Task 2 - secured_and_monitored_web_infrastructure

Definitions and Explanations

1.For every additional element, why you are adding it?

We added 3 firewalls one for each server to protect it from being attacked, 1 SSL certificate to serve our server over HTTPS and 3 monitoring for each server to collect data and send it to our data collector (Sumologic).

2.What are firewalls for ?

Firewalls are designed to provide network security by monitoring and controlling incoming and outgoing network traffic, it basically establishes a barrier between a trusted network and an untrusted network.

3.Why is the traffic served over HTTPS?

HTTPS is a secure version of HTTP, the protocol used for transmitting data over the internet. It adds a layer of encryption using SSL/TLS protocols, ensuring that the data exchanged between the client (browser) and the server is encrypted and secure.

4.What monitoring is used for?

Monitoring is used for observation of systems, networks, or applications to gather data, track performance, and identify potential issues.

5.How the monitoring tool is collecting data?

It collects logs of the application server, MySQL database and Nginx web server. A log in computing context is the automatically produced and time-stamped documentation of events relevant to a particular system.

6.Explain what to do if you want to monitor your web server QPS?

A web server may handle an amount of 1000 queries per second, it could be monitored in two levels, either in network or application level.

Issues

1.Why terminating SSL at the load balancer level is an issue?

Terminating SSL at the load balancer level would leave the traffic between the load balancer and the web servers unencrypted.

2.Why having only one MySQL server capable of accepting writes is an issue?

Having one MySQL server is an issue because it is not scalable and can act as a single point of failure for the web infrastructure.

3.Why having servers with all the same components (database, web server and application server) might be a problem?

Having servers with all the same components would make the components contend for resources on the server like CPU, Memory, I/O, etc., which can lead to poor performance and also make it difficult to locate the source of the problem.