```
1 ###################### Packetbeat Configuration Example
#########################
2
3 # This file is an example configuration file highlighting only the most common
4 # options. The packetbeat.reference.yml file from the same directory contains all
the
5 # supported options with more comments. You can use it as a reference.
6 #
7 # You can find the full configuration reference here:
8 # https://www.elastic.co/guide/en/beats/packetbeat/index.html
9
10 # ============================== Network device
==============================
11
12 # Select the network interface to sniff the data. On Linux, you can use the
13 # "any" keyword to sniff on all connected interfaces.
14 packetbeat.interfaces.device: any
15
16 # The network CIDR blocks that are considered "internal" networks for
17 # the purpose of network perimeter boundary classification. The valid
18 # values for internal_networks are the same as those that can be used
19 # with processor network conditions.
20 #
21 # For a list of available values see:
22 #
https://www.elastic.co/guide/en/beats/packetbeat/current/defining-processors.html#condition-
network
23 packetbeat.interfaces.internal_networks:
24   - private
25
26 # ================================== Flows
==================================
27
28 # Set `enabled: false` or comment out all options to disable flows reporting.
29 packetbeat.flows:
30   # Set network flow timeout. Flow is killed if no packet is received before being
31   # timed out.
32   timeout: 30s
33
34   # Configure reporting period. If set to -1, only killed flows will be reported
35   period: 10s
36
37 # ========================== Transaction protocols
==========================
38
39 packetbeat.protocols:
40 - type: icmp
41   # Enable ICMPv4 and ICMPv6 monitoring. The default is true.
```

```
  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
  # Configure the ports where to listen for Cassandra traffic. You can disable
  # the Cassandra protocol by commenting out the list of ports.
  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]

- type: http
  # Configure the ports where to listen for HTTP traffic. You can disable
  # the HTTP protocol by commenting out the list of ports.
  ports: [80, 8080, 8000, 5000, 8002]

- type: memcache
  # Configure the ports where to listen for memcache traffic. You can disable
  # the Memcache protocol by commenting out the list of ports.
  ports: [11211]

- type: mysql
  # Configure the ports where to listen for MySQL traffic. You can disable
  # the MySQL protocol by commenting out the list of ports.
  ports: [3306,3307]

- type: pgsql
  # Configure the ports where to listen for Pgsql traffic. You can disable
  # the Pgsql protocol by commenting out the list of ports.
  ports: [5432]

- type: redis
  # Configure the ports where to listen for Redis traffic. You can disable
  # the Redis protocol by commenting out the list of ports.
  ports: [6379]

- type: thrift
  # Configure the ports where to listen for Thrift-RPC traffic. You can disable
```

```
  # the Thrift-RPC protocol by commenting out the list of ports.
  ports: [9090]

- type: mongodb
  # Configure the ports where to listen for MongoDB traffic. You can disable
  # the MongoDB protocol by commenting out the list of ports.
  ports: [27017]

- type: nfs
  # Configure the ports where to listen for NFS traffic. You can disable
  # the NFS protocol by commenting out the list of ports.
  ports: [2049]

- type: tls
  # Configure the ports where to listen for TLS traffic. You can disable
  # the TLS protocol by commenting out the list of ports.
  ports:
    - 443   # HTTPS
    - 993   # IMAPS
    - 995   # POP3S
    - 5223  # XMPP over SSL
    - 8443
    - 8883  # Secure MQTT
    - 9243  # Elasticsearch

- type: sip
  # Configure the ports where to listen for SIP traffic. You can disable
  # the SIP protocol by commenting out the list of ports.
  ports: [5060]

# ======================= Elasticsearch template setting ======================

setup.template.settings:
  index.number_of_shards: 1
  #index.codec: best_compression
  #_source.enabled: false

# ================================== General ===================================

# The name of the shipper that publishes the network data. It can be used to group
# all the transactions sent by a single shipper in the web interface.
#name:

# A list of tags to include in every event. In the default configuration file
# the forwarded tag causes Packetbeat to not add any host fields. If you are
```

```
135 # monitoring a network tap or mirror port then add the forwarded tag.
136 #tags: [forwarded]
137
138 # Optional fields that you can specify to add additional information to the
139 # output.
140 #fields:
141 #  env: staging
142
143 # ================================== Dashboards
==================================
144 # These settings control loading the sample dashboards to the Kibana index.
Loading
145 # the dashboards is disabled by default and can be enabled either by setting the
146 # options here or by using the `setup` command.
147 setup.dashboards.enabled: true
148
149 # The URL from where to download the dashboards archive. By default this URL
150 # has a value which is computed based on the Beat name and version. For
released
151 # versions, this URL points to the dashboard archive on the artifacts.elastic.co
152 # website.
153 #setup.dashboards.url:
154
155 # =================================== Kibana
===================================
156
157 # Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana
API.
158 # This requires a Kibana endpoint configuration.
159 setup.kibana:
160
161   # Kibana Host
162   # Scheme and port can be left out and will be set to the default (http and 5601)
163   # In case you specify and additional path, the scheme is required:
http://localhost:5601/path
164   # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
165
166
167
168 host: "140.130.34.20:5601"
169 #username: "USER"
170  # password: "PSW”
171   # Kibana Space ID
172   # ID of the Kibana Space into which the dashboards should be loaded. By
default,
173   # the Default Space will be used.
174   #space.id:
175
```

```
176 # ============================== Elastic Cloud ==============================
177
178 # These settings simplify using Packetbeat with the Elastic Cloud (https://cloud.elastic.co/).
179
180 # The cloud.id setting overwrites the `output.elasticsearch.hosts` and
181 # `setup.kibana.host` options.
182 # You can find the `cloud.id` in the Elastic Cloud web UI.
183 #cloud.id:
184
185 # The cloud.auth setting overwrites the `output.elasticsearch.username` and
186 # `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
187 #cloud.auth:
188
189 # ================================== Outputs ===================================
190
191 # Configure what output to use when sending the data collected by the beat.
192
193 # ---------------------------- Elasticsearch Output ----------------------------
194 output.elasticsearch:
195   # Array of hosts to connect to.
196   hosts: ["140.130.34.20:9200"]
197
198   # Protocol - either `http` (default) or `https`.
199   #protocol: "https"
200
201   # Authentication credentials - either API key or username/password.
202   #api_key: "id:api_key"
203   username: "USER"
204   password: "<PSW>"
205
206 # ------------------------------ Logstash Output -------------------------------
207 #output.logstash:
208   # The Logstash hosts
209  # hosts: ["140.130.34.20:5044"]
210
211   # Optional SSL. By default is off.
212   # List of root certificates for HTTPS server verifications
213   #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]
214
215   # Certificate for SSL client authentication
216   #ssl.certificate: "/etc/pki/client/cert.pem"
217
218   # Client Certificate Key
219   #ssl.key: "/etc/pki/client/cert.key"
220
```

```
221 # ================================== Processors
===================================
222
223 processors:
224   - # Add forwarded to tags when processing data from a network tap or mirror.
225     if.contains.tags: forwarded
226     then:
227     - drop_fields:
228               fields: [host]
229     else:
230     - add_host_metadata: ~
231   - add_cloud_metadata: ~
232   - add_docker_metadata: ~
233   - detect_mime_type:
234     field: http.request.body.content
235     target: http.request.mime_type
236   - detect_mime_type:
237     field: http.response.body.content
238     target: http.response.mime_type
239
240 # ================================== Logging
===================================
241
242 # Sets log level. The default log level is info.
243 # Available log levels are: error, warning, info, debug
244 #logging.level: debug
245
246 # At debug level, you can selectively enable logging only for some components.
247 # To enable all selectors use ["*"]. Examples of other selectors are "beat",
248 # "publisher", "service".
249 #logging.selectors: ["*"]
250
251 # ============================= X-Pack Monitoring
==============================
252 # Packetbeat can export internal metrics to a central Elasticsearch monitoring
253 # cluster.  This requires xpack monitoring to be enabled in Elasticsearch.  The
254 # reporting is disabled by default.
255
256 # Set to true to enable the monitoring reporter.
257 #monitoring.enabled: false
258
259 # Sets the UUID of the Elasticsearch cluster under which monitoring data for this
260 # Packetbeat instance will appear in the Stack Monitoring UI. If
output.elasticsearch
261 # is enabled, the UUID is derived from the Elasticsearch cluster referenced by
output.elasticsearch.
262 #monitoring.cluster_uuid:
263
```

```
264 # Uncomment to send the metrics to Elasticsearch. Most settings from the
265 # Elasticsearch output are accepted here as well.
266 # Note that the settings should point to your Elasticsearch *monitoring* cluster.
267 # Any setting that is not set is automatically inherited from the Elasticsearch
268 # output configuration, so if you have the Elasticsearch output configured such
269 # that it is pointing to your Elasticsearch monitoring cluster, you can simply
270 # uncomment the following line.
271 #monitoring.elasticsearch:
272
273 # ============================== Instrumentation
==============================
274
275 # Instrumentation support for the packetbeat.
276 #instrumentation:
277     # Set to true to enable instrumentation of packetbeat.
278     #enabled: false
279
280     # Environment in which packetbeat is running on (eg: staging, production,
etc.)
281     #environment: ""
282
283     # APM Server hosts to report instrumentation results to.
284     #hosts:
285     #  - http://localhost:8200
286
287     # API Key for the APM Server(s).
288     # If api_key is set then secret_token will be ignored.
289     #api_key:
290
291     # Secret token for the APM Server(s).
292     #secret_token:
293
294
295 # ================================= Migration
=================================
296
297 # This allows to enable 6.7 migration aliases
298 #migration.6_to_7.enabled: true
299
```