

**Server & Cloud Security**

## School of InfoComm Technology

Diploma in Information Security and Forensics

Diploma in Information Technology

**Practice Paper**

(Marking Scheme)

Date:

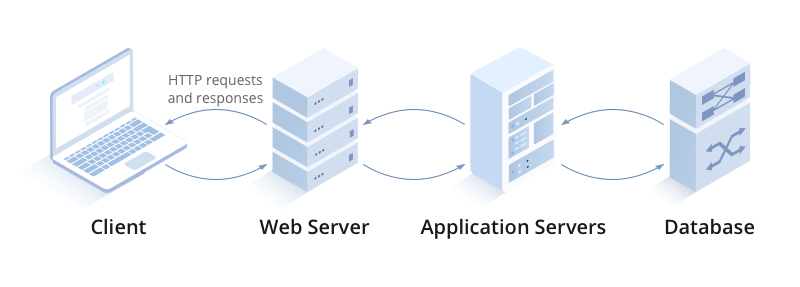
Time:

INSTRUCTIONS TO CANDIDATES:

1. Write your Student Number, Name, Module Group and Seat Number CLEARLY in the boxes provided above.
2. This paper consists of 9 pages including this cover page. Check carefully to make sure your set is complete.
3. There are FIVE questions. Answer **ALL** questions.
4. Write your answers in the blank space provided for each question in this paper.

|  |  |
| --- | --- |
| **GRADE** |  |

* 1. Explain the various server roles in a 3-tier client-server architecture.



|  |
| --- |
| * Web servers are used to provide access to information to users connecting to the server using a web browser, which is the client part of the application. * An application server is one that users connect to and then run their applications on. In many cases this server is the middle tier in a three-tier architecture that accepts users’ requests to its application and then communicates with a database server where content is stored. * A database server is one that runs database software such as SQL Server or Oracle. It contains information stored in the database and users can search the database, either directly by issuing commands or by using an application that does this through a GUI. |

* 1. With the aid of a well-labelled diagram, explain how a SYN flood attack exploits the TCP connection.

|  |
| --- |
| TCP Three-way handshake diagram  In a normal TCP connection:   * First, the client sends a SYN packet to the server in order to initiate the connection. * The server then responds to that initial packet with a SYN/ACK packet, in order to acknowledge the communication. * Finally, the client returns an ACK packet to acknowledge the receipt of the packet from the server. After completing this sequence of packet sending and receiving, the TCP connection is open and able to send and receive data.   SYN flood DDoS attack animation  In a SYN flood:   * an attacker exploits the fact that after an initial SYN packet has been received, the server will respond back with one or more SYN/ACK packets and wait for the final step in the handshake. * When a server is leaving a connection open but the machine on the other side of the connection is not, the connection is considered half-open. * In this type of DoS attack, the targeted server is continuously leaving open connections and waiting for each connection to timeout before the ports become available again. |

* 1. Briefly explain what is disaster recovery and list THREE examples of disaster.

|  |
| --- |
| A disaster is an unexpected problem resulting in a slowdown, interruption, or network outage in an IT system. Outages come in many forms, including the following examples:   * An earthquake or fire * Technology failures * System incompatibilities * Simple human error * Cyber attacks such as malware, DDoS and ransomware attacks |

* 1. The following steps were recommended to secure a server:
* Server hardening
* Secure the server network
* Manage Privileged Identities

1. For each of the recommended steps, list ONE reason why it should be performed.

|  |
| --- |
| * Server hardening   Server hardening is an inexpensive and simple task to improve the overall operating system for maximum performance and to reduce failures. Hardening: In computing, hardening is usually the process of securing a system by reducing its surface of vulnerability. A hardened system is configured and updated to protect against attacks   * Secure the Server Network   Securing the server network is to prevent the common network security threats.   * Manage Privileged Identities   Manage Privileged Identities enables you to limit standing administrator access to privileged roles, discover who has access, and review privileged access. |

1. Describe TWO measures you would implement for each of the recommended steps.

|  |
| --- |
| * Server hardening   - Implementing EFS  - Malware Protection   * Secure the Server Network   - Implementing Windows firewall  - Implementing IPSec   * Manage Privileged Identities   - Implementing Password policies  - Implementing Account lockout policies |

* 1. Company XYZ would like to have a cloud solution with a selection of OSs provisioned for exclusive use. Identify the cloud deployment model and cloud service model best suited for Company XYZ. Explain your answer.

|  |
| --- |
| * Deployment model: Private cloud.   Private cloud is exclusive used by a single organization.   * Service model: PaaS   PaaS contains everything included in IaaS, with the addition of OSs. The cloud vendor usually offers a selection of OSs, so that the customer can use any or all of the available choices. |

* 1. Discuss the shared responsibility models for IaaS, PaaS and SaaS.

|  |
| --- |
| * In IaaS service model, the service provider will be responsible for all **cloud infrastructure up to the hypervisor level.** The customer is responsible for the VM and higher. * The security demarcation for PaaS is that the cloud provider assumes responsibility for security up to the operating system, and the c**ustomer manages the application and operating system** configuration. * The Software as a Service model is where the customer of the service accesses application software that is owned and controlled by the cloud company, which has complete responsibility for the management and support of the application. |

* 1. Discuss the differences between IAM users and roles.

|  |
| --- |
| * An IAM role is very similar to an IAM user, in that it is an identity with permission policies that determine what the identity can and cannot do in AWS. However, a role does not have any credentials (password or access keys) associated with it. Instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. * When you use IAM roles, you don’t need to grant long-term security credentials to each entity that requires access to a resource. An IAM user can assume a role to temporarily take on different permissions for a specific task. |

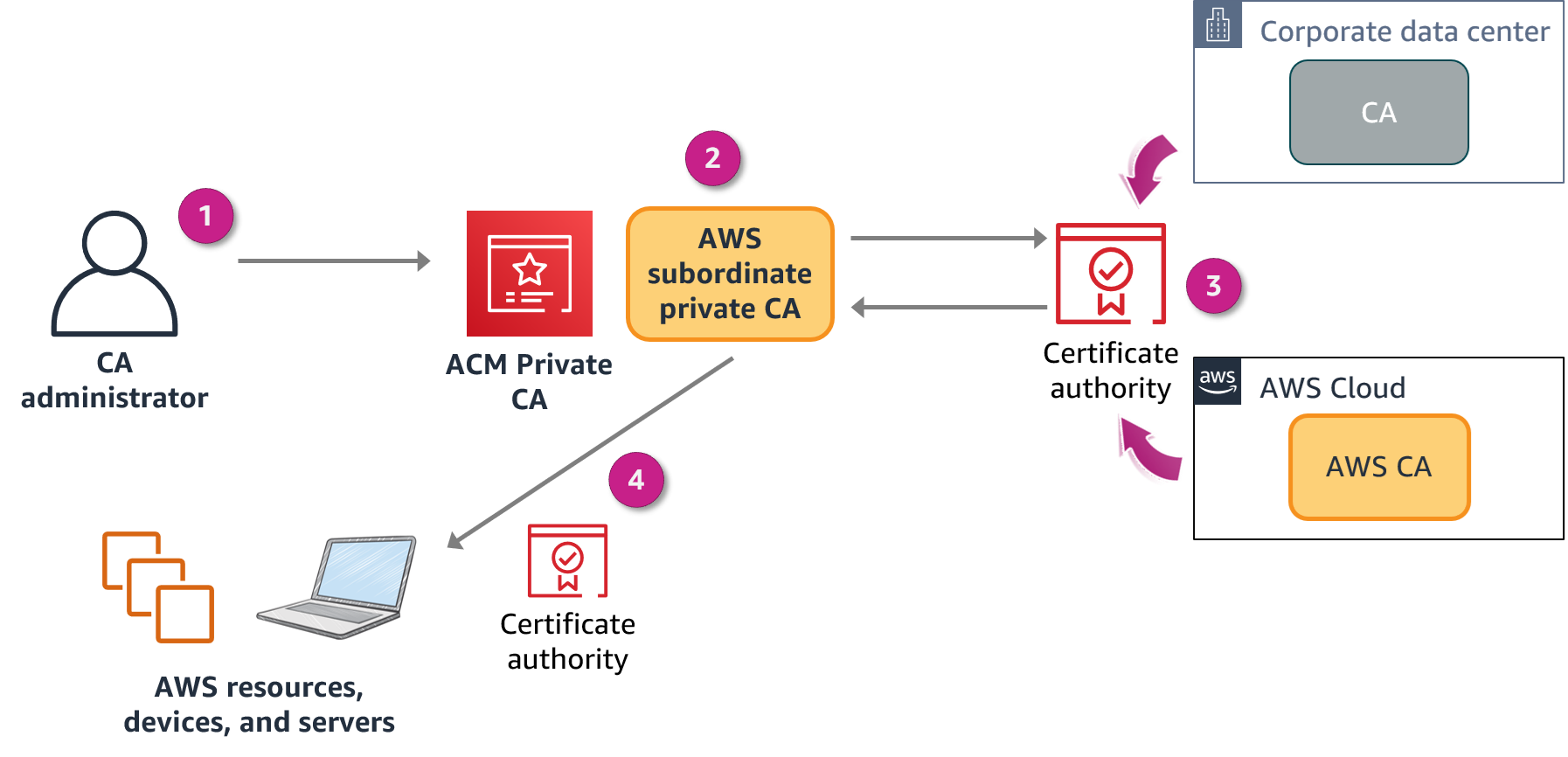
* 1. Briefly explain the differences between identity-based and resource-based policies in AWS IAM.

|  |
| --- |
| * Identity-based policies are attached to an IAM user, group, or role. They indicate what that identity can do. * Resource-based policies are attached to a resource. They indicate what a specified user (or group of users) is permitted to do with the resource. |

* 1. Briefly explain the how the encryption keys are managed for the following ways of cloud data encryption:
* Client-side Encryption (CSE)
* SSE with customer-provided keys (SSE-C)
* SSE with Amazon S3 managed keys (SSE-S3)
* SSE with AWS KMS keys (SSE-KMS)

|  |
| --- |
| * With client-side encryption (CSE), your applications encrypt data locally before submitting it to AWS and decrypt data after receiving it from AWS. You create and manage your own encryption keys. Data is stored in an encrypted form, with keys and algorithms known only to you. * With server-side encryption with customer-provided keys (SSE-C), you manage the encryption keys. * When you use server-side encryption with Amazon S3 managed keys (SSE-S3), each object is encrypted with a unique key. * Server-side encryption with AWS KMS keys (SSE-KMS) is similar to SSE-S3, there are separate permissions for the use of a KMS key that provide added protection against unauthorized access of your objects in Amazon S3. |

* 1. Explain with reference to the below diagram on how AWS Certificate Manager helps to manage the digital certificate of the cloud consumer.



|  |
| --- |
| * The CA administrator creates a subordinate CA to issue certificates. * The subordinate CA sends the certificate to be signed. * The on-premises CA or AWS CA signs the certificate. * ACM Private CA issues the signed certificate to resources. |

* 1. Briefly explain the two focus areas of a matured security operations.

|  |
| --- |
| * Reactively respond to attacks detected by tools. * Proactively hunt for attacks that slipped past reactive detections. |

* 1. Explain the TWO differences between AWS CloudTrail and CloudWatch.

|  |  |
| --- | --- |
| **AWS CloudTrail** | **Amazon CloudWatch** |
| Continuously monitors and logs user activities | Continuously monitors resource and application performance |
| Useful for compliance auditing, security analysis, and troubleshooting | Useful for detecting anomalous service behavior, setting alarms, and discovering insights |

* 1. Briefly explain the two phases of incident response in AWS cloud operations.

|  |
| --- |
| * Phase 1: Discovery and recognition   + Incident identification, logging, and categorization   + Incident notification and escalation   + Investigation and diagnosis * Phase 2: Resolution and recovery   + Forensic isolation (if software, reproduce the bug)   + Stage a fix   + Deploy the fix   + Incident closure |

\*\* END OF PAPER \*\*