Beats

¿Qué es Beats?

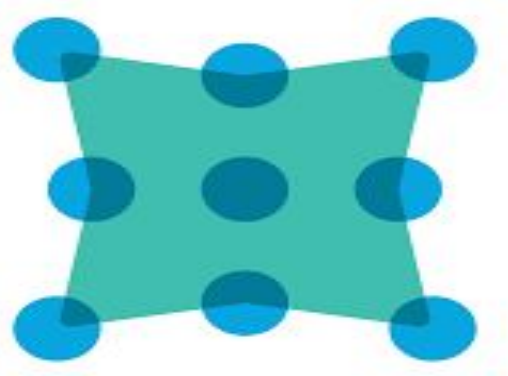
- Agentes ligeros para recolección de datos para enviarla a la salida seleccionada (ej: Logstash, Elasticsearch)
- Trabajan con múltiples puntos de recolección
- Variedad de beats dependiendo del tipo de datos a recolectar

Beats

- Filebeat
- Packetbeat
- Metricbeat
- Commonbeat
- Winlogbeat
- Auditbeat
- Heartbeat
- Otros...

Packetbeat

- Recolecta información del tráfico dé una interfaz de red definida en su archivo de configuración



Packetbeat: Instalar Biblioteca Adicional

Instalar Biblioteca necesaria para la captura de paquetes

- Windows 10: http://www.win10pcap.org/
- Linux o Mac: https://www.elastic.co/guide/en/beats/packetbeat/current/packetbeat-installation.html

Packetbeat: Configuracion

- Seleccionar dispositivo de la interfaz de red que se va a monitorear
- Listar los dispositivos y seleccionar el que corresponda a la interfaz deseada

```
PS D:\Users\Usuario\Desktop\Elastic\packetbeat-7.1.1-windows-x86_64> ./packetbeat.exe devices
0: {4FF9AEDF-00D4-4252-A793-54057C10BBAB} (Intel(R) 82579LM Gigabit Network Connection) (0.0.0.0)
1: {69FABC1F-EFA0-4C0F-A254-A4493AC03954} (TeamViewerVPN Adapter) (0.0.0.0)
2: {DE877AE1-A1F2-4542-B515-1C302BB383D9} (Microsoft) (192.168.86.24)
3: {DCC8930C-716A-4733-999C-97FB56C066F2} (Microsoft) (0.0.0.0)
```

```
#============================ Network device ================================

# Select the network interface to sniff the data. On Linux, you can use the
# "any" keyword to sniff on all connected interfaces.
packetbeat.interfaces.device: 2
```

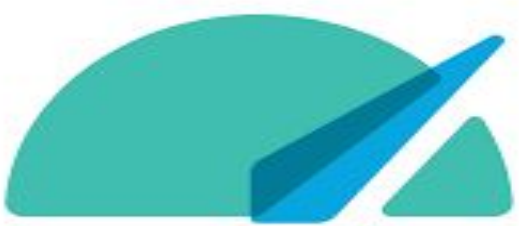
Packetbeat: Configuración Protocolos

- Monitoreo del tráfico para múltiples protocolos.
- Especificación de los puertos de cada protocolo
- Monitoriza tráfico de red, como dé base datos.

```
packetbeat.protocols:
- type: icmp
  # Enable ICMPv4 and ICMPv6 monitoring. Default: false
  enabled: true

- type: amqp
  # Configure the ports where to listen for AMQP traffic. You can disable
  # the AMQP protocol by commenting out the list of ports.
  ports: [5672]

- type: cassandra
  #Cassandra port for traffic monitoring.
  ports: [9042]

- type: dhcpv4
  # Configure the DHCP for IPv4 ports.
  ports: [67, 68]

- type: dns
  # Configure the ports where to listen for DNS traffic. You can disable
  # the DNS protocol by commenting out the list of ports.
  ports: [53]
```

Metricbeat

- Permite monitorear las métricas de los procesos en cuanto al consumo de recursos del sistema. Envía la información en tiempo real a Elasticsearch.



Metricbeat: Módulos Preconfigurados

- Módulos preconfigurados para distintos tipos de proceso
- Posibilidad de habilitarlos por consola, o por configuración
- Variedad de metricsets para todos los módulos de acuerdo a las métricas a monitorear

```
metricbeat.modules:

#------------------------- Apache Status Module
-------------------------
- module: apache
  metricsets: ["status"]
  period: 1s
  hosts: ["http://127.0.0.1/"]

#------------------------- MySQL Status Module
-------------------------
- module: mysql
  metricsets: ["status"]
  period: 2s
  hosts: ["root@tcp(127.0.0.1:3306)/"]
```

Metricbeat: Activar módulos por config (metricbeat.yml)

- metricbeat.modules: Lista de módulos que se activan cuando se ejecuta metric beat
- Cada módulo debe especificar su host, y la lista metricsets que se quiere indexar en ElasticSearch

```
metricbeat.modules:

#------------------ Apache Status Module ----------------
- module: apache
  metricsets: ["status"]
  period: 1s
  hosts: ["http://127.0.0.1/"]

#------------------ MySQL Status Module -----------------
- module: mysql
  metricsets: ["status"]
  period: 2s
  hosts: ["root@tcp(127.0.0.1:3306)/"]
```

Metricbeat: Activar módulos por Consola

- Listar los módulos existentes en la consola con `modules list`
- Indica los módulos activos e inactivos
- Mediante `modules enable <nombre_del_modulo>` se activa el módulo
- Editar metricsets desde el archivo correspondiente en “modules.d”

```
zookeeper
PS D:\Users\Usuario\Desktop\Elastic\metricbeat-7.1.1-windows-x86_64> .\metricbeat.exe modules list
Enabled:
mongodb
system

Disabled:
aerospike
apache
PS D:\Users\Usuario\Desktop\Elastic\metricbeat-7.1.1-windows-x86_64> .\metricbeat.exe modules enable mongodb
Module mongodb is already enabled
```

Metricbeat: Activar dashboards por defecto

- Activar dashboards incluidos en metrics beats
- Dashboards adaptados a la información que brinda cada módulo

```
setup.dashboards.enabled: true
```

Heartbeat

- Consulta en tiempo real el estado de los servicios corriendo en el servidor, enviando un pulso continuo consultando si están vivos.

Heartbeat: Configuración Monitores

- Configurar los monitores que van enviar PING a los servicios.
- Lista de URLs donde consultar si el servicio sigue vivo.
- **Check** incluye la respuesta esperada en ese protocolo señalando que el proceso está funcionando.

```
# Define a directory to load monitor definitions from. Definitions take the form
# of individual yaml files.
heartbeat.config.monitors:
  # Directory + glob pattern to search for configuration files
  path: ${path.config}/monitors.d/*.yml
  # If enabled, heartbeat will periodically check the config.monitors path for changes
  reload.enabled: false
  # How often to check for changes
  reload.period: 5s

# Configure monitors inline
heartbeat.monitors:
- type: http

  # List or urls to query
  urls: ["http://localhost:9200",
         "http://localhost:5601"
  ]

  check.response.status: 200

  # Configure task schedule
  schedule: '@every 5s'
```

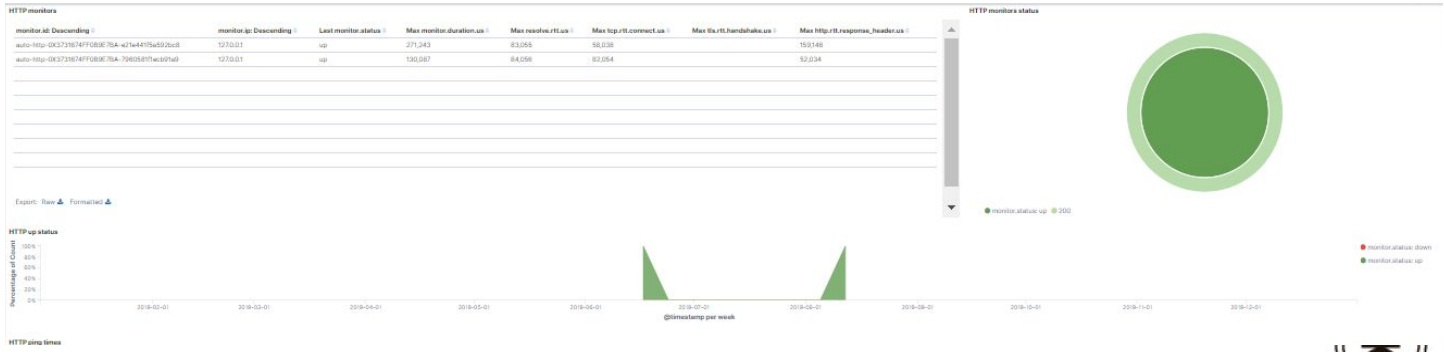
Heartbeat: Dashboards

- Mantener lo dashboards deshabilitados, Heartbeat en su última versión no los posee

```
setup.dashboards.enabled: false
```

- Para descargar dashboards hay que ingresar al siguiente repositorio:

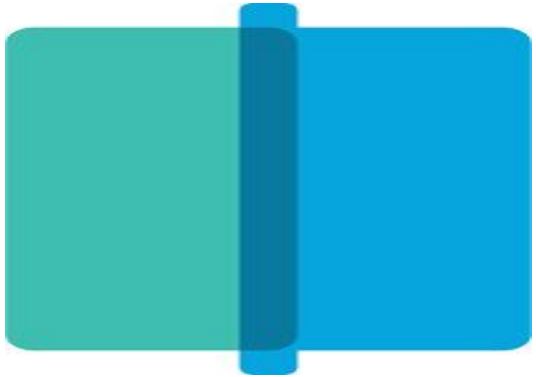
  https://github.com/elastic/uptime-contrib



UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

Auditbeat

- Monitorea y recopila información de la actividad de los usuarios o procesos en sistemas basados en Unix, enviando esta información a ElasticSearch en tiempo real.



Winlogbeat

- Es similar a Auditbeat, se concentra en recolectar eventos de logueo de sistemas windows y enviarlos en tiempo real a Elasticsearch

Filebeat

- Sirve para recolectar información desde un archivo, permite eliminar o reordenar el contenido antes de enviarlo a Elasticsearch o Logstash modificando su archivo de configuración

Configuración Filebeat: Input

- Habilitar input de tipo log, seteando **enabled** en true
- En el campo **paths** se deberá especificar la ruta del directorio
- Acepta patrones en la ruta para incluir múltiples archivos

```
filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

- type: log

  # Change to true to enable this input configuration.
  enabled: true

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - D:/Users/Usuario/Desktop/Elastic/logs/log-generator*.log
    #- c:\programdata\elasticsearch\logs\*
```

Configuración Filebeat: Preprocesamiento

- **exclude_lines**: Va a excluir todas las líneas que contengan el patrón o patrones en el array
- **include_lines**: Es el análogo de **exclude_includes** pero para la inclusión de líneas
- **exclude_files**: En este caso va a excluir los archivos con las extensiones especificadas en el array

```
# Exclude lines. A list of regular
# matching any regular expression f
exclude_lines: ['^DEBUG']

# Include lines. A list of regular
# matching any regular expression f
include_lines: ['^ERR', '^WARN']

# Exclude files. A list of regular
# are matching any regular expressi
exclude_files: ['.gz$']
```

Configuración Filebeat: Preprocesamiento

- multiline.pattern: recibe una expresión regular que va a evaluar para definir cuales son las líneas que corresponden a un solo log.
- multiline.negate: Aplica la negación de la expresión regular del punto anterior.
- multiline.match: define a qué evento se van a asociar las líneas que no correspondan a un evento.

```
multiline.pattern: ^(DEBUG|INFO|ERROR|TRACE).*

# Defines if the pattern set under pattern shou
multiline.negate: true

# Match can be set to "after" or "before". It i
# that was (not) matched before or after or as
# Note: After is the equivalent to previous and
multiline.match: after
```

Configuración Filebeat: Output

- Se habilita el output deseado en la lista de outputs
- Designa donde se enviará la recolección de Filebeat

```
#------------------------------ Logstash output -------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["localhost:5044"]
```

Configuraciones Generales

- Habilitar el monitoreo (en Kibana) de recolección de datos y el rendimiento del beat
- Habilitar los dashboards por defecto para visualización en Kibana
- Salida seleccionada para el envío de los datos recolectados

```
# Set to true to enable the monitoring reporter.
xpack.monitoring.enabled: true
```

```
# options here or by using the `setup` command.
setup.dashboards.enabled: true
```

```
#------------------------- Elasticsearch output ------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["localhost:9200"]
```

Preguntas?