X-PACK
ALERTING

ALERTING

Ayuda a generar una serie de acciones si se cumplen condiciones en los datos.

Útil para alertar de cambios o anomalías en los datos, ya preestablecidos por el administrador.

1.

INTRODUCCIÓN

INTRODUCCIÓN

X-Pack proporciona una API para crear, gestionar, probar y borrar *watches*. Un *watch* es una alerta y puede contener múltiples acciones de notificación. Se compone de 4 partes:

- **Schedule.** Programar cada cuánto se va a ejecutar las consultas para que sean evaluadas por la condición.

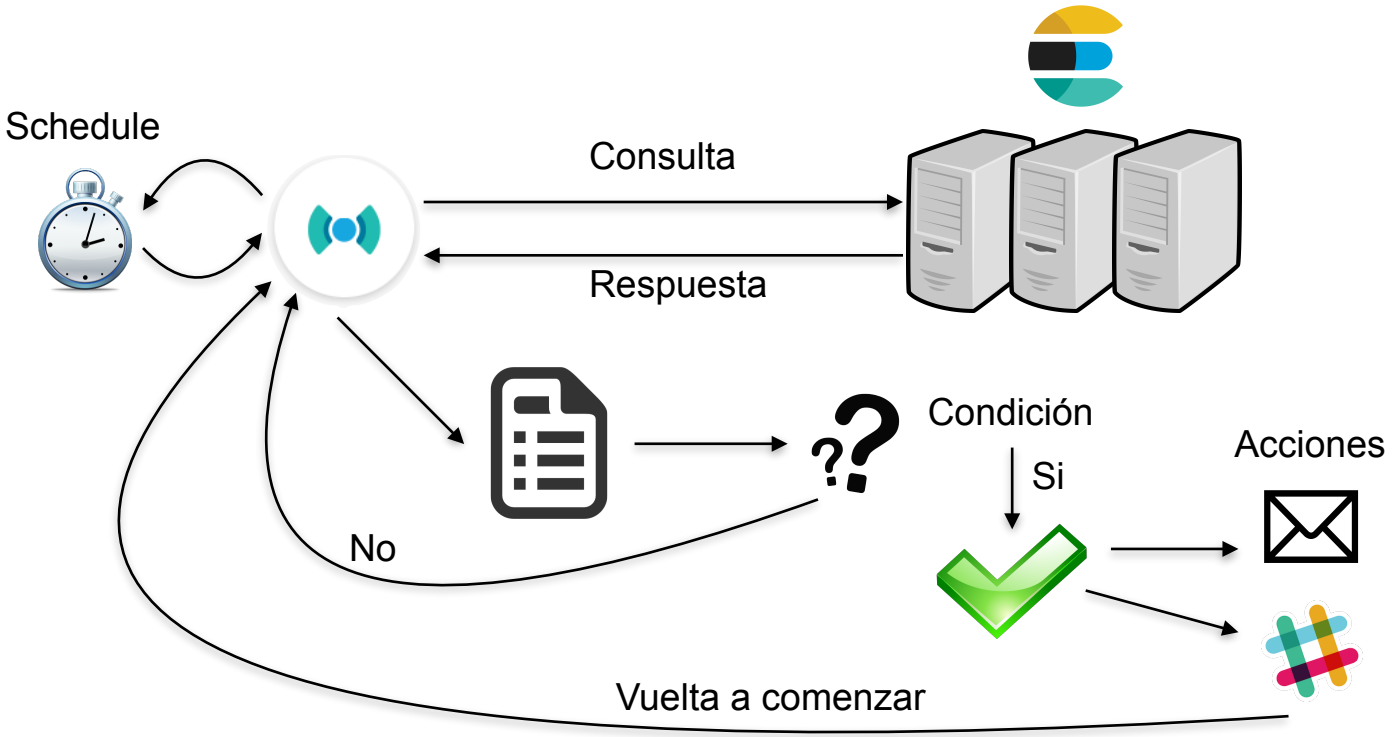
- **Consulta.** Consulta a ejecutar que será la entrada de la condición.

INTRODUCCIÓN

- **Condición.** Determina cuándo si o no ejecutar las acciones. Se puede usar condiciones simples o scripting para casos de uso más sofisticados.

- **Acciones.** Se pueden ejecutar una o más como: enviar correo, registrarla o usar algún chat como HipChat o Slack.

INTRODUCCIÓN



2.

CREACIÓN DE WATCHERS

CREACIÓN DE WATCHERS

Inputs

Cuando salta el *trigger*, el proceso de *input* mete datos en la ejecución del Watcher. Soporta 4 tipos de entradas:

- *Simple*: carga datos estáticos.
- *Search*: carga los datos de una búsqueda.
- *HTTP*: carga los datos de una consulta HTTP.
- *Chain*: usa una serie de inputs para introducir datos.

CREACIÓN DE WATCHERS

Inputs

```
"input": {
  "search": {
    "request": {
      "indices": "heartbeat-*",
      "types": "http",
      "body": {
        "query": {
          "bool": {
            "should": [
              {"wildcard": { "url": “*172.16.2.23*" }}
] } } } } } }
```

CREACIÓN DE WATCHERS

Triggers

Indica cuándo debe comenzar la ejecución de un watcher, es decir, cada cuánto ejecutarse por ejemplo.

Opciones disponibles:

Hourly, daily, weekly, monthly, yearly, cron, interval.

CREACIÓN DE WATCHERS

Triggers

```
"trigger": {
    "schedule": {
      "interval": "1m"
    }
}
```

CREACIÓN DE WATCHERS

Condiciones

Recoge los datos devueltos en la consulta, los valora con las condiciones y determina si es necesario ejecutar o no las acciones.

Opciones disponibles:

Always, *never*, *compare*, *array_compare* y *script.*

CREACIÓN DE WATCHERS

Condiciones

```
"condition": {
  "compare": {
    "ctx.payload.hits.hits.0._source.up": {
      "eq": "false"
    }
  }
},
```

CREACIÓN DE WATCHERS

Acciones

Cuando se cumple una condición se ejecutará una o más acciones.

Se pueden utilizar las siguiente acciones:

Email, *Webhook*, *Index*, *Logging*, *HipChat*, *Slack*, *PagerDuty*, *Jira*.

CREACIÓN DE WATCHERS

Acciones

```
"actions" : {
  "send_email" : {
  “throttle_period": "15m"
    "email" : {
      "from" : "root@elastic03",
      "to" : “destination@gmail.com",
      "subject" : "ALERT APACHE: Server Down",
      "body" : "Se han detectado eventos de una posible caida del servidor
{{ctx.payload.hits.hits.0._source.url}}  \n  - Hora del evento:
{{ctx.payload.hits.hits.0._source.@timestamp}} \n  - Mensaje:
{{ctx.payload.hits.hits.0._source.error.message}}"
    } } }
```

CREACIÓN DE WATCHERS

Resultado