ALX Web infrastructure design

2-secured_and_monitored_web_infrastructure

Additional Elements:

- Firewalls:

Why?: Firewalls are added to control incoming and outgoing traffic, providing a security barrier between the servers and the external network. They help prevent unauthorized access and protect against potential security threats.

- SSL Certificate:

Why?: SSL (Secure Sockets Layer) certificates are added to encrypt the traffic between clients and the web server. This ensures the confidentiality and integrity of data in transit, enhancing security.

- Monitoring Clients (Uptime Robot):

Why?: Monitoring tools are added to track the performance, availability, and security of the infrastructure. Uptime Robot, as an example, serves as a data collector for logs and metrics, providing insights into the system's health.

Specifics about the Infrastructure:

- Terminating SSL at the Load Balancer Level:

Issue: Termination at the load balancer level means that traffic between the load balancer and the servers is not encrypted. To address this, SSL termination should occur at the web server level to ensure end-to-end encryption.

- Single MySQL Server Capable of Accepting Writes:

Issue: A single point of failure exists if the MySQL server accepting writes goes down. It should be considered implementing a MySQL cluster with a primary-replica setup for better fault tolerance and scalability.

- Servers with Identical Components:

Issue: Having identical components on all servers might lead to a lack of diversity in the infrastructure. It's advisable to diversify server roles and configurations to avoid a single vulnerability affecting all servers simultaneously.

Explaining Additional Elements:

- Why HTTPS:

HTTPS encrypts data in transit, protecting it from interception and tampering. It's crucial for securing sensitive information such as login credentials and user data.

- Why Firewalls:

Firewalls provide a security barrier, controlling incoming and outgoing traffic based on predetermined security rules. They are essential for safeguarding the servers from unauthorized access and potential threats.

- Why Monitoring:

Monitoring tools track the performance, availability, and security of the infrastructure. They help identify issues, ensure optimal performance, and facilitate proactive management and troubleshooting.

- How Monitoring Collects Data:

Monitoring tools like uptime Robot collect data through log and metric aggregation. They analyze logs and metrics generated by servers, applications, and network devices to provide insights into the system's behavior.

- Monitoring Web Server QPS:

To monitor web server Query Per Second (QPS), set up monitoring tools to collect and analyze relevant metrics. Monitor server resource utilization, response times, and error rates to gauge the server's capacity and performance.

By addressing these issues and incorporating security, encryption, and monitoring, the infrastructure becomes more robust, secure, and capable of providing a reliable service to users.