0x09. Web infrastructure design

TASK 2 : 2. Secured and monitored web infrastructure

MAIN CONCEPTS:

Additional elements:

In this case I added the third server in order to boost reliability and performance of the web infrastructure, a firewall for each server to protect them from being attacked and exploited, 1 SSL certificate to server www.foobar.com over HTTPS and three monitoring clients that will collect logs and send them to our data collector Sumologic.

Here bellow the Schema of the current case's infrastructure:

- 3 servers
- 3 firewalls
- 1 SSL certificate
- 3 monitoring clients

Firewalls:

A Firewall is a security system to protect an internal network from unauthorized servers and networks based on predefined rules.

The traffic served over HTTPS:

As mentioned in the last task's concepts, HTTPS is safer than HTTP. Clearly, HTTPS is special because of the encryption using TLS (SSL) plus verification. Thus, that's why the traffic was served over HTTPS.

Usage of monitoring:

Provides the capability to detect and diagnose any web application performance issues proactively.

How monitoring collects data:

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

Monitoring Web Server QPS:

Track the query per second (QPS) metric through monitoring tools.

ISSUES:

Terminating SSL at the load balancer level is an issue:

Reason why SSL should terminate at the load balancer level is an issue is because it offers a centralized place to correct SSL attacks such as CRIME or BEAST. In addition to that, decryption at the load balancer can lead data to potential attacks.

Having only one MySQL server capable of accepting writes is an issue:

Literally, once it is down it means do data can be added or updated meaning some features of the application won’t work.

Having servers with all the same components (database, web server and application server) might be a problem:

In fact, once you have a bug in one of the components in one of the servers then the bug will be valid in the other servers.