

 **ONE IDENTITY™**

Syslog-ng 101, part 11: Enriching log messages

Peter Czanik

Enriching log messages

- PatternDB
 - Can describe log messages: action=login status=failure
- GeoIP: find the geo-location of an IP address
 - Country name, longitude/latitude and many more info
 - Detect anomalies
 - Display locations on a map
- Add metadata from CSV files
 - For example: host role, contact person
 - Less time spent on locating extra information
 - More accurate alerts or dashboards

Using loggen with a network source

- loggen can generate logs or post existing log file
- `loggen -i -S -d -R /root/iptables_nohead_short localhost 514`
- Important options
 - -i: Internet
 - -S: TCP and unix-stream
 - -d: don't parse
 - -R /path/to/file : read log messages from a file
 - Host & port

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

Example

```
@version:3.38
```

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

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

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

```
source s_tcp { tcp(port(514)); };  
destination d_file {  
  file("/var/log/fromnet" template("$(format-json --scope rfc5424  
    --scope dot-nv-pairs --rekey .* --shift 1 --scope nv-pairs  
    --exclude DATE @timestamp=${ISODATE}})\n\n") );
```

```
};  
log {  
  source(s_tcp);  
  parser(p_kv);  
  parser(p_geoip2);  
  destination(d_file);  
};
```

 **ONE IDENTITY™**