Kibana Logs Queries

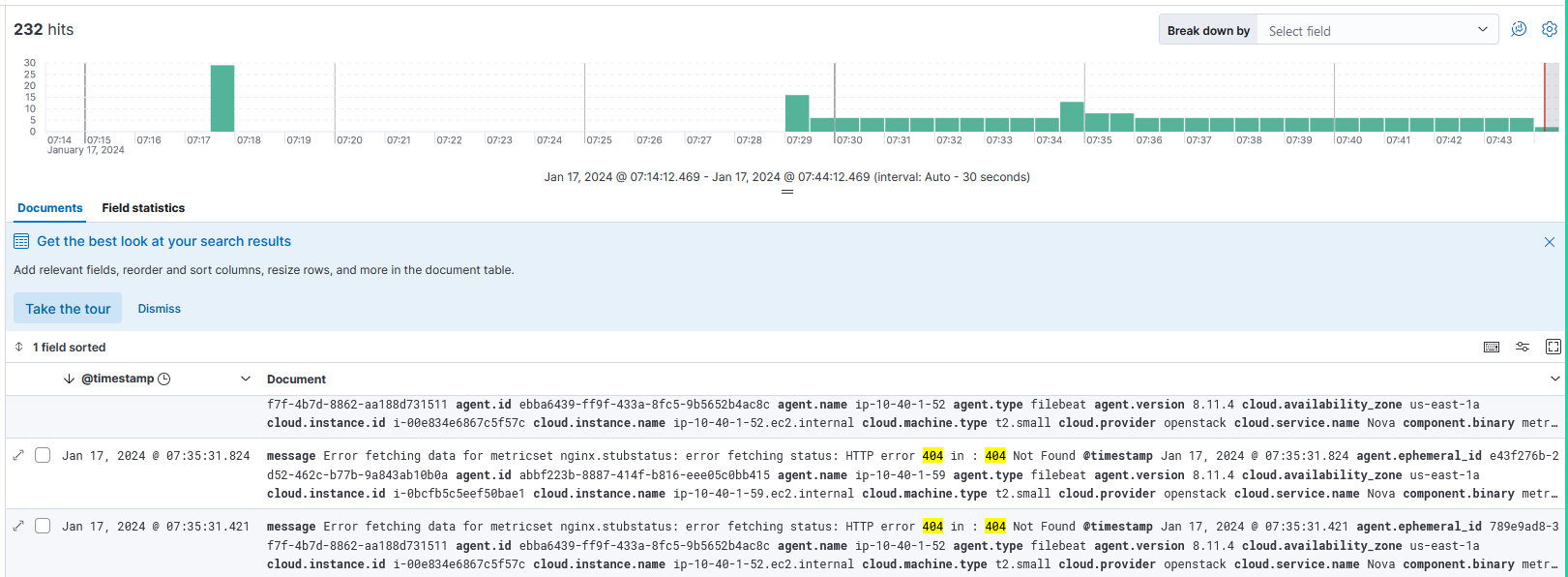
Kibana Portal can be accessed from Elastic Console → Analytics → Discover

On top left we have metrics-\* & logs-\*

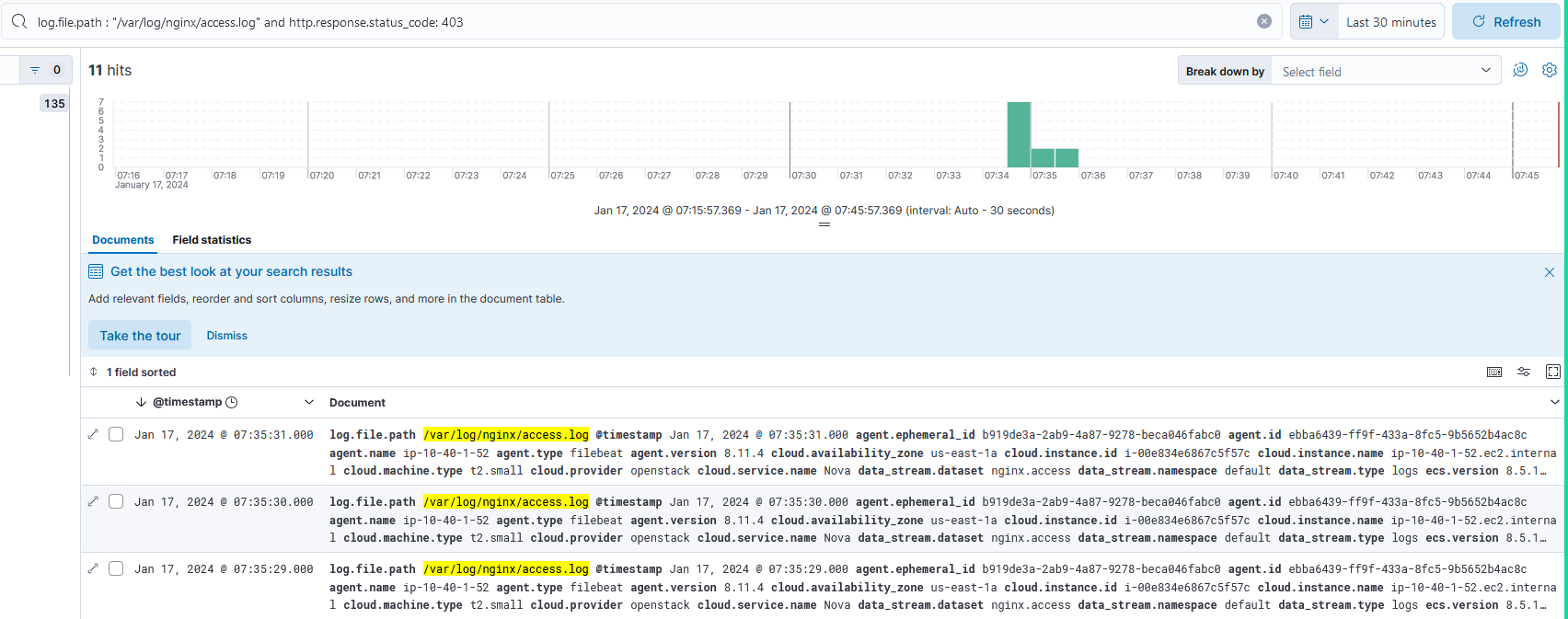
Select logs-\* and run the query as

*container.labels.com\_docker\_swarm\_service\_name: "flask"*

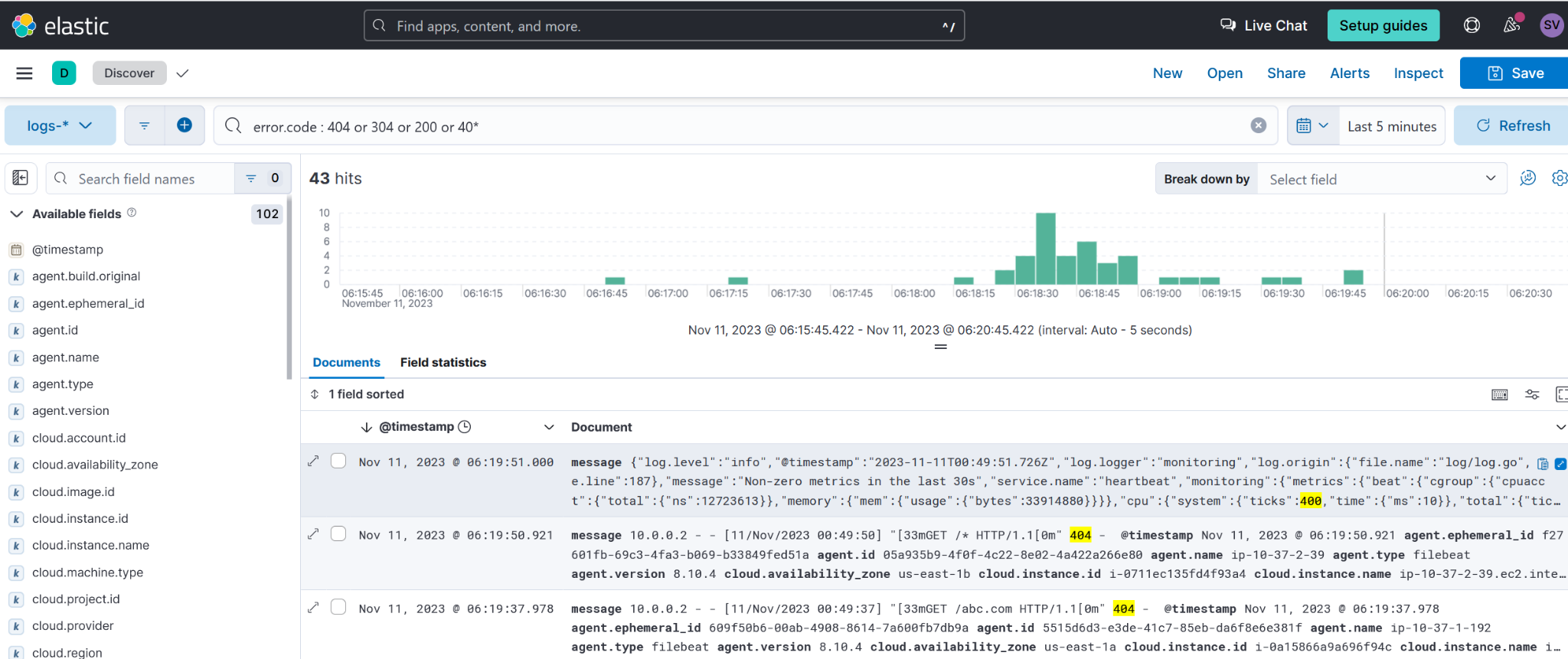
*http.response.status\_code: 403 or 404*

**

*log.file.path : "/var/log/nginx/access.log" and http.response.status\_code: 403*

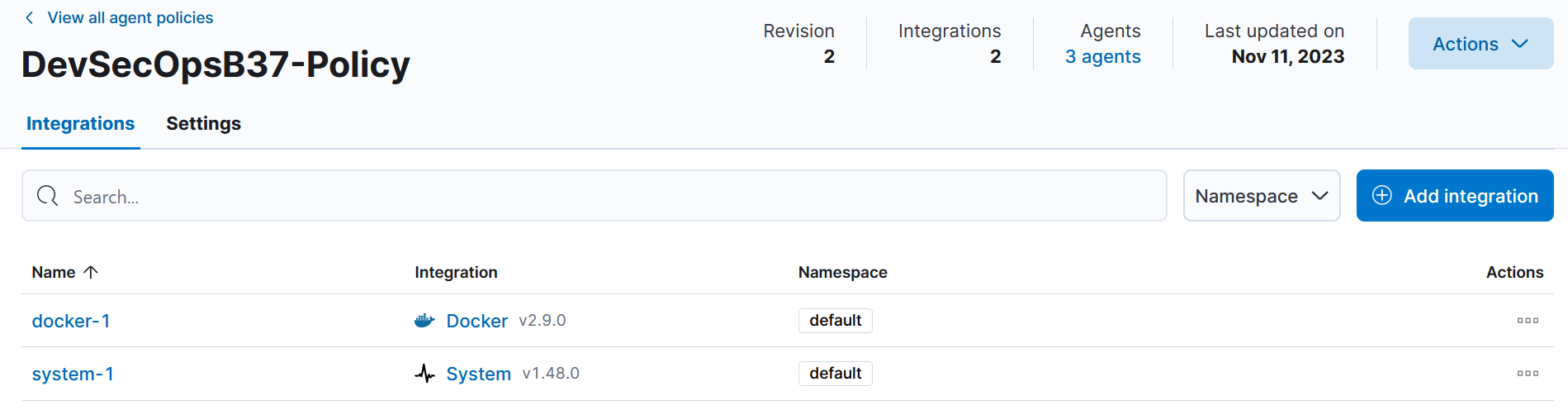
**

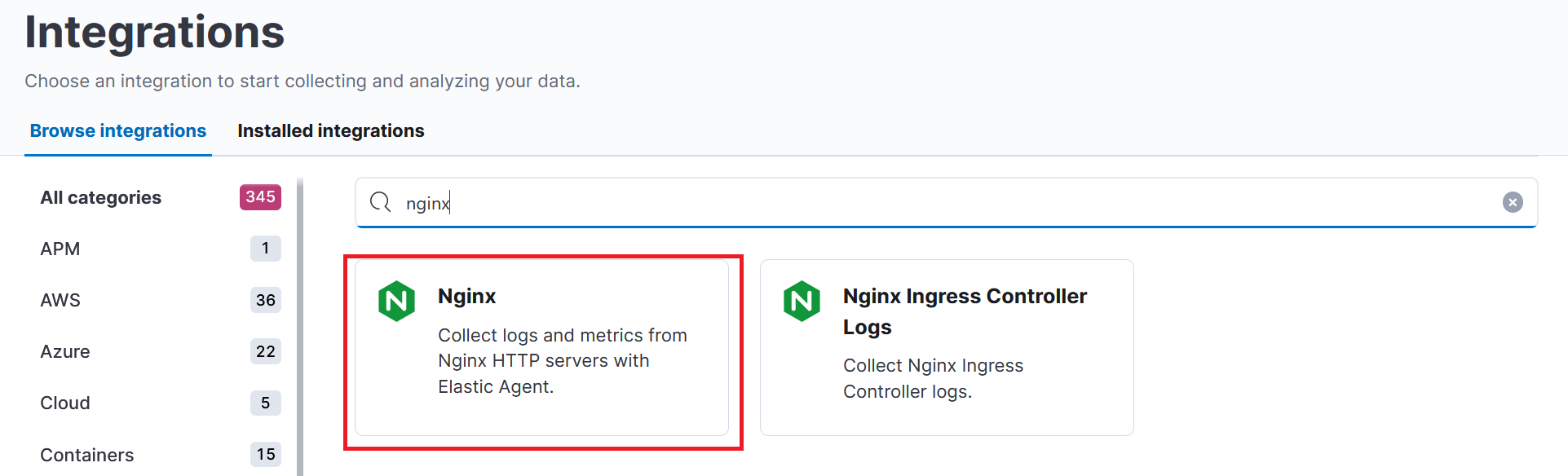
Error codes can be searched in logs: error.code : 404 or 304 or 200 or 40\*



**Collecting Nginx Logs Using Filebeat:**

We need to add Nginx Integration for the agent policy as shown below. In this case I am adding to DevSecOpsB37-Policy. As you can see in the picture we only have docker and system integrations.





Click on **Add Nginx** on the next screen.

