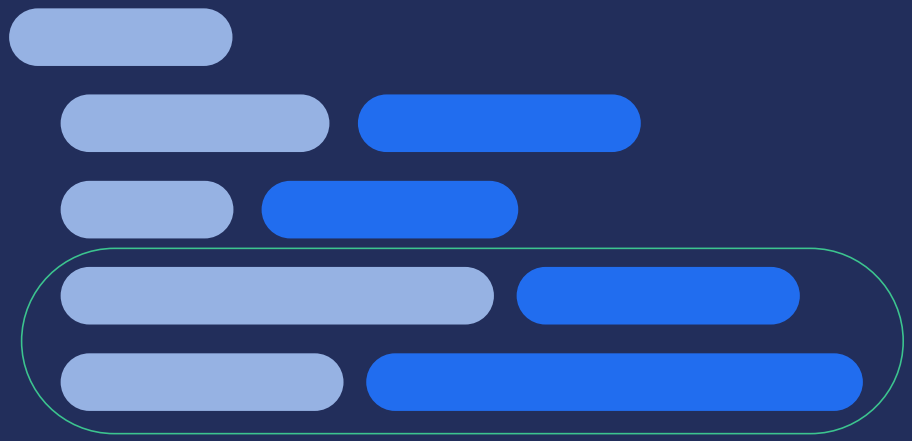
"Mapping Explosions"

"Mapping Explosions"

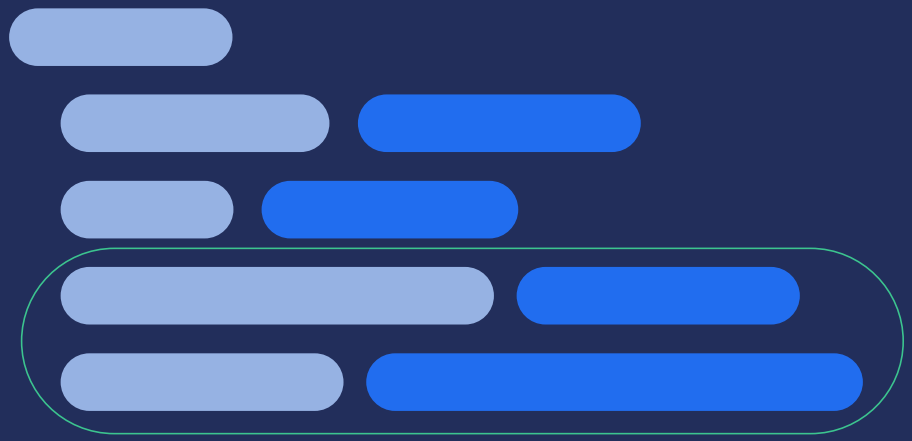


Sundog Education

Coralogix

PROF. FERNANDO AMARAL

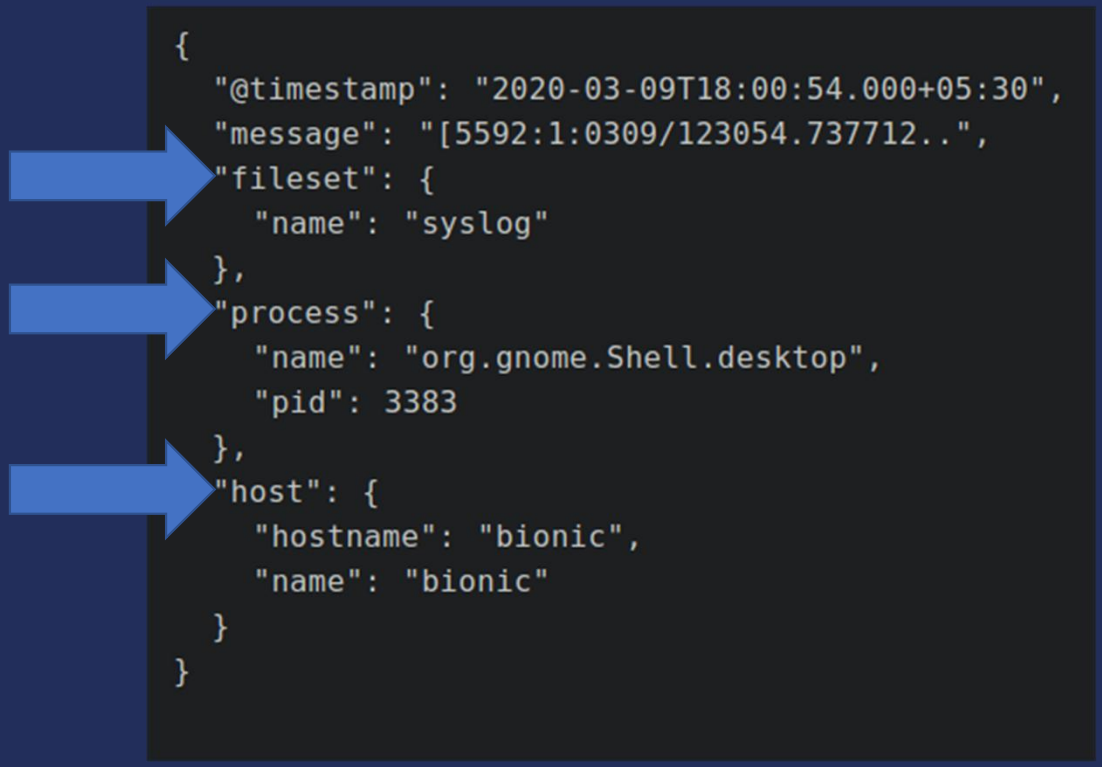
"Mapping Explosions"



TOTAL MAPPINGS

0

Exemplo de log



What Changed?

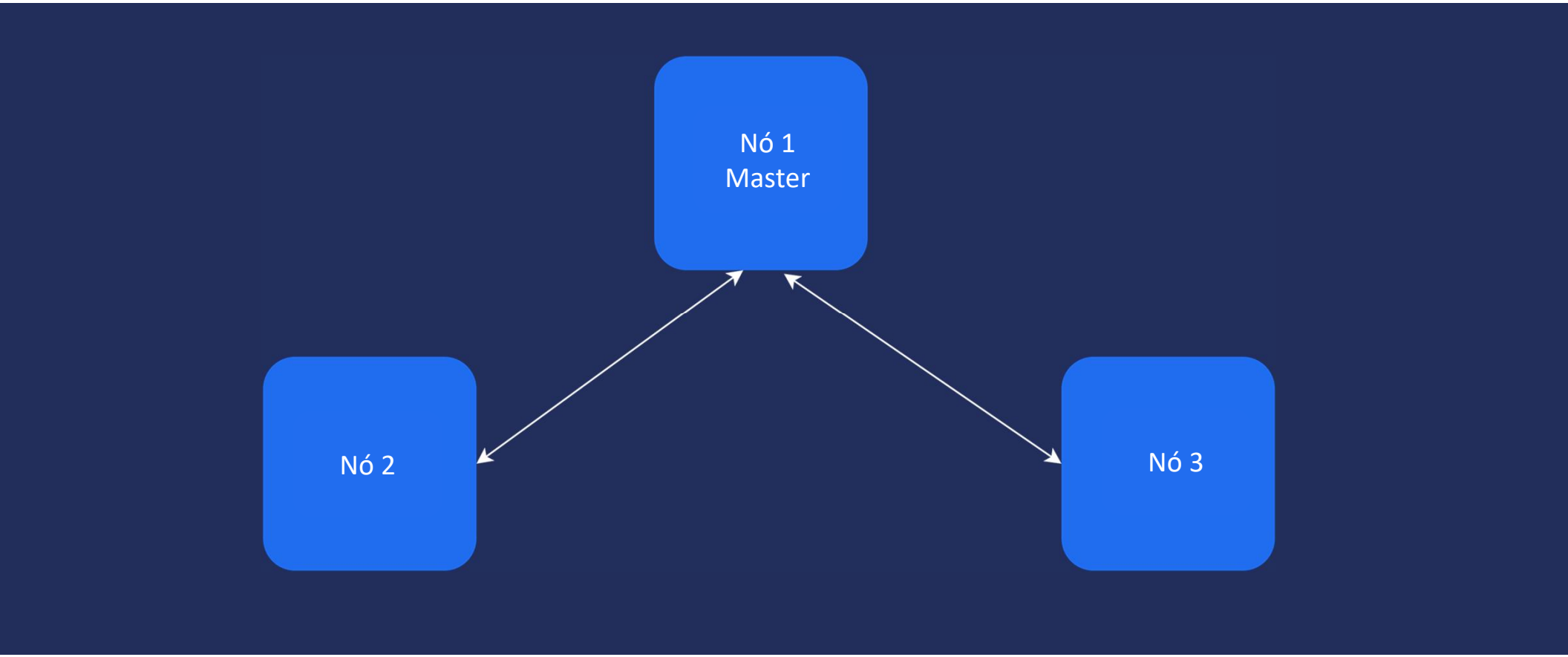
FIRST LOG


```
{
  "@timestamp": "2020-03-09T18:00:54.000+05:30",
  "message": "[5592:1:0309/123054.737712..",
  "fileset": {
    "name": "syslog"
  },
  "process": {
    "name": "org.gnome.Shell.desktop",
    "pid": 3383
  },
  "host": {
    "hostname": "bionic",
    "name": "bionic"
  }
}
```

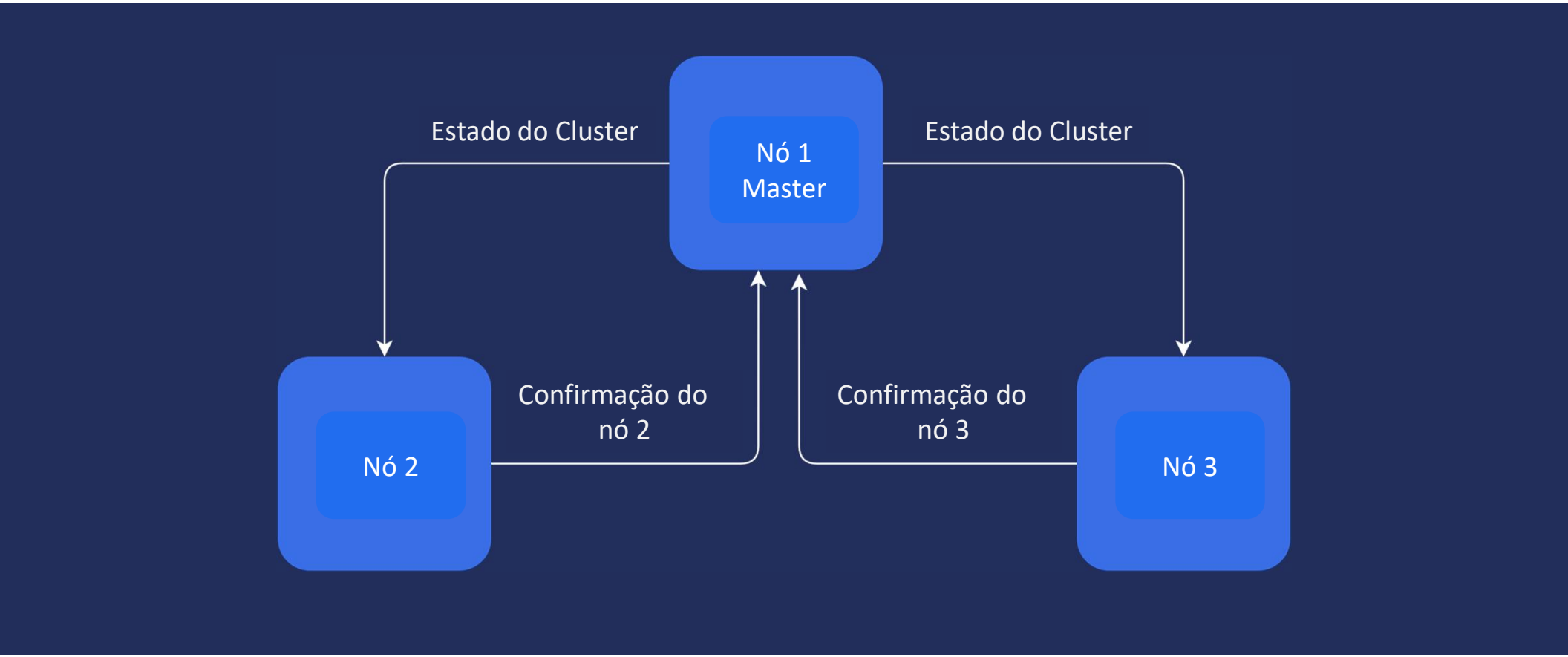

SECOND LOG - with new inner fields


```
{
  "@timestamp": "2020-03-09T18:00:54.000+05:30",
  "message": "[5592:1:0309/123054.737712..",
  "fileset": {
    "name": "syslog"
  },
  "process": {
    "name": "org.gnome.Shell.desktop",
    "pid": 3383
  },
  "host": {
    "hostname": "bionic",
    "name": "bionic",
    "osArchitecture": "x86_64",
    "osVersion": "Bionic Beaver"
  }
}
```

Elasticsearch Cluster



Atualizando o Estado do Cluster



Resumo de Match em Consultas

Texto	Resultado	Motivo
“Bionic Beaver”	Documento retorna com valor de oSVersion como “Bionic Beaver”	Match exato da consulta com o valor do campo host.osVersion
“bionic beaver”	Nenhum document retorna	Diferença nas letras maísculas
“Beaver”	Nenhum document retorna	A consulta tem apenas um token, mas o campo tem “Bionic Beaver”

Tipos de Consultas Suportados pelo tipo Flattened

- term , terms e terms_set
- prefix
- range (operações de intervalos não numéricas)
- match e multi_match (temos que fornecer palavras exatas)
- query_string e simple_query_string
- exists