

title: Drop Events Filter description: Drop events before logs are shipped to any destination

Output filter: drop-events

This plugin drops events by include/exclude criteria for each field. The **filters** property contains a list of fields. For each field, you can specify a regular expression to keep (include) or drop (exclude) the event from processing.

Configuration

The following example configuration reads log files from `/var/log` and applies various filters with the following rules:

- Keep logs with **severity** error and warn
- Drop logs with **severity** debug and info
- Drop logs from **service** ntpd
- Keep logs when **message** contains the words critical,error,auth or failed

```
# tail server logs
input:
  files:
    - '/var/log/**/*.log'

outputFilter:
  dropEvents:
    module: drop-events
    debug: false
    filters:
      severity:
        # don't drop logs with severity error and warn
        include: !!js/regexp /error|warn/i
        # drop logs with severity debug and info
        exclude: !!js/regexp /debug|info/i
      service:
        # drop logs from service ntpd
        exclude: !!js/regexp ntpd
      message:
        # don't drop logs with
        # messages containing the words critical,error,auth or failed
        include: !!js/regexp /critical|auth|error|failed/
```

Run Logagent with your config:

```
logagent --config logagent-example-config.yml --yaml
```