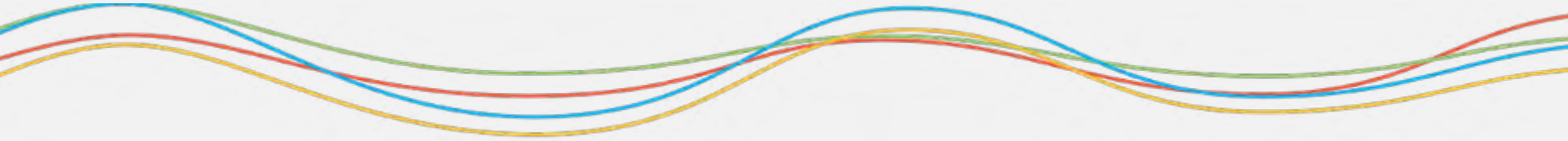
Disaster Engineer —逆向运维

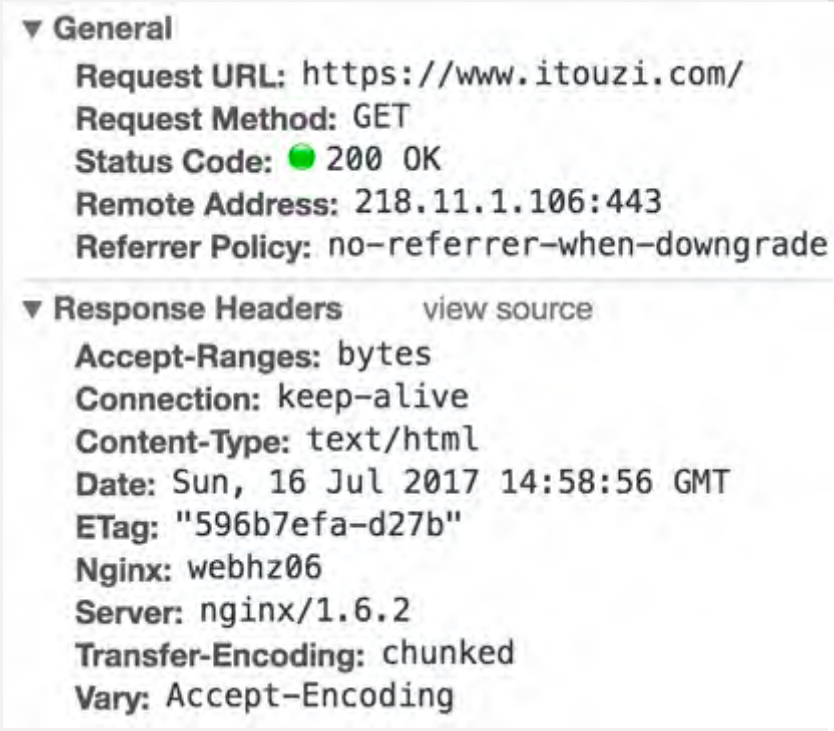
爱投资—李鑫



1

传统运维

运维好似冰山，深度如冰山之下看不见；效果如冰山之上可感知

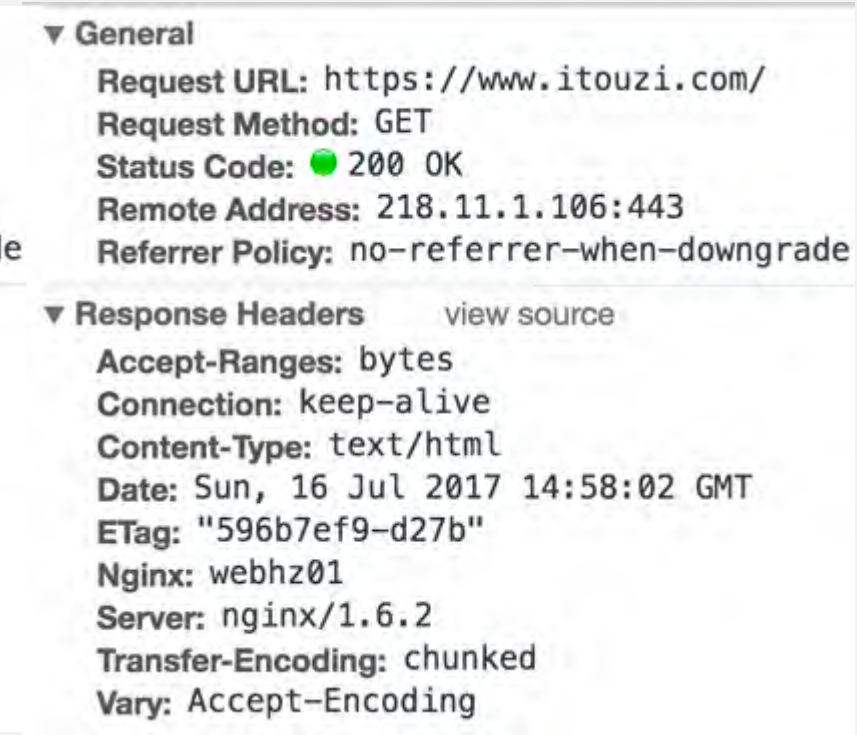


▼ General

Request URL: https://www.itouzi.com/
Request Method: GET
Status Code: 200 OK
Remote Address: 218.11.1.106:443
Referrer Policy: no-referrer-when-downgrade

▼ Response Headers view source

Accept-Ranges: bytes
Connection: keep-alive
Content-Type: text/html
Date: Sun, 16 Jul 2017 14:58:56 GMT
ETag: "596b7efa-d27b"
Nginx: webhz06
Server: nginx/1.6.2
Transfer-Encoding: chunked
Vary: Accept-Encoding



▼ General

Request URL: https://www.itouzi.com/
Request Method: GET
Status Code: 200 OK
Remote Address: 218.11.1.106:443
Referrer Policy: no-referrer-when-downgrade

▼ Response Headers view source

Accept-Ranges: bytes
Connection: keep-alive
Content-Type: text/html
Date: Sun, 16 Jul 2017 14:58:02 GMT
ETag: "596b7ef9-d27b"
Nginx: webhz01
Server: nginx/1.6.2
Transfer-Encoding: chunked
Vary: Accept-Encoding


VeriSign Class 3 Public Primary Certification Authority - G5
Symantec Class 3 EV SSL CA - G3
www.itouzi.com
www.itouzi.com
签发者：Symantec Class 3 EV SSL CA - G3
过期时间：2018年5月28日 星期一 中国标准时间 上午7:59:59
此证书有效
细节
好

SSLLABS

APMCon

SL Report: www.iseecapital.com (120.55.226.220)

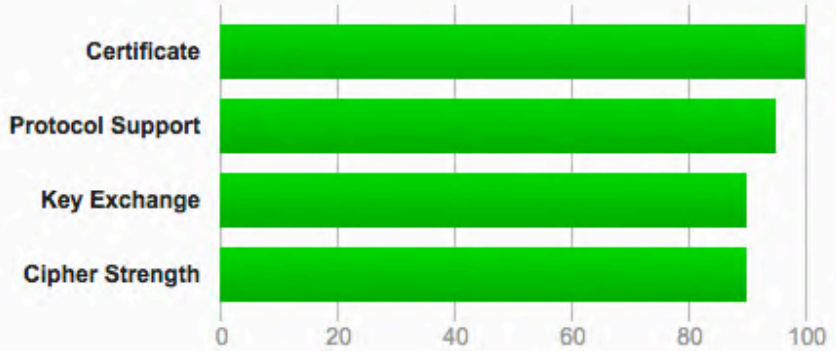
essed on: Sat, 29 Jul 2017 06:28:24 UTC | Hide | Clear cache

Scan Anothe

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

Q HSTS

Tips

请求头——

Strict-Transport-Security: max-age=172800

注意——

部分集群配置SSL-Cache

Safari浏览器SSL断开连接

2

DevOps

不会开发的运维不是好测试

- 日志存储
- 容错与扩展
- 预警/报警
- 自动化

冰山之下

APMCon

2. 掌握Java或Python，精通Shell，能熟练使用来完成日常系统运维等工作；

3. 熟悉Linux操作系统，了解常用开源系统（如LVS、redis、nginx、tomcat等）的架构、配置、优化

4. 网络相关基础知识扎实，对常见网络协议有深刻理解（DNS, HTTP, TCP/UDP, VPN等）；

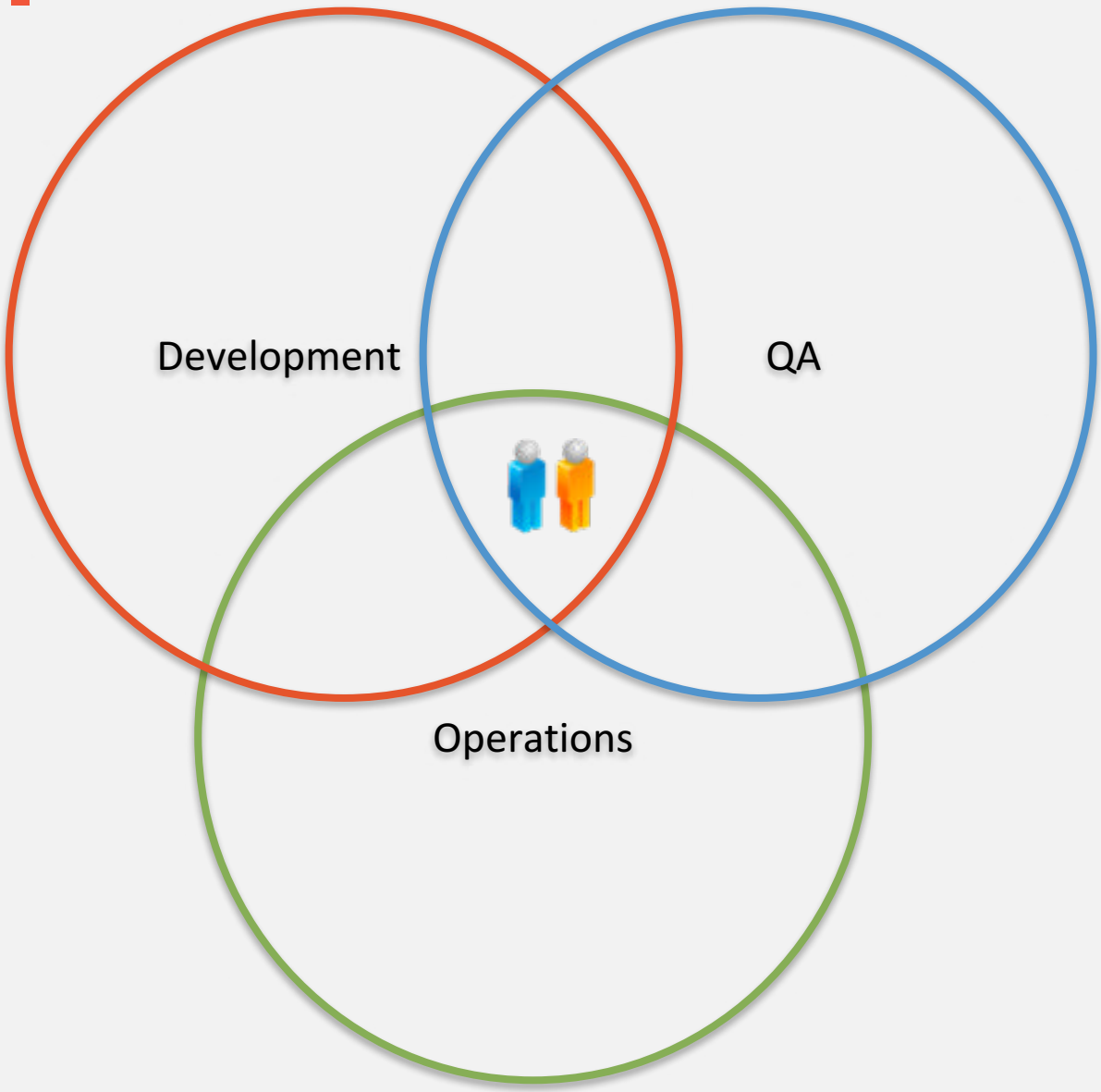
5. 了解Hadoop/HBase/Storm/HDFS/Zookeeper，并有相关编程经验；

6. 熟练使用各种调试抓包工具，能独立分析、解决和归纳问题（有移动设备调试经验者加分，熟悉性能者加分）；

7. 对分布式系统有了解的优先，在开源社群活跃并有积极贡献者优先；（简历请附github个人地址等）

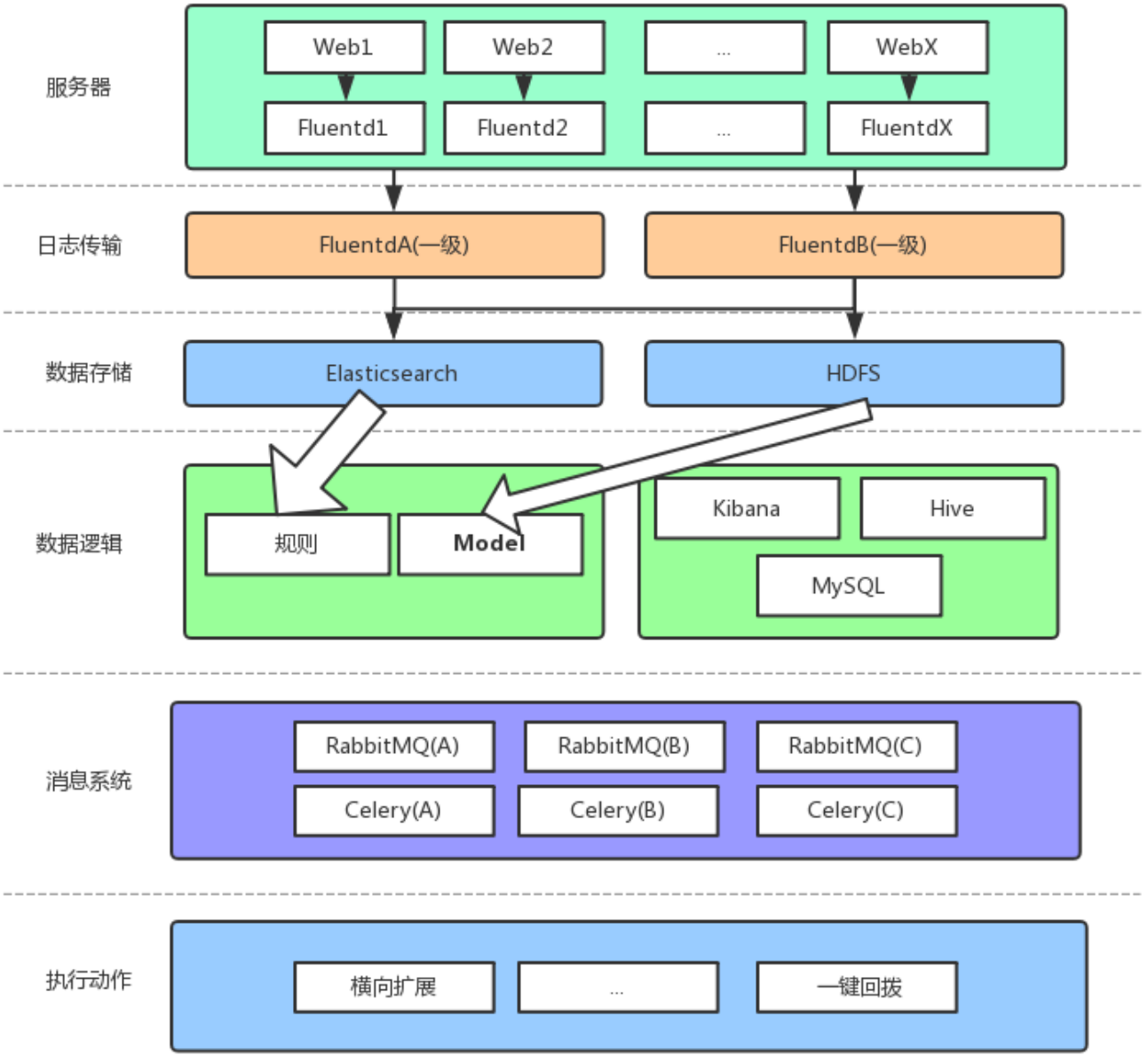
DevOps

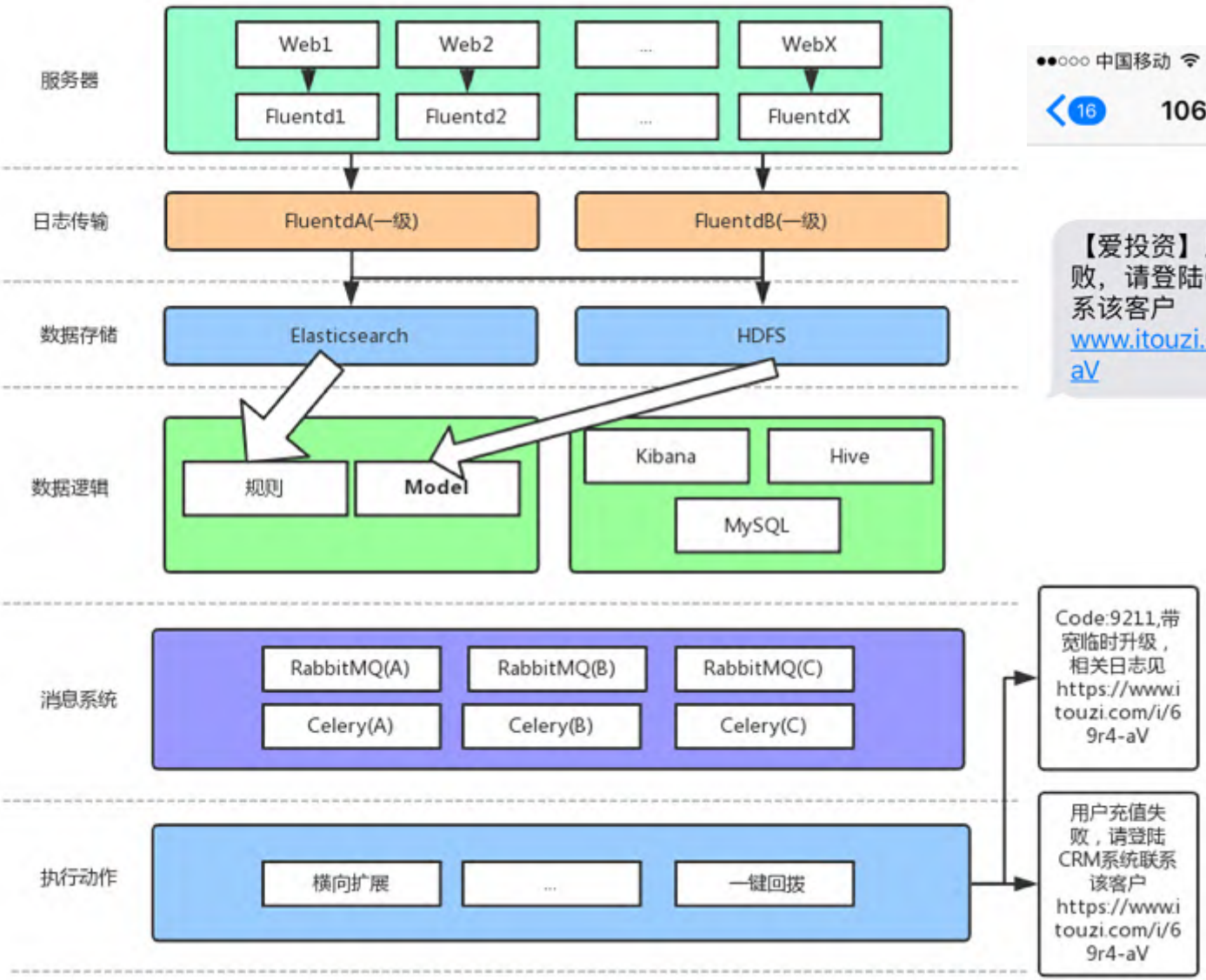
APMCon



- 熟悉计算机网络
- 熟悉Linux
- 使用ZABBIX
- 使用Jenkins
- 使用Ansible
- 搭建ELK

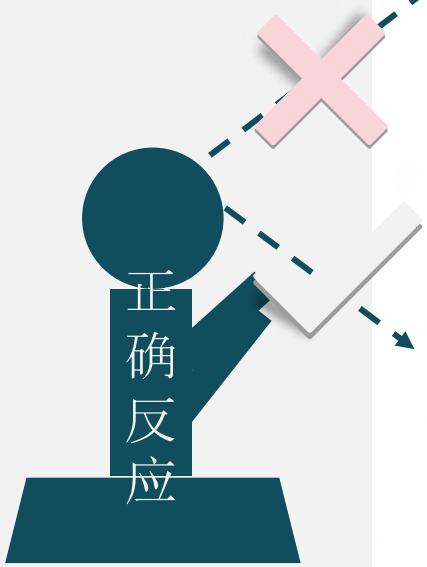
在上线前后，一类可以 加速版本迭代，并保障接近实时的业务异常响应 的IT工程师

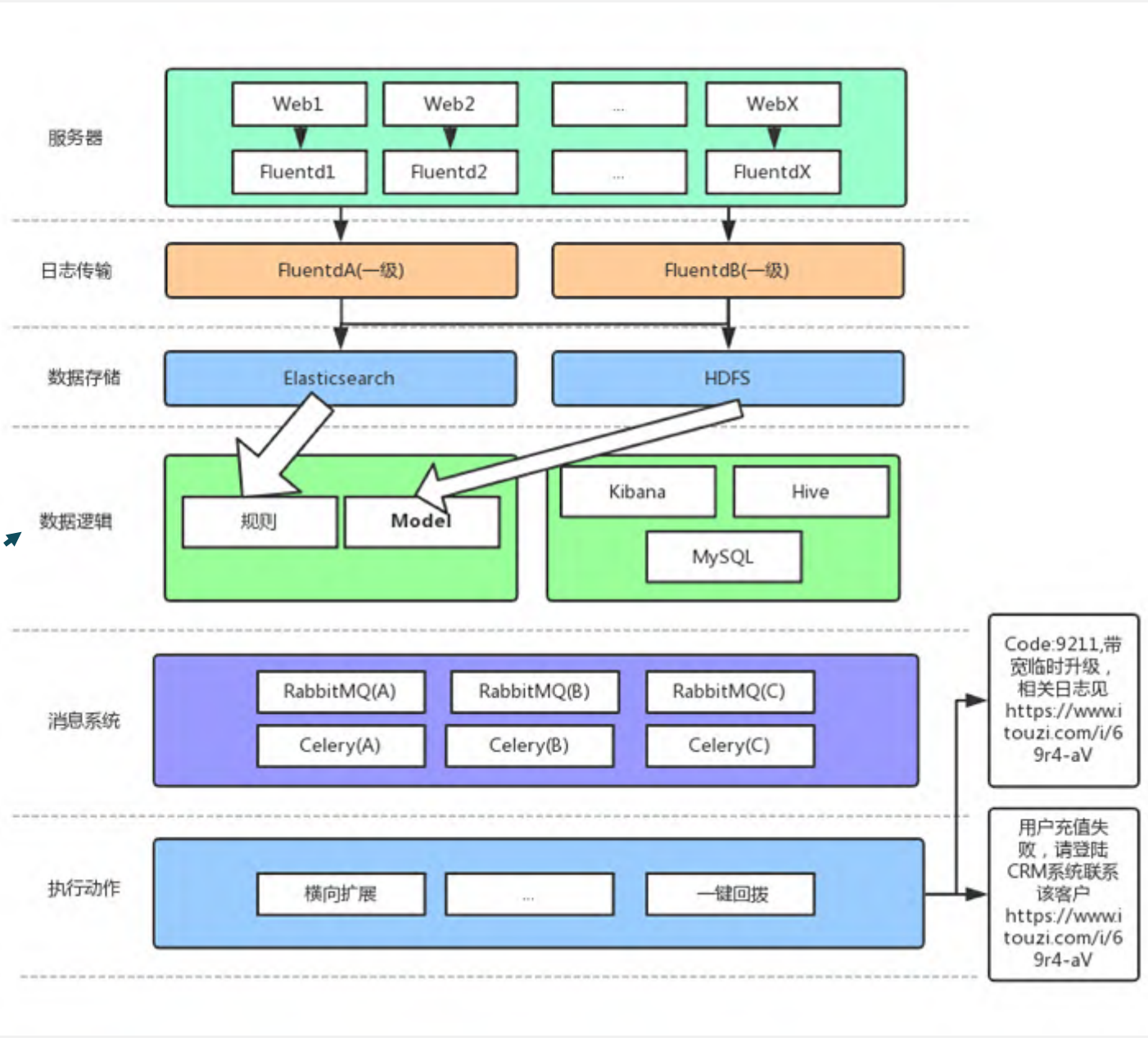



服务器
Web1
Web2
...
WebX
Fluentd1
Fluentd2
...
FluentdX
日志传输
FluentdA(一级)
FluentdB(一级)
数据存储
Elasticsearch
HDFS
数据逻辑
规则
Model
Kibana
Hive
MySQL
消息系统
RabbitMQ(A)
RabbitMQ(B)
RabbitMQ(C)
Celery(A)
Celery(B)
Celery(C)
执行动作
横向扩展
...
一键回拨
Code:9211,带宽临时升级，相关日志见https://www.itouzi.com/i/69r4-aV
用户充值失败，请登陆CRM系统联系该客户https://www.itouzi.com/i/69r4-aV


●●○○○ 中国移动
10:44
16
106906611217281
短信/彩信
今天10:38
【爱投资】用户充值失败，请登陆CRM系统联系该客户
www.itouzi.com/i/69r4-aV

重预测？还是重反应


正确反应


服务器
Web1
Web2
...
WebX
Fluentd1
Fluentd2
...
FluentdX
日志传输
FluentdA(一级)
FluentdB(一级)
数据存储
Elasticsearch
HDFS
数据逻辑
规则
Model
Kibana
Hive
MySQL
消息系统
RabbitMQ(A)
RabbitMQ(B)
RabbitMQ(C)
Celery(A)
Celery(B)
Celery(C)
执行动作
横向扩展
...
一键回拨
Code:9211,带宽临时升级，相关日志见https://www.touzi.com/i/69r4-aV
用户充值失败，请登陆CRM系统联系该客户https://www.touzi.com/i/69r4-aV

用户预测

1. 补充缺失值
2. 人工筛选维度
3. DictVectorizer向量化
4. XGB / RandomForest
5. GridSearchCV

重预测？还是重反应

APMCon

```
import pandas as pd
from sklearn.feature_extraction import DictVectorizer
from sklearn.ensemble import RandomForestClassifier
from xgboost import XGBClassifier
from sklearn.grid_search import GridSearchCV
X_train = train[selected_features]
X_test = test[selected_features]
y_train = train['Invested']
X_train['Age'].fillna(X_train['Age'].mean(), inplace=True)
X_test['Age'].fillna(X_test['Age'].mean(), inplace=True)
dict_vec = DictVectorizer(sparse=False)
X_train = dict_vec.fit_transform(X_train.to_dict(orient='record'))
X_test = dict_vec.transform(X_test.to_dict(orient='record'))
params = {'max_depth':range(2, 7), 'n_estimators':range(100, 1100, 200), 'learning_rate':[0.05, 0.1, 0.25, 0.5, 1.0]}
xgbc_best = XGBClassifier()
gs = GridSearchCV(xgbc_best, params, n_jobs=-1, cv=5, verbose=1)
gs.fit(X_train, y_train)
```

探究知识背景

深度拓展

横向拓展

纵向拓展

与类似的知识联系

与不同的知识联系

真正的运维都是擅长做出正确**反应**的人

而不是**预言家**

AI(Artificial Intelligence):让机器模仿人类智能
IA(Intelligence Amplification)让机器增强人类智能
人的决策反馈使得机器更聪明
机器智能帮助人做出更快更准确的决策

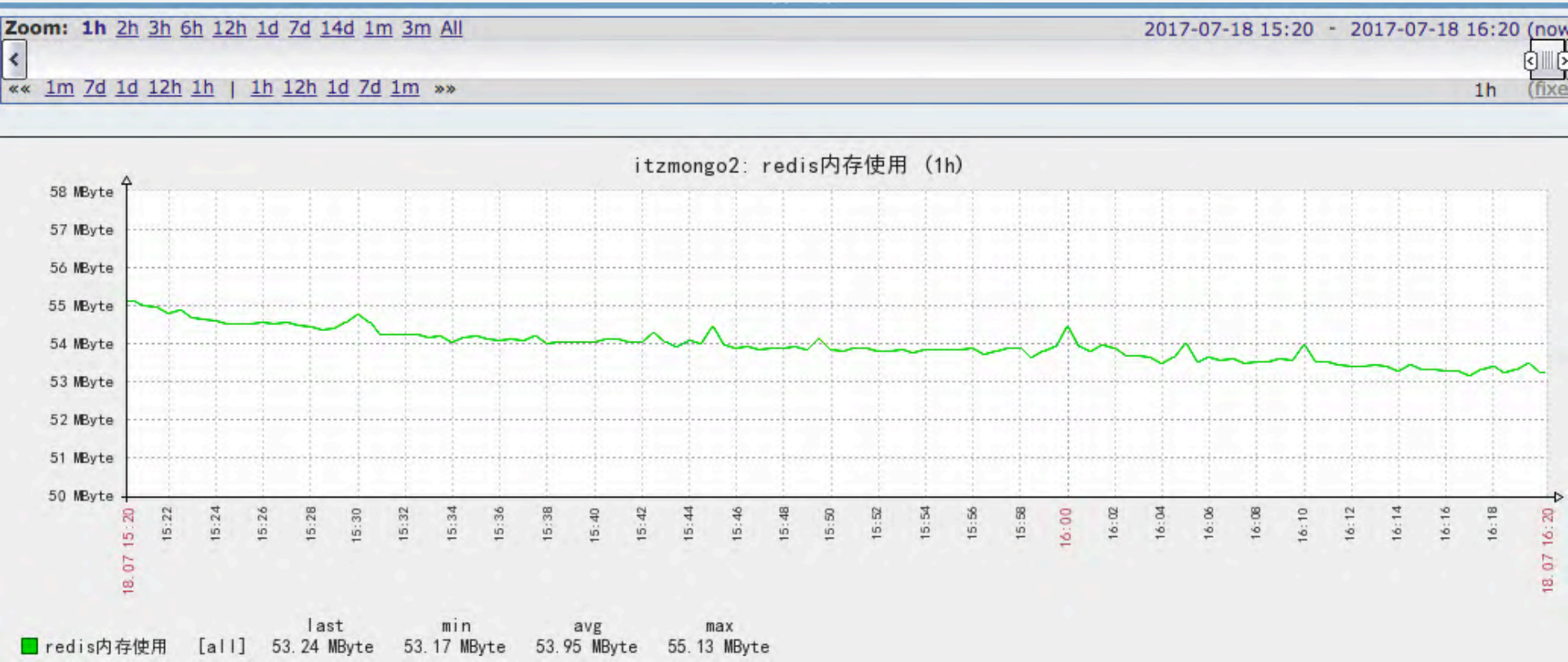
3

IAOps

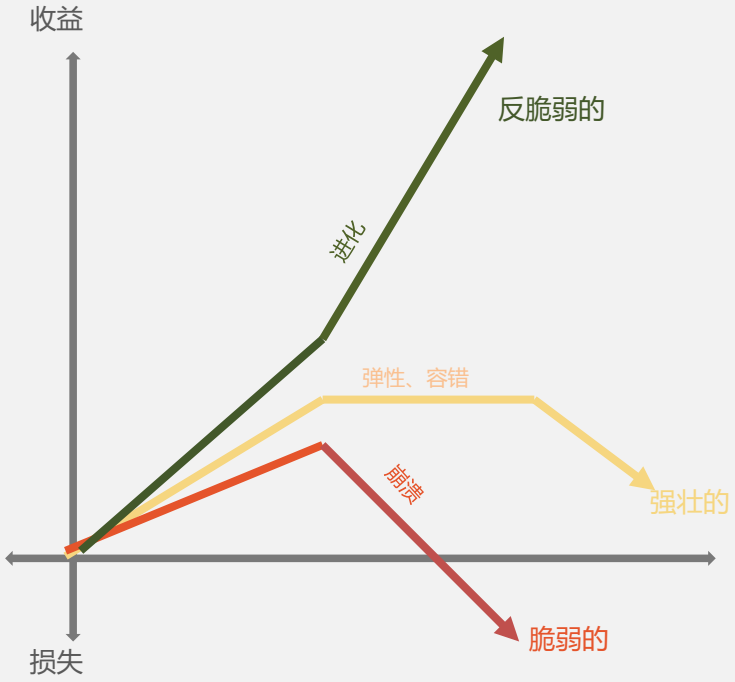
运维发展之路

APMCon

人工 → 自动 → 智能 → 智慧



反脆弱—迭代式进化



脆弱性	强韧性	反脆弱性
		

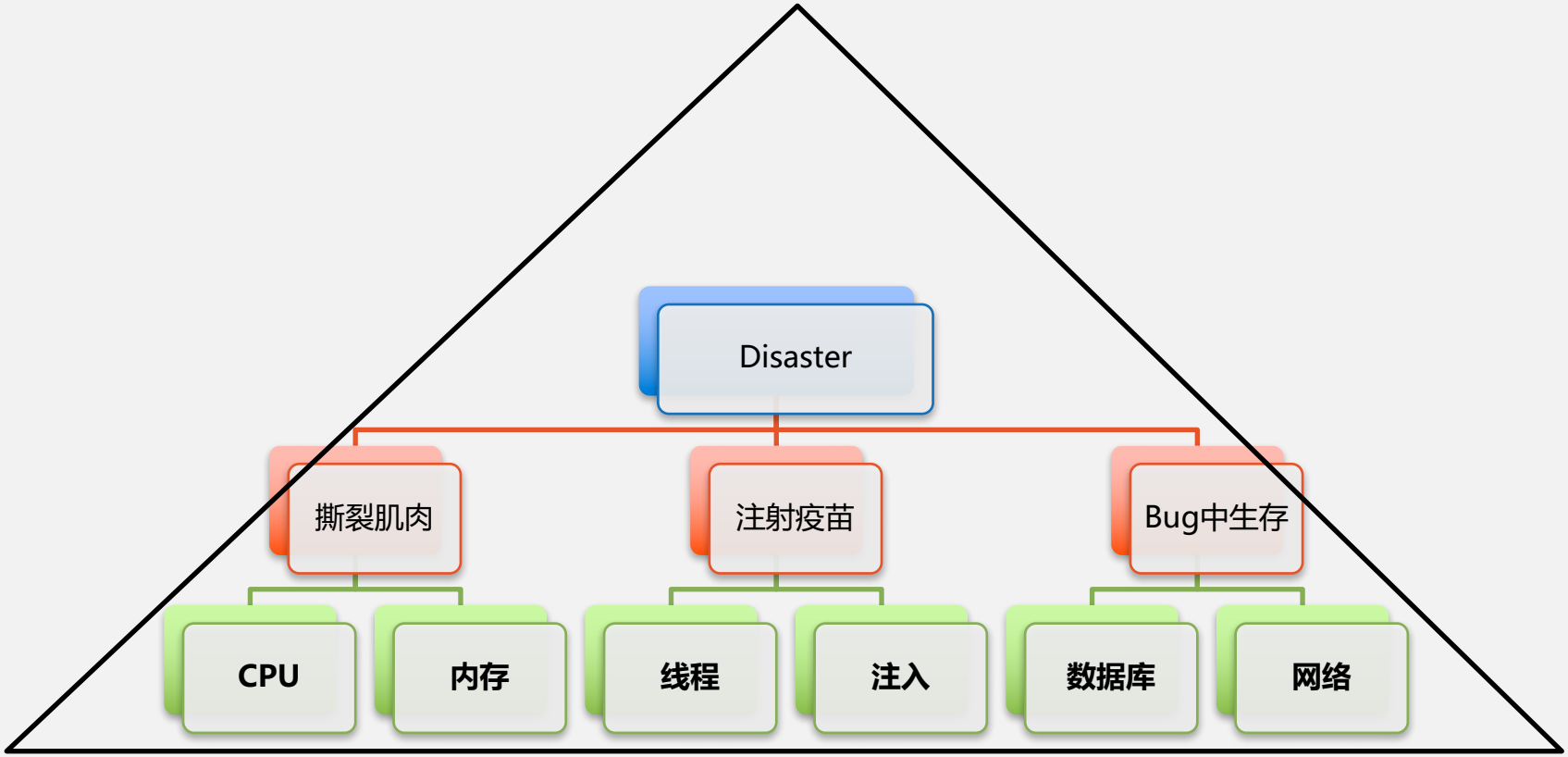
不确定性喜好程度	**厌恶**不确定性 **喜欢**确定性	中性	**喜欢**不确定性 **厌恶**确定性
对不确定性的反应	从确定性中**受益** 从不确定性中**受损**	在任何状态下 既不受损也不受益	从确定性中**受损** 从不确定性中**受益**
喜好领域	秩序领域	中性	混乱领域

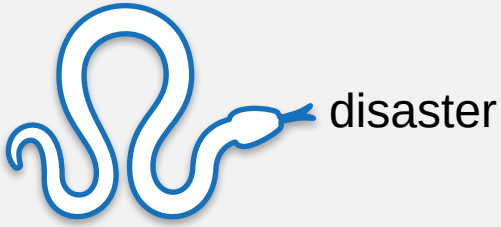
有漏洞升级系统，没漏洞制造漏洞升级系统

4

Disaster

虫洞





疯狂杀戮

APMCon

随机杀掉进程，看程序是否有 预警 报警 自修复 并且 不影响线上业务

Fabric

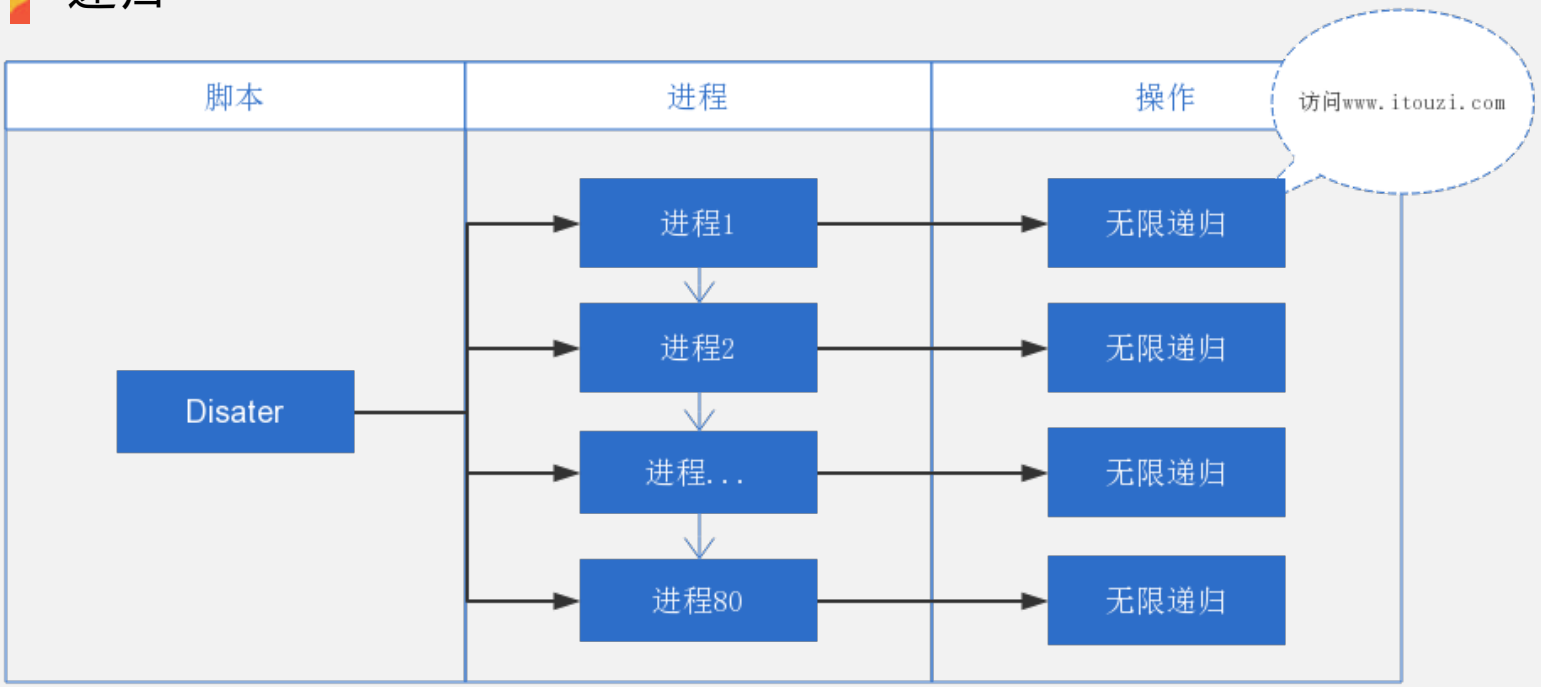
计划执行

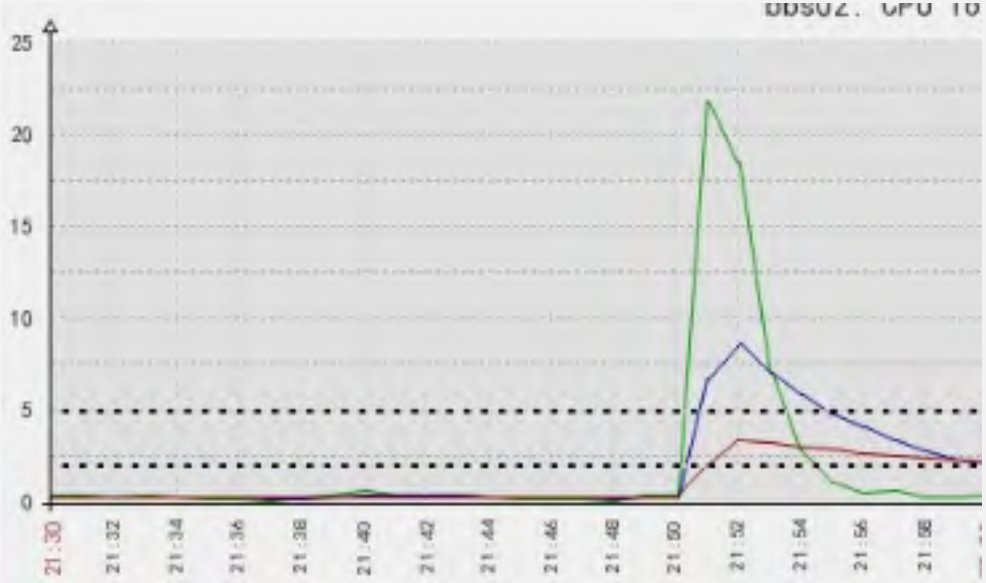
```
ps -ef|grep APMCon |awk ‘{print $2}’|xargs -i -t kill -9 {}
```

实际执行

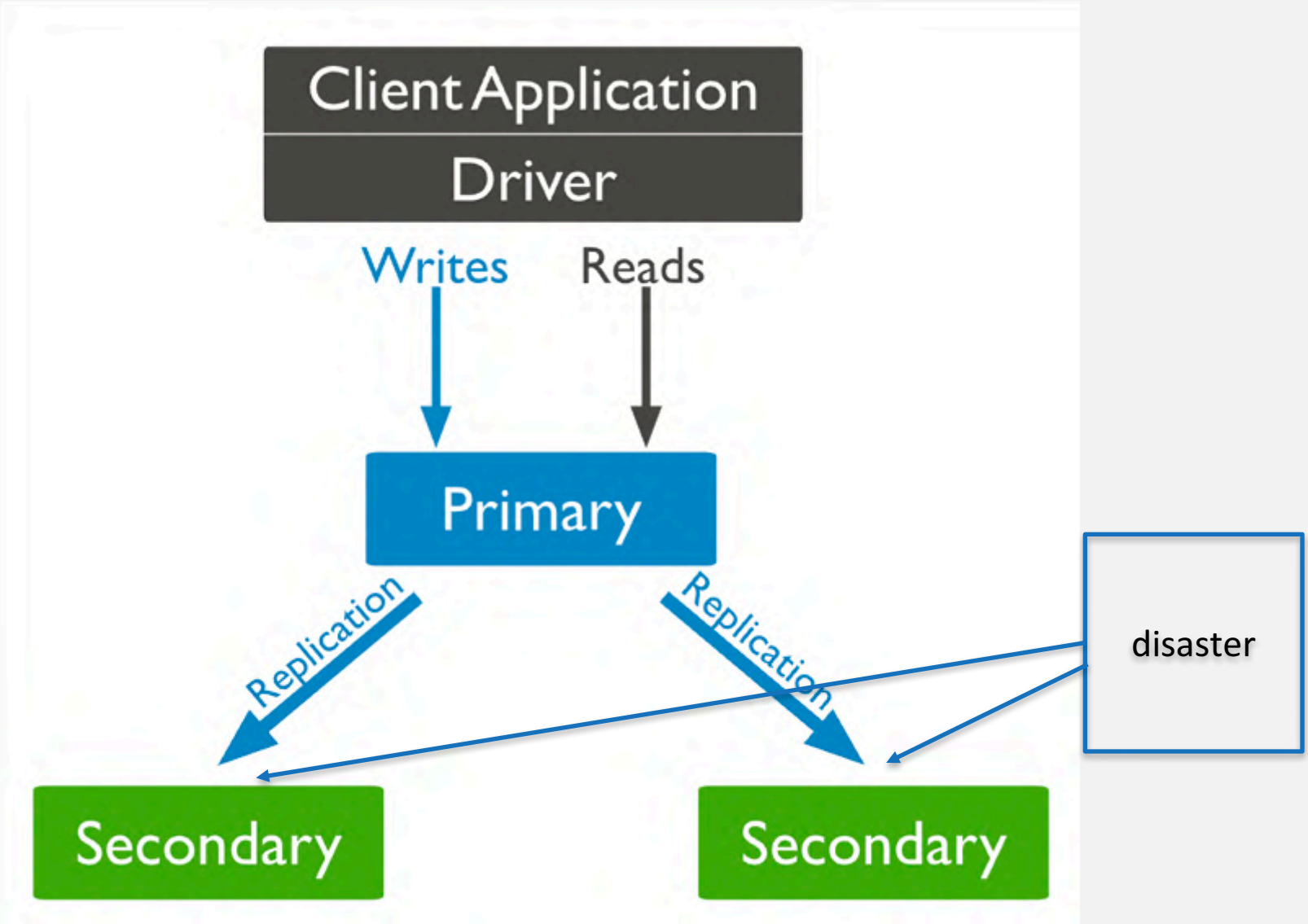
```
“ps -ef{|grep APMCon}|awk '{print $2}'|xargs -i -t kill -9 {}”
```

递归


脚本
进程
操作
访问www.itouzi.com
Disater
进程1
进程2
进程...
进程80
无限递归
无限递归
无限递归
无限递归

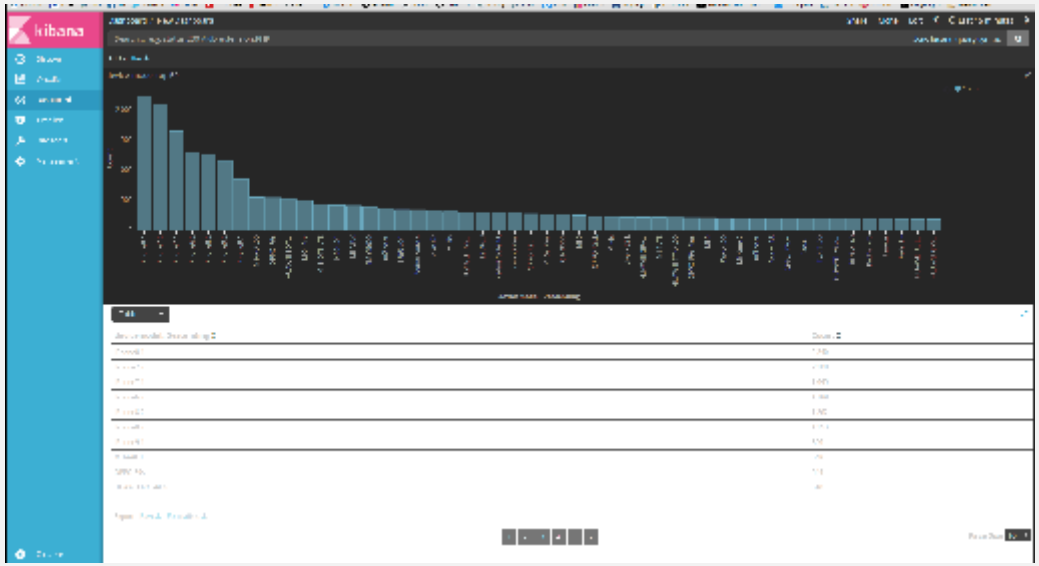

25
20
15
10
5
0
21:30
21:32
21:34
21:36
21:38
21:40
21:42
21:44
21:46
21:48
21:50
21:52
21:54
21:56
21:58

MongoDB副本集


Client Application
Driver
Writes
Reads
Primary
Replication
Replication
disaster
Secondary
Secondary

Disaster之二——掌握工具（Elasticsearch/Kibana5.5）

APMCon



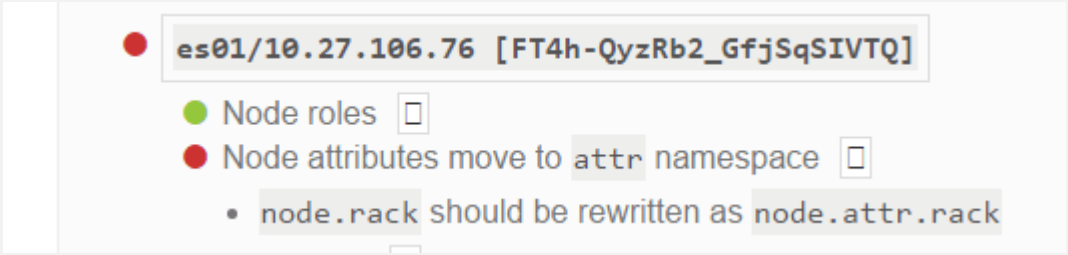
2.3升级到5.5

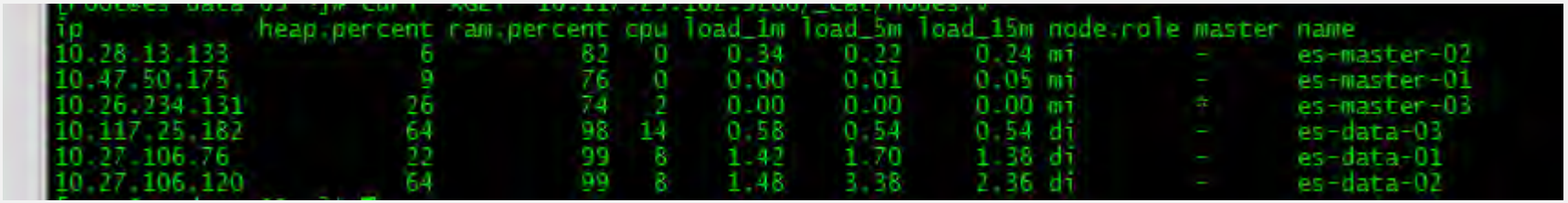
同样配置 2T数据 QPS 快1/3

利用migration检测 平滑升级

5.5 一次请求最多1000个分片

date, numeric， ip 和 Geospatial





APMCon

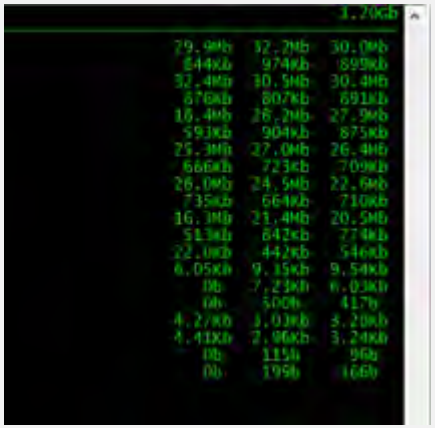
Xteam —— siege –c 50

任务

- 寻找脆弱点；
- SLA评分！

压测

- 大缓存压测网络IO；
- 非缓存压测磁盘IO！



Disaster之二——问题

APMCon

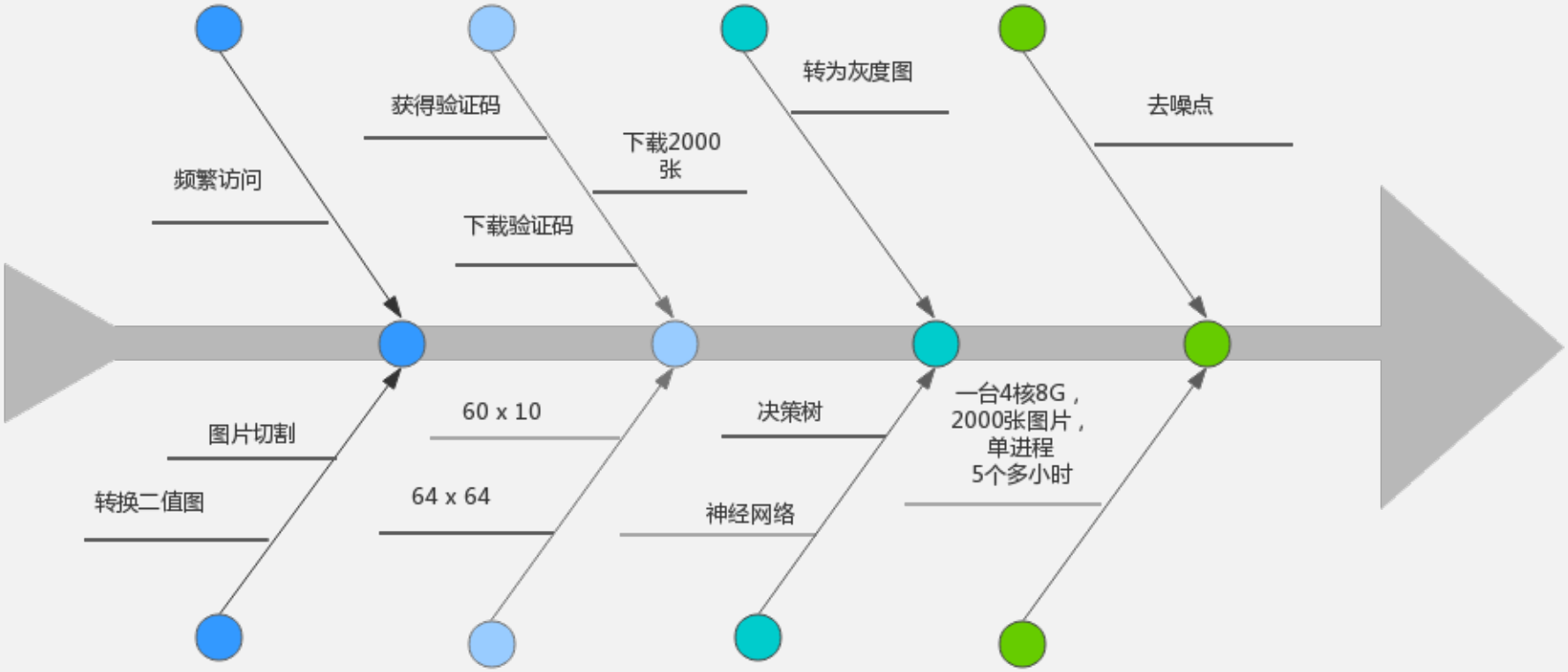
Anemometer 慢SQL分析

Showing 20 results

checksum	snippet	index_ratio	query_time_avg	rows_sent_avg	ts_cnt	Query_time_sum	Lock_time_sum	Rows_sent_sum	Rows_examined_sum	Full_scan_
58D2998B0CF56E07	SELECT distinct dw_u	446.46	4.993713208891887	4992	718	3585.486083984375	0.10355900228023529	3584476	1600322944	
34E97B2A8260DF97	SELECT sum(money) a	5320.00	2.5582717938980144	1	702	1795.9067993164062	0.056527999229729176	702	3734643	
307796BBBF49B243	SELECT	3421874.74	85.56780133928571	10	14	1197.94921875	0.0009679999784566462	140	479062464	
F743692C395A165E	SELECT sum(interest)	34019046.82	19.236003437980276	1	61	1173.3962097167969	0.002919000107795	61	2075161856	
39DB66E7B0E21B21	SELECT COUNT(*) FROM	3747.84	1.5701268334903626	1	426	668.8740310668945	0.04170495846804887	426	1596581	
3589A5739D02B1EE	select user_id ,sum(	680.54	46.33497183663504	50134	14	648.6896057128906	0.0011519999625395644	701883	477660608	
E707317290298F7B	SELECT distinct dw_u	431.42	7.239645755652226	4863	66	477.8166198730469	0.009294000454246998	320963	138471280	
6A5378178D979C57	select a.id,a.user_i	726.23	409.7249755859375	27242	1	409.7249755859375	0.02593499980866909	27242	19783984	
E45411CC72C0CD48	SELECT COUNT(*) FROM	5738.33	2.7457933213975694	1	135	370.6820983886719	0.027658999897539616	135	774674	
93D7494F85D6B169	SELECT interest,valu	6.66	3.8709790459994613	618	87	336.7751770019531	0.007805999834090471	53794	358154	
3070087603108D4F	SELECT * FROM `dw_ac		4.279040362383868	0	74	316.64896681640625	0.007594000082463026	0	131863264	
95AC62D7244B299D	SELECT * FROM `dw_us	22997.29	8.15712511217272	96	37	301.8136291503906	0.005164999980479479	3560	81870360	
73AF033E4BF20E57	SELECT COUNT(*) FROM	9765269.54	20.4636958195613	1	13	266.0280456542969	0.0010110000148415565	13	126948504	
880F4CDE51E35308	SELECT COUNT(*) FROM	37456068.00	15.389204978942871	1	16	246.22727966308594	0.0007779999868944287	16	599297088	
D254FCD5DA2EE063	select user_id,total		4.658919578374818	0	43	200.3335418701172	0.0032819999614730477	0	172539728	
94CF9B70B16CFD3C	select id,user_id,to		4.402464046034702	0	43	189.3059539794922	0.003956999978981912	0	172539728	
A13FAB51F0874C31	select user_id, sum(	61014.19	12.401647295270648	50	14	173.62306213378906	0.0011399999493733048	700	42709936	
5B3562254ABF2F17	SELECT distinct dw_u	432.16	5.169625946969697	4860	33	170.59765625	0.005086999852210283	160372	69306568	
7A43FDC1F337977E	SELECT sum(account_i	352878.21	10.392657143729073	10	14	145.49720001220703	0.0011269999959040433	140	49402960	
A7BC7749113EF131	select id, account,		3.2487485131552054	0	43	139.69616606567383	0.0027149999514222145	0	143337888	

```
SELECT * FROM itz_forum_thread force index(displayorder01) WHERE
`fid`='15' AND `displayorder` IN('0','1','2','3','4')
ORDER BY displayorder DESC, dateline DESC LIMIT 16680, 20;
```

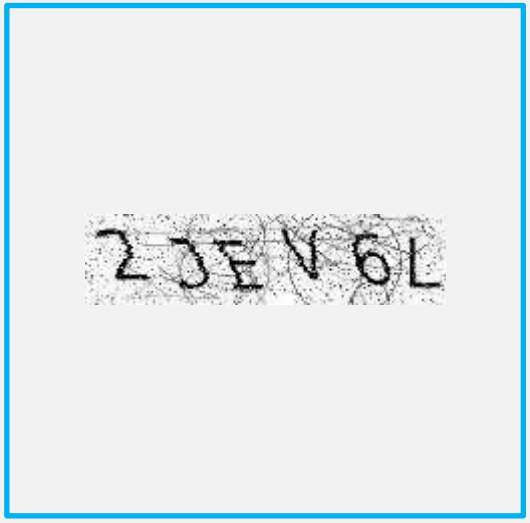
Disaster之二——防范(验证码)

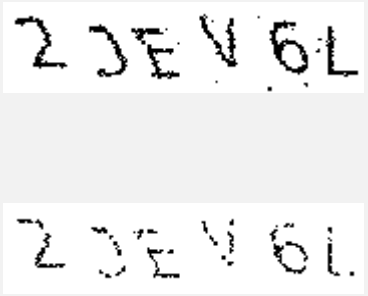


转为灰度图

黑白照片，其实照片里并不是只有黑白两种颜色

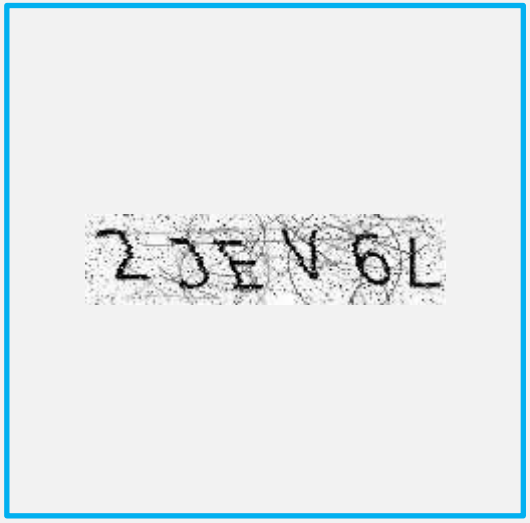
转为二值图，灰度阀值80

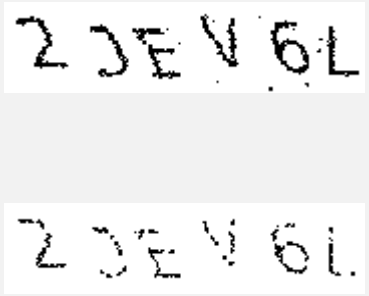




阈值越底，干扰点越少，反之，干扰点越多

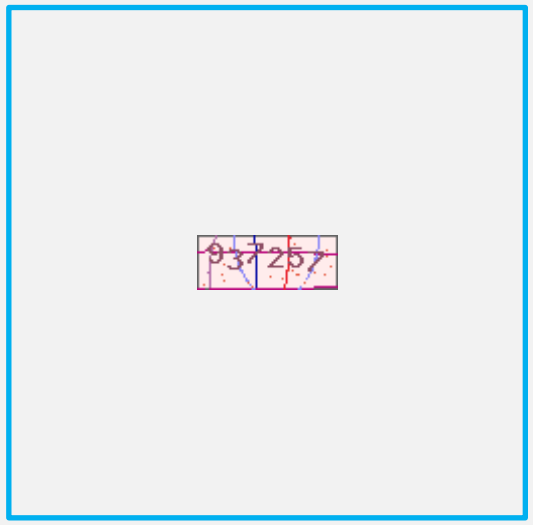
去杂质，周围8个像素中黑色小于3





多次循环去杂质点

极端情况，按照色彩分布

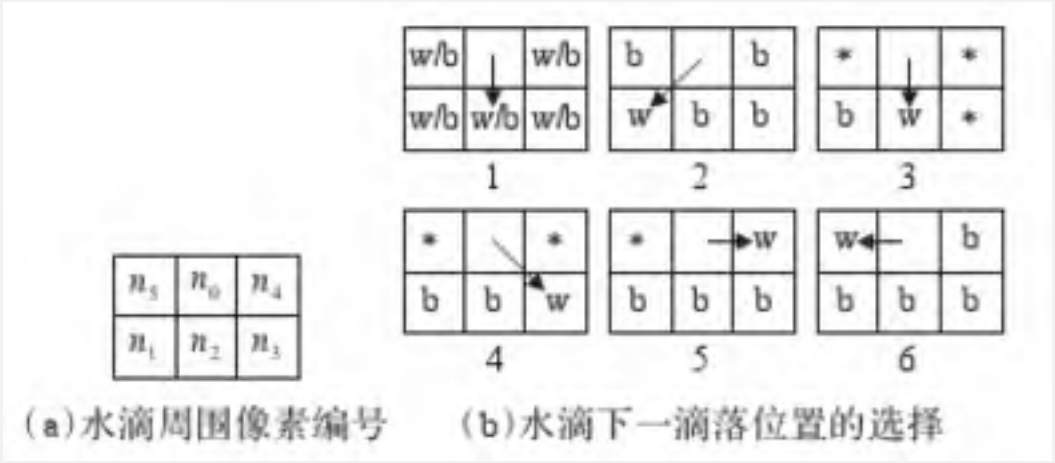


色彩第一多的是底图，第二多的是字母/数字

根据X轴Y轴投影切割

字符向X轴方向的投影不重叠

垂直像素立方图 与 滴水法



Disaster之二——防范(验证码)

APMCon

图片规范成32*32的像素，按2*2切分成16*16个子局域，统计局域内的黑色像素的个数，由此得到一个256维的特征矢量

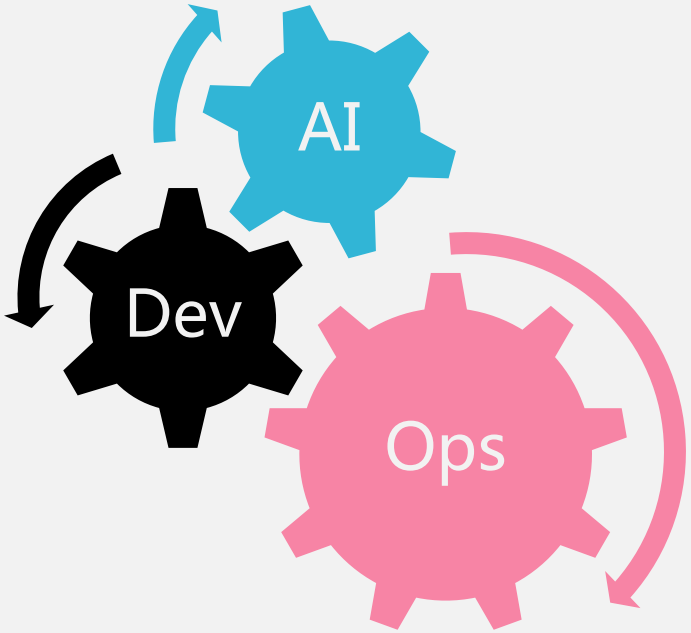
需要识别的字符集比如是0-9的数字，因此将目标输出值设置为一个10维的列向量，比如字母4所对应的列向量为[0,0,0,0,1,0,0,0,0,0]

设置隐含层为64，学习率为0.001，进行训练并保存训练结果

单个字符图片通过第一步转成256维的特征矢量并输入到神经网络中，最终会得到一个10维的输出，用这个输出同0-9各自所对应的特征矢量进行欧式距离计算，距离最近的那个字符就是识别的最终结果

Tips

BP人工神经网络pyneurgen



算法无处不在

垂直像素立方图

感知哈希算法

扭曲还原算法

滴水法

腐蚀算法

凸包算法

旋转卡壳算法

IA + Dev + Ops

人工/Selenium

- 响应时间
- 坐标间距
- 重试次数
- 点击位置
- 加速度
- 点击后等待时间

三方合作—听云


100(安全)
70(良好)
0(危险)
3
06/25
06/27
06/29
07/01
07/03
07/05
07/07
07/09
07/11
07/13
07/15
07/17
07/19
07/21
07/23
我的
行业
所在行业：金融
修改


攻击防护
Web攻击
100k
50k
06-25
07-02
07-09
07-16
07-23
昨日: 10 万
今日: 1034
30天: 19 万
CC攻击
500k
06-25
07-02
07-09
07-16
07-23
昨日: 47 万
今日: 31 万
30天: 1188 万
访问控制事件
400k
06-25
07-02
07-09
07-16
07-23


风险预警
黑客攻击
您的网站www.itouzi.com...遭到真人黑客 1 人高危攻击 1 次，
2017-03-29
防护建议
短信监刷
您的网站www.itouzi.com...遭到大量涉及短信业务请求 391072 次，拦截0次，
2017-07-23
防护建议
robots脚本
您的网站bbs.itouzi.com...遭到大量Robot机器人脚本访问 190298 次，拦截 142162 次，请确认是否为合法Robot，
2017-07-24
防护建议
爬虫访问
您的网站*.itzcdn.com...遭到大量业务爬虫访问 67359 次，拦截 12 次，请确认是否为合法爬虫，
2017-07-24
防护建议
行业预警
您所在行业1周内流行本地文件包含、CRLF、CSRF，请关注并及时配置相关防护
2017-07-24
防护建议
消息
规则更新
更新Nginx敏感信息泄漏防护规则(CVE-2017-7529)
2017-07-13
规则更新
更新XSS 0day防护规则
2017-07-10
规则更新
更新Struts2 0day防护规则(S2-048)
2017-07-07
查看
规则更新
更新Drupal远程命令执行漏洞防护规则
2017-06-27
查看

You built it, you own it

THANK YOU