	3rd Place	2nd Place	1st Place
PaaS	AWS	Azure	GCP
Serverless		AWS	Azure
Containers	AWS	Azure	GCP
Databases	Azure & GCP		AWS
Telemetry	AWS	Azure	GCP
Application Support	GCP	Azure	AWS
Data Engineering	AWS & GCP		Azure
Geographies	GCP	AWS & Azure	
Price	AWS & Azure		GCP

Recommendations

- Go with AWS if you just want something that works everywhere
- Go with GCP if this is your first rodeo
- Go with Azure if you're living in Microsoft world and want everything and the kitchen sink
- Go Hybrid
- Don't choose on PaaS alone
- Pass if you only require a simple VPS

VPC.Route tables. Subnets.
Security groups.Virtual Machines.
Relational and NoSQL database offerings.
DNS.Deployment tools.

1.VPC

Google Cloud Platform

Virtual Private Cloud (VPC) Network Overview

发送反馈

A Virtual Private Cloud (VPC) is a global private isolated virtual network partition that provides managed networking functionality for your Google Cloud Platform (GCP) resources. A Google VPC has the following properties:

- VPC provides a global private communications space.
- VPC supports multi-tenancy deployments via shared VPC for your organization. A shared VPC network can be shared by different autonomously administered GCP projects.
- VPC networks can be privately peered, even with networks in other organizations.
- VPC provides private communication between compute resources you create, and you can also enable private communication to Google managed services like Google Cloud Storage, Spanner, big data and analytics, and Machine Learning.
- VPC configuration access can be secured using Identity and Access Management (IAM). VPC ingress and egress traffic connections can be restricted using firewall rules.
- VPC can be extended privately across hybrid environments.

VPC networks and subnets

A VPC network is a virtual version of the traditional physical networks that exist within and between physical data centers. A VPC network provides connectivity for your Compute Engine virtual machine (VM) instances, Kubernetes Engine containers, App Engine Flex services, and other network-related resources.

Each GCP project contains one or more VPC networks. Each VPC network is a global entity spanning all GCP regions. This global VPC network allows VM instances and other resources to communicate with each other via internal, private IP addresses.

Each VPC network is subdivided into subnets, and each subnet is contained within a single region. You can have more than one subnet in a region for a given VPC network. Each subnet has a contiguous private RFC1918 IP space. You create instances, containers, and the like in these subnets. When you create an instance, you must create it in a subnet, and the instance draws its primary internal IP address from that subnet.

Virtual machine (VM) instances in a VPC network can communicate with instances in other subnets of the same VPC network using RFC 1918 private IP addresses, provided that firewall rules allow such communication. You can also isolate instances in different subnets using firewall rules. Refer to the firewall rules section for more detail.

Types of VPC networks

There are two types of VPC networks:

- When an **auto mode** VPC network is created, one subnet from each region is automatically created within it. These automatically created subnets use a set of predefined IP ranges. If new regions become available, new subnets in those regions are automatically added to auto mode networks. In addition to the automatically created subnets, you may manually add more subnets to auto mode networks, in regions you choose and using IP ranges you specify.
- When a **custom mode** VPC network is created, no subnets are automatically created. This type of network provides you with complete control over its subnets. You decide which subnets to create, in regions you choose, and using IP ranges you specify.

You can switch a VPC network from auto mode to custom mode. This conversion is one-way; custom mode networks cannot be changed to auto mode networks. Carefully review the considerations for auto mode networks to help you decide which type of network meets your needs.

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications.

You can easily customize the network configuration for your Amazon VPC. For example, you can create a public-facing subnet for your web servers that has access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

Additionally, you can create a Hardware Virtual Private Network (VPN) connection between your corporate data center and your VPC and leverage the AWS Cloud as an extension of your corporate data center.

Features and Benefits

MULTIPLE CONNECTIVITY OPTIONS

A variety of connectivity options exist for your Amazon VPC. You can connect your VPC to the Internet, to your data center, or other VPCs, based on the AWS resources that you want to expose publicly and those that you want to keep private.

- Connect directly to the Internet (public subnets)– You can launch instances into a publicly accessible subnet where they can send and receive traffic from the Internet.
- Connect to the Internet using Network Address Translation (private subnets) – Private subnets can be used for instances that you do not want to be directly addressable from the Internet. Instances in a private subnet can access the Internet without exposing their private IP address by routing their traffic through a Network Address Translation (NAT) gateway in a public subnet.
- Connect securely to your corporate datacenter– All traffic to and from instances in your VPC can be routed to your corporate datacenter over an industry standard, encrypted IPsec hardware VPN connection.
- Connect privately to other VPCs- Peer VPCs together to share resources across multiple virtual networks owned by your or other AWS accounts.
- Privately connect to AWS Services without using an Internet gateway, NAT or firewall proxy through a VPC Endpoint. Available AWS services include S3, DynamoDB, Kinesis Streams, Service Catalog, EC2 Systems Manager (SSM), Elastic Load Balancing (ELB) API, and Amazon Elastic Compute Cloud (EC2) API.
- Privately connect to SaaS solutions supported by AWS PrivateLink.
- Privately connect your internal services across different accounts and VPCs within your own organizations, significantly simplifying your internal network architecture.

SECURE

Amazon VPC provides advanced security features, such as security groups and network access control lists, to enable inbound and outbound filtering at the instance level and subnet level. In addition, you can store data in Amazon S3 and restrict access so that it's only accessible from instances in your VPC. Optionally, you can also choose to launch Dedicated Instances which run on hardware dedicated to a single customer for additional isolation.

SIMPLE

You can create a VPC quickly and easily using the AWS Management Console. You can select one of the common network setups that best match your needs and press "Start VPC Wizard." Subnets, IP ranges, route tables, and security groups are automatically created for you so you can concentrate on creating the applications to run in your VPC.

ALL THE SCALABILITY AND RELIABILITY OF AWS

Amazon VPC provides all of the same benefits as the rest of the AWS platform. You can instantly scale your resources up or down, select Amazon EC2 instances types and sizes that are right for your applications, and pay only for the resources you use - all within Amazon's proven infrastructure.

2.Database Offerings

Databases

- You can implement **SQL solutions** with Amazon's Relational Database Service (RDS) (supporting many DBMS), Google's Cloud SQL (supporting only MySQL at the moment), and with Azure's SQL Database, SQL Data Warehouse and SQL Server Stretch Database.
- Also newer **NoSQL solutions** are available with Amazon's DynamoDB, Google's Bigtable and Cloud Datastore, and Azure's DocumentDB and Table storage.
- But who wants a DB when all you need is a **cache**? If that's the case, then Amazon's ElastiCache and Azure's Redis Cache might do it.
- For more, check the **solution** that amazon offers — Cloud Databases with AWS.

Google Cloud Platform

Managed Databases (RDBMS, NoSQL), Object Storage and Archival

Whatever your storage needs, Google Cloud Platform has you covered. We offer **object storage** for different needs and price points as well as **managed MySQL** and **globally-scalable NoSQL** databases. Our **archival storage** provides industry-leading pricing with the performance of disc.

Highly Scalable NoSQL Database

Cloud Datastore is a highly-scalable NoSQL database for your applications. Cloud Datastore **automatically handles sharding and replication**, providing you with a highly available and durable database that scales automatically to handle your applications' load. Cloud Datastore provides a myriad of capabilities such as **ACID transactions, SQL-like queries, indexes and much** more.

CLOUD SQL FEATURES

Cloud SQL is a fully-managed MySQL and PostgreSQL database service.

Scalability

Easily scale up to 64 processor cores and more than 400GB of RAM. Quickly scale out with read replicas.

High Performance

Designed to scale from small development workloads up to performance-intensive workloads.

Integrated

Cloud SQL instances are accessible from just about any application, anywhere. Easily connect from App Engine, Compute Engine, and your workstation.

Fully Managed

Replicated, managed and backed up, so you can make better use of your time.

Standard APIs

Build and deploy for the cloud faster because Cloud SQL offers standard MySQL and PostgreSQL [BETA] databases. Use standard connection drivers and built-in migration tools to get started quickly.

Availability Protection

Live migration of Compute Engine instances makes maintenance of our underlying infrastructure transparent. In case of a zone failure, High Availability protects your data to get you up and running quickly in another zone.

Partnerships & Integrations

Take advantage of our growing partner ecosystem and tools to make working with Cloud SQL even easier. Our partners can help you streamline the process of loading your data, create rich

aws

Relational Databases

Amazon RDS

Aurora

MySQL

Commercial

ORACLE

Microsoft SQL Server

Community

MySQL

PostgreSQL

MariaDB

Amazon Redshift

Data Warehouse

PostgreSQL

Non-Relational Databases

Amazon DynamoDB

Key Value

Amazon ElastiCache

In-Memory Data Store

redis

MEMCACHED

Amazon Neptune

Graph

Document

AWS Database Migration Service

A relational database is a collection of data items with pre-defined relationships between them. These items are organized as a set of tables with columns and rows. Tables are used to hold information about the objects to be represented in the database. Each column in a table holds a certain kind of data and a field stores the actual value of an attribute. The rows in the table represent a collection of related values of one object or entity. Each row in a table could be marked with a unique identifier called a primary key, and rows among multiple tables can be made related using foreign keys. This data can be accessed in many different ways without reorganizing the database tables themselves.

NoSQL is a term used to describe high-performance, non-relational databases. NoSQL databases utilize a variety of data models, including document, graph, key-value, and columnar. NoSQL databases are widely recognized for ease of development, scalable performance, high availability, and resilience. Below are several resources to help you get started using NoSQL databases.

Download the whitepaper Migration Best Practices - RDBMS to Amazon DynamoDB.

Microsoft Azure

SQL Database

The intelligent relational cloud database service

Azure SQL Database is the intelligent, fully-managed relational cloud database service built for developers. Accelerate app development and make maintenance easy and productive using the SQL tools you love to use. Take advantage of built-in intelligence that learns app patterns and adapts to maximize performance, reliability, and data protection.

Let's Compare!

Amazon introduced "commoditized" cloud computing services through its first AWS service launched back in 2004, and ever since then they kept innovating and adding features, which somehow allowed them having the upper hand in the business by building the most extensive array of services and solutions for the cloud. They are also, in many regards, the most expensive.

Google, and later Microsoft, came into the game and are quickly coming up to par, bringing their own infrastructure and ideas, offering deals, and pulling the prices down.

Storage

To **store objects** (that is, pretty much anything), Amazon Simple Storage Service (S3) is the service that's been running the longest, and as such it has extensive documentation, including free webinars, tons of sample code and libraries, articles and tutorials and very active discussion forums where Amazon developers provide very useful feedback on a regular basis. Of course, Google Cloud Storage and Microsoft Azure Storage provide a service that's as reliable and robust, but the resources you'll find don't come even close that of Amazon's. That being said, Google and Microsoft may have an edge on the price, so read the fine print.

service		provider	GB/month
Block Storage	w	Rackspace Cloud	$0.12
Cloud Files	w	Rackspace Cloud	$0.1
Cloud Storage	w	Google Cloud Platform	$0.026 (standard) / $0.02 (DRA[1])
Data Lake Store	w	Microsoft Azure	$0.04
Simple Storage Service (S3)	w	Amazon Web Services	$0.03 (standard) / $0.0125 (infrequent)
Storage	w	Microsoft Azure	$0.024 (LRS[2]) / $0.048 (GRS[3]) / $0.061 (RA-GRS[4])

Locations

When deploying your services, you may want to choose a data center that's close to your primary target of users. For example, if you're doing real estate or retail hosting in the West Coast of the United States, you'll want to deploy your services right there to minimize the latency and provide a better user experience (UX). Of course, you can still deploy from afar, but the UX will suffer.

Amazon clearly has the most extensive coverage:

AWS locations. Diagram by Amazon

Azure comes close, with fairly good support for Asia:

Azure locations. Diagram by Microsoft

Google Cloud locations

Networking

- You can network in the cloud by doing **domain name system (DNS)** with Amazon's Route 53, Google DNS or Azure DNS.
- Or do **load balancing** with Amazon's Elastic Load Balancing, Google Cloud Loud Balancing and Azure's Load Balancer.
- And, of course, set your **virtual private network (VPN)** with Amazon's Virtual Private Cloud VPC, Google's Cloud Virtual Network and Azure's VPN Gateway.

Route Tables

A *route table* contains a set of rules, called *routes*, that are used to determine where network traffic is directed.

Each subnet in your VPC must be associated with a route table; the table controls the routing for the subnet. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table.

Amazon EC2 Security Groups for Linux Instances

A *security group* acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group. When we decide whether to allow traffic to reach an instance, we evaluate all the rules from all the security groups that are associated with the instance.

If you need to allow traffic to a Windows instance, see Amazon EC2 Security Groups for Windows Instances in the *Amazon EC2 User Guide for Windows Instances*.