



袋鼠云

DTSTACK.COM

基于ELK的云日志产品实践

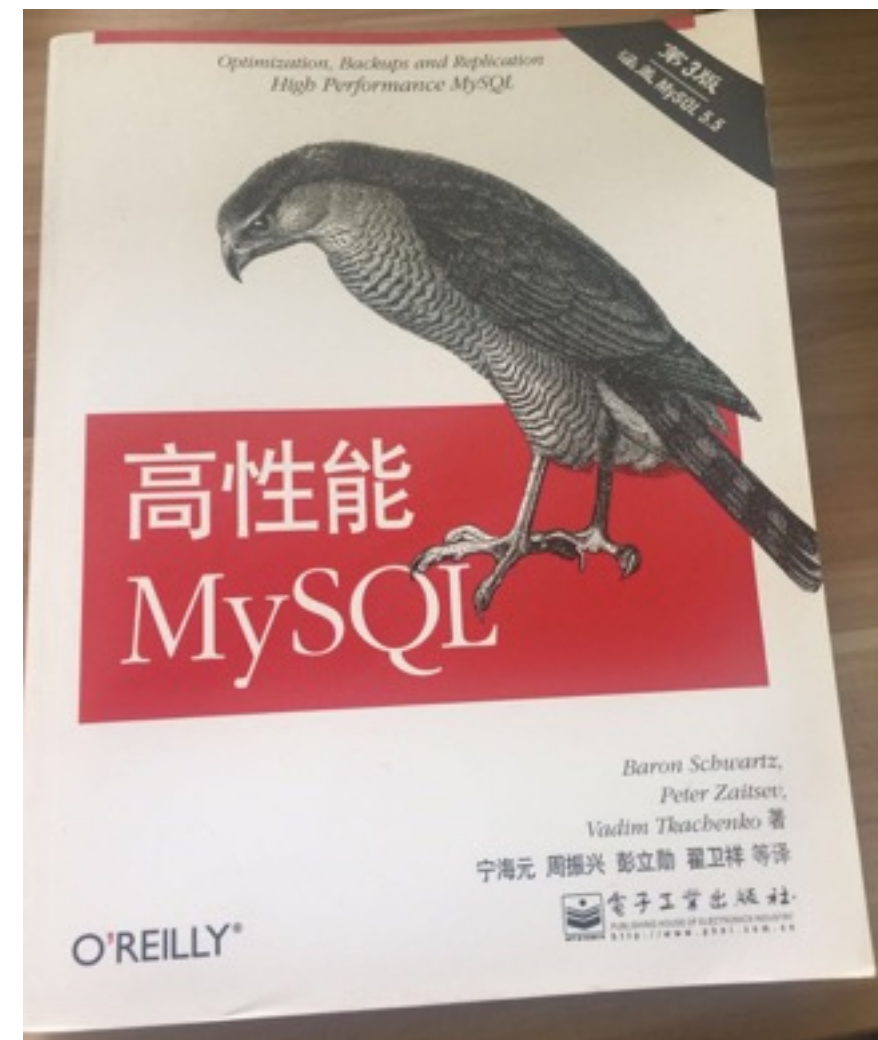
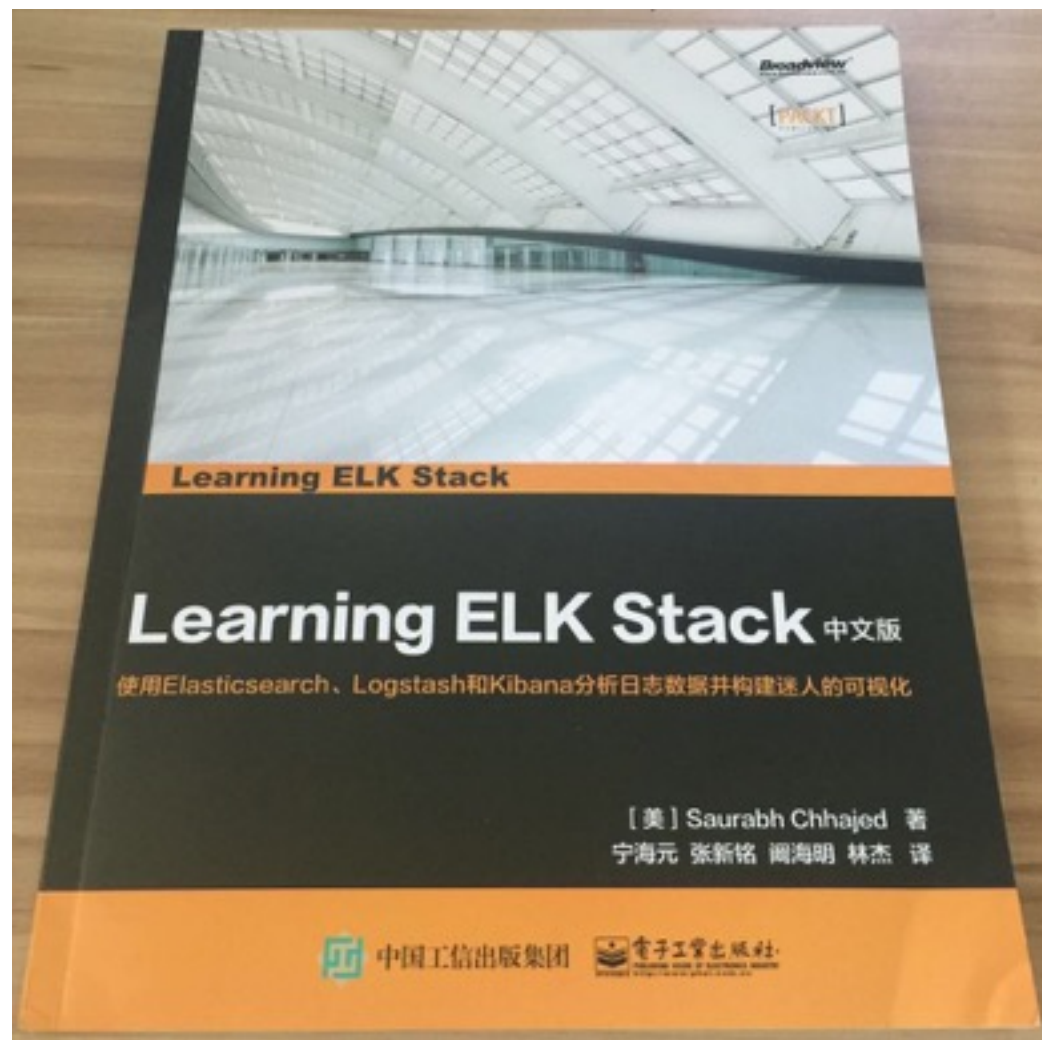
袋鼠云 江枫

2016.06.18

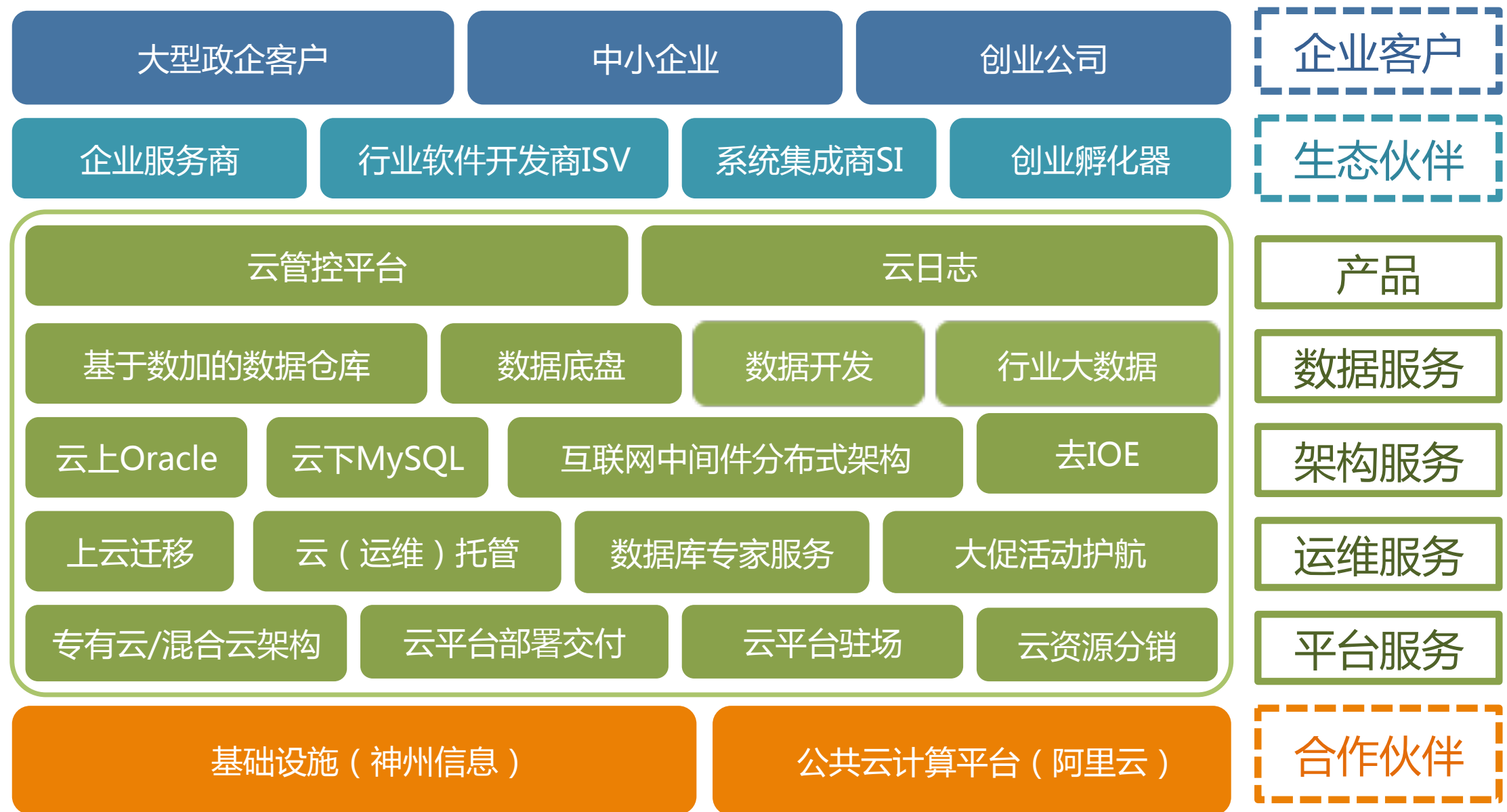
Who am I

- 宁海元、江枫、NinGoo
- 2007年加入淘宝DBA团队
- 2012年负责无线数据团队
- 2015年负责阿里云数加技术团队
- 2015年11月离职，创办袋鼠云

Who am I



袋鼠云是干什么的



袋鼠云日志

- 日志是大数据的通用需求
- 运维、业务、安全都需要
- 典型的实时场景
- Splunk / ELK

袋鼠云日志

- ELK的一些问题
 - 多租户&权限隔离
 - 日志结构化自定义解析规则
 - 上传日志身份验证
 - 异构数据源支持
 - Kibana的使用成本和二次开发能力
 - Logstash正则解析的CPU消耗

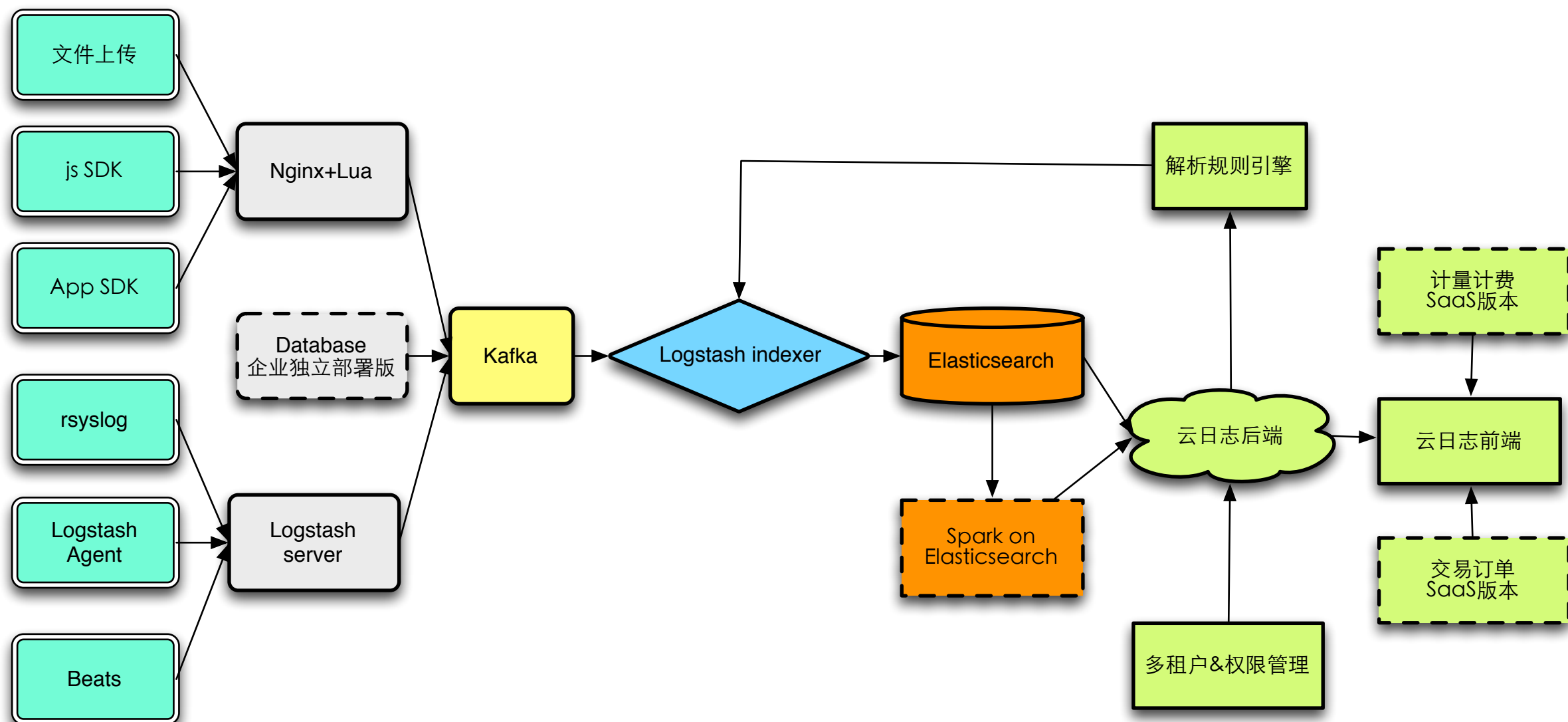
袋鼠云日志

采集&接收

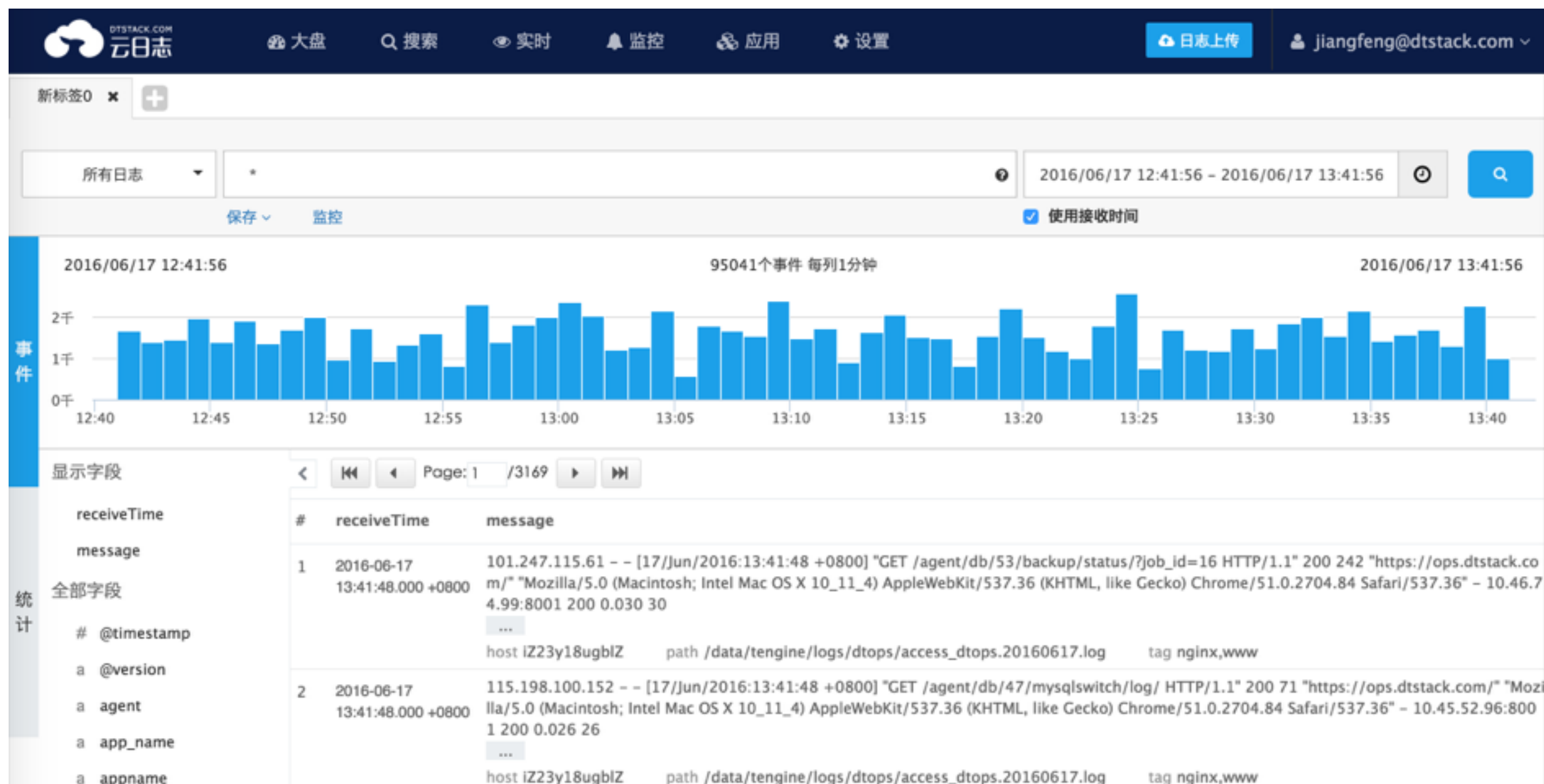
解析

存储&计算


展现&应用



袋鼠云日志



袋鼠云日志

DTSTACK.COM
云日志

大盘

Q 搜索

实时

🔔 监控

🔗 应用

⚙️ 设置

📄 日志上传

👤 jiangfeng@dtstack.com ▾

实时日志

iz23y18ugblz ▾

all ▾

all ▾

暂停

🔽

🗑️

```
"https://ops.dtstack.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.84 Safari/537.36" - 10.45.52.96:8001 200 0.023 23
iz23y18ugblz dtops dt_app_log [2016/06/17 13:48:51] DEBUG [celery.py:118] async update_ten_minute_disk_monitor_data by disk_id:586
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:00] DEBUG [celery.py:118] async update_ten_minute_disk_monitor_data by disk_id:627
iz23y18ugblz dtstack_access nginx_access_log 100.97.186.233 - - [17/Jun/2016:13:49:00 +0800] "HEAD / HTTP/1.0" 301 0 "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)" 112.126.75.174 - - - 0
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:10] DEBUG [celery.py:90] async update_ten_minute_instance_monitor_data by instance_id:328
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:17] DEBUG [celery.py:118] async update_ten_minute_disk_monitor_data by disk_id:754
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:22] DEBUG [celery.py:108] async async_update_minute_disk_monitor_data by disk_id:684
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:30] DEBUG [celery.py:118] async update_ten_minute_disk_monitor_data by disk_id:911
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:37] DEBUG [celery.py:118] async update_ten_minute_disk_monitor_data by disk_id:970
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:46] DEBUG [celery.py:90] async update_ten_minute_instance_monitor_data by instance_id:573
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:52] DEBUG [celery.py:108] async async_update_minute_disk_monitor_data by disk_id:1154
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:57] DEBUG [celery.py:108] async async_update_minute_disk_monitor_data by disk_id:1190
iz23y18ugblz dtops dt_app_log [2016/06/17 13:50:02] DEBUG [celery.py:108] async async_update_minute_disk_monitor_data by disk_id:1218
```

iz23y18ugblz ▾

all ▾

all ▾

暂停

🔽

🗑️

✕

```
"https://ops.dtstack.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.84 Safari/537.36" - 10.45.52.96:8001 200 0.023 23
iz23y18ugblz dtops dt_app_log [2016/06/17 13:48:51] DEBUG [celery.py:118] async update_ten_minute_disk_monitor_data by disk_id:586
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:00] DEBUG [celery.py:118] async update_ten_minute_disk_monitor_data by disk_id:627
iz23y18ugblz dtstack_access nginx_access_log 100.97.186.233 - - [17/Jun/2016:13:49:00 +0800] "HEAD / HTTP/1.0" 301 0 "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)" 112.126.75.174 - - - 0
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:10] DEBUG [celery.py:90] async update_ten_minute_instance_monitor_data by instance_id:328
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:17] DEBUG [celery.py:118] async update_ten_minute_disk_monitor_data by disk_id:754
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:22] DEBUG [celery.py:108] async async_update_minute_disk_monitor_data by disk_id:684
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:30] DEBUG [celery.py:118] async update_ten_minute_disk_monitor_data by disk_id:911
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:37] DEBUG [celery.py:118] async update_ten_minute_disk_monitor_data by disk_id:970
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:46] DEBUG [celery.py:90] async update_ten_minute_instance_monitor_data by instance_id:573
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:52] DEBUG [celery.py:108] async async_update_minute_disk_monitor_data by disk_id:1154
iz23y18ugblz dtops dt_app_log [2016/06/17 13:49:57] DEBUG [celery.py:108] async async_update_minute_disk_monitor_data by disk_id:1190
iz23y18ugblz dtops dt_app_log [2016/06/17 13:50:02] DEBUG [celery.py:108] async async_update_minute_disk_monitor_data by disk_id:1218
```

袋鼠云日志



袋鼠云日志

- SaaS版： <https://log.dtstack.com>
- 企业独立部署版

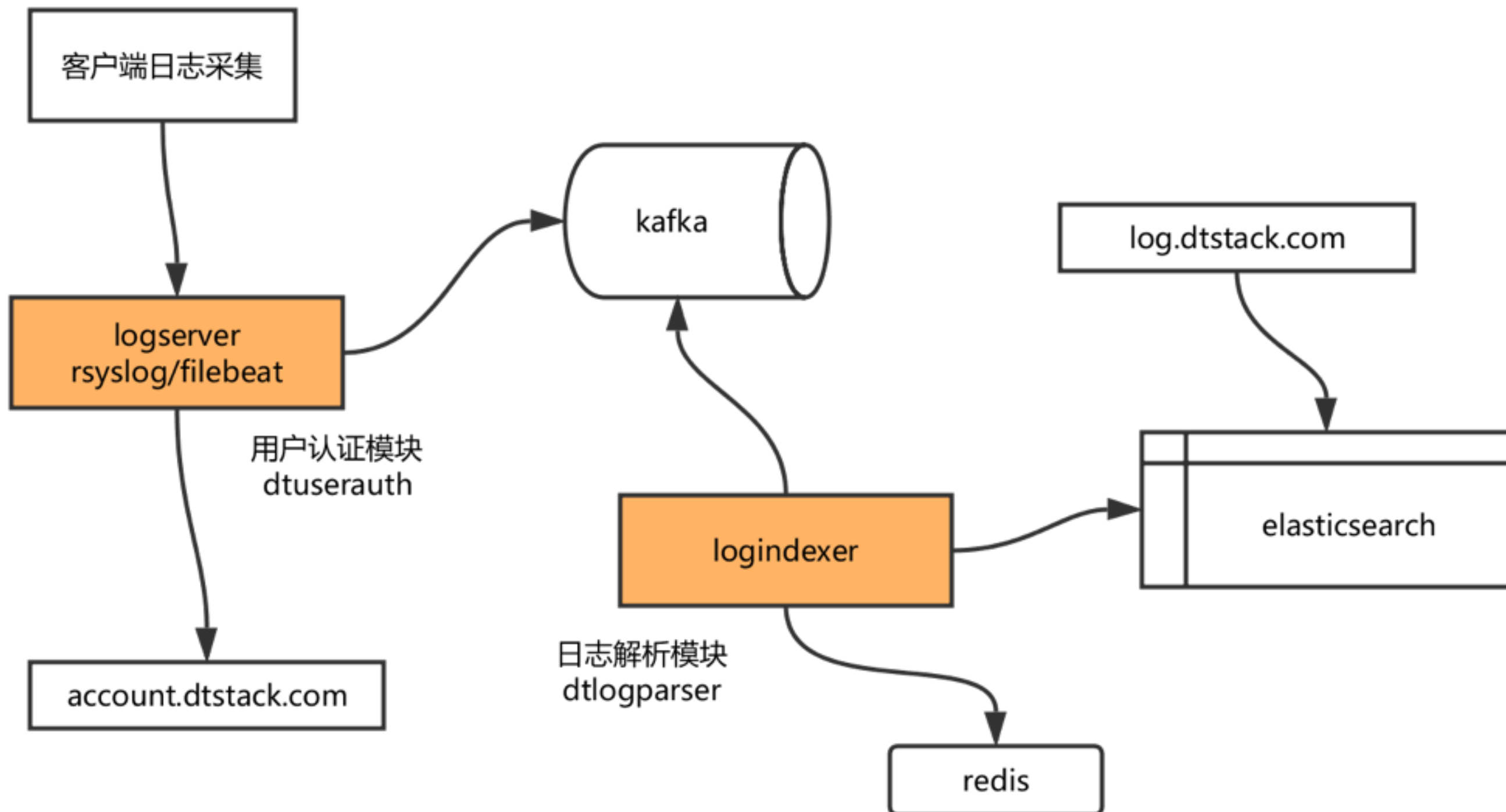
袋鼠云日志

- 第一阶段做好基本功能：搜索、分析、实时、大盘、监控、日志上传
- 第二阶段帮助中大型企业做好应用场景：安全分析、Web统计、移动统计、日志脱敏、跨表关联分析、流式计算等
- 第三阶段开放应用场景接口，支持第三方应用接入

袋鼠云日志

- 碰到的一些问题：
 - 大盘的前端挑战
 - Logstash插件优化：
 - 上传token验证
 - 自定义规则解析
 - ipip地理位置解析
 - Logstash CPU优化
 - 多版本部署配置

袋鼠云日志



袋鼠云日志

