Integrando nuestro toolbox

Elastic & AppDynamics

🙋‍♂️ Santiago Lator Arias - 2021

¿Quien soy?

Mi nombre es Santiago Lator Arias. Vivo en La Plata, Argentina.

Actualmente soy **Senior Consultant** en **MajorKey Technologies**, desarrollando soluciones de Monitoreo & Observabilidad. Anteriormente me desempeñé como **Team Leader** del equipo de M&O en **BGH Tech Partner**.

Trabajo de manera profesional con el stack de Elastic desde hace aproximadamente 5 años y gran parte de mis actividades con esta tecnología han involucrado la necesidad de integrar con otras plataformas.

¿Por qué hablar de integración?

✅ Las necesidades de nuestros clientes y sus soluciones son cada vez más diversas, es fundamental la posibilidad de integrar nuestro toolbox de manera fácil y transparente.

✅ Necesitamos que nuestras herramientas y plataformas "hablen" entre sí para sacarle el máximo provecho a nuestros datos.

✅ Los distintos y variados ecosistemas de las empresas pueden resultar complejos e imprevisibles a la vez. Por eso, nuestras soluciones deben poder adaptarse de manera creativa a estos desafíos.

Elastic & AppDynamics

Breve definición

¿Qué es Elasticsearch?

Es un **motor de analítica y análisis distribuido** y open source para todos los tipos de datos, incluidos textuales, numéricos, geoespaciales, estructurados y desestructurados.

Elasticsearch permite procesar + almacenar gran cantidad de datos en tiempo real y realizar búsquedas & agregaciones super rápidas de esos datos.

Elastic Stack

Esta compuesto por **Elasticsearch** como núcleo principal y se incorpora un conjunto de herramientas open source y propietarias para la ingesta, el enriquecimiento, el almacenamiento, el análisis y la visualización de datos. El stack básico o esencial está compuesto por:

Beats ⇢ Logstash ⇢ Elasticsearch ⇄ Kibana

Un data shipper que mueve los datos de las máquinas a los otros componentes del stack.

Analiza, transforma y prepara los datos

Ingesta, almacena y procesa los datos.

Interactúa con Elasticsearch, produciendo análisis que muestra en gráficos, tablas, mapas y alarmas (watchers)

¿Qué es AppDynamics?

AppDynamics es una solución APM (Application Performance Monitoring) que utiliza inteligencia artificial (IA) y machine learning para proporcionar visibilidad e insights en tiempo real de entornos IT.

👓 Es parte de la estrategia Full-Stack Observability de CISCO.

🏆 En 2021, por 9° año consecutivo, fue nombrada líder del cuadrante de Gartner para soluciones APM.

APPDYNAMICS

¿Como funciona AppDynamics?

El Controller recibe datos de rendimiento en tiempo real de los agentes de AppDynamics. Los agentes son plug-ins o extensiones que se instalan en todo el ecosistema de la aplicación.

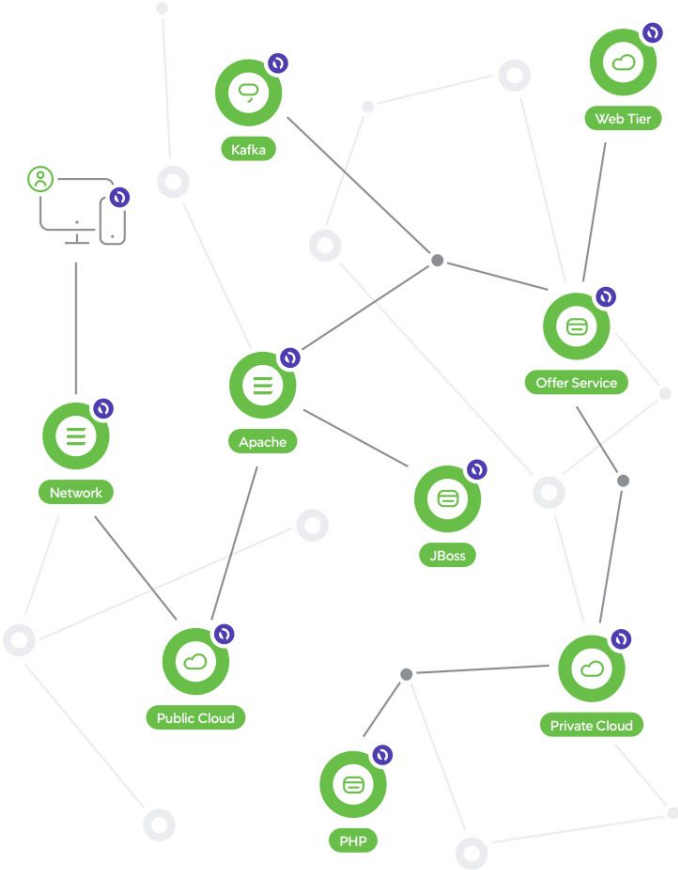
01 | Agentes y Controller

02 | Auto-discovery y Mapping

03 | Business Transactions

04 | Deteccion de anomalias

05 | Diagnóstico de causa raíz



¿Como funciona AppDynamics?

AppDynamics descubre automáticamente el flujo de todas las solicitudes de tráfico del entorno y crea dinámicamente un mapa de topología para visualizar el rendimiento en todo el ecosistema de aplicaciones.

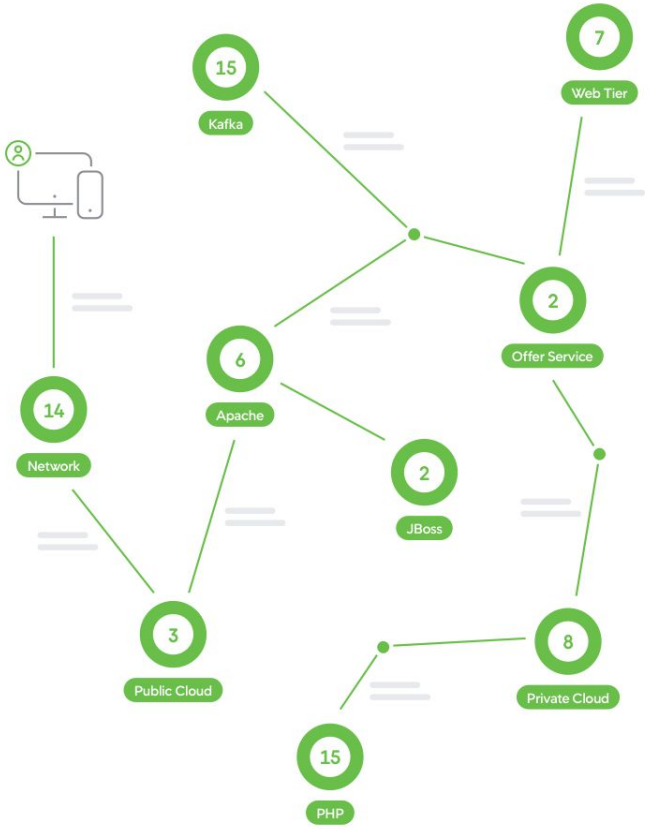
01 | Agentes y Controller

02 | Auto-discovery y Mapping

03 | Business Transactions

04 | Deteccion de anomalias

05 | Diagnóstico de causa raíz



¿Como funciona AppDynamics?

Observa y da soporte a las Business Transactions clave, que se componen de todos los servicios que cumplen y entregan las solicitudes iniciadas por el usuario, como los inicios de sesión, el canasto de compra y los pagos.

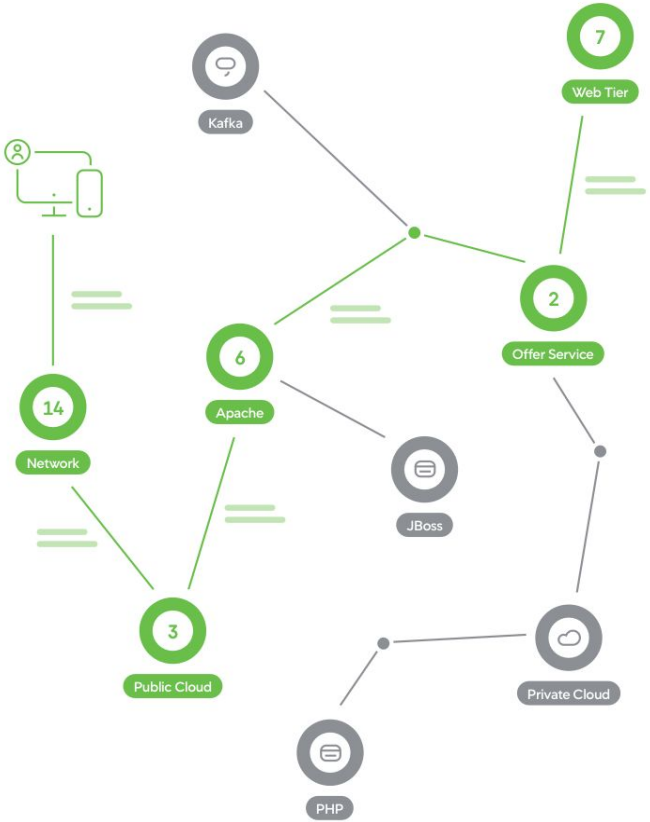
01 | Agentes y Controller

02 | Auto-discovery y Mapping

03 | Business Transactions

04 | Deteccion de anomalias

05 | Diagnóstico de causa raíz



¿Como funciona AppDynamics?

Genera un baseline de rendimiento y establece alertas para identificar y resolver los problemas antes de que sus clientes o empleados se den cuenta.

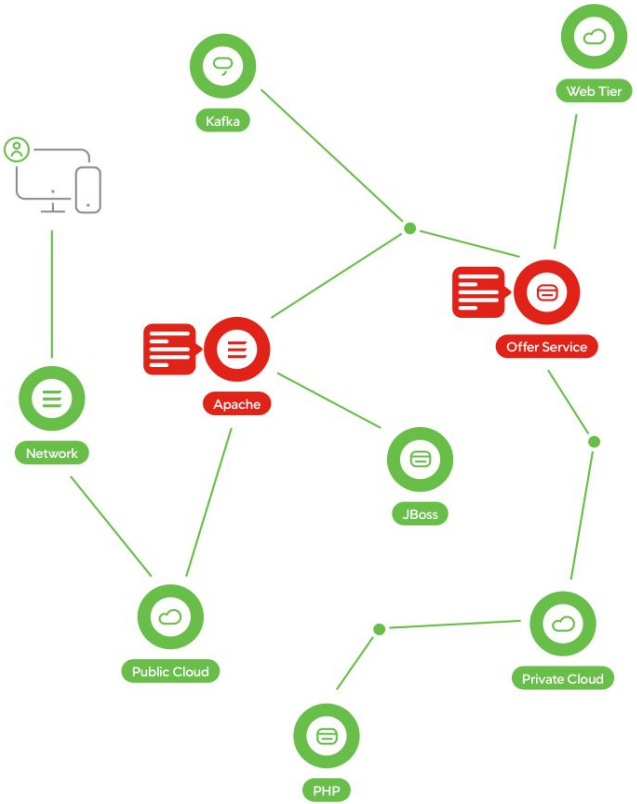
01 | Agentes y Controller

02 | Auto-discovery y Mapping

03 | Business Transactions

04 | Deteccion de anomalias

05 | Diagnóstico de causa raíz



¿Como funciona AppDynamics?

Prioriza la reducción del tiempo medio de resolución (MTTR) con información que ayude a los equipos de IT a priorizar y resolver las Business Transactions más problemáticas, antes de que afecten a la experiencia del usuario.

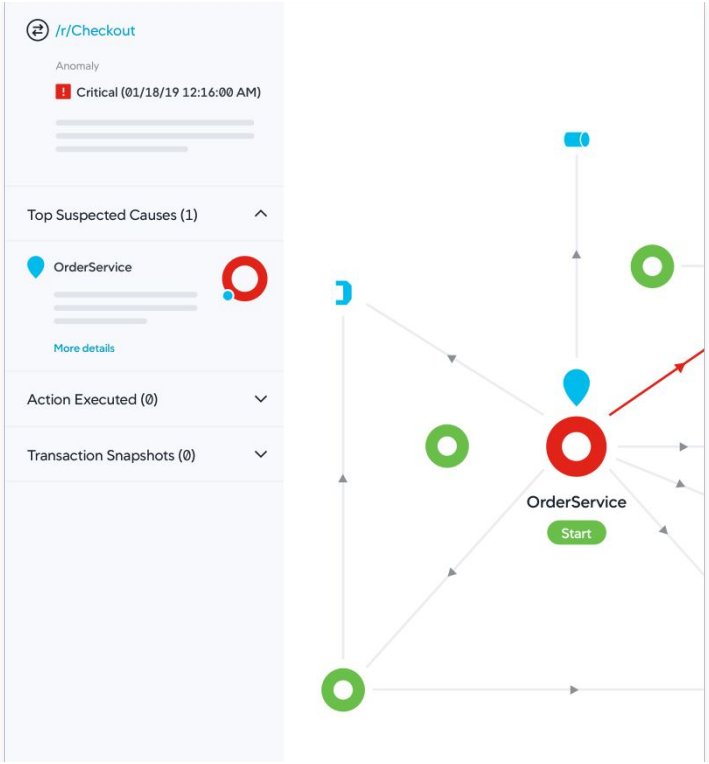
01 | Agentes y Controller

02 | Auto-discovery y Mapping

03 | Business Transactions

04 | Deteccion de anomalias

05 | Diagnóstico de causa raíz



Caso de uso

Cliente

Una de las entidades bancarias más grandes de Argentina con +100 años de actividad.

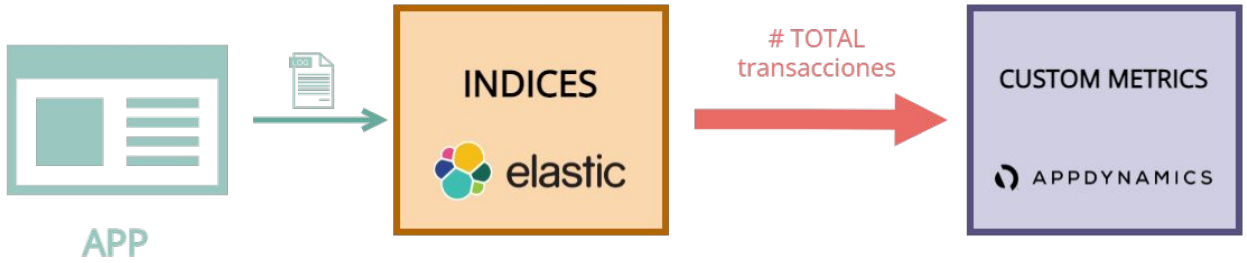
Se estima que tiene más de 6000 empleados en sus distintas unidades.

Reconocido internacionalmente por su programa de transformación digital.

Metodologías ágiles en gran parte de sus proyectos y equipos.

Requerimiento

Enviar información (# total transacciones) contenida en indices de Elastic a AppDynamics para ser consumida como custom metrics



Alternativas evaluadas

1) Conector/ plugin oficial

❌ No existe desarrollo para queries, solo una extensión para obtener info de las cat APIs

2) Levantar logs desde AppDynamics

❌ No se cuenta con la licencia requerida y no es una opción adquirirla.

❌ Requiere replantear la estrategia de logging, no es posible destinar tiempo.

3) Script - Consumo de API

❌ Mantenimiento

❌ Tiempos de desarrollo

4) Utilizar el Event Services (Elasticsearch backend)

❌ Más pasos = más puntos de falla

❌ Tiene cierto delay

5) Watcher + Listener

✅ Implica solo 2 componentes principales

✅ El procesamiento lo realiza todo Elastic

✅ Mantenimiento desde UI

Diagrama de la propuesta

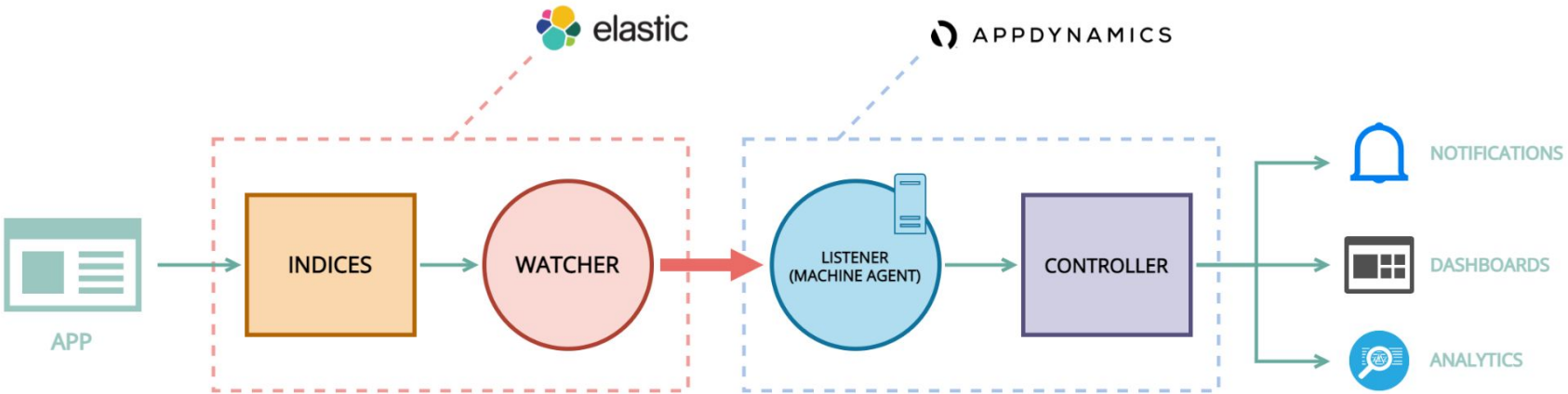
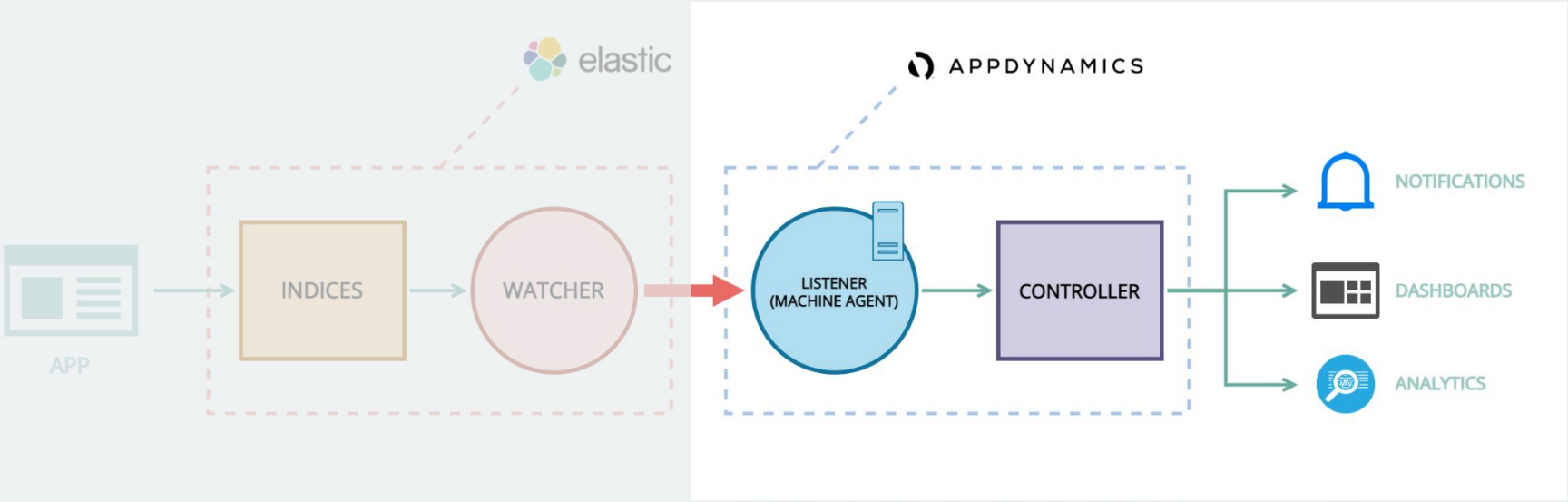


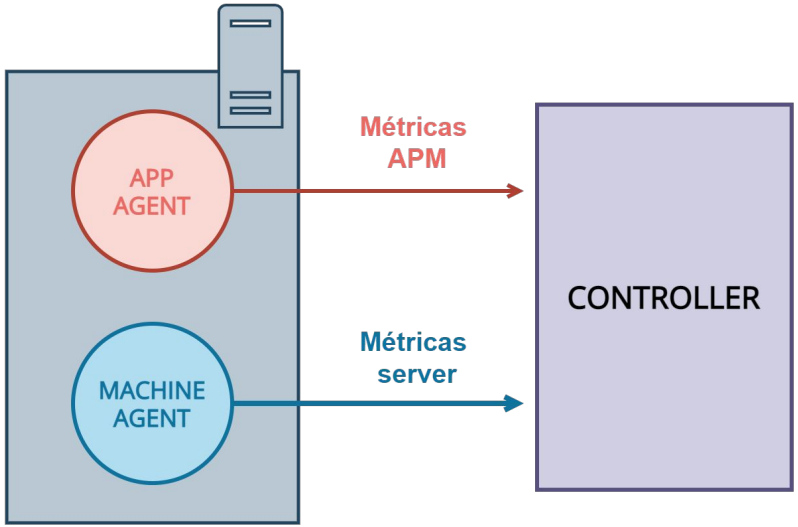
Diagrama de la propuesta



Machine Agent

El Machine Agent recopila métricas de infraestructura de varias extensiones y las envía al Controller.

Puede utilizar estas métricas para **encontrar correlaciones** entre los problemas de infraestructura y los problemas de rendimiento de las aplicaciones.



Machine Agent

Algunas funcionalidades del agente:

- Reportar las métricas básicas de hardware del sistema operativo del servidor, por ejemplo, % de utilización de la CPU y de la memoria, E/S del disco y de la red
- Reportar las métricas pasadas al Controller por las extensiones (plugins)
- Ejecución de scripts de auto-remediación
- Posee un listener HTTP

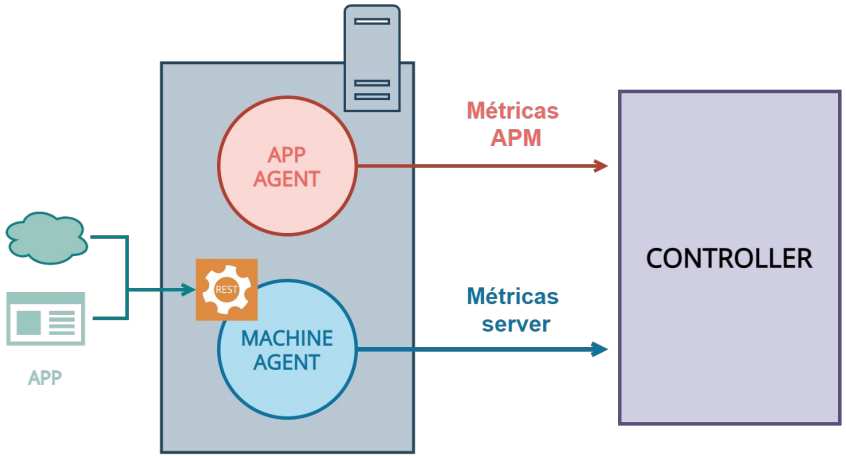
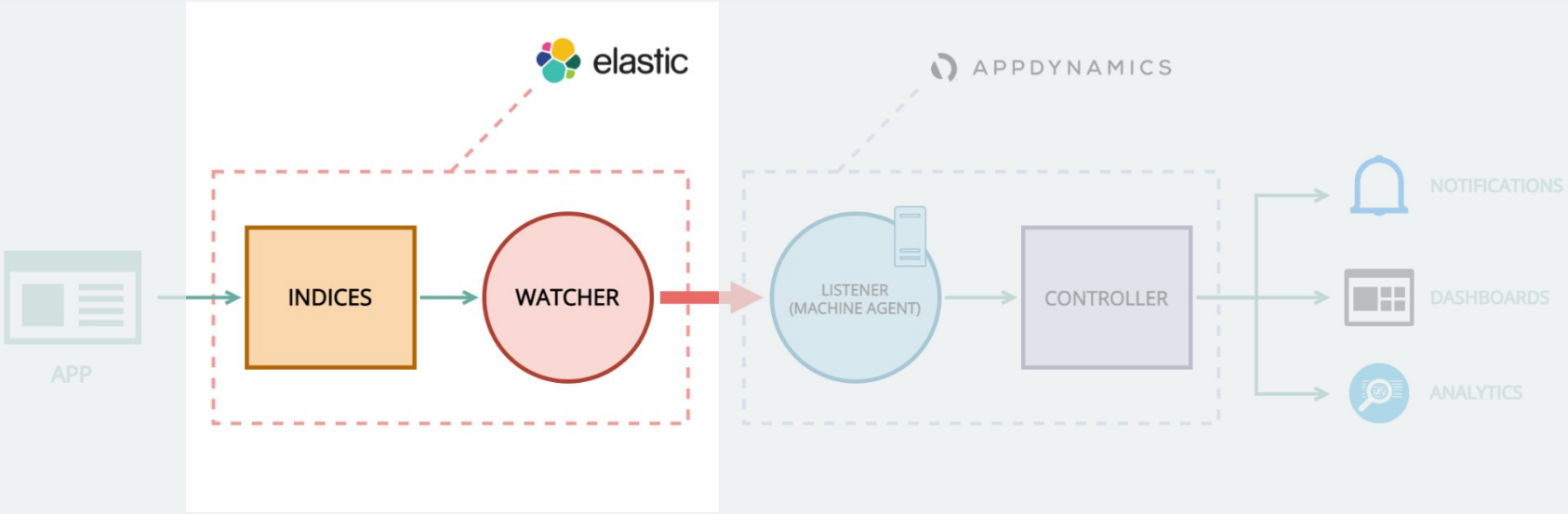


Diagrama de la propuesta



```
{
  "trigger": {
    "schedule": {
      "interval": "30m"
    }
  },
  "input": {
    "search": {
      "request": {
        "body": {
          "size": 0,
          "query": {
            "match_all": {}
          }
        },
        "indices": [
          "*"
        ]
      }
    }
  },
  "condition": {
    "compare": {
      "ctx.payload.hits.total": {
        "gte": 10
      }
    }
  },
  "actions": {
    "my-logging-action": {
      "logging": {
        "text": "There are {{ctx.payload.hits.total}}
documents in your index. Threshold is 10."
      }
    }
  }
}
```

Repaso de la composición de un watcher

```
{
  "trigger": {
    "schedule": {
      "interval": "30m"
    }
  },
  "input": {
    "search": {
      "request": {
        "body": {
          "size": 0,
          "query": {
            "match_all": {}
          }
        },
        "indices": [
          "*"
        ]
      }
    }
  },
  "condition": {
    "compare": {
      "ctx.payload.hits.total": {
        "gte": 10
      }
    }
  },
  "actions": {
    "my-logging-action": {
      "logging": {
        "text": "There are {{ctx.payload.hits.total}}
documents in your index. Threshold is 10."
      }
    }
  }
}
```

Trigger

Determina cuando se ejecuta el watcher (requerido)

```
{
  "trigger": {
    "schedule": {
      "interval": "30m"
    }
  },
  "input": {
    "search": {
      "request": {
        "body": {
          "size": 0,
          "query": {
            "match_all": {}
          }
        },
        "indices": [
          "*"
        ]
      }
    }
  },
  "condition": {
    "compare": {
      "ctx.payload.hits.total": {
        "gte": 10
      }
    }
  },
  "actions": {
    "my-logging-action": {
      "logging": {
        "text": "There are {{ctx.payload.hits.total}}
documents in your index. Threshold is 10."
      }
    }
  }
}
```

Input

Carga data en el payload del watcher, si no se especifica el input se carga un payload vacío. Es decir, específica que hay que buscar.

```
{
  "trigger": {
    "schedule": {
      "interval": "30m"
    }
  },
  "input": {
    "search": {
      "request": {
        "body": {
          "size": 0,
          "query": {
            "match_all": {}
          }
        },
        "indices": [
          "*"
        ]
      }
    }
  },
  "condition": {
    "compare": {
      "ctx.payload.hits.total": {
        "gte": 10
      }
    }
  },
  "actions": {
    "my-logging-action": {
      "logging": {
        "text": "There are {{ctx.payload.hits.total}}
documents in your index. Threshold is 10."
      }
    }
  }
}
```

Condition

Controla si las actions del watcher se ejecutan.
Si no se especifica una condición se ejecuta siempre.

```
{
  "trigger": {
    "schedule": {
      "interval": "30m"
    }
  },
  "input": {
    "search": {
      "request": {
        "body": {
          "size": 0,
          "query": {
            "match_all": {}
          }
        },
        "indices": [
          "*"
        ]
      }
    }
  },
  "condition": {
    "compare": {
      "ctx.payload.hits.total": {
        "gte": 10
      }
    }
  },
  "actions": {
    "my-logging-action": {
      "logging": {
        "text": "There are {{ctx.payload.hits.total}}
documents in your index. Threshold is 10."
      }
    }
  }
}
```

Actions

Especifica qué sucede cuando la condición del watcher es cumplida. Se pueden usar templates `mustache` para incorporar contenido dinámico

```
{
  "trigger":{
    "schedule":{
      "hourly":{
        "minute":[
          0
        ]
      }
    }
  },
  "input":{
    "search":{
      "request":{
        "search_type":"query_then_fetch",
        "indices":[
          "kibana_sample_data_ecommerce*"
        ],
        "rest_total_hits_as_int":true,
        "body":{
          "size":1,
          "query":{
            "bool":{
              "must":[

              ],
              "filter":[
                {
                  "range":{
                    "order_date":{
                      "format":"strict_date_optional_time",
                      "gte":"now-1h",
                      "lte":"now"
                    }
                  }
                }
              ],
              "should":[],
              "must_not":[]
            }
          }
        }
      }
    }
  },
  "condition":{
    "always":{
    }
  },
  "actions":{
    "webhook_total":{
      "webhook":{
        "scheme":"http",
        "host":"168.197.49.81",
        "port":8293,
        "method":"post",
        "path":"/api/v1/metrics",
        "params":{

        },
        "headers":{
          "Accept":"application/json",
          "Content-Type":"application/json"
        },
        "body":"""[{"metricName":"Custom
Metrics|Elasticsearch-test-1|eCommerce|TOTAL_RECORDS","aggregatorT
ype":"OBSERVATION","value":{{ctx.payload.hits.total}}}]"""
      }
    }
  }
}
```

Watcher propuesto

Fin

¿Fin?

¿Fin?

Se complejiza el requerimiento.

Requerimiento

desagregada por variables

Enviar información (# total transacciones) contenida en indices de Elastic a AppDynamics para ser consumida como custom metrics

```
            . . . }
              }
            ],
            "should": [],
            "must_not": []
          }
        },
        "aggs": {
          "0": {
            "terms": {
              "field": "geoip.city_name",
              "order": {
                "_count": "desc"
              },
              "size": 10
            }
          },
          "1": {
            "terms": {
              "field": "category.keyword",
              "order": {
                "_count": "desc"
              },
              "size": 10
            }
          }
        }
      }
    }
  }
},
"condition": {
  "always": {}
},
"actions": {. . .
```

`aggregations`

Sumariza datos en forma de métricas, estadísticas u otras analiticas.

En este caso usamos `bucket` aggregations, que agrupan los documentos en "buckets" o contenedores, en función de los valores de campos, rangos u otros criterios

Watcher propuesto 2

```
. . . },
 "webhook_foreach_city": {
   "foreach": "ctx.payload.aggregations.0.buckets",
   "max_iterations": 100,
   "webhook": {
     "scheme": "http",
     "host": "168.197.49.81",
     "port": 8293,
     "method": "post",
     "path": "/api/v1/metrics",
     "params": {},
     "headers": {
       "Accept": "application/json",
       "Content-Type": "application/json"
     },
     "body": """[{{#ctx.payload}}{"metricName":"Custom
Metrics|Elasticsearch-test-2|eCommerce|City|{{key}}","aggregatorTy
pe":"OBSERVATION","value":{{doc_count}}}{{/ctx.payload}}]"""
   }
 }, . . .
```

`foreach` action

Se puede utilizar para desencadenar la acción configurada para cada elemento dentro del array.

Watcher propuesto 2

```
. . . },
"webhook_foreach_city": {
  "foreach": "ctx.payload.aggregations.0.buckets",
  "max_iterations": 100,
  "webhook": {
    "scheme": "http",
    "host": "168.197.49.81",
    "port": 8293,
    "method": "post",
    "path": "/api/v1/metrics",
    "params": {},
    "headers": {
      "Accept": "application/json",
      "Content-Type": "application/json"
    },
    "body": """[{{#ctx.payload}}{"metricName":"Custom
Metrics|Elasticsearch-test-2|eCommerce|City|{{key}}","aggregatorTy
pe":"OBSERVATION","value":{{doc_count}}}{{/ctx.payload}}]"""
  }
}, . . .
```

```
. . . },
"webhook_foreach_cat": {
  "foreach": "ctx.payload.aggregations.1.buckets",
  "max_iterations": 100,
  "webhook": {
    "scheme": "http",
    "host": "168.197.49.81",
    "port": 8293,
    "method": "post",
    "path": "/api/v1/metrics",
    "params": {},
    "headers": {
      "Accept": "application/json",
      "Content-Type": "application/json"
    },
    "body": """[{{#ctx.payload}}{"metricName":"Custom
Metrics|Elasticsearch-test-2|eCommerce|Category|{{key}}","aggregat
orType":"OBSERVATION","value":{{doc_count}}}{{/ctx.payload}}]"""
  }
}
}
```

Watcher propuesto 2

Fin Fin.

Gracias! 👋

 in/santiago-lator

 /santiagolator

✉️ santiago.lator@gmail.com | slator@majorkeytech.com