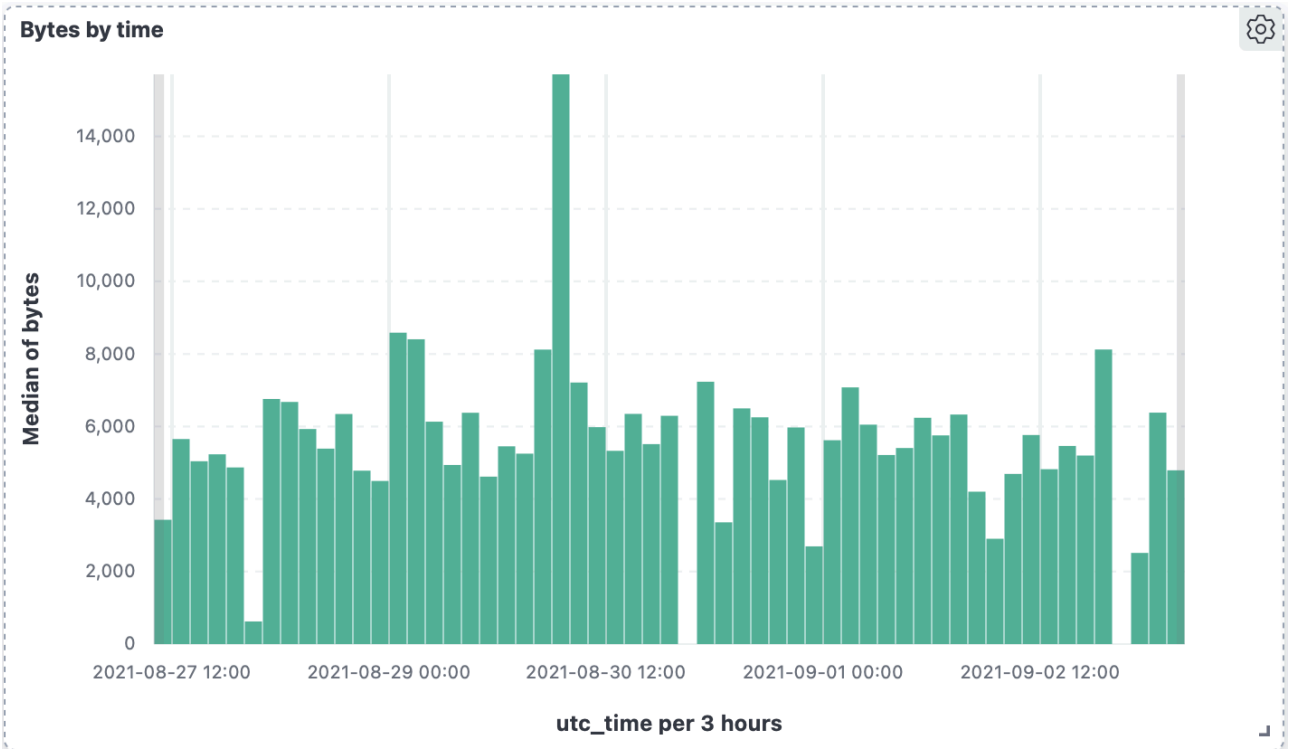
Sprint 19, Tasca 1

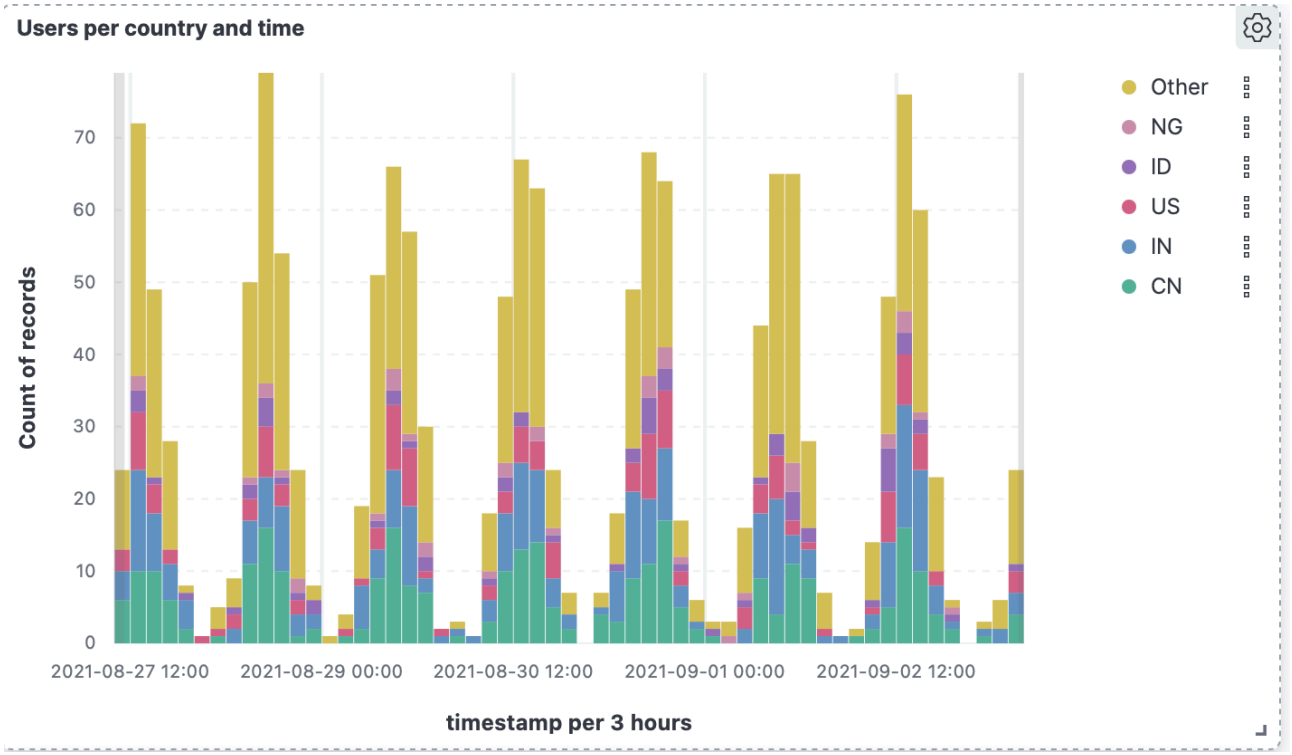
Descarrega't Kibana i mostra algunes gràfiques utilitzant conjunts de dades d'Exemple. Implementa un dashboard que visualitzi interactivament les dades que triïs. Implementa un dashboard que generi gràfics utilitzant cadascun dels diferents tipus de gràfics que ofereix Kibana.

Per aquest exercici, he pres el registre de logs donat per Elasticsearch com a exemple. Al final del document s'adjunten links al dashboard per si fos possible accedir-hi online.

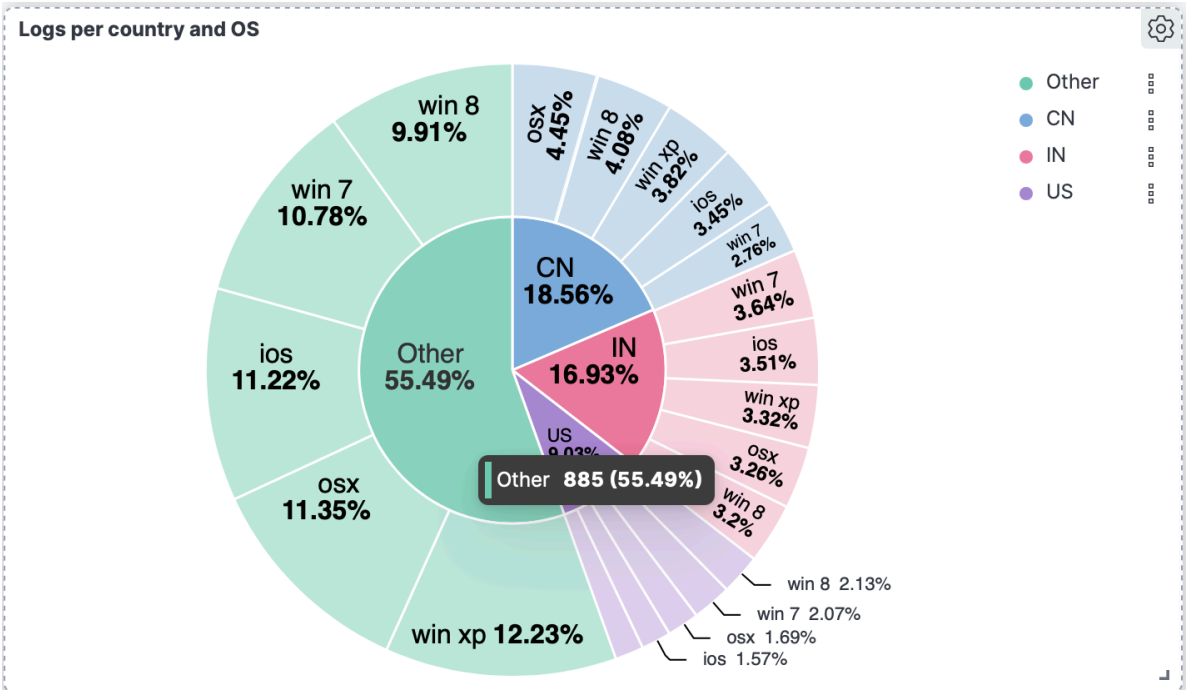
Primer, un gràfic de barres que indica la relació entre demanda en bytes i hora del dia. Noti's que la demanda es manté més o menys estable durant tot el dia a excepció d'una hora on es van demanar més de 15k bytes. Aquests gràfics poden ser molt útils per a detectar atacs de hackers o abusos dels servidors.



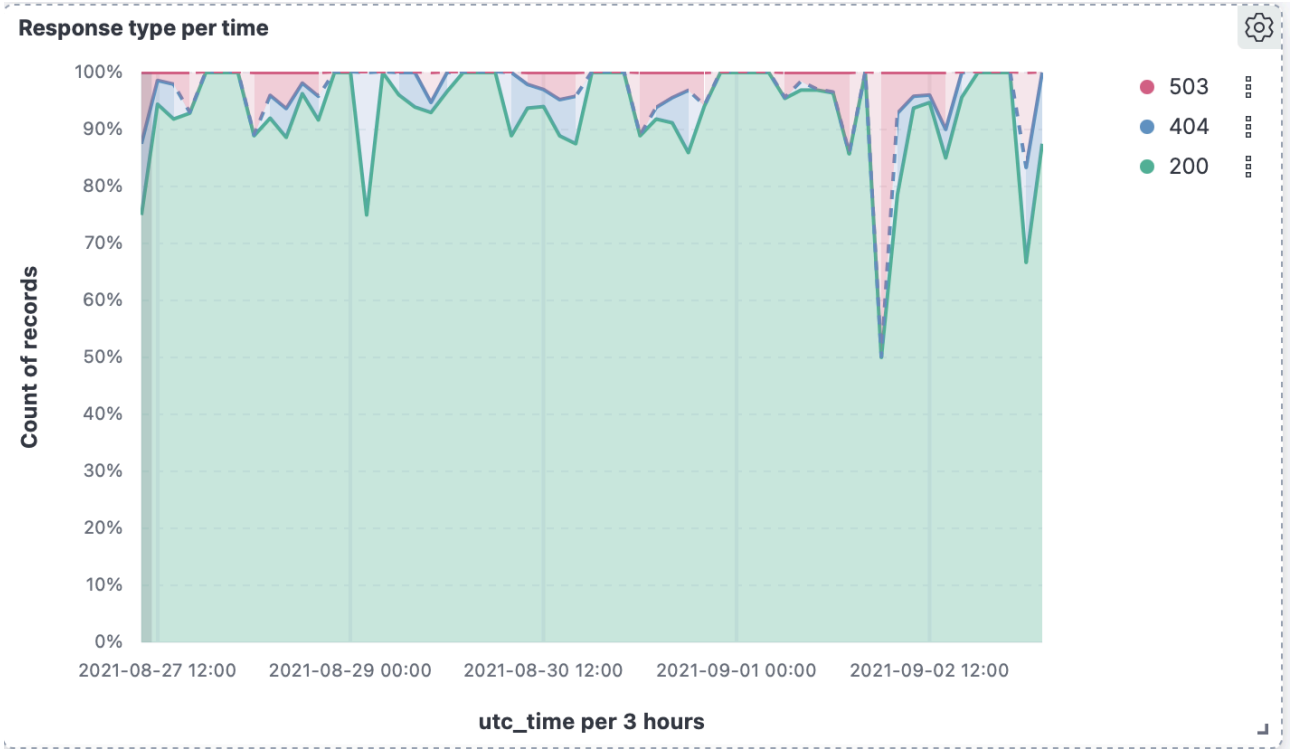
En segon lloc, la relació entre usuaris per hora del dia i països de procedència.



Molt del tràfic procedeix de la Xina o la Índia.



Gràfic de dònut mostrant logs per país i, dintre d'aquests, per sistema operatiu de l'usuari.



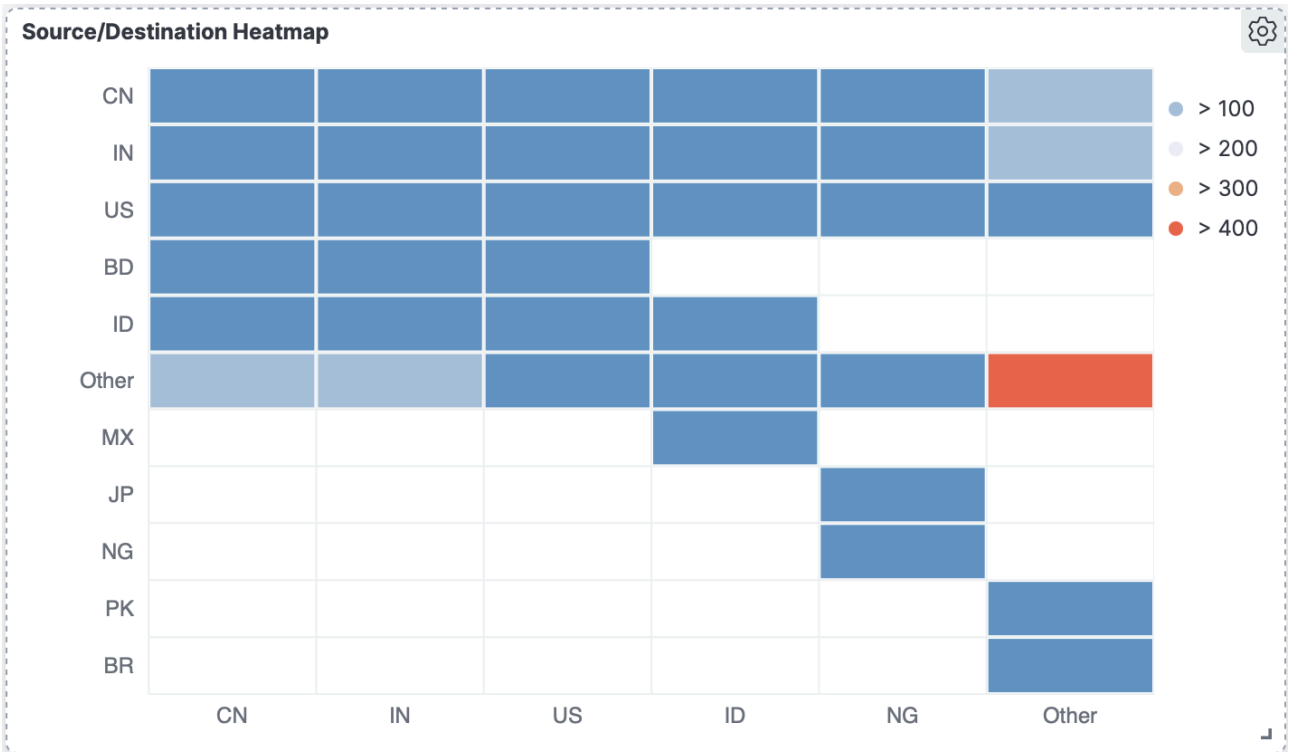
Gràfic d'àrea per tipus de resposta del servidor i temps del dia. Útil per a monitorejar atacs detectats o mal funcionament del servidor.

Taula amb la relació entre sistema operatiu i resposta del servidor. No es detecta cap OS amb més sol·licituts denegades.

Server Response per OS

Top values of response.keyw	Top values of machine.os.key	Count of records
200	osx	308
200	win xp	308
200	win 8	288
200	Other	570
404	osx	14
404	win 7	14
404	ios	12
404	Other	22
503	ios	17
503	win xp	16

Heatmap amb origen i destinacions de les sol·licituds.



Link del dashboard:
http://localhost:5601/app/dashboards#/view/edf84fe0-e1a0-11e7-b6d5-4dc382ef7f5b?_g=(filters%3A!()%2Cquery%3A(language%3Akuery%2Cquery%3A'')%2CrefreshInterval%3A(pause%3A!f%2Cvalue%3A900000)%2Ctime%3A(from%3Anow-7d%2Cto%3Anow))