😊 Log Analytics Queries

1. Azure Log Analytics is a powerful tool for querying and analyzing log data within Azure Monitor. It uses a query language called Kusto Query Language (KQL) which is designed for ad-hoc querying of large datasets.
2. All of our data, our logs are being sent to the Log Analytics Workspace and you can see that the data is being stored like records within different tables. You can use something known as the Kusto Query Language to query the data within these tables.
3. Below all the queries are mentioned and I am attaching the snapshots for the same use them and see for yourself how things work.
4. To use these queries you need to go to Log Analytics Workspace and then in the Logs section, you can use these queries.

1. This can be used for search for a keyword in the event table

```
Event | search "demovm"
```

---

2. This can used to pick up 10 events taken in no specific order

```
Event | top 10 by TimeGenerated
```

---

3. This is used to filter based on a particular property of an event

```
Event | where EventLevel == 4
```

---

4. This can be used to check for the events generated in the previous 5 minutes

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

---

5. This can be used to project certain properties

```
Event | where TimeGenerated > ago(5m) | project EventLog, Computer
```

---

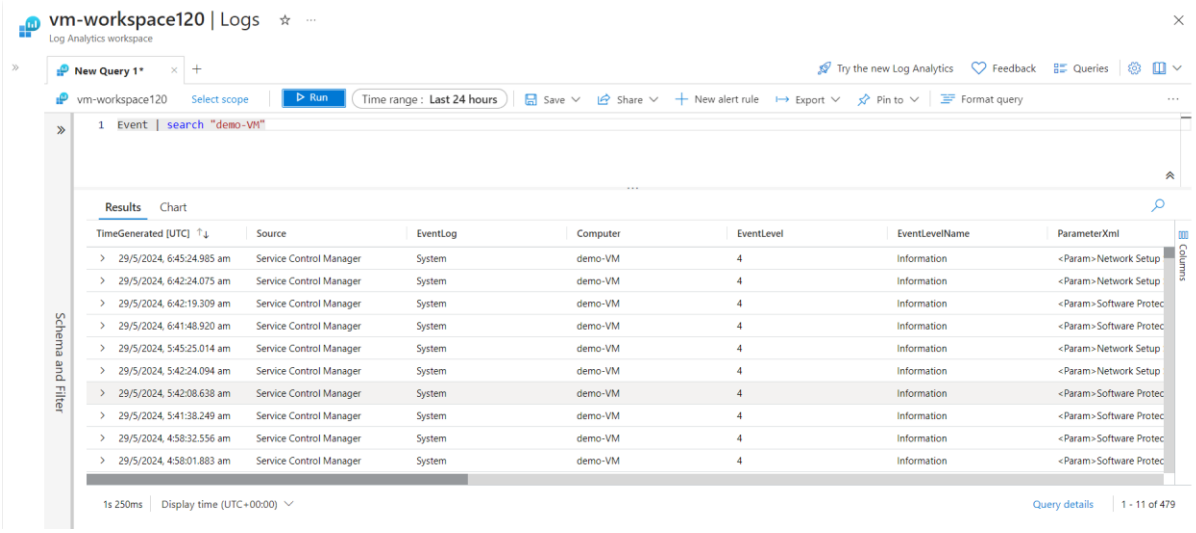
6. Here you can summarize the events

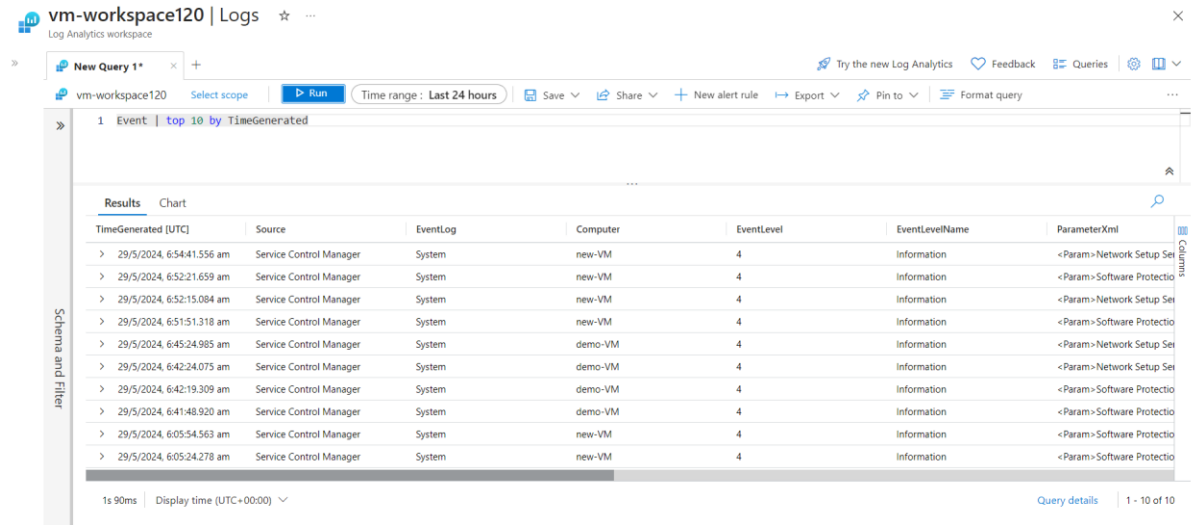
```
Event |  where TimeGenerated > ago(1d) | summarize count() by Computer,Source
```

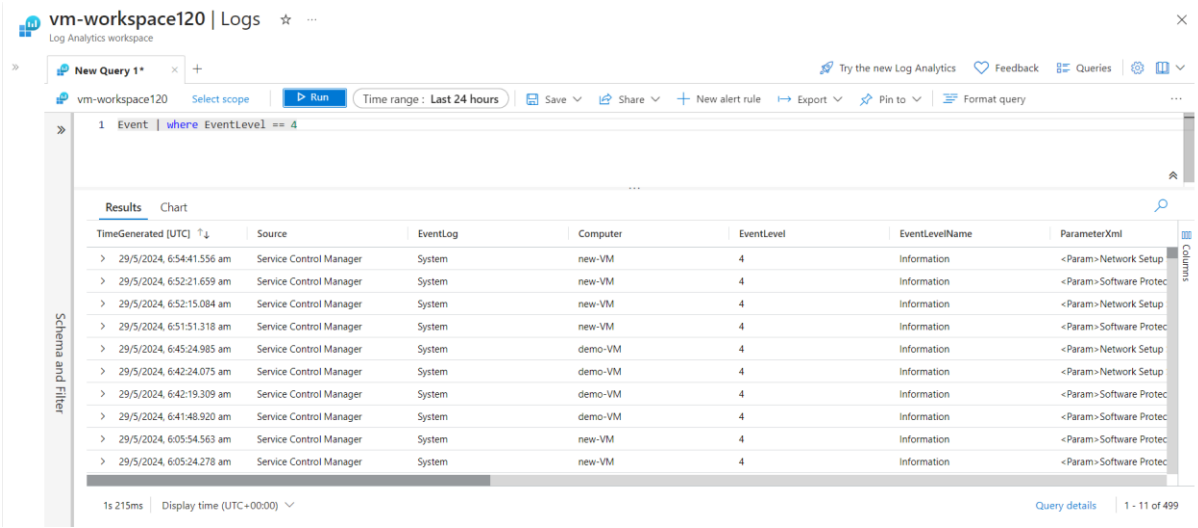
---

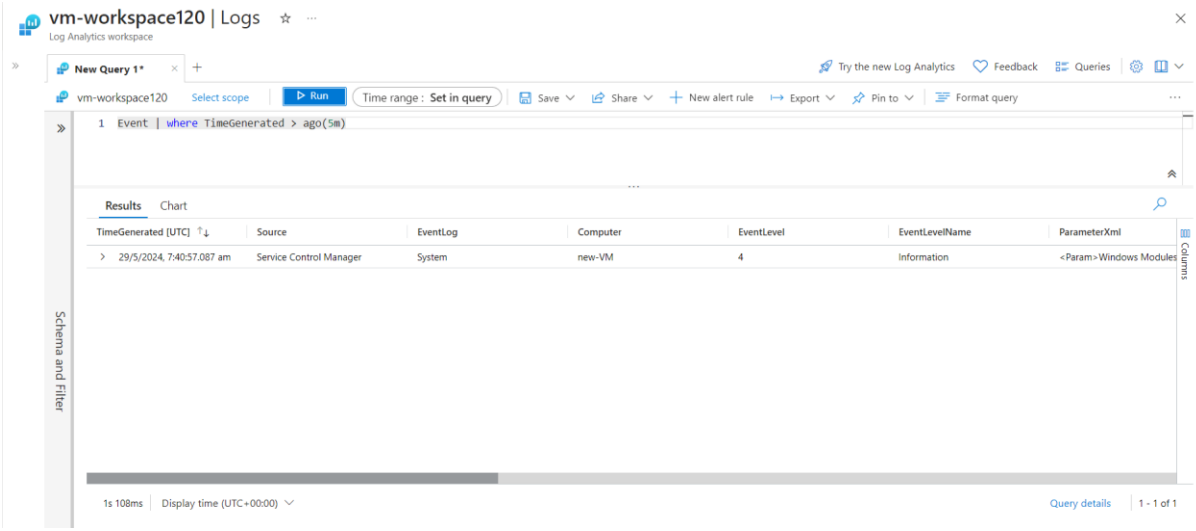
7. Here you can render a bar chart based on the data

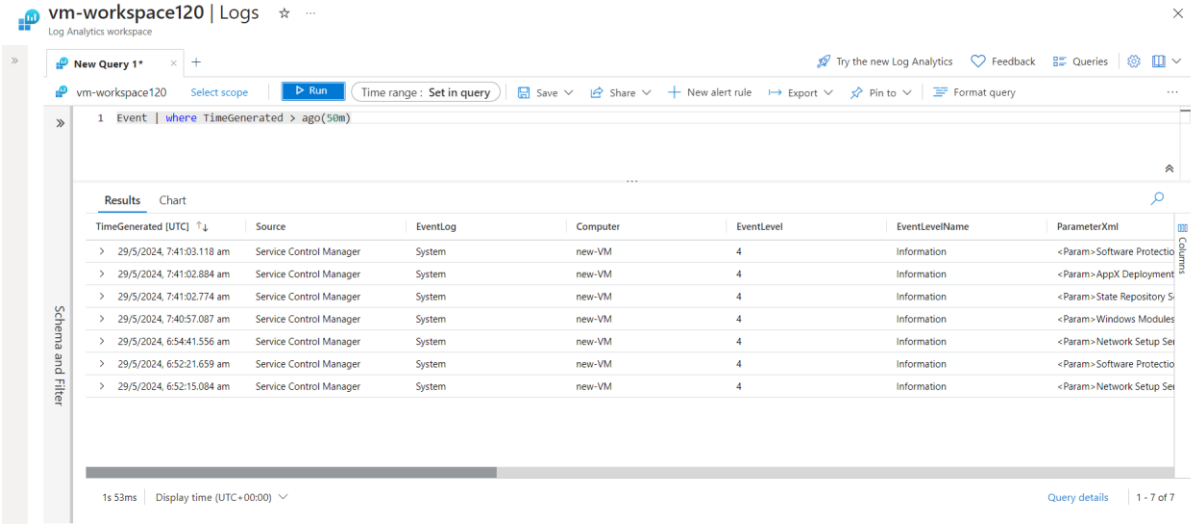
Event | where TimeGenerated > ago(1d) | summarize count() by Computer,Source | render barchart

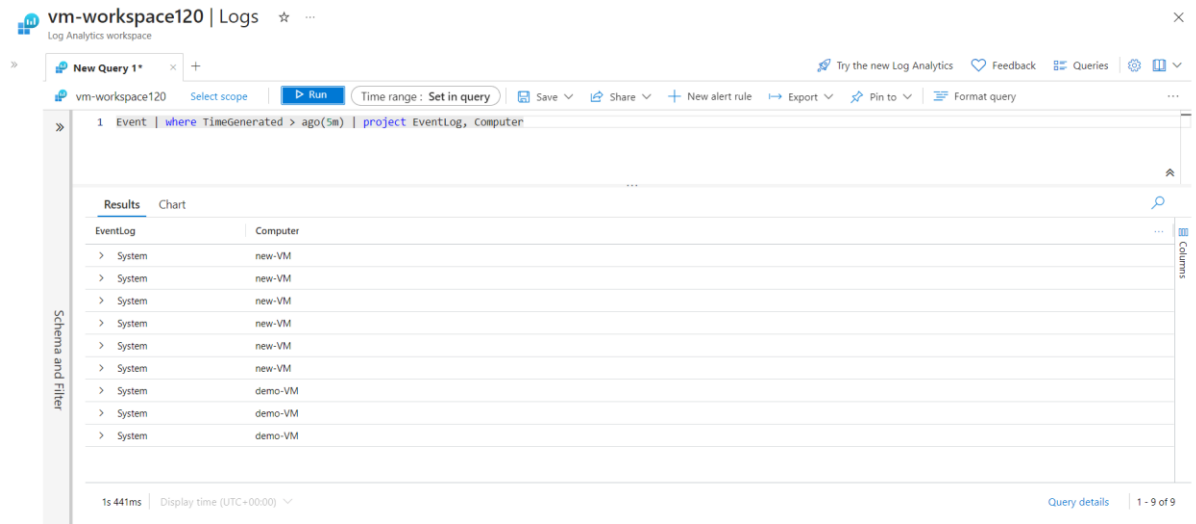


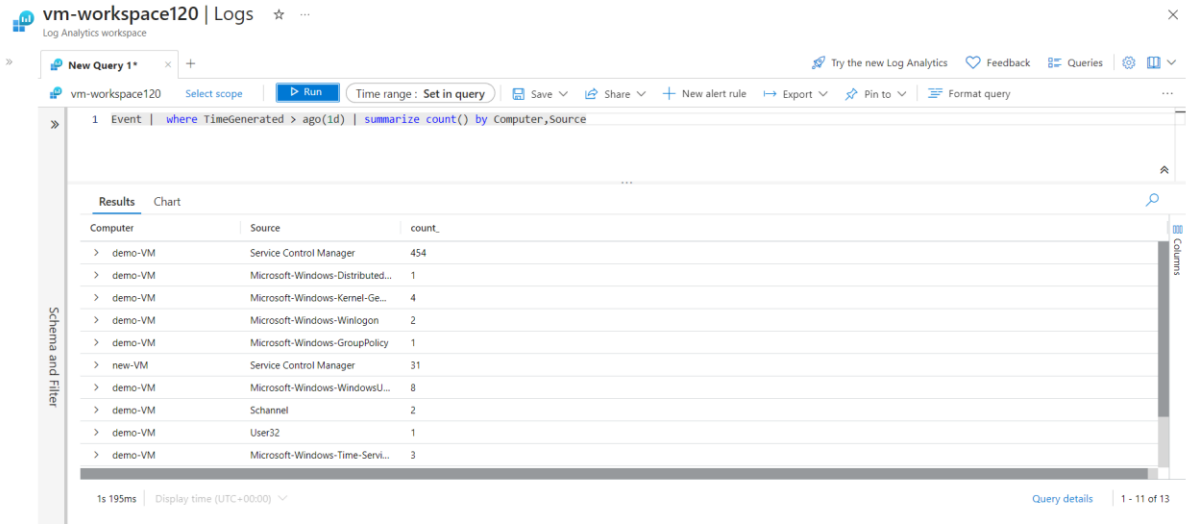


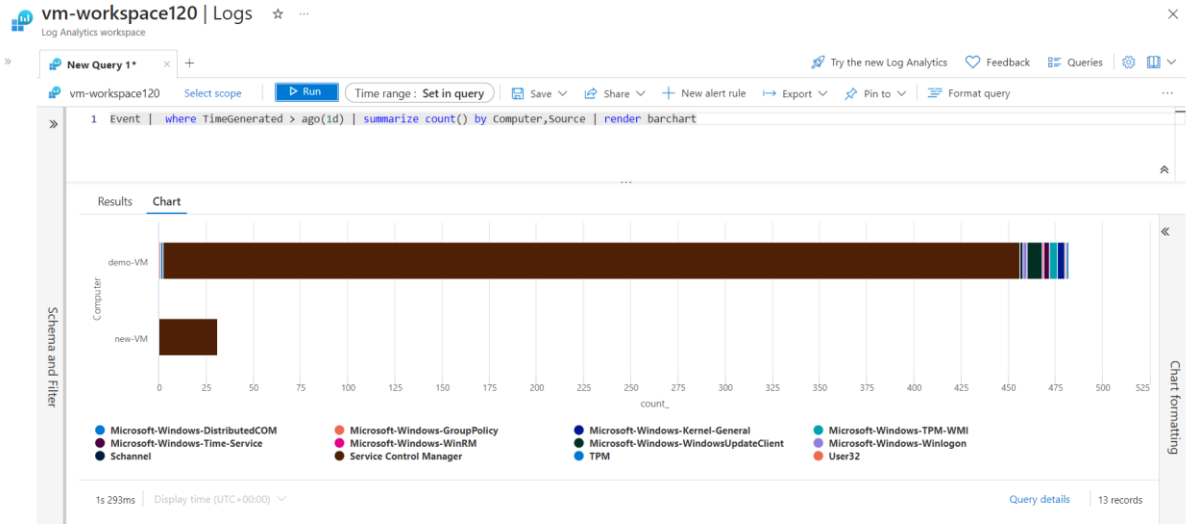



vm-workspace120 | Logs
Log Analytics workspace
New Query 1*
vm-workspace120
Select scope
Run
Time range : Set in query
Save
Share
New alert rule
Export
Pin to
Format query
Try the new Log Analytics
Feedback
Queries
1 Event | where TimeGenerated > ago(5m)
Results
Chart
TimeGenerated [UTC]
Source
EventLog
Computer
EventLevel
EventLevelName
ParameterXml
29/5/2024, 7:40:57.087 am
Service Control Manager
System
new-VM
4
Information
<Param>Windows Modules
Columns
Schema and Filter
1s 108ms
Display time (UTC+00:00)
Query details
1 - 1 of 1


vm-workspace120 | Logs
Log Analytics workspace
New Query 1*
vm-workspace120
Select scope
Run
Time range : Set in query
Save
Share
New alert rule
Export
Pin to
Format query
Try the new Log Analytics
Feedback
Queries
1 Event | where TimeGenerated > ago(50m)
Results
Chart
TimeGenerated [UTC]
Source
EventLog
Computer
EventLevel
EventLevelName
ParameterXml
29/5/2024, 7:41:03.118 am
Service Control Manager
System
new-VM
4
Information
<Param>Software Protectio
29/5/2024, 7:41:02.884 am
<Param>AppX Deployment
29/5/2024, 7:41:02.774 am
<Param>State Repository S
29/5/2024, 7:40:57.087 am
<Param>Windows Modules
29/5/2024, 6:54:41.556 am
<Param>Network Setup Se
29/5/2024, 6:52:21.659 am
<Param>Software Protectio
29/5/2024, 6:52:15.084 am
<Param>Network Setup Se
Columns
Schema and Filter
1s 53ms
Display time (UTC+00:00)
Query details
1 - 7 of 7


vm-workspace120 | Logs
Log Analytics workspace
New Query 1*
vm-workspace120
Select scope
Run
Time range : Set in query
Save
Share
New alert rule
Export
Pin to
Format query
Try the new Log Analytics
Feedback
Queries
1 Event | where TimeGenerated > ago(5m) | project EventLog, Computer
Results
Chart
EventLog
Computer
System
new-VM
System
new-VM
System
new-VM
System
new-VM
System
new-VM
System
new-VM
System
demo-VM
System
demo-VM
System
demo-VM
Columns
Schema and Filter
1s 441ms
Display time (UTC+00:00)
Query details
1 - 9 of 9


vm-workspace120 | Logs
Log Analytics workspace
New Query 1*
Try the new Log Analytics
Feedback
Queries
vm-workspace120
Select scope
Run
Time range : Set in query
Save
Share
New alert rule
Export
Pin to
Format query
1 Event | where TimeGenerated > ago(1d) | summarize count() by Computer,Source
Results
Chart
Computer
Source
count_
demo-VM
Service Control Manager
454
demo-VM
Microsoft-Windows-Distributed...
1
demo-VM
Microsoft-Windows-Kernel-Ge...
4
demo-VM
Microsoft-Windows-Winlogon
2
demo-VM
Microsoft-Windows-GroupPolicy
1
new-VM
Service Control Manager
31
demo-VM
Microsoft-Windows-WindowsU...
8
demo-VM
Schannel
2
demo-VM
User32
1
demo-VM
Microsoft-Windows-Time-Servi...
3
Columns
Schema and Filter
1s 195ms
Display time (UTC+00:00)
Query details
1 - 11 of 13


vm-workspace120 | Logs
Log Analytics workspace
New Query 1*
Try the new Log Analytics
Feedback
Queries
vm-workspace120
Select scope
Run
Time range : Set in query
Save
Share
New alert rule
Export
Pin to
Format query
1 Event | where TimeGenerated > ago(1d) | summarize count() by Computer,Source | render barchart
Results
Chart
demo-VM
new-VM
Computer
0
25
50
75
100
125
150
175
200
225
250
275
300
325
350
375
400
425
450
475
500
525
count_
Microsoft-Windows-DistributedCOM
Microsoft-Windows-GroupPolicy
Microsoft-Windows-Kernel-General
Microsoft-Windows-TPM-WMI
Microsoft-Windows-Time-Service
Microsoft-Windows-WinRM
Microsoft-Windows-WindowsUpdateClient
Microsoft-Windows-Winlogon
Schannel
Service Control Manager
TPM
User32
Schema and Filter
Chart formatting
1s 293ms
Display time (UTC+00:00)
Query details
13 records