UCan下午茶

# 大数据入侵风险检测规则引擎的研发建设

苗东华

有所值

UCLOUD

# 目录

1. 大数据与入侵及风险检测
2. 规则引擎与入侵及风险检测
3. UCloud安全中心的规则引擎
4. 规则引擎的故障检测和高可用
5. 优化大数据安全分析引擎-UEBA

# 目录

# 大数据与入侵及风险检测

## 入侵与风险检测的必要性

- 网络入侵，无处不在
- 勒索病毒
- 软件漏洞时不时爆出
  - mongodb
  - redis
  - hadoop生态 等等
- 外部入侵，内鬼，边界风险

# 大数据与入侵及风险检测

## 入侵与风险检测项目

- 木马检测
- 异常登录，暴力破解
- 软件安全基线
- web安全基线
- 反连shell 等等

# 大数据与入侵及风险检测

## 入侵及风险检测的难点及要求

- 企业安全数据种类多-bash，进程，网络等
- 企业安全数据量大-每天以千亿计
- 历史追述时间要求长-年为单位
- 入侵和风险监测告警响应时间要短-分钟

# 大数据与入侵及风险检测

UCloud安全中心采用大数据技术构建了一套成熟稳定的入侵与风险检测的系统。

- 入侵及风险分析规则引擎
- 离线查询分析
- 历史操作回溯

# 大数据与入侵及风险检测

## UCloud安全中心安全分析涉及的大数据技术

- **实时分析**

Spark Streaming，Flink

- **离线分析**

Spark Core ，Spark Sql，hive

- **OLAP分析**

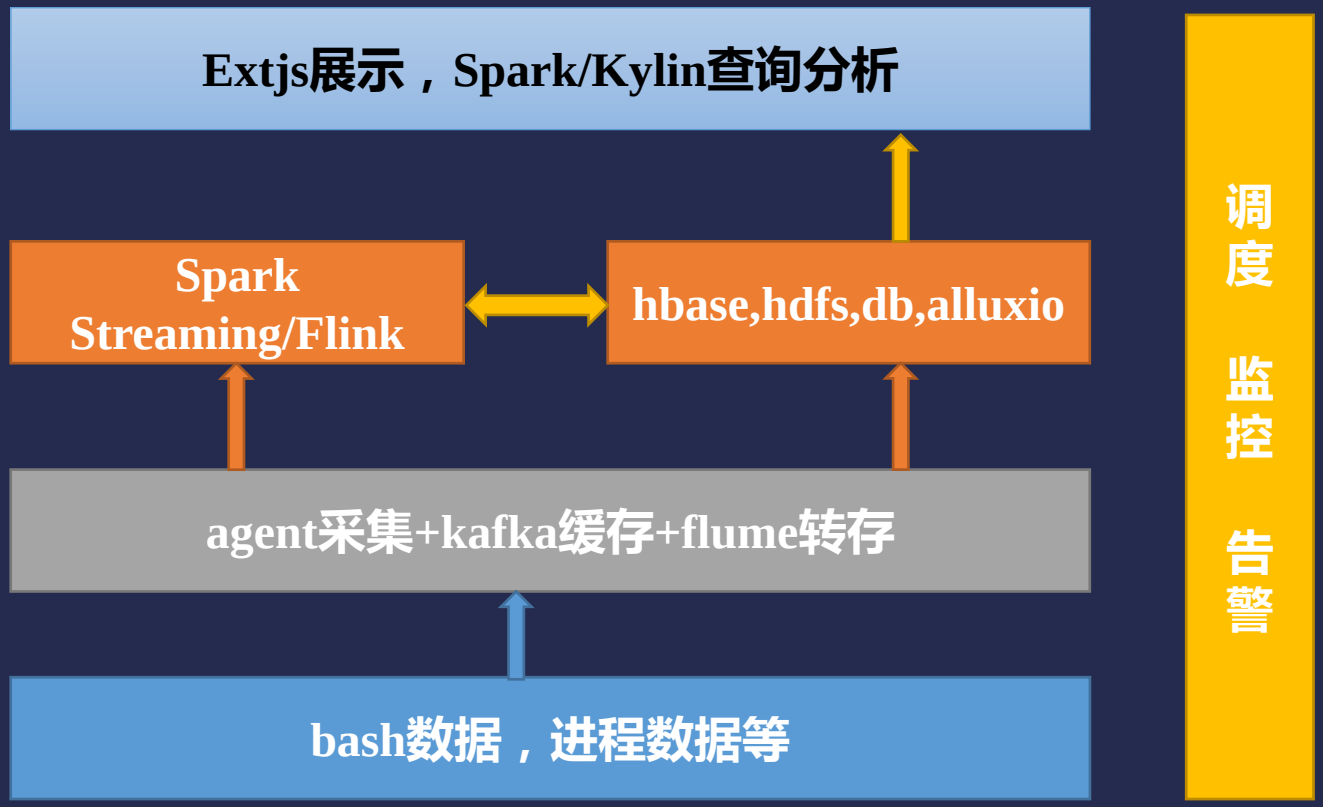
kylin，也可Spark Sql

- **存储**

Hbase，HDFS

# 大数据与入侵及风险检测

## UCloud安全中心入侵及风险检测的大数据架构



# 目录

1. 大数据与入侵及风险检测
2. 规则引擎与入侵及风险检测
3. UCloud安全中心的规则引擎
4. 规则引擎的故障检测和高可用
5. 优化大数据安全分析引擎-UEBA

# 规则引擎与入侵及风险检测

## 为啥要用规则引擎？

- 数据种类多，入侵及风险检测项多
- 入侵和风险检测规则变更频繁
- 需要动态增删黑白名单
- 运营人员开发能力稍微薄弱

# 规则引擎与入侵及风险检测

## 大数据规则引擎的建设过程

- 第一代 Spark Streaming+ Drools
- 第二代 SQL引擎+Scala quasiquotes

# 规则引擎与入侵及风险检测

## 第一代 Spark Streaming+ Drools

- 效率超低
- 开发难度有点高

# 规则引擎与入侵及风险检测

## 第一代 Spark Streaming+ Drools

E.g：特权用户检测

- 定义类

```
public class SysUserInfo {
    public String user;
    public int uid;
    public String host;
}
```

- 编写规则

```
import ucloud.SysUserInfo;
import ucloud.SerilizeTools;
rule "PrivilegedAccountCheckWarn"
    no-loop true
    when
        m : SysUserInfo((uid == 0)&&(user != "root"))
    then
        System.out.println("warnings")
        retract(m);
end
```

# 规则引擎与入侵及风险检测

## 第二代SQL引擎+Scala quasiquotes

### 基于Spark Sql

- Catalyst
- 内存计算
- Spark Context形式的job调度

### scala quasiquotes

- 嵌入少，固定

### 要求

- 数据格式整理并注册成表

# 规则引擎与入侵及风险检测

## 第二代SQL引擎+Scala quasiquotes

E.g:特权用户检测

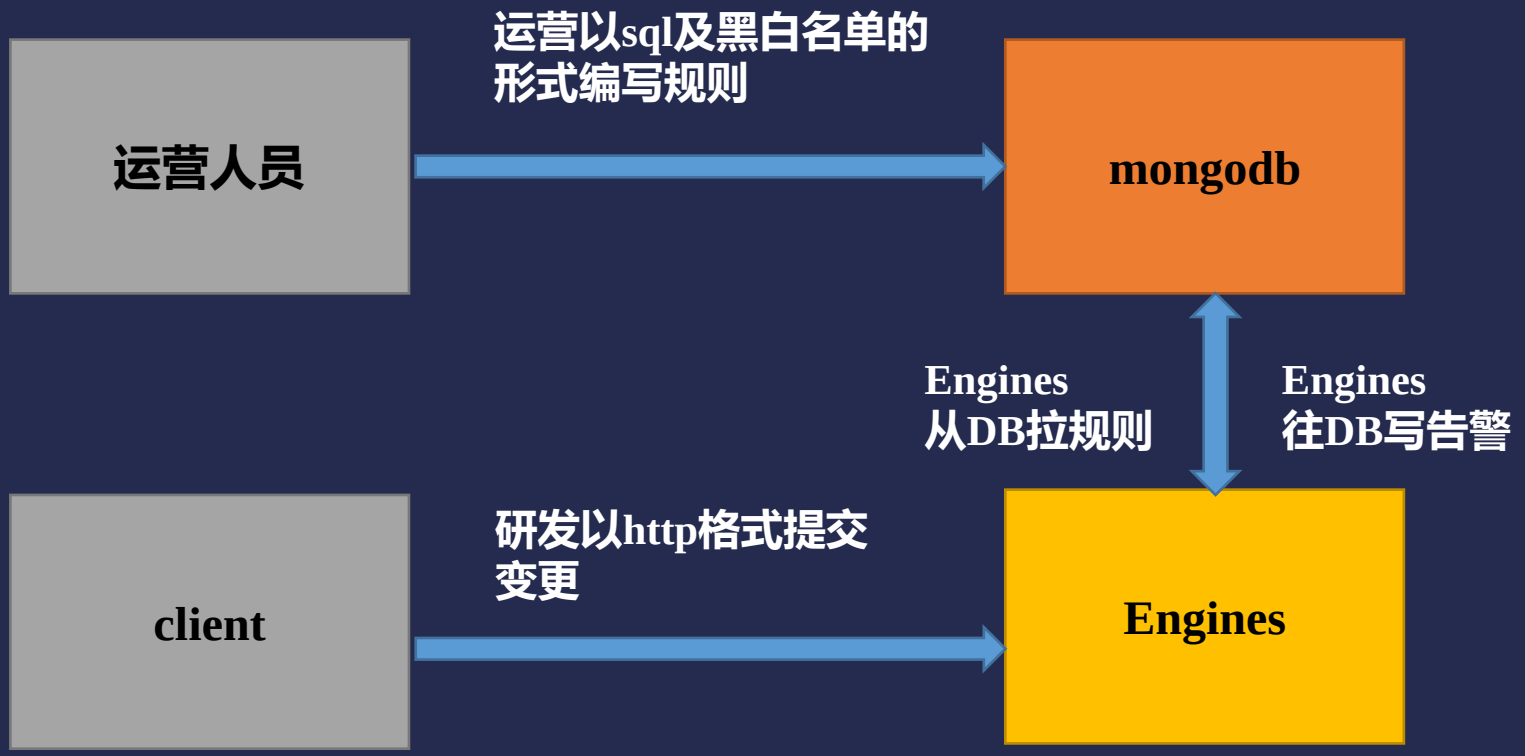
- json格式数据
- 规则

select * from userinfo where uid ==0 and user != root

# 目录

# UCloud安全中心的规则引擎

## 规则引擎使用结构



# UCloud安全中心的规则引擎

## 规则引擎的使用

### 运营人员

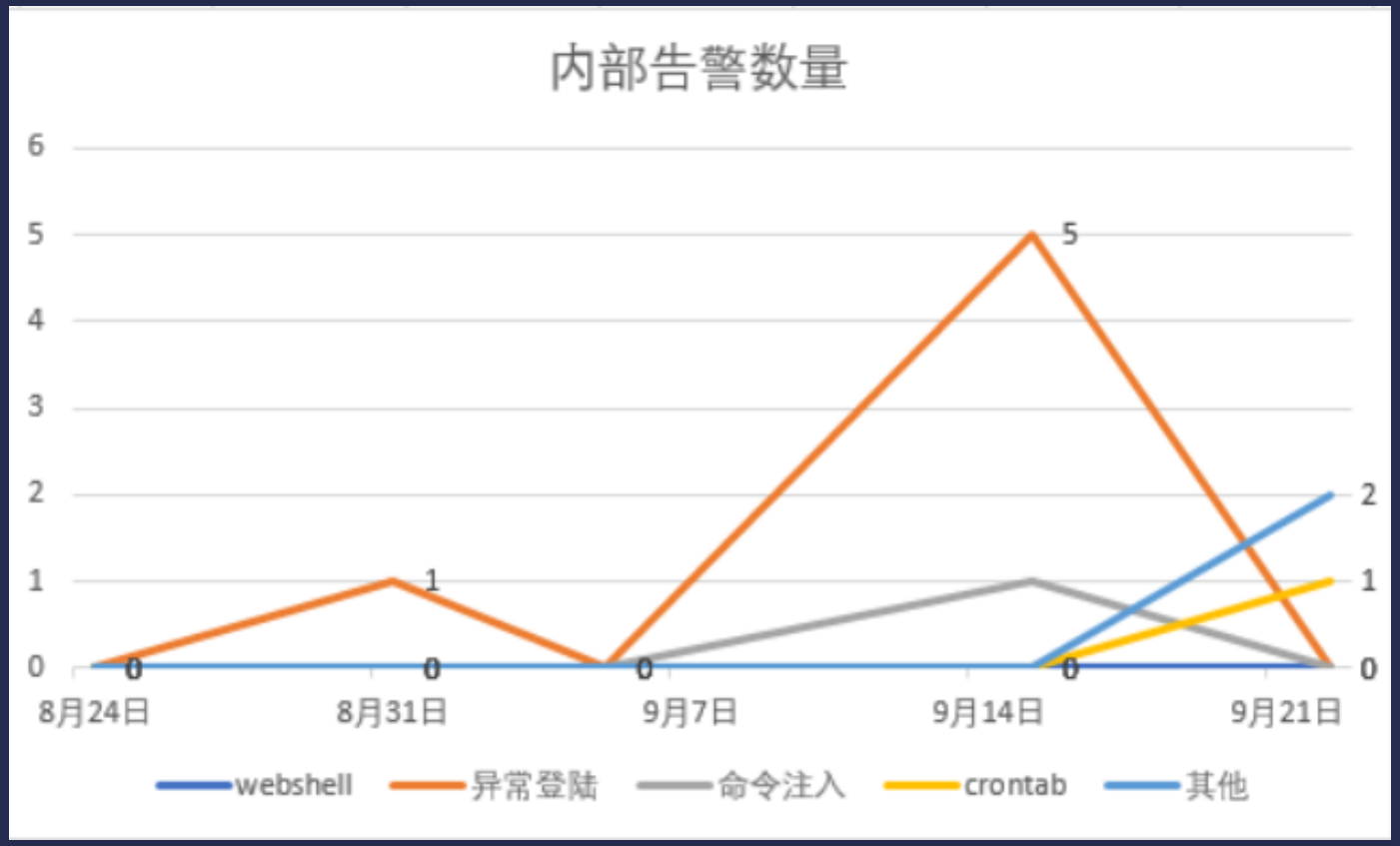
- 编写Sql检测规则
- 添加黑白名单过滤

### 研发人员

- scala quasiquotes对规则引擎进行简单更新

# UCloud安全中心的规则引擎

## 规则引擎告警情况



# UCloud安全中心的规则引擎

## 规则引擎告警方式

- 邮件
- 短信
- 微信
- 电话

# 目录

1. 大数据与入侵及风险检测
2. 规则引擎与入侵及风险检测
3. UCloud安全中心的规则引擎
4. 规则引擎的故障检测和高可用
5. 优化大数据安全分析引擎-UEBA

# 规则引擎的故障检测和高可用

- 引擎运行状态监控
  - 统计处理数据和告警数据-累加器
- 引擎故障检测告警及恢复
  - 引擎故障-yarn
  - 故障恢复-自定义服务
  - 故障原因分析及告警-自定义服务
- 引擎高可用
  - 引擎系统基于zk做了两个节点的高可用

# 目录

1. 大数据与入侵及风险检测
2. 规则引擎与入侵及风险检测
3. UCloud安全中心的规则引擎
4. 规则引擎的故障检测和高可用
5. 优化大数据安全分析引擎-UEBA

# 优化大数据安全分析引擎-UEBA

## UEBA

- User and Entity Behavior Analytics

  用户和实体行为分析

## 分析

- 行为或者属性数据抽象成特征向量
- 特征-统计分析，Sql分析，机器学习

# 优化大数据安全分析引擎-UEBA