Google Cloud Platform (GCP)

Last updated by | shakibesaib | Sep 29, 2023 at 3:00 PM GMT+6

What is GCP?

GCP is a public cloud vendor — like competitors Amazon Web Services (AWS) and Microsoft Azure. With GCP and other cloud vendors, customers are able to access computer resources housed in Google's data centers around the world for free or on a pay-per-use basis.

GCP offers a suite of computing services to do everything from GCP cost management to data management to delivering web and video over the web to AI and machine learning tools.

Google Cloud vs Google Cloud Platform

Google Cloud includes a combination of services available over the internet that can help organizations go digital. Google Cloud Platform (which provides public cloud infrastructure for hosting web-based applications and is the focus of this blog post) is a part of Google Cloud.

Some other services that are a part of Google Cloud include:

- Google Workspace, formerly known as G Suite and Google Apps. This product provides identity management for organizations, Gmail, and collaboration tools.
- Enterprise versions of Android and Chrome OS. These phone and laptop operating systems are ways for users to connect to web-based applications.
- Application programming interfaces (APIs) for machine learning and enterprise mapping services. These provide software-to-software communication.

While Google's GCP cloud infrastructure is the backbone of applications like Google Workplace, these applications aren't what we're talking about when we talk about GCP. For this post, we're focusing on Google Cloud Platform.

Google Cloud Platform infrastructure, regions, and zones

Google's global infrastructure currently has 24 locations around the world where Google Cloud Platform resources are offered.

Locations start with a region and within a region are availability zones. These zones are isolated from a single point of failure. Some resources such as the HTTP global load balancer are global and can receive requests from any of the Google edge locations and regions.

Other resources, like storage, can be regional. The storage is distributed across multiple zones within a region for redundancy.

And finally zonal resources, including compute instances, are only available in one specific zone within one specific region.

When deploying applications on GCP, you must select the locations depending on the performance, reliability, scalability, and security needs of your organization.

What are Google Cloud Platform services?

Each GCP region offers a category of services. Some services are limited to specific regions. Major services of Google Cloud Platform include:

- Computing and hosting
- Storage and database

- Networking
- Big Data
- Machine learning

Best practices for optimizing your cloud costs
Useful Resources:

- https://cloud.google.com/blog/topics/cost-management/best-practices-for-optimizing-your-cloud-costs
- https://cloud.google.com/architecture/cost-efficiency-on-google-cloud

GCP Security

Securing your Google Cloud Platform (GCP) environment is essential to ensure the safety and integrity of your data and resources. GCP offers a range of security features and tools to help you protect your environment, but there are also a few simple steps you can take to enhance the security of your GCP account.

- **Enable multi-factor authentication (MFA) for all user accounts**
  One of the most effective ways to secure your GCP account is to enable MFA for all user accounts. MFA requires users to provide an additional form of authentication, such as a code sent to their phone or a security key, when logging in to their GCP account. This helps to prevent unauthorized access to your account, even if someone has obtained your password.

- **Set up firewall rules**
  GCP's firewall allows you to control inbound and outbound traffic to and from your GCP resources. This is an important step in protecting your resources from external threats and unauthorized access.

- **Use identity and access management (IAM)**
  IAM allows you to control access to your GCP resources by setting up roles and permissions for different users and groups. This is an important step in ensuring that only authorized users have access to the resources they need.

- **Encrypt sensitive data**
  Encrypting your data helps to protect it from unauthorized access, both at rest and in transit. GCP offers several options for encrypting data, including using customer-managed encryption keys, which allow you to control the encryption keys used to encrypt your data.

- **Use virtual private clouds (VPCs)**
  Virtual private clouds (VPCs) allow you to create a virtual network within GCP and control access to the resources within that network. This can be a useful tool for isolating your resources and controlling access to them.

- **VPC Service Controls**
  Virtual Private Cloud (VPC) service controls are a security feature in Google Cloud Platform (GCP) that allow you to control access to your resources within a VPC network. VPC service controls allow you to create a perimeter around your resources and specify which actions can be taken on those resources.

- **Cloud Armour for your Publicly available worklaods**
  Google Cloud Armor is a network security service that provides distributed denial of service (DDoS) protection for Google Cloud Platform (GCP) resources, including Compute Engine and Google Kubernetes Engine (GKE) clusters. It is designed to protect against external threats such as DDoS attacks, and can also be used to protect against application-level attacks by using Web Application Firewall (WAF) rules.

- **Use Cloud Identity-Aware Proxy (Cloud IAP)**
  Cloud Identity-Aware Proxy (Cloud IAP) allows you to control access to your GCP resources based on the identity of the user. Cloud IAP allows you to grant or deny access to specific resources based on the user's identity and their role in your organization. This can be a useful tool for controlling access to sensitive resources and protecting them from unauthorized access.

- **Regularly review and monitor your resources**
  Regularly reviewing and monitoring your GCP resources can help you ensure that they are secure. This can include monitoring for security threats and vulnerabilities, as well as performing regular security assessments and audits.

Implement security best practices

In addition to the specific security measures mentioned above, it's important to implement security best practices to help protect your GCP environment from potential security threats. Some best practices to consider include:

- Regularly updating software: Ensuring that all software is up to date with the latest security patches can help to protect your resources from known vulnerabilities.
- Using strong, unique passwords: Strong passwords that are unique to each user can help to prevent unauthorized access to your GCP account.
- Limiting access to sensitive resources: Only grant access to sensitive resources to users who need it, and regularly review and revoke access as needed.
- Conducting regular security assessments and audits: Regularly reviewing your security practices and conducting security assessments and audits can help you identify potential weaknesses in your GCP environment and take steps to address them.

For implementation and more details- https://medium.com/google-cloud/gcp-security-101-a-beginners-guide-to-keeping-your-resources-safe-6da1cc09b5a1