Reports and dashboards in Azure Log Analytics

Install and use the log analytics views for Azure Active Directory

To view contributors to this article access the link below

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-install-use-log-analytics-views?wt.mc_id=4039827

In this article

The Azure Active Directory log analytics views helps you analyze and search the Azure AD activity logs in your Azure AD tenant. Azure AD activity logs include:

- Audit logs: The audit logs activity report gives you access to the history of every task that's performed in your tenant.
- Sign-in logs: With the sign-in activity report, you can determine who performed the tasks that are reported in the audit logs.

Prerequisites

To use the log analytics views, you need:

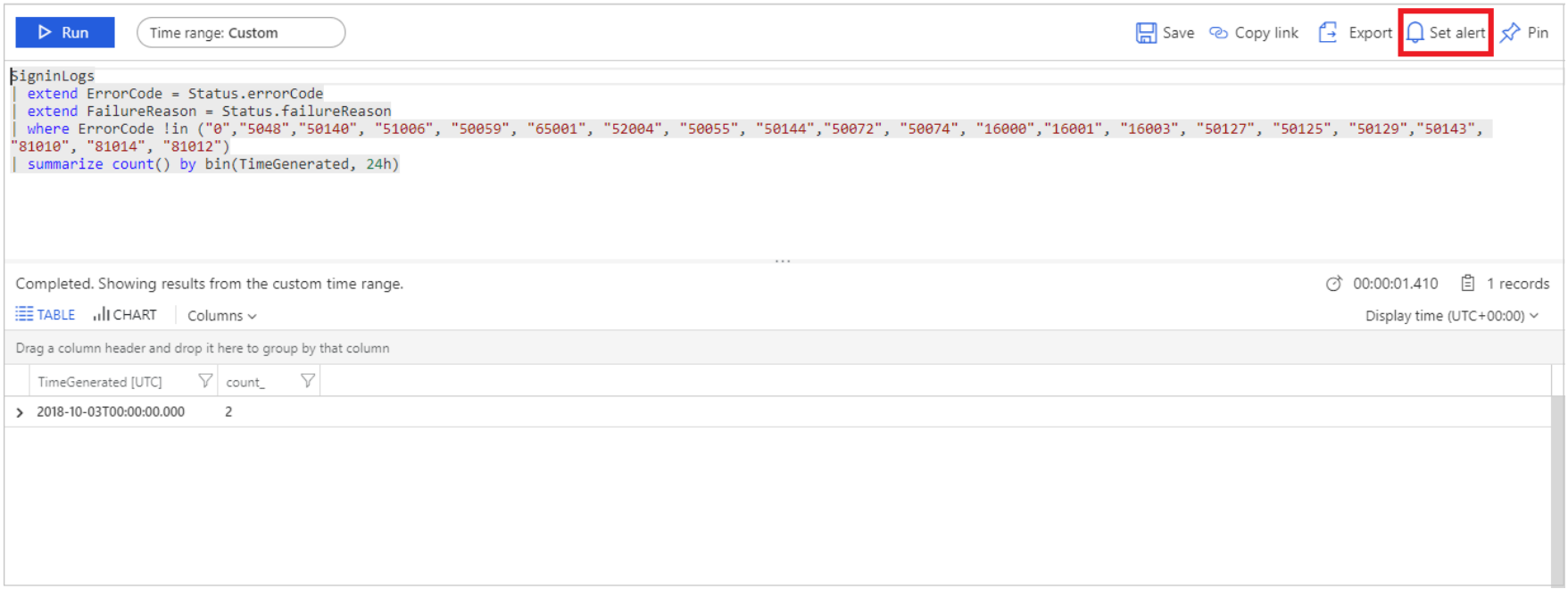
- A Log Analytics workspace in your Azure subscription. Learn how to create a Log Analytics workspace.
- First, complete the steps to route the Azure AD activity logs to your Log Analytics workspace.
- Download the views from the GitHub repository to your local computer.

Install the log analytics views

1. Navigate to your Log Analytics workspace. To do this, first navigate to the Azure portal and select **All services**. Type **Log Analytics** in the text box, and select **Log Analytics workspaces**. Select the workspace you routed the activity logs to, as part of the prerequisites.
2. Select **View Designer**, select **Import** and then select **Choose File** to import the views from your local computer.
3. Select the views you downloaded from the prerequisites and select **Save** to save the import. Do this for the **Azure AD Account Provisioning Events** view and the **Sign-ins Events** view.

Use the views

1. Navigate to your Log Analytics workspace. To do this, first navigate to the Azure portal and select **All services**. Type **Log Analytics** in the text box, and select **Log Analytics workspaces**. Select the workspace you routed the activity logs to, as part of the prerequisites.
2. Once you're in the workspace, select **Workspace Summary**. You should see the following three views:
    - **Azure AD Account Provisioning Events**: This view shows reports related to auditing provisioning activity, such as the number of new users provisioned and provisioning failures, number of users updated and update failures and the number of users de-provisioned and corresponding failures.
    - **Sign-ins Events**: This view shows the most relevant reports related to monitoring sign-in activity, such as sign-ins by application, user, device, as well as a summary view tracking the number of sign-ins over time.
3. Select either of these views to jump in to the individual reports. You can also set alerts on any of the report parameters. For example, let's set an alert for every time there's a sign-in error. To do this, first select the **Sign-ins Events** view, select **Sign-in errors over time** report and then select **Analytics** to open the details page, with the actual query behind the report.



4. Select **Set Alert**, and then select **Whenever the Custom log search is <logic undefined>** under the **Alert criteria** section. Since we want to alert whenever there's a sign-in error, set the **Threshold** of the default alert logic to **1** and then select **Done**.

Configure signal logic

<- Back to signal selection

Custom log search

* Search query

```
SigninLogs
| extend ErrorCode = Status.errorCode
| extend FailureReason = Status.failureReason
```

Query to be executed : *SigninLogs | extend ErrorCode = Status.errorCode | extend FailureReason = Status.failureReason | where ErrorCode !in ("0","5048","50140", "51006", "50059", "65001", "52004", "50055", "50144","50072", "50074", "16000","16001", "16003", "50127", "50125", "50129","50143", "81010", "81014", "81012") | summarize count() by bin(TimeGenerated, 24h) ↵| count*
For time window : *10/3/2018, 11:15:10 AM - 10/3/2018, 11:20:10 AM*

Alert logic

5. Enter a name and description for the alert and set the severity to **Warning**.

Create rule

Rules management

1. Define alert condition

Alert condition configuration requires 1) Target selection and 2) Alert criteria definition where signal(s) and alert logic is configured. Start by selecting a Target.

* Alert target	Target Hierarchy
[redacted]	Pay-As-You-Go > default-activitylogalerts

+ Select target

* Alert criteria	Monthly cost in USD (Estimated)	
Whenever the Custom log search is <logic undefined>	$ 1.50	
	Total $ 1.50	

+ Add criteria

We currently support configuring only two metrics signals or one log search signal or one activity log signal per alert rule. An alert will be triggered when the conditions for all the above configured criteria are met

2. Define alert details

* Alert rule name
Alert on sign-in error

* Description
Alert whenever there's a sign-in error

* Severity
Warning(Sev 1)

Enable rule upon creation

Yes | No

Suppress Alerts

6. Select the action group to alert. In general, this can be either a team you want to notify via email or text message, or it can be an automated task using webhooks, runbooks, functions, logic apps or external ITSM solutions. Learn how to create and manage action groups in the Azure portal.
7. Select **Create alert rule** to create the alert. Now you will be alerted every time there's a sign-in error.