**Cloud+ CV0-003 Quick Study**

**Quick Study**

* Cloud Hardware: GPU Pass-through, SR-IOV, Disk IOPS, Throughput?
  + **Pass-through**: Assign a **dedicated** physical **GPU** to a **single VM**, providing exceptional performance for demanding workloads.
  + **SR-IOV**: Single Root Input/Output Virtualization. Allows VMs NIC to **directly access physical network adapters**, **bypassing the hypervisor** and achieving superior network performance.
  + **Disk IOPS**: Input/Output per second. How many bits disk can **Read or Write** per second.
  + **Throughput**: how fast disk can **transfer** the read/write bits.
* What platform can be database as a service? (IaaS, PaaS, SaaS)
  + PaaS.
* Describe iPAM:
  + Software consolidating **management** of multiple **DHCP** and **DNS** services to provide oversight into **IP address** allocation across an cloud enterprise **network**.
  + IP address allocations tracked across multiple **DHCP** and **DNS** services.
* Describe: Cloud Bursting, Right-Sizing, Auto-Scaling, Horizontal Scaling, Vertical Scaling, Cluster, Node, Peering, Replication?
  + **cloud bursting**: **Extending workloads to the cloud** during **peak demand** to avoid resource constraints.
  + **Right-sizing**: Selecting compute capabilities that match the estimated workload
  + **Auto-scaling**:Automatic scaling of resources to meet the actual workload
  + **Horizontal scaling**: Scaling additional instances to meet the workload requirements (also known as scaling out)
  + **Vertical scaling**: Scaling additional compute resources to an existing instance to meet the workload requirements (also known as scaling up)
  + **cluster**: two or more servers that have the same data for failover. treated as a single entity. network ip for both is single ip address.
  + **node**: each cluster member is called a node. all nodes will be configured the same way and share the same ip.
  + **peering**: Establishes **direct communication between VPCs** without traversing the public internet, minimizing latency and enhancing performance and security.
    - Appear to customer as single network.
    - Peering is used in the **hub-and-spoke model** to connect the spoke networks with the hub network. Note that the spoke networks are not peered to each other in the hub-and-spoke model.
  + **Replication**: Creates **copies** of data across different storage locations **for disaster recovery** and **data availability**.
* Describe Permissions: Discretionary-based, Non-Discretionary-based, Attribute-based, Mandatory-based, Role-based, ACL, 802.1X?
  + **Discretionary-based**: **Owner access** controls. Allows **users** to **control access** to their **own resources**. Access is managed with an access control list (ACL) that lists who has access and what level of access they have.
  + **Non-Discretionary-based**: **Rule based access control**. Access controlled by an **administrator** or system based on rules and policies.
  + **Attribute-based**: determine access by user characteristics, object characteristics, action types.
  + **Mandatory-based**: **Access via security model**. **Labels** set on objects (files) by the administrator. Users cannot manipulate these labels. Users are given matching classifications. If both match, user is granted access.
  + **Role-based**: Grants **access** based on predefined **roles** and associated permissions. Given to **groups**.
  + **ACL**: Access Control List. Lists who has access to resource and what level of access they have.
  + **802.1X**: pNAC. Port Network Access Control. Must be authorized to access the switch ports. Can't just plug into ethernet port and start communication.
* Describe: Business Continuity Plan, IRDR, Tabletop Exercise, Root Cause Analysis, N-1?
  + **business continuity plan**: A roadmap for maintaining essential business operations during any unexpected disruptions. It outlines response procedures, communication protocols, and recovery strategies to minimize downtime and ensure critical functions resume swiftly.
    - **BCP**: "The playbook for keeping the business open during disruptions."
  + **IRDR**: Incident response/disaster recovery documentation. A detailed guide for handling security incidents and data breaches. It describes roles and responsibilities, escalation procedures, forensic analysis methods, and disaster recovery steps to restore systems and data swiftly.
    - **IRDR**: "The manual for responding to security threats and recovering from disasters."
  + **A tabletop exercise**: practical and interactive(role play) approach to simulate various disaster scenarios, allowing individuals to discuss and practice their roles and responsibilities during an incident. It tests the BCP and IRDR, identifies weaknesses, and improves response capability through simulated decision-making and communication.
    - **Tabletop Exercise**: "Playing out a crisis to make sure everyone knows their roles."
  + **A root cause analysis**: An in-depth investigation to identify the underlying cause of an incident or problem. It involves gathering evidence, analyzing data, and tracing the root cause through a logical sequence of events. RCA helps prevent similar incidents and improve overall performance.
    - **Root Cause Analysis**: "Figuring out the real reason behind a problem to stop it from happening again."
  + **N-1**: Following n-1 updating policies ensures **one version behind the latest** for **stability**.
* Describe Storage: Thin Provisioning, Thick Provisioning, Deduplication, SDS, iSCSI Storage, SAN, NAS, Object, Tenants, Buckets, Hyperconverged, LUN, Oversubscription?
  + **Thin Provisioning**: **Allocates storage dynamically based on actual usage**, minimizing upfront costs.
  + **Thick Provisioning**: **Allocates all storage space upfront, ensuring consistent performance**.
  + **Deduplication**: Eliminates redundant data copies, replacing the content with pointers.
  + **SDS**: Software-defined Storage. leveraging **software** to **manage storage resources**. SDS resides between the data request and the hardware, abstracting the hardware, allowing storage control of SAN, NAS, or traditional storage.
  + **iSCSI Storage**: Block-level storage protocol for accessing storage over IP networks. Encapsulates SCSI commands over TCP/IP.
  + **SAN**: Storage Area Network. Data is divided into chunks called **blocks**. Block storage is not reliant on a server’s filesystem, and data chunks may be distributed across several storage devices. Block storage organizes the data for the benefit of the data itself (where file storage organizes data for the system’s benefit). Block storage is used with SANs, which can also be **difficult and expensive** to implement.
  + **NAS**: Network Attached Storage. Data is stored as a discrete file, such as a document, a spreadsheet, or an image file. This type of storage is **inexpensive** and useful for relatively small pieces of data.
  + **Objects**: Stores unstructured data as individual objects (think of them as boxes in the warehouse). Each object has a unique identifier for easy access and retrieval. No specific folder hierarchy – objects are flatly stored in a "bucket".
  + **Tenants**: Many organizations have **concerns** regarding data **security** and **privacy** in multi-tenant public cloud infrastructures. One key security factor is the **tenant identifier** that uniquely labels the consumer and helps filter access to resources. Multi-tenancy: allows sharing of storage resources while maintaining data isolation and security.
  + **Buckets**: Buckets are the primary **storage** unit for **data objects.** Virtual containers within object storage systems used to organize and manage large data volumes. Buckets are given a **globally unique name** and location when they are created.
  + **Hyperconverged**: Cloud-like infrastructure on premises.
    - Integrates compute, storage, and networking resources into a single platform for simplified management and scalability.
    - x86 compute + Storage(SSD's) + VM software: emulate multiple cloud VM's for efficient scaling.
  + **LUN**: Logical Unit Number. Number used to identify a logical unit, which is a device addressed by the iSCSI protocol or by SAN.
  + **Oversubscription**: primarily employed for **cost** efficiency. It involves provisioning virtual resources that **collectively exceed the available physical resources**. This approach assumes that **saturation will not occur**, making it a common pattern for public cloud providers. Oversubscription can apply to CPU, memory, and network throughput.
* Describe vLan, vxLAN, Affinity, Anti-Affinity, NVGRE, STT, GENEVE, Micro-Segmentation:
  + **vLAN**: Network at Layer 2 (the data link layer of the OSI model). This is accomplished by **tagging** data **frames** with vLAN membership information. Switch isolates the traffic to the appropriate vLAN. Router routes traffic between vLANs. Helps segment network. Ease congestion.
  + **vxLAN**: Improvements over vLAN. 16 million network segments(vLAN 4096). Provides **Tunneling** services. Better Link aggregation and Layer 3 routing. Greater scalability. **Stretching**: VXLAN traffic crosses between the local network and the cloud network using a bi-directional tunnel. Traffic **mirroring**: traffic and be sent to another network for auditing.
  + **Affinity**: Hypervisor affinity. Deliberate **grouping** of VM instances on a **single host for centralized management, high network throughput and low latency**. Reduces latency. Cons, Creates single point of failure, hard to scale.
  + **Anti-affinity**: deliberately **distributes** VM instances across **multiple hosts** to avoid **single points of failure**. Pros: Scaling, redundancy, failover. Cons: can be more difficult to monitor. slower performance.
  + **NVGRE**: Network Virtualization using Generic Routing Encapsulation. Used by Microsoft for network segmentation.
  + **STT**: Stateless Transfer Tunnel. Another technology for segmenting networks.
  + **GENEVE**: protocol designed to allow the coexistence of multiple network segmentation technologies (VXLAN, NVGRE, STT) within the same network infrastructure. Usually required across **multi-cloud deployments**.
  + **Micro-segmentation**: Zero Trust. **Dividing a network** at the **workload**(application) level. Reduced attack surface. Increased containment of security breaches. Increase compliance. Easier management via policies.
* CompTIA Cloud Troubleshooting Methodology?
  + Mnemonic: "**I Do Eat Three Eggs In Virginia IP Daily**"
  + Identify the problem.
  + Determine the scope of the problem.
  + Establish a theory of probable cause, or question the obvious.
  + Test the theory to determine the cause.
  + Establish a plan of action.
  + Implement the solution, or escalate.
  + Verify full system functionality.
  + Implement preventive measures.
  + Perform a root cause analysis.
  + Document findings, actions, and outcomes throughout the process.
* Describe Security: WAF, vADC, IPS, IDS, DLP, NAC, NPB, HA Firewalls, HIDS, HIPS, EDR, FIM, Network Flows, LDAP, SAML, DoH/DoT, DNSSEC, Risk Register, CMDB CASB?
  + **WAF**: web application firewall. Work at Layer 7 to protect web applications from common attacks like cross-site scripting, cross-site forgery, SQL injections and DDoS.
  + **vADC**: Virtual Application Delivery Controller. **Load balances** traffic across multiple servers and provides additional security features like **URL filtering** and denial-of-service (**DoS**) protection. Typically, these devices are placed in a DMZ.
  + **IPS**: Intrusion Protection System. Monitor and **Prevent** malicious activity. Dynamically blocks the connection and traffic identified as a threat.
  + **IDS**: Intrusion Detection System. **Monitors** network traffic for malicious activity and prevents or **alerts** on detected threats. Passive devices that match network traffic and patterns against known vulnerabilities. Monitor/alert the network environment but do not stop.
  + **DLP**: Data Loss Prevention. Detects/Prevents data exfiltration.
  + **NAC**: Network Access Control. Combine several aspects of security into a single unit. Workstation security (endpoints): anti-virus, anti-spyware, patching, and vulnerability scans. Authentication: single sign-on and multifactor authentication. Network security: firewalls, network IDS, patching, and updated anti-virus definitions.
  + **NPB**: Network Packet brokers. Mirror network traffic to security and monitoring tools for analysis and troubleshooting. Exist between the network infrastructure and infrastructure security tools to gather information and **expose packet** to the appropriate **tools**.
  + **HA Firewalls**: High Availability. Two or more firewalls for redundancy with failover.
  + **HIDS**: Host based intrusion detection. monitoring activities and events at the host or individual instance level. Organizations have bare-metal or virtual machines, monitors identified threats by alerting malicious traffic.
  + **HIPS**: Host based prevention detection. monitoring activities and events at the host or individual instance level. Organizations have bare-metal or virtual machines, actively prevents or mitigates identified threats by blocking or isolating malicious traffic.
  + **EDR**: Endpoint Detection Response. Typically involves installing an agent on each endpoint to passively monitor for threats.
  + **FIM**: File Integrity Monitor. Continuously monitors files for modifications and alerts on unauthorized changes.
  + **Network Flows**: **visualize** and understand how data moves through a **network** infrastructure.
    - Detect anomalous behavior, potential threats, bottlenecks or suspicious activity.
  + **LDAP**: Lightweight Directory Access Protocol. Centralize information about clients, access, privileges on the network. Corporations use this along with Active Directory for AAA.
  + **SAML**: Security Assertion Markup Language. The markup that support Federation SSO.
    - Single Sign On across different organizations. ex.. log into github with your google credentials.
  + **DoH/DoT**: DNS over HTTPS. DNS over TLS. Encrypting traffic to/from DNS server.
  + **DNSSEC**: PKI certs preventing DNS hijacking. DNS identity checking.
  + **Risk Register**: Maintain a comprehensive record of identified vulnerabilities, their associated risks, and planned mitigation strategies.
  + **CMDB**: Configuration Management Database. Stores information about hardware and software deployed throughout the company. **Entries** in the database are referred to as **configuration items**.
  + **CASB**: act as **intermediaries(proxy)** between cloud applications and users, providing additional security and compliance controls. CASBs offer features like data encryption, access control, threat detection, and **compliance reporting**. Enforce rules, even if SaaS is a 3rd party.
* Describe: P2V, V2V, SLA, Vendor Lock-in, MOU
  + **P2V**: Physical to virtual. **migrating physical servers** and **applications** to virtual machines (**VMs**) within the cloud, enhancing agility, scalability, and resource management.
  + **V2V**: Virtual to virtual. **Moving VMs** from one cloud **platform to another**.
  + **SLA**: Service-Level Agreement. contract between a customer and a cloud services provider that ensures minimum levels of service quality. **Monetary penalties**.
  + **Vendor Lock-In**: Lock-in occurs when the **cost** (whether time, money, or resources) is **too high to switch** from the current CSP to a different desired provider.
    - **Avoiding** dependence on a specific **vendor's proprietary** solutions or APIs is crucial.
    - **Choose cloud-agnostic** technologies and tools to ensure flexibility and portability across platforms, mitigating lock-in risks.
  + **MOU**: Memorandum of Understanding. An agreement outlining the terms and responsibilities of parties in a partnership or collaboration. Informal letter of intent. **Does not include monetary penalties**.
* Describe Disaster Recovery: Failover, Failback, RTO, RPO, MTTR, Snapshot, 3-2-1 Rule, HA, Redundancy?
  + **Failover**: switch to DR site when primary fails/testing.
  + **Failback**: switch back to primary site after fix/testing.
  + **RTO**: Recovery Time Object. Maximum acceptable **downtime** for **restoring services**.
  + **RPO**: Recovery Point Object. Maximum allowable **data loss** during a system outage.
    - ex.. you backup every 24 hours of data, you have 24 hours max RPO.
  + **MTTR**: Mean Time to Recover. Average time required to **recover** from a **system failure**.
  + **Snapshot**: Replicates the **state** of data at a **specific point in time**, allowing for rollback to that state.
  + **3-2-1**: **Three Copies of Data**: Keep at least three copies of your important data. This includes the original data and two additional copies. **Two** separate forms of media(physical drive and cloud storage). **One** copy off site.
  + **HA**: High Availability. Definition: The characteristic of a system where it continues to function despite the complete failure of any component within the architecture. However, HA acknowledges that there may be an interruption of service, but it **should not exceed the time limits defined by the Recovery Time Objective (RTO)**.
  + **Redundancy**: closely related to high availability but differs in that it ensures a system continues to function without degradation in performance even in the event of a complete component failure. **Redundancy does not imply any interruption of service** and is typically more challenging to achieve than simple high availability.
* Describe Licensing: Socket, Core, Volume, Per User, Subscription?
  + **Volume**: licensing is a special type of software licensing setup that uses a single license key to authorize the software on multiple computers. For instance, a company may purchase a software license that allows up to 50 of their employees to use the software at the same time.
  + **Socket**: based license means that a license for each physical socket is bought regardless of how many CPU cores it has. This license gets less expensive as the number of CPU cores per socket increase and load more VMs onto the system.
  + **Core-based**: licensing requires all physical cores in the server to be licensed. Servers are licensed based on the number of processor cores in the physical server.
  + **Per User**: cost per user.
  + **Subscription**: model or the **pay-as-you-grow** model allows billing for only their use of resources.
* Describe Environments: Development, QA, Staging, Production, Blue-Green, Canary, DR?
  + **Development**: Initial environment for coding and experimentation.
  + **QA**: Quality Assurance. Testing environment for functional, regression, and security testing.
    - regression: breaks something already established.
  + **Staging**: Environment for **simulating production** conditions and testing the solution with real-world data.
  + **Production**: Full-sized infrastructure for end-user access.
  + **Blue-Green**: exact copies where one is modified and switched to. If no problems, becomes primary.
  + **Canary**: Gradual deployment to a small subset of production.
  + **DR**: **Backup** and **recovery infrastructure** to ensure business continuity in case of an outage.
* Describe Testing: Vulnerability, Penetration, Performance, Regression, Functional, Usability?
  + **Vulnerability**: Identifies **existing** weaknesses in the solution that could be exploited by attackers. The goal is to identify the vulnerability so that it can be **mitigated**.
  + **Penetration**: Simulates real-world attacks to test the **effectiveness of the security** measures.
    - **authorized** attempt to **identify security misconfigurations**.
    - Such testing begins with an **analysis** of available resources, looking for older, unpatched, or vulnerable software.
  + **Performance**: Test **responsiveness** and **stability** of the solution **under load**.
  + **Regression testing**: Also called **Post**-deployment validation.
    - Verifying changes do not effect other dependencies, **after** the update has been **deployed**.
    - Otherwise, the application has fallen back, or “regressed,” to an earlier stage of functionality.
  + **Functional testing**: **Tests** against specified **requirements**. Does it **do** what it’s **supposed to do**?
  + **Usability testing**: Assesses how easy and intuitive the solution is for users to interact with.
    - Performed by the **end-users** and provides direct **feedback** on the interface, features, and practical use.
* Describe: Tagging, Chargebacks, Showbacks, Quotas?
  + **Tagging**: **Labels** assigned to **resources**. Utilizing tagging enables efficient categorization and **tracking** of resources in the cloud environment.
  + **Chargebacks**: **Monitoring costs** helps in optimizing resource usage and staying within budget.
    - **Assigning costs to specific departments** or projects facilitates transparent **cost allocation**.
  + **Showbacks**: Report the utilization of services **without billing** the business unit.
    - Providing cost breakdowns fosters awareness of resource consumption.
  + **Quotas**: Sets limits on resources for individual users or groups.
* Describe Port Numbers: DNS, HTTP, NTP, SNMP, HTTPS, SMB-CIFs, LDAP(encrypted), MySQL, RDP?
  + DNS: 53
  + HTTP: 80
  + NTP: 123
  + SNMP: 161/162
  + HTTPS: 443
  + SMB-CIFs: 445
  + LDAP(encrypted): 636
  + MySQL: 3306
  + RDP: 3389

**CompTIA Cloud+ CV0-003 Acronyms Small**

**Acronyms**

* AAA
  + Authentication, Authorization, and Accounting
* ACL
  + Access Control List
* ADC
  + Application Delivery Controller
* BCP
  + Business Continuity Plan
* BGP
  + Border Gateway Protocol
* BIA
  + Business Impact Analysis
* BRD
  + business requirements document
* CAB
  + Change Advisory Board
* CAS
  + Content Addressed Storage
* CASB
  + Cloud Access Security Broker
* CSP
  + Content Service Provider
* DR
  + Disaster Recovery
* FC
  + Fibre Channel
* FCoE
  + Fibre Channel over Ethernet
* FIM
  + File Integrity Monitoring
* IAM
  + Identity and Access Management
* IdM
  + Identity Management
* IoT
  + Internet of Things
* IPC
  + Instructions Per Cycle
* IPS
  + Intrusion Prevention System
* IPSec
  + IP Security
* iSCSI
  + Internet Small Computer System Interface
* KVM
  + Kernel Virtual Machine
* L2TP
  + Layer 2 Tunneling Protocol
* LAN
  + Local Area Network
* LDAP
  + Lightweight Directory Access Protocol
* MAC
  + Mandatory Access Control
* MPLS
  + Multiprotocol Label Switching
* MSP
  + Managed Service Provider
* MTBF
  + Mean Time Between Failure
* MTTF
  + Mean Time To Failure
* MTTR
  + Mean Time To Repair
* MTU
  + Maximum Transmission Unit
* NAC
  + Network Access Control
* NAS
  + Network Attached Storage
* NAT
  + Network Address Translation
* NFS
  + Network File System
* NIC
  + Network Interface Controller
* NIS
  + Network Information Service
* NOC
  + Network Operations Center
* NTP
  + Network Time Protocol
* NTS
  + Network Time Security
* RPO
  + Recovery Point Objective
* RTO
  + Recovery Time Objectives
* SAN
  + Storage Area Network
* SAS
  + Serial Attached SCSI
* SDLC
  + Software Development Life Cycle
* SDN
  + Software-Defined Network
* SDS
  + Software-Defined Storage
* SMT
  + Simultaneous Multithreading
* SOC
  + Security Operations Center
* SSO
  + Single Sign-On
* TPM
  + Trusted Platform Module
* TTL
  + Time to Live
* V2P
  + Virtual to Physical
* V2V
  + Virtual to Virtual
* VAT
  + Virtual Allocation Table
* vCPU
  + Virtual CPU
* VDI
  + Virtual Desktop Infrastructure
* vGPU
  + Virtual Graphics Processing Unit
* VHD
  + Virtual Hard Disk
* vLAN
  + Virtual Local Area Network
* VM
  + Virtual Machine
* VMFS
  + Virtual Machine File System
* VNC
  + Virtual Network Computing
* vNIC
  + Virtual NIC
* VoIP
  + Voice over IP
* VPC
  + Virtual Private Cloud
* VPN
  + Virtual Private Network
* vRAM
  + Virtual Random Access Memory
* vSAN
  + Virtual Storage Area Network
* WAF
  + Web Application Firewall
* WAN
  + Wide Area Network