

 **ONE IDENTITY™**

Syslog-ng 101, part 12: Elasticsearch (and Opensearch, Zinc, Humio, etc.)

Peter Czanik

History of Elasticsearch support

- Old: Java-based destination
- Cannot be included in distros
- New: wrapper around the http() destination
 - Slack, Sumologic, Telegram, etc. are similar

elasticsearch-http

```
destination d_elasticsearch_http {  
  elasticsearch-http(  
    index("syslog-ng")  
    type("")  
    user("elastic")  
    password("Gr3CmhxxxxxxxxxCWB")  
    url("https://localhost:9200/_bulk")  
    template("${format-json --scope rfc5424 --scope dot-nv-pairs  
--rekey .* --shift 1 --scope nv-pairs  
--exclude DATE @timestamp=${ISODATE}}")  
    tls(peer-verify(no))  
  );  
};
```

GeoIP rewrite

```
rewrite r_geoip2 {  
  set(  
    "${geoip2.location.latitude},${geoip2.location.longitude}",  
    value( "geoip2.location2" ),  
    condition(not "${geoip2.location.latitude}" == "")  
  );  
};
```

- New name-value pair for Kibana, if not empty

Mapping

```
{
  "mappings" : {
    "properties" : {
      "geoip2" : {
        "properties" : {
          "location2" : {
            "type" : "geo_point"
          }
        }
      }
    }
  }
}
```

- Lets Kibana know that name-value pair contains geographical coordinates

Example 1/2

```
@version:3.37
@include "scl.conf"

source s_sys { system(); internal(); };
destination d_mesg { file("/var/log/messages"); };
log { source(s_sys); destination(d_mesg); };

source s_tcp {
    tcp(ip("0.0.0.0") port("514"));
};

parser p_kv {kv-parser(prefix("kv.")); };

parser p_geoip2 { geoip2( "${kv.SRC}", prefix( "geoip2." ) database( "/usr/share/GeoIP/GeoLite2-City.mmdb" ) ); };

rewrite r_geoip2 {
    set(
        "${geoip2.location.latitude},${geoip2.location.longitude}",
        value( "geoip2.location2" ),
        condition(not "${geoip2.location.latitude}" == "")
    );
};
```

Example 2/2

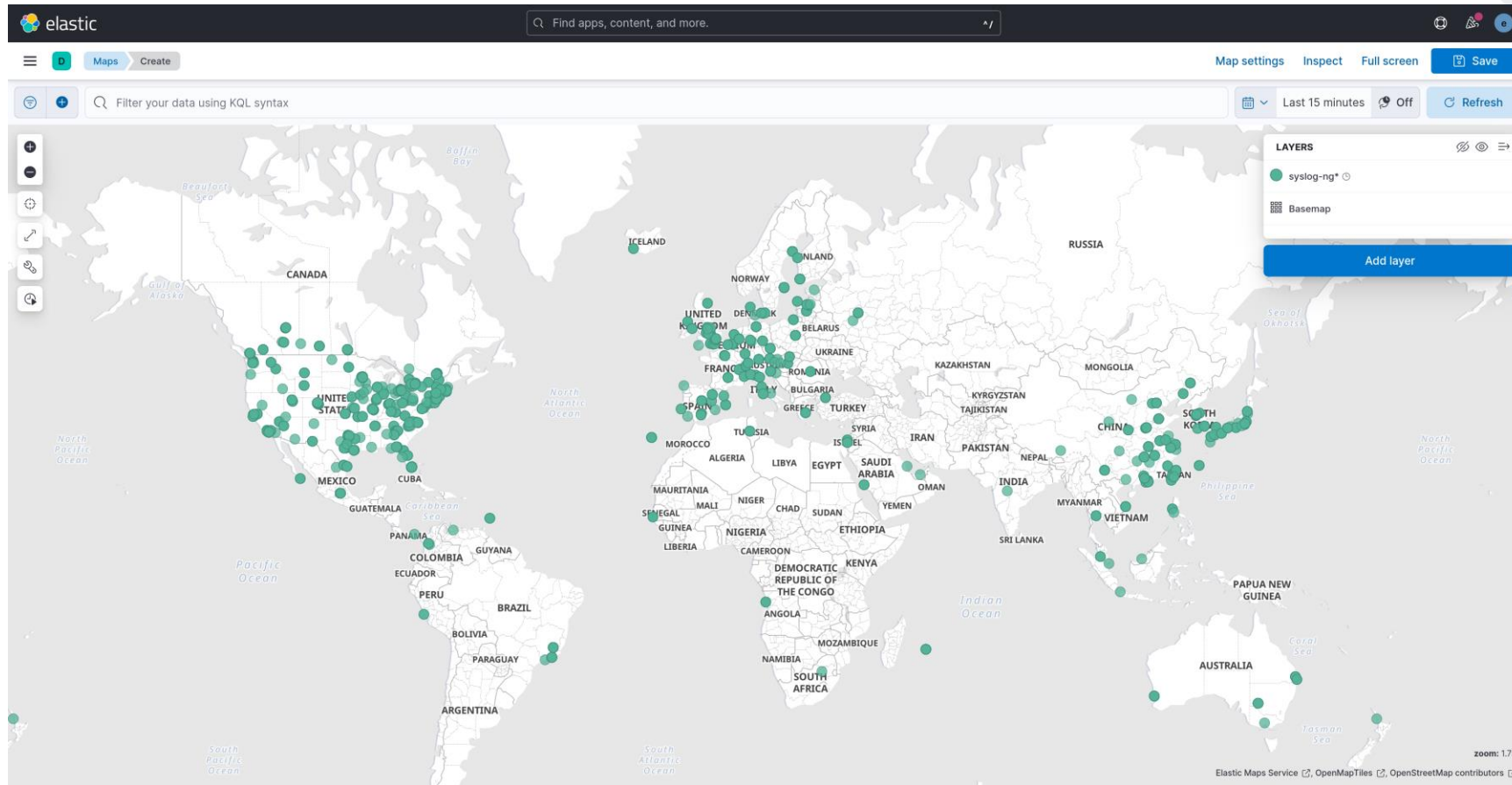
```
destination d_elasticsearch_http {
  elasticsearch-http(
    index("syslog-ng")
    type("")
    user("elastic")
    password("Gr3CmxxxxxCWB")
    url("https://localhost:9200/_bulk")
    template("${format-json --scope rfc5424 --scope dot-nv-pairs
      --rekey .* --shift 1 --scope nv-pairs
      --exclude DATE @timestamp=${ISODATE}}")
    tls(peer-verify(no))
  );
};

log {
  source(s_sys);
  source(s_tcp);
  if (match("s_tcp" value("SOURCE"))) {
    parser(p_kv);
    parser(p_geoip2);
    rewrite(r_geoip2);
  };
  destination(d_elasticsearch_http);
  flags(flow-control);
};
```


Iptables sample logs

- Feb 27 14:31:01 bridge kernel: INBOUND UDP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=212.123.153.188 DST=11.11.11.82 LEN=404 TOS=0x00 PREC=0x00 TTL=114 ID=19973 PROTO=UDP SPT=4429 DPT=1434 LEN=384
- Feb 27 14:34:41 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=206.130.246.2 DST=11.11.11.100 LEN=40 TOS=0x00 PREC=0x00 TTL=51 ID=9492 DF PROTO=TCP SPT=2577 DPT=80 WINDOW=17520 RES=0x00 ACK FIN URGP=0
- Feb 27 14:34:55 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=4.60.2.210 DST=11.11.11.83 LEN=48 TOS=0x00 PREC=0x00 TTL=113 ID=3024 DF PROTO=TCP SPT=3124 DPT=80 WINDOW=64240 RES=0x00 SYN URGP=0

IP addresses on map using GeoIP and Kibana



 **ONE IDENTITY™**