# Lab Guide for Log Analytics Wizardry!

Hello! Welcome to the Lab Guide for the Log Analytics Wizadry! Session held at the MVP Summit 2020. Read on to learn more about writing queries, setting up alerts and using Workbooks in Azure Monitor Log Analytics.

## Requirements & Limitations

For this lab you should have:

* An Azure subscription with at least one P1 licensed admin. If you don't have an Azure subscription, you can [sign up for a free trial](https://azure.microsoft.com/free/).
* An Azure AD tenant.
* A user who's a global administrator or security administrator for the Azure AD tenant.

## 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

## Resources

# [Tutorial: Collect and analyze resource logs from an Azure resource](https://docs.microsoft.com/en-us/azure/azure-monitor/learn/tutorial-resource-logs)

# [How to integrate activity logs with Log Analytics](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics)

# [Manage emergency access account in Azure AD](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-emergency-access)

* [KQL quick reference](https://docs.microsoft.com/en-us/azure/data-explorer/kql-quick-reference)
* [Azure Monitor Workbooks](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/workbooks-overview)

## 

## Steps

### Task 1: 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**   * Complete these steps from an internet-connected Windows computer. * Make sure you are logged on to the management portal (<https://portal.azure.com>) with the global admin account of **your visual studio subscription**. * Search for **Log Analytics workspaces** |  |
| **Create a new Log Analytics Workspace**   * Click **+ Add** * Enter a name for your workspace * Choose the **Subscription** * Choose a **Resource Group** or Create a new Resource Group * Choose a **Location** * Choose a **Pricing tier** * Select **Ok** * 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**   * Return to the home page of Azure * Select **Azure Active Directory** * Under the Monitoring section, select **Diagnostic settings** * Click **Add diagnostic setting** * Enter a descriptive **Diagnostic setting name** of your choice * Check the boxes for **Audit and** **SigninLogs** * Select **Destination details** to **Send to Log Analytics** * Confirm the Subscription and Log Analytics workspace * Click **Save**   Now your Audit & SignIn Logs are being saved to Log Analytics! |  |
|  |  |

### Task 2: Query logs in Log Analytics

This task will outline how to query your data with basic Kusto Query Language (KQL)

|  |  |
| --- | --- |
|  |  |
| **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   * sea   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 |  |

### Task 3: Create a 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**   * 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](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-emergency-access).   * Shift+Enter to run the query |  |
| **Create a new alert rule**   * Click on +New alert rule * In the **Create rule** window, under **Resource**, verify that the subscription is the one with which you want to associate the alert rule. |  |
| **Set Condition criteria for the new alert**   * Verify workspace, subscription and resource group is correct * Under **Condition**, click on pre-populated condition * 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. * Select **Done**. You may now view the estimated monthly cost of this alert. |  |
| **Finish creating the alert rule**   * Select an **action group** of users to be notified by the alert. If you want to create one, see [Create an action group](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-emergency-access). * To customize the email notification sent to the members of the action group, select actions under **Customize Actions**. * Under **Alert Details**, specify the alert rule name and add an optional description. * Set the **Severity** level of the event. We recommend that you set it to Critical(Sev 0). * Under **Enable rule upon creation**, leave it set as yes. * 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. * Click **Create alert rule**. |  |

### Task 4: 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** |  |

### Task 5: 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 |  |
|  |  |
|  |  |

### More KQL Queries:

* View number of signs ins by client app type

SigninLogs

| summarize count() by ClientAppUsed

* Count the sign ins by day

SigninLogs

| summarize NumberOfEntries=count()

by bin(TimeGenerated, 1d)

* Take 5 random entries and project the columns you wish to see in the results

SigninLogs

| take 5

| project ClientAppUsed, Identity, ConditionalAccessStatus, Status, TimeGenerated

* Take the top 5 in descending order and project the columns you wish to see

SigninLogs

| take 5

| project ClientAppUsed, Identity, ConditionalAccessStatus, Status, TimeGenerated

* Create a new column by combining the values to two other columns

SigninLogs

| limit 10

| extend RiskUser = strcat(RiskDetail, "-", Identity)

| project RiskUser, ClientAppUsed