0x09-web_infrastructure_design

Task2 explanations:

I. **Infrastructure Components:**

1. **Server 1 (Primary Web Server):**
   Hosts website's static content (HTML, CSS, JavaScript).
2. **Server 2 (Replica Web Server):**
   A replica of the primary web server, hosting identical static content.
3. **Server 3 (Database Server):**
   Dedicated server for the MySQL database, separates database and web server functions for security and performance.
4. **Web Server (Nginx):**
   Handles user requests and serves web pages.
5. **Application Server:**
   Manages dynamic content, interacts with the database.
6. **Load Balancer (HAproxy):**
   Distributes user requests evenly between primary and replica web servers for performance and redundancy.
7. **Firewalls:**
   Added for security, to control incoming and outgoing traffic, preventing unauthorized access.
8. **SSL Certificate (HTTPS):**
   Encrypts traffic between the user's browser and the web server, ensuring data privacy and security.
9. **Monitoring Clients (Data Collectors):**
   Used to collect performance and system health data for monitoring and analysis.

II. **Additional Elements Explained:**

- **Firewalls:** Added for security to control and monitor traffic, preventing unauthorized access to the servers.
- **HTTPS (SSL Certificate):** Encrypts data in transit, protecting user information from eavesdropping.
- **Monitoring:** Used to track system performance, identify issues, and ensure uptime.
- **Monitoring Tool (Data Collector):** Collects data, like server metrics and logs, for analysis and alerts.

III. **Why Firewalls:**

- Firewalls control and secure traffic, protecting the infrastructure from unauthorized access and cyber threats.

IV. **Why HTTPS (SSL Certificate):**

- HTTPS encrypts data, ensuring user privacy and protecting sensitive information during transmission.

V. **Why Monitoring:**

- Monitoring helps detect and address issues proactively, ensuring the website runs smoothly.

VI. **Monitoring Data Collection:**

- Monitoring clients (data collectors) gather data on server performance, traffic, and other metrics.

VII. **Monitoring Web Server QPS:**

- To monitor web server Query Per Second (QPS), set up monitoring tools to track incoming requests and server response times. If QPS exceeds predefined thresholds, the system can trigger alerts.

VIII. **Issues with this Infrastructure:**

- **Terminating SSL at Load Balancer Level:**
    - This could be an issue because SSL termination at the load balancer means data is decrypted there. If not handled securely, it can expose sensitive information.
- **Single MySQL Server for Writes:**
    - Having only one MySQL server capable of accepting writes is risky because it creates a single point of failure. If it fails, the website loses its ability to update data.
- **Identical Server Components:**
    - Using identical components on all servers may lead to inefficiencies or security risks as different server functions have different resource requirements and security needs.