ICT & Infra S3 Supporting Services and Monitoring week 13

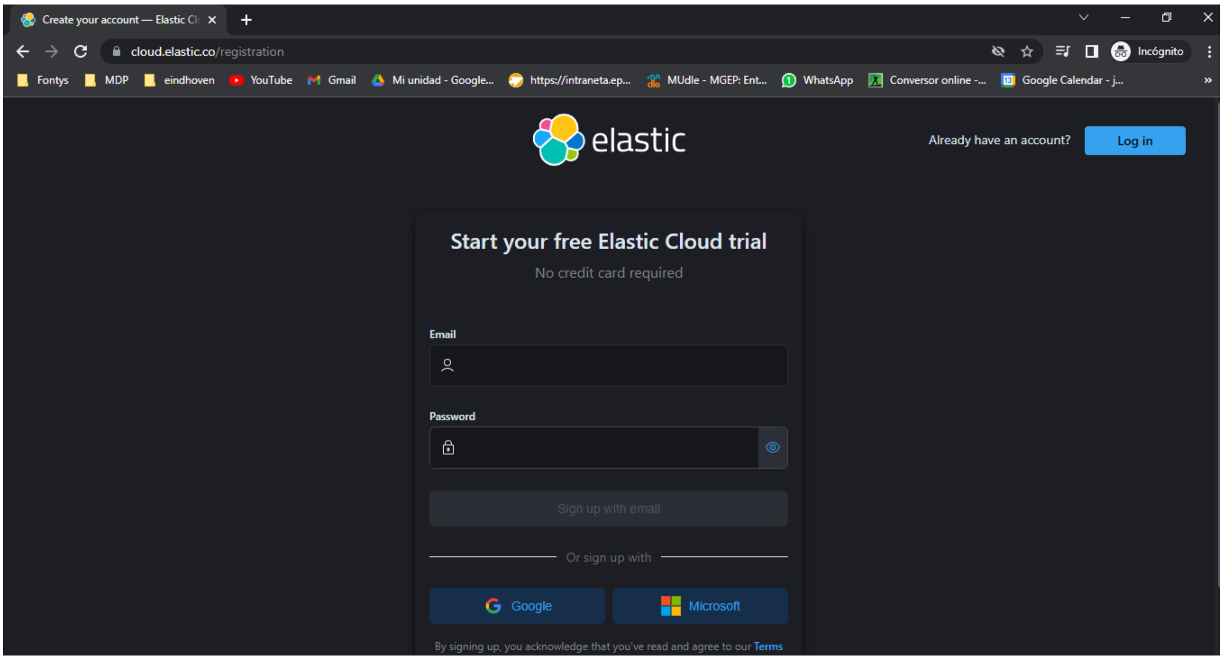
Class:	***CB01***
Student number:	***4961854***
Student name:	***Heiko Morales***

Introduction

In order to learn more about monitoring I also wanted to use elastic with the agent. So in this report I am going to explain what I have done to monitor a database.

Assignment 1. Setting up elastic

first we will register at elastic



cloud.elastic.co/registration

Start your free Elastic Cloud trial

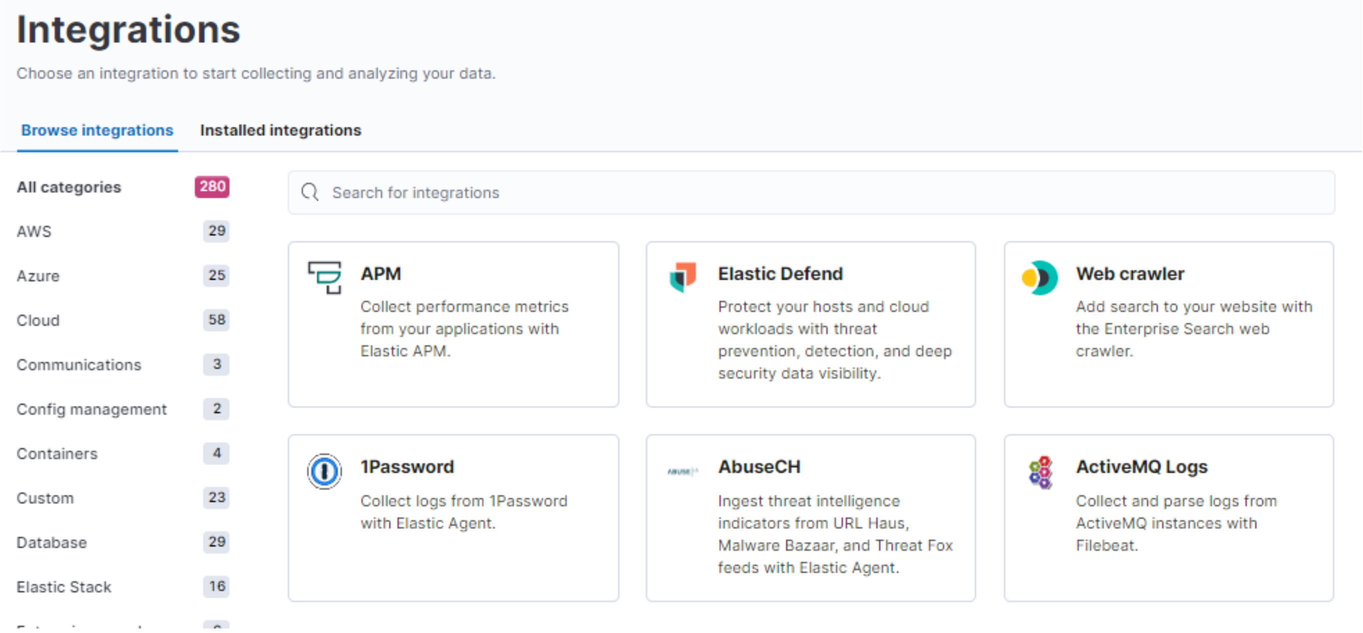
No credit card required

Email

Password

By signing up, you acknowledge that you've read and agree to our Terms

Once inside we will go to the integrations section



Integrations

Choose an integration to start collecting and analyzing your data.

All categories	280
AWS	29
Azure	25
Cloud	58
Communications	3
Config management	2
Containers	4
Custom	23
Database	29
Elastic Stack	16

APM
Collect performance metrics from your applications with Elastic APM.

Elastic Defend
Protect your hosts and cloud workloads with threat prevention, detection, and deep security data visibility.

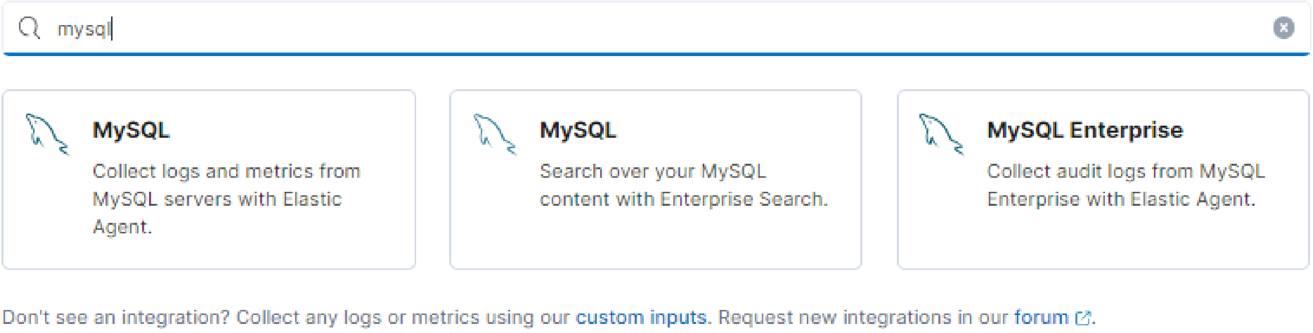
Web crawler
Add search to your website with the Enterprise Search web crawler.

1Password
Collect logs from 1Password with Elastic Agent.

AbuseCH
Ingest threat intelligence indicators from URL Haus, Malware Bazaar, and Threat Fox feeds with Elastic Agent.

ActiveMQ Logs
Collect and parse logs from ActiveMQ instances with Filebeat.

here, we will search for mysql and select 1



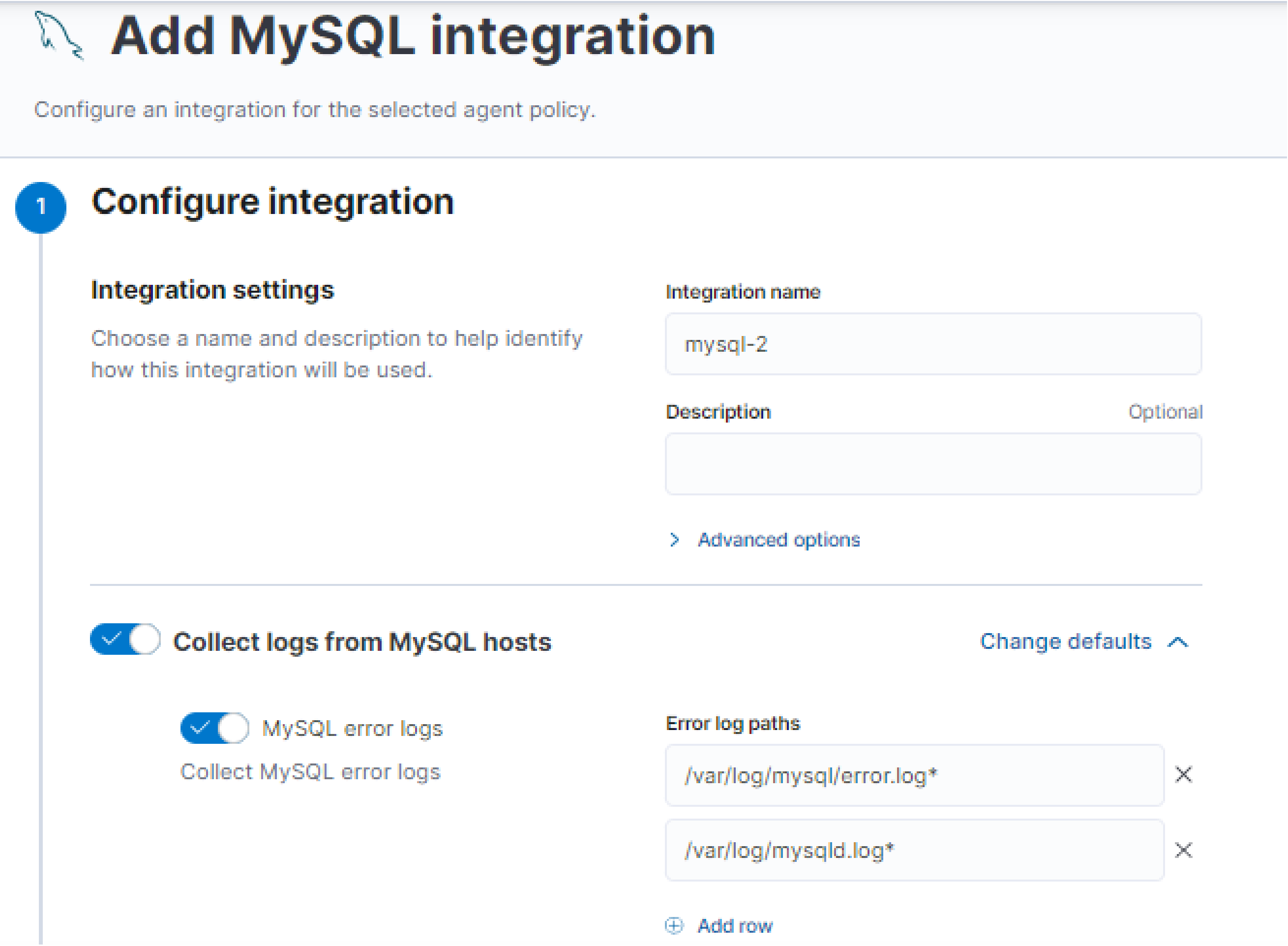
MySQL
Collect logs and metrics from MySQL servers with Elastic Agent.

MySQL
Search over your MySQL content with Enterprise Search.

MySQL Enterprise
Collect audit logs from MySQL Enterprise with Elastic Agent.

Don't see an integration? Collect any logs or metrics using our custom inputs. Request new integrations in our forum.

we will fill in all the data and install the agent as shown in the help



Add MySQL integration

Configure an integration for the selected agent policy.

1 Configure integration

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name: mysql-2

Description (Optional):

Collect logs from MySQL hosts

MySQL error logs

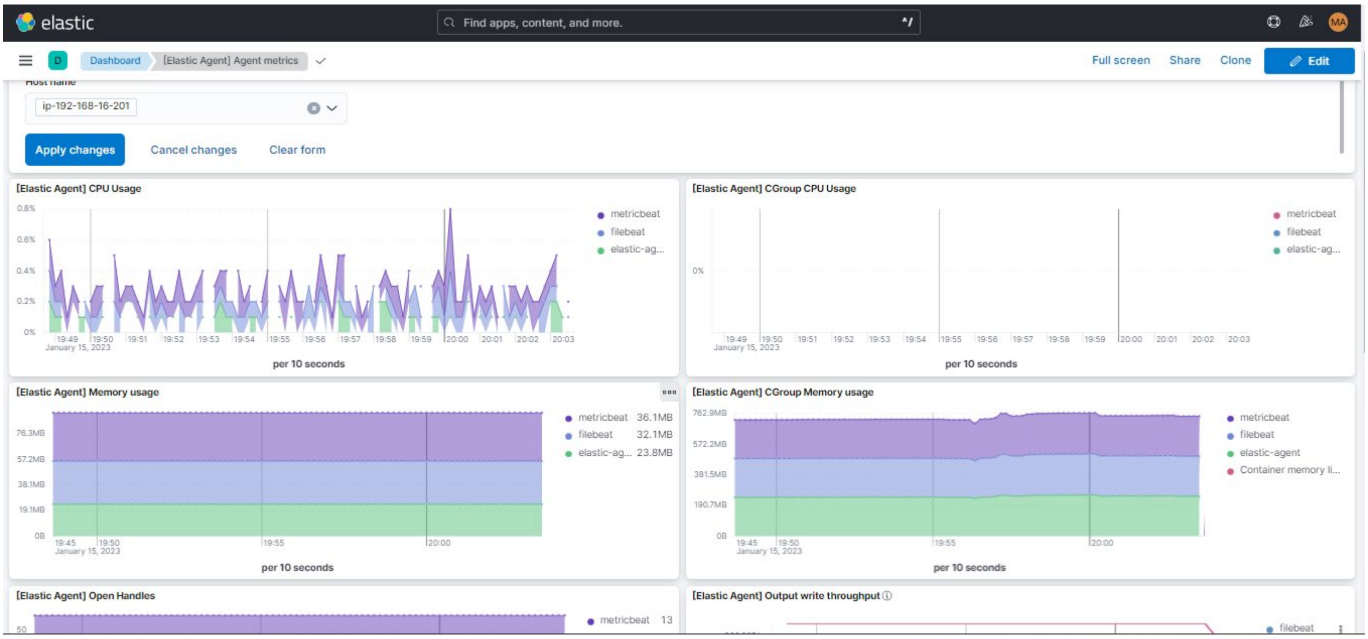
Collect MySQL error logs

Error log paths:

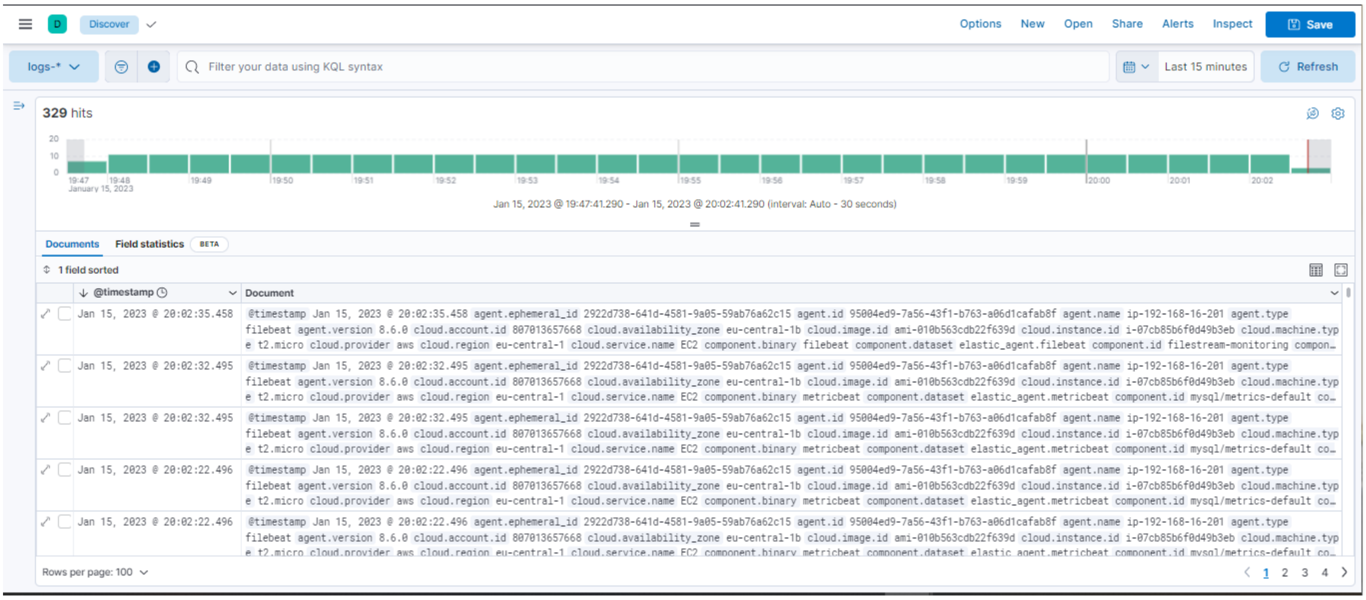
/var/log/mysql/error.log*

/var/log/mysqld.log*

Once installed and having left some time we can see that we are able to receive the data from the database.



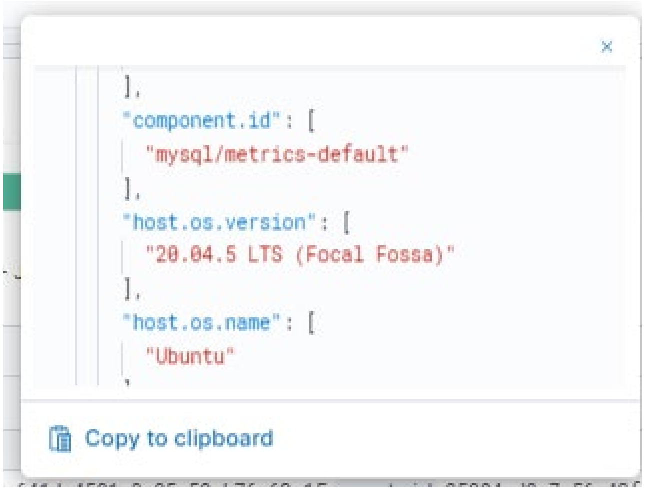
And we even have the logs that we receive from the machine itself.



Jan 15, 2023 @ 19:47:41.290 - Jan 15, 2023 @ 20:02:41.290 (interval: Auto - 30 seconds)

```
@timestamp                   Document
Jan 15, 2023 @ 20:02:35.458  @timestamp Jan 15, 2023 @ 20:02:35.458 agent.ephemeral_id 2922d738-641d-4581-9a05-59ab76a62c15 agent.id 95004ed9-7a56-43f1-b763-a06d1cafab8f agent.name ip-192-168-16-201 agent.type
                             filebeat agent.version 8.6.0 cloud.account.id 807013657668 cloud.availability_zone eu-central-1b cloud.image.id ami-010b563cdb22f639d cloud.instance.id i-07cb85b6f0d49b3eb cloud.machine.typ
                             e t2.micro cloud.provider aws cloud.region eu-central-1 cloud.service.name EC2 component.binary filebeat component.dataset elastic_agent.filebeat component.id filestream-monitoring compon…
Jan 15, 2023 @ 20:02:32.495  @timestamp Jan 15, 2023 @ 20:02:32.495 agent.ephemeral_id 2922d738-641d-4581-9a05-59ab76a62c15 agent.id 95004ed9-7a56-43f1-b763-a06d1cafab8f agent.name ip-192-168-16-201 agent.type
                             filebeat agent.version 8.6.0 cloud.account.id 807013657668 cloud.availability_zone eu-central-1b cloud.image.id ami-010b563cdb22f639d cloud.instance.id i-07cb85b6f0d49b3eb cloud.machine.typ
                             e t2.micro cloud.provider aws cloud.region eu-central-1 cloud.service.name EC2 component.binary metricbeat component.dataset elastic_agent.metricbeat component.id mysql/metrics-default co…
Jan 15, 2023 @ 20:02:32.495  @timestamp Jan 15, 2023 @ 20:02:32.495 agent.ephemeral_id 2922d738-641d-4581-9a05-59ab76a62c15 agent.id 95004ed9-7a56-43f1-b763-a06d1cafab8f agent.name ip-192-168-16-201 agent.type
                             filebeat agent.version 8.6.0 cloud.account.id 807013657668 cloud.availability_zone eu-central-1b cloud.image.id ami-010b563cdb22f639d cloud.instance.id i-07cb85b6f0d49b3eb cloud.machine.typ
                             e t2.micro cloud.provider aws cloud.region eu-central-1 cloud.service.name EC2 component.binary metricbeat component.dataset elastic_agent.metricbeat component.id mysql/metrics-default co…
Jan 15, 2023 @ 20:02:22.496  @timestamp Jan 15, 2023 @ 20:02:22.496 agent.ephemeral_id 2922d738-641d-4581-9a05-59ab76a62c15 agent.id 95004ed9-7a56-43f1-b763-a06d1cafab8f agent.name ip-192-168-16-201 agent.type
                             filebeat agent.version 8.6.0 cloud.account.id 807013657668 cloud.availability_zone eu-central-1b cloud.image.id ami-010b563cdb22f639d cloud.instance.id i-07cb85b6f0d49b3eb cloud.machine.typ
                             e t2.micro cloud.provider aws cloud.region eu-central-1 cloud.service.name EC2 component.binary metricbeat component.dataset elastic_agent.metricbeat component.id mysql/metrics-default co…
Jan 15, 2023 @ 20:02:22.496  @timestamp Jan 15, 2023 @ 20:02:22.496 agent.ephemeral_id 2922d738-641d-4581-9a05-59ab76a62c15 agent.id 95004ed9-7a56-43f1-b763-a06d1cafab8f agent.name ip-192-168-16-201 agent.type
                             filebeat agent.version 8.6.0 cloud.account.id 807013657668 cloud.availability_zone eu-central-1b cloud.image.id ami-010b563cdb22f639d cloud.instance.id i-07cb85b6f0d49b3eb cloud.machine.typ
                             e t2.micro cloud.provider aws cloud.region eu-central-1 cloud.service.name EC2 component.binary metricbeat component.dataset elastic_agent.metricbeat component.id mysql/metrics-default co…
```

To make sure we enter a log of the received and we can see that it is from the database



```
  ],
  "component.id": [
    "mysql/metrics-default"
  ],
  "host.os.version": [
    "20.04.5 LTS (Focal Fossa)"
  ],
  "host.os.name": [
    "Ubuntu"
  ],
```