Graylog
4.0

Search docs

GRAYLOG

Architectural considerations

Getting Started

Installing Graylog

Upgrading Graylog

Configuring Graylog

Securing Graylog

⊟ Sending in log data

What are Graylog message inputs?

⊟ Log sources

Ingest syslog

Ingest journald

Ingest Windows eventlog

Ingest CEF

Ingest Raw/Plaintext

Ingest GELF

**Ingest from files**

Ingest JSON path from HTTP API

Ingest Application Data

Individual Inputs

Using Apache Kafka as transport queue

Using RabbitMQ (AMQP) as transport queue

Input Throttling

Graylog Sidecar

Searching

Streams

Alerts

Dashboards

Read the Docs v: 4.0

» Sending in log data » Ingest from files

Edit on GitHub

# Ingest from files

Log files come in many different flavors and formats, much more than any single program could handle.

That is why Graylog does not collect files directly but uses a wide range of collectors and agents specially made for this. The collectors can be configured and controlled by the already available configuration management software in the environment, our Graylog Sidecar that needs to be installed and configured, or manually.

Of course, you can still use any program supporting the GELF or Syslog protocol (among others) to send your logs to Graylog.

The most recommended way to pick a log file from Windows or Linux systems is filebeat. This collector is build to collect log files and ship them to a central location. The output module in filebeat is called logstash needed to send messages to a Graylog beats input.

A basic filebeat configuration for filebeat on Linux can look like the following:

```
fields_under_root: true
fields.collector_node_id: ${sidecar.nodeName}
fields.gl2_source_collector: ${sidecar.nodeId

filebeat.inputs:
- input_type: log
  paths:
    - /var/log/*.log
  type: log
output.logstash:
    hosts: ["graylog:5044"]
path:
  data: /var/lib/graylog-sidecar/collectors/fi
  logs: /var/lib/graylog-sidecar/collectors/fi
```

For Windows, the basic filebeat configuration can be like:

```
fields_under_root: true
fields.collector_node_id: ${sidecar.nodeName}
fields.gl2_source_collector: ${sidecar.nodeId}

output.logstash:
   hosts: ["graylog:5044"]
path:
  data: C:\Program Files\Graylog\sidecar\cache
  logs: C:\Program Files\Graylog\sidecar\logs
tags:
 - windows
filebeat.inputs:
  type: log
  enabled: true
  paths:
    - C:\logs\log.log
```

Previous Next

Revision 91655126.

Built with Sphinx using a theme provided by Read the Docs.