| **LOKI** |
| --- |



Ángel González Martínez

Nicolás Jaraiz Bravo

Rubén Bautista Maya

SMX 2 A

**ÍNDICE**

[**DESCRIPCIÓN GENERAL DEL SERVICIO 3**](#_mjymoerfjzpw)

[**INSTALACIÓN DEL SERVICIO 3**](#_yilstfiqymex)

[**CONFIGURACIÓN DEL SERVICIO 3**](#_kb1ts8wqsbh0)

### **DESCRIPCIÓN GENERAL DEL SERVICIO**

Loki es un sistema de almacenamiento y consulta de logs (registros de eventos) diseñado específicamente para ser eficiente y escalable. Fue desarrollado por Grafana Labs y es parte del ecosistema de herramientas para observabilidad que incluye Grafana, Prometheus y otros.

Hemos optado por introducir este servicio ya que hemos visto que es bastante completo en cuanto a información, y en grafana, presenta de forma muy gráfica los logs importantes.

### **INSTALACIÓN DEL SERVICIO**

Para llevar a cabo la instalación del servicio Grafana Loki, vamos a realizar los siguientes pasos:

En primer lugar, vamos a instalar Loki:

*wget https://github.com/grafana/loki/releases/download/v3.0.0/loki\_3.0.0\_amd64.deb*

*apt install ./loki\_3.0.0\_amd64.deb*

En segundo lugar y, una vez hemos instalado Loki en nuestro ordenador (en nuestro caso es en el contenedor senna, 192.168.233.19), vamos a instalar Promtail en todos los equipos que queramos monitorizar siguiendo los siguientes pasos:

Lo primero de todo es la instalación, que es similar a la de Loki-

*wget https://github.com/grafana/loki/releases/download/v3.0.0/promtail\_3.0.0\_amd64.deb*

*apt install ./promtail\_3.0.0\_amd64.deb*

Después, hemos de editar el fichero */etc/group* para añadir a promtail en el grupo adm.

Y ya podremos continuar con la configuración.

### **CONFIGURACIÓN DEL SERVICIO**

En primer lugar, debemos editar, de cada equipo que se va a monitorizar, el fichero */etc/promtail/config.yml* y dejarlo de una manera similar a la siguiente:

| server:  http\_listen\_port: 9080  grpc\_listen\_port: 0  positions:  filename: /tmp/positions.yaml  clients:  - url: http://192.168.233.19:3100/loki/api/v1/push  scrape\_configs:  - job\_name: system  static\_configs:  - targets:  - localhost  labels:  job: varlogs  \_\_path\_\_: /var/log/\*log  - job\_name: journal  journal:  max\_age: 12h  path: /var/log/journal  labels:  job: systemd-journal  relabel\_configs:  - source\_labels: ['\_\_journal\_\_systemd\_unit']  target\_label: 'unit'  - source\_labels:  - \_\_journal\_\_hostname  target\_label: nodename |
| --- |

Con esta configuración, estaremos haciendo que los equipos de la red envíen sus registros de log del directorio */var/log/*, y también los logs del journal.

Y para rematar, nos faltaría un *systemctl restart promtail*, y en el servidor Loki un *systemctl restart loki*

Una vez importado el datasource con su plantilla de visualización en Grafana, nos ha quedado de la siguiente manera:

