**GLOSSARY**

|  |  |
| --- | --- |
| TERM | DESCRIPTION |
| Tomcat server | Apache Tomcat is a long-lived, open source Java servlet container that implements several core Java enterprise specs, namely the Java Servlet, JavaServer Pages (JSP), and WebSockets APIs |
| Binary Authorization | * Binary Authorization is a deploy-time security control that ensures only trusted container images are deployed on Google Kubernetes Engine (GKE). * With Binary Authorization, you can require images to be signed by trusted authorities during the development process and then enforce signature validation when deploying. * By enforcing validation, you can gain tighter control over your container environment by ensuring only verified images are integrated into the build-and-release process. |
| Container Analysis API | An implementation of the Grafeas API, which stores, and enables querying and retrieval of critical metadata about all of your software artifacts. |
| gVisor | * gVisor is more lightweight than a VM while maintaining a similar level of isolation. * gVisor is an application kernel for containers that provides efficient defense-in-depth anywhere. * By providing each container with its own application kernel, gVisor limits the attack surface of the host. |
| Containerd | * industry-standard container runtime that's supported by Kubernetes, and used by many other projects. * Containerd provides the layering abstraction that allows for the implementation of a rich set of features like [gVisor](https://gvisor.dev/) to extend Kubernetes functionality. * Containerd is considered more resource efficient and secure when compared to the Docker runtime. |
| Squid Proxy Server | * Squid is a full-featured web proxy cache server application which provides proxy and cache services for HTTP, File Transfer Protocol (FTP), and other popular network protocols. * Squid can implement caching and proxying of SSL requests and caching of DNS lookups, and perform transparent caching. |
| LDAP | * LDAP (Lightweight Directory Access Protocol) is an open and cross platform protocol used for directory services authentication. * Directory services store the users, passwords, and computer accounts, and share that information with other entities on the network. |
| Passing a startup script through command line | * You can only pass a local startup script file by using the **gcloud** command-line tool. Include the **--metadata-from-file** flag, followed by a metadata key pair, **startup-script=**PATH\_TO\_FILE, replacing PATH\_TO\_FILE with a relative path to the startup script: * gcloud compute instances create example-instance \   --metadata-from-file startup-script=examples/scripts/install.sh |
| gcloud topic filters | * gcloud topic filters - resource filters supplementary help * The **--format=**NAME[ATTRIBUTES]**(**PROJECTION**)** and **--filter=**EXPRESSION flags along with projections can be used to format and change the default output to a more meaningful result. |
| SDK Properties | * Properties are settings that govern the behavior of the gcloud CLI and other SDK tools. * Properties can be used to define a per-product or per-service setting such as the account used by the gcloud CLI and other Cloud SDK tools for authorization, the default region to be used when working with Google Compute Engine resources, or even the option to turn off automatic Cloud SDK component updates. * Properties can also be used to define gcloud command-line tool preferences like verbosity level and prompt configuration for gcloud CLI commands. |
| RFC1918 | * An [RFC1918](https://tools.ietf.org/html/rfc1918) address is an IP address that is assigned by an enterprise organization to an internal host. These IP addresses are used in [private networks](https://en.wikipedia.org/wiki/Private_network), which are not available, or reachable, from the Internet. * 10.0.0.0 – 10.255.255.255  (10/8 prefix) * 172.16.0.0 – 172.31.255.255  (172.16/12 prefix) * 192.168.0.0 – 192.168.255.255 (192.168/16 prefix) |
| gcloud services enable | * gcloud services enable - enables a service for consumption for a project * [gcloud services list](https://cloud.google.com/sdk/gcloud/reference/services/list) --available * gcloud services enable my-consumed-service * gcloud services enable my-consumed-service --async * gcloud services enable service1 service2 service3 |
| SPF - Sender Policy Framework | An SPF record is a TXT record that is part of a domain's DNS (Domain Name Service). An SPF record lists all authorized hostnames / IP addresses that are permitted to send email on behalf of your domain. |
| DKIM - DomainKeys Identified Mail | DKIM is a process to validate sending domain names associated to email messages through cryptographic authentication. It achieves this by inserting a digital signature into the message header which is later verified by the receiving host to validate the authenticity of the sending domain. |
| DNSSEC | The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. |
| gRPC  RPC - remote procedure call | * connect services in and across data centers with pluggable support for load balancing, tracing, health checking and authentication. * It is also applicable in last mile of distributed computing to connect devices, mobile applications and browsers to backend services. |
| SDK Configurations | A configuration is a named set of SDK [properties](https://cloud.google.com/sdk/docs/properties). These properties are key-value pairs, organized in sections, that govern the behavior of the gcloud command-line tool and other SDK tools. |
| Cloud Auto ML | Cloud AutoML enables developers with limited machine learning expertise to train high-quality models specific to their business needs. |
| Cloud Tasks | * Cloud Tasks is a fully managed service that allows you to manage the execution, dispatch, and delivery of a large number of distributed tasks. * Using Cloud Tasks, you can perform work asynchronously outside of a user or service-to-service request. |
| Shielded VMs | * Shielded VMs are virtual machines (VMs) on Google Cloud hardened by a set of security controls that help defend against rootkits and bootkits. * Using Shielded VMs helps protect enterprise workloads from threats like remote attacks, privilege escalation, and malicious insiders. * Shielded VMs leverage advanced platform security capabilities such as secure and measured boot, a virtual trusted platform module (vTPM), UEFI firmware, and integrity monitoring. |
| gcloud projects | * The gcloud projects group lets you create and manage IAM policies for projects |
| query dry run | When you run a query in the **bq** command-line tool, you can use the **--dry\_run** flag to estimate the number of bytes read by the query. You can also use the **dryRun** parameter when submitting a query job using the API or client libraries.  You can use the estimate returned by the dry run to calculate query costs in the pricing calculator. You are not charged for performing the dry run. |
| Signed URL | * A signed URL is a URL that provides limited permission and time to make a request. Signed URLs contain authentication information in their query string, allowing users without credentials to perform specific actions on a resource. * When you generate a signed URL, you specify a user or [service account](https://cloud.google.com/iam/docs/service-accounts) which must have sufficient permission to make the request that the signed URL will make. * After you generate a signed URL, anyone who possesses it can use the signed URL to perform specified actions, such as reading an object, within a specified period of time. |
| Sink-ing logs | * Every time a log entry arrives in a project, folder, billing account, or organization resource, Logging compares the log entry to the sinks in that resource. Each sink whose filter matches the log entry writes a copy of the log entry to the sink's export destination. |
| Live Migration | Live migration migrates your running instances to another host in the same zone so that Google can perform maintenance such as a software or hardware update. It can not be used for changing machine type. |
| MaxSurge | maxSurge specifies the maximum number of instances that can be created over the desired number of instances. If maxSurge is set to 0, the rolling update can not create additional instances and is forced to update existing instances. |
| Traffic Splitting | * You can use traffic splitting to specify a percentage distribution of traffic across two or more of the versions within a service. Splitting traffic allows you to conduct A/B testing between your versions and provides control over the pace when rolling out features. * Each application in the app engine is different and it is not possible to split traffic between applications in App Engine. You can use traffic splitting to specify a percentage distribution of traffic across two or more of the versions within a service but not across applications. |
| App Engine flexible | * Not serverless |
| Activity Logs | * Activity logs display a list of all actions and you can restrict this down to a user and further filter by specifying Data access as the Activity types and GCS Bucket as the Resource type. * But that is the extent of the filter functionality in Activity logs.   It is not possible to restrict the activity logs to just some specific buckets that we are interested in. Secondly, it is not possible to restrict the activity logs to just the gets and updates. |
| Cloud Run | * Cloud Run implements the Knative serving API, an open-source project to run serverless workloads on top of Kubernetes. * That means you can deploy Cloud Run services anywhere Kubernetes runs. * And if you need more control over your services (like access to GPU or more memory), you can also deploy these serverless containers in your own GKE cluster instead of using the fully managed environment. When using the fully managed environment, Cloud Run on GKE is serverless. |
| cross region SSH IAM permissions. | * No such thing |
| RPS | Requests per sec |
| to modify the gcloud configuration such that you are prompted for a zone when you execute the create instance commands above. | gcloud config unset compute/zone |
| IPSec VPN | * IPsec VPN is one of two common VPN protocols, or set of standards used to establish a VPN connection. * IPsec is set at the IP layer, and it is often used to allow secure, remote access to an entire network (rather than just a single device). IPsec VPNs come in two types: tunnel mode and transport mode. |
| Ad hoc SQL query (done in bq) | In SQL, an ad hoc query is a loosely typed command/query whose value depends upon some variable. Each time the command is executed, the result is different, depending on the value of the variable. ... An ad hoc query is short lived and is created at runtime |
| Expand Subnets | gcloud compute networks subnets expand-ip-range –region= –prefix-length=27 |
| Parallel uploading files to GCS | * It splits a large file into component pieces, uploads them in parallel and then recomposes them once they’re in the cloud (and deletes the temporary components it created locally). * gsutil -o GSUtil:parallel\_composite\_upload\_threshold=150M cp ./localbigfile gs://your-bucket Where “localbigfile” is a file larger than 150MB. This divides up your data into chunks ~150MB and uploads them in parallel, increasing upload performance. * Faster than multi threading |
| .boto file | The boto configuration file contains values that control how gsutil behaves. For example, the prefer\_api variable determines which API gsutil preferentially uses. Boto configuration file variables can be changed by editing the configuration file directly. While most users won't need to edit these variables, those do typically do so for one of the following reasons:   * Setting up gsutil to work through a proxy. * Using [customer-managed or customer-supplied encryption keys](https://cloud.google.com/storage/docs/encryption). * Performing specialized customization of global gsutil behavior. |
| TCP port 22 | For SSH (Ubuntu, Linux) |
| TCP port 3389 | For RDP |
| Cloud Audit Logs | Cloud Audit Logs provides the following audit logs for each Cloud project, folder, and organization:   * Admin Activity audit logs * Policy Denied audit logs * Data Access audit logs * System Event audit logs |
| BigQuery data | Can’t be accessed by members outside the organization |
| VPC Flow Logs | VPC Flow Logs record a sample of network flows sent from and received by VM instances. These logs can be used for network monitoring, forensics, real-time security analysis, and expense optimization.  Flow logs are aggregated by connection, at 5-second intervals, from Compute Engine VMs and exported in real time. By subscribing to Cloud Pub/Sub, you can analyze flow logs using real-time streaming APIs. |
| VPC Network Logs | No such thing |
| Deploying a Cloud Function | deploy your function from the directory containing your function code with thegcloud functions deploy command:  gcloud functions deploy NAME –runtime RUNTIME TRIGGER [FLAGS…] |
| Bastion Hosts | A **bastion host** is a special-purpose computer on a network specifically designed and configured to withstand attacks. The computer generally **hosts** a single application, for example a proxy **server**, and all other services are removed or limited to reduce the threat to the computer. |
| NAT – Network Address Translation | **Network address translation** (NAT) is a method of remapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. |

|  |  |
| --- | --- |
| CNAME | * .A CNAME record is a type of DNS record. It directs traffic that requests a URL from your domain to the resources you want to serve, eg, objects in your Cloud Storage buckets. * For www.example.com, the CNAME record might contain the following information: NAME TYPE DATA www.example.com CNAME c.storage.googleapis.com. |
| Data Catalog | * fully managed and scalable metadata management service that empowers organizations to quickly discover, understand, and manage all their data. * It offers a simple and easy-to-use search interface for data discovery, a flexible and powerful cataloging system for capturing both technical and business metadata, and a strong security and compliance foundation with Cloud Data Loss Prevention (DLP) and Cloud Identity and Access Management (IAM) integrations. |
| Binary Logging | * The binary log is a set of log files that contain information about data modifications made to a MySQL server instance. The log is enabled by starting the server with the --log-bin option. The binary log was introduced in MySQL 3.23. ... It contains all statements that update data. |
| Cloud Composer |  |
| signurl - Create a signed url | * gsutil signurl [-c <content\_type>] [-d <duration>] [-m <http\_method>] \ * [-p <password>] [-r <region>] [-b <project>] (-u | <private-key-file>) \ * (gs://<bucket\_name> | gs://<bucket\_name>/<object\_name>)... |
| Add memory | * Stop instance and change it’s machine type |
| Cloud Composer | * A fully managed workflow orchestration service built on Apache Airflow. * Author, schedule, and monitor pipelines that span across hybrid and multi-cloud environments * Cloud Composer's managed nature and Apache Airflow compatibility allows you to focus on authoring, scheduling, and monitoring your workflows as opposed to provisioning resources. |

BILLING ACCOUNT ROLES

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Purpose | Level | Use Case |
| Billing Account Creator (roles/billing.creator) | Create new self-serve (online) billing accounts. | Organization | Use this role for initial billing setup or to allow creation of additional billing accounts. Users must have this role to sign up for Google Cloud with a credit card using their corporate identity. Tip: Minimize the number of users who have this role to help prevent proliferation of untracked cloud spend in your organization. |
| Billing Account Administrator (roles/billing.admin) | Manage billing accounts (but not create them). | Organization or billing account. | This role is an owner role for a billing account. Use it to manage payment instruments, configure billing exports, view cost information, link and unlink projects and manage other user roles on the billing account. |
| Billing Account User (roles/billing.user) | Link projects to billing accounts. | Organization or billing account. | This role has very restricted permissions, so you can grant it broadly, typically in combination with Project Creator. These two roles allow a user to create new projects linked to the billing account on which the role is granted. |
| Billing Account Viewer (roles/billing.viewer) | View billing account cost information and transactions. | Organization or billing account. | Billing Account Viewer access would usually be granted to finance teams, it provides access to spend information, but does not confer the right to link or unlink projects or otherwise manage the properties of the billing account. |
| Project Billing Manager (roles/billing.projectManager) | Link/unlink the project to/from a billing account. | Organization, folder, or project. | This role allows a user to attach the project to the billing account, but does not grant any rights over resources. Project Owners can use this role to allow someone else to manage the billing for the project without granting them resource access. |

GCS ROLES

| Role | Description |  |
| --- | --- | --- |
| Storage Object Creator (roles/storage.objectCreator) | Allows users to create objects. Does not give permission to view, delete, or replace objects. |  |
| Storage Object Viewer (roles/storage.objectViewer) | Grants access to view objects and their metadata, excluding ACLs.  Can also list the objects in a bucket. |  |
| Storage Object Admin (roles/storage.objectAdmin) | Grants full control over objects, including listing, creating, viewing, and deleting objects. |  |
| Storage HMAC Key Admin (roles/storage.hmacKeyAdmin) | Full control over HMAC keys in a project. This role can only be applied to a project. |  |
| Storage Admin (roles/storage.admin) | Grants full control of buckets and objects.  When applied to an individual bucket, control applies only to the specified bucket and objects within the bucket. |  |

APP ENGINE ROLES

| Role | Title | Description |  |  |
| --- | --- | --- | --- | --- |
| roles/appengine.appAdmin | App Engine Admin | Read/Write/Modify access to all application configuration and settings.  To deploy new versions, you must also grant the [Service Account User](https://cloud.google.com/iam/docs/impersonating-service-accounts#allow-impersonation) (roles/iam.serviceAccountUser) role.  To use the gcloud tool to deploy, you must add the Storage Admin (roles/compute.storageAdmin) and Cloud Build Editor (roles/cloudbuild.builds.editor) roles. |  |  |
| roles/appengine.appCreator | App Engine Creator | Ability to create the App Engine resource for the project. |  |  |
| roles/appengine.appViewer | App Engine Viewer | Read-only access to all application configuration and settings. |  |  |
| roles/appengine.codeViewer | App Engine Code Viewer | Read-only access to all application configuration, settings, and deployed source code. |  |  |
| roles/appengine.deployer | App Engine Deployer | Read-only access to all application configuration and settings.  To deploy new versions, you must also grant the [Service Account User](https://cloud.google.com/iam/docs/impersonating-service-accounts#allow-impersonation) (roles/iam.serviceAccountUser) role.  To use the gcloud tool to deploy, you must add the Storage Admin (roles/compute.storageAdmin) and Cloud Build Editor (roles/cloudbuild.builds.editor) roles.  Cannot modify existing versions other than deleting versions that are not receiving traffic. |  |  |
| roles/appengine.serviceAdmin | App Engine Service Admin | Read-only access to all application configuration and settings.  Write access to module-level and version-level settings. Cannot deploy a new version. |  |  |

GCE ROLES

Just read em from google

SUPPORT LEVEL FOR PERMISSIONS

|  |  |
| --- | --- |
| Support level | Description |
| SUPPORTED | The permission is fully supported in custom roles. |
| 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. |
| NOT\_SUPPORTED | The permission is not supported in custom roles. |

CLOUD STORAGE STATIC WEBSITE

To host a static site in Cloud Storage, you need to create a Cloud Storage bucket, upload the content, and test your new site. You can serve your data directly from storage.googleapis.com, or you can verify that you own your domain and use your domain name. Either way, you’ll get consistent, fast delivery from global edge caches.  
You can create your static web pages however you choose. For example, you could hand-author pages by using HTML and CSS. You can use a static-site generator, such as Jekyll, Ghost, or Hugo, to create the content. Static-site generators make it easier for you to create a static website by letting you author in markdown, and providing templates and tools. Site generators generally provide a local web server that you can use to preview your content.  
After your static site is working, you can update the static pages by using any process you like. That process could be as straightforward as hand-copying an updated page to the bucket. You might choose to use a more automated approach, such as storing your content on GitHub and then using a webhook to run a script that updates the bucket. An even more advanced system might use a continuous-integration /continuous-delivery (CI/CD) tool, such as Jenkins, to update the content in the bucket. Jenkins has a Cloud Storage plugin that provides a Google Cloud Storage Uploader post-build step to publish build artifacts to Cloud Storage.  
If you have a web application that needs to serve static content or user-uploaded static media, using Cloud Storage can be a cost-effective and efficient way to host and serve this content, while reducing the amount of dynamic requests to your web application.

APP ENGINE ENVIRONMENTS

## The App Engine environments

App Engine is well suited to applications that are designed using a [microservice](https://wikipedia.org/wiki/Microservices) architecture, especially if you decide to utilize both environments. Use the following sections to learn and understand which environment best meets your application's needs.

### When to choose the standard environment

Application instances run in a [sandbox](https://en.wikipedia.org/wiki/Sandbox_(computer_security)), using the runtime environment of a supported language listed below.

Applications that need to deal with rapid scaling.

The standard environment is optimal for applications with the following characteristics:

* Source code is written in specific versions of the supported programming languages:
  + Python 2.7, Python 3.7, Python 3.8
  + Java 8, Java 11
  + Node.js 8, Node.js 10, and Node.js 12
  + PHP 5.5, PHP 7.2, PHP 7.3, and PHP 7.4
  + Ruby 2.5, Ruby 2.6, and Ruby 2.7
  + Go 1.11, Go 1.12, Go 1.13, and Go 1.14
* Intended to run for free or at very low cost, where you pay only for what you need and when you need it. For example, your application can scale to 0 instances when there is no traffic.
* Experiences sudden and extreme spikes of traffic which require immediate scaling.

### When to choose the flexible environment

Application instances run within Docker containers on Compute Engine virtual machines (VM).

Applications that receive consistent traffic, experience regular traffic fluctuations, or meet the parameters for scaling up and down gradually.

The flexible environment is optimal for applications with the following characteristics:

* Source code that is written in a version of any of the supported programming languages:  
  Python, Java, Node.js, Go, Ruby, PHP, or .NET
* Runs in a Docker container that includes a custom runtime or source code written in other programming languages.
* Uses or depends on frameworks that include native code.
* Accesses the resources or services of your Google Cloud project that reside in the Compute Engine network.

## Comparing high-level features

The following table summarizes the differences between the two environments:

| Feature | Standard environment | Flexible environment |
| --- | --- | --- |
| Instance startup time | Seconds | Minutes |
| Maximum request timeout | Depends on the [runtime and type of scaling.](https://cloud.google.com/appengine/docs/standard/python/how-instances-are-managed#timeout) | 60 minutes |
| Background threads | Yes, with restrictions | Yes |
| Background processes | No | Yes |
| SSH debugging | No | Yes |
| Scaling | Manual, Basic, Automatic | Manual, Automatic |
| Scale to zero | Yes | No, minimum 1 instance |
| Writing to local disk | * Java 8, Java 11, Node.js, Python 3, PHP 7, Ruby, Go 1.11, and Go 1.12+ have read and write access to the /tmp directory. * Python 2.7 and PHP 5.5 don't have write access to the disk. | Yes, ephemeral (disk initialized on each VM startup) |
| Modifying the runtime | No | Yes (through Dockerfile) |
| Deployment time | Seconds | Minutes |
| Automatic in-place security patches | Yes | Yes (excludes container image runtime) |
| Access to Google Cloud APIs & Services such as [Cloud Storage](https://cloud.google.com/storage/docs), [Cloud SQL](https://cloud.google.com/sql/docs), [Memorystore](https://cloud.google.com/memorystore/docs), [Tasks](https://cloud.google.com/tasks/docs) and others. | Yes | Yes |
| WebSockets | No Java 8, Python 2, and PHP 5 provide a proprietary Sockets API (beta), but the API is not available in newer standard runtimes. | Yes |
| Supports installing third-party binaries | * Yes for Java 8, Java 11, Node.js, Python 3, PHP 7, Ruby, Go 1.11, and Go 1.12+. * No for Python 2.7 and PHP 5.5. | Yes |
| Location | North America, Asia Pacific, or Europe | North America, Asia Pacific, or Europe |
| Pricing | Based on [instance hours](https://cloud.google.com/appengine/pricing#standard_instance_pricing) | Based on usage of [vCPU, memory, and persistent disks](https://cloud.google.com/appengine/pricing#costs-for-flexible-environment-instances) |

For an in-depth comparison of the environments, see the guide for your language: [Python](https://cloud.google.com/appengine/docs/flexible/python/flexible-for-standard-users), [Java](https://cloud.google.com/appengine/docs/flexible/java/flexible-for-standard-users), [Go](https://cloud.google.com/appengine/docs/flexible/go/flexible-for-standard-users), or [PHP](https://cloud.google.com/appengine/docs/flexible/php/flexible-for-standard-users).

## Comparing the flexible environment to Compute Engine

The App Engine flexible environment has the following differences to Compute Engine:

* Flexible environment VM instances are restarted on a weekly basis. During restarts, Google's management services apply any necessary operating system and security updates.
* You always have root access to Compute Engine VM instances. By default, SSH access to the VM instances in the flexible environment is disabled. If you choose, you can enable root access to your app's VM instances.
* Code deployments can take longer as container images are built by using the Cloud Build service.
* The geographical region of a flexible environment VM instance is determined by the location that you specify for the [App Engine application](https://cloud.google.com/appengine/docs/locations) of your Cloud project. Google's management services ensures that the VM instances are co-located for optimal performance.

## Testing on App Engine

Before configuring a new version to receive traffic, you can test it on App Engine. For example, to test a new version of your default service:

1. Deploy your new version and include the --no-promote flag:

gcloud app deploy --no-promote

1. Access your new version by navigating to the following URL:

https://VERSION\_ID-dot-default-dot-PROJECT\_ID.[REGION\_ID](https://cloud.google.com/appengine/docs/flexible/nodejs/testing-and-deploying-your-app#appengine-urls).r.appspot.com

**Note:** You can find the version ID in the [Cloud Console](https://console.cloud.google.com/appengine/versions), or specify one when you deploy with the --version flag. The gcloud tool also outputs the version ID when you deploy.

Now you can test your new version in the App Engine runtime environment. You can debug your application by viewing its logs in the Google Cloud Console [Logs Viewer](https://console.cloud.google.com/logs). For more information, see [Writing Application Logs](https://cloud.google.com/appengine/docs/flexible/nodejs/writing-application-logs).

Requests sent to https://PROJECT\_ID.[REGION\_ID](https://cloud.google.com/appengine/docs/flexible/nodejs/testing-and-deploying-your-app#appengine-urls).r.appspot.com will still be routed to the version previously configured to receive traffic.

1. When you want to send traffic to the new version, use the Cloud Console to migrate traffic: Select the version you just deployed and click **Migrate traffic**.