暴揍ELK 痛打Loki – VictoriaLogs 搭建Syslog日志收集存储系统

原创 网工格物 网工格物 2025年02月11日 22:05 河北

为什么要用VictoriaLogs ？

- 与Elasticsearch /Grafana Loki 相比几十倍的CPU/内存/存储资源占用的差距，能极大的节省硬件资源。
- 单体软件可以实现ELK的Web查询、日志压缩存储、syslog 日志接收。

官方文档：https://docs.victoriametrics.com/victorialogs/quickstart/

具体优势

VictoriaLogs 和 Elasticsearch (ES) 都是用于日志管理的工具，各有其优势，具体取决于使用场景和需求。以下是它们在存储方面的一些优势对比：

VictoriaLogs 的优势：

1. **资源效率**：VictoriaLogs 通常设计为资源高效型，在内存和存储的使用上可能更为节省。
2. **高压缩率**：其存储引擎可能使用更高效的数据压缩技术，减小存储空间需求。
3. **简单部署和管理**：VictoriaLogs 通常易于部署和管理，适合小型团队或不需要复杂功能的用户。
4. **面向特定日志场景优化**：如果你的需求与其优化场景一致，可能会体验到出色的性能。

Elasticsearch 的优势：

1. **成熟度和社区支持**：ES 是一个成熟的项目，有广泛的社区支持和丰富的文档。
2. **扩展性**：ES 支持大规模集群，可以处理从小型到大规模的应用很好的扩展。
3. **强大的查询功能**：ES 提供丰富的查询语言和功能，能够满足复杂数据分析的需求。
4. **生态系统广泛**：ES 有大量的插件和生态系统支持，包括 Kibana 等工具，方便进行可视化和分析。

使用建议：

- 如果你的项目需要高效的资源使用和简单的日志处理，VictoriaLogs 可能是一个不错的选择。
- 如果你的项目需要复杂的查询能力、大规模数据处理和强大的社区支持，Elasticsearch 或许更合适。

最终的选择应基于具体的需求、现有的基础设施以及团队的技术能力。

PS：VictoriaLogs 吃内存和硬盘空间较小 ，性能很高。但功能没ES完善，没有集群功能等，查询界面简陋。

部署背景

接收服务器或网络设备发送的syslog协议的日志，用于存储和日常查询。

Docker 要求较新版本，支持compose v2。

Docker安装教程：https://yeasy.gitbook.io/docker_practice/install/centos

Docker 部署

```
docker run -d --restart always \
  -p 9428:9428 \
  -p 514:514/udp \
  -v ./victoria-logs-data:/victoria-logs-data \
  --name victoria-logs-syslog-songxwn.com \
  docker.io/victoriametrics/victoria-logs:latest \
  -syslog.listenAddr.udp=:514


# by songxwn.com
```

- 9428为HTTP端口，用于访问Web UI等。(无安全认证)
- 514/udp为 syslog 接收端口，-syslog.listenAddr.udp=:514 用于开启UDP接收syslog。
- 配置当前目录下创建数据存储文件夹。

Docker compose 部署

创建VictoriaLogs文件夹，创建文件 docker-compose.yml

```
services:
  victoria-logs-syslog:
    image: docker.io/victoriametrics/victoria-logs:latest
    container_name: victoria-logs-syslog
    restart: always
    ports:
      - "9428:9428"
      - "514:514/udp"
    volumes:
      - ./victoria-logs-data:/victoria-logs-data
    command:
      - '-syslog.listenAddr.udp=:514'


# by songxwn.com
```

- 9428为HTTP端口，用于访问Web UI等。(无安全认证)
- 514/udp为 syslog 接收端口，-syslog.listenAddr.udp=:514 用于开启UDP接收syslog。
- 配置当前目录下创建数据存储文件夹。

compose 部署示例命令

```
mkdir VictoriaLogs

cd VictoriaLogs

mkdir victoria-logs-data

vim docker-compose.yml

# 创建compose文件，并写入上面的内容

docker compose up -d
```

compose 升级示例命令

```
cd VictoriaLogs

docker compose down

docker compose pull

docker compose up -d
```

VictoriaLogs 日志保留时间

默认情况下，VictoriaLogs 存储时间戳在时间范围 `[now-7d, now]` 内的日志条目，同时删除给定时间范围之外的日志。例如它使用7天的保留。可以使用 `-retentionPeriod` 命令行标志配置保留。该标志接受从 1d （一天）到 100y （100 年）的值。

例如，以下命令启动 VictoriaLogs 并保留 30 天：

```
services:
  victoria-logs-syslog:
    image: docker.io/victoriametrics/victoria-logs:latest
    container_name: victoria-logs-syslog-songxwn.com
    restart: always
    ports:
      - "9428:9428"
      - "514:514/udp"
    volumes:
      - ./victoria-logs-data:/victoria-logs-data
    command:
      - '-syslog.listenAddr.udp=:514'
      - '--retentionPeriod=30d'

  # by songxwn.com
```

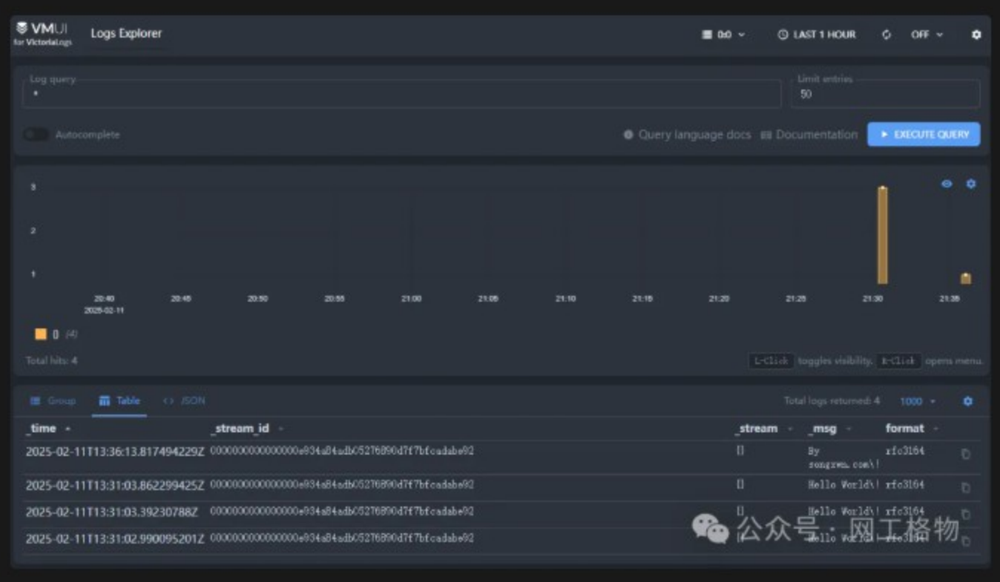
http://localhost:9428/flags 可查看启动参数。

Web UI 搜索

浏览器访问 http://localhost:9428 ，然后选择 select/vmui - Web UI for VictoriaLogs 进入，

查询语法：直接输入查询可全局搜索，右上角选择时间。查询两个关键词： abc AND bcd

文档：https://docs.victoriametrics.com/victorialogs/logsql/



监控VictoriaLogs

VictoriaLogs 在 page 上以 Prometheus 公开格式公开内部指标。 建议通过 VictoriaMetrics 设置对这些指标的监控

访问路径 http://localhost:9428/metrics

运维技术交流群

发送邮件到 me@songxwn.com

或者关注WX公众号：网工格物

微信扫码

博客（最先更新）

https://songxwn.com/

#开源项目 8 #开源 9 #日志 3

开源项目 · 目录

〈上一篇
NetBox 4.1 VMware OVF快速部署

下一篇 〉
ELK Stack 8 接入ElasticFlow

个人观点，仅供参考

阅读原文