**Onboarding GCP to sentinel via Azure Functions.**

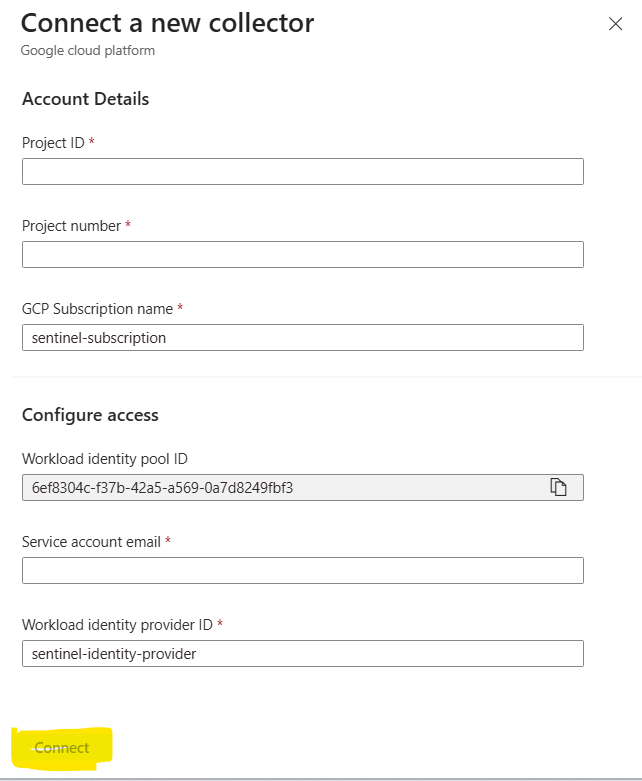
1. Set up your GCP environment

You must have the following GCP resources defined and configured: topic, subscription for the topic, workload identity pool, workload identity provider and service account with permissions to get and consume from subscription. Terraform provides API for the IAM that creates the resources.

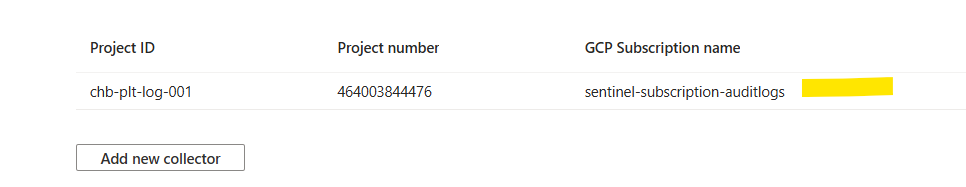
Ref : <https://github.com/Azure/Azure-Sentinel/tree/master/DataConnectors/GCP/Terraform/sentinel_resources_creation>

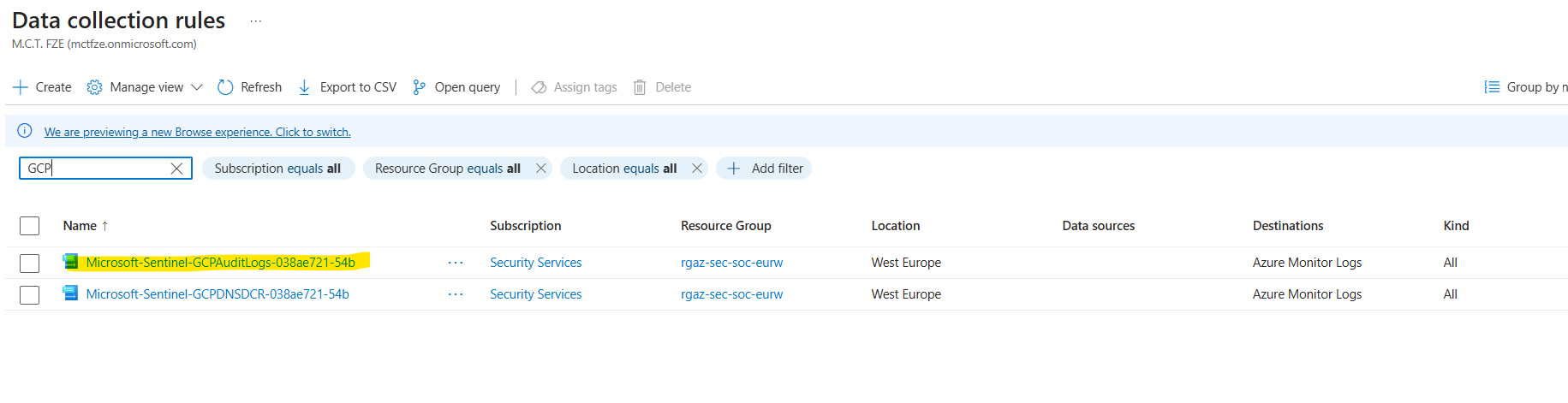
1. **Connect new collectors**

To enable GCP Audit Logs for Microsoft Sentinel, click the Add new collector button, fill the required information in the context pane and click on Connect.



1. Once we Fill the above details and click on connect, a new connector will get create with DCR.

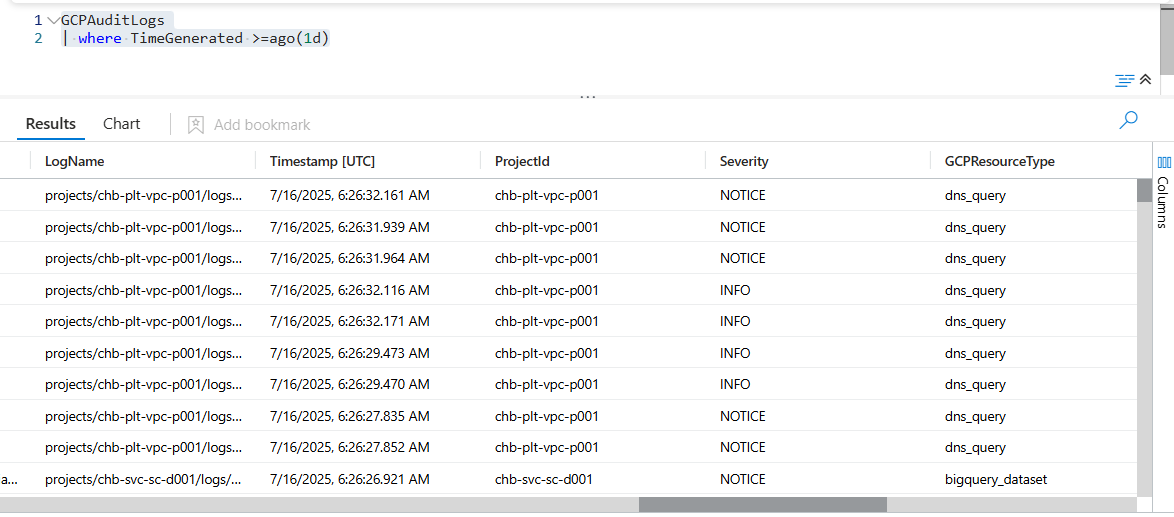




1. Once it is done, a log ingestion will be started, to validate log ingestion goto sentinel >> logs and run below query.,

GCPAuditLogs

| where TimeGenerated >=ago(1d)



GCPCloudDNS

| where TimeGenerated >=ago(1d)

A screenshot of a computer

AI-generated content may be incorrect.