Cloud Technologies Comparison

AWS VS GOOGLE CLOUD VS MICROSOFT AZURE

1. Compute:

AWS	GCP	Azure
The computing technology is called as the Elastic Cloud Compute(EC2) AWS Lambda is Amazon's event-driven, serverless platform for computing.	The computing technology is called as the Google Compute Engine (GCE)	The computing technology is called as the Azure Virtual Machines

2. Databases:

AWS	GCP	Azure
• Dynamo DB is Amazon's fully managed cloud database used for a variety of web applications. • Amazon Glacier stores photos, videos, and documents in an archive format as single files or aggregated into TAR or ZIP files. • Simple Storage Service (S3) is Amazon's massive scale object storage service used to store data for websites, mobile apps, and various other purposes.	• Google's Cloud Platform similarly provides both temporary storage and persistent disks. For Object storage, GCP has Google Cloud Storage. • GCP supports relational DBs through Google Cloud SQL. • Technologies pioneered by Google, like Big Query, Big Table, and Hadoop, are naturally fully supported.	• Azure uses temporary storage (D drive) and Page Blobs (Microsoft's Block Storage option) for VM-based volumes. • Block Blobs and Files serve for Object Storage. • Azure supports both relational and NoSQL databases, and Big Data, through Windows Azure Table and HDInsight.

3. Networking:

AWS	GCP	Azure
• Amazon's Virtual Private Clouds (VPCs) and Azure's Virtual Network (VNET) allow users to group VMs into isolated networks in the cloud. • Using VPCs and VNETs, users can define a network topology, create subnets, route tables, private IP address ranges, and network gateways.	• There's not much to choose between AWS vs Azure on this: they both have solutions to extend your on-premise data center into the public (or hybrid) cloud. • GCP uses Cloud Virtual Network to achieve VPN	• Google Compute Engine instance belongs to a single network, which defines the address range and gateway address for all instances connected to it. Firewall rules can be applied to an instance, and it can receive a public IP address. • Azure uses VPN Gatewayto achieve VPN

4. Deployment:

AWS	GCP	Azure
• Amazon Route 53 is a scalable cloud DNS web service that connects user requests with AWS hosted applications. • AWS Cloudformation is Amazon's service for provisioning and updating AWS resources while keeping them organized. • Amazon CodeStar was released in 2017 as a platform for developing, building, deploying apps on Amazon.	• Google Cloud Deployment Manager allows you to specify all the resources needed for your application in a declarative format • With GCP, its deployment processes are repeatable, uses declarative language, template driven and is mainly application focused. • No equivalent service on Azure or Google Cloud for Amazon's CodeStar product.	• No service provided with respect to Azure • Azure Resource Manager enables you to repeatedly deploy your app and have confidence your resources are deployed in a consistent state. • No equivalent service on Azure or Google Cloud for Amazon's CodeStar product.

5. Network Security:

AWS	GCP	Azure
• AWS security groups enable you to model network security policies into logical groups of servers, then apply a policy at scale. A security group policy can be modified at any time, and automatically be applied to the instances associated with the security group AWS • **Network Access Control List (NACL)-** Amazon regards NACLs as an optional layer of security regulating the inbound and outbound traffic of a subnet.	• Google has yet a different approach to network security. The basic construct is simply named 'firewall', which is a container for a single rule. This tag-based security control is similar to AWS security groups insofar as it groups certain elements together. • Like AWS (and unlike Azure), you can specify 'sourceTags' to control which instances are allowed to access a rule's targets (again, without hard-coding IP addresses).	• Azure introduced Virtual Networks (VNet), isolated private networks. As Azure matured, so did its network security capabilities, including the Azure NACL and Network Security Groups (NSGs) • **Network Access Control List (NACL)-** As opposed to AWS security groups, Azure NACLs did not allow you to configure and segregate internal networks.