1. Service load balancing architecture uses mechanisms such as round-robin, least connections, and IP hash to distribute incoming network traffic across multiple servers, ensuring optimal resource utilization and high availability.
2. Security considerations in cloud computing include data privacy, identity management, compliance with regulations, network security, and secure access controls to protect against unauthorized access and data breaches.
3. Key forms of virtualization that influenced cloud computing include hardware virtualization (VMs), storage virtualization, and network virtualization, enabling the abstraction and efficient utilization of resources.
4. Concerns with remote management software include potential security vulnerabilities, unauthorized access risks, and the need for robust encryption to protect sensitive data during remote server management activities.
5. An API Gateway is a server that acts as an API front-end, receiving API requests, enforcing throttling and security policies, and forwarding requests to the appropriate backend services. APIs in cloud services enable seamless integration and communication between different components and services.
6. A Virtual Private Cloud (VPC) is a private network within a public cloud infrastructure, allowing users to isolate and control their resources securely. It is important for enhancing security, customization, and network management in cloud environments.
7. Mechanisms like data transformation services are used to facilitate runtime data transformation, enabling interoperability and accessibility of a cloud service for a broader range of consumers with varying data formats.
8. Different types of virtualization include server virtualization, network virtualization, storage virtualization, application virtualization, and desktop virtualization.
9. Integration of cloud storage providers involves connecting cloud storage services with applications and systems, allowing seamless data storage, retrieval, and management across various platforms.
10. Cloud computing introduces utilization models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) for remote provisioning of resources based on user needs.
11. OS virtualization advantages include resource optimization, improved server efficiency, and the ability to run multiple isolated operating systems on a single physical machine.
12. OS-based virtualization can introduce performance overhead due to the need for emulation and translation layers, impacting the efficiency of resource utilization.
13. Community cloud characteristics include shared infrastructure among organizations with common concerns, collaborative policies, and a specific community focus, providing benefits of both public and private clouds.
14. Azure Content Delivery Network (CDN) advantages include improved website performance, reduced latency, and enhanced user experience through the efficient delivery of content from edge locations.
15. System integrators in cloud computing are companies or professionals that specialize in integrating various cloud services and technologies to create comprehensive and customized solutions for businesses.
16. Popularly used cloud computing services include Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, and various SaaS offerings like Salesforce and Dropbox.
17. Key features of cloud computing include on-demand resource provisioning, scalability, pay-as-you-go pricing, self-service access, and geographic flexibility.
18. Issues with cloud computing include security concerns, data privacy challenges, potential downtime, dependency on internet connectivity, and compliance with regulatory requirements.
19. Different datacenters deployed for cloud computing include public datacenters owned by cloud service providers and private datacenters maintained by individual organizations for their specific needs.
20. Cloud storage levels include raw storage, object storage, block storage, and file storage, each serving different purposes in cloud environments.
21. Cloud enabling technologies encompass virtualization, containerization, automation tools, orchestration platforms, and software-defined networking, among others.
22. Cloud architecture provides automation through tools like orchestration and management platforms, ensuring resource scalability and performance transparency by abstracting underlying infrastructure complexities.
23. Limitations of Cloud Computing include security concerns, potential data breaches, reliance on internet connectivity, limited customization in some public clouds, and regulatory compliance challenges.
24. Cloud architecture contributes to business benefits by providing cost efficiency, scalability, flexibility, and accessibility to a wide range of computing resources, enabling innovation and rapid deployment of applications.
25. Cloud security involves measures such as encryption, access controls, identity management, and regular audits to protect data and infrastructure. Concerns include data breaches, unauthorized access, and compliance with industry regulations.
26. AWS provides security for its customers through services like Identity and Access Management (IAM), Virtual Private Cloud (VPC), encryption, and monitoring tools to ensure a secure cloud computing environment.
27. Security management in cloud computing involves implementing security policies, access controls, encryption, and regular audits to safeguard data and infrastructure from threats and vulnerabilities.
28. EUCALYPTUS in cloud computing stands for "Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems." It is an open-source software infrastructure that allows organizations to create private cloud environments compatible with Amazon Web Services (AWS).
29. Hybrid cloud combines public and private cloud infrastructures, allowing data and applications to move seamlessly between them. Community cloud is shared among organizations with common concerns, forming a collaborative and focused cloud environment.
30. Yes, public clouds owned by third parties offer commercialized cloud services and IT resources to consumer organizations. These services include computing power, storage, and applications provided over the internet for a fee.
31. A Virtual Machine (VM) is a software emulation of a physical computer that runs an operating system and applications. VMs enable the efficient use of physical resources by allowing multiple operating systems to run on a single physical machine.

1. Which mechanism are used in service load balancing architecture?

2. What are the SECURITY CONSIDERATIONS in cloud?

3. The primary technology innovations that influenced and inspired key distinguishing features and aspects of cloud computing include which forms of virtualization ?

4. What concerns are associated with the usage of remote management software, which is employed for connecting to physical server consoles and deploying operating systems?

5. What is an API Gateways? Why API's is used in cloud services?

6. What is a Virtual Private Cloud (VPC) and why is it important?

7. Which mechanisms is nosed to facilitate runtime data transformation so as to make a cloud service accessible to a wider range of cloud service consumer

8. Write diferent types of Virtualization

9. Describe integration of cloud storage providers.

10. What utilization models does cloud computing, a specialized form of distributed computing, introduce for the remote provisioning of resources?

11. What are the advantages of OS Virtualization?

12. Which OS-based virtualization can introduce demands and issues related to performance overhead.

13. What are the characteristics of a community cloud?

14. What are the advantages of using Azure Content Delivery Network?

15. What are system integrators in cloud computing?

16. What are some of the popularly used cloud computing services?

17. What are some of key features of cloud computing?

18. What are some issues with cloud computing?

20. What are different datacenters deployed for cloud computing?

21. What are cloud storage levels?

22. What are cloud enabling technologies?

23. Mention in what ways cloud architecture provides automation and performance transparency?

24. List out the limitations of Cloud Computing.

25. How is cloud architecture involved in business benefits?

26. How does cloud security works and what are the primary concerns?

27. How does AWS provide security for its customers?

28. Explain the security management regarding cloud computing.

29. Explain the full form and usage of “EUCALYPTUS” in cloud computing?

30. Explain hybrid and community cloud?

31. Do public clouds owned third parties offers commercialized cloud services and IT resources to consumer organizations? Justify your answer.

32. Define Virtual Machine.

1. Start-up A deploying its web application on a cloud server would likely have lower initial investment costs compared to start-up B deploying on its own infrastructure. Cloud services offer a pay-as-you-go model, eliminating the need for large upfront hardware investments, maintenance costs, and providing scalability based on usage.
2. The primary business drivers for cloud computing include the need for cost efficiency, scalability, flexibility, rapid deployment of applications, and the demand for on-demand access to computing resources without the burden of managing physical infrastructure.
3. Start-up A deploying its web application on a cloud server represents a multitenant environment. In this scenario, multiple users (tenants) share the same physical resources of the cloud infrastructure. Cloud providers use virtualization and resource allocation mechanisms to ensure isolation and efficient utilization among multiple tenants.

34. Start-up A opts to deploy its web application on a cloud server whereas start-up B opts to deploy the application on its own infrastructure. Excluding other expenses, compare investment cost of both start-up with proper reasoning.

35. What are the primary business drivers that exposed the need for cloud computing and led to its formation?

36. Which one of the above scenario is a multitenant environment? And how does it work?

1. Pooling of physical resources in cloud computing involves aggregating and sharing computing resources such as servers, storage, and networking, to efficiently allocate and meet the dynamic demands of multiple users or applications.
2. Various storage systems technologies used in the cloud include Object Storage, Block Storage, File Storage, and Content Delivery Networks (CDNs), each serving different purposes in terms of scalability, accessibility, and performance.
3. Multiple ways of launching a Denial of Service (DoS) attack include flooding the network with traffic (flood attack), exploiting vulnerabilities to crash servers (exploit attack), and overwhelming resources by exhausting connection limits (connection exhaustion attack).
4. Mechanisms used to collect audit tracking data in the cloud include logging and monitoring tools for networks, while IT resources are monitored using performance metrics and logs. For regulatory and contractual obligations, compliance management tools track adherence to specified standards and requirements.
5. Migrating in cloud computing refers to the process of moving applications, data, or IT resources from an on-premise environment to a cloud-based infrastructure, often to leverage the benefits of scalability, cost-efficiency, and flexibility.
6. Authentication verifies the identity of a user, ensuring they are who they claim to be, while authorization determines the permissions and access levels granted to authenticated users or entities.
7. A cloud VPN (Virtual Private Network) is a network technology that allows secure communication over the public internet between on-premise networks or devices and resources in a cloud environment.
8. A cloud usage monitor is a tool or service that tracks and analyzes the consumption of cloud resources, providing insights into usage patterns, costs, and efficiency.
9. Cloud delivery models include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), representing different levels of abstraction and management responsibility.
10. Security benefits of cloud computing include data encryption, regular security updates, automated threat detection, and the ability to leverage the expertise of specialized security teams employed by cloud service providers.
11. Different roles in Azure include administrator roles, user roles, and specialized roles such as contributor, reader, and owner, each with varying levels of permissions and responsibilities.
12. Different phases associated with cloud architecture include planning and assessment, design, migration, deployment, and ongoing management and optimization.
13. Automated scaling listeners can respond to workload fluctuations by adjusting the number of instances, resources, or containers based on demand, ensuring optimal performance and resource utilization.
14. The mechanism activated when three cloud service consumers try to access a single cloud service simultaneously is load balancing, which distributes incoming traffic across multiple servers to ensure even resource utilization and improved performance.
15. PaaS environments provide less administrative control than IaaS but still offer features such as application development tools, middleware, and runtime environments for developers to build and deploy applications.
16. If the IP address or hostname of a data node changes, it may result in data node unavailability or loss of communication with other nodes, impacting the overall stability and functionality of the distributed storage system.
17. For unpredictable usage peaks of the Remote Upload Module, a serverless architecture in the cloud would be suitable. Serverless computing allows automatic scaling based on demand, ensuring resources are allocated dynamically to handle varying workloads.
18. Threat agents are individuals or entities with the intent to exploit vulnerabilities or compromise security. Their role in cloud security involves posing risks to cloud infrastructure, data, and applications, necessitating robust security measures.
19. Hybrid cloud combines both public and private cloud environments, allowing data and applications to move seamlessly between them. It offers flexibility, scalability, and the ability to maintain sensitive data on-premise.
20. Service-Oriented Architecture (SOA) is an architectural approach where software components are designed as services that can be independently deployed, accessed, and composed to create complex applications.
21. Systems of systems refer to interconnected and interoperable systems that work together to achieve common goals. Examples include smart cities, where various systems like transportation, energy, and healthcare collaborate to enhance overall efficiency.
22. Virtualization platforms in implementing cloud provide the abstraction and isolation of physical hardware, enabling the creation and management of virtual machines or containers to run applications independently of the underlying infrastructure.
23. EC2 (Elastic Compute Cloud) instance in AWS is a virtual server in the cloud that can be configured and launched based on user requirements, providing scalable compute capacity.
24. System integrators in cloud computing bring expertise in integrating diverse cloud services, ensuring seamless functionality, data flow, and collaboration across various platforms, ultimately optimizing overall system performance.
25. Microsoft Azure is a cloud computing platform that offers a wide range of services, including virtual machines, databases, AI services, and developer tools, as part of the Windows Azure operating system.
26. AWS (Amazon Web Services) in cloud computing is a comprehensive platform offering various services such as computing power, storage, databases, machine learning, and more. Key components include EC2, S3, RDS, and Lambda.
27. Cloud computing is the delivery of computing services over the internet, providing on-demand access to a shared pool of configurable computing resources. Main features include scalability, self-service, pay-as-you-go pricing, and resource pooling.
28. Web 2.0 represents a major revolution in internet technology characterized by user-generated content, collaboration, and interactive web applications, fostering a more dynamic and participatory online experience.
29. Different types of models in cloud computing include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), each offering varying levels of abstraction and management.
30. Three cloud services in cloud computing are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), representing different levels of service and management responsibilities.
31. Scaling in cloud computing refers to adjusting resources based on demand. Different types of scaling include vertical scaling (increasing resources within a single instance) and horizontal scaling (adding more instances to distribute workload).
32. Different boundaries defined in a cloud computing system include organizational boundaries, data boundaries, and geographic boundaries, each influencing the design, deployment, and management of cloud services.
33. Vendor lock-in in cloud computing refers to the risk of being tied to a specific cloud service provider's proprietary technologies and services. To avoid vendor lock-in, businesses can adopt standards-based technologies, use multi-cloud strategies, and ensure data portability.

37. Write the use of "pooling of physical resources".

38. Mention various storage systems technologies used in cloud?

39. DoS attack is to overload IT resources to the point where they cannot function properly. Write multiple ways of launching DoS attack.

40. Which of mechanisms are used to collect (1) audit tracking data for networks, (2) IT resources in support of regulatory and (3) contractual obligations in cloud environment?

41. Whatismean by migrating in cloud computing?

42. What are the differences between Authentication and Authorization?

43. What is a cloud VPN?

44. What do you mean by cloud usage monitor?

45. What do you mean by cloud delivery models?

46. What are the security benefits of cloud computing?

47. What are the different roles in AZURE?

48. What are the different phases associated with cloud architecture?

49. What kinds of responses to workload fluctuations can be offered by automated scaling listeners\*

50. In the provided diagram, three cloud service consumers are trying to access a single cloud service simultaneously. What mechanism is activated when

51. PaaS environments provide less administrative control than IaaS environments, but still offer a significant range of management features. Mention

those features.

52. What happens if the IP address or hostname of a data node changes?

53. An in-house solution that a company named ATN did not migrate to the cloud is the Remote Upload Module; a program that is used by their clients to

upload accounting and legal documents to a central archive on a daily basis. Usage peaks occur without warning since, the quantity of documents received on a day by-day basis is unpredictable. The Remote Upload Module currently rejects upload attempts when it is operating at capacity, which is problematic for users that need to archive certain documents before the end of a business day or prior to a deadline. ATN decides to take advantage of its cloud-based environment. Which Architecture would be suitable for this?

54. Define threat AgentsP Explain their role in cloud security.

55. Write a note on Hybrid cloud.

56. Define SOA?

57. What do you mean by systems of systems\* Give examples.

58. What is the usage of virtualization platform in implementing cloud?

59. What is the EC2 (Elastic Compute Cloud) instance?

61. What is the benefits of using system integrators in cloud computing?

62. What is Microsoft Azure? Name the services offered by the Windows Azure operating system.

63. What is AWS in cloud computing? Mention the key components of AWS.

64. Define cloud computing and Identify the main features of cloud computing.

65. Explain the major revolution introduced by web 2.0

66. Explain the different types of models in the cloud computing

67. Explain the three cloud services in cloud computing

68. What is scaling in cloud computing? What are different types of scaling? explain in brief.

69. Explain different boundaries defined in a cloud computing system?

70. What is vendor lockin problem in CC, what are the risks associated with vendor lockin problem, what are the possible ways to avoid Vendor Lock In problem.Top of Form