ALX Web infrastructure design

TASK 2-secured_and_monitored_web_infrastructure

Infrastructure Design:

1. **Server 1 (Web Server)**:
   - Web Server (Nginx)
   - Application Server
   - Application Files (Codebase)
2. **Server 2 (Web Server)**:
   - Web Server (Nginx)
   - Application Server
   - Application Files (Codebase)
3. **Server 3 (Database Server)**:
   - Database: MySQL (Primary-Replica Cluster)
   - Firewall 1 (Protecting the Database)
   - Firewall 2 (Protecting the Web Servers)
4. **Load Balancer**:
   - Distributes traffic between Web Servers
   - SSL Termination (Terminates SSL and decrypts traffic before sending it to web servers)
   - Firewall 3 (Protecting the Load Balancer)
5. **Monitoring Clients**:
   - Collect data for monitoring services (e.g., Sumo Logic)
6. **SSL Certificate**:
   - Enables HTTPS for secure and encrypted data transmission.
7. **User's Computer**:
   - Initiates requests to www.foobar.com.

Specifics and Explanations:

- **Firewalls**:
  - Firewalls are added to enhance security. Firewall 1 protects the database, Firewall 2 protects the web servers, and Firewall 3 protects the load balancer. They control inbound and outbound traffic, ensuring only authorized access.
- **HTTPS**:
  - Traffic is served over HTTPS to encrypt data in transit, ensuring data confidentiality and integrity. This is essential for secure communication, especially when handling sensitive user data.
- **Monitoring**:
  - Monitoring is used to track the health and performance of the infrastructure, helping to identify issues, optimize resources, and detect security threats. Monitoring clients (data collectors) collect and send data to a monitoring service (e.g., Sumo Logic).

- **Data Collection for Monitoring**:
  - Monitoring clients collect various data points, such as server resource usage, response times, error rates, and security events. They send this data to the monitoring service, which provides insights and alerts based on predefined thresholds and patterns.
- **Monitoring Web Server QPS (Queries Per Second)**:
  - To monitor web server QPS, you can set up monitoring to track the number of HTTP requests received by each web server over time. Monitoring tools can generate alerts when QPS exceeds defined thresholds, helping you manage traffic spikes and identify potential issues.

Issues with the Infrastructure:

1. **Terminating SSL at the Load Balancer Level**:
   - Terminating SSL at the load balancer is less secure because, once decrypted, data flows unencrypted within the internal network. To address this issue, you can implement end-to-end encryption by re-encrypting data between the load balancer and web servers.
2. **Single MySQL Server Capable of Accepting Writes**:
   - Having a single MySQL server for writes creates a single point of failure. If this server fails, it can lead to data loss and downtime. To address this, consider implementing a database clustering solution with multiple write-capable nodes for high availability.
3. **Servers with All the Same Components**:
   - Having all servers with the same components can be a problem for scaling and redundancy. Ideally, web servers should be stateless, making it easier to scale horizontally. Separating web, application, and database components allows for more flexibility in scaling and maintenance.