



DEPLOYMENT

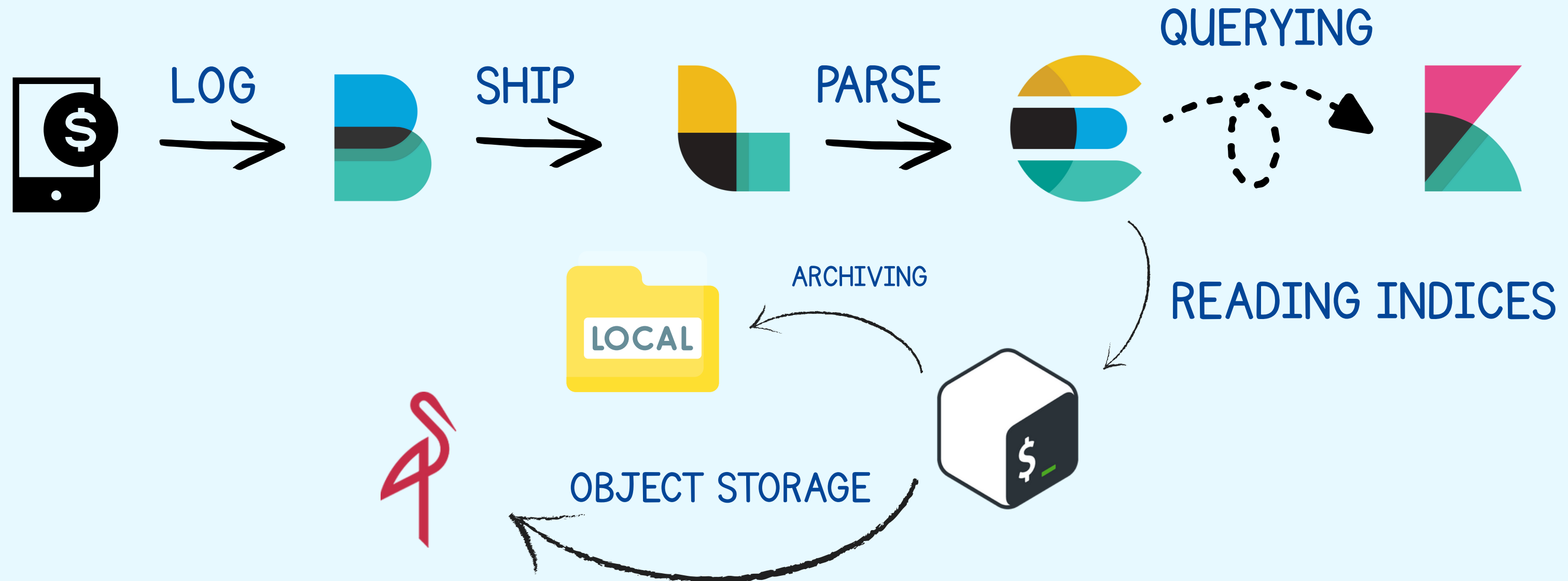
FEATURING   

Presented by Amirhossein Ebrahimzade
(who knows how to quit VIM)

WHY ELK?

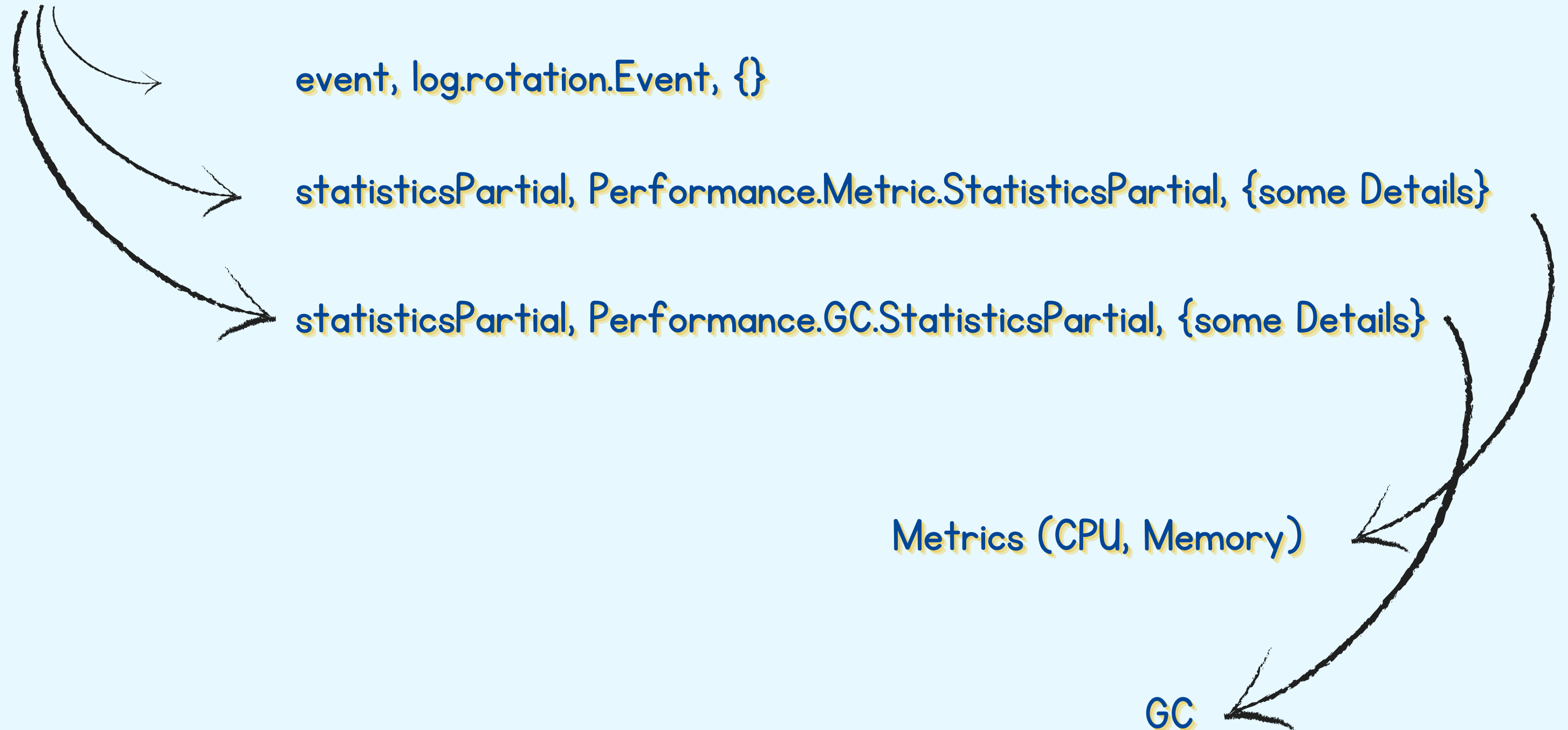
- In modern infrastructures, logs are valuable but massive
- Problem: Long-term log retention explodes storage costs
- Goal: Build a reliable system to collect, visualize, and archive logs efficiently

WHAT WE HAVE HERE? (HLD)



EDBSE & TRACON CONFIGURATION:

- Common Structure, Different in Details:
 - Common points: id, processtag, timestamp, transaction_id, log_type, details, ...
 - Differences: log_type, process_tag, details,



DOCKER COMPOSE:

- Elasticsearch
 - 8.15.0, NoAuth, PV: es_data, Port 9200
- Logstash
 - 8.15.0, Filebeat input, Custom Pipeline, Logstash.conf
- Kibana
 - 8.15.0, GUI, Port Exposed on 5601
- Filebeat
 - 8.15.0, /var/log/*.json Mounted, filebeat.yml
- Elasticdump
 - Custom Image with Local Dockerfile, Dumps indices and Uploads to MinIO, Uses export-and-uplod.sh
- MinIO
 - SelfHosted, Port Exposed on 9000, 9001

SHARED: elk-net(bridge), Health Checks



FILEBEAT CONFIGURATION:

```
filebeat.inputs:  
- type: filestream  
  id: my-json-logs  
  enabled: true  
  paths:  
    - /var/log/elk/*.json
```

Instead of "log", Cause It's improved.

```
  parsers:  
    - multiline:  
      pattern: '^\\{'  
      negate: true  
      match: 'after'
```

Looks for initial {, negates following lines, then completes with }

```
output.logstash:  
  hosts: ["logstash:5044"]
```

Logstash endpoint for shipping logs

LOGSTASH CONFIGURATION:

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

Input from the Filebeat, on endpoint port 5044

```
filter {
  json {
    source => "message"
  }

  date {
    match => [ "timestamp", "ISO8601" ]
    target => "@timestamp"
  }

  mutate {
    remove_field => [ "agent", "ecs", "host", "log", "input", "tags", "message" ]
  }
}
```

Filtering, Timestamp issues, mutation

```
output {
  if [process_tag] == "log.rotation.Event" {
    elasticsearch {
      hosts => ["http://elasticsearch:9200"]
      index => "event-logs-%{+YYYY.MM.dd}"
    }
  } else if [process_tag] == "Performance.GC.StatisticsPartial" {
    elasticsearch {
      hosts => ["http://elasticsearch:9200"]
      index => "gc-logs-%{+YYYY.MM.dd}"
    }
  } else if [process_tag] == "Performance.Metric.StatisticsPartial" {
    elasticsearch {
      hosts => ["http://elasticsearch:9200"]
      index => "metric-logs-%{+YYYY.MM.dd}"
    }
  } else {
    elasticsearch {
      hosts => ["http://elasticsearch:9200"]
      index => "unhandled-logs-%{+YYYY.MM.dd}"
    }
  }
}
```

Indices based on “process_tag”, handles unknown logs via unknown “process_tag” in “unhandled-logs-*”

WHAT WE SEE ON KIBANA:

elastic

Find apps, content, and more.

New Open Share Alerts Inspect Save

event Filter your data using KQL syntax Refresh

Search field names

Available fields 8

- @timestamp
- @version
- event.original
- id
- log_type
- process_tag
- timestamp
- transaction_id

Meta fields 4

Documents (4) Field statistics

Sort fields

```

@timestamp Nov 1, 2023 @ 00:00:06.159 @version 1 event.original { "id": "b4116a78-23fb-4435-98ad-1b8204fad3a7", "process_tag": "log.rotation.Event", "parent_pr
oc": null, "timestamp": "2023-11-01T00:00:06.159358+03:30", "user_name": null, "token_user_name": null, "distributed_transaction_id": null, "transaction_id": "b
4116a78-23fb-4435-98ad-1b8204fad3a7", "request_id": null, "log_type": "event", "user_name_title": null, "token_user_name_title": null, "source_ip_port": null,
"source_ip": null, "source_ip_chain_port": null, "source_ip_chain": null, "origin_ip_port": null, "origin_ip": null, "destination_ip_port": null, "destination_
ip": null, "details": {} } id b4116a78-23fb-4435-98ad-1b8204fad3a7 log_type event process_tag log.rotation.Event timestamp Nov 1, 2023 @ 00:00:06.15
9 transaction_id b4116a78-23fb-4435-98ad-1b8204fad3a7_id -bPmJ5gBIxnET4NM3aUW_ignored event.original.keyword_index event-logs-2023.10.31_score 1

@timestamp Nov 2, 2023 @ 00:00:02.754 @version 1 event.original { "id": "07bbe824-bb5d-445d-a0f9-0a103d573cba", "process_tag": "log.rotation.Event", "parent_pr
oc": null, "timestamp": "2023-11-02T00:00:02.754202+03:30", "user_name": null, "token_user_name": null, "distributed_transaction_id": null, "transaction_id": "0
7bbe824-bb5d-445d-a0f9-0a103d573cba", "request_id": null, "log_type": "event", "user_name_title": null, "token_user_name_title": null, "source_ip_port": null,
"source_ip": null, "source_ip_chain_port": null, "source_ip_chain": null, "origin_ip_port": null, "origin_ip": null, "destination_ip_port": null, "destination_
ip": null, "details": {} } id 07bbe824-bb5d-445d-a0f9-0a103d573cba log_type event process_tag log.rotation.Event timestamp Nov 2, 2023 @ 00:00:02.75
4 transaction_id 07bbe824-bb5d-445d-a0f9-0a103d573cba_id 97PmJ5gBIxnET4NM3aUW_ignored event.original.keyword_index event-logs-2023.11.01_score 1

@timestamp Nov 3, 2023 @ 00:00:14.844 @version 1 event.original { "id": "25b9eccc-3cd6-45c1-99b6-6bd9d11a9749", "process_tag": "log.rotation.Event", "parent_pr
oc": null, "timestamp": "2023-11-03T00:00:14.844183+03:30", "user_name": null, "token_user_name": null, "distributed_transaction_id": null, "transaction_id": "2
5b9eccc-3cd6-45c1-99b6-6bd9d11a9749", "request_id": null, "log_type": "event", "user_name_title": null, "token_user_name_title": null, "source_ip_port": null,
"source_ip": null, "source_ip_chain_port": null, "source_ip_chain": null, "origin_ip_port": null, "origin_ip": null, "destination_ip_port": null, "destination_
ip": null, "details": {} } id 25b9eccc-3cd6-45c1-99b6-6bd9d11a9749 log_type event process_tag log.rotation.Event timestamp Nov 3, 2023 @ 00:00:14.84
4 transaction_id 25b9eccc-3cd6-45c1-99b6-6bd9d11a9749_id -rPmJ5gBIxnET4NM3aUc_ignored event.original.keyword_index event-logs-2023.11.02_score 1

@timestamp Nov 4, 2023 @ 00:00:00.114 @version 1 event.original { "id": "64997a6a-06a1-4ee9-96c7-35acdca3b3e6", "process_tag": "log.rotation.Event", "parent_pr
    
```

Add a field

elastic

Find apps, content, and more.

New Open Share Alerts Inspect Save Refresh

gc Filter your data using KQL syntax

Available fields 23

- @timestamp
- @version
- details.activity
- details.area
- details.fail
- details.full_version
- details.gen0Size
- details.gen1Size
- details.gen2Size
- details.generation
- details.LOHSize
- details.major_version
- details.numberOFCollections
- details.process_name
- details.reason
- details.service_name

Add a field

Documents (76) Field statistics

Document
<pre>@timestamp Nov 1, 2023 @ 00:10:57.912 @version 1 details.activity GC details.area Performance details.fail 0 details.full_version 28.0.4.0 details.gen0Size 12,835,392 details.gen1Size 26,592 details.gen2Size 49,425,448 details.generation 1 details.LOHSize 78,748,208 details.major_version 2 8 details.numberOFCollections 268 details.process_name MSSE.BaseModule details.reason InducedNotForced details.service_name MSSE.BaseModule e details.success 1 event.original { "id": "a4160b96-348f-4d85-947e-9ea4c2f28abf", "process_tag": "Performance.GC.StatisticsPartial", "parent_proc": null, "time stamp": "2023-11-01T00:10:57.912340+03:30", "user_name": null, "token_user_name": null, "distributed_transaction_id": null, "transaction_id": "a4160b96-348f-4d85-947e-9ea4c2f28abf", "request_id": null, "log_type": "statisticsPartial", "user_name.title": null, "token_user_name.title": null, "source_ip.port": null, "source_ip": null, "source_ip_chain.port": null, "source_ip_chain": null, "origin_ip.port": null, "origin_ip": null, "destination_ip.port": null, "destination_ip": null, "details": { "process_name": "MSSE.BaseModule", "service_name": "MSSE.BaseModule", "full_version": "28.0.4.0", "major_version": "28", "area": "Performanc...</pre>
<pre>@timestamp Nov 1, 2023 @ 00:53:58.374 @version 1 details.activity GC details.area Performance details.fail 0 details.full_version 28.0.4.0 details.gen0Size 4,930,224 details.gen1Size 76,848 details.gen2Size 49,425,448 details.generation 0 details.LOHSize 78,748,208 details.major_version 2 8 details.numberOFCollections 269 details.process_name MSSE.BaseModule details.reason InducedNotForced details.service_name MSSE.BaseModule e details.success 1 event.original { "id": "650e9091-bcd8-472a-9945-5497b887dfd5", "process_tag": "Performance.GC.StatisticsPartial", "parent_proc": null, "time stamp": "2023-11-01T00:53:58.374609+03:30", "user_name": null, "token_user_name": null, "distributed_transaction_id": null, "transaction_id": "650e9091-bcd8-472a-9945-5497b887dfd5", "request_id": null, "log_type": "statisticsPartial", "user_name.title": null, "token_user_name.title": null, "source_ip.port": null, "source_ip": null, "source_ip_chain.port": null, "source_ip_chain": null, "origin_ip.port": null, "origin_ip": null, "destination_ip.port": null, "destination_ip": null, "details": { "process_name": "MSSE.BaseModule", "service_name": "MSSE.BaseModule", "full_version": "28.0.4.0", "major_version": "28", "area": "Performanc...</pre>
<pre>@timestamp Nov 1, 2023 @ 01:24:58.717 @version 1 details.activity GC details.area Performance details.fail 0 details.full_version 28.0.4.0 details.gen0Size 4,778,552 details.gen1Size 121,632 details.gen2Size 49,425,448 details.generation 0 details.LOHSize 78,748,208 details.major_version 2 8 details.numberOFCollections 270 details.process_name MSSE.BaseModule details.reason InducedNotForced details.service_name MSSE.BaseModule e details.success 1 event.original { "id": "72eb59cf-3cb6-4282-956e-2ad19aa8ac7", "process_tag": "Performance.GC.StatisticsPartial", "parent_proc": null, "time stamp": "2023-11-01T01:24:58.717044+03:30", "user_name": null, "token_user_name": null, "distributed_transaction_id": null, "transaction_id": "72eb59cf-3cb6-4282-956e-2ad19aa8ac7", "request_id": null, "log_type": "statisticsPartial", "user_name.title": null, "token_user_name.title": null, "source_ip.port": null, "source_ip": null, "source_ip_chain.port": null, "source_ip_chain": null, "origin_ip.port": null, "origin_ip": null, "destination_ip.port": null, "destination_ip": null, "details": { "process_name": "MSSE.BaseModule", "service_name": "MSSE.BaseModule", "full_version": "28.0.4.0", "major_version": "28", "area": "Performanc...</pre>

Rows per page: 100

Documents (20,788)		Field statistics
Document		
<input type="checkbox"/>	<div> <div>@timestamp Nov 1, 2023 @ 00:00:21.177 @version 1 details.activity Metric details.area Performanc</div> <div>e details.cpuCoreCount 4 details.cpuProcKernel 0 details.cpuProcTotal 0.182 details.cpuProcUser 0.182 details.cpuSysKernel 0.156 details.cpuSysTotal 0.46</div> <div>7 details.cpuSysUser 0.312 details.fail 0 details.full_version 28.0.4.0 details.major_version 28 details.memoryProcGCTotal 153,742,16</div> <div>8 details.memoryProcNonpagedSystem 244,768 details.memoryProcPaged 565,784,576 details.memoryProcPagedSystem 416,384 details.memoryProcPeakPaged 5,622,378,49</div> <div>6 details.memoryProcPeakVirtual 2,223,280,173,056 details.memoryProcPeakWorkingSet 5,511,069,696 details.memoryProcPeakWorkingSetPer 32.0</div> <div>8 details.memoryProcPrivate 565,784,576 details.memoryProcPrivatePer 3.293 details.memoryProcVirtual 2,223,265,210,368 details.memoryProcWorkingSet 406,335,48</div> <div>8 details.memoryProcWorkingSetPer 2.365 details.memorySysFree 11,245,314,048 details.memorySysFreePer 65.458 details.memorySysTotal 17,179,332,60</div> <div>8 details.memorySysUse 5,934,018,560 details.memorySysUsePer 34.542 details.process_name MSSE.BaseModule details.service_name MSSE.BaseModul...</div> </div>	
<input type="checkbox"/>	<div> <div>@timestamp Nov 1, 2023 @ 00:01:21.216 @version 1 details.activity Metric details.area Performanc</div> <div>e details.cpuCoreCount 4 details.cpuProcKernel 0 details.cpuProcTotal 0 details.cpuProcUser 0 details.cpuSysKernel 0.078 details.cpuSysTotal 0.31</div> <div>2 details.cpuSysUser 0.234 details.fail 0 details.full_version 28.0.4.0 details.major_version 28 details.memoryProcGCTotal 154,027,82</div> <div>4 details.memoryProcNonpagedSystem 244,360 details.memoryProcPaged 565,678,080 details.memoryProcPagedSystem 416,384 details.memoryProcPeakPaged 5,622,378,49</div> <div>6 details.memoryProcPeakVirtual 2,223,280,173,056 details.memoryProcPeakWorkingSet 5,511,069,696 details.memoryProcPeakWorkingSetPer 32.0</div> <div>8 details.memoryProcPrivate 565,678,080 details.memoryProcPrivatePer 3.293 details.memoryProcVirtual 2,223,260,491,776 details.memoryProcWorkingSet 406,274,04</div> <div>8 details.memoryProcWorkingSetPer 2.365 details.memorySysFree 11,250,839,552 details.memorySysFreePer 65.491 details.memorySysTotal 17,179,332,60</div> <div>8 details.memorySysUse 5,928,493,056 details.memorySysUsePer 34.509 details.process_name MSSE.BaseModule details.service_name MSSE.BaseModul...</div> </div>	
<input type="checkbox"/>	<div> <div>@timestamp Nov 1, 2023 @ 00:01:51.232 @version 1 details.activity Metric details.area Performanc</div> <div>e details.cpuCoreCount 4 details.cpuProcKernel 0 details.cpuProcTotal 0 details.cpuProcUser 0 details.cpuSysKernel 0.286 details.cpuSysTotal 2.21</div> <div>3 details.cpuSysUser 1.927 details.fail 0 details.full_version 28.0.4.0 details.major_version 28 details.memoryProcGCTotal 154,160,24</div> <div>0 details.memoryProcNonpagedSystem 244,360 details.memoryProcPaged 565,678,080 details.memoryProcPagedSystem 416,384 details.memoryProcPeakPaged 5,622,378,49</div> <div>6 details.memoryProcPeakVirtual 2,223,280,173,056 details.memoryProcPeakWorkingSet 5,511,069,696 details.memoryProcPeakWorkingSetPer 32.0</div> <div>8 details.memoryProcPrivate 565,678,080 details.memoryProcPrivatePer 3.293 details.memoryProcVirtual 2,223,260,491,776 details.memoryProcWorkingSet 406,274,04</div> <div>8 details.memoryProcWorkingSetPer 2.365 details.memorySysFree 11,252,314,112 details.memorySysFreePer 65.499 details.memorySysTotal 17,179,332,60</div> </div>	

ELASTIC DUMP AND MOREOVER:

Docker file:

FROM node:18

RUN npm install -g elasticdump \
 && curl -O https://dl.min.io/client/mc/release/linux-amd64/mc \
 && chmod +x mc && mv mc /usr/local/bin/mc

WORKDIR /dumps

COPY export-and-upload.sh /elasticdump/export-and-upload.sh

RUN chmod +x /elasticdump/export-and-upload.sh

CMD ["/bin/bash", "/elasticdump/export-and-upload.sh"]

export-and-uplod.sh

```
#!/bin/bash

ES_HOST="http://elasticsearch:9200"
MINIO_BUCKET="elk-exports"
EXPORT_DIR="/dumps"
PATTERNS=("event-logs-" "gc-logs-" "metric-logs-")

export_to_minio() {
  for PREFIX in "${PATTERNS[@]"; do
    INDICES=$(curl -s "$ES_HOST/_cat/indices?h=index" | grep "^${PREFIX}")

    for INDEX in $INDICES; do
      FILE="$EXPORT_DIR/${INDEX}.json.gz"
      if [[ -f "$FILE" ]]; then
        echo "[SKIP] $INDEX already exported"
        continue
      fi

      echo "[EXPORT] Dumping $INDEX"
      elasticdump --input="$ES_HOST/${INDEX}" --output="$EXPORT_DIR/${INDEX}.json" --type=data
      gzip -f "$EXPORT_DIR/${INDEX}.json"


      echo "[UPLOAD] Uploading $INDEX to MinIO"
      mc alias set minio http://minio:9000 minioadmin minio12345678@
      mc mb -q --ignore-existing minio/$MINIO_BUCKET
      mc cp "$FILE" minio/$MINIO_BUCKET/
    done
  done
}

# Loop forever
while true; do
  export_to_minio
  echo "[WAIT] Sleeping for a minute..."
  sleep 60
done
```


MINIO:

Why Minio?

- S3 Compatibility
- Local Backup Storage
- Fast and Easy Deployment
- Reliable & Scalable
- Powerful CLI tool (MC)

 **elk-exports**

Created on: Sun, Jul 20 2025 16:25:10 (GMT+3:30) Access: PRIVATE 1.8 MiB - 14 Objects










Rewind ↺

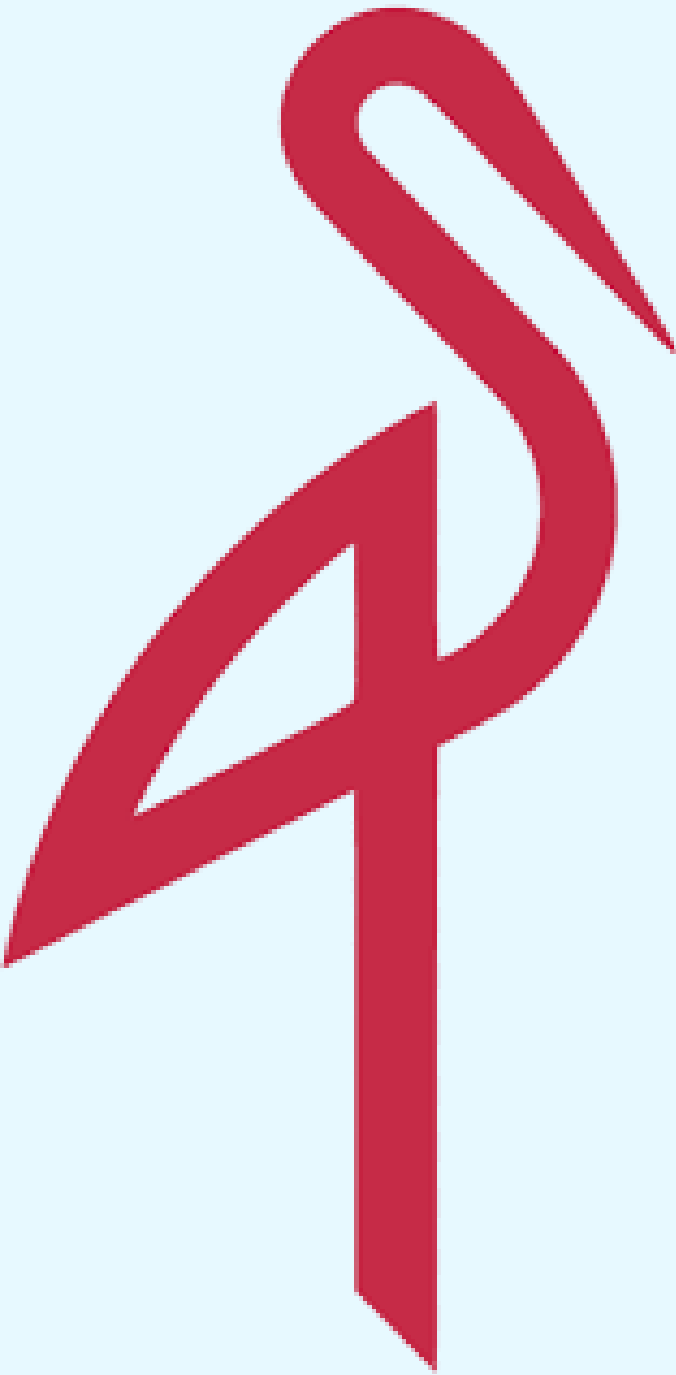
Refresh ↻

Upload ↗

< elk-exports

Create new path .//

<input type="checkbox"/> ▲ Name	Last Modified	Size
<input type="checkbox"/>  event-logs-2023.10.31.json.gz	Sun, Jul 20 2025 16:25 (GMT+3:30)	532.0 B
<input type="checkbox"/>  event-logs-2023.11.01.json.gz	Sun, Jul 20 2025 16:25 (GMT+3:30)	527.0 B
<input type="checkbox"/>  event-logs-2023.11.02.json.gz	Sun, Jul 20 2025 16:25 (GMT+3:30)	530.0 B
<input type="checkbox"/>  event-logs-2023.11.03.json.gz	Sun, Jul 20 2025 16:25 (GMT+3:30)	527.0 B
<input type="checkbox"/>  gc-logs-2023.10.31.json.gz	Sun, Jul 20 2025 16:25 (GMT+3:30)	1.3 KiB
<input type="checkbox"/>  gc-logs-2023.11.01.json.gz	Sun, Jul 20 2025 16:25 (GMT+3:30)	1.1 KiB
<input type="checkbox"/>  gc-logs-2023.11.02.json.gz	Sun, Jul 20 2025 16:25 (GMT+3:30)	1.2 KiB
<input type="checkbox"/>  gc-logs-2023.11.03.json.gz	Sun, Jul 20 2025 16:25 (GMT+3:30)	1.1 KiB
<input type="checkbox"/>  gc-logs-2023.11.04.json.gz	Sun, Jul 20 2025 16:27 (GMT+3:30)	1.8 KiB



FUTURE IMPROVEMENTS (PRODUCTION READY):

- Security Enhancements, env variables or secret managers
- Data Handling & Storage (ILM)
- Alerting Modules
- Move to K8S, Using Helm charts
- Automating Backups using CronJobs

THANKS FOR WATCHING! :D