|  |  |
| --- | --- |
| QUESTION | ANSWER/MISTAKE |
| You have a project for your App Engine application that serves a development environment. The required testing has succeeded and you want to create a new project to serve as your production environment. | * Use gcloud to create the new project, and then deploy your application to the new project * The deployment manager configuration file contains configuration about the resources that need to be created in Google cloud, however, it does not offer the feature to copy app engine deployment into a new project |
| You have a website hosted on App Engine standard environment. You want 1% of your users to see a new test version of the website. You want to minimize complexity. | Deploy the new version in the same application and use the --splits option to give a weight of 99 to the current version and a weight of 1 to the new version. |
| You have an application deployed in a GKE Cluster as a Kubernetes workload with Daemon Sets. Your application has become very popular and is now struggling to cope up with increased traffic. You want to add more pods to your workload and want to ensure your cluster scales up and scales down automatically based on volume. | Enable autoscaling on Kubernetes Engine  Enable Horizontal Pod Autoscaling for the Kubernetes deployment. is not right. Horizontal Pod Autoscaling can not be enabled for Daemon Sets, this is because there is only one instance of a pod per node in the cluster. |
| You have an application running in App Engine standard environment. You want to add a custom C# library to enhance the functionality of this application. However, C# isn’t supported by App Engine standard. You want to maintain the serverless aspect of your application. | * Containerize your new application and deploy it to a Cloud Run environment. * Containerize your new application and deploy it to a Cloud Run on GKE environment. |
| You have an application running in Google Kubernetes Engine (GKE) with cluster autoscaling enabled. This application exposes a TCP endpoint. There are several replicas of the application. You have a Compute Engine instance in the same region but in another Virtual Private Cloud (VPC) called pt-network that has no overlapping CIDR range with the other VPC. The instance needs to connect to the application on GKE. You want to minimize effort. | In GKE, create a Service of type LoadBalancer that uses the application’s Pods as backend. 2. Add an annotation to this service cloud.google.com/load-balancer-type: Internal 3. Peer the two VPCs together 4. Configure the Compute Engine instance to use the address of the load balancer that has been created. |
| You have an application that receives SSL-encrypted TCP traffic on port 443. Clients for this application are located all over the world. You want to minimize latency for the clients. | Network load balancer is used |
| You have annual audits every year and you need to provide external auditors access to the last 10 years of audit logs. You want to minimize the cost and operational overhead while following Google recommended practices. | Grant external auditors Storage Object Viewer role on the logs storage bucket  Configure a lifecycle management policy on the logs bucket to delete objects older than 10 years  Export audit logs to Cloud Storage via an audit log export sink. |
| You have asked your supplier to send you a purchase order and you want to enable them to upload the file to a cloud storage bucket within the next 4 hours. Your supplier does not have a Google account. You want to follow Google recommended practices. | Create a service account with just the permissions to upload files to the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -m PUT -d 4h gs:///po.pdf. |
| You have one project called ptech-sa where you manage all your service accounts. You want to be able to use a service account from this project to take snapshots of VMs running in another project called ptech-vm. | Grant the service account the IAM Role of Compute Storage Admin in the project called ptech-vm. |
| You have sensitive data stored in three Cloud Storage buckets and have enabled data access logging. You want to verify activities for a particular user for these buckets, using the fewest possible steps. You need to verify the addition of metadata labels and which files have been viewed from those buckets | Using the GCP Console, filter the Stackdriver log to view the information. is the right answer. Data access logs is already enabled, so we already record all API calls that read the configuration or metadata of resources, as well as user-driven API calls that create, modify, or read user-provided resource data. |
| You have two compute instances in the same VPC but in different regions. You can SSH from one instance to another instance using their external IP address but not their internal IP address. What could be the reason for SSH failing on the internal IP address? | The firewall rule can be configured to allow SSH traffic from 0.0.0.0/0 but deny traffic from the VPC range e.g. 10.0.0.0/8. In this case, all SSH traffic from within the VPC is denied but external SSH traffic (i.e. on external IP) is allowed. |
| You have two compute instances in the same VPC but in different regions. You can SSH from one instance to another instance using their internal IP address but not their external IP address. What could be the reason for SSH failing on external IP address? | * The combination of compute instance network tags and VPC firewall rules only allow SSH from the subnets IP range. is the right answer. * The combination of compute instance network tags and VPC firewall rules can certainly result in SSH traffic being allowed from only subnets IP range. * The firewall rule can be configured to allow SSH traffic from just the VPC range e.g. 10.0.0.0/8. |
| You want to configure auto-healing for network load balancer for a group of Compute Engine instances that run in multiple zones using the fewest possible steps. You need to configure the recreation of VMs if they are unresponsive after 3 attempts of 10 seconds each | * Create a managed instance group. Set the Autohealing health check to healthy (HTTP) * Create a HTTP load balancer with a backend configuration that references an existing instance group. Define a balancing mode and set the maximum RPS to 10 is not right. You set RPS (Requests per Second) on load balancer when using RATE balancing mode. This has no effect on auto-healing. |
| You need to set up permissions for a set of Compute Engine instances to enable them to write data into a particular Cloud Storage bucket. You want to follow Google-recommended practices. | Create a service account with an access scope. Use the access scope 'https://www.googleapis.com/auth/cloud-platform'. |
| You need to set up a policy so that videos stored in a specific Cloud Storage Regional bucket are moved to Coldline after 90 days and then deleted after one year from their creation. | * Use Cloud Storage Object Lifecycle Management using Age conditions with SetStorageClass and Delete actions. Set the SetStorageClass action to 90 days and the Delete action to 365 days. is the right answer. * Object Lifecycle Management does not rewrite an object when changing its storage class. * This means that when an object is transitioned to Nearline Storage, Coldline Storage, or Archive Storage using the SetStorageClass feature, any subsequent early deletion and associated charges are based on the original creation time of the object, regardless of when the storage class changed. |
| You need to reduce GCP service costs for a division of your company using the fewest possible steps. You need to turn off all configured services in an existing GCP project | 1. Verify that you are assigned the Project Owners IAM role for this project. 2. Locate the project in the GCP console, click Shut down and then enter the project ID. |
| You need to produce a list of the enabled Google Cloud Platform APIs for a GCP project using the gcloud command line in the Cloud Shell. The project name is my-project. | * Run gcloud projects list to get the project ID, and then run gcloud services list --project . is the right answer. For the gcloud services list command, --enabled is the default. So running gcloud services list --project is the same as running gcloud services list --project --enabled which would get all the enabled services for the project. * --available. is not right. --available return the services available to the project to enable and not the services that are enabled. |
| You have two workloads on GKE (Google Kubernetes Engine) – create-order and dispatch-order. create-order handles the creation of customer orders, and dispatch-order handles dispatching orders to your shipping partner. Both create-order and dispatch-order workloads have cluster autoscaling enabled. The create-order deployment needs to access (i.e. invoke web service of) dispatch-order deployment. dispatch-order deployment cannot be exposed publicly. | * Create a Service of type NodePort for dispatch-order and an Ingress Resource for that Service. Have create-order use the Ingress IP address. is not right.   Exposes the Service on each Node’s IP at a static port (the NodePort). If the compute instance has public connectivity, the dispatch-order can be accessed publicly which is undesirable. Secondly, dispatch-order has auto-scaling enabled so we shouldn't create a service of NodePort. If autoscaler spins up another pod on the node, it fails to initialize as the port on the node is already taken by an existing pod on the same node.   * Create a Service of type ClusterIP for dispatch-order. Have create-order use the Service IP address. is the right answer.   ClusterIP exposes the Service on a cluster-internal IP that is only reachable within the cluster. This satisfies our requirement that dispatch-order shouldn't be publicly accessible. create-order which is also located in the same GKE cluster can now access the ClusterIP of the service to reach dispatch-order |
| You host a static website in Cloud Storage. Recently you began to include links to PDF files on this site. Currently, when users click on links to these PDF files, their browser prompts them to save the file to their machine locally. However, you want the clicked PDF files to be displayed within the browser window directly without prompting the user to save the files locally. | * Set Content-Type metadata to application/pdf on the PDF file objects is the right answer. Content-Type allows browsers to render the object properly. * If the browser prompts users to save files to their machine, it is likely the browser does not see the Content-Type as application/pdf. Setting this would ensure the browser displays PDF files within the browser instead of popping up a download dialog. |
| You installed Stackdriver Logging agent on all compute instances. You now need to forward logs from all Compute Engine instances to a BigQuery dataset called pt-logs. You want to minimize cost. What should you do? | * Give the BigQuery Data Editor role on the pt-logs dataset to the service accounts used by your instances. Update your instances' metadata to add the following value: logs-destination: bq://pt-logs. is not right. * Among other things, roles/bigquery.dataEditor lets you Create, update, get, and delete the dataset's tables. However, setting a metadata tag logs-destination to bq://pt-logs has no effect on how the logs are generated or forwarded. * The stack driver agent is already installed so the logs are forwarded to stack driver logging and not to the BigQuery dataset * In Stack driver Logging, create a filter to view only Compute Engine logs. 2. Click Create Export. 3. Choose BigQuery as Sink Service, and the pt-logs dataset as Sink Destination. is the right answer. In stack driver logging, it is possible to create a filter to just query the compute engine logs which is what we are interested in. |
| You need to create a custom IAM role for use with a GCP service. All permissions in the role must be suitable for use. You also want to clearly share with your organization the status of the custom role. This will be the first version of the custom role. | * Use permissions in your role that use the SUPPORTED support level for role permissions. Set the role stage to ALPHA while testing the role permissions. * TESTING - The permission is being tested to check its compatibility with custom roles. You can include the permission in custom roles, but you might see unexpected behavior. Not recommended for production use. Since we want the role to be suitable for production use, we need "SUPPORTED" and not "TESTING". |
| You need to create a custom VPC with a single subnet. The subnet’s range must be as large as possible. | Only one of three IPA CIDR blocks and out of them, whichev one has lowest no. of occupied bits  10.0.0.0/  192.168.0.0/  172.16.0.0/ |
| You need to create a new billing account and then link it with an existing Google Cloud Platform project. | Project Billing Manager has power not Billing Admin |
| You need to host an application on a Compute Engine instance in a project shared with other teams. You want to prevent the other teams from accidentally causing downtime on that application. | * shielded VMs don't offer protection for accidental termination of the instance. * Enable deletion protection on the instance. is the right answer. |
| You need to monitor resources that are distributed over different projects in Google Cloud Platform. You want to consolidate reporting under the same Stackdriver Monitoring dashboard. | * Configure a single Stackdriver account, and link all projects to the same account. is the right answer. You can monitor resources of different projects in a single Stackdriver account by creating a Stackdriver workspace. * Use Shared VPC to connect all projects, and link Stackdriver to one of the projects. is not right. Linking Stackdriver to one project brings metrics from that project alone. A Shared VPC allows an organization to connect resources from multiple projects to a common Virtual Private Cloud (VPC) network so that they can communicate with each other securely and efficiently using internal IPs from that network. But it does not help in linking all projects to a single Stackdriver workspace/account. |
| You are designing a large distributed application with 30 microservices. Each of your distributed microservices needs to connect to a database back-end. You want to store the credentials securely. | recommended practice to store the credentials in a secret management system such as KMS. Applications often require access to small pieces of sensitive data at build or run time. These pieces of data are often referred to as secrets. |
| Your company’s test suite is a custom C++ application that runs tests throughout each day on Linux virtual machines. The full test suite takes several hours to complete, running on a limited number of on-premises servers reserved for testing. Your company wants to move the testing infrastructure to the cloud, to reduce the amount of time it takes to fully test a change to the system, while changing the tests as little as possible. | Google Compute Engine managed instance group can help the testing application to scale to reduce the amount of time to run tests. |
| A Company is planning the migration of their web application to Google App Engine. However, they would still continue to use their on-premises database. | Setup the application using App Engine Flexible environment with Cloud VPN to connect to database  App Engine standard cannot use Cloud VPN |
| A lead software engineer tells you that his new application design uses websockets and HTTP sessions that are not distributed across the web servers. You want to help him ensure his application will run properly on Google Cloud Platform. | * Meet with the cloud operations team and the engineer to discuss load balancer options. * We ain’t gonna redesign system without websockets just to migrate to GCP |
| You have an application server running on Compute Engine in the europe-west1-d zone. You need to ensure high availability and replicate the server to the europe-west2-c zone using the fewest steps possible. | * Create a snapshot from the disk. Create a disk from the snapshot in the europe-west2-c zone. Create a new VM with that disk. * Disks are zonal resources, so they reside in a particular zone for their entire lifetime. The contents of a disk can be moved to a different zone by snapshotting the disk (using gcloud compute disks snapshot) and creating a new disk using –source-snapshot in the desired zone. The contents of a disk can also be moved across project or zone by creating an image (using gcloud compute images create) and creating a new disk using –image in the desired project and/or zone. |
| Your developers are trying to select the best compute service to run a static website. They have a dozen HTML pages, a few JavaScript files, and some CSS. They need the site to be highly available for the few weeks it is running. They also have a limited budget. What is the best service to use to run the site? | the website is static and needs to be hosted with high availability and limited budget, Cloud Storage would be an ideal choice. |
| Your developers have been thoroughly logging everything that happens in the API. The API allows end users to request the data as JSON, XML, CSV, and XLS. Supporting all of these formats is taking a lot of developer effort. Management would like to start tracking which options are used over the next month. Without modifying the code, what’s the fastest way to be able to report on this data at the end of the month? | User-defined (logs-based) metrics are created by a user on a project. They count the number of log entries that match a given filter, or keep track of particular values within the matching log entries.  Faster than sinking to bigQuery |
| You are a project owner and need your co-worker to deploy a new version of your application to App Engine. You want to follow Google’s recommended practices. Which IAM roles should you grant your co-worker? | App Engine Deployer |
| You’re writing a Python application and want your application to run in a sandboxed managed environment with the ability to scale up in seconds to account for huge spikes in demand. Which service should you host your application on? | App Engine Standard Environment provides rapid scaling as compared to App Engine Flexible Environment and is ideal for applications requiring quick start times and handle sudden and extreme spikes. |
| You are creating a solution to remove backup files older than 90 days from your backup Cloud Storage bucket. You want to optimize ongoing Cloud Storage spend. What should you do? | Write a lifecycle management rule in JSON and push it to the bucket with gsutil  XML ain’t supported by gsutil |
| You need to create a new Kubernetes Cluster on Google Cloud Platform that can autoscale the number of worker nodes. What should you do? | Create a cluster on Kubernetes Engine and enable autoscaling on Kubernetes Engine. |
| Your company has appointed external auditors for auditing the security of your setup. They want to check all the users and roles configured. | Ask Auditors to navigate to the IAM page and check member and roles section |
| Your company has created a new billing account and needs to move the projects to the billing account. What roles are needed to change the billing account? | To change the billing account for an existing project, you must be an owner on the project and a billing administrator on the destination billing account. (Project Billing Manager not required) |
| You’re migrating an on-premises application to Google Cloud. The application uses a component that requires a licensing server. The license server has the IP address 10.28.0.10. You want to deploy the application without making any changes to the code or configuration. How should you go about deploying the application? | * Create a subnet with a CIDR range of 10.28.0.0/28. Reserve a static internal IP address of 10.28.0.10. Assign the static address to the license server instance * the IP is internal it can be reserved using the static internal IP address, which blocks it and prevents it from getting allocated to other resource. |
| You have a project using BigQuery. You want to list all BigQuery jobs for that project. You want to set this project as the default for the bq command-line tool. What should you do? | Use "gcloud config set project" to set the default project |
| You are creating a Kubernetes Engine cluster to deploy multiple pods inside the cluster. All container logs must be stored in BigQuery for later analysis. You want to follow Google-recommended practices. Which two approaches can you take? | Turn on Stackdriver Logging during the Kubernetes Engine cluster creation.  Use the Stackdriver Logging export feature to create a sink to BigQuery. Specify a filter expression to export log records related to your Kubernetes Engine cluster only. |
| You have created a Kubernetes deployment, called Deployment-A, with 3 replicas on your cluster. Another deployment, called Deployment-B, needs access to Deployment-A. You cannot expose Deployment-A outside of the cluster. What should you do? | Create a Service of type ClusterIP for Deployment A. Have Deployment B use the Service IP address. |
| You have an App Engine application serving as your front-end. It’s going to publish messages to Pub/Sub. The Pub/Sub API hasn’t been enabled yet. What is the fastest way to enable the API? | * simplest way to enable an API for the project is using the GCP console. * providing the Pub/Sub Admin role does not provide the access to enable API. Enabling an API requires the following two Cloud Identity and Access Management permissions: 1. The servicemanagement.services.bind permission on the service to enable. This permission is present for all users for public services. For private services, you must share the service with the user who needs to enable it. 2. The serviceusage.services.enable permission on the project to enable the service on. This permission is present in the Editor role as well as in the Service Usage Admin role. |
| Your manager needs you to test out the latest version of MS-SQL on a Windows instance. You’ve created the VM and need to connect into the instance. What steps should you follow to connect to the instance? | * connecting to Windows instance involves installation of the RDP client. GCP does not provide RDP client and it needs to be installed. Generate Windows instance password to connect to the instance. * GCP Console does not have a direct RDP connectivity. |
| Your security team wants to be able to audit network traffic inside of your network. What’s the best way to ensure they have access to the data they need? | VPC Flow Logs |
| You’ve been tasked with getting all of your team’s public SSH keys onto to a specific Bastion host instance of a particular project. You’ve collected them all. With the fewest steps possible, what is the simplest way to get the keys deployed? | Add all of the keys into a file that's formatted according to the requirements. Use the gcloud compute instances add-metadatacommand to upload the keys to each instance  Not added over project as only specific instance is granted the privilege |
| Your billing department has asked you to help them track spending against a specific billing account. They’ve indicated that they prefer to use Excel to create their reports so that they don’t need to learn new tools. Which export option would work best for them? | File Export with CSV |
| Your project manager wants to delegate the responsibility to upload objects to Cloud Storage buckets to his team members. Considering the principle of least privilege, which role should you assign to the team members? | roles/storage.objectCreator  Not the ”object admin” role as only uploading of objects is required |
| Your application has a large international audience and runs stateless virtual machines within a managed instance group across multiple locations. One feature of the application lets users upload files and share them with other users. Files must be available for 30 days; after that, they are removed from the system entirely. Which storage solution should you choose? | Multi region GCS bucket  Not Filestore as disks are regional and not ideal for sharable content |
| Your company wants to track whether someone is present in a meeting room reserved for a scheduled meeting. There are 1000 meeting rooms across 5 offices on 3 continents. Each room is equipped with a motion sensor that reports its status every second. The data from the motion detector includes only a sensor ID and several different discrete items of information. Analysts will use this data, together with information about account owners and office locations. Which database type should you use? | NoSQL like Bigtable and Datastore solution is an ideal solution to store sensor ID and several different discrete items of information. It also provides an ability to join with other data. Datastore can also be configured to store data in multi-region locations. |
| You’re attempting to deploy a new instance that uses the centos 7 family. You can’t recall the exact name of the family. Which command could you use to determine the family names? | gcloud compute images list |
| You’ve been tasked with getting all of only the operations team’s public SSH keys onto to a specific Bastion host instance of a particular project. Currently Project wide access has already been granted to all the instances within the projects. With the fewest steps possible, how do you block or override the project level access on the Bastion host? | Use the gcloud compute instances add-metadata [INSTANCE\_NAME] --metadata block-project-ssh-keys=TRUEcommand to block the access  This will only allow users whose public SSH key is stored in instance-level metadata to access the instance. If you want your instance to use both project-wide and instance-level public SSH keys, set the instance metadata to allow project-wide SSH keys. |
| You have created an App engine application in the development environment. The testing for the application has been successful. You want to move the application to production environment. How can you deploy the application with minimal steps? | Perform app engine deploy using the --project parameter  gcloud app deploy allows the –project parameter to be passed to override the project that the app engine application needs to be deployed to. Refer GCP documentation – Cloud SDK |
| Your company has deployed their application on managed instance groups, which is served through a network load balancer. They want to enable health checks for the instances. How do you configure the health checks? | Perform the health check using HTTP by hosting a basic web server  Network Load Balancer does not support TCP health checks and hence HTTP health checks need to be performed. You can run a basic web server on each instance for health checks. |
| An engineer from your team accidentally deployed several new versions of NodeJS application on Google App Engine Standard. You are concerned the new versions are serving traffic. You have been asked to produce a list of all the versions of the application that are receiving traffic as well the percent traffic split between them. What should you do? | * gcloud app versions list --hide-no-traffic |
| Every employee of your company has a Google account. Your operational team needs to manage a large number of instances on the Compute Engine. Each member of this team needs only administrative access to the servers. Your security team wants to ensure that the deployment of credentials is operationally efficient and must be able to determine who accessed a given instance. What should you do? | * Ask each member of the team to generate a new SSH key pair and to add the public key to their Google account. * Grant the "compute.osAdminLogin" role to the Google group corresponding to this team. |
| For service discovery, you need to associate each of the Compute Engine instances of your VPC with an internal (DNS) record in a custom zone. You want to follow Google recommended practices. What should you do? | * Create a Cloud DNS zone, set its visibility to private and associate it with your VPC. Create records for each instance in that zone. is the right answer. * You should absolutely do this when you want internal DNS records in a custom zone. Cloud DNS gives you the option of private zones and internal DNS names. |
| You are building an application that will run in your data center. The application will use Google Cloud Platform (GCP) services like AutoML. You created a service account that has appropriate access to AutoML. You need to enable authentication to the APIs from your on-premises environment. What should you do? | * Use gcloud to create a key file for the service account that has appropriate permissions. is the right answer. * To use a service account outside of Google Cloud, such as on other platforms or on-premises, you must first establish the identity of the service account. Public/private key pairs provide a secure way of accomplishing this goal. You can create a service account key using the Cloud Console, the gcloud tool, the serviceAccounts.keys.create() method, or one of the client libraries. |
| You are hosting an application on bare metal servers in your data center. The application needs access to Cloud Storage. However, security policies prevent the servers hosting the application from having public IP addresses or access to the internet. You want to follow Google recommended practices to provide the application with access to Cloud Storage. What should you do? | * Using Cloud VPN or Interconnect, create a tunnel to a VPC in GCP Using Cloud Router to create a custom route advertisement for 199.36.153.4/30. Announce that network to your on-premises network through the VPN tunnel. In your on-premises network, configure your DNS server to resolve \*.googleapis.com as a CNAME to restricted.googleapis.com is the right answer right, and it is what Google recommends. * You must configure routes so that Google API traffic is forwarded through your Cloud VPN or Cloud Interconnect connection, firewall rules on your on-premises firewall to allow the outgoing traffic, and DNS so that traffic to Google APIs resolves to the IP range you've added to your routes.” “You can use Cloud Router Custom Route Advertisement to announce the Restricted Google APIs IP addresses through Cloud Router to your on-premises network. The Restricted Google APIs IP range is 199.36.153.4/30. While this is technically a public IP range, Google does not announce it publicly. This IP range is only accessible to hosts that can reach your Google Cloud projects through internal IP ranges, such as through a Cloud VPN or Cloud Interconnect connection.” Without having a public IP address or access to the internet, the only way you could connect to cloud storage is if you have an internal route to it. So Negotiate with the security team to be able to give public IP addresses to the servers is not right. Following “Google recommended practices” is synonymous with “using Google’s services” |
| You have a number of compute instances belonging to an unmanaged instances group. You need to SSH to one of the Compute Engine instances to run an ad hoc script. You’ve already authenticated gcloud, however, you don’t have an SSH key deployed yet. In the fewest steps possible, what’s the easiest way to SSH to the instance? | Use the gcloud compute ssh command. |
| You have a Linux VM that must connect to Cloud SQL. You created a service account with the appropriate access rights. You want to make sure that the VM uses this service account instead of the default Compute Engine service account. What should you do? | * When creating the VM via the web console, specify the service account under the ‘Identity and API Access’ section. is the right answer. You can set the service account at the time of creating the compute instance. * You can also update the service account used by the instance - this requires that you stop the instance first and then update the service account. Setting/Updating the service account can be done either via the web console or by executing gcloud command or by the REST API. |
| You have a development project with appropriate IAM roles defined. You are creating a production project and want to have the same IAM roles on the new project, using the fewest possible steps. What should you do? | * Use gcloud iam roles copy and specify the production project as the destination project. * In the Google Cloud Platform Console, use the 'create role from role' functionality. is not right. This creates a role in the same (development) project, not in the production project. |
| You have a developer laptop with Cloud SDK installed on Ubuntu. The cloud SDK was installed from Google Cloud Ubuntu package repository. You want to test your application locally on your laptop with Cloud Datastore. What should you do? | * Install the cloud-datastore-emulator component using the gcloud components install command. is the right answer. * The Datastore emulator provides local emulation of the production Datastore environment. You can use the emulator to develop and test your application locally |
| You deployed an App Engine application using gcloud app deploy, but it did not deploy to the intended project. You want to find out why this happened and where the application deployed. What should you do? | Go to Cloud Shell and run gcloud config list to review the Google Cloud configurations used for deployment. |
| You deployed a number of services to Google App Engine Standard. The services are designed as microservices with several interdependencies between them. Most services have few version upgrades but some key services have over 20 version upgrades. You identified an issue with the service pt-createOrder and deployed a new version v3 for this service. You are confident this works and want this new version to receive all traffic for the service. You want to minimize effort and ensure the availability of service. What should you do? | Execute gcloud app versions migrate v3 --service="pt-createOrder" |
| You built an application on Google Cloud Platform that uses Cloud Spanner. The support team needs to monitor the environment but should not have access to the data. You need a streamlined solution to grant the correct permissions to your support team, and you want to follow Google recommended practices. What should you do? | Add the support team group to the roles/monitoring.viewer role |
| You are using multiple configurations for gcloud. You want to review the configured Kubernetes Engine cluster of an inactive configuration using the fewest possible steps. What should you do? | Use kubectl config get-contexts to review the output. |
| You are using Google Kubernetes Engine with autoscaling enabled to host a new application. You want to expose this new application to the public, using HTTPS on a public IP address. What should you do? | * Create a Kubernetes Service of type NodePort for your application, and a Kubernetes Ingress to expose this Service via a Cloud Load Balancer. is the right answer. * This meets all our requirements. With (Global) Cloud Load Balancing, a single anycast IP front-ends all your backend instances in regions around the world. It provides cross-region load balancing, including automatic multi-region failover, which gently moves traffic in fractions if backends become unhealthy. * The ingress accepts traffic from the cloud load balancer and can distribute the traffic across the pods in the cluster. |
| You are using Deployment Manager to create a Google Kubernetes Engine cluster. Using the same Deployment Manager deployment, you also want to create a DaemonSet in the kube-system namespace of the cluster. You want a solution that uses the fewest possible services. What should you do? | * Add the cluster's API as a new Type Provider in Deployment Manager, and use the new type to create the DaemonSet. * A type provider exposes all resources of a third-party API to Deployment Manager as base types that you can use in your configurations. * If you have a cluster running on Google Kubernetes Engine, you could add the cluster as a type provider and access the Kubernetes API using Deployment Manager. Using these inherited API, you can create a DaemonSet. |
| You are setting up a Windows VM on Compute Engine and want to make sure you can log in to the VM via RDP. What should you do? | * After the VM has been created, use gcloud compute reset-windows-password to retrieve the login credentials for the VM. is the right answer. * You can generate Windows passwords using either the Google Cloud Console or the gcloud command-line tool. This option uses the right syntax to reset the windows password. gcloud compute reset-windows-password windows-instance |
| You are migrating a mission critical on-premises application to cloud. The application requires 96 vCPUs to perform its task. You want to make sure the application runs in a similar environment on GCP. What should you do? | When creating the VM, use machine type n1-standard-96.  Create the VM using Compute Engine default settings. Use gcloud to modify the running instance to have 96 vCPUs. is not right. You can't increase the vCPUs to 96 without changing the machine type. While it is possible to set machine type using gcloud, this would mean downtime for the mission-critical application |
| You have a managed instance group comprised of preemptible VM’s. All of the VM’s keep deleting and recreating themselves every minute. What is a possible cause of this behavior? | * Your managed instance group's VM's are toggled to only last 1 minute in preemptible settings. |
| You write a Python script to connect to Google BigQuery from a Google Compute Engine virtual machine. The script is printing errors that it cannot connect to BigQuery. What should you do to fix the script? | * Run your script on a new virtual machine with the BigQuery access scope enabled * by default an instance is associated with default service account and default access scope, neither of which provides an access to BigQuery. While Service account is the recommended approach and Access scope are legacy, access scope still need to granted to the instance for applications to access the services. So enabling only the Service Account with role would not enable the script to access BigQuery. |
| You have created a Kubernetes engine cluster named ‘project-1’. You’ve realized that you need to change the machine type for the cluster from n1-standard-1 to n1-standard-4. What is the command to make this change? | * When you need to change the machine profile of your Compute Engine cluster, you can create a new node pool and then migrate your workloads over to the new node pool. To migrate your workloads without incurring downtime, you need to: Mark the existing node pool as unschedulable. Drain the workloads running on the existing node pool. Delete the existing node pool. |
| You need to have a backup/rollback plan in place for your application that is distributed across a large managed instance group. What is the preferred method for doing so? | * Use the Rolling Update feature to deploy/roll back versions with different managed instance group templates. |
| You’re deploying an application to a Compute Engine instance, and it’s going to need to make calls to read from Cloud Storage and Bigtable. You want to make sure you’re following the principle of least privilege. What’s the easiest way to ensure the code can authenticate to the required Google Cloud APIs? | * Create a new service account and key with the required limited permissions. Set the instance to use the new service account. Edit the code to use the service account key. * Default GCE does not have permission only to APIs so no point in even thinking about access scopes for it |
| A SysOps admin has configured a lifecycle rule on an object versioning disabled multi-regional bucket. Which of the following statement effect reflects the following lifecycle config? | * Move objects to Coldline Storage after 365 days if the storage class in Multi-regional First rule has no effect on the bucket. * Since object versioning is disabled, object will never be live i.e. never have a latest version |
| The development team has provided you with a Kubernetes Deployment file. You have no infrastructure yet and need to deploy the application. What should you do? | * Use gcloud to create a Kubernetes cluster. Use kubectl to create the deployment. |
| One of the microservices in your application has an intermittent performance problem. You have not observed the problem when it occurs but when it does, it triggers a particular burst of log lines. You want to debug a machine while the problem is occurring. What should you do? | * Set up a log metric in Stackdriver Logging, and then set up an alert to notify you when the number of log lines increases past a threshold. |
| You’re writing a Java application with lot a threading and concurrency. You want your application to run in a sandboxed managed environment with the ability to perform SSH debugging to check on any thread dump for troubleshooting. Which service should you host your application on? | * App Engine provides the managed service and Flexible environment supports the ability to perform SSH debugging. |
| A company is hosting their Echo application on Google Cloud using Google Kubernetes Engine. The application is deployed with deployment echo-deployment exposed with echo-service. They have a new image that needs to be deployed for the application. How can the change be deployed with minimal downtime? | * Update image using kubectl set image deployment * the image can be directly updated using the kubectl command and Kubernetes Engine performs a rolling update. |
| A company uses Cloud Storage for storing their critical data. As a part of compliance, the objects need to be encrypted using customer-supplied encryption keys. How should the object be handled to support customer-supplied encryption? | * Use gsutil with GSUtil:encryption\_key=[YOUR\_ENCRYPTION\_KEY] to pass the encryption key |
| The development team needs a regional MySQL database with point-in-time recovery for a new proof-of-concept application. What’s the most inexpensive way to enable point-in-time recovery? | * Binary Logging |
| Your application deployed on a Google Compute Engine virtual machine instance needs to connect to Google Cloud Pub/Sub. What is the best way to provision the access to the application? | * VM needs to be granted permissions using the service account to be able to communicate with Cloud Pub/Sub. * Without permission, there is no point of having an access scope |
| Your company pushes batches of sensitive transaction data from its application server VMs to Cloud Pub/Sub for processing and storage. What is the Google-recommended way for your application to authenticate to the required Google Cloud services? | * Ensure that VM service accounts are granted the appropriate Cloud Pub/Sub IAM roles. |
| You have an application deployed on Kubernetes Engine using a Deployment named echo-deployment. The deployment is exposed using a Service called echo-service. You need to perform an update to the application with minimal downtime to the application. What should you do? | * Use kubectl set image deployment/echo-deployment * image can be directly updated using the kubectl command and Kubernetes Engine performs a rolling update. |
| You have a Linux VM that must connect to Cloud SQL. You created a service account with the appropriate access rights. You want to make sure that the VM uses this service account instead of the default Compute Engine service account. What should you do? | * When creating the VM via the web console, specify the service account under the 'Identity and API Access' section. |
| You have a project for your App Engine application that serves a development environment. The required testing has succeeded and you want to create a new project to serve as your production environment. What should you do? | * Use gcloud to create the new project, and then deploy your application to the new project. * You can’t copy an application to another project |
| You created an instance of SQL Server 2017 on Compute Engine to test features in the new version. You want to connect to this instance using the fewest number of steps. What should you do? | * Install a RDP client on your desktop. Verify that a firewall rule for port 3389 exists |
| You’re working on setting up a cluster of virtual machines with GPUs to perform some 3D rendering for a customer. They’re on a limited budget and are looking for ways to save money. What is the best solution for implementing this? | * Use an autoscaled managed instance group containing some preemptible instances. * No GPUs supported for app engine |
| You need to connect to one of your Compute Engine instances using SSH. You’ve already authenticated gcloud, however, you don’t have an SSH key deployed yet. In the fewest steps possible, what’s the easiest way to connect to the app? | * Use gcloud compute ssh * gcloud compute ssh is a thin wrapper around the ssh(1) command that takes care of authentication and the translation of the instance name into an IP address. gcloud compute ssh ensures that the user’s public SSH key is present in the project’s metadata. If the user does not have a public SSH key, one is generated using ssh-keygen(1) (if the –quiet flag is given, the generated key will have an empty passphrase). |
| You want to migrate an application from Google App Engine Standard to Google App Engine Flex. Your application is currently serving live traffic and you want to ensure everything is working in Google App Engine Flex before migrating all traffic. You want to minimize effort and ensure the availability of service. What should you do? | * Set env: flex in app.yaml gcloud app deploy --no-promote --version=[NEW\_VERSION] * Validate [NEW\_VERSION] in App Engine Flex * gcloud app versions migrate [NEW\_VERSION] |
| You want to use Google Cloud Storage to host a static website on [http://www.example.com](http://www.example.com/) for your staff. You created a bucket example-static-website and uploaded index.html and css files to it. You turned on static website hosting on the bucket and set up a CNAME record on [http://www.example.com](http://www.example.com/) to point to c.storage.googleapis.com. You access the static website by navigating to [http://www.example.com](http://www.example.com/) in the browser but your index page is not displayed. What should you do? | * Delete the existing bucket, create a new bucket with the name www.example.com and upload the html/css files. is the right answer. We need to create a bucket whose name matches the CNAME you created for your domain. For example, if you added a CNAME record pointing www.example.com to c.storage.googleapis.com., then create a bucket with the name "www.example.com". |
| Your company has an existing GCP organization with hundreds of projects and a billing account. Your company recently acquired another company that also has hundreds of projects and its own billing account. You would like to consolidate all GCP costs of both GCP organizations onto a single invoice and you would like to do this as soon as possible. What should you do? | * Link the acquired company's projects to your company's billing account. * Migrating em to existing org takes a lotta time |
| Your company has migrated most of the data center VMs to Google Compute Engine. The remaining VMs in the data center host legacy applications that are due to be decommissioned soon and your company has decided to retain them in the datacenter. Due to a change in the business operational model, you need to introduce changes to one of the legacy applications to read files from Google Cloud Storage. However, your data center does not have access to the internet and your company doesn’t want to invest in setting up internet access as the data center is due to be turned off soon. Your data center has a partner interconnect to GCP. You wish to route traffic from your datacenter to Google Storage through partner interconnect. What should you do? | * In on-premises DNS configuration, map \*.googleapis.com to restricted.googleapis.com, which resolves to the 199.36.153.4/30. 2. Configure Cloud Router to advertise the 199.36.153.4/30 IP address range through the Cloud VPN tunnel. 3. Add a custom static route to the VPC network to direct traffic with the destination 199.36.153.4/30 to the default internet gateway. 4. Created a Cloud DNS managed private zone for \*.googleapis.com that maps to 199.36.153.4/30 and authorize the zone for use by VPC network |
| Your Company is planning to migrate all Java web applications to Google App Engine. However, you still want to continue using your on-premise database. How can you set up the app engine to communicate with your on-premise database while minimizing effort? | * Setup the application using App Engine Standard environment with Cloud VPN to connect to an on-premise database. * Converting to a container model involves effort and we want to minimize effort |
| Your company procured a license for a third-party cloud-based document signing system for the procurement team. All members of the procurement team need to sign in with the same service account. Your security team prohibits sharing service account passwords. You have been asked to recommend a solution that lets the procurement team login as the service account in the document signing system but without the team knowing the service account password. What should you do? | * Register the application as a password vaulted app and set the credentials to the service account credentials. * As a G Suite or Cloud Identity administrator, the password vaulted apps service enables you to manage access to some of the apps that don't support federation and that are available to users on the User Dashboard. |
| Your company stores sensitive PII data in a cloud storage bucket. The objects are currently encrypted by Google-managed keys. Your compliance department has asked you to ensure all current and future objects in this bucket are encrypted by customer-managed encryption keys. You want to minimize effort. What should you do? | * In the bucket advanced settings, select the Customer-managed key and then select a Cloud KMS encryption key. 2. Rewrite all existing objects using gsutil rewrite to encrypt them with the new Customer-managed key. |
| Your company uses a legacy application that still relies on the legacy LDAP protocol to authenticate. Your company plans to migrate this application to cloud and is looking for a cost effective solution while minimizing any developer effort. What should you do? | * Use secure LDAP to authenticate the legacy application and ask users to sign in through Gmail * Using cloud directory sync takes developer effort |
| Your company uses BigQuery for data warehousing. Over time, many different business units in your company have created 1000+ datasets across hundreds of projects. Your CIO wants you to examine all datasets to find tables that contain an employee\_ssn column. You want to minimize effort in performing this task. What should you do? | * Go to Data Catalog and search for employee\_ssn in the search box. |
| Your company wants to move all documents from a secure internal NAS drive to a Google Cloud Storage (GCS) bucket. The data contains personally identifiable information (PII) and sensitive customer information. Your company tax auditors need access to some of these documents. What security strategy would you recommend on GCS? | * Grant no Google Cloud Identity and Access Management (Cloud IAM) roles to users, and use granular ACLs on the bucket. |
| Your managed instance group raised an alert stating that new instance creation has failed to create new instances. You need to maintain the number of running instances specified by the template to be able to process expected application traffic. What should you do? | * Verify that the instance template being used by the instance group contains valid syntax. Delete any persistent disks with the same name as instance names. Set the disks.autoDelete property to true in the instance template. |
| Your customer has implemented a solution that uses Cloud Spanner and notices some read latency-related performance issues on one table. This table is accessed only by their users using a primary key. The table schema is shown below. | * Change the primary key to not have monotonically increasing values. * You should be careful when choosing a primary key to not accidentally create hotspots in your database. One cause of hotspots is having a column whose value monotonically increases as the first key part because this results in all inserts occurring at the end of your keyspace. This pattern is undesirable because Cloud Spanner divides data among servers by key ranges, which means all your inserts will be directed at a single server that will end up doing all the work. |