

Q. No	Question	Mark	BL	CO	PO	PI Code
1	<b>Which is referred to the amount of time and effort required to exploit an attack vector?</b> a. Attack surface                      b. Attack vector b. <b>Work factor</b> d. DOS	1	L2	5	4	1.7.1
2	<b>A control mechanism on the switches that segments the network in to specific paths to be used for data traffic is called</b> a. LNU                                      b. <b>Zoning</b> b. ACL                                      d. Role based control access	1	L3	5	4	2.5.2
3	<b>Which of the following refers to a situation in which any existing security threat in the cloud spreads more rapidly in cloud infrastructures.</b> a. <b>Velocity of Function</b> b. Data privacy b. Information assurance      d. Data protection	1	L2	4	4	2.5.2
4	<b>Where the single point of security failure for all the VM s running on the cloud infrastructure will happen</b> a. Physical server                      b. <b>Hypervisor</b> b. Supervisor                      d. Controller	1	L2	4	4	2.5.2
5	<b>Which of the following is not a cloud enabling technology?</b> a. Grid Computing                      b. Virtualization b. Utility Computing                      d. <b>Edge Computing</b>	1	L2	4	4	1.7.1
6	<b>What type of computing technology refers to services and applications that typically run on a distributed network through virtualized resources?</b> a. Cloud Computing                      b. <b>Soft Computing</b> b. Parallel Computing                      d. Distributed Computing	1	L2	6	2	1.7.1
7	<b>In which one of the following, a strategy record or Document is created respectively to the events, conditions a user may face while applying cloud computing mode.</b> a. Cloud Computing Value Proposition b. <b>Cloud Computing Strategy Planning</b> c. Planning Phase	1	L2	5	1	5.4.1

	d. Business Architecture Development					
8	<b>Redundancy has to be implemented at the _____ architectural level for effective results in cloud computing.</b> a. Lower <b>b. Higher</b> c. Middle d. Poor Performances	1	L2	4	4	2.5.2
9	<b>Which of the following protocol is used for discovering and retrieving objects from a cloud?</b> <b>a. OCCI</b> b. SMTP c. HTTP d. TCP/IP	1	L2	4	4	2.5.2
10	<b>Which of the following is the correct statement about cloud types?</b> a. Cloud Square Model is meant to show is that the traditional notion of a network boundary being the network's firewall no longer applies in cloud computing <b>b. A deployment model defines the purpose of the cloud and the nature of how the cloud is located.</b> c. Service model defines the purpose of the cloud and the nature of how the cloud is located. d. Cloud services modules.	1	L1	5	2	2.5.2

---

**Part – B ( 4 x 5 = 20 Marks)**

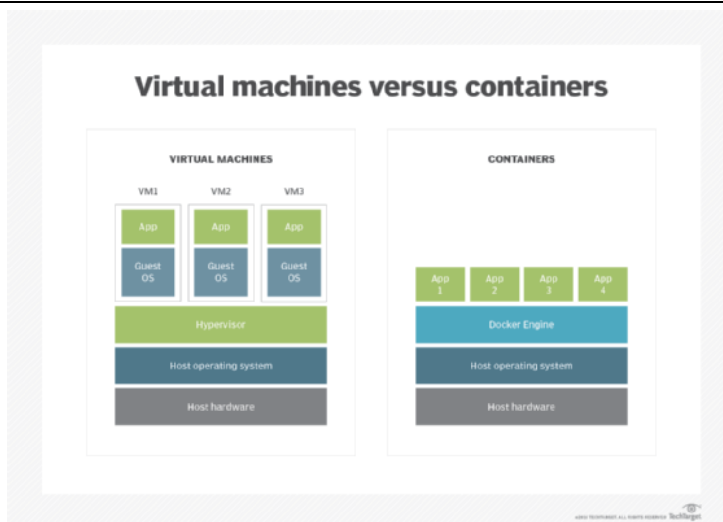
## Answer All the Questions

11	<p><b>Elaborate storage security domain and threats in each domain.</b></p> <p>Storage Security Domains</p> <p>Securing the Application Access Domain</p> <ul style="list-style-type: none"> <li>• Common threats <ul style="list-style-type: none"> <li>▶ Spoofing administrator's identity</li> <li>▶ Elevating administrative privileges</li> <li>▶ Network snooping and DoS</li> </ul> </li> <li>• Available controls <ul style="list-style-type: none"> <li>▶ Authentication, authorization, and management access control</li> <li>▶ Private management network</li> <li>▶ Disable unnecessary network services</li> <li>▶ Encryption of management traffic</li> </ul> </li> </ul> <p>Securing Backup, Replication, and Archive Domain</p> <ul style="list-style-type: none"> <li>• Common threats <ul style="list-style-type: none"> <li>▶ Spoofing DR site identity</li> <li>▶ Tampering with data in-flight and at rest</li> <li>▶ Network snooping</li> </ul> </li> <li>• Available controls <ul style="list-style-type: none"> <li>▶ Access control – primary to secondary storage</li> </ul> </li> </ul>	5	L3	4	2	2.5.2
----	--	---	----	---	---	-------

RegNo															
-------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

	<ul style="list-style-type: none"> <li>▶ Backup encryption</li> <li>▶ Replication network encryption</li> </ul>					
12	<b>Compare active and passive attacks with examples</b>  Attacks can be classified as passive or active <ul style="list-style-type: none"> <li>a. Passive attacks               <ul style="list-style-type: none"> <li>i. Attempt to gain unauthorized access into the system</li> <li>ii. Attempt to threat the confidentiality of information</li> </ul> </li> <li>b. Active attacks               <ul style="list-style-type: none"> <li>i. Attempt data modification, Denial of Service (DoS), and repudiation attacks</li> <li>ii. Attempt to threat data integrity, availability, and accountability</li> </ul> </li> </ul>	5	L2	4	2	2.5.2
13	<b>Discuss in detail about the enabling technologies of the cloud computing.</b> Virtualization Service-Oriented Architecture (SOA) Grid Computing Utility Computing	5	L2	6	4	2.7.1
14	<b>Containers create an isolation boundary at the application level rather than at the server level. If anything goes wrong in that single container - for example, excessive consumption of resources by a process, in such cases elaborate how the containers will handle the situation write up with a solution.</b>  The key thing to recognize with cloud containers is that they are designed to virtualize a single application. For example, you have a MySQL container, and that's all it does -- it provides a virtual instance of that application. Containers create an isolation boundary at the application level rather than at the server level. This isolation means that, if anything goes wrong in that single container -- for example, excessive consumption of resources by a process -- it only affects that individual container and not the whole VM or whole server. It also eliminates compatibility problems between containerized applications that reside on the same OS. Major cloud vendors offer containers-as-a-service products, including Amazon Elastic Container Service, AWS Fargate, Google Kubernetes Engine, Microsoft Azure Container Instances, Azure Kubernetes Service and IBM Cloud Kubernetes Service. Containers can also be deployed on public or private cloud infrastructure without the use of dedicated products from a cloud vendor.  There are still key questions that need answers: How exactly do containers differ from traditional hypervisor-based VMs? And, just because containers are so popular,	5	L2	5	4	1.7.1

<p>does it mean they are better?</p> <p>Cloud containers vs. VMs</p> <p>The key differentiator with containers is the minimalist nature of their deployment. Unlike VMs, they don't need a full OS to be installed within the container, and they don't need a virtual copy of the host server's hardware. Containers can operate with a minimum amount of resources to perform the task they were designed for -- this can mean just a few pieces of software, libraries and the basics of an OS. This results in being able to deploy two to three times as many containers on a server than VMs, and they can be spun up much faster than VMs.</p> <p>Cloud containers are also portable. Once a container has been created, it can easily be deployed to different servers. From a software lifecycle perspective, this is great, as containers can quickly be copied to create environments for development, testing, integration and production. From a software and security testing perspective, this is advantageous because it ensures the underlying OS is not causing a difference in the test results. Containers also offer a more dynamic environment as IT can scale up and down more quickly based on demand, keeping resources in check.</p> <p>One downside of containers is the problem of splitting your virtualization into lots of smaller chunks. When there are just a few containers involved, it's an advantage because you know exactly what configuration you're deploying and where. However, if you fully invest in containers, it's quite possible to soon have so many containers that they become difficult to manage. Just imagine deploying patches to hundreds of different containers. If a specific library needs updating inside a container because of a security vulnerability, do you have an easy way to do this? Problems of container management are a common complaint, even with container management systems, such as Docker, that aim to provide easier orchestration for IT.</p> <p>Containers are deployed in two ways: either by creating an image to run in a container or by downloading a pre-created image, such as from Docker Hub. Although Docker is by far the largest and most popular container platform, there are alternatives. However, Docker has become synonymous with containerization. Originally built on LXC, Docker has become the predominant force in the world of containers.</p>					
--	--	--	--	--	--



---

**Part – C ( 2 x 10 = 20 Marks)**

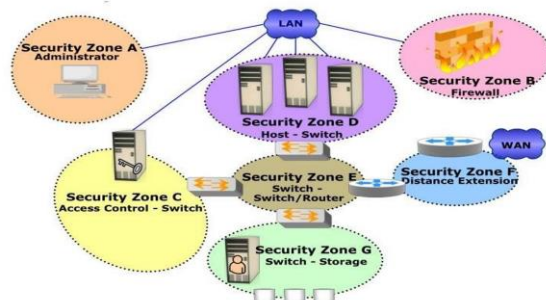
## Answer All the Questions

15	a. <b>Explain the process of security implementation in SAN.</b>
----	--

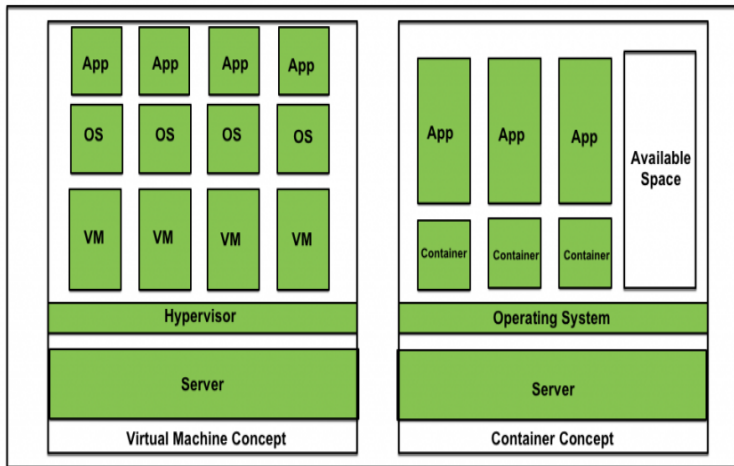
Storage networking environments are a potential target for unauthorized access, theft, and misuse because of the vastness and complexity of these environments. Therefore, security strategies are based on the defense in depth concept, which recommends multiple integrated layers of security. This ensures that the failure of one security control will not compromise the assets under protection. Figure illustrates various levels (zones) of a storage networking environment that must be secured and the security measures that can be deployed.

FC SANs not only suffer from certain risks and vulnerabilities that are unique, but also share common security problems associated with physical security and remote administrative access. In addition to implementing SAN-specific security measures, organizations must simultaneously leverage other security implementations in the enterprise. For example, two-factor authentication is implemented widely; in a simple implementation it requires the use of a username/password and an additional security component such as a smart card for authentication.

## LUN masking and zoning



OR					
<p><b>b. Elaborate how containers are built on virtualization technique and How they offer an alternative to virtual machines.</b></p> <p>To answer how containers enable virtualization let us discuss in detail what is virtualization and how containers come into play with this concept.</p> <p>Virtualization is a technique, which essentially creates an illusion of a resource such as a desktop, storage, network or an operating system. Devices, applications and human users possess the capability of interacting with these resources. This illusion also called virtualization expands the capabilities of traditional systems, which are limited by their own physical resources.</p> <p>Now, containers enable this virtualization for applications that are deployed in them. Applications in containers run independently, isolated from any physical resource. Containers virtualize the OS, CPU, memory, storage and network resources there by providing a controlled environment that can be scaled up or down as required. A container also packages the application along with its dependencies and necessary files, which enables the application to be deployed on any environment without having to configure the server, hardware or software</p> <p>This still sounds similar to virtualization implemented through virtual machines right? So before we get into what more containers can do let us clear up how containers differ from virtual machines</p> <p>A virtual machine is a form of hardware virtualization. The hardware is logically separated from the other resources. The hardware can be any system such as a desktop (with hardware and its own OS) called the host machine, on which several virtual machines or guest machines can run, each with their own separate operating systems. This is made possible by a firmware called the hypervisor.</p>	10	L3	4	2	2.5.2



16	<p><b>a. Sketch the any ten tools of cloud computing</b></p> <p><b>1. Cloudwatch</b></p> <p>The amazon web services are one of the best cloud computing management systems that allow cloud resources and applications running under the amazon services, enabling you to track and view instances. It gives you a brief insight into the overall health and performance of the system. This system can be used in a great way to optimize operations. The best part of cloud services is that you do not need to install any kind of software or invest in heavy installation services. This is the most fantastic thing about the multi-cloud management strategies. All the security services are provided by amazon itself in any kind of mess or when things go wrong.</p> <p><b>2. Cloud Monitoring Tool</b></p> <p>The famous Microsoft cloud monitoring tool, which runs on Azure, is one of the virtualization tools in cloud computing, which monitors your workload. It gives you great insights into your workload to monitor and analyze logs and identifies security threats. The main advantage of the cloud monitoring tool here is that it is easy to set up and transparent. It provides complete access to the performance and health of the applications with infrastructure and workloads. The main similarity in these cloud monitoring tools is that you do not need any extra software installation with any additional costs incurred.</p> <p><b>3. Infrastructure Manager</b></p> <p>The DX infrastructure manager is a great management platform in the cloud computing platforms list. It helps deliver intelligent analytics for infrastructure monitoring. It is a fantastic tool that is quite proactive in solving troubleshooting issues that might affect the loud infrastructure's performance. Without a doubt, this is a</p>	10	L2	6	4	2.7.1
----	---	----	----	---	---	-------



great tool that manages storage services, networks, and servers, etc. It depicts specific distinct patterns or analytics by mapping out the latest trends, simplifying the troubleshooting process, and reporting various activities. It is a user-friendly platform with customizable dashboards to enhance visualization. It monitors every aspect of the cloud eco-system. It also features turning the DX IM into a useful incident management tool that improves monitoring capabilities.

## 4. AppDynamics

AppDynamics, acquired by cisco in 2017, is one of the excellent cloud development tools which provides a cloud-based monitoring system for accelerating application performance. It allows the users to learn the real state of the cloud applications and help with business operational and coding levels. This is quite an environmentally adaptable system with magnificent capabilities. This tool is quite useful in cloud performance monitoring.

## 5. Relic

The New Relic is one of the cloud computing software tools which is quite efficient in managing complex and ever-changing applications. It helps the servers running real-time and also gives an insight into the issues and resolves them quickly. It also allows you to scale your operations with the usage. It considers various processes and optimization of the apps, whether it is either mobile or web-based applications. It helps to place all the data in one place in the dashboard, which gives you a clear picture of every part of the cloud. These are many top-notch companies using this cloud structure.

## 6. True Sight Pulse

The BMC true sight pulse is again one of the cloud-based monitoring tools that helps you to boost performance and manage operations along with cost management structure. It gives you an end-user performance experience to detect problems and monitor resources. It provides a fair chance to develop cloud operations management tools. It also allows you to control costs, optimize, and manage the right resources at cost-effective prices. It helps to breakdown the cost, which businesses can later use and invest in business needs.

## 7. Solar Winds

This cloud computing monitoring tool provides cloud monitoring services and networking and database solutions. This cloud management platform allows you to monitor applications, servers, and virtual machines' performance and health. It is encrypted with the infrastructure management tool, which can monitor cloud environments.

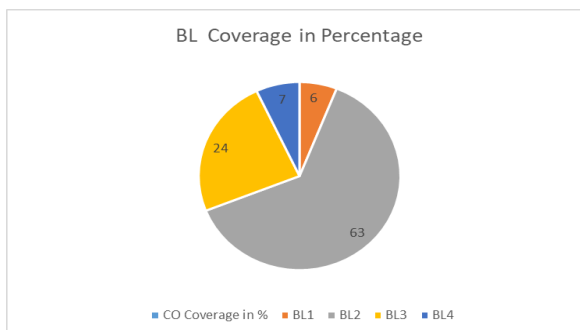
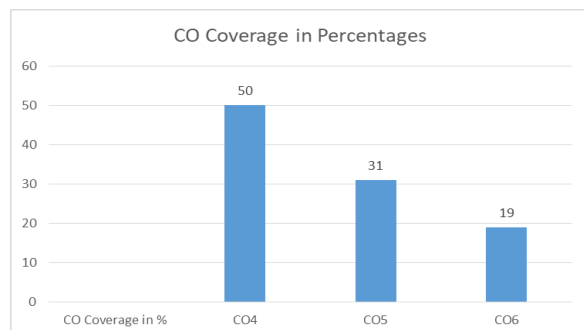


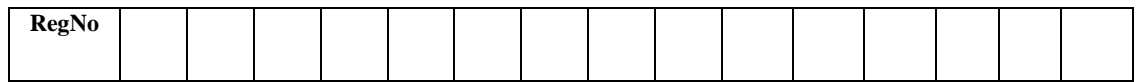
<p><b>8. Retrace</b> It is again one of the cloud-based tools designed for developers and designers helping with code and design development. This is considered top in the cloud computing tools list. It helps in tracking execution and ensure the developers to create advanced coding at all times. The idea is to make the developers more productive with fewer complications and make the developer and designer much more manageable with much faster work. It fits small and medium businesses with an affordable price range.</p> <p><b>9. Exoprice</b> The SaaS monitoring tool or service offers you security and optimization of the services, enabling the cloud app up and running. These tool applications such as dropbox, salesforce, etc., watch and manage all the tools with troubleshooting and fixing problems that can directly or indirectly impact your business—the central business and company platforms such as Starbucks, PayPal, and P&amp;G.</p> <p><b>10. Sematext</b> It is again one of the useful cloud computing tools which collectively manages performance and solutions available in the cloud and on-premises. It enables the users to efficiently diagnose and solve performance issues and the latest trends for an ultimate user experience.</p> <p><b>11. Aternity</b> This cloud is specially designed for the end-user experience. It ranks in the virtual screen system with the mobile end-user experience. Various tests are performed to manage such a system and look into the proper functionality. It detects the page loading time along with any traffic problems. It also optimizes user interaction. It offers an extensive list of tools that enhance the user experience in the most effective way.</p>					
OR					
<p><b>b. Develop a checklist for auditing the security of a storage environment with SAN, NAS, and iSCSI implementations. Explain how you will perform the audit. Assume that you discover at least five security loopholes during the audit process. List them and provide control mechanisms that should be implemented to eliminate them.</b></p> <p>SAN, NAS, iSCSI Servers (Production, management, backup, third party, NAS)</p> <ul style="list-style-type: none"> <li>○ What data or object was accessed /attempted to access?</li> <li>○ What action was performed?</li> <li>○ When was executed?</li> </ul>	10	L3	4	2	2.5.2

	<ul style="list-style-type: none"> <li>○ Who authorized and performed the action?</li> <li>○ NFS/CIFS access (shared files)</li> <li>● Fabric/ IP network <ul style="list-style-type: none"> <li>○ Physical and logical access</li> </ul> </li> <li>● Switches <ul style="list-style-type: none"> <li>○ Physical and logical access</li> <li>○ Zoning</li> </ul> </li> <li>● Storage <ul style="list-style-type: none"> <li>○ Which volume was accessed /attempted to access?</li> <li>○ What action was performed?</li> <li>○ When was executed?</li> <li>○ Who authorized and performed the action?</li> <li>○ LUN masking</li> <li>○ Provisioning</li> <li>○ Upgrade/replacement</li> <li>○ Handling of physical media</li> </ul> </li> </ul> <p>Process</p> <ul style="list-style-type: none"> <li>Collect log and correlate</li> <li>● Analyze access and change control <ul style="list-style-type: none"> <li>○ Production and DR site</li> <li>○ Backup and replication</li> <li>○ Third party service</li> </ul> </li> <li>● Check alerting mechanism</li> <li>● Check security controls <ul style="list-style-type: none"> <li>○ Physical</li> <li>○ Administrative</li> <li>○ Technological</li> </ul> </li> <li>● Identify security gap</li> </ul> <p>Five security loopholes</p> <ol style="list-style-type: none"> <li>1. Authentication allows multiple login</li> <li>2. No firewall</li> <li>3. No authentication at the switch level</li> <li>4. No encryption for in-flight data</li> <li>5. Poor physical security at the data center</li> </ol> <p>Control</p> <p>Restriction in number of login attempt, two part password</p> <ol style="list-style-type: none"> <li>1. Implement firewall to block inappropriate or dangerous traffic</li> <li>2. Authenticate users/administrators of FC switches using RADIUS (Remote Authentication Dial In User Service), DH-CHAP (Diffie-Hellman Challenge Handshake Authentication Protocol), etc.</li> <li>3. Encrypting the traffic in transit</li> <li>4. Increase security manpower and implement biometric security</li> </ol>					
--	---	--	--	--	--	--

RegNo															
-------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

**\*Program Indicators are available separately for Computer Science and Engineering in AICTE examination reforms policy.**  
**Course Outcome (CO) and Bloom's level (BL) Coverage in Questions**





Q. No	Question	Mark	BL	CO	PO	PI Code
1	How many types of security domains are there? a. 2 <b>b. 3</b> c. 4    d. 5	1	L2	4	4	1.7.1
2	What is ACL? <b>a. Access Control list</b> b. Accountability Control List c. Access confidentiality list b. Access Control Layer	1	L3	4	4	2.5.2
3	_____ is the feature of cloud computing that allows the service to change in size or volume in order to meet a user's needs. a. <b>Scalability</b> c. Virtualization b. Security                          d. Cost-savings	1	L2	5	4	2.5.2
4	Which of the following is the most refined and restrictive cloud service model? a. SaaS                                  c. IaaS b. <b>PaaS</b> d. CaaS	1	L2	5	4	2.5.2
5	Which of the following is the most common way to approach the problem of interoperability by vendors? a. Cloud Maintances b. create scalable websites for different devices c. create reliable websites for different devices <b>d. create individual sites within a Web site for different devices</b>	1	L2	5	4	1.7.1
6	An application that provides for transaction overflow in a reservation system is an example of _____ a. <b>Cloud Bursting</b> c. Cloud Prevising b. Cloud Services                      d. Cloud Orchestrate	1	L2	6	2	1.7.1
7	The major storage infrastructure components that should be managed are a. <b>Storage Arrays</b> c. Redundant Fabrics b. Multipathing software              d. RAID sets	1	L2	4	1	5.4.1

8	<p><b>Logical Unit Number masking prevents data corruption on the storage array by restricting host access to a defined set of logical devices</b></p> <p>a. Data security                      c. Data redundancy b. Data deduplication              d. <b>Data corruption</b></p>	1	L2	5	4	2.5.2
9	<p>Which of the following is not a cloud infrastructure mechanisms?</p> <p>a. Logical Network Perimeter      c. Cloud Usage Monitor b. <b>Flexible scaling</b>                      d. Virtual server</p>	1	L2	5	4	2.5.2
10	<p>Cloud consumers that install or lease virtual servers can customize their environments independently from other cloud consumers that may be using _____hosted by the same underlying physical server.</p> <p>a. Ready-Made Environment      c. Cloud Storage Device b. <b>Virtual servers</b>                      d. Resource Replication</p>	1	L1	4	2	2.5.2

**Part – B ( 4 x 5 = 20 Marks)**

## Answer All the Questions

11	<p><b>Brief about Risk Triad</b></p> <p><b>Risk Triad</b></p> <ul style="list-style-type: none"> <li>Defines risk in terms of threats, assets, and vulnerabilities</li> </ul> <p>EMC Proven Professional Copyright © 2012 EMC Corporation. All Rights Reserved . Module 14: Securing the Storage Infrastructure 6</p>	5	L3	4	2	2.5.2
12	<p><b>Brief about vulnerable factors in storage security</b></p> <p>Paths that provide access to information are vulnerable to potential attacks</p> <p>Requires implementation of “defense in depth”</p> <p>Factors to consider when assessing the extent to which an environment is vulnerable:</p> <ul style="list-style-type: none"> <li>Attack surface</li> <li>Attack vectors</li> <li>Work factor</li> </ul> <p>Managing vulnerabilities</p> <ul style="list-style-type: none"> <li>Minimize the attack surface and maximize the work factor</li> <li>Install controls (or countermeasures)</li> </ul>	5	L3	4	2	2.5.2
13	<p><b>Enumerate the characteristics and benefits of cloud computing.</b></p>	5	L3	6	4	2.7.1

RegNo															

14	<p><b>A performance problem has been reported on a database. Monitoring confirms that at 12:00 a.m., a problem surfaced, and access to the database is severely affected until 3:00 p.m. every day. This time slot is critical for business operations and an investigation has been launched. A reporting process that starts at 12:00 p.m. contends for database resources and constrains the environment. What monitoring and management procedures, tools, and alerts would you establish to ensure accessibility, capacity, performance, and security in this environment</b></p> <p>Monitoring:</p> <ul style="list-style-type: none"> <li>• Setting up monitoring and reporting for accessibility, capacity, performance and security on production and replication data</li> <li>• Monitoring and management tools such as ECC Performance manager need to be deploy to gather all performance statistics data (historical data)</li> <li>• Performance analysis – performance constraint is because of the resource</li> </ul> <p>Management:</p> <ul style="list-style-type: none"> <li>• Requirement: Database need to be replicate for reporting process Based on requirement and infrastructure chosen replication software need to be deploy</li> <li>• Provision storage capacity for replication</li> <li>• Configure the environment for accessing replicated data (need configuration at host, network and storage)</li> <li>• Configure adequate capacity based on policy on data retention and change</li> <li>• Configure security for replicated data</li> </ul>	5	L4	4	4	1.7.1
----	--	---	----	---	---	-------

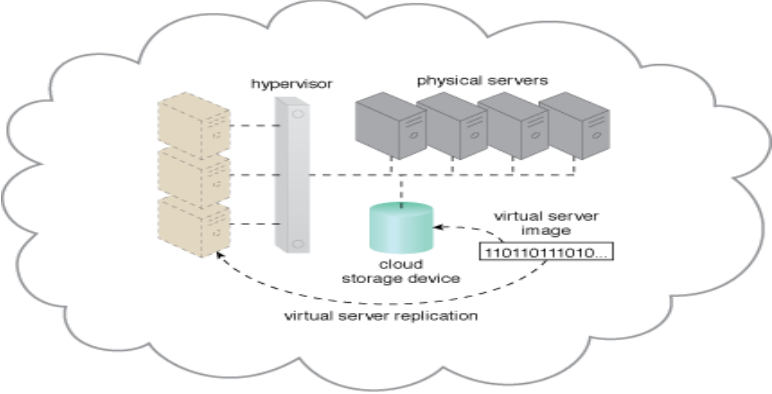
**• Part – C ( 2 x 10 = 20 Marks)**

**• Answer All the Questions**

15	<p><b>a. List out and explain the management tasks in a storage infrastructure.</b></p> <p>All the management tasks in a storage infrastructure can be broadly categorized into,</p> <ul style="list-style-type: none"> <li>– availability management</li> <li>– capacity management</li> <li>– performance management</li> <li>– security management</li> <li>– reporting</li> </ul> <p>• The major storage infrastructure components that should be managed are</p> <ul style="list-style-type: none"> <li>– Servers, databases and applications</li> <li>– Network ((SAN) and IP Networks (switches, routers, bridges))</li> <li>– Storage Arrays</li> </ul>	10	L2	6	4	2.7.1
----	---	----	----	---	---	-------

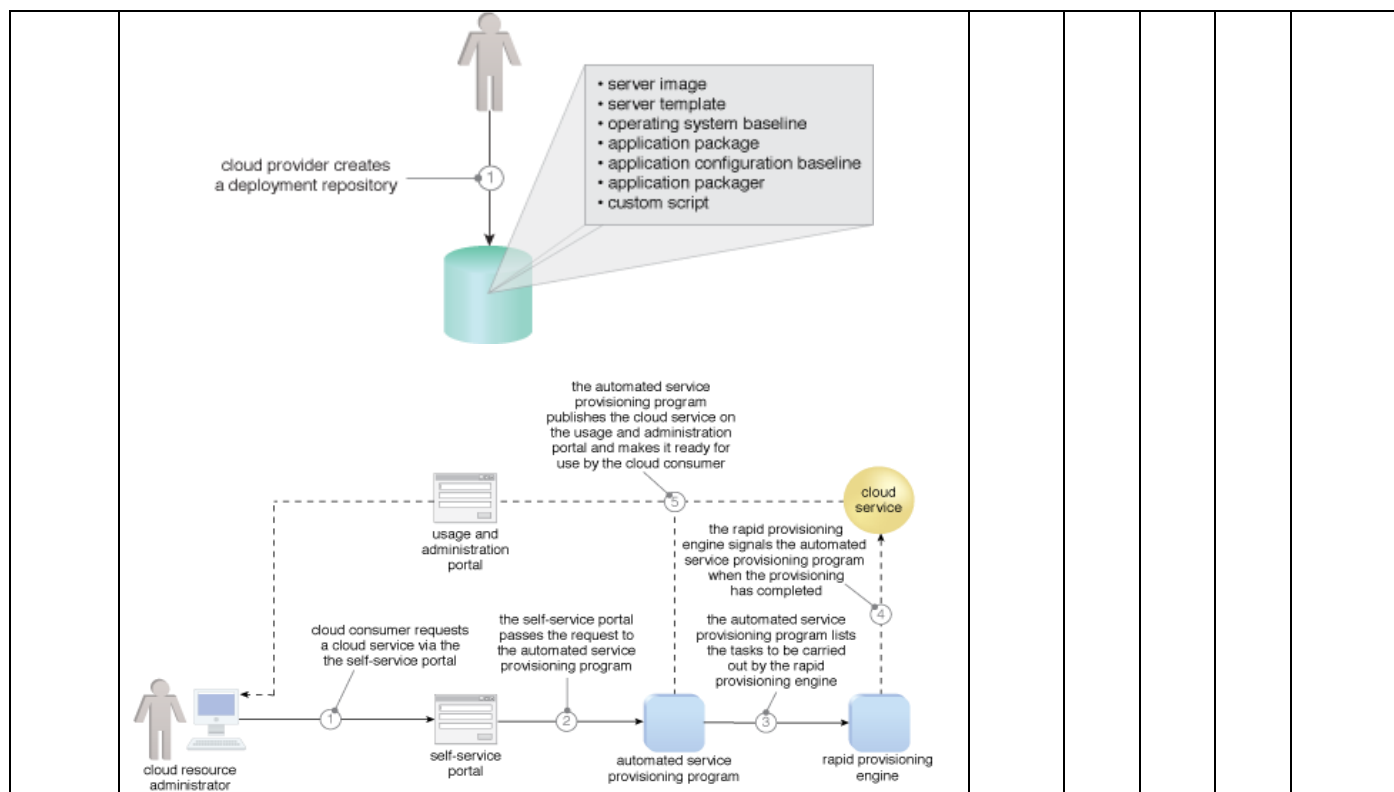
**OR**

RegNo															

	<p><b>b. Outline the cloud service models and also analyse the benefits of cloud computing.</b></p> <p>Cloud Service Models</p> <p>According to NIST, cloud service offerings are classified primarily into three models:</p> <ol style="list-style-type: none"> <li>1. Infrastructure-as-a-Service (IaaS)</li> <li>2. Platform-as-a-Service (PaaS)</li> <li>3. Software-as-a-Service (SaaS)</li> </ol>	10	L3	6	4	2.7.1
16	<p><b>a. List out the cloud infrastructure mechanisms, explain any three of the mechanisms in detail.</b></p> <p>Cloud infrastructure mechanisms</p> <p>Cloud infrastructure mechanisms are foundational building blocks of cloud environments that establish primary artefacts to form the basis of fundamental cloud technology architecture</p> <p><b>Cloud infrastructure mechanisms are,</b></p> <ol style="list-style-type: none"> <li>1. Logical Network Perimeter</li> <li>2. Virtual Server</li> <li>3. Cloud Storage Device</li> <li>4. Cloud Usage Monitor</li> <li>5. Resource Replication</li> <li>6. Ready-Made Environment</li> </ol>	10	L2	5	2	2.5.2
OR						
	<p><b>b. Illustrate the working model of Resource replication in cloud environment.</b></p> <p>Resource replication is defined as the creation of multiple instances of the same IT resource, and is typically performed when an IT resource's availability and performance need to be enhanced. Virtualization technology is used to implement the resource replication mechanism to replicate cloud-based IT resources (Fig 1).</p> <p>The resource replication mechanism is commonly implemented as a hypervisor. For example, the virtualization platform's hypervisor can access a virtual server image to create several instances, or to deploy and replicate ready-made environments and entire applications.</p> 	10	L4	6	4	2.7.1



RegNo																				



**\*Program Indicators are available separately for Computer Science and Engineering in AICTE examination reforms policy.**

**Course Outcome (CO) and Bloom's level (BL) Coverage in Questions**

