12-Cloud-Security

# Part 1

1. What are 3 common job roles that combine security and cloud skills?

Cloud Security Analyst or Cloud Penetration Tester, Cloud Architect and DevSecOps

1. What are the 3 biggest cloud provider platforms?

AWS, Azure, and Google Cloud

1. What are the 6 most common cloud services (and their acronyms)?

**IaaS (Infrastructure as a Service)**: A service provider offers pay-as-you-go access to storage, networking, servers and other computing resources in the cloud.

**PaaS (Platform as a Service)**: A service provider offers access to a cloud-based environment in which users can build and deliver applications. The provider supplies the underlying infrastructure.

**SaaS (Software as a Service)**: A service provider delivers software and applications through the internet. Users subscribe to the software and access it through the web or vendor APIs.

**DaaS/DBaaS (Data as a Service/Database as a Service)**: A service that provides a company's data product to the user on demand, regardless of geographic or organizational distance between provider and consumer.

**CaaS (Communications as a Service)**: A service that provides an outsourced communications solution. Such communications can include Voice over IP (VoIP or Internet telephony), instant messaging (IM), and collaboration and video conference applications.

**XaaS (Anything as a Service)**: Cloud services providing all any combination of the offerings mentioned so far. These services are presented differently by different providers. As well, some providers offer simplified versions of these services to make them easier to implement.

1. What is the difference between a virtual network and a physical network?

Physical networks connect computers through cables and other hardware whereas virtual networks extend these capabilities by providing software management capabilities that can connect computers and servers over the internet.

1. What is the point of setting your first firewall rule to block *all* traffic?

This is inline with following the Principle of Least Privilege where a user, program and process should have only the minimum privilege to perform their function. Thus the first firewall rule is to block all traffic and then allow only the required traffic.

1. What is the difference between physical computing components (CPU, RAM, HDD/SSD) and virtual computing components?

Physical computing components like CPU, RAM and HDD/SSD are physical components in a computer or server, however, Virtual computing components are defined by software.

For example a server could have 12 CPUs, 160GB RAM and 2000GB of Diskspace which are all physical computing components of this server. However, using software we can define multiple Virtual Servers on this one Physical server with Virtual computing components like 2 Virtual machines with 2CPU 8GB RAM and 200GB Disk Space and 3 Virtual machines with 1 CPU 16GB RAM and 100GB Disk Space, or any other configuration we may need.

1. What is the purpose of using an encrypted ssh key to connect to a machine?

SSH key is used to authenticate with the machine. SSH key provides cryptographic strength that even extremely long passwords cannot provide. SSH key also improves the security considerably because the user does not have to remember extremely long secure passwords or write them down.

1. What is the difference between a container and a virtual machine?

Containers are smaller than VMs, being megabytes rather than gigabytes, and require fewer CPU resources. Virtual machines are usually larger than containers and a single virtual machine can run multiple containers. Containers are smaller and can be easily distributed unlike Virtual machines.

1. What is a provisioner? Provide 3 examples of common provisioning software.

A Provisioner is a tool that can be used to configure Virtual Machines or containers automatically. This reduces repetitive work and reduces the potential for human errors. Ansible, Puppet, and Chef are the commonly used provisioning tools.

1. What is meant by Infrastructure as Code?

Infrastructure as code (IaC) is the concept of defining all of your equipment and network with code. When using virtual machines and containers, almost every server, database, workstation and other component in your infrastructure can be individually defined with code.

1. What is Continuous Integration/Continuous Deployment?

Continuous Integration/Continuous Deployment (CI/CD) is the concept of automatically updating machines on your network whenever your IaC files change. In other words, whenever you change a machine's configuration file, CI ensures that a new version of that machine is built immediately. CD ensures that this new version is automatically deployed to your live environment. - The primary advantage to CI/CD is that it allows you to manage your entire network by simply updating IaC text files.

1. What is a VPN and when should us use one?

A VPN creates a direct connection between local network and a remote network. It can also encrypt all traffic between the local network and the remote network thus improving security.

VPN should be used in the below cases to improve security:

1. Public Wifi - VPN improves security by encrypting all traffic and thus stopping hackers on the public network from snooping.
2. Organizations - When working for Organizations, VPNs are helpful to access internal work resources remotely which may not be available over the internet.
3. When someone wants to view internet content that is not available in their country, VPN helps by pretending the traffic to be coming from a different unrestricted country
4. Paid VPN can be used by individuals when they do not want ISPs to sell their data
5. What is the purpose of a load balancer?

A load balancer is used to receive traffic from the internet and direct the requests to multiple servers. It servers multiple benefits like:

1. Load balancers can be used to distribute requests among servers based on load, latency, geo-graphy etc;
2. Since Load balancers are the first point of entry and available with a public IP address, it is used to deploy firewalls to prevent attacks such as DDoS.
3. A load balancer abstracts the backend servers from internet, thus changes in IP address of servers does not impact Public DNS
4. A load balancer is usually coupled with a health probe which directs traffic to only those servers which are running and healthy
5. What is a resource group in Azure?

A resource group is a logical grouping of all resources used for a particular setup or project. The resource group will contain the network, firewalls, virtual computers, and other resources that are needed for setup.

1. What is Region in Azure?  
   A region in Azure is a set of data centers deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network.

# Part 2

Detailed diagram of Cloud Infrastructure

