## Plugin: Syslog input

Receives Syslog messages via UDP.

### Configuration

```
input:
  syslog:
    address: 0.0.0.0
    port: 1514

output:
  bindAddress: 0.0.0.0
  elasticsearch:
    module: elasticsearch
    diskBufferDir: /tmp/logagent
    url: http://localhost:9200
    index: logs
```

Start Logagent

```
logagent --config myconfig.yml
```

### Alternative usage via command-line

Receive UDP messages and write parsed logs to stdout in YAML format.

```
logagent -u 1514 --yaml
```

### Example with Docker Syslog driver and Logagent

We could use Logagent to receive Docker container logs using Docker logging driver:

```
logagent -u 1514 --yaml &
docker run -d --log-driver syslog --log-opt syslog-address="udp://localhost:1514" --log-opt ta
curl http://localhost:8080
```

Logagent will receive and parse syslog fields and applies existing parser rules to the message field, which results in structured web server logs:

```
logSource:    nginx/flamboyant_kalam/4399ab53cc1f[1903]
_type:        access_log_combined
client_ip:    172.17.0.1
remote_id:    -
user:         -
```

```
method:       GET
path:         / HTTP/1.1
status_code:  200
size:         612
referer:      -
user_agent:   curl/7.54.0
@timestamp:   Fri Sep 08 2017 21:20:20 GMT+0200 (CEST)
message:      GET / HTTP/1.1
severity:     info
facility:     daemon
syslog-tag:   nginx/flamboyant_kalam/4399ab53cc1f[1903]
syslogClient: 192.168.178.31
```