The Top 3 Tech Giant Cloud Services

Ivan Marchany

Abstract

The new virtual techniques, and the increase in the use of computer networks has led to the emergence of cloud computing.
Cloud computing represents a new tool for the use of technology resources that are completely based on internet, which allows the user to access on demand to a set of shared resources and computer services, such as infrastructure, platform and applications.
There are more and more companies offering their cloud services. Cloud providers provide access to computer resources through the network, and offer a series of additional value-added services that will bring the provider's offer closer to their client's needs. Depending on the completeness of this added value, we can say that we have a solution of one level or another.

The development of cloud computing started through large Internet service companies like Google and Amazon which built their own infrastructure. From there arose an architecture: a system of distributed resources in a horizontal way, introduced as virtual technology services of information scaled massively and managed as resources grouped and configured continuously.
There is a sector of technology group people that understands that cloud computing is too rigorous, limiting the self-determination of users and making them as dependent on the service provider. But there is an unpredictable aspect as it moves in the cloud and is security, because to achieve all the potential of computing in the cloud the person needs to overcome the challenges of performance, reliability and scalability that the Internet presents. This paper proposes to analyze, compare and understand the cloud computing by exploring current offerings of AWS EC2, Microsoft Azure Container Service and Google Compute Engine, as well as the challenges they face due to its dependence on Internet services.

Amazon Elastic Compute Cloud (Amazon EC2)

Description:
Amazon Elastic Compute Cloud (Amazon EC2, http://aws.amazon.com/es/) is a Web service that offers computing resources in the cloud. Allows the deployment of virtual machine images over pre-defined size instances to provide on-demand computing. The virtual machine is like an ISO image that contains a hardware configuration, installation of an operating system, applications and data. Amazon EC2 represents a virtual computer that allows to use Web service interfaces to start instances with different operating systems. It includes several interfaces that allow managing in the Amazon Elastic Compute Cloud (EC2) isolated applications in Docker containers. AWS uses the term instance to refer to a virtual machine where each instance type can have a different number (CPU), amount of memory, capacity, and number of disks. Amazon EC2 allows to increase or reduce capacity in a matter of minutes without waiting for long hours. The user could send as many instances they want to the server at the same time. Amazon EC2 can be integrated with other in-house services such as: AWS Identity and Access Management (IAM), Elastic Load Balancing, AWS Cloud Trail, and Amazon Cloud Formation.

Main features:

Amazon EC2 allows to increase or reduce the capacity in a matter of minutes, without waiting hours or days. The user can send one, hundreds, or even thousands of instances of the server at the same time. Of course, since all this process is managed through web service, the application will scale (increase or decrease its capacity) depending on the specific needs.

Control:
Total Control over the instances. User may have access to all them, and might interact with instances as with any other machine. The user has the ability to stop the instances and can preserve the partition data to start the same instance using the Web Service applications.

Using the web service application programming interface, the user could restart instances remotely. In addition, the user could have access to the console problem of instances

Flexible
The user has the advantage of being able to select which of the instances will be used, the operating system and also the software. It is common that the operating system includes distributions of Linux servers and Microsoft Windows. It is versatile in its use as it can be used with other Web services. For example, Amazon EC2 is compatible with the Amazon simple Storage service (Amazon S3), Amazon relational Database service (Amazon RDS), Amazon SimpleDB and Amazon Simple Queue service (Amazon SQS). In this sense, it allows the user to have a complete service of computation that goes from the queries to the storage of several applications.

Reliable
In the context of reliability, Amazon EC2 offers a very reliable structure since replacement instances can be handled in a fast and early manner. Amazon's configured network and structure is used to perform the services. The advantage of the Amazon EC2 service is that it is available in each of its areas, representing a 99.95% availability. In addition, its functionality is secure as it uses Amazon's private virtual cloud.

Price
Amazon EC2 allows the user to enjoy the financial advantages of Amazon. Amazon EC2 rates are low taking into consideration the computing capacity that is used. Depending on the rate type, there are different types of instances to buy:
Instances on demand: The user has the alternative of paying per hour according to the capacity that he uses in demand instances, so he is not subject to a long-term contract. In this way the user is not tied to fixed costs related to the acquisition and maintenance of the hardware and so can greatly reduce fixed costs and convert them into variable costs much smaller and affordable and reasonable. Therefore, it will no longer be necessary to buy a safety net of capacity to manage the high traffic spikes. New customers can use the Amazon EC2 service for free as part of the free layer program. Once the customer is registered, he or she receives each month and for one year the following EC2 services:

- 750 hours of use of EC2 with an instance t2 micro of Linux, RHEL, or SLES.
  750 hours of use of EC2 with an instance t2. Microsoft Windows Server.

Security
In terms of security AWS offers several alternatives aimed at avoiding unauthorized use. For EC2 it offers Security Groups, Network ACL’s (Access Control List) and

IAM (Identity Access Management). Security Groups acts like a virtual firewall that can be configured on your instance allowing or denying inbound or outbound traffic. Security Groups can provide protocol you can allow or deny, the user has the choice to choose an IP address or choose his own IP and describe what specific rule would be used for. For Network ACL's, they are stateless because they are rule oriented. This feature can be configured to allow or deny traffic on your instances. Among the measures are the use of *https* binding points to transmit encrypted data, certifications to control access, create different user accounts to validate identity in access, the registration of the user activity to control the security and security checks of trusted advisor. AWS uses different types of authentication to ensure that only users who are authorized and validated processes are those who have access to the account and its services; For example, AWS has digital signatures, certificates, cryptographic keys, and passwords available. In addition, it is available as an option to require multifactor authentication to initiate the session in the AWS account or accounts as a user of IAM.

Azure Container Service (AKS)

Microsoft Azure Container Service is an optimized hosting environment for Microsoft's Azure cloud computing platform that allows its users to develop container-based applications and deploy them in clusters of scalable computers. Applications in the cloud can be managed through a browser access portal. The cloud platform is open and flexible. The set of services that it offers in the cloud allows to build and deploy cloud applications using almost any programming language or tool. Since February 2017, Azure Container Service users can turn Kubernetes to automate the management, deployment and scaling of container-applications in Azure clusters. Microsoft renamed Azure Container Service as "AKS" where K stands for "Kubernetes, focusing on this orchestrator.

What is Kubernetes?

Kubernetes (K8S) is defined as an open-source system for the automation of deployments, scaling and management of containerized applications.
This container orchestrator was initially designed by Google, who later donated it to the Cloud Native Computing Foundation. The options to use Kubernetes have hardly any restriction, almost any option of use is possible due to all the possibilities of installation that it offers and because many solutions are integrating in its architecture. Since it is not an "original" support in the sense that Kubernetes is a service for maintaining files by Azure it is deployed using Azure Resource Manager template.
The advantage of containers, which is why they have become so popular, is because they allow developers to write applications that run in an isolated and portable way, so that they are easily transferable from a server environment to a desktop environment.

Main Features:

Scaling and auto-scaling: depending on the CPU usage, it allows the vertical scaling of user applications automatically or manually (through a command or through the interface).

Discovery of services and load balancing: it is not necessary to use an external mechanism for the discovery of services because Kubernetes uses its own IP addresses that it assigns to its containers and a domain main system that is unique for a group of containers that can balance the load.

Self-repair: in case of a container failure user can restart it automatically. User can replace or re-plan containers when a node dies. And if there are containers that do not respond to the 'health checks" defined by the user, the person can stop them.

Automatic rollbacks and deployments: when an application needs to be updated or its settings changed, Kubernetes deploys the changes progressively while monitoring its health to ensure that it does not eliminate all instances at once, and in case of failure, it automatically rolls back.

Planning: it is responsible for deciding in which node each container will be executed according to the resources it requires and other restrictions. Mix critical workloads and "best-effort" to enhance utilization and resource savings.

Configuration management and secrets: sensitive information, such as passwords or "sshkeys", is stored in Kubernetes hidden in "secrets". Both the configuration of the application and the secrets are deployed and updated without having to reconstruct the image or expose confidential information.

Storage orchestration: can automatically mount the necessary storage system, either local storage, storage in a public cloud provider such as AWS or even a network storage system such as Network File System.

Batch execution: Another feature of Kubernetes is that it can handle the batch and CI (Converged Infrastructure) workloads and change the defective containers.

Price: the user only pays for the resources used, so there are no cluster prices.

Security: Azure offers a variety of security features in the cloud. In Container Service it offers image security, which are containers that have an image integrated and are stored in a repository. Those images have layers of software that possibly could be vulnerable. According to Microsoft Azure Documentation (2017), "It is key to understand the origin of the container image, including the owner of the image (to determine if it is a reliable source or not), the software layers it consists of, and the software versions." Another security feature that Container Service provides is orchestrator considerations. One of the benefits is to allow a limitation of using SSH keys for a particular orchestrator that you are running either on the command line interface (CLI) or in the user interface (UI). There are more security features under each orchestrator that goes beyond but are not part of Container Services. Azure provides Identify and Access Management (IAM) to Container Service to create a user and assign the user for a resource that can have access to. The user would have permission on what he can do in the resource if he has access to, or whether it is read or write access.

Google Compute Engine

Google Compute Engine allows users to use high-performance virtual machines with technology from Google Network worldwide, using pay-per-use. For this deployment, the Compute Engine cases are the equivalent of the servers running through Hadoop. This service provides maximum flexibility and management of elements such as private networks, load balancers and Google container Engine (Clusters of managed Docker containers). It is considered one of the most complete platforms for WEB development, providing easy-to-manage storage and scaling, with a resilience capability that eliminates many of the backup and replication issues of traditional storage.

Services

There are various types of services offered within the platform:

Google drive
Google cloud storage
Google cloud SQL
Google BigQuery
Google app engine
Google compute engine –

Main Features

Availability

It is available to all, which means that developers who want to use this technology can do it. Before, it was closed, or it was available by express invitation from someone at Google. Now, it can be run in virtual Linux servers.

Maintenance

It means that virtual machines can continue running while the software and data center is installed, updated or carrying out maintenance work. If a failure occurs, Google automatically reboots the virtual machines and puts them online in just minutes.

Storage and databases

It allows to store objects through the cloud storage service and databases, scalable and high performance, both database related to cloud SQL as databases NoSQL with cloud Bigtable or cloud Datastore.

Scalability

It is highly scalable; Whether it's through a small application or the construction of a large system, cloud storage can manage it.

Security

The cloud resources are controlled on a platform and they are secured by the security model that Google Compute Engine offers. It is possible to manage encryption keys, analyze applications to detect common vulnerabilities. One of the features that offers to detect vulnerabilities is its network firewall rule maintenance. This feature would allow to set your own rules for outbound traffic. For inbound would be set to default. Setting up a firewall on your virtual machine would have the option to set what security protocols would you allow, and which one would be denied. With the right configuration, the virtual machine would be in a safe environment that would be protected from outside traffic. Another security feature that Google provides to Compute Engine is the data encryption. The data that you create in the virtual machine would have Advanced Encryption Standard (AES) 256-bit that would be highly secured from hackers trying to crack into it. If they try to brute force the encryption, the encryption keys would automatically rotate with a set of master keys that would be harder to decrypt the data.

Price

	Free daily limit	Price when the free limit is exceeded
Instances Network	28 hours	.05USD/instance/hour
Traffic-exit	1GB	.12USD/GB
Network Traffic-entrance	1GB	Free
Cloud Storage	5GB	.026 USD/GB/month

Conclusions and Contrasts

Iconic companies such as Netflix, Coca-Cola, Spotify, Expedia, Adobe and many others have developed a dependency on cloud services to successfully maintain their operations through online services. In this way, these companies have been able to concentrate on the core of their skills and business since technological advances are managed by companies specializing in computer engineering which are constantly in the forefront of technology. However, this is not limited only to big companies. In today's world, practically everyone either a big company or an individual business proprietorship without almost any investment capital can have access to the world-class infrastructure platforms for storage, administration, management of data and pay for these services as they are used. The three big companies herein studied have a lot to contribute in these topics.

Since in 2004 Amazon introduced its “massive consumption” in the cloud computing service it has not stopped in the evolution and development of its platforms and has maintained continually improving its system and adding features which has allowed them to stay in the vanguard in front of other competitors regarding new services and solutions in the cloud.

However, in other terms, Amazon is the most expensive. Then came into the field of game, Google and Microsoft who have developed their own structures in the cloud which have created a price competition. Elastic Compute Cloud (EC2) represents the “war horse” for Amazon in terms of computing scalability and competes directly with Google and Azure regarding the use of virtual machines and systems in scale. According to the herein study, the service of Amazon is the most complete, but at the same time, the prices of EC2 are more complex; the same happens with the prices offered by the Azure in their virtual machines. On the other hand, the prices offered by Google are less complex but at the same time less flexible.

Nevertheless, it is a reality that the cloud storage service of Google and Microsoft is very safe and durable as it is the Amazon; but in the same way, Google and Microsoft Azure have an advantage in terms of prices. Cloud Security is one of the most caring aspects of the providers of these systems. Microsoft, Amazon, and Google, and many other cloud computing providers, try to include strong security measures so that the user does not have to worry about this when using their services. However, this does not mean that the provider removes all possible threats to the cloud. Some threats may remain in the form of external risks such as DoS attacks (denial of service), to which even the most robust cloud can succumb. Others may come from access to service credentials, which can be stolen through phishing methods.

As it was discussed in this paper, all three offer largely similar basic competences on their applications: all of them comprise features showing flexible compute, storage, loading and networking. In addition, they are investing heavily in the improvement of their cloud services.

Certainly, the selection of one cloud over the others will depend on the specific needs of each client-user and the workloads they are running.

References

1. Agarwal, S., Pandey, A., Pati, S. (2016). Cloud Computing Security. *International Journal of Recent Trends In Engineers and Research.* Volume 02, Issue 04.
2. Monory, G., Peterson, N., Crider, K., & Macy, M. (2017, July 21). Introduction to Azure Container Service for Kubernetes. *Microsoft Azure.*
3. Security and Compliance on the Google Cloud Platform. *Google Cloud Platform*.

4. Amazon EC2 Security Groups for Windows Instances. *Amazon Elastic Compute Cloud Documentation.*
5. Azure Container Service (AKS). *Azure Container Service (AKS) Documentation - Tutorials, API Reference.*
6. (2017, July 21), Kubernetes in the Cloud: AWS vs. GCP vs. Azure. *Codefresh.*
7. Azure Container Service (AKS). *Microsoft Azure*
8. Compute Engine. *Google Cloud Platform.*
9. Amazon EC2. *Amazon Web Services.*
10. Das, S., Peterson, N., Crider, K., & Macy, M. (2017, March 28). Container security in Azure Container Service. *Microsoft Azure*