2. Configure Stackdriver monitoring on an AWS EC2 instance using the monitoring agent. Also explore how to monitor both AWS and GCP projects at a single place.

1. Create a new GCP project or use an existing one.
2. Create a Workspace:
   a) In the GCP Navigation menu, Under Stackdriver, click on Monitoring.
   b) If the 'Add your project to a Workspace' dialog is displayed, create a new Workspace by selecting your GCP project under New Workspace and then clicking Add.
3. Create an AWS role:
   a) Log into your AWS IAM console and in the menu, click on Roles.
   b) Click on Create New Role.
   c) For Role type, select Another AWS account.
   d) In Account ID field, enter the account ID provided to you by Stackdriver.
   e) Check Require external ID.
   f) In the External ID field, enter the external ID provided to you by Stackdriver.
   g) Don't select Require MFA.
   h) Click on Next.
   i) In Policy names, select ReadOnlyAccess and click on Next.
   j) Review the configuration and click on Create Role.
   k) You'll see a summary page. Copy the Role ARN.
4. Add and AWS account to an existing Workspace:
   a) Go to Stackdriver Monitoring console.
   b) In the Workspace menu, select your Workspace.
   c) Click on Workspace Settings.
   d) Click on Monitoring accounts.
   e) Click on Add AWS account and enter the Account ID and External ID.
   f) In the Role ARN field, enter the Role ARN that you had copied while creating the AWS Role. Enter a short description.
   g) Click on Add AWS account.
5. Create a service account:
   a) Open the Service accounts page under IAM & Admin.
   b) Select the AWS connector project.
   c) Click on Create service account.
   d) Give it an appropriate name.
   e) In the Role field, for Monitoring, set Monitoring Metric Writer and for Logging, set Logs Writer.
   f) Select the Furnish a new private key checkbox.
   g) For Key type, select JSON.
   h) Uncheck the 'Enable G Suite Domain-wide Delegation' box.
   i) Click on Create and download the private-key file. Save the location of the credentials file in the variable CREDS on your workstation:
   CREDS="path/to/[PROJECT_NAME]-[KEY_ID].json"
6. Add a service account to a VM instance:
   a) From your workstation, copy the Stackdriver private-key credentials file to your AWS EC2 instance and save it in a file named temp.json by running the following command:
   scp -i "/path/to/key.pem" "$CREDS" AWS_USERNAME@AWS_HOSTNAME:temp.json
   b) On your EC2 instance, move the credentials to /etc/google/auth/application_default_credentials.json.
7. Install the Stackdriver Monitoring and Logging agents by running the following commands:
   curl -sSO https://dl.google.com/cloudagents/install-monitoring-agent.sh
   sudo bash install-monitoring-agent.sh

   curl -sSO https://dl.google.com/cloudagents/install-logging-agent.sh
   sudo bash install-logging-agent.sh –structured
8. Now, you can use Stackdriver services with AWS.