ALX PROJECT

`0x09-web_infrastructure_design`

`2-secured_and_monitored_web_infrastructure`

1. **Load Balancer (LB):**
    - The load balancer distributes incoming traffic across multiple servers to ensure high availability and scalability.
    - Terminating SSL at the load balancer level is an issue because it adds overhead to each request. Ideally, SSL termination should happen at the server level.
    - **Solution:** Use a separate SSL certificate on each server to handle HTTPS traffic directly.
2. **Web Servers (WS1, WS2, WS3):**
    - Web servers host the website content and serve HTTP/HTTPS requests.
    - They handle SSL decryption (if SSL is terminated at the server level).
    - Install the SSL certificate on each web server.
    - Use a web server like Nginx or Apache.
    - Ensure proper security configurations (firewalls, access controls).
3. **Application Servers (AS1, AS2, AS3):**
    - Application servers process dynamic content (e.g., PHP, Python, Node.js).
    - Separate from web servers to improve scalability and security.
    - Use a reverse proxy (e.g., Nginx) to route requests to the appropriate application server.
4. **Database Servers (DB1, DB2, DB3):**
    - MySQL servers for data storage.
    - Having only one MySQL server capable of accepting writes is an issue because it creates a single point of failure.
    - **Solution:** Implement database replication (master-slave or master-master) for redundancy and failover.
5. **Firewalls (FW1, FW2, FW3):**
    - Firewalls protect servers from unauthorized access.
    - Control incoming/outgoing traffic based on rules (allow/deny).
    - Use stateful firewalls to track connections.
    - Block unnecessary ports (e.g., block direct access to MySQL ports from the internet).
6. **Monitoring Clients (MC1, MC2, MC3):**
    - Monitoring tools collect performance data, detect issues, and ensure uptime.
    - Sumologic or other monitoring services can be used.
    - Collect metrics (CPU, memory, disk usage) and logs.
    - Set up alerts for abnormal behavior (e.g., high CPU usage).
    - Monitor QPS (Queries Per Second) by tracking web server logs or using specialized tools.
7. **SSL Certificate:**
    - Serves www.foobar.com over HTTPS.

- Encrypts data in transit.
- Obtain a valid SSL certificate (e.g., Let’s Encrypt) and install it on each web server.

8. **Security Groups and ACLs:**
    - Configure security groups (AWS) or access control lists (ACLs) to restrict network traffic.
    - Allow only necessary ports (HTTP, HTTPS, SSH) and block others.
9. **Backup and Restore Strategy:**
    - Regularly back up databases and website content.
    - Implement automated backups and test restoration procedures.
10. **Scaling Strategy:**
    - Plan for future growth.
    - Add more web/application servers as needed.
    - Use auto-scaling groups (AWS) for dynamic scaling.