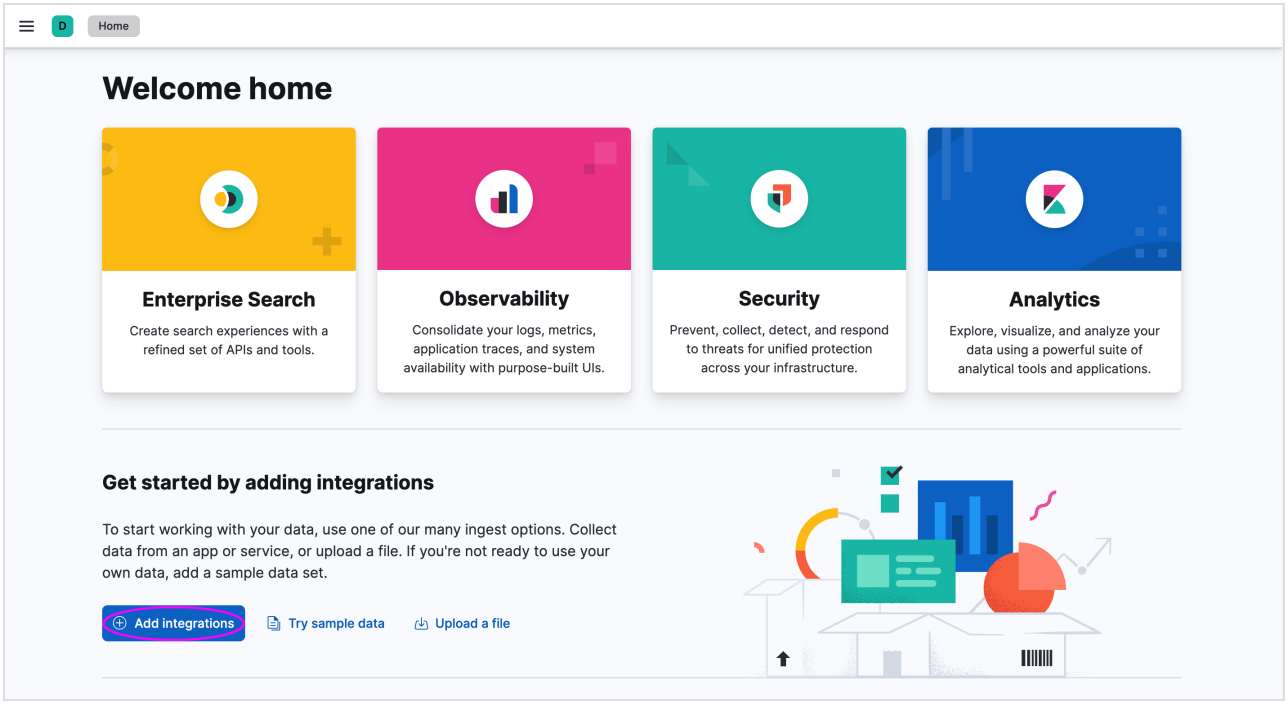
Lab 2: Logs

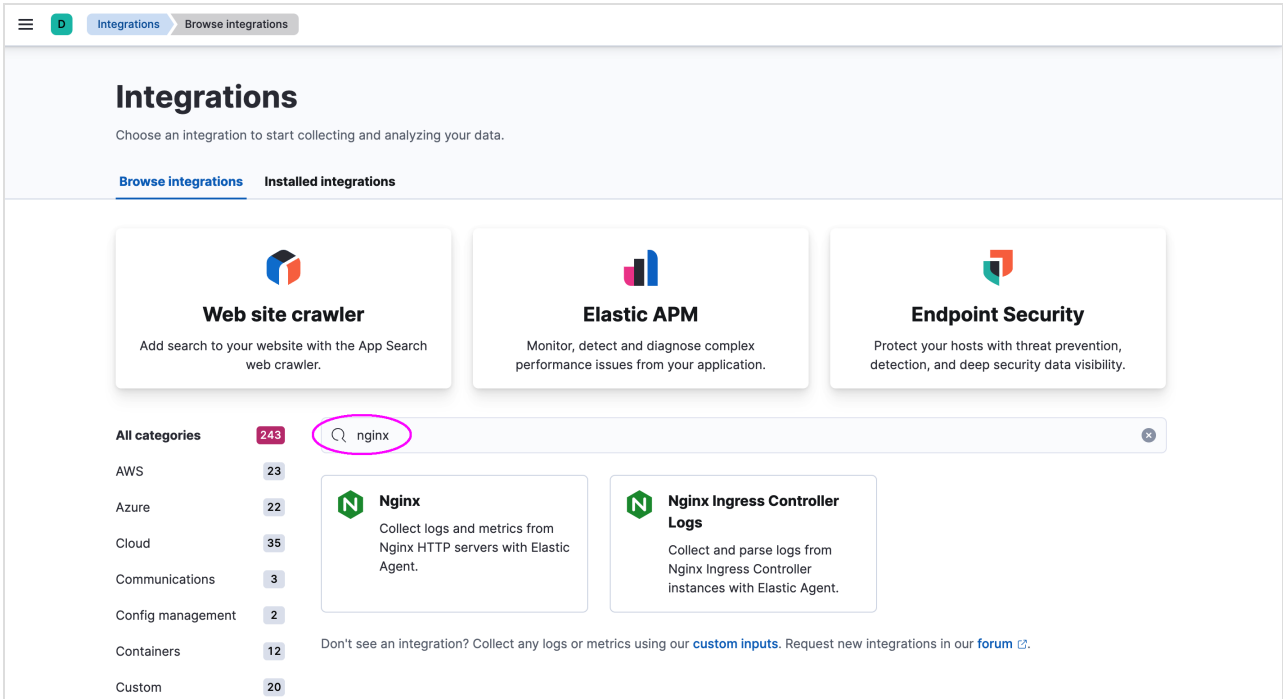
Objective:

In this lab, you will read Nginx log files with Elastic Agent and index them into Elasticsearch. You will also explore Kibana dashboards and see how you can monitor Nginx logs.

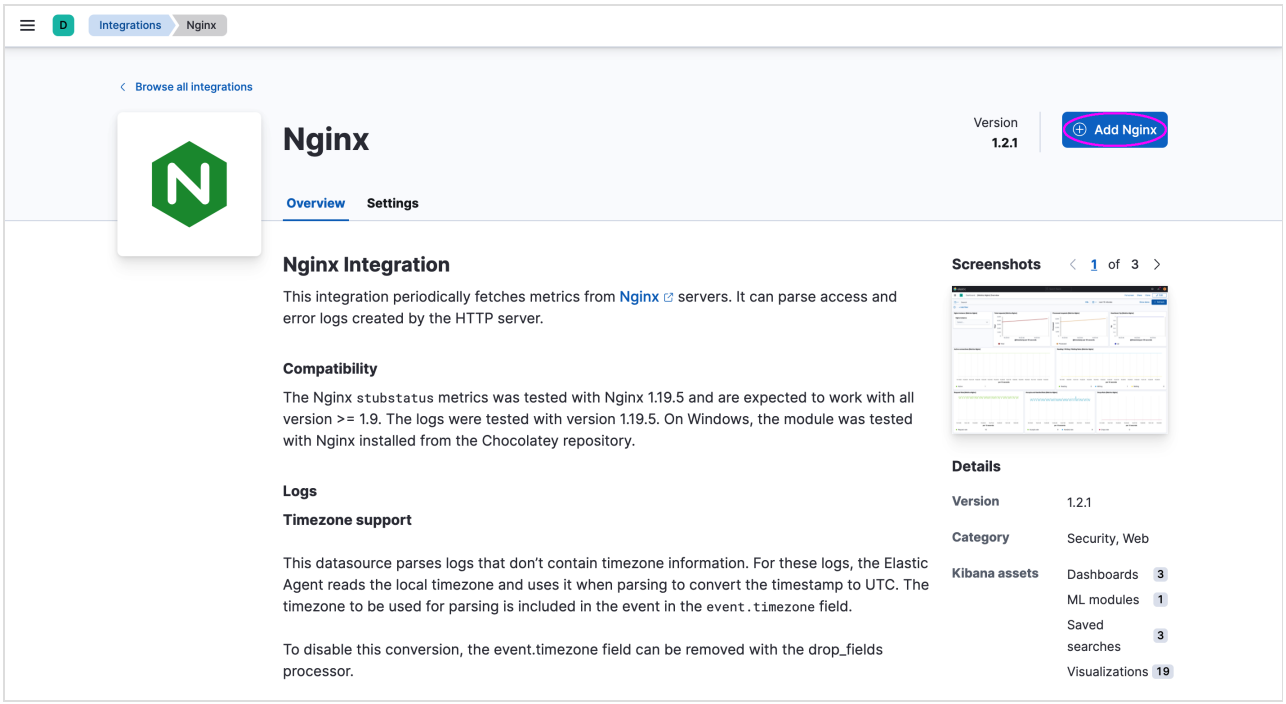
1. From the Kibana home page click **Add integrations**.



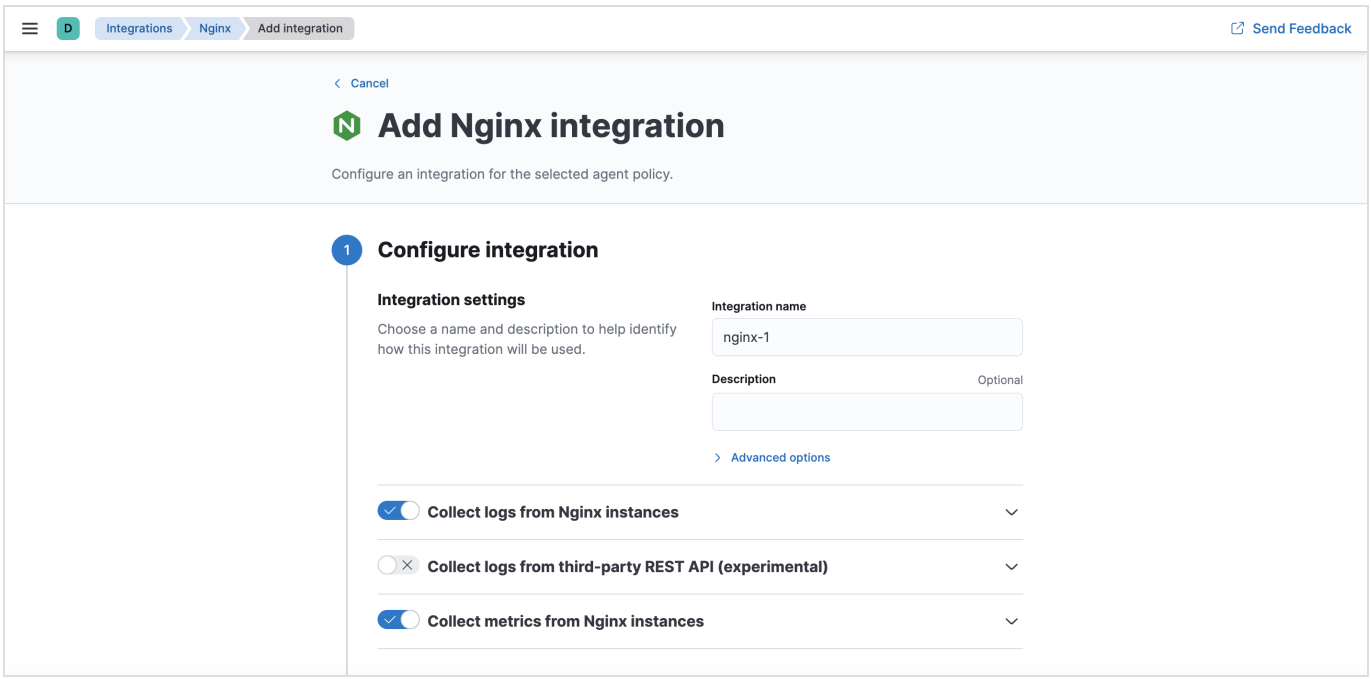
2. Next, search for **nginx** integrations and you will find two: the **Nginx** integration we are looking for and the **Nginx Ingress Controller Logs** that you can use in case you have a Kubernetes environment and need to parse `ingress-nginx` logs.



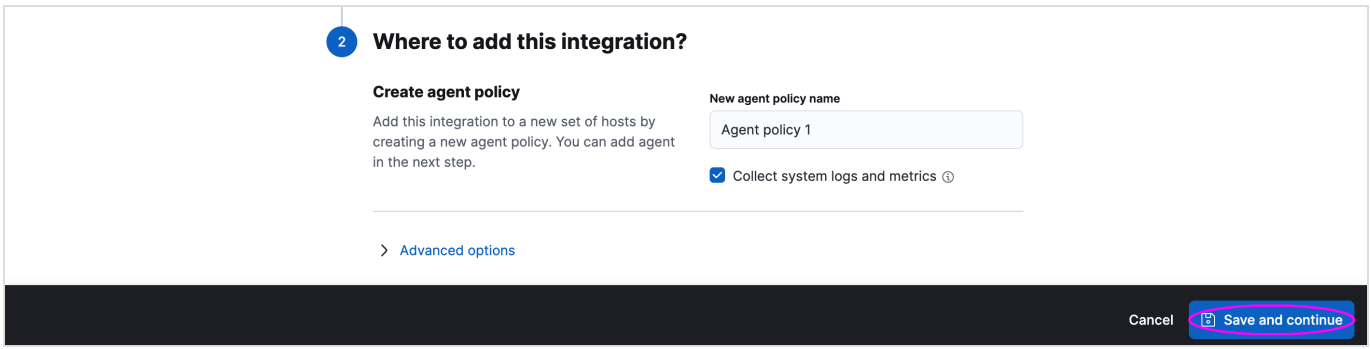
3. Access the **Nginx** integration. Note that some integrations already collect both logs and metrics by default, like the **Nginx** integration. Don't worry about metrics right now, as we will get back to them in the next lab.
4. Click **Add Nginx** to add the **Nginx integration**.



5. Even though we are more interested in Nginx logs for now, let's leave the metrics configuration already enabled for next lab.

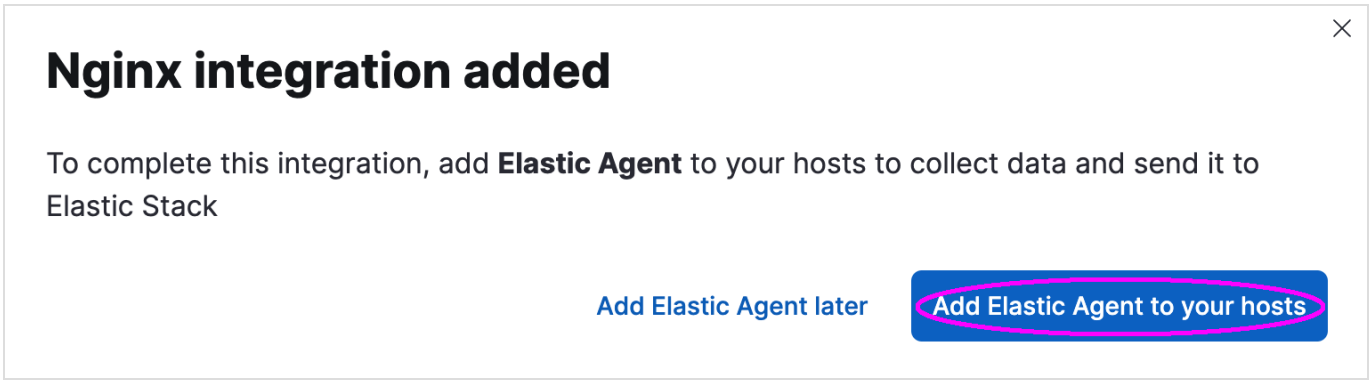


6. Click **Save and continue** to add the Nginx integration.



Note that the Nginx integration already suggests collecting logs and metrics through the system integration. You will explore the system integration in the next lab and can leave it as it is for now.

7. After adding the Nginx integration, click **Add Elastic Agent to your hosts** to start collecting logs and metrics from the Nginx server that is running on your lab environment.



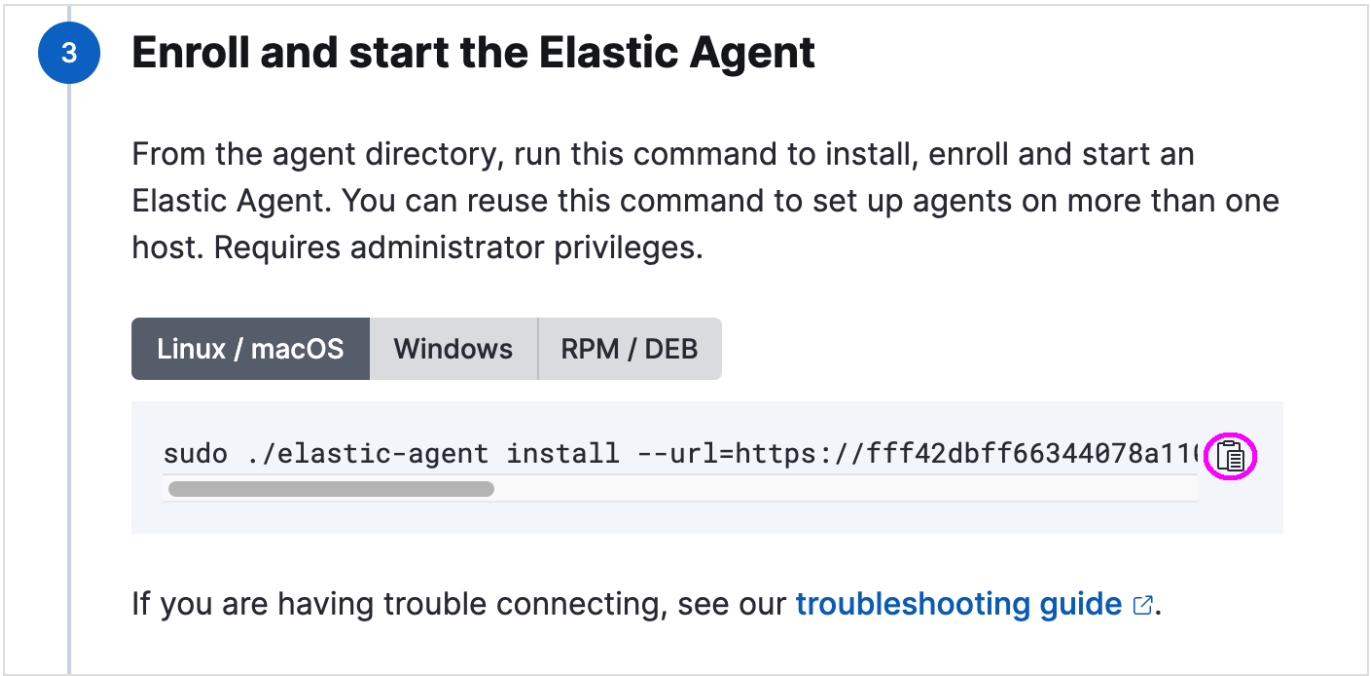
8. You will be using the default enrollment token, so the next step is to download the Elastic Agent to your host.
9. Download and install (actually just extract) the Elastic Agent. To do that, open a new terminal window and run the following commands. Note that you should download an Elastic Agent version that matches your Elastic Cloud deployment, so change `8.1.0` accordingly if your deployment is running on a different version.

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.1.0-linux-x86_64.tar.gz

tar -xzf elastic-agent-8.1.0-linux-x86_64.tar.gz

cd elastic-agent-8.1.0-linux-x86_64
```

10. Next, you will enroll and start the Elastic Agent. To do that, copy the enrollment line you see in Kibana and execute it in the terminal.



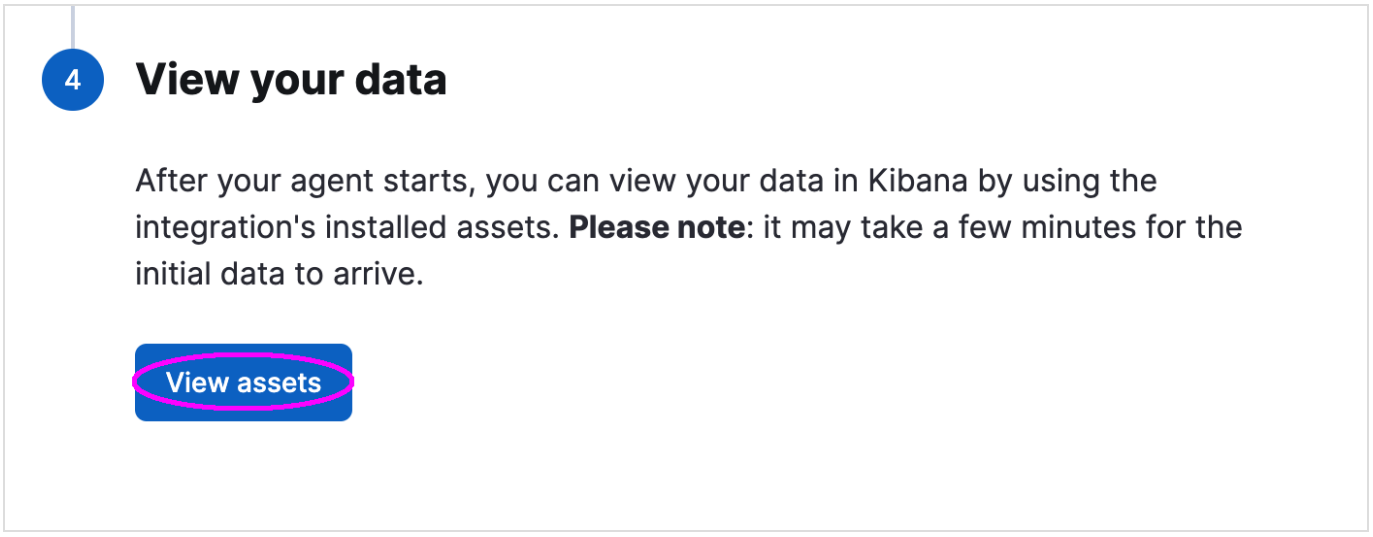
11. After executing the enrollment line, you will see the following message. Press `Enter` to continue.

```
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you want to continue? [Y/n]:
```

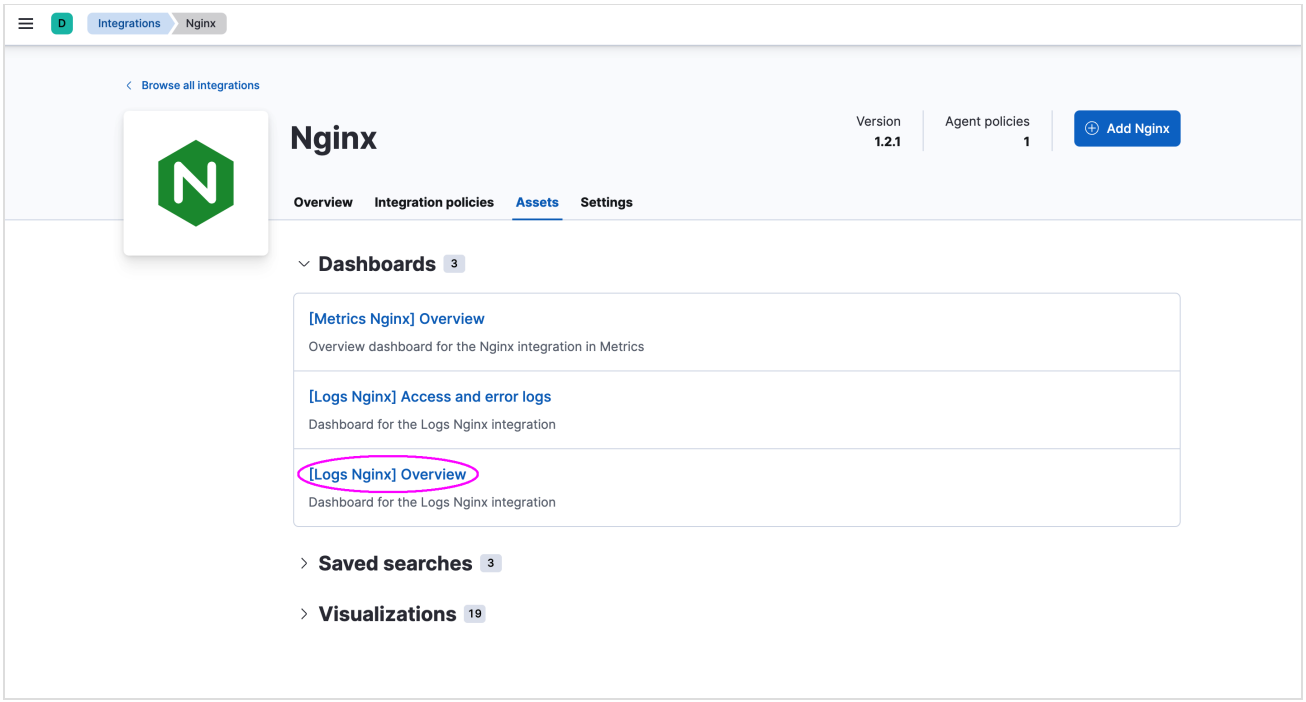
12. Next, you will use a **curl**-based script to simulate load on the Nginx server. Open a new terminal window and run the following command:

```
./artificial_load.sh
```

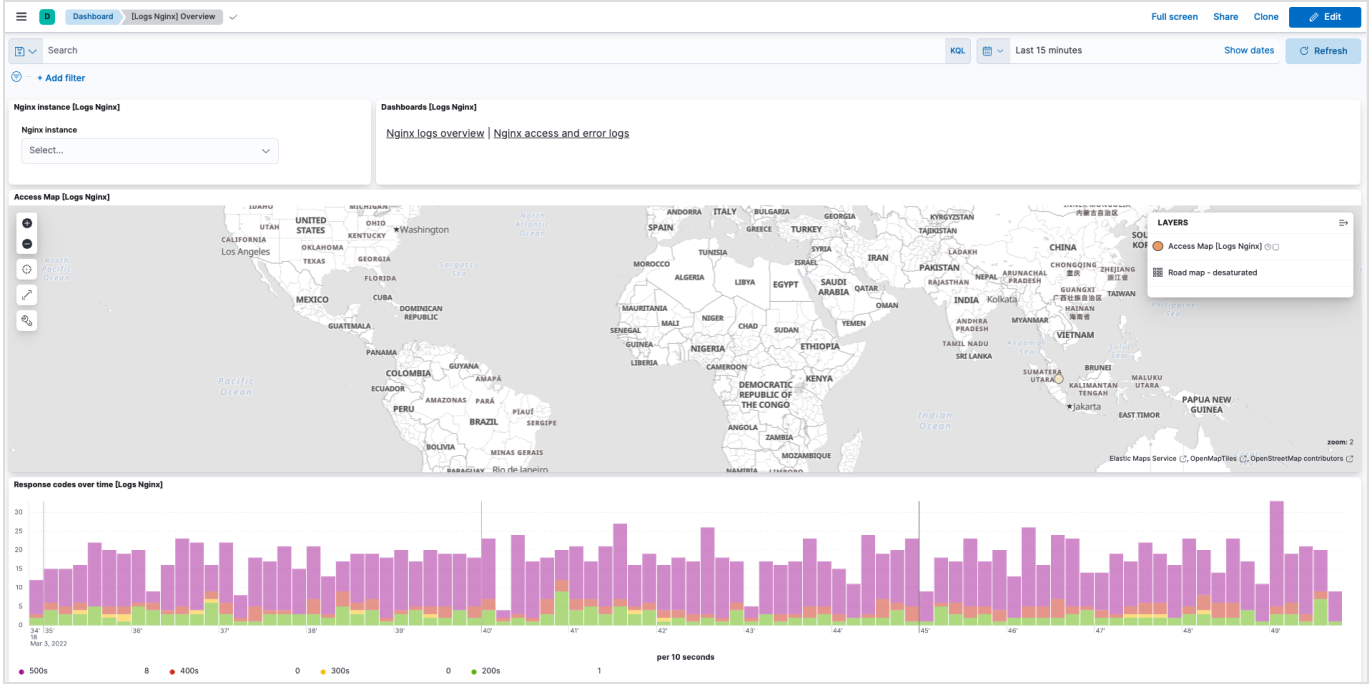
13. Go back to Kibana and click **View Assets** to see the available dashboards for the Nginx integration.



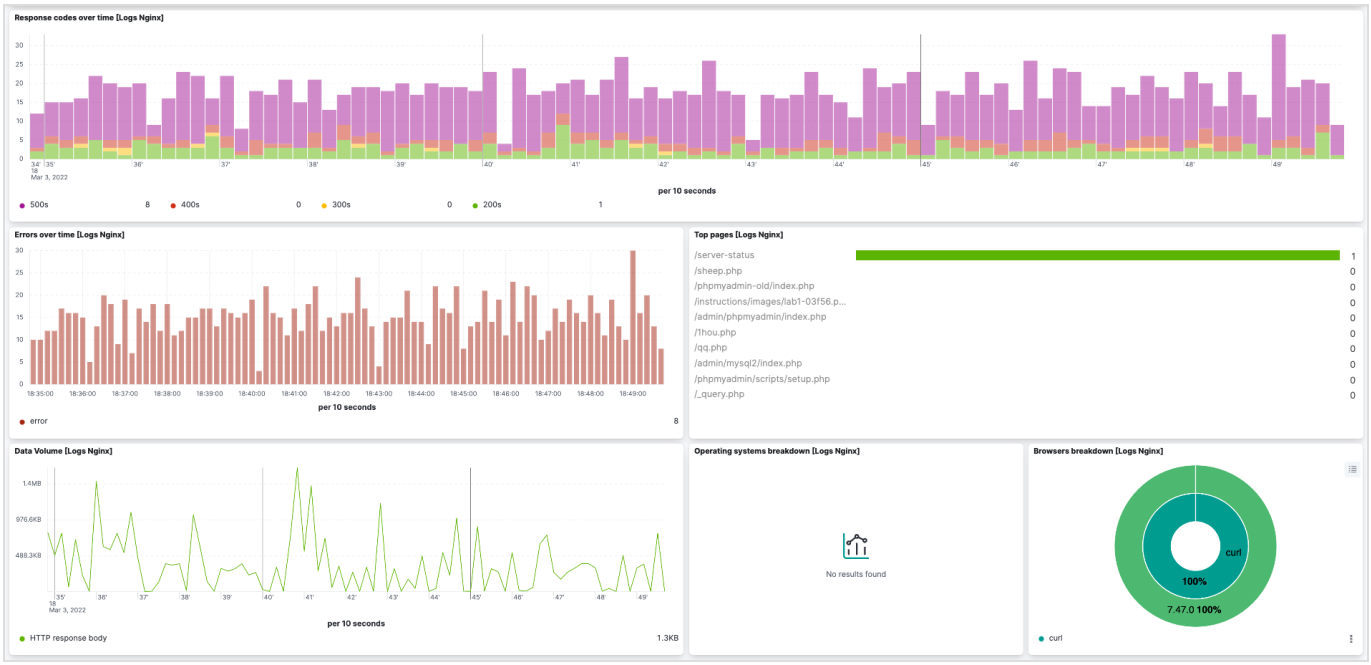
14. Since we are interested in Nginx logs, open the **[Logs Nginx] Overview** dashboard.



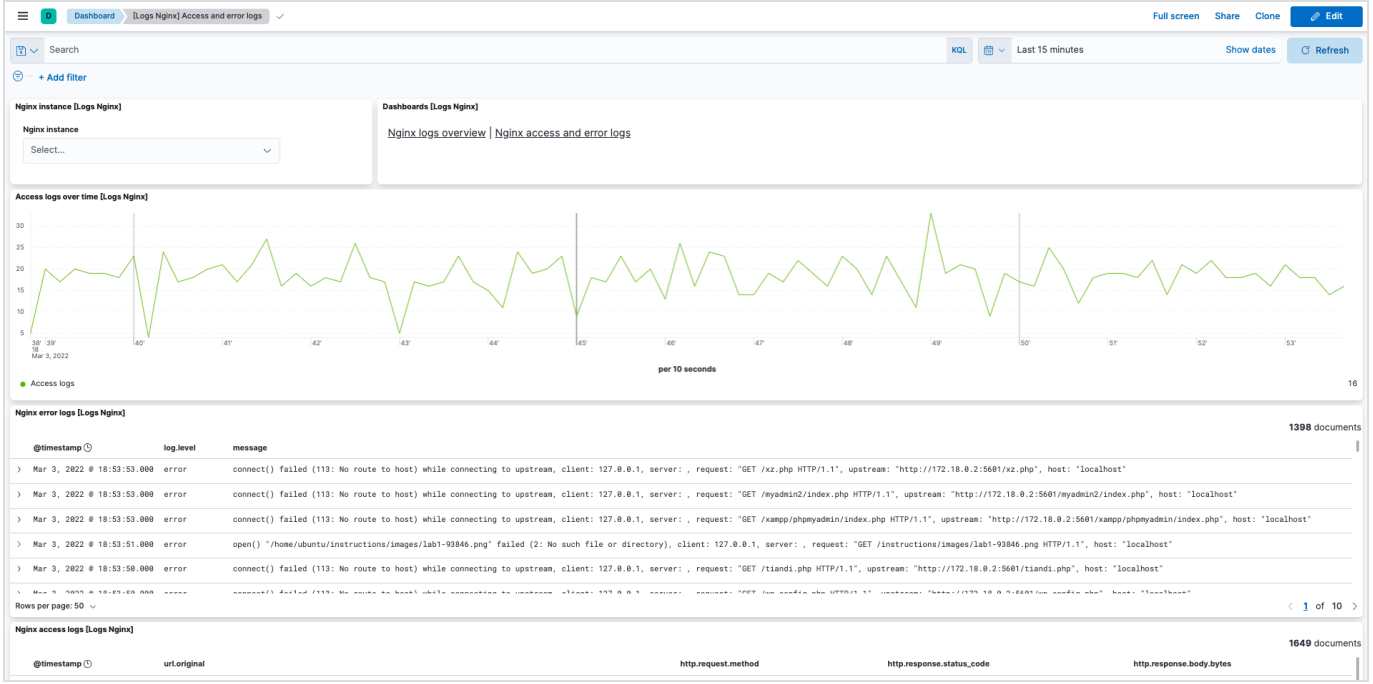
This will open the dashboard:



15. Scroll down and check what the most used browser is. It should be **curl** because it is being used by the load simulation script.



16. Now, click **Nginx access and error logs** at the top of the current dashboard. This will open the dashboard with the access and error logs that Elastic Agent has collected from Nginx.



Summary:

In this lab, you have read Nginx log files with Elastic Agent and indexed them into Elasticsearch. You also explored Kibana dashboards and saw how you can monitor Nginx logs.