CS435 MCQ's

1. The workload is distributed based on a load-balancing algorithm with the scope/s of VMs, Cloud storage devices and cloud services.
2. In order to avoid data loss and service unavailability due to disk failure, redundant storage is applied.
3. in case of network failure, the disruptions in Cloud services can be avoided through redundant storage incident.
4. The failure of the physical server cripples the **hypervisor** and therefore the hosted VMs also become unavailable.
5. The capacity planner modules **dynamically** matches the capacities of physical servers and the resource demands of hosted VMs.
6. The failure of the physical server results in the unavailability ofVMs hosted on that server.
7. The **Zero downtime architecture** implements a failover system through which the VMs (from the failed physical server) are dynamically shifted to another physical server without any interruption
8. The **automated scaling listener** redirects the requests of service consumers towards multi-cloud redundant implementations of service instances based on on-going scaling and performance requirements
9. It may be possible to **detect and counter** some failures in Cloud environment if there is an automated system with failure diagnosis and solution selection intelligence.
10. Logical Unit Number is **a logical drive** that represents a partition of a physical drive.
11. By using ***link aggregation*** techniques, network traffic can be distributed among multiple physical uplinks.
12. The need for multiple paths arises to provide **resiliency** when a physical link fails.
13. The federation agreement may be timely or permanent.
14. Federation can be performed horizontally or vertically based on extending the SaaS, PaaS and IaaS of the federation buyer.
15. If a Cloud infrastructure cannot meet the requests' deadlines, then it is experiencing resource shortage or *congestion.*
16. Cloud resource pools and resource management systems can be used to provide **scalability.**
17. Replication is used to ensure high **availability** and form a failover system.
18. Multipath resource access architecture is used to provide **reliability.**
19. The PaaS environments also help establish **multitenanc**y and **auto scalability** features in developed applications.

20. Automated scaling listeners and load balancers are utilized for **workload distribution.**
21. SaaS instances are unique from IaaS and PaaS instances due to concurrent users.
22. A multi-device broker mechanism for heterogeneous device-based access usually supports mobile-based SaaS implementations.
23. The term **Inter-Cloud** refers to as *Cloud of Clouds* just as **Internet** is regarded as *network of networks.*
24. Technological giants such **as IBM, HP, CISCO, RedHat etc**. are actively working on establishment of cloud-of-clouds.
25. Cumulative of, or separate of outbound and inbound network traffic in **bytes** over the monitored time
26. Service quality metrics are required to be ***quantifiable, repeatable, comparable*** and *easily* ***obtainable***
27. *Network Capacity Metric*: Measured as bandwidth/throughput in bits per second.
28. *Storage Device Capacity Metric*: Measured as size in GB.
29. CloudSim requires **Sun's Java 8 or newer version**. Older versions of Java are not compatible.
30. A service named as ***Cloud Information Service (CIS)*** contains the registry of the data center.
31. **Confidentiality**: Allowing only authorized access and disclosure to the information.
32. **Integrity**: Guarding against unauthorized modification and/or destruction of information
33. Trust is broader term than security because the trust is also based upon experience and criteria.
34. The trust in Cloud computing is of two types**: *Persistent trust*** (long term) and ***Dynamic trust*** (short term).
35. The United States Computer Emergency Readiness Team (**US-CERT**)
36. **Secure Socket Layer (SSL):** It s security protocol for encrypting the communication between a web browser and web server.
37. **Wired Equivalent Privacy (WEP):** Designed to provide the same level of security as the wired networks.
38. **Wired Equivalent Privacy (WEP):** Uses RC4 standard to generate encryption keys of length 40-128 bits.
39. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (**CCMP)**
40. The algorithm used for encryption is called ***cypher*.**
41. The encryption key is combined with the plaintext to create the encrypted text.
42. **Hashing:** It is a process of deriving a hashing code or *message digest* from a message.
43. The message digest is of a fixed length and is shorter than the original message.
44. The encrypted hash code and hashing algorithm is the digital signature.
45. An encryption key is a string of bits which is paired with the original data to transform it into *encrypted data* or *cyphertext*.

46. STEM skills (Science, Technology, Engineering and Mathematics)
47. Up to 70% of Europeans were concerned about the non authorized secondary usage of their data.
48. In-fact, the 'On-demand' and 'pay-as-you-go' models may be based upon weak trust relationships.
49. **Lack of trust** is the key factor which inhibits the wide adoption of Cloud services by the end-users.
50. Measuring the **reliability** of a specific Cloud will be difficult due to the complexity of Cloud procedures
51. The trust management system should be able to measure the "trustfulness" of the Cloud services.
52. **Turnaround efficiency**: The actual vs. promised turnaround time. It is the time from the placement of the consumer's task to finishing that task.
53. NIST and other US govt agencies are evolving methods to solve the compliance issues between consumers and providers.
54. The forensic analysis for SaaS is the responsibility of the **provider** while the forensic analysis of IaaS is the responsibility of the **consumer.**
55. The in-house data centers can use huge and expensive uninterruptable power supply (UPS) devices and/or generators.
56. Remember a rule that a 20% of code usually performs the 80% of processing.
57. Both capacity planning and scalability should be performed in harmony.
58. cost constraint may take the priority over other constraints and thus may introduce starvation for some tasks.
59. Better to use a hybrid approach for resource scheduling to gain cost as well as to minimize task deadline violations.
60. The bargain based scheduling can achieve low cost and meet deadline if negotiation is successful.
61. ***Aging*** factor can be applied to increase the priority of low-priority tasks to avoid or lower the starvation.
62. mobile commerce applications face the **complexities** such as **bandwidth limitation, device configuration and security**.
63. The mobile learning apps face the **limitations** in terms of **high cost of devices & data plan and network bandwidth.**
64. The mobile devices can be connected to **a *cloudlet,*** *a* set of **multi-core computers** connected to remotely placed Cloud servers.
65. Data access over mobile Cloud applications may be **challenging** in case **of low bandwidth, signal loss and/or battery life.**
66. Typically, both the Cloud computing and Mobile Cloud computing are dependent upon remote usage of IT resources offered by Cloud.
67. **Software Defined Networking (SDN)** is the new paradigm of networking that separates the control plane from data plane.
68. SDN has its roots in history as long ago as 80s and 90s with the development **of Network Control Point (NCP)** technology.
69. All the vNICs on a physical host (server) are interconnected through a virtual switch (vSwitch).
70. A physical ethernet switch can be virtualized by implementing IEEE Bridge Port Extension standard **802.1BR.**

71. Centralized controllers such as ***Beacon*** can handle more than **12 million flows per second** and can fulfill the requirements of enterprise level networks and data centers for hosting Cloud.
72. The SDN can be helpful in **monitoring, filtering and managing the network traffic** over virtual as well as physical networks inside a Cloud hosting data center.
73. Fog will support **Internet of Everything (IoE)** applications such as industrial automation, transportation, network of sensors and actuators etc….

ABBREVIATIONS

1. automated scaling listener (ASL)
2. **Network Control Point (NCP)**
3. **Software Defined Networking (SDN)**
4. Hadoop Distributed File System (HDFS)
5. multimedia edge Cloud (MEC)
6. content delivery network (CDN).
7. application program interface (API)
8. Optical character recognition (OCR)
9. the Identity as a Service (IDaaS)
10. disaster recovery plan (DRP).
11. total cost of ownership (TCO)
12. Identity and Access Management (IAM)
13. mean time between failure (MTBF).
14. Redundant Array of Independent Disks (RAID)
15. Cloud Service Provider (CSP)
16. **Identity and Access Management (IAM)**
17. **Public Key Infrastructure (PKI)**
18. Message Authentication Code Protocol (**CCMP)**
19. **Wi-Fi Protected Access (WPA)**
20. Temporal Key Integrity Protocol (TKIP)
21. Advanced Encryption Standard (AES)
22. **Wired Equivalent Privacy (WEP)**
23. **Secure Socket Layer (SSL)**
24. Intrusion detection system (**IDS)**
25. personal identification number **(PIN)**
26. **Denial of Service (DoS)**
27. *Mean-Time to Switchover **(MTSO**) Metric.*
28. *Mean-Time System Recovery **(MTSR**) Metric*
29. **TCO** (Total cost of ownership)