David Garcia

Using KQL to monitor failed logs on

Introduction

KQL, or Kusto Query Language, is a query language used to query and analyze data in Azure Data Explorer (ADX). ADX is a data exploration and analytics service provided by Microsoft Azure. It is commonly used for log analytics, monitoring, and troubleshooting scenarios. Still, in this case, I was using KQL to monitor failed logs on my virtual machines, which I created and left all inbound traffic open on the internet.

Technologies and Azure Components Employed:

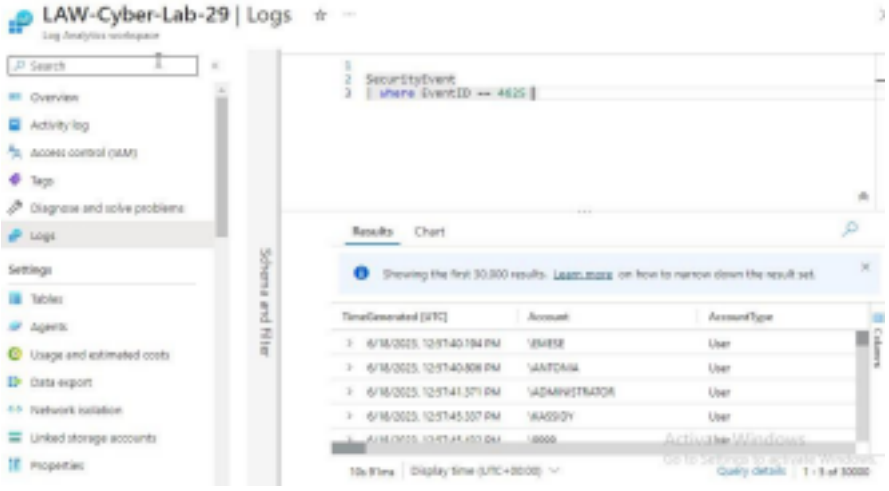
- Azure Virtual Network (VNet)
- Azure Network Security Group (NSG)
- Virtual Machines (2x Windows, 1x Linux)
- Log Analytics Workspace with Kusto Query Language (KQL) Queries
- Microsoft Sentinel for Security Information and Event Management (SIEM) **To**

monitor failed logs in Azure using KQL

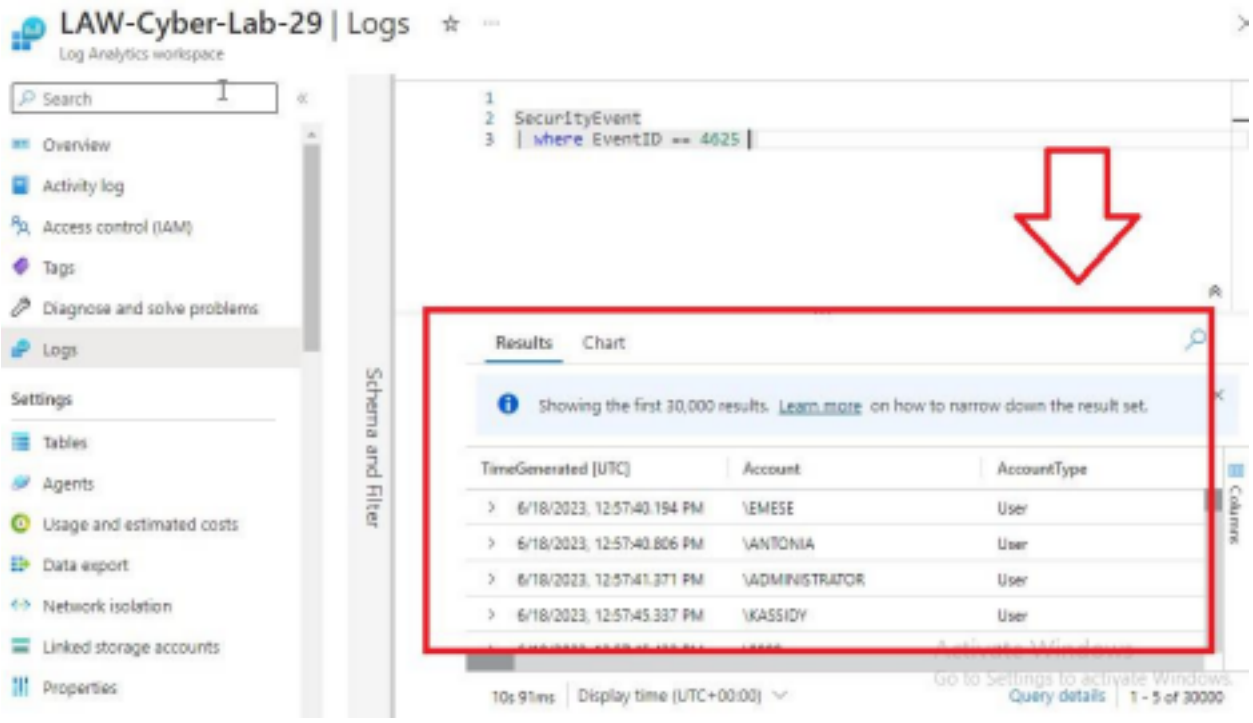
Identify the relevant data source: Determine where the logs related to the failures are stored. This could be Azure Monitor Logs, Azure Activity Logs, or custom logs ingested into ADX. In this case, my logs come from my Windows and Linux virtual machines.

Connect to Azure Data Explorer: Access the ADX environment or cluster where the logs are stored. This can be done via the Azure portal, Azure Data Explorer Explorer, or programmatically using SDKs or APIs.

Write a KQL query: using the KQL syntax, you can create a query that will retrieve and filter the failed logs. The query will be specific to your logs' structure and content.For example, if you're using Azure Monitor Logs, you might query the securityevent | where eventid == 4625. The below query filters and retrieves records from the "securityevent" table where the "eventid" column equals 4625.

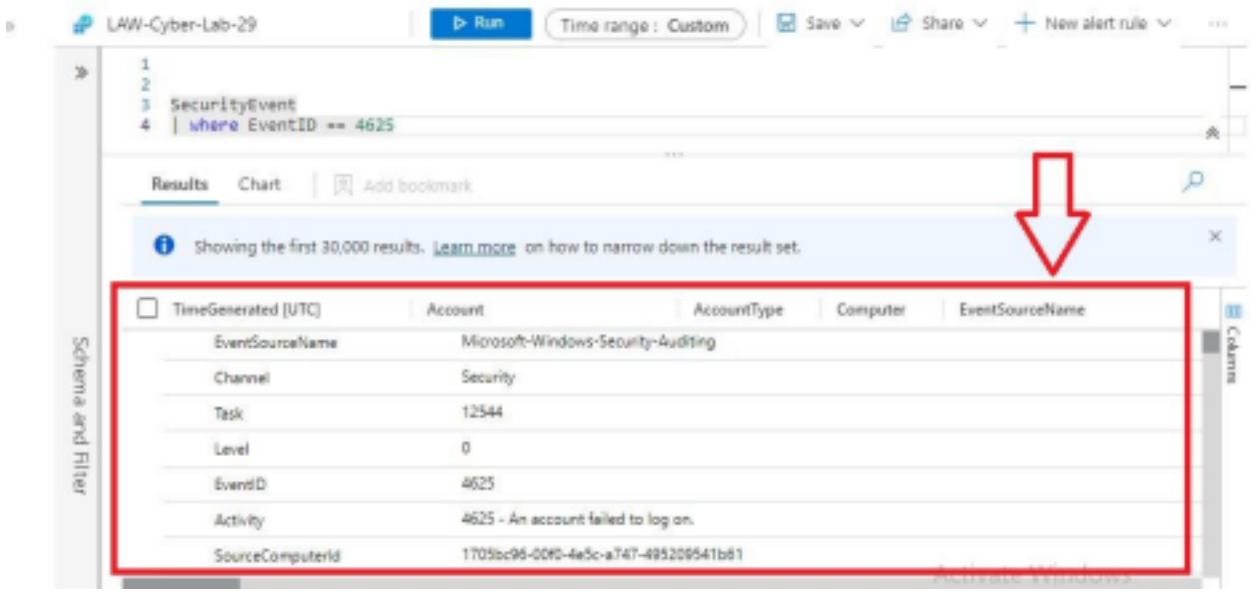


Execute the query: Run the KQL query against the data source within ADX. The query engine will process the query and return the matching results.



Analyze the results: To understand the failed logs better, you can review the query results and explore the various columns. You can also add filters and aggregate the data for better insight.

Results: As we can see, the eventID of 4625 shows a failed log-on activity



Conclusion

In conclusion, this query retrieves records from the "security event" table where the "eventid" equals 4625. The specific meaning of event ID 4625 can vary depending on the context, but Windows Security event logs typically represent a failed logon attempt. By leveraging the power of KQL, you can efficiently search, filter, and analyze large volumes of logs to monitor and troubleshoot failed events within Azure.