Question #191 (Page:48)

You have deployed multiple Linux instances on Compute Engine. You plan on adding more instances in the coming weeks. You want to be able to access all of these instances through your SSH client over the internet without having to configure specific access on the existing and new instances. You do not want the Compute Engine instances to have a public IP. What should you do?

- A. Configure Cloud Identity-Aware Proxy for HTTPS resources.
- B. Configure Cloud Identity-Aware Proxy for SSH and TCP resources Most Voted
- C. Create an SSH keypair and store the public key as a project-wide SSH Key.
- D. Create an SSH keypair and store the private key as a project-wide SSH Key.

Correct Answer: B

- B is correct as question say no public IP on the instance.
- https://cloud.google.com/iap/docs/using-tcPage:forwarding#tunneling_ssh_connections

---

Question #168 (Page:42)

You are working for a hospital that stores its medical images in an on-premises data room. The hospital wants to use Cloud Storage for archival storage of these images. The hospital wants an automated process to upload any new medical images to Cloud Storage. You need to design and implement a solution. What should you do?

- A. Create a Pub/Sub topic, and enable a Cloud Storage trigger for the Pub/Sub topic. Create an application that sends all medical images to the Pub/Sub topic.
- B. Deploy a Dataflow job from the batch template, ג€Datastore to Cloud Storage.ג€ Schedule the batch job on the desired interval.
- C. Create a script that uses the gsutil command line interface to synchronize the on-premises storage with Cloud Storage. Schedule the script as a cron job.
- D. In the Cloud Console, go to Cloud Storage. Upload the relevant images to the appropriate bucket.

Correct Answer: C

- Pub/Sub will be good for all future files in in-prem data-storage. we want to sync all + new, so a local on-prem server running a cron job (not GCE CronJob) to run gsutil to transfer files to Cloud Storage would work.
- Answer is C. gsutil rsync <source_location> <destination_location>. This can sync content with Google cloud storage locations

---

Question #155 (page 39)

You are storing sensitive information in a Cloud Storage bucket. For legal reasons, you need to be able to record all requests that read any of the stored data. You want to make sure you comply with these requirements. What should you do?

- A. Enable the Identity Aware Proxy API on the project.
- B. Scan the bucket using the Data Loss Prevention API.

- C. Allow only a single Service Account access to read the data.
- D. Enable Data Access audit logs for the Cloud Storage API.

Correct Answer: D

- Cloud Audit Logs with Cloud Storage - Admin Activity audit log, Data Access audit log

---

Question #152 (Page:38)

Your company runs its Linux workloads on Compute Engine instances. Your company will be working with a new operations partner that does not use Google Accounts. You need to grant access to the instances to your operations partner so they can maintain the installed tooling. What should you do?

- A. Enable Cloud IAP for the Compute Engine instances, and add the operations partner as a Cloud IAP Tunnel User.
- B. Tag all the instances with the same network tag. Create a firewall rule in the VPC to grant TCP access on port 22 for traffic from the operations partner to instances with the network tag.
- C. Set up Cloud VPN between your Google Cloud VPC and the internal network of the operations partner.
- D. Ask the operations partner to generate SSH key pairs, and add the public keys to the VM instances.

Correct Answer: B

- the IAP allow you to access compute engine from the internet without having to have a GCP account
- IAP controls access to your App Engine apps and Compute Engine VMs.
- By default, IAP uses Google identities and IAM. By leveraging Identity Platform instead, you can authenticate users with a wide range of external identity providers, such as:
    - Email/password
    - OAuth (Google, Facebook, Twitter, GitHub, Microsoft, etc.)
    - SAML
    - OIDC
    - Phone number
    - Custom
    - Anonymous
- This is useful if your application is already using an external authentication system, and migrating your users to Google accounts is impractical.

Question #153(Page:39)

You have created a code snippet that should be triggered whenever a new file is uploaded to a Cloud Storage bucket. You want to deploy this code snippet. What should you do?

- A. Use App Engine and configure Cloud Scheduler to trigger the application using Pub/Sub.
- B. Use Cloud Functions and configure the bucket as a trigger resource.
- C. Use Google Kubernetes Engine and configure a CronJob to trigger the application using Pub/Sub.

- D. Use Dataflow as a batch job, and configure the bucket as a data source.

Correct Answer: B

- Google Cloud Storage Triggers

Question #130(page 33)

You manage an App Engine Service that aggregates and visualizes data from BigQuery. The application is deployed with the default App Engine Service account. The data that needs to be visualized resides in a different project managed by another team. You do not have access to this project, but you want your application to be able to read data from the BigQuery dataset. What should you do?

- A. Ask the other team to grant your default App Engine Service account the role of BigQuery Job User.
- B. Ask the other team to grant your default App Engine Service account the role of BigQuery Data Viewer.
- C. In Cloud IAM of your project, ensure that the default App Engine service account has the role of BigQuery Data Viewer.
- D. In Cloud IAM of your project, grant a newly created service account from the other team the role of BigQuery Job User in your project.

Correct Answer: B

Question #113 (page:29)

You need to assign a Cloud Identity and Access Management (Cloud IAM) role to an external auditor. The auditor needs to have permissions to review your Google Cloud Platform (GCP) Audit Logs and also to review your Data Access logs. What should you do?

- A. Assign the auditor the IAM role roles/logging.privateLogViewer. Perform the export of logs to Cloud Storage.
- B. Assign the auditor the IAM role roles/logging.privateLogViewer. Direct the auditor to also review the logs for changes to Cloud IAM policy.
- C. Assign the auditor's IAM user to a custom role that has logging.privateLogEntries.list permission. Perform the export of logs to Cloud Storage.
- D. Assign the auditor's IAM user to a custom role that has logging.privateLogEntries.list permission. Direct the auditor to also review the logs for changes to Cloud IAM policy

Correct Answer: C

- Yes, B is correct because: 1) Question doesn't ask us to export and store logs for any long period of time.
- why here cloud storage is mentioned ? they are mentioning only access and why this is coming in the middle

---

Question #106 (page:27)

Your organization has a dedicated person who creates and manages all service accounts for Google Cloud projects. You need to assign this person the minimum role for projects. What should you do?

- A. Add the user to roles/iam.roleAdmin role.
- B. Add the user to roles/iam.securityAdmin role.
- C. Add the user to roles/iam.serviceAccountUser role.
- D. Add the user to roles/iam.serviceAccountAdmin role.

Correct Answer: D

- Service Account User (roles/iam.serviceAccountUser): Includes permissions to list service accounts, get details about a service account, and impersonate a service account.

- Service Account Admin (roles/iam.serviceAccountAdmin): Includes permissions to list service accounts and get details about a service account. Also includes permissions to create, update, and delete service accounts, and to view or change the IAM policy on a service account.