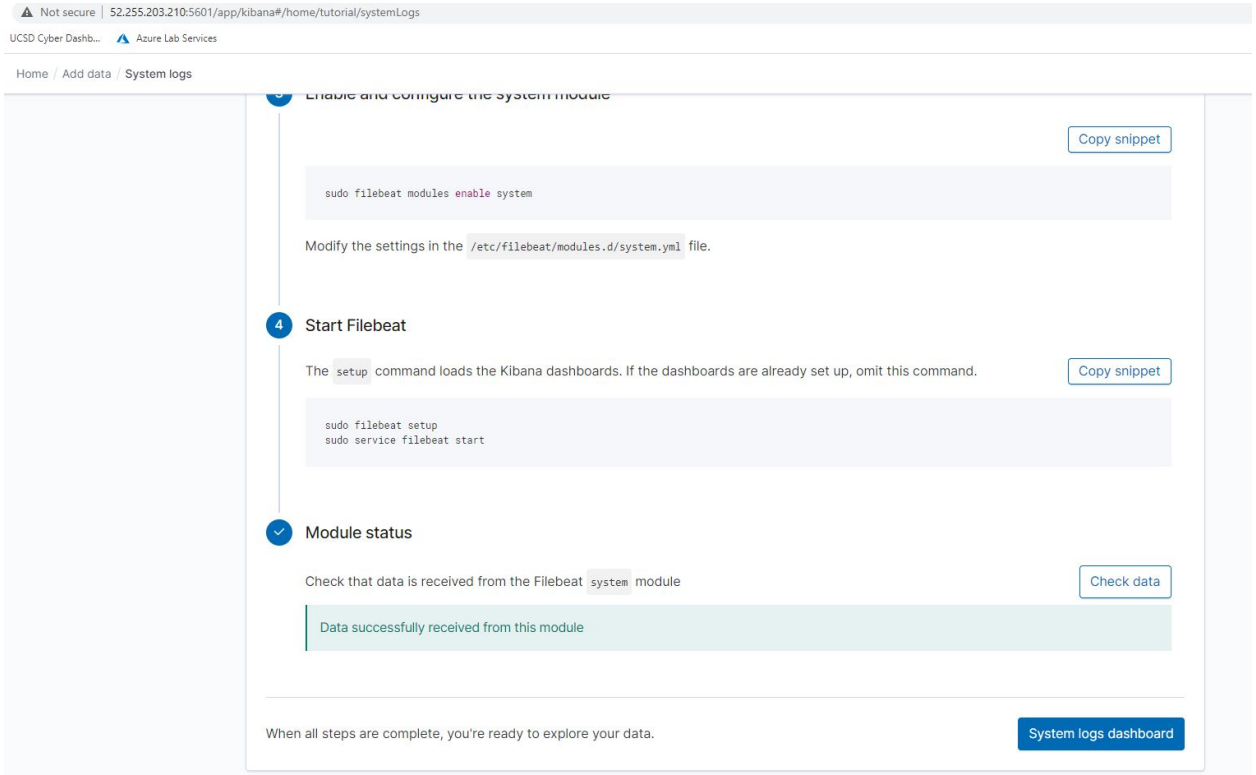
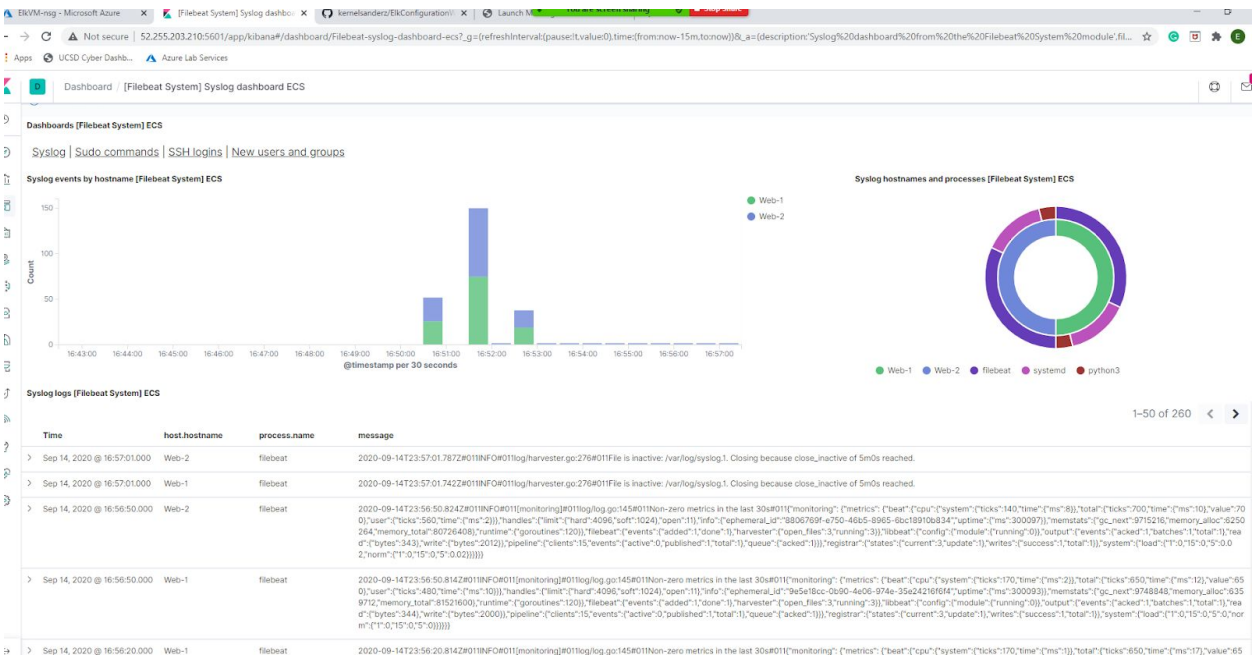

Not secure | 52.255.203.210:5601/app/kibana#/home/tutorial/systemLogs
UCSD Cyber Dashb...
Azure Lab Services
Home / Add data / System logs
Copy snippet
sudo filebeat modules enable system
Modify the settings in the /etc/filebeat/modules.d/system.yml file.
4
Start Filebeat
The setup command loads the Kibana dashboards. If the dashboards are already set up, omit this command.
Copy snippet
sudo filebeat setup
sudo service filebeat start
Module status
Check that data is received from the Filebeat system module
Check data
Data successfully received from this module
When all steps are complete, you're ready to explore your data.
System logs dashboard


Dashboard / [Filebeat System] Syslog dashboard ECS
Dashboards [Filebeat System] ECS
Syslog | Sudo commands | SSH logins | New users and groups
Syslog events by hostname [Filebeat System] ECS
Count
@timestamp per 30 seconds
Web-1
Web-2
Syslog hostnames and processes [Filebeat System] ECS
Web-1 Web-2 filebeat systemd python3
Syslog logs [Filebeat System] ECS
1–50 of 260
Time
host.hostname
process.name
message