TASK 2

Definitions and Explanations.

1. **For every additional element, why you are adding it:** The integration of three new elements into the infrastructure serves distinct purposes aimed at bolstering security and enhancing operational efficiency. Firstly, the deployment of individual firewalls for each server fortifies the network perimeter, safeguarding against unauthorized access and potential cyber threats. Secondly, the implementation of an SSL certificate for server www.foobar.com ensures secure data transmission by encrypting traffic over the HTTPS protocol, mitigating the risk of interception and data compromise. Lastly, the incorporation of three monitoring clients facilitates proactive performance monitoring by collecting and transmitting logs to the designated data collector, Sumo Logic, thereby enabling real-time insights into system health and performance metrics.
2. **What are firewalls for:** Firewalls serve as formidable guardians of network security, tasked with monitoring and regulating incoming and outgoing network traffic based on predefined security policies. By establishing a robust barrier between trusted and untrusted networks, firewalls fortify the network perimeter, thwarting unauthorized access attempts and potential cyber intrusions.
3. **Why is the traffic served over HTTPS:** The transition to serving traffic over HTTPS stems from the imperative to enhance data security and privacy. While HTTP transfers data in plain text, rendering it susceptible to interception and eavesdropping, HTTPS encrypts data using Transport Layer Security (TLS), thereby safeguarding sensitive information during transit and bolstering confidentiality and integrity across communication channels.
4. **What monitoring is used for:** Monitoring emerges as a pivotal tool in the arsenal of system administrators, furnishing the capability to proactively detect and diagnose web application performance issues. By continuously monitoring key performance metrics, stakeholders can identify potential bottlenecks or anomalies, enabling timely

interventions to optimize system performance and enhance user experience.

5. **What monitoring is used for:** Monitoring tools harness the power of logs to glean insights into system behavior and performance. By collecting and analyzing logs from diverse sources such as application servers, MySQL databases, and Nginx web servers, monitoring tools generate comprehensive documentation of events relevant to system operation, enabling administrators to pinpoint issues and optimize system performance.
6. **Explain what to do if you want to monitor your web server QPS:** In the pursuit of monitoring web server Query Per Second (QPS) metrics, administrators adopt a multi-faceted approach encompassing network and application-level monitoring. By scrutinizing network traffic patterns and application performance metrics, administrators gain visibility into QPS trends, enabling them to optimize server resources and ensure optimal performance under varying workloads.

Issues with the infrastructure

1. **Explain what to do if you want to monitor your web server QPS:** The decision to terminate SSL encryption at the load balancer level raises concerns regarding resource utilization and CPU overhead. While offloading decryption duties to the load balancer frees up server resources for application tasks, it also introduces performance implications and potential scalability challenges. Further exploration is warranted to comprehensively assess the trade-offs associated with SSL termination.
2. **Explain what to do if you want to monitor your web server QPS:** The reliance on a single MySQL server capable of accepting write operations poses a significant single point of failure. In the event of server downtime, the inability to add or update data compromises the functionality of the application, potentially disrupting critical business operations and user experiences.
3. **Why having servers with all the same components (database, web server and application server) might be a problem:** The uniformity of server components, encompassing databases, web servers, and

application servers, introduces systemic vulnerabilities. Any bugs or vulnerabilities present in one server component are replicated across all servers, amplifying the risk of widespread system compromise and operational disruptions. Diversifying server configurations can mitigate this risk by reducing the likelihood of a systemic failure stemming from a single point of vulnerability.