224

10

Scoring Indicators

COURSE NAME : DIPLOMA EXAMINATION IN ENGINEERING/TECHNOLOGY/ MANAGEMENT/COMMERCIAL PRACTICE.

VIRTUALIZATION TECHNOLOGY AND CLOUD COMPUTING

COURSE CODE : TED (21) – 5133A QID : **2109230294**

Q No	Scoring Indicators	Split score	Sub Total	Total score
	PART A			**9**
I.	Cloud computing refers to the delivery of various computing services, including servers, storage, databases, networking, software, analytics, and intelligence, over the internet to offer faster innovation, flexible resources, and economies of scale		1	
2	Xen,KVM,Virual Box etc		1	
3	virtualization and virtual machines (VMs), "storage" refers to the allocation and management of data storage resources for the VM.		1	
4	Hypervisor		1	
5	Reduce Cost, Works from any ware, Can work on own devices, Applications can easily kept updated		1	
6	Microsoft Azure, AWS, VMWare, Oracle, Google Cloud, IBM, Amazon etc		1	
7	Availability, Security, Simplicity, Easy of Backup, Pay only for what used		1	
8	Public , Private, Community , Hybrid		1	
9	Application, DBMS, Compute, Storage, Network		1	
	PART B			**24**
1	Type II hypervisors, also known as hosted hypervisors or desktop hypervisors, are virtualization software that runs on top of a conventional operating system, rather than directly on the physical hardware of a computer. These hypervisors are typically used for virtualization on desktop or laptop computers and are designed to allow users to run multiple virtual machines (VMs) on a single physical machine. Here are some key characteristics and features of Type II hypervisors: 1. Hosted Environment 2. User-Friendly 3. Resource Sharing 4. Examples	1 2*1	3	

	5. Compatibility 6. Use Cases			
2	A virtual machine (VM) is a software-based emulation of a physical computer. It acts as an isolated and self-contained computing environment within a host operating system (OS) or on dedicated hardware. Virtual machines are designed to mimic the hardware and functionality of a physical computer, allowing multiple operating systems and applications to run concurrently on a single physical machine.		3	
3	Network virtualization is a technology that allows the creation of multiple virtual network segments or instances on a single physical network infrastructure. It decouples the network's underlying hardware from the software that manages it, enabling more efficient and flexible network management and utilization. Network virtualization is commonly used in data centers, cloud computing environments, and enterprise networks to improve resource allocation,		3	
4	VM clones, short for Virtual Machine clones, are duplicates or copies of existing virtual machines (VMs) in a virtualized computing environment. These clones are created to replicate the configuration and state of the original VM at a specific point in time. VM cloning is a common practice in virtualization technologies like VMware, Hyper-V, and others **Purpose**: VM clones are typically created for various purposes, such as testing, development, disaster recovery, and scaling. They provide a convenient way to replicate a known working configuration without having to manually recreate all settings and software installations. 1. Types of Cloning: • Full Clone • Linked Clone:	2 1	3	
5	Desktop virtualization is a technology that allows multiple virtual desktop environments to run on a single physical computer or server. It separates the desktop operating system and applications from the underlying hardware, enabling users to access their desktops remotely or run multiple desktop instances on a single machine Application virtualization refers to the practice of encapsulating and isolating software applications from the underlying hardware and operating system, allowing them to run in a self-contained environment. This technology enables the execution of applications on a wide range of computer systems without needing to install them directly on each individual system. Instead, the applications are packaged along with their dependencies, settings, and runtime components into a virtualized container or package.	1.5*2	3	
6	Scalability, Cost Efficiency, Accessibility, Flexibility	3*1	3	
7	Cloud infrastructure refers to the foundational technology and resources that make up cloud computing environments. Cloud computing is a model for delivering and accessing computing services over the internet on a pay-as-you-go basis. Cloud infrastructure provides the underlying framework that enables the	1	3	

	delivery of these services. It typically includes the following components: 1. **Data Centers** 2. **Virtualization** 3. **Networking** 4. **Storage** 5. **Compute Resources** 6. **Load Balancers** 7. **Security** 8. **Monitoring and Management Tools.** 9. **Scalability.** 10. **Service Models.**	2*1		
8	Storage management in cloud computing refers to the strategies and practices employed to efficiently and securely store data in a cloud environment. Cloud computing offers scalable and flexible storage solutions that can meet the diverse needs of businesses and individuals. Here are key aspects of storage management in cloud computing Data Storage Models: • Object Storage • Block Storage • File Storage Scalability, Data Redundancy and Durability Data Backup and Recovery, Data Lifecycle Management Data Encryption, Access Control and Permissions Cost Optimization, Data Transfer and Migration Monitoring and Management Compliance and Governance Hybrid and Multi-Cloud Storage		3	
9	Virtual switch load balancing is a crucial concept in the context of virtualization and network management. Virtual Switch: A virtual switch is a software-based network switch that operates within a hypervisor or virtualization platform. It connects virtual machines (VMs) to physical network infrastructure. 1. Load Balancing Algorithms 2. Network Performance 3. Redundancy 4. Failover. 5. Management and. 6. Scalability. 7. Security		3	
10	Computing on demand" in the context of cloud computing refers to the ability to access and use computing resources as needed: 1. **Resource Provisioning**: Cloud providers offer a variety of resources such as virtual machines (VMs), storage, databases, and networking services. Users can provision		3	

	these resources through a web interface or APIs based on their requirements. 2. **Scalability**: One of the primary advantages of cloud computing is the ability to scale resources up or down as needed. This can be done manually by the user or automatically based on defined policies. For example, if a website experiences a sudden increase in traffic, additional servers can be provisioned to handle the load, and when the traffic subsides, those resources can be released. 3. **Pay-as-You-Go**: Cloud computing typically operates on a pay-as-you-go or pay-for-what-you-use model. Users are billed based on their actual usage of resources, which can lead to cost savings compared to traditional on-premises infrastructure where you have to purchase and maintain hardware even during periods of low demand. 4. **Elasticity**: Elasticity is a key feature of cloud computing. It means that resources can automatically scale up or down based on real-time demand. This ensures that applications can handle varying workloads without manual intervention. 5. **Self-Service**: Cloud computing platforms are designed to be self-service, allowing users to provision, configure, and manage resources without the need for direct involvement from IT or system administrators. 6. **Global Accessibility**: Cloud services are accessible from anywhere with an internet connection, making them suitable for global operations and remote work. 7. **Resource Management**: Cloud providers offer tools and services for managing and monitoring resources. This includes features like load balancing, auto-scaling, and performance monitoring. 8. **Security and Compliance**: Cloud providers invest heavily in security measures to protect data and resources. Users can also configure security settings to meet their specific requirements. Compliance certifications are often provided to ensure adherence to industry standards. 9. **Backup and Disaster Recovery**: Cloud providers typically offer backup and disaster recovery solutions, making it easier for organizations to protect their data and applications.			
	PART C			**42**
III	1. Resource Optimization 2. Cost Reduction 3. Improved Disaster Recovery 4. Scalability and Flexibility 5. Testing and Development 6. Enhanced Security 7. Legacy Application Support 8. Simplified Management	7*1	7	7
IV	1. Resource Allocation 2. Isolation and Security 3. Virtual Machine Management 4. Performance Optimization 5. Migration and High Availability	7*1	7	7

	6. Snapshot and Backup 7. Resource Monitoring and Reporting 8. Networking and Storage Virtualization 9. Compatibility and Integration License Management			
V	1. Hardware Virtualization • Full Virtualization • Para-Virtualization 2. Container Virtualization 3. Application Virtualization 4. Network Virtualization 5. Storage Virtualization 6. Desktop Virtualization 7. Operating System-level Virtualization 8. Storage Area Network (SAN) Virtualization. 9. Hardware-assisted Virtualization	7*1	7	7
VI	Hypervisors, also known as virtual machine monitors (VMMs), are software or hardware components that enable multiple virtual machines (VMs) to run on a single physical host system. There are two primary types of hypervisors: Type 1 (bare-metal) and Type 2 (hosted) **Type 1 Hypervisor (Bare-Metal Hypervisor):** • **Installation**: Type 1 hypervisors are installed directly on the physical hardware of the host system, without the need for an underlying operating system. They run directly on the hardware. • **Performance**: They generally offer better performance compared to Type 2 hypervisors because they have direct access to the hardware resources. • **Use Cases**: Type 1 hypervisors are commonly used in enterprise environments and data centers for virtualization, where performance, security, and isolation are critical. • **Examples**: VMware vSphere/ESXi, Microsoft Hyper-V (when installed as a standalone hypervisor), Xen, KVM. **Type 2 Hypervisor (Hosted Hypervisor):** • **Installation**: Type 2 hypervisors run on top of an existing operating system (host OS). Users install them as applications within the host OS. • **Performance**: They tend to have slightly higher overhead compared to Type 1 hypervisors because they must go through the host OS to access hardware resources. • **Use Cases**: Type 2 hypervisors are often used for development, testing, or running multiple operating systems on a personal computer or workstation. • **Examples**: VMware Workstation, Oracle VirtualBox, Parallels Desktop (for Mac). **Comparison Factors:**	1 1 1	7	7

	• **Performance**: Type 1 hypervisors generally offer better performance because they don't have the overhead of a host operating system. They provide direct access to hardware resources. • **Security**: Type 1 hypervisors are considered more secure since they have a smaller attack surface compared to Type 2 hypervisors, which rely on the security of the host operating system. • **Resource Isolation**: Type 1 hypervisors provide stronger resource isolation between VMs since they have direct control over hardware resources. Type 2 hypervisors may have resource contention due to the underlying host OS. • **Ease of Use**: Type 2 hypervisors are often easier to set up and use for personal or non-production purposes because they run on top of a familiar operating system. Type 1 hypervisors may require more expertise. • **Use Cases**: Type 1 hypervisors are typically used in enterprise environments, cloud data centers, and production environments where performance and security are paramount. Type 2 hypervisors are more suitable for development, testing, or running multiple OS environments on a single desktop or laptop. • **Examples**: Type 1 hypervisors include VMware ESXi and XenServer, while Type 2 hypervisors include VirtualBox and VMware Workstation.	4*1		
VII	Benefits of Network Virtualization: 1. Resource Optimization 2. Isolation and Security 3. Flexibility and Agility 4. Fault Isolation 5. Enhanced Management 6. Improved Testing and Development Components of Network Virtualization: 1. Hypervisor or Virtual Switch 2. Virtual Network Adapters 3. Virtual LANs (VLANs 4. Overlay Networks 5. Network Virtualization Software 6. Network Policies 7. Orchestration and Management 8. Centralized Controllers.	3.5 3.5	7	7
VIII	Advantages:	3.5	7	7

	1. Compatibility 2. Isolation 3. Simplified Deployment 4. Resource Efficiency 5. Security Disadvantages: 1. Unavailability 2. Initial Cost	3.5		
IX	1. Location Selection 2. Hardware Infrastructure 3. Power and Cooling 4. Security Measures 5. Connectivity 6. Scalability and Redundancy 7. Virtualization and Hypervisors 8. Network Architecture 9. Storage Solutions 10. Management and Orchestration 11. Compliance and Data Governance 12. Monitoring and Analytics 13. Backup and Disaster Recovery 14. Documentation and Documentation 15. Resource Allocation and Billing 16. Customer Support and SLAs 17. Environmental Sustainability 18. Regulatory Compliance 19. Staffing and Training 20. Regular Maintenance and Upgrades 21. Testing and Quality Assurance 22. Disaster Recovery Testing 23. Cost Management 24. Documentation and Auditing	Any 7*1	7	7
X	1. On-Demand Self-Service 2. Broad Network Access 3. Resource Pooling 4. Rapid Elasticity 5. Measured Service 6. Service Models • Infrastructure as a Service (IaaS • Platform as a Service (PaaS • Software as a Service (SaaS 7. Deployment Models: • Public Cloud • Private Cloud • Hybrid Cloud 8. Reliability and Redundancy 9. Security 10. Automation and Management 11. Geographic Reach 12. Ecosystem and Integration	Any 7*1	7	7

XI	1. **Public Cloud:** • Ownership • Accessibility • Multi-Tenancy • Scalability. • Cost-Efficiency • Examples of Public Cloud Providers: AWS, Azure, GCP, IBM Cloud, Oracle Cloud. **Use Cases:** • Web hosting and website development • Application development and testing • Big data and analytics • Disaster recovery and backup • Content delivery and streaming • Software as a Service (SaaS) applications 2. **Private Cloud:** • Ownership • Control • Security and Privacy • Scalability • Cost • **Use Cases:** • Highly regulated industries (e.g., finance, healthcare) with strict data privacy and compliance requirements. • Organizations with specific security or performance needs. • Large enterprises that want more control over their cloud infrastructure. • Research institutions or government agencies handling sensitive data.	3.5 3.5	7	7
XII	Cloud storage refers to a service that allows you to store and access data and files over the internet instead of on your local computer or physical storage devices like hard drives or USB drives. It is a popular and convenient way to store, manage, and share data, offering several advantages: 1. Accessibility 2. Scalability 3. Cost-Efficiency 4. Data Redundancy and Backup 5. Collaboration 6. Security and Data Protection. 7. Automatic Synchronization Some popular cloud storage providers include: 1. **Google Drive**: Offers storage for various types of files and integrates seamlessly with Google Workspace (formerly G Suite) applications.	2 4 1	7	7

	2. **Dropbox**: Known for its user-friendly interface and file-sharing capabilities, Dropbox is popular among individuals and businesses. 3. **Microsoft OneDrive**: Integrated with Microsoft 365 (formerly Office 365), OneDrive provides cloud storage for Microsoft Office files and other data. 4. **Amazon S3 (Simple Storage Service)**: A widely used solution for developers and businesses, providing scalable object storage in the Amazon Web Services (AWS) ecosystem. 5. **Apple iCloud**: Apple's cloud storage service, primarily designed for Apple device users, offers storage for photos, documents, and app data. 6. **Box**: Popular among businesses, Box offers secure and collaborative cloud storage solutions.			
XIII	Compare SaaS and PaaS Software as a Service (SaaS) and Platform as a Service (PaaS) are both cloud computing service models, but they serve different purposes and provide different levels of control and flexibility to users. 1. Purpose: • SaaS: SaaS provides ready-to-use software applications that are hosted in the cloud and delivered over the internet to end-users. These applications are typically designed for specific business functions, such as email, CRM, productivity tools, or collaboration software. • PaaS: PaaS provides a platform and environment for developers to build, deploy, and manage their own applications. It offers tools, frameworks, and infrastructure for application development and hosting. 2. Control and Customization: • SaaS: SaaS applications are pre-built and maintained by the service provider. Users have limited control over the underlying infrastructure and software, and customization options are often restricted to configuring settings within the application. • PaaS: PaaS provides more control and customization options. Developers can build and customize their applications using the platform's tools and resources. They have greater flexibility to tailor applications to their specific requirements. 3. Development: • SaaS: SaaS applications are not typically used for development purposes. They are designed for end-users to consume the functionality provided by the software. • PaaS: PaaS is specifically designed for application development. Developers use PaaS platforms to build, test, and deploy their applications. PaaS providers offer development tools, databases, and runtime environments.	1 3*2	7	7

	4. Deployment: • SaaS: SaaS applications are already deployed and hosted by the service provider. Users simply access them through a web browser or client application without worrying about deployment details. • PaaS: PaaS users are responsible for deploying their applications onto the platform. The PaaS provider manages the underlying infrastructure, but users have control over how their applications are deployed and scaled. 5. Maintenance and Updates: • SaaS: Service providers are responsible for maintaining and updating SaaS applications. Users do not need to worry about patching, security, or software updates. • PaaS: PaaS providers manage the underlying infrastructure and platform components, but users are responsible for maintaining and updating their own applications. 6. Use Cases: • SaaS: SaaS is ideal for businesses and individuals who want to access software applications without the burden of managing infrastructure or development. Examples include email services like Gmail, customer relationship management (CRM) tools like Salesforce, and productivity suites like Microsoft 365. • PaaS: PaaS is suitable for developers and organizations that want to build, customize, and deploy their own applications. It is commonly used for web and mobile application development, database management, and application hosting.			
XIV	Disaster recovery (DR) in cloud computing refers to the set of strategies and procedures put in place to protect an organization's data, applications, and IT infrastructure in the event of a disaster or disruptive event. These disasters can range from natural calamities like earthquakes or floods to human-made incidents such as cyberattacks, hardware failures, or data corruption. The goal of disaster recovery in the cloud is to ensure that business operations can be quickly resumed with minimal data loss and downtime. Here are key components and concepts related to disaster recovery in cloud computing: 1. Backup and Replication 2. RTO and RPO: Recovery Time Objective (RTO) and Recovery Point Objective (RPO) 3. High Availability (HA) 4. Data Centers and Regions 5. Failover and Failback 6. Disaster Recovery as a Service (DRaaS 7. Testing and Maintenance 8. Security and Compliance 9. Cost Considerations	2 5*1	7	7