Question 2

Step 1 :

Create a new workspace or use the existing and identify your trusted account ID and external ID

- To obtain those, navigate to Stackdriver Monitoring console
- Select your workspace from besides the stackdriver logo
- Navigate to Workspace Settings and click Monitored accounts
- Click Add AWS account and record the Account ID and External ID
- Now before adding the account, you need to create an AWS role

Step 2 :

To create the AWS role -

- Log into your AWS IAM console and click Roles in the left-side menu
- Click Create New Role -
    - For the Role type, select Another AWS account.
    - In the Account ID field, enter the account ID provided by Stackdriver.
    - Select the Require external ID checkbox.
    - In the External ID field, enter the external ID provided by Stackdriver.
    - Don't select Require MFA.
    - Click Next: Permissions.
- From the Policy name drop-down list, select ReadOnlyAccess
- Now review the information that has been filled and create a role
- From the summary page, copy the Role ARN string so that you can give it to Stackdriver

Step 3 :

Now to connect to the AWS Account -

- On the Stackdriver Monitoring console select your workspace and navigate to the Managed Accounts section from Workspace Settings
- Now click Add AWS account and enter the Account ID and External ID
- Enter the Role ARN in the dedicated field and also put some description
- Now hit Add to connect the account

Step 4 :

So after connecting, we need to authorize applications running on AWS to access GCP services such as StackDriver or any other service

- For that purpose, a service account is created from the IAM section
- Select the AWS connector project that you have named
- As the project might not contain a service account if it is new, create one
    - In the Service account name field, enter Stackdriver agent authorization.
    - In the Role field, add both of the following values:
    - Monitoring > Monitoring Metric Writer
    - Logging > Logs Writer
    - Select Furnish a new private key checkbox.
    - For Key type, click JSON.

- Clear the Enable G Suite Domain-wide Delegation checkbox
- And finally hit Create which will download the service account's private-key file

Step 5 :

Now add Service Account to the VM Instance -

- From your workstation, copy the Stackdriver private-key credentials file to your AWS EC2 instance and save it in a file named temp.json. In the scp command, specify the path to key.pem, your AWS SSH key pair file, and provide your AWS credentials

  KEY="/path/to/key.pem"

  scp -i "$KEY" "$CREDS" AWS_USERNAME@AWS_HOSTNAME:temp.json
- On your EC2 instance, move the credentials to /etc/google/auth/application_default_credentials.json

  GOOGLE_APPLICATION_CREDENTIALS="/etc/google/auth/application_default_credentials.json"

  sudo mkdir -p $(dirname "$GOOGLE_APPLICATION_CREDENTIALS")

  sudo mv "$HOME/temp.json" "$GOOGLE_APPLICATION_CREDENTIALS"
  - Make sure the environment variable GOOGLE_APPLICATION_CREDENTIALS is visible to the agents and other applications that are authorized to use GCP. The environment variable name is understood by the standard GCP client libraries

Step 6 :

Install the agents -

- Install the Stackdriver Monitoring and Logging agents by running the following commands on your EC2 instance

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

Step 7 :

Now to use Stackdriver -

- Create an Uptime Check
- Create an Alerting Policy
- Create a dashboard and chart
- View your logs
  - In the Stackdriver Monitoring console left-side menu, go to Logging > AWS Link
  - The Logs Viewer for your AWS connector project, containes your AWS logs