

ExercAula07 -Elastic Logstash

Paramos o serviço do docker com docker-compose stop, pois vamos alterar arquivos de configuração.

1. Enviar o arquivo <local>/paris-925.logs para o Logstash, com uso do Filebeat.

Resposta:

```
marco@DESKTOP-G2455QH:~/treinamentos/elastic$ cd filebeat-7.9.2-linux-x86_64/
```

```
marco@DESKTOP-G2455QH:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64$ sudo vi filebeat.yml
```

Alterar o output para:

filebeat.inputs:

Each - is an input. Most options can be set at the input level, so
you can use different inputs for various configurations.
Below are the input specific configurations.

- type: log

Change to true to enable this input configuration.

enabled: true

Paths that should be crawled and fetched. Glob based paths.

paths:

- /home/marco/treinamentos/elastic/dataset/paris-925.logs

output.logstash:

The Logstash hosts

hosts: ["localhost:5044"]

2. Configurar e executar o logstash com as seguintes configurações

Entrada:

```
beats {  
    port => 5044  
}
```

Saída:

```
elasticsearch {  
    hosts => [ "elasticsearch:9200" ]  
}
```

```

        index => "seu_nome-%{+YYYY.MM.dd}"
    }

```

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX RESPONDENDO

RESPOSTA:

Dentro da pasta elastic/pipeline configurar o arquivo logstash.conf

```
marco@DESKTOP-G2455QH:~/treinamentos/elastic/pipeline$ sudo vi logstash.conf
```

```
marco@DESKTOP-G2455QH:~/treinamentos/elastic/pipeline$
```

```

input {
  beats {
    port => 5044
  }
}

output {
  stdout {
    codec => "json"
  }
  elasticsearch {
    hosts => ["elasticsearch:9200"]
    index => "marco-%{+yyyy.MM.dd}"
  }
}

```

3. Verificar a quantidade de documentos do índice criado pelo Logstash e visualizar seus 10 primeiros documentos

Dica: Precisamos subir os serviços, docker-compose up -d, olhe a outra dica posteriormente.

```
marco@DESKTOP-G2455QH:~/treinamentos/elastic/pipeline$ docker-compose up -d
```

```
Starting elastic_elasticsearch_1 ... done
```

```
Starting elastic_kibana_1 ... done
```

```
Starting elastic_logstash_1 ... error
```

```

ERROR: for elastic_logstash_1  Cannot start service logstash: OCI runtime create failed: container_linux.go:380: starting container
process caused: process_linux.go:545: container init caused: rootfs_linux.go:76: mounting
"/run/desktop/mnt/host/wsl/docker-desktop-bind-mounts/Ubuntu-20.04/fc54e41936ccc057a8a93d469bcf2242545cbe74d3e19728
1eb86e0002beadcd" to rootfs at "/usr/share/logstash/pipeline/logstash.conf" caused: mount through procfd: no such file or
directory: unknown

```

```

ERROR: for logstash  Cannot start service logstash: OCI runtime create failed: container_linux.go:380: starting container process
caused: process_linux.go:545: container init caused: rootfs_linux.go:76: mounting
"/run/desktop/mnt/host/wsl/docker-desktop-bind-mounts/Ubuntu-20.04/fc54e41936ccc057a8a93d469bcf2242545cbe74d3e19728
1eb86e0002beadcd" to rootfs at "/usr/share/logstash/pipeline/logstash.conf" caused: mount through procfd: no such file or
directory: unknown
ERROR: Encountered errors while bringing up the project.

```

Dica: Esse erro ocorreu pois embora tenhamos parado o serviço, o volume estava montado e fizemos uma alteração em um arquivo que faz parte de sua configuração.

Portanto o correto seria usar o docker-compose down (ao invés de stop), não fique preocupado pois seu volume continuará existindo, ficará salvo, não será perdido.

```
marco@DESKTOP-G2455QH:~/treinamentos/elastic/pipeline$ docker-compose down
Stopping elastic_kibana_1          ... done
Stopping elastic_elasticsearch_1 ... done
Removing elastic_logstash_1       ... done
Removing elastic_kibana_1         ... done
Removing elastic_elasticsearch_1 ... done
Removing network elastic_elastic
marco@DESKTOP-G2455QH:~/treinamentos/elastic/pipeline$ docker-compose up -d
Creating network "elastic_elastic" with driver "bridge"
Creating elastic_elasticsearch_1 ... done
Creating elastic_kibana_1         ... done
Creating elastic_logstash_1       ... done
marco@DESKTOP-G2455QH:~/treinamentos/elastic/pipeline$
```

Indo para pasta do filebeat:

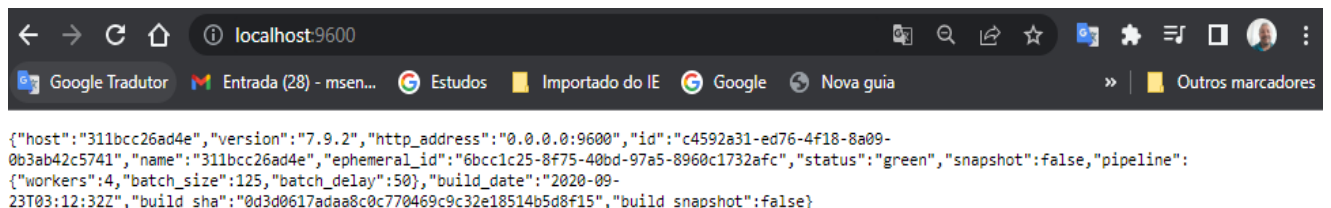
```
marco@DESKTOP-G2455QH:~/treinamentos/elastic/pipeline$ cd ../filebeat-7.9.2-linux-x86_64/
marco@DESKTOP-G2455QH:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64$ ls
LICENSE.txt  README.md  fields.yml  filebeat.reference.yml  kibana  module
NOTICE.txt   data      filebeat   filebeat.yml            logs    modules.d
```

Testando os serviços antes de inicializar

```
marco@DESKTOP-G2455QH:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64$ sudo ./filebeat test config
Config OK
marco@DESKTOP-G2455QH:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64$ sudo ./filebeat test output
logstash: localhost:5044...
connection...
  parse host... OK
  dns lookup... OK
  addresses: 127.0.0.1
  dial up... OK
  TLS... WARN secure connection disabled
  talk to server... OK
marco@DESKTOP-G2455QH:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64$
```

Dica: Podemos observar que a porta que o beat vai enviar usar para enviar os dados para o **logstash: localhost:5044...**

Para saber se o logstash está funcionando, basta no browe chamar localhos:9600



```
{
  "host": "311bcc26ad4e",
  "version": "7.9.2",
  "http_address": "0.0.0.0:9600",
  "id": "c4592a31-ed76-4f18-8a09-0b3ab42c5741",
  "name": "311bcc26ad4e",
  "ephemeral_id": "6bcc1c25-8f75-40bd-97a5-8960c1732afc",
  "status": "green",
  "snapshot": false,
  "pipeline": {
    "workers": 4,
    "batch_size": 125,
    "batch_delay": 50,
    "build_date": "2020-09-23T03:12:32Z",
    "build_sha": "0d3d0617ad4a8c0c770469c9c32e18514b5d8f15",
    "build_snapshot": false
  }
}
```

O mais importante é o **status** está **green** (Ok está funcionando.) Isso garante que está habilitado a receber os dados.

São criadas duas pastas **data** e **logs** automaticamente para garantir que se houver algum problema, ele possa recuperar a posição de onde parou.

```
marco@DESKTOP-G2455QH:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64$ ls
LICENSE.txt  README.md  fields.yml  filebeat.reference.yml  kibana  module
NOTICE.txt   data       filebeat    filebeat.yml            logs    modules.d
```

Como nós já enviamos o arquivo **paris-925.logs**, no exercício anterior, precisamos remover essas pastas para que quando formos reiniciar o filebeat ele recrie novamente e envie o arquivo que vamos trabalhar novamente. Caso contrário provavelmente irá dar um erro.

Removendo as pastas **data** e **log**

```
marco@DESKTOP-G2455QH:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64$ sudo rm -rf data/
```

```
[sudo] password for marco:
```

```
marco@DESKTOP-G2455QH:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64$ sudo rm -rf logs/
```

Verificando

```
marco@DESKTOP-G2455QH:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64$ ls
LICENSE.txt  NOTICE.txt  README.md  fields.yml  filebeat  filebeat.reference.yml  filebeat.yml  kibana  module  modules.d
marco@DESKTOP-G2455QH:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64$
```

```
marco@DESKTOP-G2455QH:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64$ sudo ./filebeat -e
2022-04-01T08:24:24.593-0300 INFO instance/beat.go:640 Home path:
[/home/marco/treinamentos/elastic/filebeat-7.9.2-linux-x86_64] Config path:
[/home/marco/treinamentos/elastic/filebeat-7.9.2-linux-x86_64] Data path:
[/home/marco/treinamentos/elastic/filebeat-7.9.2-linux-x86_64/data] Logs path:
[/home/marco/treinamentos/elastic/filebeat-7.9.2-linux-x86_64/logs]
2022-04-01T08:24:24.599-0300 INFO instance/beat.go:648 Beat ID: ac6a45c9-e62a-4f76-ad16-8ff453e86afe
2022-04-01T08:24:24.731-0300 INFO [seccomp] seccomp/seccomp.go:124 Syscall filter successfully installed
2022-04-01T08:24:24.731-0300 INFO [beat] instance/beat.go:976 Beat info
{"system_info": {"beat": {"path": {"config": "/home/marco/treinamentos/elastic/filebeat-7.9.2-linux-x86_64", "data":
"/home/marco/treinamentos/elastic/filebeat-7.9.2-linux-x86_64/data", "home":
"/home/marco/treinamentos/elastic/filebeat-7.9.2-linux-x86_64", "logs":
"/home/marco/treinamentos/elastic/filebeat-7.9.2-linux-x86_64/logs"}, "type": "filebeat", "uuid":
"ac6a45c9-e62a-4f76-ad16-8ff453e86afe"}}}
2022-04-01T08:24:24.732-0300 INFO [beat] instance/beat.go:985 Build info
{"system_info": {"build": {"commit": "2ab907f5ccec9fd82fe37105082e89fd871f684", "libbeat": "7.9.2", "time":
"2020-09-22T23:19:45.000Z", "version": "7.9.2"}}}
2022-04-01T08:24:24.732-0300 INFO [beat] instance/beat.go:988 Go runtime info
{"system_info": {"go": {"os": "linux", "arch": "amd64", "max_procs": 4, "version": "go1.14.7"}}}
2022-04-01T08:24:24.733-0300 INFO [beat] instance/beat.go:992 Host info
{"system_info": {"host":
{"architecture": "x86_64", "boot_time": "2022-03-31T16:01:36-03:00", "containerized": false, "name": "DESKTOP-G2455QH", "ip": ["127.0.0.1/8", "::1/128", "172.19.190.80/20", "fe80::215:5dff:fe3d:1ee7/64"], "kernel_version": "5.10.16.3-microsoft-standard-WSL2", "mac": ["aa:74:a1:84:5e:e2", "4a:4a:24:cf:68:af", "00:15:5d:3d:1e:e7"], "os": {"family": "debian", "platform": "ubuntu", "name": "Ubuntu", "version": "20.04.3 LTS (Focal Fossa)", "major": 20, "minor": 4, "patch": 3, "codename": "focal"}, "timezone": "-03", "timezone_offset_sec": -10800}}}
2022-04-01T08:24:24.733-0300 INFO [beat] instance/beat.go:1021 Process info
{"system_info": {"process": {"capabilities":
{"inheritable": null, "permitted": ["chown", "dac_override", "dac_read_search", "fowner", "fsetid", "kill", "setgid", "setuid", "setpcap", "linux_immutable", "net_bind_service", "net_broadcast", "net_admin", "net_raw", "ipc_lock", "ipc_owner", "sys_module", "sys_rawio", "sys_chroot", "sys_ptrace", "sys_pacct", "sys_admin", "sys_boot", "sys_nice", "sys_resource", "sys_time", "sys_tty_config", "mknod", "lease", "audit_write", "audit_control", "setfcap", "mac_override", "mac_admin", "syslog", "wake_alarm", "block_suspend", "audit_read", "38", "39", "40"], "effective": ["chown", "dac_override", "dac_read_search", "fowner", "fsetid", "kill", "setgid", "setuid", "setpcap", "linux_immutable", "net_bind_service", "net_broadcast", "net_admin", "net_raw", "ipc_lock", "ipc_owner", "sys_module", "sys_rawio", "sys_chroot", "sys_ptrace", "sys_pacct", "sys_admin", "sys_boot", "sys_nice", "sys_resource", "sys_time", "sys_tty_config", "mknod", "lease", "audit_write", "audit_control", "setfcap", "mac_override", "mac_admin", "syslog", "wake_alarm", "block_suspend", "audit_read", "38", "39", "40"], "bounding": ["chown", "dac_override", "dac_read_search", "fowner", "fsetid", "kill", "setgid", "setuid", "setpcap", "linux_immutable", "net_bind_service", "net_broadcast", "net_admin", "net_raw", "ipc_lock", "ipc_owner", "sys_module", "sys_rawio", "sys_chroot", "sys_ptrace", "sys_pacct", "sys_admin", "sys_boot", "sys_nice", "sys_resource", "sys_time", "sys_tty_config", "mknod", "lease", "audit_write", "audit_control", "setfcap", "mac_override", "mac_admin", "syslog", "wake_alarm", "block_suspend", "audit_read", "38", "39", "40"], "ambient": null}, "cwd":
```

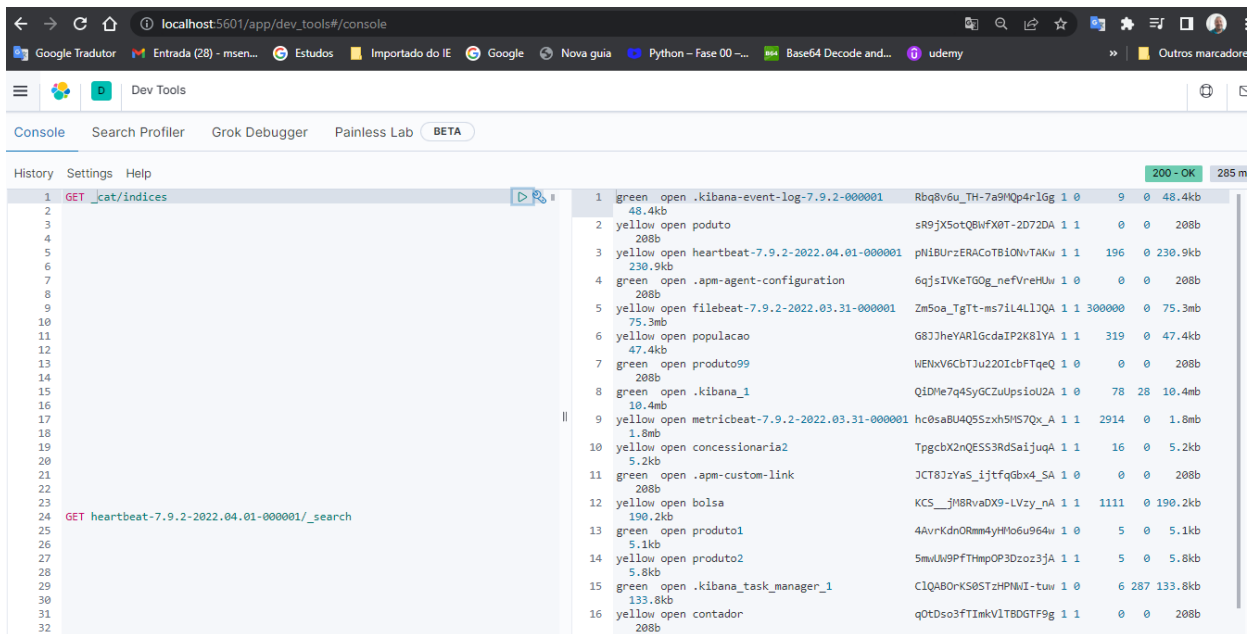
```

"/home/marco/treinamentos/elastic/filebeat-7.9.2-linux-x86_64", "exe":
"/home/marco/treinamentos/elastic/filebeat-7.9.2-linux-x86_64/filebeat", "name": "filebeat", "pid": 1481, "ppid": 1480, "seccomp":
{"mode": "filter", "no_new_privs": true, "start_time": "2022-04-01T08:24:23.550-0300"}}}
2022-04-01T08:24:24.733-0300 INFO instance/beat.go:299 Setup Beat: filebeat; Version: 7.9.2
2022-04-01T08:24:24.734-0300 INFO [publisher] pipeline/module.go:113 Beat name: DESKTOP-G2455QH
2022-04-01T08:24:24.735-0300 WARN beater/filebeat.go:178 Filebeat is unable to load the Ingest Node pipelines for the
configured modules because the Elasticsearch output is not configured/enabled. If you have already loaded the Ingest Node pipelines
or are using Logstash pipelines, you can ignore this warning.
2022-04-01T08:24:24.735-0300 INFO [monitoring] log/log.go:118 Starting metrics logging every 30s
2022-04-01T08:24:24.735-0300 INFO instance/beat.go:450 filebeat start running.
2022-04-01T08:24:24.740-0300 INFO memlog/store.go:119 Loading data file of
'/home/marco/treinamentos/elastic/filebeat-7.9.2-linux-x86_64/data/registry/filebeat' succeeded. Active transaction id=0
2022-04-01T08:24:24.740-0300 INFO memlog/store.go:124 Finished loading transaction log file for
'/home/marco/treinamentos/elastic/filebeat-7.9.2-linux-x86_64/data/registry/filebeat'. Active transaction id=0
2022-04-01T08:24:24.740-0300 WARN beater/filebeat.go:381 Filebeat is unable to load the Ingest Node pipelines for the
configured modules because the Elasticsearch output is not configured/enabled. If you have already loaded the Ingest Node pipelines
or are using Logstash pipelines, you can ignore this warning.
2022-04-01T08:24:24.740-0300 INFO [registrar] registrar/registrar.go:109
States Loaded from registrar: 0
2022-04-01T08:24:24.741-0300 INFO [crawler] beater/crawler.go:71 Loading Inputs: 1
2022-04-01T08:24:24.741-0300 INFO log/input.go:157 Configured paths:
[/home/marco/treinamentos/elastic/dataset/paris-925.logs]
2022-04-01T08:24:24.741-0300 INFO [crawler] beater/crawler.go:141 Starting input (ID: 6083233558314642369)
2022-04-01T08:24:24.741-0300 INFO [crawler] beater/crawler.go:108 Loading and starting Inputs completed.
Enabled inputs: 1
2022-04-01T08:24:24.741-0300 INFO cfgfile/reload.go:164 Config reloader started
2022-04-01T08:24:24.742-0300 INFO log/harvester.go:299 Harvester started for file:
/home/marco/treinamentos/elastic/dataset/paris-925.logs
2022-04-01T08:24:24.742-0300 INFO cfgfile/reload.go:224 Loading of config files completed.
2022-04-01T08:24:27.602-0300 INFO [add_cloud_metadata] add_cloud_metadata/add_cloud_metadata.go:89
add_cloud_metadata: hosting provider type not detected.
2022-04-01T08:24:27.712-0300 INFO [publisher_pipeline_output] pipeline/output.go:143
Connecting to backoff(async(tcp://localhost:5044))
2022-04-01T08:24:27.712-0300 INFO [publisher] pipeline/retry.go:219 retryer: send unwait signal to consumer
2022-04-01T08:24:27.712-0300 INFO [publisher] pipeline/retry.go:223 done
2022-04-01T08:24:27.713-0300 INFO [publisher_pipeline_output] pipeline/output.go:151
Connection to backoff(async(tcp://localhost:5044)) established

```

Dica: Comando para verificar todos os indices existentes

GET _cat/indices



Dica: Se acrescentarmos ?v é exibido o cabeçalho.
GET _cat/indices?v

History Settings Help			200 - OK	191 ms
1	GET _cat/indices?v			
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
32				

Pronto já está enviando os dados para logstash

Resposta:

GET marco-2022.04.01/_count

```
1 GET marco-2022.04.01/_count
2
3
4
5
6
7
8
9
10
11
12
13
14
```

```
1 {
2   "count" : 304096,
3   "shards" : {
4     "total" : 1,
5     "successful" : 1,
6     "skipped" : 0,
7     "failed" : 0
8   }
9 }
10
```

200 - OK 154 ms

Para visualizar seus 10 primeiros documentos

Resposta

GET marco-2022.04.01/_search

```
1 GET marco-2022.04.01/_search
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
```

```
8   "failed" : 0
9 },
10 "hits" : {
11   "total" : {
12     "value" : 10000,
13     "relation" : "gte"
14   },
15   "max_score" : 1.0,
16   "hits" : [
17     {
18       "_index" : "marco-2022.04.01",
19       "_type" : "_doc",
20       "_id" : "XmJH8BN0nCakwCnHb",
21       "_score" : 1.0,
22       "_source" : {
23         "host" : {
24           "ip" : [
25             "172.19.190.80",
26             "fe80::215:5dff:fe3d:1ee7"
27           ],
28           "architecture" : "x86_64",
29           "hostname" : "DESKTOP-G2455QH",
30           "os" : {
31             "platform" : "ubuntu",
32             "version" : "20.04.3 LTS (Focal Fossa)",
33             "kernel" : "5.10.16.3-microsoft-standard-WSL2",
34             "name" : "Ubuntu",
35             "codename" : "focal",
36             "family" : "debian"
37           },
38           "name" : "DESKTOP-G2455QH",
39           "containerized" : false,
40           "mac" : [
```

200 - OK 1259 ms

```

41 |         "aa:74:a1:84:5e:e2",
42 |         "4a:4a:24:cf:68:af",
43 |         "00:15:5d:3d:1e:e7"
44 ^     ],
45 ^     },
46 ^     "tags" : [
47 |         "beats_input_codec_plain_applied"
48 ^     ],
49 ^     "@timestamp" : "2022-04-01T11:27:02.642Z",
50 ^     "@version" : "1",
51 ^     "message" : "95.167.122.14 - - [04/Sep/2014:11:49:01 +0000] \"GET /style2.css HTTP/1
        .1\" 200 4877 \"http://www.semicomplete.com/articles/openldap-with-saslauthd/\"
        \"Mozilla/5.0 (Windows NT 6.1; rv:27.0) Gecko/20100101 Firefox/27.0\"",
52 ^     "agent" : {
53 |         "id" : "ac6a45c9-e62a-4f76-ad16-8ff453e86afe",
54 |         "type" : "filebeat",
55 |         "version" : "7.9.2",
56 |         "hostname" : "DESKTOP-G2455QH",
57 |         "name" : "DESKTOP-G2455QH",
58 |         "ephemeral_id" : "aaa05ce6-42cf-4f10-b8cd-63fb8c3617d3"
59 ^     },
60 ^     "ecs" : {
61 |         "version" : "1.5.0"
62 ^     },
63 ^     "container" : {
64 |         "id" : "dataset"
65 ^     },
66 ^     "input" : {
67 |         "type" : "log"
68 ^     },
69 ^     "log" : {
70 |         "file" : {
71 |             "path" : "C:\\ProgramData\\Microsoft\\Windows Defender\\Signature\\",
72 |             "offset" : 17978153
73 |         }
74 ^     }
75 ^ }
76 ^ },
77 ^ {
78 |     "_index" : "marco-2022.04.01",
79 |     "_type" : "_doc",
80 |     "_id" : "K2_h5H8BNDnCaKwACnHb",
81 |     "_score" : 1.0,
82 ^     "_source" : {
83 |         "host" : {
84 |             "architecture" : "x86_64",
85 |             "os" : {
86 |                 "platform" : "ubuntu",
87 |                 "kernel" : "5.10.16.3-microsoft-standard-WSL2",
88 |                 "version" : "20.04.3 LTS (Focal Fossa)",
89 |                 "name" : "Ubuntu",
90 |                 "codename" : "focal",
91 |                 "family" : "debian"
92 ^             },
93 |             "hostname" : "DESKTOP-G2455QH",
94 ^             "ip" : [
95 |                 "172.19.190.80",
96 |                 "fe80::215:5dff:fe3d:1ee7"
97 ^             ],
98 |             "name" : "DESKTOP-G2455QH",
99 |             "containerized" : false,
100 ^             "mac" : [
101 |                 "aa:74:a1:84:5e:e2",

```

E continua.....

4. Clicar no botão de Enviar Tarefa, e enviar o texto: ok

