Final Examination for the Course Software Defined Systems

Maximum score: 50%

Time Allowed: 2hrs

Item	True/ False	MSQ	Short Answer	Scenario based	Total
Value	5%	25%	12%	8%	50%
Score					

Part I: True or False Items *(5pts)*

1. [False]
2. [False]
3. [False]
4. [True]
5. [False]

Part II: Multiple Choice Items *(25pts)*

1. [B]	8. [A]	15. [C]	22. [B]
2. [A]	9. [C]	16. [C]	23. [B]
3. [C]	10. [B]	17. [A]	24. [C]
4. [B]	11. [B]	18. [C]	25. [B]
5. [C]	12. [B]	19. [C]	
6. [D]	13. [B]	20. [D]	
7. [D]	14. [A]	21. [B]	

Part III: Short Answer Items *(12pts)*

1. Traditional network management relies on a decentralized approach where each network device—such as routers and switches—has its own control plane, requiring manual configuration and management. This can lead to complexities and inconsistencies, as changes must be made individually on each device. In contrast, Software-Defined Networking (SDN) centralizes the control plane in an SDN controller, allowing for programmatic management of the network. This enables more dynamic and agile network configurations, easier policy enforcement, and improved automation, making it simpler to manage large-scale networks.

2. **Routing**

   Routing determines the best path for data packets to travel across a network. Routers make forwarding decisions based on destination IP addresses and routing tables.

   Switching

   Switching involves directing data packets within a local area network (LAN). Switches operate at the data link layer and connect devices within the same network, ensuring efficient data transmission.

   Firewalling

   Firewalls provide security by monitoring and controlling incoming and outgoing network traffic based on predetermined security rules. They protect networks from unauthorized access and threats.

   Load Balancing

   Load balancers distribute network traffic across multiple servers to optimize resource use and avoid overload on any single server. This enhances application availability and performance.

3. Elasticity in cloud computing refers to the ability to automatically scale resources up or down based on demand. This means that cloud services can dynamically allocate or release resources (such as CPU, memory, and storage) in response to varying workloads. Elasticity differs from scalability, which is the ability to increase system capacity by adding resources; scalability can be manual and may not be instantaneous. Elasticity emphasizes the automated and responsive nature of resource management in cloud environments.

4. A Secure Channel in an SDN Controller ensures secure communication between the SDN controller and network devices. This is critical to prevent unauthorized access and ensure data integrity. Common protocols used in SDN for establishing secure channels include:
   - **Transport Layer Security** (**TLS**): Provides encryption and secure communication over networks.
   - **Secure Socket Layer** (**SSL**): An earlier protocol for secure communication, now largely replaced by TLS.
   - **OpenFlow**: While primarily a communication protocol for SDN, it also supports secure communication features.

5. **Public Cloud**

   Control: Limited control over infrastructure as it is owned by a third-party provider.
   Security: Generally less secure than private clouds, as resources are shared among multiple tenants.
   Cost: Cost-effective, as it operates on a pay-as-you-go model without upfront capital investment.

   Private Cloud

   Control: Full control over the infrastructure and resources. Organizations can customize the environment to meet specific needs.
   Security: More secure than public clouds, as resources are dedicated to a single organization, reducing the risk of data breaches.
   Cost: Higher initial investment and ongoing maintenance costs compared to public clouds.

   Hybrid Cloud

   Control: Offers a balance between public and private clouds, allowing for more control over sensitive data while leveraging public resources for less critical workloads.
   Security: Provides enhanced security for sensitive applications while utilizing public cloud resources for scalability.
   Cost: Can be cost-effective if managed properly, but complexity in management can lead to higher costs if not optimized.

Part IV – Scenario based Items *(8pts)*

1. Virtualization is the process of creating a virtual version of physical hardware resources, such as servers, storage devices, and network components. It allows multiple virtual machines (VMs) to run on a single physical server, each operating independently with its own operating system and applications.

   How It Works:

   - **Hypervisor**: Virtualization relies on a hypervisor, a software layer that sits between the physical hardware and the VMs. The hypervisor manages the allocation of physical resources (CPU, memory, storage) to each VM.
   - **Isolation**: Each VM operates in an isolated environment, enabling multiple operating systems to run concurrently on the same hardware without interference.

- **Resource Allocation**: The hypervisor dynamically allocates resources based on demand, ensuring efficient use of the underlying hardware

2. **Improved Resource Utilization**
   Virtualization allows for better utilization of physical server resources by running multiple VMs on a single server. This maximizes the use of CPU, memory, and storage, reducing waste.

   Increased Flexibility
   Organizations can quickly deploy, modify, or scale VMs as needed. This flexibility supports rapid development and testing environments, allowing IT to respond swiftly to changing business demands.

   Cost Savings
   By reducing the need for physical hardware, virtualization can significantly lower capital expenditures on servers and associated costs (e.g., power, cooling, and space). It also streamlines management, leading to operational cost savings.

3. **Select a Hypervisor**
   Choose between a Type 1 hypervisor (bare-metal) like VMware ESXi or Microsoft Hyper-V, or a Type 2 hypervisor (hosted) like Oracle VirtualBox, depending on your needs and existing infrastructure.

   Plan VM Configurations
   Determine the specifications for each VM, including CPU, memory, storage, and network requirements. Assess the workload characteristics to allocate resources effectively.

   Migrate Existing Workloads
   Develop a migration plan for existing applications and data. Use tools like VMware vMotion or Microsoft's Live Migration to move workloads to the new virtualized environment with minimal downtime. Test the migration process in a staging environment before executing it in production.

4. **Resource Contention**
   Challenge: Multiple VMs competing for limited physical resources can lead to performance degradation.
   Mitigation: Carefully monitor resource usage and implement resource allocation policies to prioritize critical workloads. Use tools for performance monitoring and balancing.

Security Risks

Challenge: Virtual environments can introduce new security vulnerabilities, such as VM sprawl or insufficient isolation between VMs.

Mitigation: Implement strict access controls, network segmentation, and regular security audits. Use security solutions designed for virtualized environments.

Complexity in Management

Challenge: Managing a virtualized environment can become complex, especially as the number of VMs increases.

Mitigation: Utilize centralized management tools that provide visibility and control over the virtual infrastructure. Train staff on best practices for managing virtual environments.