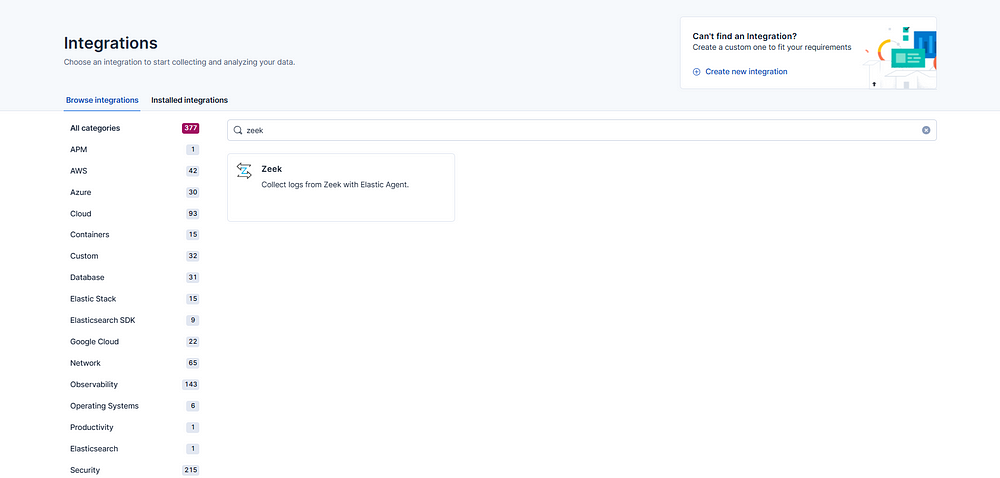
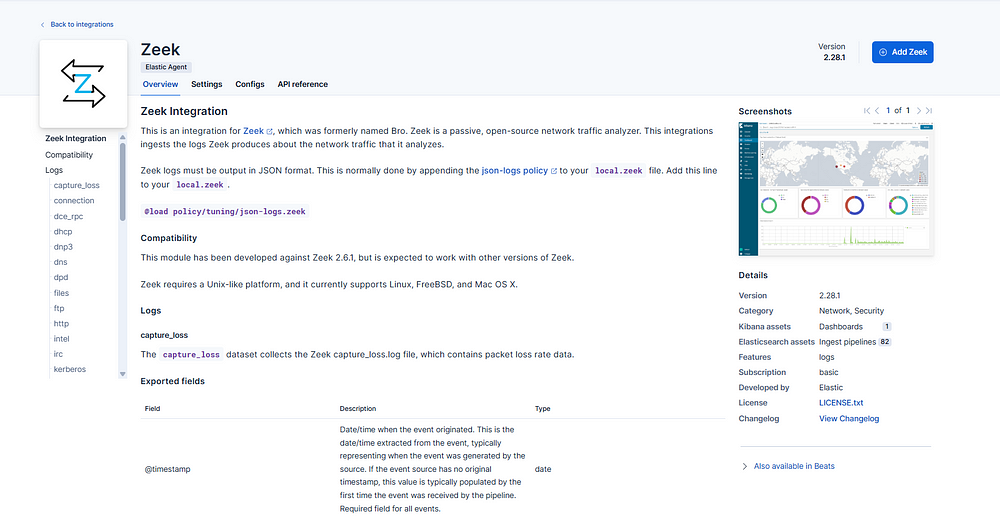
### **Zeek Integration in Elastic**

For instructions on installing and configuring Zeek on Ubuntu, refer to the Zeek—Ubuntu blog.

To configure Zeek integration within Elastic Cloud, navigate to the Integrations section, search for "Zeek integration," and select the corresponding option.



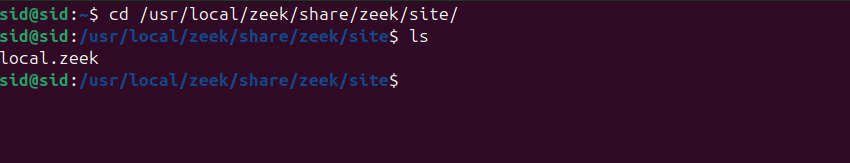
Upon initiating this integration, a prompt appears requesting the submission of Zeek logs in JSON format..



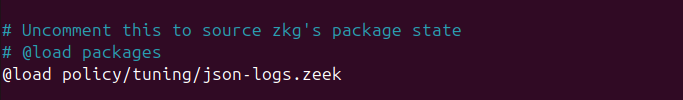
Let us proceed with this task.

Please access the Ubuntu operating system and navigate to the subsequent directory:

cd /usr/local/zeek/share/zeek/site



The file "local.zeek" can be modified by appending the following directive: "@load policy/tuning/json-logs.zeek".



To initiate Zeek and generate logs, execute the following command in a separate terminal with elevated privileges:

sudo zeekctl deploy

Subsequently, in the preceding terminal session, navigate to the log directory using the command:

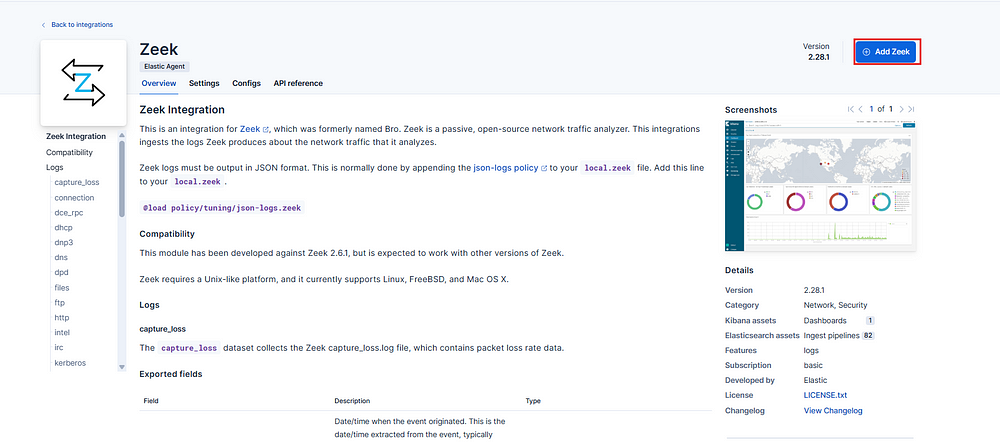
cd /usr/local/zeek/logs/current

Finally, select a log file and display its contents using the `cat` command.

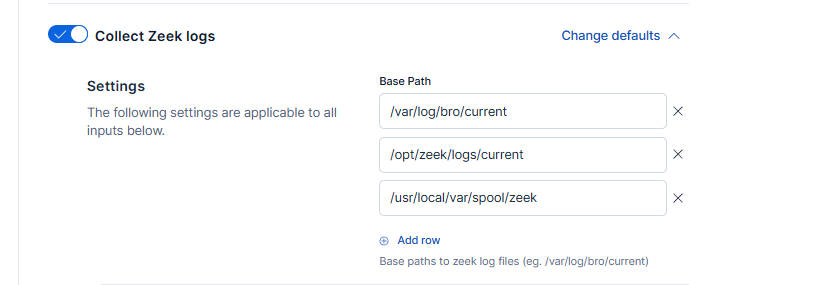


As illustrated above, the log file's contents are formatted in JSON.

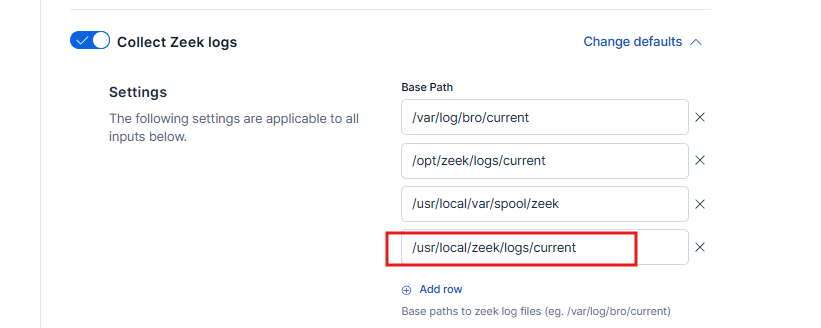
Proceed to the Elastic Cloud platform and select the "Add Zeek" option.



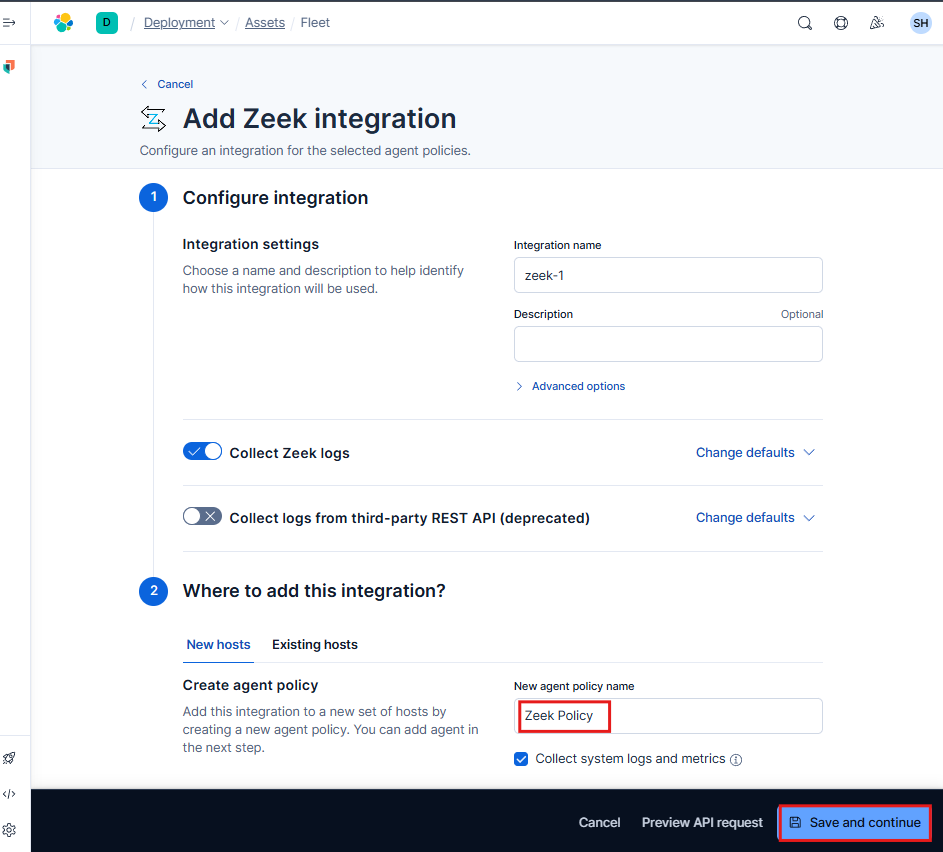
Subsequently, within the section dedicated to collecting Zeek logs, select the option to modify default settings..



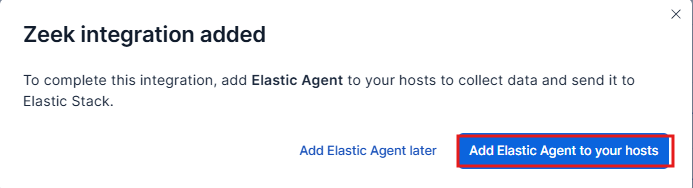
To add a path to the Zeek logs, please select "Add row" and enter the desired path.



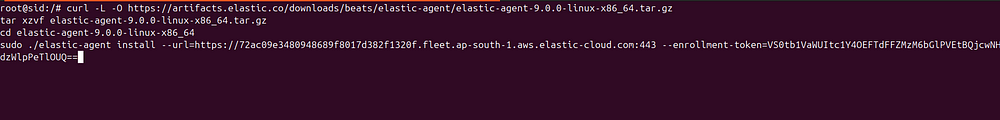
Subsequently, designate the policy name and proceed by selecting 'Save and Continue'..



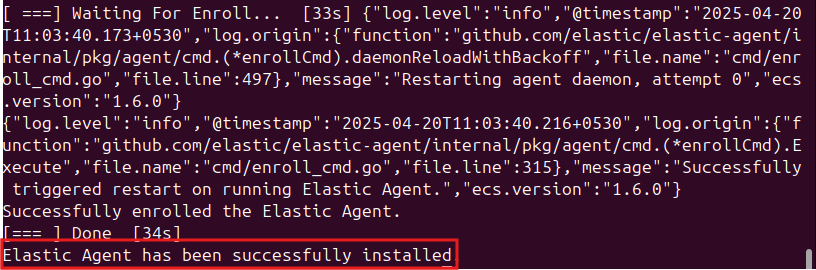
Subsequently, proceed by selecting "Add Elastic Agent to your Host."



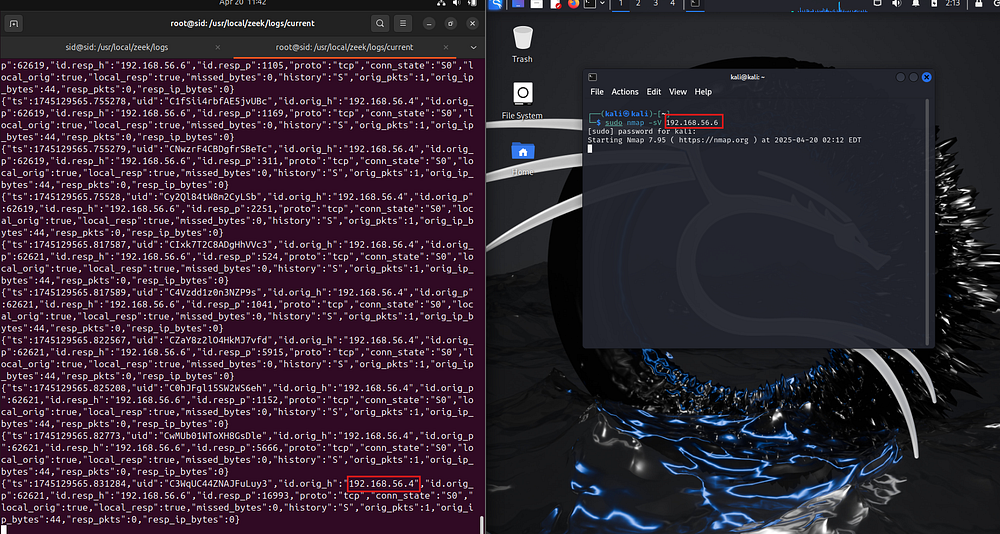
Subsequently, transfer the commands to integrate the Elastic agent into the host. Navigate to the Ubuntu machine and execute these commands within a terminal operating under root privileges.



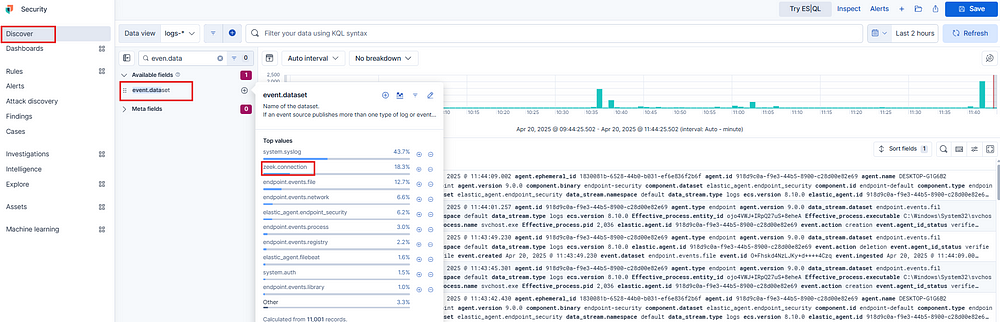
Following the completion of a brief interval, the installation procedure will conclude, and a confirmation message indicating successful installation will be displayed.



Subsequently, an nmap scan was executed, and the resultant data was observed.



The log collection from the Nmap scan has been successfully achieved. Confirmation of log ingestion into Elasticsearch is feasible via examination within the "Discover" section, specifically by searching for and selecting "event.dataset".



As demonstrated, successful log generation and ingestion into Elastic have been achieved.