03.538 AM	Microsoft-Windows-Security-Auditi...	Security	VM1	0	Information	<Param>S-1-5-21-1596025935-449522239-2031758366-5...	<DataItem Typ

TenantId	b9775be7-57f4-4d44-8a7f-6089cda4df93
SourceSystem	OpsManager
TimeGenerated [UTC]	2025-01-28T09:35:03.5383722Z
Source	Microsoft-Windows-Security-Auditing
EventLog	Security
Computer	VM1
EventLevel	0
EventLevelName	Information
ParameterXml	<Param>S-1-5-21-1596025935-449522239-2031758366-500</Param><Param>manohar</Param><Param>VM1</Param><Param>0x92187</Param><Param>Security</Param><Param>-</Paran
EventData	<DataItem Type="System.XmlData" time="2025-01-28T09:35:03.5383722Z" sourceHealthServiceId="d1508417-7905-4855-9101-f8d42f973b37"><EventData xmlns="http://schemas.microsoft.com/w </Data><Data Name="Service">-</Data><Data Name="PrivilegeList">SeTcbPrivilege</Data><Data Name="ProcessId">0x14d0</Data><Data Name="ProcessName">C:\Windows\System32\svch
EventID	4673

Now we can run certain queries in log analytics workspace & search through the data within the tables in log analytics workspace.

We will use the kusto query language

If I want to see all of the records within the table.



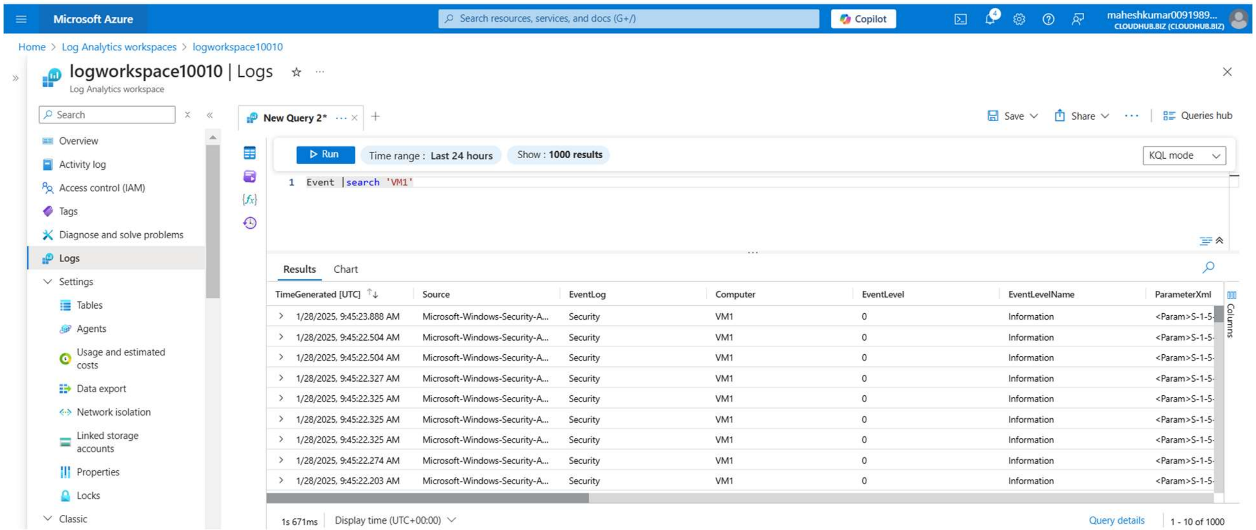
Time range : Last 24 hours Show : 1000 results KQL mode

```
Event
```

TimeGenerated [UTC]	Source	EventLog	Computer	EventLevel	EventLevelName	ParameterXml
1/28/2025, 9:35:03.687 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>(null),
1/28/2025, 9:35:03.682 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>(null),
1/28/2025, 9:35:03.657 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>(null),
1/28/2025, 9:35:03.623 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>All</F
1/28/2025, 9:35:03.587 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>All</F
1/28/2025, 9:35:03.538 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-
1/28/2025, 9:35:03.538 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-
1/28/2025, 9:35:03.534 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-
1/28/2025, 9:35:03.534 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-

3s 50ms Display time (UTC+00:00) Query details 1 - 10 of 1000

Free text search- I want to search the data which contains the text VM1



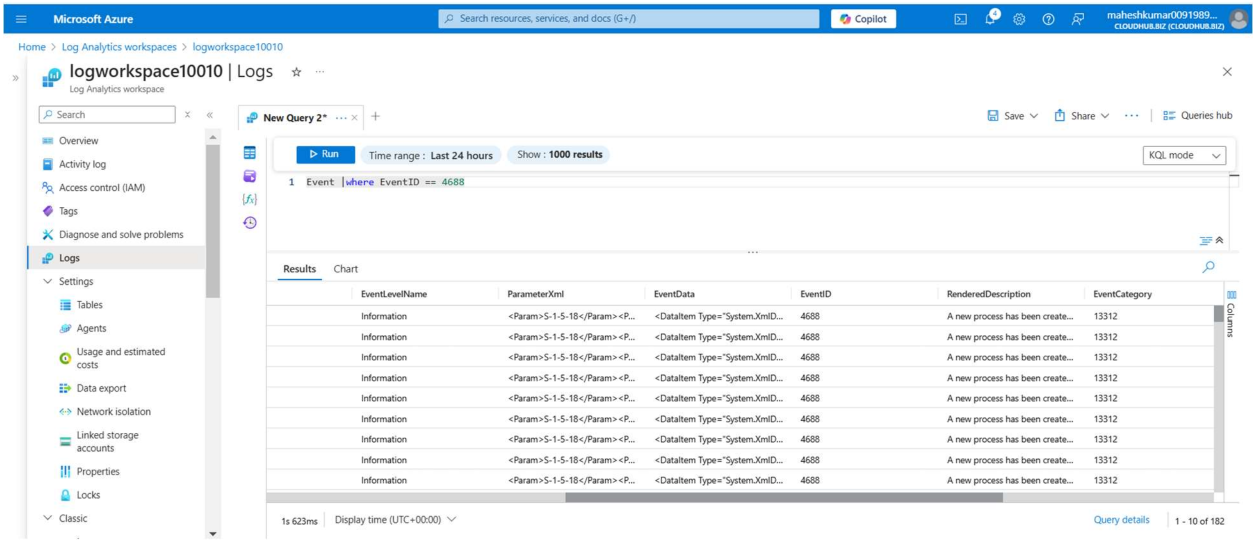
Time range : Last 24 hours Show : 1000 results KQL mode

```
Event |search 'VM1'
```

TimeGenerated [UTC]	Source	EventLog	Computer	EventLevel	EventLevelName	ParameterXml
1/28/2025, 9:45:23.888 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-
1/28/2025, 9:45:22.504 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-
1/28/2025, 9:45:22.504 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-
1/28/2025, 9:45:22.327 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-
1/28/2025, 9:45:22.325 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-
1/28/2025, 9:45:22.325 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-
1/28/2025, 9:45:22.325 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-
1/28/2025, 9:45:22.274 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-
1/28/2025, 9:45:22.203 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-

1s 671ms Display time (UTC+00:00) Query details 1 - 10 of 1000

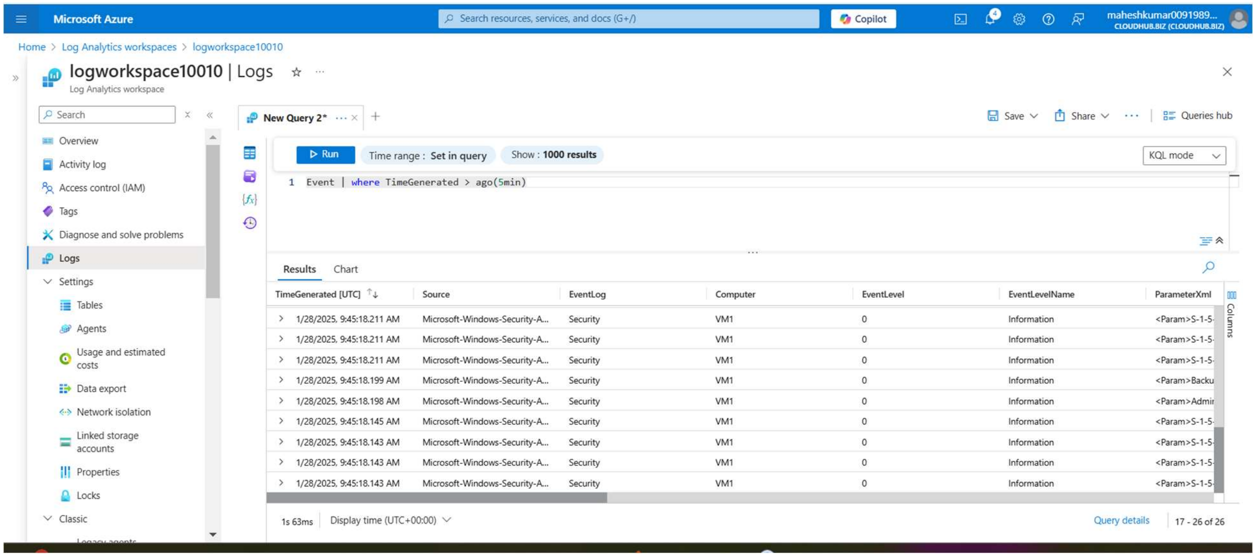
Search data based on a particular column value eg- Event ID



```
Event |where EventID == 4688
```

EventLevelName	ParameterXml	EventData	EventID	RenderedDescription	EventCategory
Information	<Param>S-1-5-18</Param><P...	<DataItem Type="System.XmlD...	4688	A new process has been create...	13312
Information	<Param>S-1-5-18</Param><P...	<DataItem Type="System.XmlD...	4688	A new process has been create...	13312
Information	<Param>S-1-5-18</Param><P...	<DataItem Type="System.XmlD...	4688	A new process has been create...	13312
Information	<Param>S-1-5-18</Param><P...	<DataItem Type="System.XmlD...	4688	A new process has been create...	13312
Information	<Param>S-1-5-18</Param><P...	<DataItem Type="System.XmlD...	4688	A new process has been create...	13312
Information	<Param>S-1-5-18</Param><P...	<DataItem Type="System.XmlD...	4688	A new process has been create...	13312
Information	<Param>S-1-5-18</Param><P...	<DataItem Type="System.XmlD...	4688	A new process has been create...	13312
Information	<Param>S-1-5-18</Param><P...	<DataItem Type="System.XmlD...	4688	A new process has been create...	13312
Information	<Param>S-1-5-18</Param><P...	<DataItem Type="System.XmlD...	4688	A new process has been create...	13312

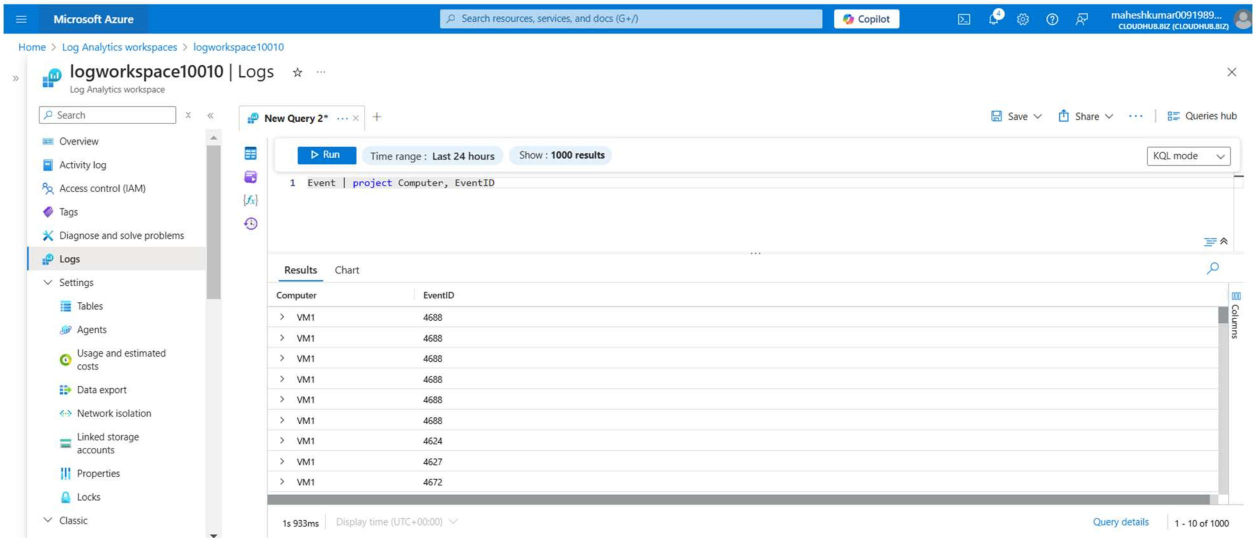
Search data which is generated 5 mins ago



```
Event | where TimeGenerated > ago(5min)
```

TimeGenerated [UTC]	Source	EventLog	Computer	EventLevel	EventLevelName	ParameterXml
1/28/2025, 9:45:18.211 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-
1/28/2025, 9:45:18.211 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-
1/28/2025, 9:45:18.211 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-
1/28/2025, 9:45:18.199 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>Backu
1/28/2025, 9:45:18.198 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>Admir
1/28/2025, 9:45:18.145 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-
1/28/2025, 9:45:18.143 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-
1/28/2025, 9:45:18.143 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-
1/28/2025, 9:45:18.143 AM	Microsoft-Windows-Security-A...	Security	VM1	0	Information	<Param>S-1-5-

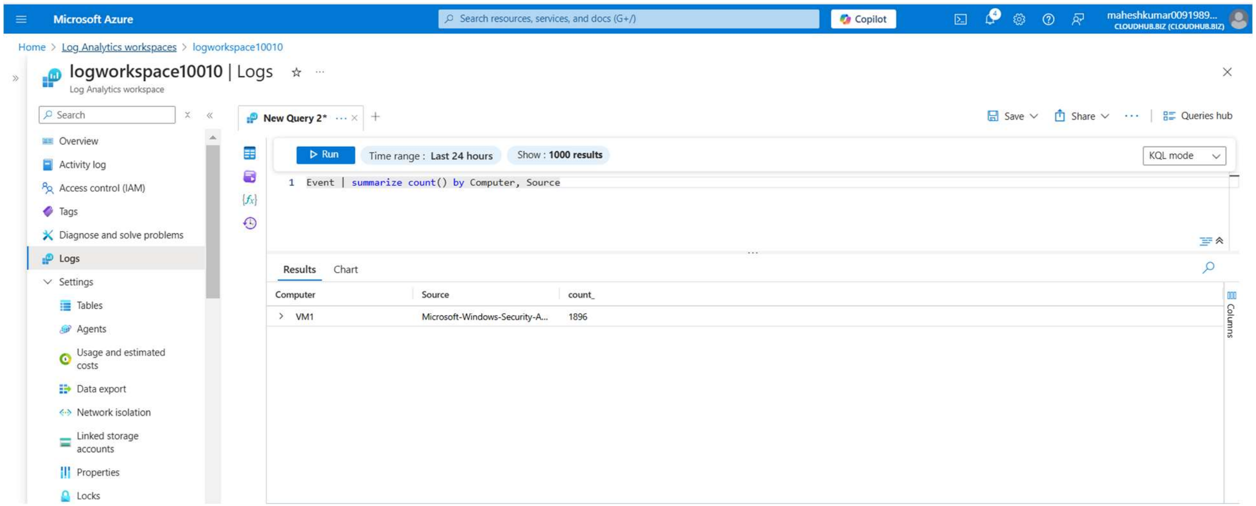
I only want to see the computer and Event ID column



```
Event | project Computer, EventID
```

Computer	EventID
VM1	4688
VM1	4688
VM1	4688
VM1	4688
VM1	4688
VM1	4688
VM1	4624
VM1	4627
VM1	4672

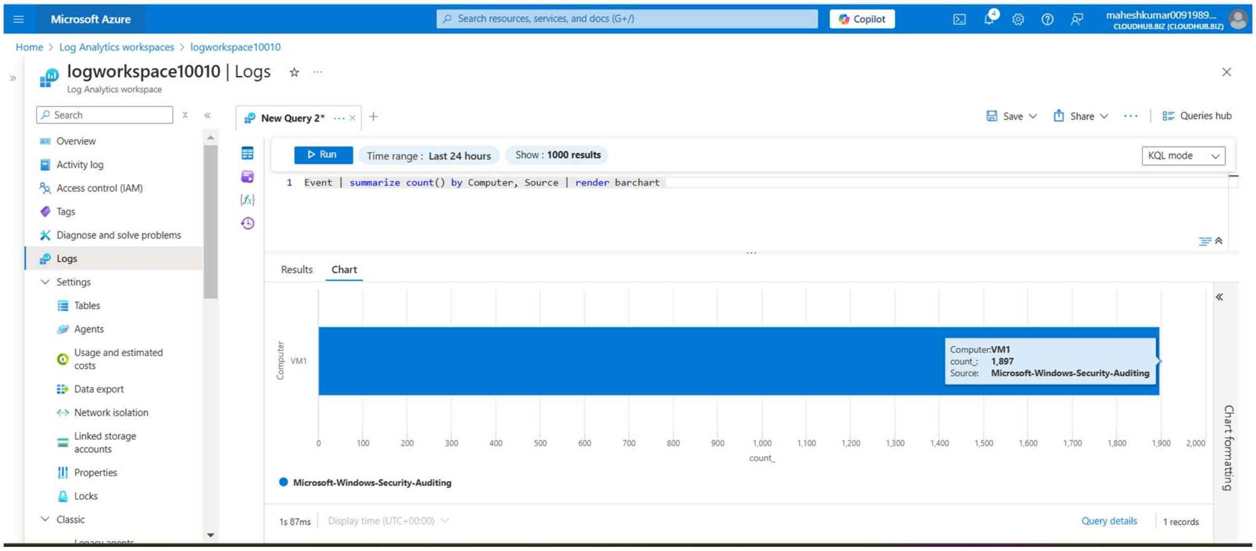
Summarize the events-it shows vm1 has total 1896 records



```
Event | summarize count() by Computer, Source
```

Computer	Source	count_
VM1	Microsoft-Windows-Security-A...	1896

render a bar chart based on the data



logworkspace10010 | Logs

Time range : Last 24 hours

Show : 1000 results

```
Event | summarize count() by Computer, Source | render barchart
```

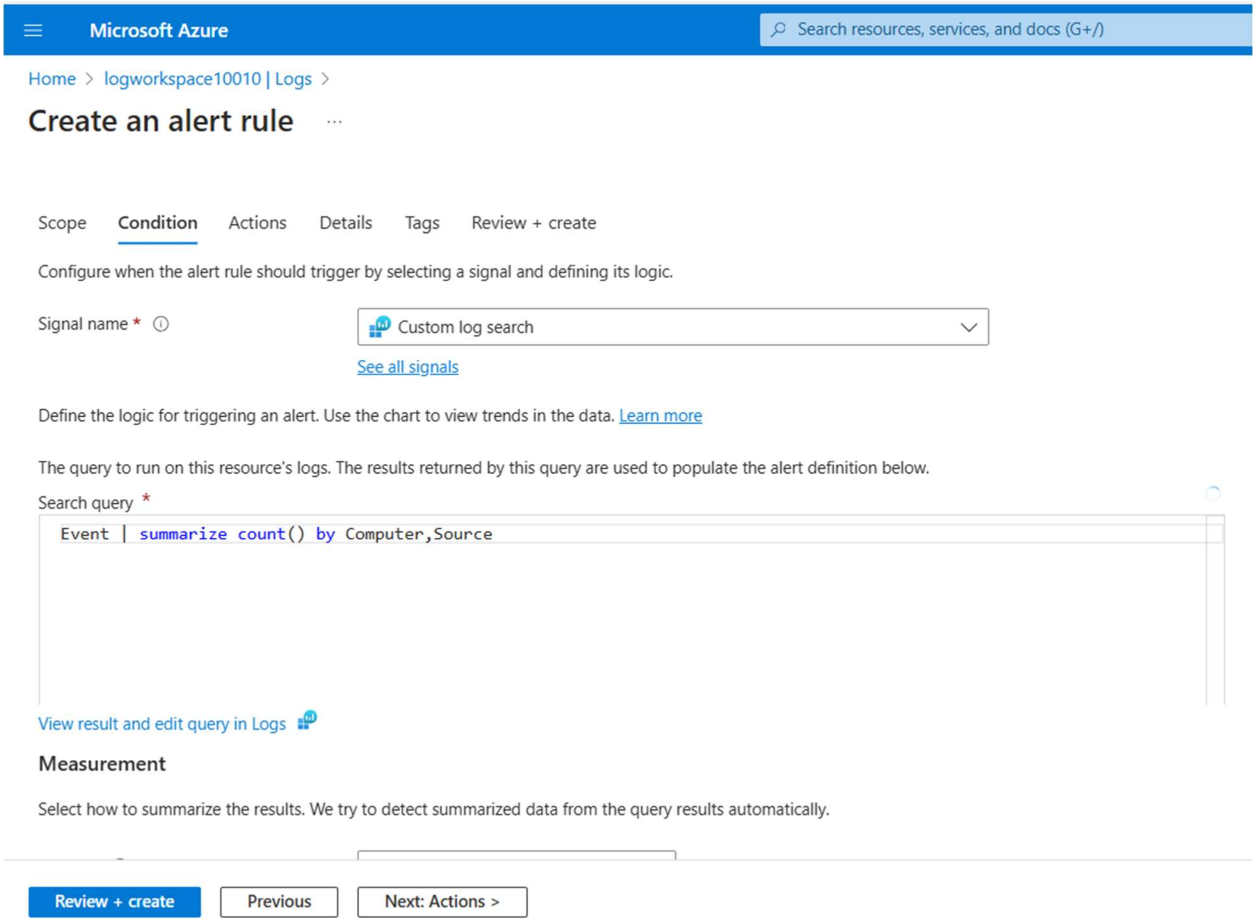
Computer: VM1
count_: 1,897
Source: Microsoft-Windows-Security-Auditing

1s 87ms

Display time (UTC+00:00)

1 records

We can also create alert rule based on queries which we have define in the log analytics workspace



Create an alert rule

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Signal name * : Custom log search

Define the logic for triggering an alert. Use the chart to view trends in the data. Learn more

The query to run on this resource's logs. The results returned by this query are used to populate the alert definition below.

Search query *

```
Event | summarize count() by Computer,Source
```

Measurement

Select how to summarize the results. We try to detect summarized data from the query results automatically.