Getting Started with Azure AD Workbooks

Wednesday, February 16, 2022 12:56 PM

Contents

Lab Guide Summary

This guide will walk you through setting up an Azure Monitor Workspace, creating alerts, querying with KQL and building your own workbook with Log Analytics - all using Azure AD data.

Requirements & Limitations

Note: This walk-through assumes you are setting up an Azure Monitor Workspace for the first time. If you are using a tenant that already has a Workspace set up, you can skip this section.

For this to work in your personal demo environment, you will need to do one of the following:

1. Activate $100 Azure monthly credit - for directions, click here
2. Transfer billing ownership of an Azure Subscription - for directions, click here
   You can also go to aka.ms/LADEMO to practice KQL anytime outside of demo environment. Learn more here: KQL from Scratch

Objectives

1. Integrate Audit and Sign-in Logs with Azure Monitor Log Analytics
2. Query Signin and Audit logs using KQL
3. Create an alert based on a query
4. Add a query to an existing Workbook

Send Audit and Signin Logs to Log Analytics

This task will outline how to send your sign-in logs to Log Analytics in the Azure portal.

Navigating to Log Analytics Workspaces

- Make sure you are logged on to the management portal (https://portal.azure.com) with the global admin account of your visual studio subscription.

1. Search for Log Analytics workspaces
2. Create a new Log Analytics Workspace
3. Click + Add
4. Enter a name for your workspace
5. Choose the Subscription
6. Choose a Resource Group or Create a new Resource Group
7. Choose a Location
8. Choose a Pricing tier
9. Select Ok
10. Wait for validation that deployment succeeded. You may need to refresh the page to see the new workspace

Add Diagnostic setting and select logs to send to Log Analytics

1. Return to the home page of Azure
2. Select Azure Active Directory
3. Under the Monitoring section, select Diagnostic settings
4. Click Add diagnostic setting
5. Enter a descriptive Diagnostic setting name of your choice
6. Check the boxes for Audit and SigninLogs
7. Select Destination details to Send to Log Analytics
8. Confirm the Subscription and Log Analytics workspace
9. Click Save
   Now your Audit & SignIn Logs are being saved to Log Analytics!

Query logs in Log Analytics

Navigating to Logs

- In your browser, go to the Azure Active Directory Management Portal (https://aad.portal.azure.com) Under Monitoring, select Logs
- Click on Get Started
- A New Query window will open

Test out the following queries using KQL

- Take 10 random entries from the input data:
  ```
  SigninLogs
  | take 10
  ```
- Look at the signins where the Conditional Access was a success
  ```
  SigninLogs
  | where ConditionalAccessStatus == "success"
  | project UserDisplayName, ConditionalAccessStatus
  ```
- Count how many successes there have been
  ```
  SigninLogs
  | where ConditionalAccessStatus == "success"
  | project UserDisplayName, ConditionalAccessStatus
  | count
  ```
- Aggregate count of successful signins by user by day
  ```
  SigninLogs
  | where ConditionalAccessStatus == "success"
  | summarize SuccessfulSignins = count()
     by UserDisplayName
     , bin(TimeGenerated, 1d)
  ```
- View how many times a user does a certain operation in specific time period
  ```
  AuditLogs
  | where TimeGenerated > ago(30d)
  | where OperationName contains "Add member to role"
  | summarize count() by OperationName, Identity
  ```
- Pivot the results on operation name
  ```
  AuditLogs
  | where TimeGenerated > ago(30d)
  | where OperationName contains "Add member to role"
  | project OperationName, Identity
  | evaluate pivot(OperationName)
  ```
- Merge together Audit and Sign in Logs using an inner join
  ```
  AuditLogs
  |where OperationName contains "Add User"
  |extend UserPrincipalName = tostring(TargetResources[0].userPrincipalName)
  |project TimeGenerated , UserPrincipalName
  |join kind = inner (
  SigninLogs
  ) on UserPrincipalName
  |summarize arg_min(TimeGenerated, *) by UserPrincipalName
  |extend SigninDate = TimeGenerated
  ```

Create a custom query and add an alert

This task will outline how to send alerts when the breakglass account is used.

Navigating to Logs

- In your browser, go to the Azure Active Directory Management Portal (https://aad.portal.azure.com) Under Monitoring, select Logs
- A New Query window will open

Write a new query and create a new alert

1. Type in the following query:
   SigninLogs
   |where UserDisplayName contains "BreakGlass"
   |project UserDisplayName
   Note: Modify the query depending on the UPN or UserID of your emergency access/breakglass account.

2. Shift+Enter to run the query - there may not be any results, but that is ok. Our objective here is to create an alert on this query.

3. Click on + New alert rule

4. In the Create Alert window, verify workspace, subscription and resource group is correct
5. Under Condition, click on pre-populated condition
6. Under Alert logic, enter the following:
   -Based on: Number of results
   -Operator: Greater than
   -Threshold value: 0
   -Under "Evaluated based on", select the Period (in minutes) for how long you want the query to run, and the Frequency (in minutes) for how often you want the query to run. The frequency should be less than or equal to the period
7. Select Done. You may now view the estimated monthly cost of this alert.

Finish creating the alert rule

1. Select an action group of users to be notified by the alert. If you want to create one, see Create an action group.
2. To customize the email notification sent to the members of the action group, select actions under Customize Actions.
3. Under Alert Details, specify the alert rule name and add an optional description.
4. Set the Severity level of the event. We recommend that you set it to Critical(Sev 0).
5. Under Enable rule upon creation, leave it set as yes.
6. To turn off alerts for a while, select the Suppress Alerts check box and enter the wait duration before alerting again, and then select Save.
7. Click Create alert rule

Create a custom workbook from scratch

This task will outline how to create a new workbook using the Quick start template

Navigating to Workbooks

- In your browser, go to the Azure Active Directory Management Portal (https://aad.portal.azure.com) Under Monitoring, select Workbooks
- Under Quick start, click Empty

Adding a title

- Click + Add and select Add text
- Write a title name, such as: "# Client apps used in the past week" - The # symbol formats the text with enlarged font.
- Click Done Editing

Writing a new query

We can now add our own KQL query and visualize the results in a pie chart

• Click + Add query and write query

```
SigninLogs
| where TimeGenerated > ago(7d)
| project TimeGenerated, UserDisplayName, ClientAppUsed
| summarize count() by ClientAppUsed
```

• Click Run Query to display the results

• In the toolbar above the query, click on the Visualization dropdown and select Pie chart

• Click Done Editing

Add a query to a workbook template

This task will outline how to add a query to an existing workbook template. We will add a query that shows the distribution of Conditional Access success to failures.

Navigating to Workbooks

- In your browser, go to the Azure Active Directory Management Portal (https://aad.portal.azure.com) Under Monitoring, select Workbooks
- In the Conditional access group, select Conditional Access Insights (Preview)

Editing the workbook template

- Click Edit in the toolbar above the workbook
- To add a new query below the Impact Summary tiles, click the three dots next to the Edit button to the right of the tiles
- Select + Add and then Add query

Writing a new query

- We can now add our own KQL query and visualize the results in different formats, including grids, tiles, pie charts, bar charts, and more
- Type a query into the box

```
SigninLogs
| where TimeGenerated > ago(20d)
| where ConditionalAccessPolicies != "[]"
| summarize dcount(UserDisplayName) by bin(TimeGenerated, 1d), ConditionalAccessStatus
```

- Click Run Query to display the results
- Set the Time Range to Set in query

Visualize the query result

- Set the Visualization to Bar chart
- Click Advanced Settings to add a Chart Title: “Conditional Access status over the last 20 days”
- Click Done Editing in the workbook toolbar

15 visits in last 30 days

Add a comment...

From <https://identitydivision.visualstudio.com/IdentityWiki/_wiki/wikis/IdentityWiki.wiki/21308/Getting-Started-with-Workbooks>