

Promtail

My Default Promtail Configuration

```
# Global promtail configuration
server:
  http_listen_port: 9080
  grpc_listen_port: 0

clients:
  - url: http://<log-host>:3100/loki/api/v1/push

limits_config:
  max_line_size: 384kb

scrape_configs:
  - job_name: web
    file_sd_configs:
      - files:
          - /etc/loki/web.yaml

  - job_name: flog_scrape
    docker_sd_configs:
      - host: unix:///var/run/docker.sock
        refresh_interval: 5s
        #filters:
        #  - name: label
        #    # Add logging=promtail label to enable log capture
        #    values: ["logging=promtail"]
    relabel_configs:
      - source_labels: ["__meta_docker_container_name"]
        regex: "/(.*)"
        target_label: "container"
      - source_labels: ["__meta_docker_container_log_stream"]
        target_label: "logstream"
```

```
- source_labels: ["__meta_docker_container_label_logging_jobname"]
  target_label: "job"

- job_name: systemd-journal
  journal:
    labels:
      cluster: ops-tools1
      job: default/systemd-journal
    path: /var/log/journal
  relabel_configs:
    - source_labels:
        - __journal__systemd_unit
      target_label: systemd_unit
    - source_labels:
        - __journal__hostname
      target_label: hostname
    - source_labels:
        - __journal_syslog_identifier
      target_label: syslog_identifier
```

Don't forget to verify if there is a separate promtail user that needs to be added to the docker group for container logs

Revision #3

Created 28 October 2024 13:05:32 by etorres

Updated 5 November 2024 15:58:58 by etorres