



---

# USO DE ELASTICK STACK

---

PRÁCTICA 3.4 | PARTE 1

ERIC SERRANO MARÍN  
INCIDENTES DE CIBERSEGURIDAD

## Contenido

ENUNCIADO.....	2
1. Crea un patrón de índice.....	2
2. Crea una regla de detección. ....	3
3. Haz una búsqueda de información en la pantalla de logs (Discover): Configura una vista con 4 columnas que contengan información y haz una consulta con al menos 2 parámetros. ....	4
4. Crea un tablero con 3 gráficas de diferente tipo, donde al menos una de las gráficas muestra información de 2 parámetros conjuntamente.....	5

# ENUNCIADO

En esta práctica vamos a hacer uso de Elastic Stack para revisar los datos recogidos por el módulo en los puntos finales, tratados por Logstack y almacenados en Elastic Search.

## 1. Crea un patrón de índice.

### Index patterns

Create and manage the index patterns that help you retrieve your data from Elasticsearch.

Search...

Pattern ↑

logs-\*

Default

### Create index pattern

Name

logs\*

Use an asterisk (\*) to match multiple characters. Spaces and the characters , / ? , " < , > , | are not allowed.

Timestamp field

@timestamp

Select a timestamp field for use with the global time filter.

[Show advanced settings](#)

✓ Your index pattern matches 17 sources.

logs-elastic\_agent-default

Data stream

logs-elastic\_agent.endpoint\_security-default

Data stream

logs-elastic\_agent.filebeat-default

Data stream

logs-elastic\_agent.fleet\_server-default

Data stream

logs-elastic\_agent.metricbeat-default

Data stream

Ya se nos ha creado

## logs\*

Time field: '@timestamp'

View and edit fields in logs\*. Field attributes, such as type and searchability, are based on [field mappings](#) in Elasticsearch.

Fields (1556)

Scripted fields (0)

Field filters (0)

Search

All field types

Add field

Name ↑	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date				
Endpoint.policy.applied.artifacts.global.identifiers.name	keyword				Activar Windows Ve a Configuración para activar Windows.

## 2. Crea una regla de detección.

**elastic** Search Elastic

Stack Management Rules

**Data**

- Index Management
- Index Lifecycle Policies
- Snapshot and Restore
- Rollup Jobs
- Transforms
- Remote Clusters
- Alerts and Insights**
- Rules and Connectors**
- Reporting

## Rules and Connectors

Detect conditions using rules, and take actions using connectors

**Rules** **Connectors**

**Create rule** Search

Showing: 10 of 623 rules. Active: 0 Error: 0 Ok: 5

### Create rule

**Name**

Prueba

**Tags (optional)**

**Check every**

1 minute

**Notify**

Only on status change

### Error count threshold

Alert when the number of errors in a service exceeds a defined threshold. [Documentation](#)

Cancel Activar Windows Ve a Configuración para activar Windows. Save

Rules

Connectors

Create rule

Prueba

×

Type 0 ▾

Action type 0 ▾

Status 0

Showing: 1 of 1 rules.   ● Active: 0   ● Error: 0   ● Ok: 1   ● Pending: 0   ● Unknown: 0

<input type="checkbox"/>	Ena...	Name ↑	Last run ②	Inter...	Duration ②	Status
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Prueba Error count threshold	Feb 7, 2024 16:58:58pm a few seconds ago	1 min	00:00:00.159	● Ok

Activar Wind

3. Haz una búsqueda de información en la pantalla de logs (Discover):  
Configura una vista con 4 columnas que contengan información y haz una consulta con al menos 2 parámetros.

Vista con cuatro columnas.

logs-\*

230,118 hits

Chart options

host

Filter by type 0 ▾

host.os.Ext.variant

host.os.family

host.os.full

host.os.name

host.os.platform

host.os.type

req.LocalMeta.host.architecture

req.LocalMeta.host.hostname

req.LocalMeta.host.id

req.LocalMeta.host.ip

Time ↓

host.hostname

host.ip

host.os.version

> Feb 2, 2022 @ 12:48:35.835	CentOS	192.168.122.1, 127.0.0.1, ::1, 192.168.30.10, fe80::20c:29ff:fe54:eba	8.5.2111
> Feb 2, 2022 @ 12:48:35.834	CentOS	192.168.122.1, 127.0.0.1, ::1, 192.168.30.10, fe80::20c:29ff:fe54:eba	8.5.2111
> Feb 2, 2022 @ 12:48:35.833	CentOS	192.168.122.1, 127.0.0.1, ::1, 192.168.30.10, fe80::20c:29ff:fe54:eba	8.5.2111
> Feb 2, 2022 @ 12:48:35.827	CentOS	192.168.122.1, 127.0.0.1, ::1, 192.168.30.10, fe80::20c:29ff:fe54:eba	8.5.2111

Activar Windows

Consulta con dos parámetros.

host.ip = 192.168.122.1 and host.os.version = 10.0

KQL

Jan 8, 2022 @ 12:06:15.766 → Feb 12, 2022 @ 16:11:28.503

logs-\*

90 hits

Chart options

host

Filter by type 0 ▾

Selected fields 3

Available fields 11

Popular

Time ↓

host.hostname

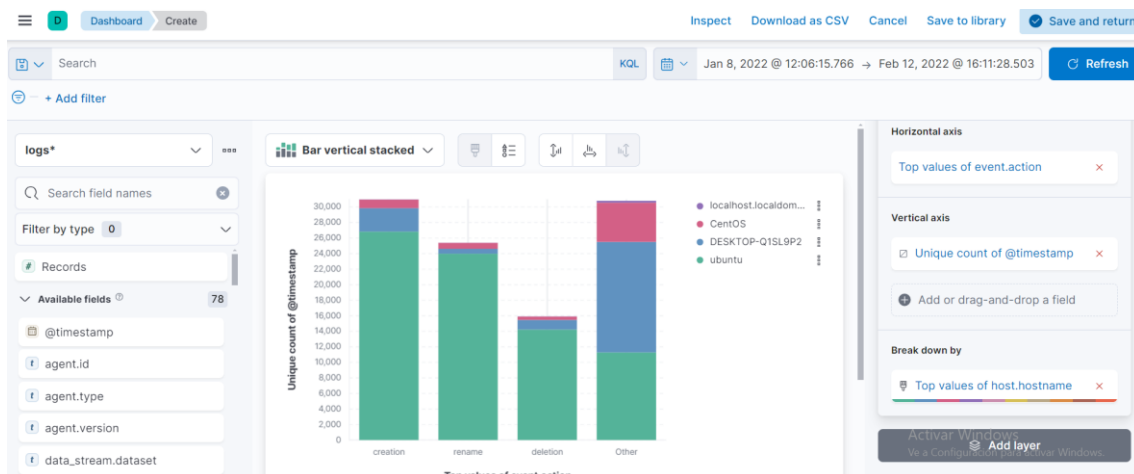
host.ip

host.os.version

> Jan 31, 2022 @ 16:29:15.784	DESKTOP-Q1SL9P2	fe80::80fc:1377:52fb:977e, 192.168.10.10	10.0
> Feb 1, 2022 @ 16:49:05.565	DESKTOP-Q1SL9P2	fe80::80fc:1377:52fb:977e, 192.168.10.10	10.0
> Feb 1, 2022 @ 16:49:05.565	DESKTOP-Q1SL9P2	fe80::80fc:1377:52fb:977e, 192.168.10.10	10.0
> Feb 1, 2022 @ 16:49:05.564	DESKTOP-Q1SL9P2	fe80::80fc:1377:52fb:977e, 192.168.10.10	10.0
> Feb 1, 2022 @ 16:49:05.564	DESKTOP-Q1SL9P2	fe80::80fc:1377:52fb:977e, 192.168.10.10	10.0

Activar Windows

#### 4. Crea un tablero con 3 gráficas de diferente tipo, donde al menos una de las gráficas muestra información de 2 parámetros conjuntamente.



Esta gráfica proporcionaría una visión detallada de cómo se distribuyen diferentes tipos de eventos para cada acción principal en tu conjunto de datos.

