# Log\_feature特征部署方案

## 目的：

让Linux 的服务日志（ceph.log,error\_log等等） 上报 到skynet 然后告警

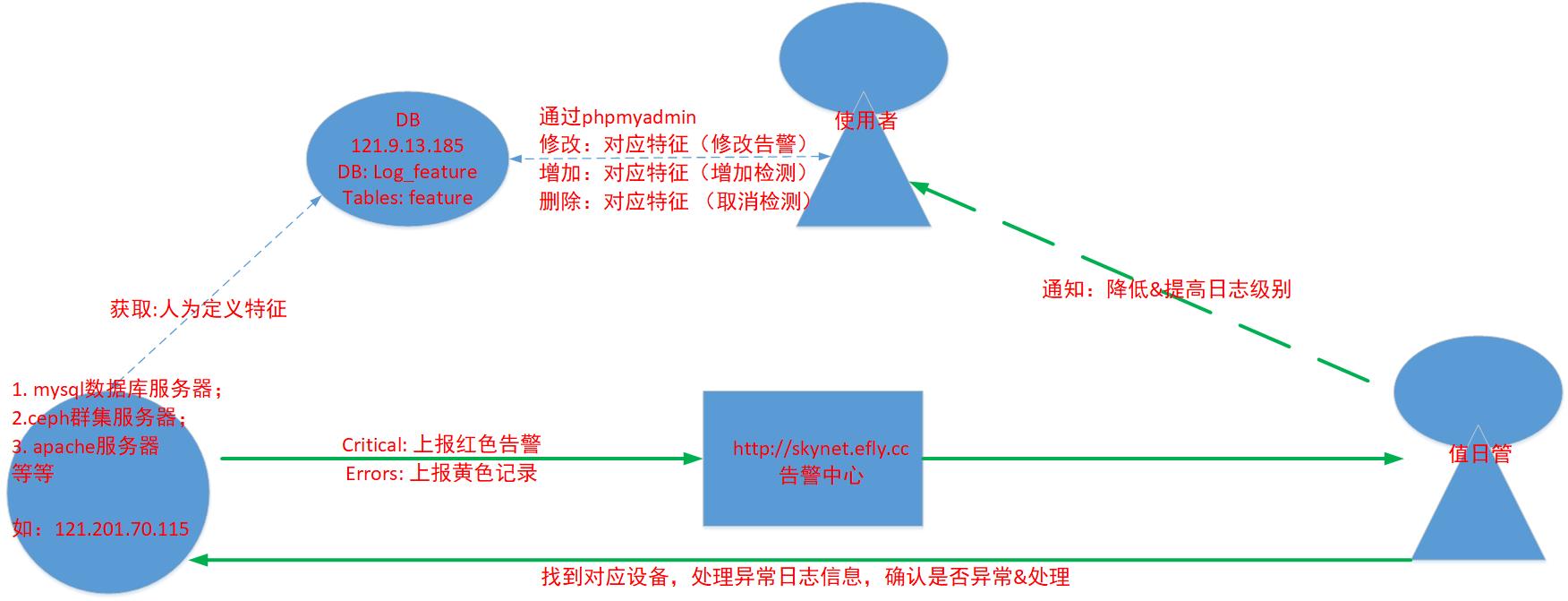
---skynet

Critical: 红色 需要关注处理

Errors: 黄色 适当观察



## 业务逻辑:



## 部署：

### 步骤1：[服务器端]部署DB –已经部署

1. 121.9.13.185 导入log\_feature.sql 文件
2. 创建 log\_mon/Rjkj#efly@123 ；只允许访问log\_feature.feature的表

### 步骤2：[监控设备]部署脚本-在检测设备121.201.70.115(数据库服务)

实例：监控日志-上报的服务器 121.201.70.115（被检测的服务器）

#### 2a. 要求确认：log\_detect.py

1. python3 （如果python 需要修改 log\_detect.py 头部第1行）
2. pip安装 requests ,pymysql
3. Linux必须有ifconfig命令
4. Linux必须跟skynet.efly.cc 可达（上报告警）
5. Linux 必须跟121.9.13.185 数据库DB 可以访问

###说明python环境已经具备

python

import requests

import pymysql 回车

#### 2b. 被监控设备必须访问121.9.13.185的数据库

##121.9.13.185

#vi /etc/iptables.rule 备注 设备用途 &&NAT过来的，只需要增加1条

-A INPUT -s 121.201.70.115/32 -p tcp -m tcp --dport 3306 -j ACCEPT

#### 2c. 使用crontab 定期检测

1. log\_detect.py放到/opt目录
2. chmod +x log\_detect.py
3. crontab -e ##确认crontab 服务有启动正常

\*/5 \* \* \* \* /opt/log\_detect.py

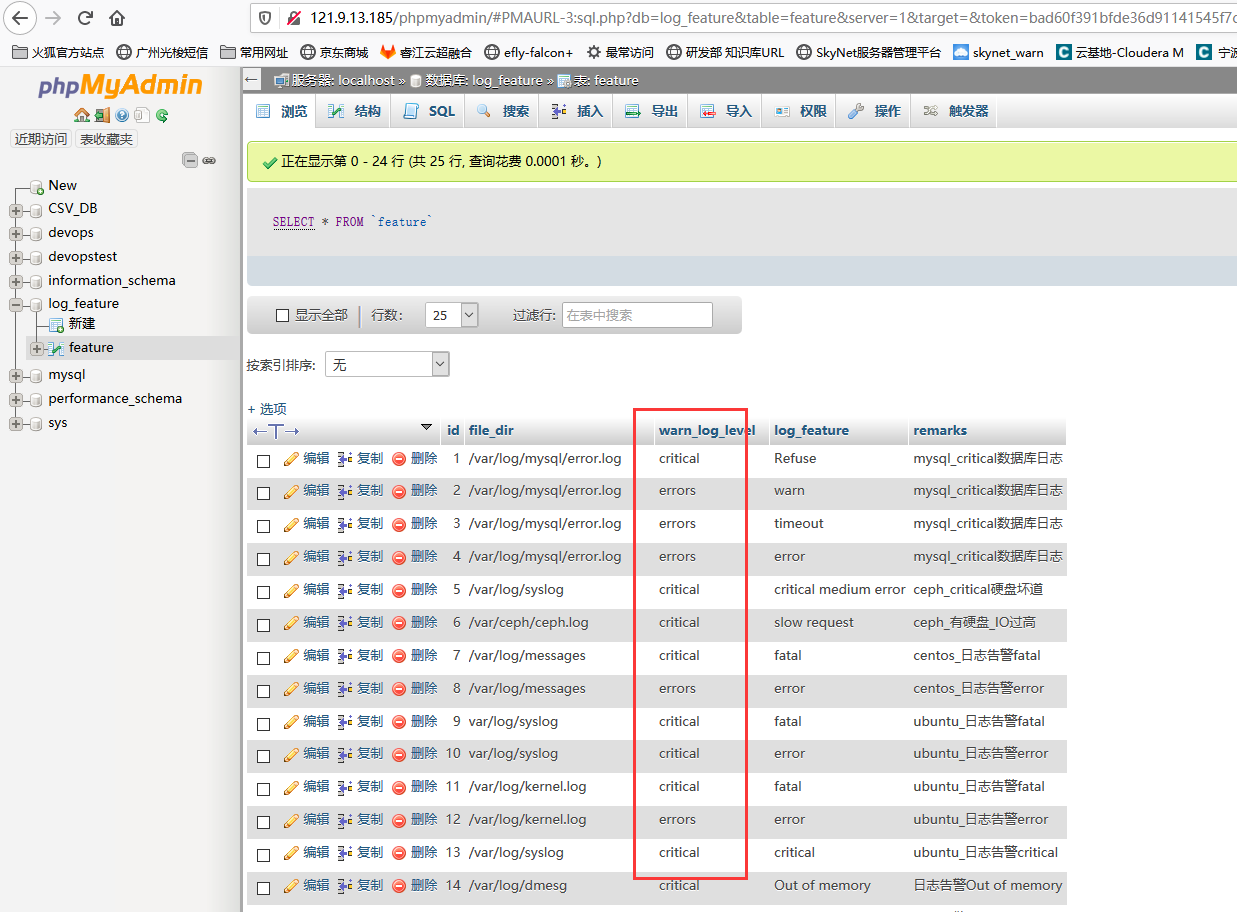
1. 观察skynet 有无falcon\_log\_monitor 字段的告警

<http://skynet.eflypro.com>

1. 手动执行python /opt/log\_detect.py 看看有无报错。

#### 2c. 如果确认告警等级，应该降低，可以修改为critical 》》》》errers(不允许标红)；当然删除数据库记录也可以

121.9.13.185数据库



## 批量执行ceph集群 发起监控：

1. 登陆到docker上、使用节点ansible
2. 确认ceph服务器有无 py的库
3. 确认ceph服务器是否可以访问到121.9.13.185 & Skynet.efly.cc

Hosts.ini 保留ceph的管理IP信息,去换root操作

ansible osds –i hosts.ini -m copy -a “src=log\_detect.py dest=/opt/log\_detect.py mode” -b

ansible osds –i hosts.ini -m file -a “path=/opt/log\_detect.py mode=0755” -b

ansible osds –i hosts.ini -m shell -a “systemctl status crond” -b

ansible osds –i hosts.ini -m cron -a “name=’log\_feature\_mon minute=\*/5 job=’/opt/log\_detect.py” -b