



## 转转权限管理系统的落地

宋斯旻 / 20181222

## 个人介绍

- 转转安全工程师 “一个人的安全部”
- 擅长安全应急响应和日志分析。
- 曾在启明星辰、知道创宇等工作，某公司内鬼盗窃100个比特币主要应急人
- 目前工作内容主要为安全开发，企业内部安全平台化。

# 目录

01 两个运维安全问题的解决方案

02 服务器权限管理系统的自研路程



## 两个运维安全问题的解决方案

## 灵魂拷问一：我的同事有没有把内部系统暴露在公网上？

2016-03-28：厂商已经确认，细节仅向厂商公开

2016-04-07：细节向核心白帽子及相关领域专家公开

2016-04-17：细节向普通白帽子公开

2016-04-27：细节向实习白帽子公开

2016-05-12：细节向公众公开

### 简要描述：

如题

### 详细说明：

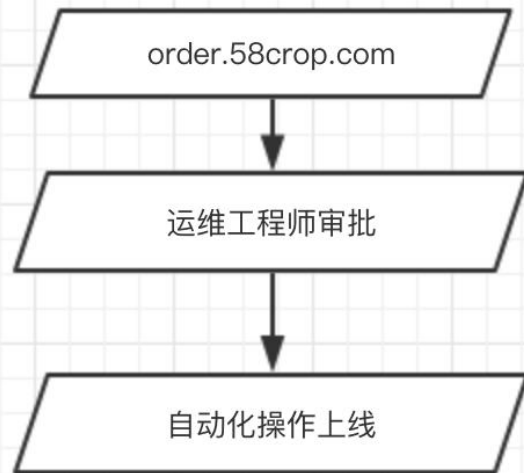
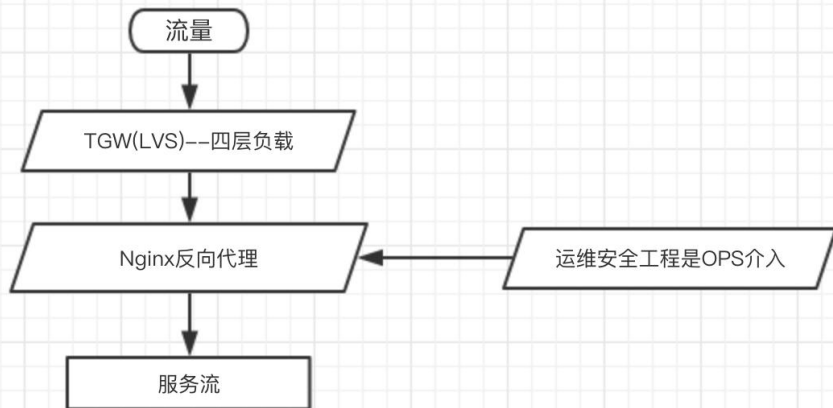
乐视影业临时简历预览系统未授权访问，导致用户敏感信息泄露

<http://event.leyingke.com/spec/recruitment/personal/>



简历列表 总数: 1230(包含重复)

## 灵魂拷问一之业界无比成熟的解决方案



## 灵魂拷问二：我的同事有没有把敏感服务开放到公网上

2016-04-07	网易某站点Zookeeper未授权访问	未授权访问/权限绕过	路人甲
2016-04-06	网易163某分站存在SQL注入	SQL注射漏洞	getshell1993
2016-04-03	网易163某站点存在隐式命令注入	命令执行	lijiejie
2016-04-01	网易163某站点MySQL报错注入	SQL注射漏洞	lijiejie
2016-03-31	网易某数据库存在弱口令涉及一点点数据	服务弱口令	Yeats
2016-03-30	网易某站Rsync未授权访问（涉及大量备份文件/源码）	系统/服务运维配置不当	V1ct0r
2016-03-29	网易某站点MySQL注入(root)和备份文件泄漏	SQL注射漏洞	lijiejie
2016-03-28	网易某站点MySQL报错注入漏洞	SQL注射漏洞	lijiejie

## 灵魂拷问二之业界成熟的解决方案

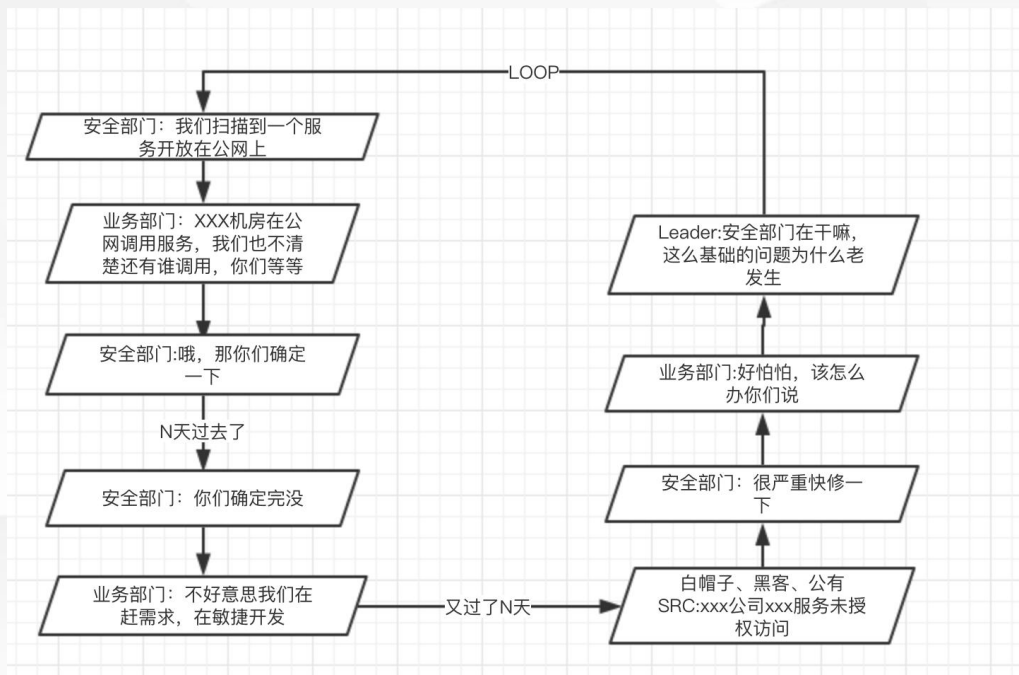
```
[root@localhost ~]# route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          0.0.0.0        0.0.0.0         UG    0      0      0 eth1
0.0.0.0          0.0.0.0        0.0.0.0         UG    0      0      0 eth1
0.0.0.0          0.0.0.0        0.0.0.0         U    0      0      0 tunnat
```

缺省路由不初始化，即只初始化生产环境的路由交换



## 思考：为何上述体量的互联网公司会出现这种问题？

- 血泪教训：运维安全应该在企业成立之初就介入，否则下面的剧本难以避免





# 转转权限管理系统的自研路程

## 我们为什么要自研权限管理系统

- 互联网企业商业堡垒机的问题-与自动化运维与生产冲突

我希望在我的mac上执行一个.sh脚本调用远程ansible执行playbook给管理服务器推送命令

我在我的服务器上写一个crontab，能定期从某台服务器上拉取数据，然后消费写入kafka

...

商业堡垒机能否进行ssh穿透？是否需要二次开发？

服务器不行加key呗，这样服务器之间的自动化运维和生产就能解决了？

# 转转权限管理系统的展现

转转权限管理平台

我的机器权限查询与操作

KDC用户管理

服务器权限管理

运维工具与系统管理

特殊权限管理

特殊审批与审批流程管理

日志审计

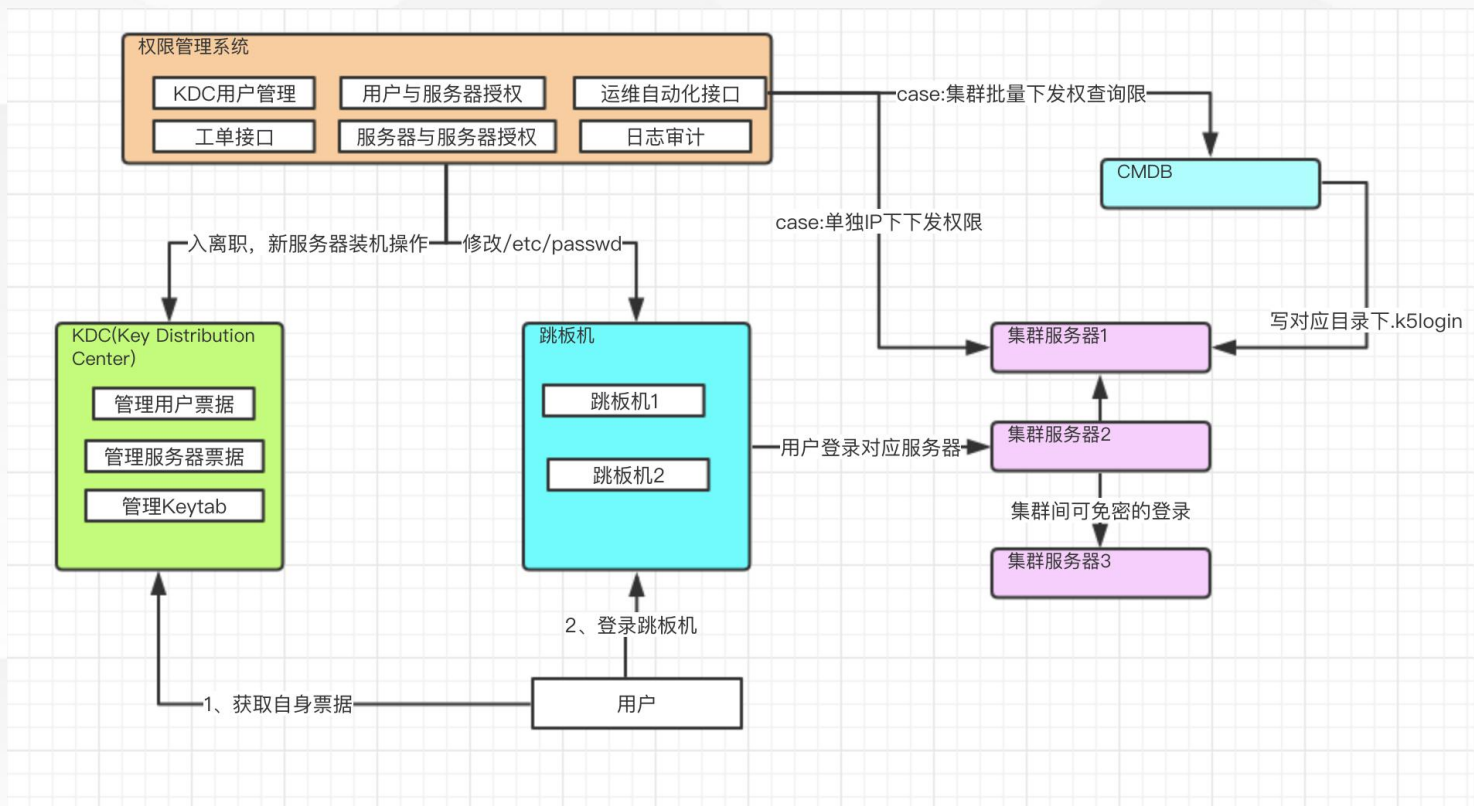
宋斯阳(songsyang)

服务器IP: 权限名称: 搜索

我的权限列表

服务器IP	拥有权限	本次权限周期(单位:天)	到期时间	操作(部分独立申请的特殊长期权限无法一键续期)
10.10.10.1	root	365	2019-08-08T00:00:00	一键续期
10.10.10.2	root	365	2019-06-29T00:00:00	一键续期
10.10.10.71	work	365	2019-07-02T00:00:00	一键续期
10.10.10.8	root	365	2019-07-05T00:00:00	一键续期
10.10.10.9	root	365	2019-07-05T00:00:00	一键续期
10.10.10.10	root	365	2019-07-05T00:00:00	一键续期
10.10.10.11	root	365	2019-10-08T00:00:00	一键续期
10.10.10.12	root	365	2019-10-08T00:00:00	一键续期
10.10.10.12	work	365	2019-10-08T00:00:00	一键续期
10.10.10.13	work	365	2019-10-08T00:00:00	一键续期

## 转转权限管理系统的整体架构与调用逻辑



## KDC的主从搭建

- 纯运维工作，按照相关BLOG文档进行搭建即可，注意控制好ACL文件

```
slave_datatrans.cjtx148-16-15.3805.org.last_prop  
[root()@ ~]# cat /var/kerberos/krb5kdc/kadm5.acl  
*/admin@ ~ COM *  
[root()@ ~]#
```

<https://blog.csdn.net/high2011/article/details/59480568>

## 用户初始化操作(建议员工OA名称来实现)

- KDC:

```
[root()@ ]# kadmin.local
Authenticating as principal host/admin@ with password.
kadmin.local:
kadmin.local:
kadmin.local: addp
addpol addprinc
kadmin.local: addp
addpol addprinc
kadmin.local: addprinc yourname
```

- 跳板机:

```
[root()@ ]# useradd yourname
```

## 服务器初始化操作

- 在每台服务器上往KDC中注册相关信息

```
kadmin.local: addprinc -randkey host/hostname
```

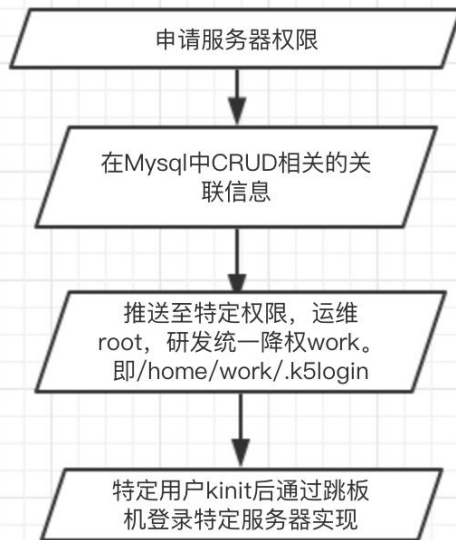
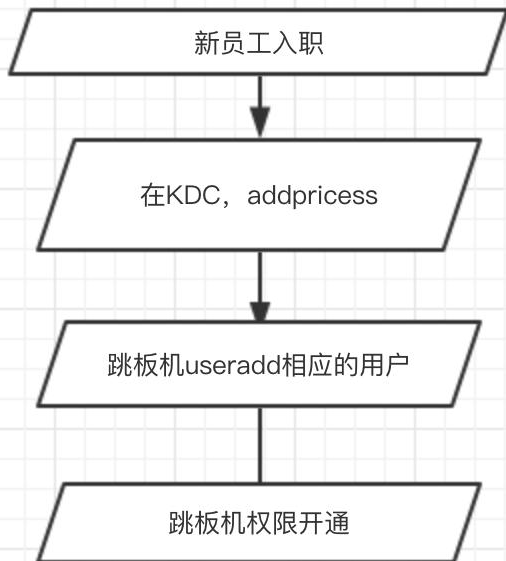
- 每台导出keytab

```
kadmin.local: ktadd host/hostname
```

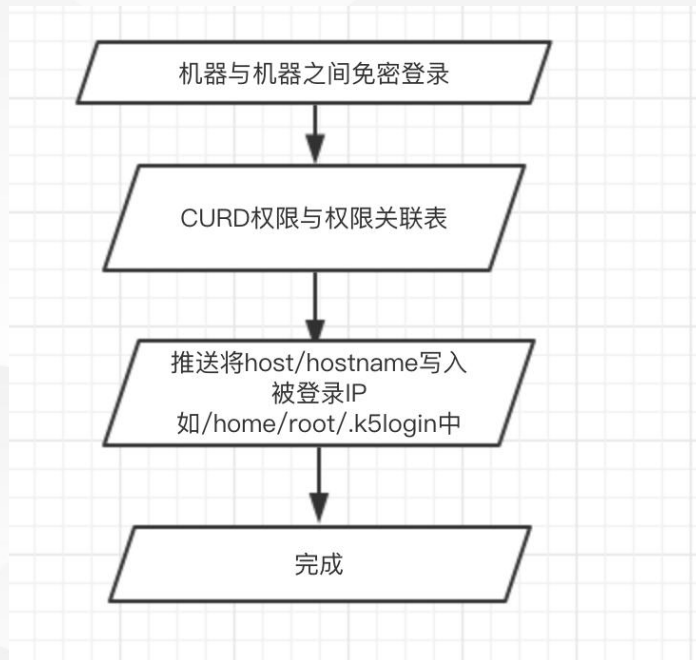
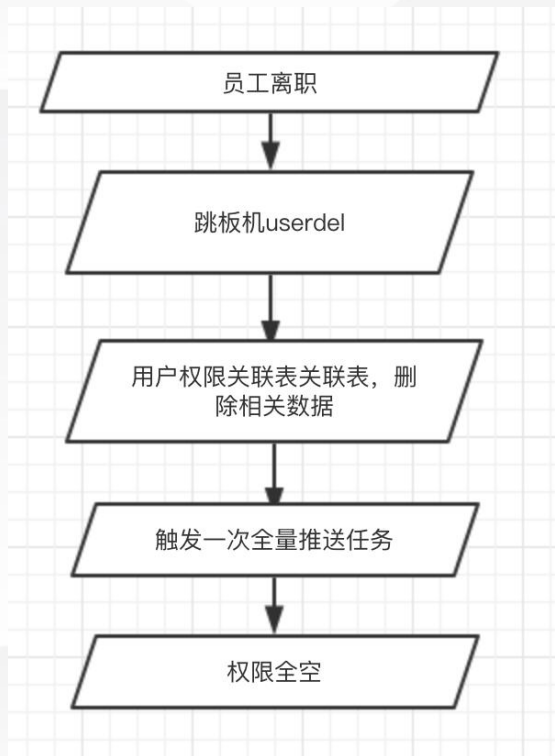
注意: hostname用服务器域名替代、hostname之间要有正反解, 用dig和dig -x 进行验证



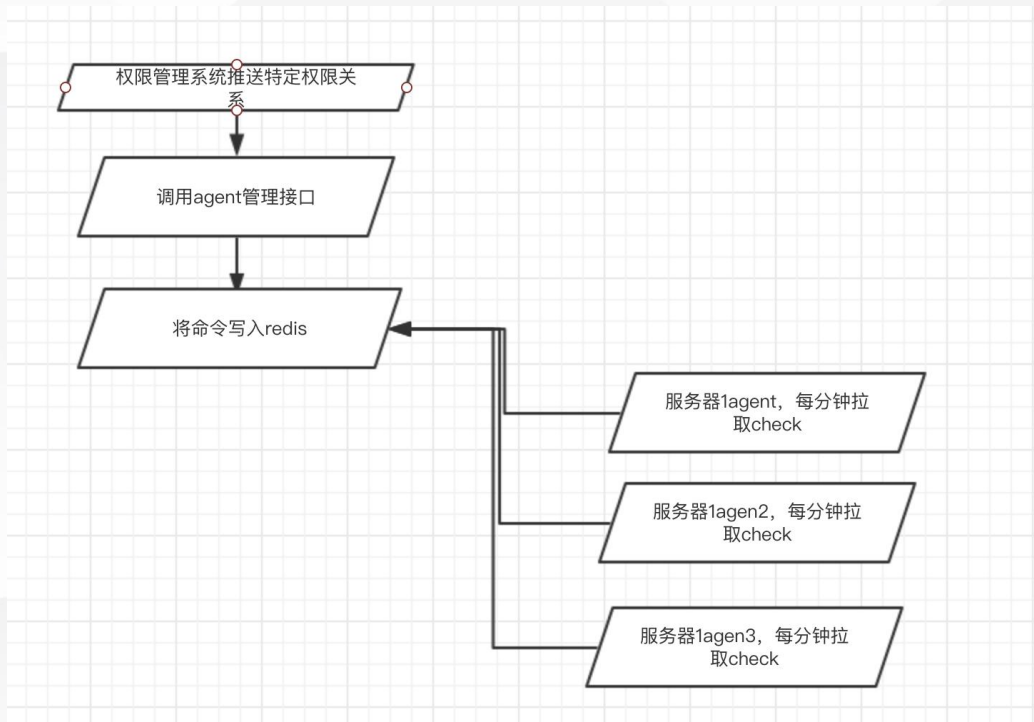
## 封装Web管理系统关键业务逻辑



## 封装Web管理系统关键业务逻辑



## 推送agent的设计



**明眼人是不是看到这里觉得这个系统少了点啥？**

**屏幕录制**

**异常行为实时监测**

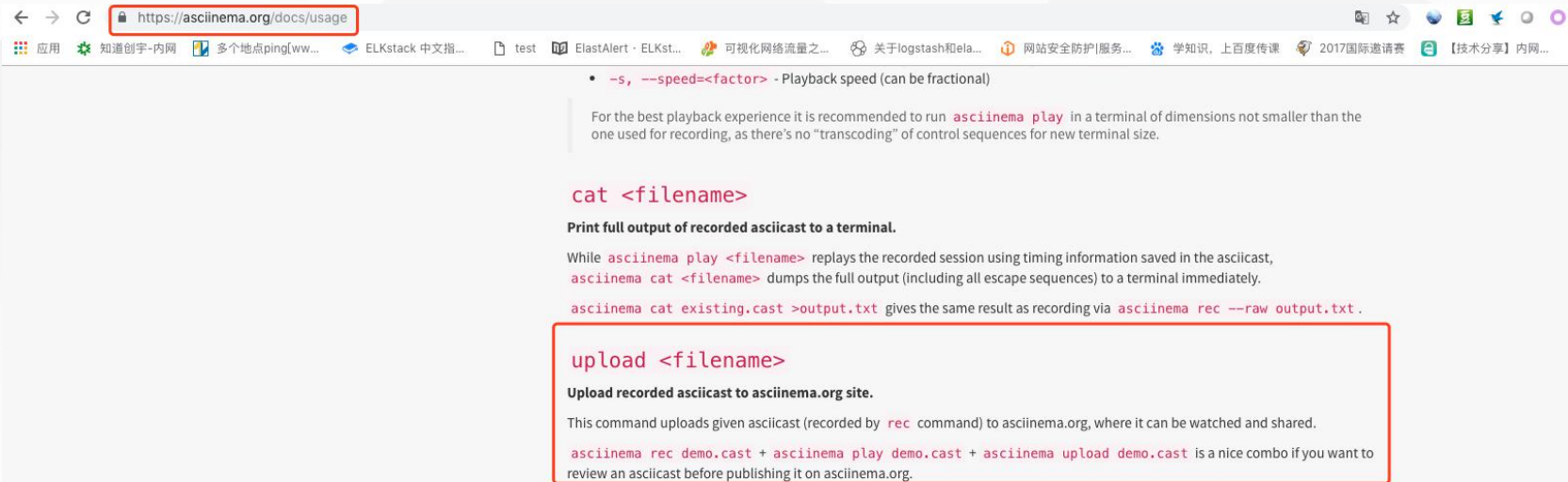
## || 屏幕录制（记录命令回显和Vim操作）

技术选型：

**ttyrpld - 内核级别keylogger**

**asciinema – 基于python的屏幕录制工具，有坑**

# 屏幕录制



← → ↻ <https://asciinema.org/docs/usage>

应用 知道创宇-内网 多个地点ping[ww... ELKstack 中文指... test ElastAlert · ELKst... 可视化网络流量之... 关于logstash和ela... 网站安全防护|服务... 学知识, 上百度传课 2017国际邀请赛 【技术分享】内网...

- `-s, --speed=<factor>` - Playback speed (can be fractional)

For the best playback experience it is recommended to run `asciinema play` in a terminal of dimensions not smaller than the one used for recording, as there's no "transcoding" of control sequences for new terminal size.

### cat <filename>

**Print full output of recorded asciicast to a terminal.**

While `asciinema play <filename>` replays the recorded session using timing information saved in the asciicast, `asciinema cat <filename>` dumps the full output (including all escape sequences) to a terminal immediately.

`asciinema cat existing.cast >output.txt` gives the same result as recording via `asciinema rec --raw output.txt`.

### upload <filename>

**Upload recorded asciicast to asciinema.org site.**

This command uploads given asciicast (recorded by `rec` command) to asciinema.org, where it can be watched and shared.

`asciinema rec demo.cast + asciinema play demo.cast + asciinema upload demo.cast` is a nice combo if you want to review an asciicast before publishing it on asciinema.org.

## 屏幕录制

```
python3 /opt/asciinema/asciinema/__main__.py rec --stdin -c "[ $UID -ne 0 ] && sh /opt/jump.sh" -q $file  
fi  
  
if [ "$UID" -ne 0 ]  
then  
    exit  
    logout
```

```
replay]# pwd  
/opt/replay
```

```
replay]#
```

## 命令审计

目标：

发现内部人员的不合规不安全行为，以及基本攻击命令

加分项：

基于机器学习分析，undo



## 命令审计

例子：

非DBA员工A莫名其妙从数据库跳板机上dump下了一个.sql文件

非运维员工B，在机器上装了个proxychain

员工C用 `echo "password" | mysql -u -p`

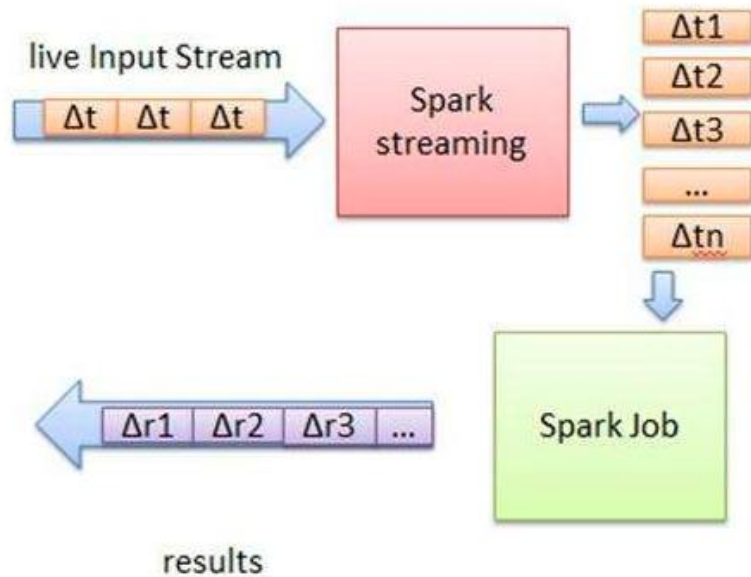
## 命令审计

技术选型：

万年三件套拯救世界之 - ELK生态

报警怎么做？

## 命令审计



# 门槛有多高？

## Spark快速大数据分析



作者: [美] Holden Karau / [美] Andy Konwinski / [美] Patrick Wendell / [加] Matei Zaharia  
 出版社: 人民邮电出版社  
 原作名: Learning Spark: Lightning-Fast Big Data Analysis  
 译者: 王道远  
 出版年: 2015-10  
 页数: 232  
 定价: 59.00元  
 丛书: 图灵程序设计丛书  
 ISBN: 9787115403094

豆瓣评分

8.0 ★★★★★  
 251人评价



更新图书信息或封面

下载

想读

在读

读过

评价: ☆☆☆☆☆

写笔记

写书评

加入购书单

添加到豆列

分享到

推荐

第3章 RDD编程 21

3.1 RDD基础 21

3.2 创建RDD 23

3.3 RDD操作 24

3.3.1 转化操作 24

3.3.2 行动操作 26

3.3.3 惰性求值 27

3.4 向Spark传递函数 27

3.4.1 Python 27

3.4.2 Scala 28

3.4.3 Java 29

3.5 常见的转化操作和行动操作 30

3.5.1 基本RDD 30

3.5.2 在不同RDD类型间转换 37

3.6 持久化(缓存) 38

3.7 总结 40

第4章 键值对操作 41

4.1 动机 41

4.2 创建Pair RDD 42

4.3 Pair RDD的转化操作 42

4.3.1 聚合操作 45

4.3.2 数据分组 49

4.3.3 连接 50

4.3.4 数据排序 51

4.4 Pair RDD的行动操作 52

4.5 数据分区(进阶) 52

4.5.1 获取RDD的分区方式 53

4.5.2 从分区中获取数据的方式 58

4.5.3 影响分区方式的操作 57

4.5.4 示例: PageRank 57

4.5.5 自定义分区方式 59

4.6 总结 61

## 门槛有多高？

```
sconf = SparkConf()
sconf.set('spark.cores.max', 30)
sc = SparkContext(appName='txt', conf=sconf)
ssc = StreamingContext(sc, 60)
brokers = "192.168.1.1:9092;192.168.1.2:9092;192.168.1.3:9092"
topic = "nginx_data"
start = 70000
partition = 0
nginx_data = KafkaUtils.createDirectStream(ssc, [topic], kafkaParams={"metadata.broker.list": brokers})
```

```
nginx_data.filter(lambda x: alarm[x])
```

```
def insertredis(rdd, redis_connect):
    try:
        str = rdd.collect()
        for item in str:
            print item
            redis_connect.insertQueue('ipalert', item)
    except Exception as e:
        print e
```

## 互联网企业运维安全的核心矛盾

- 技术人员技术水平高，喜欢自己搞很多东西和新鲜事物，最后不可控
- 节奏快，上线频繁，安全要浸润业务，却不能阻止业务的快速迭代和发展
- 做产品就避免不了被吐槽，苦力活，众口难调，需求古怪，自研承受非议和压力大

Q&A



转 转

**THANK YOU**