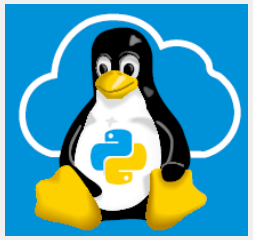
Technology Tarena 达内科技

全国1806班Security课题疑难解答



讲师：丁明一

达内 云计算学院

1806班全国系列班提交问题数

中心	项目经理	人数	提交问题数
广州云 中心	张威、姚尧	64	19
北京天坛中心	严文井	49	9
成都金融街中心	汪涛	43	4
深圳龙岗中心	张婉如	29	1
杭州西溪中心	郭玉璞	27	4
郑州科技园中心	程广文	22	0
上海云中心	姜晓宇	20	2
呼和浩特中心	张婷	19	9
石家庄中山路中心	李众生	17	4
长沙东塘中心	何求兵	14	2
西安省体中心	吴柯	14	5
洛阳王城中心	彭随光	8	2

广州云中心

1.VM1用test1用户登陆系统，使用su命令切换为test2账户，在tmp下创建一个文件（非交互式）,为什么提示需要密码

[test1@vm1 ~]$ su - test2 -c "touch /tmp/test2.txt"
密码：

su切换用户本来就是需要输入密码的啊，只有root切换账户才不需要密码

2.修改txt的文件内容，文件属性没改(权限)，ctime也会变，为什么?

因为时间变了！！时间也是属性

广州云中心

3.http_ssi_module有什么作用

SSI：服务器端嵌入或者叫服务器端包含，是Server Side Include的简写。SSI技术通过在文档中加入SSI指令，让服务器端在输出文档之前解析SSI指令，并把解析完的结果和文档一同输出给客户端。

SSI的指令如下：

<!-- #directive parameter="value" -->

其中，directive是指令名，parameter指令参数，value指令参数值

可以看到，就是html注释，事实上，Web服务器开启了SSI，并且页面包含可以解析的指令，那么Web服务器就解析这个指令。没开启器SSI或者开启了SSI，但是不是可以解析的指令，那么都当做注释。

广州云中心

4.以下命令结果的"@@ -1,2 +1,3 @@"，有什么含义?

```
[root@web1 ~]# diff -u test1.sh  test2.sh
--- test1.sh          2018-09-01 17:36:00.237559570 +0800
+++ test2.sh          2018-09-01 17:36:29.135559570 +0800
```

连个文件名，和两个文件的时间，两个文件的行号1,3是1、2、3行标记哪些行有修改

广州云中心（续一）

5.Nginx优化并发量时，要改内核参数；Zabbix服务器的搭建也需要优化Nginx的fastcgi缓存参数，等等例子；每次听到缓存，内核，CPU，内存等硬件相关内容时，都觉得比较抽象。希望听到丁大神讲讲计算机工作的原理，过程，举些例子
这个需要一天或者一周时间

6.配置了主动监控的主机web2，自动地就不能监控了，为什么?
什么是不会监控了，主动监控也是监控的一种方式，可以监控而且效率更高
主动监控和被动监控是互斥的，开了主动监控就不能被动监控!

7.在安装zabbix的时候，最开始设置网页连接数据库的时候，最后创建不成功，但是只要把提示的网页文件下载下来，然后放到对应的路径下依然可以成功的访问到zabbix的web页面，这是什么原因造成的？？
因为权限不对，她自己没有权限写入那个文件到特定的目录（前面做错了）

广州云中心（续一）

8.上一个问题的另外一种情况就是在打开的第一个页面就没办法进行下一步，不能到后面的页面中去设置数据库参数，但是，如果直接写一个最终的页面文件放到对应目录下，也是可以直接访问zabbix的web页面，这又是什么原因？

做错了

可能：没有安装php，仅安装了php-fpm，部分代码就无法执行

9.在降级启动Tomcat的时候，用ss查看端口的时候8005端口并没有启动，启动的8080端口和8009端口在开启了几秒钟以后再次查询的时候也被关闭了。删除Tomcat以后，照着历史命令再做一遍又没有问题，不知道是什么原因产生的？（随机数已经修改为了urandom）

隔几秒自动关闭，说明配置文件出错了

.

广州云中心 （续二）

10.在iptables中有办法一次删几条规则吗？（不要清空）

所有规则都保存在文件，可以修改文件删除多个规则

11.简述实现SSH密钥对验证的基本过程?

跟网站加密的流程一样

12.如何通过key搜索审计日志?

ausearch -k key的名称

13.简述ngx_http_limit_req_module模块的用法?

正课的内容(有图有真相），语法和中文解释。

```
[root@proxy ~]# vim /usr/local/nginx/conf/nginx.conf
… …
http{
… …
limit_req_zone $binary_remote_addr zone=one:10m rate=1r/s;
 server {
      listen 80;
      server_name localhost;
      limit_req zone=one burst=5;
         }
}
```

```
//limit_req_zone 语法格式如下:
//limit_req_zone key zone=name:size rate=rate;
//上面案例中是将客户端 IP 信息存储名称为 one 的共享内存，内存空间为 10M
//1M 可以存储 8 千个 IP 信息，10M 可以存储 8 万个主机连接的状态，容量可以根据需要任意调整
//每秒中仅接受 1 个请求，多余的放入漏斗
//漏斗超过 5 个则报错
[root@proxy ~]# /usr/local/nginx/sbin/nginx -s reload
```

广州云中心 （续二）

14.创建一条iptables防火墙规则，实现虚拟机用NAT模式上网的命令?

Iptables -t nat -s 192.168.4.0/24 -j SNAT --to-source 真机IP

15.简单描述Zabbix具有哪些监控功能?

可以监控端所有服务，所有系统，几乎所有硬件设备

16.使用Template OS Linux模板可以监控哪些项目?

CPU、内存、磁盘、passwd文件是否被修改，等30多项，具体参考模块后面的监控项，点击打开可见

广州云中心 （续二）

17.简单描述Zabbix自动发现的功能?

正课的实验内容：

自动发现主机并加入主机并绑定监控模板，省了人工手动添加主机

18.创建主动监控模板，完成操作图形界面不显示?

不显示啥，监控模板不显示，还是数据不显示，数据不显示，是做错了

被监控端配置，监控服务器的Web配置，是否重启服务?

都有可能

北京天坛中心

2.fastcgi_read_timeout 300与max_input_time=300 是不是指的同一个时间?
nginx让cgi读的时间就是php接收数据的时间吗?
不是，各自的独立配置，可以不同，可以相同

4.zabbix 的配置文件中的允许谁监控本机Server=127.0.0.1,192.168.2.5这里的本机为什么是127.0.0.1？ 可以写成localhost吗？或者是Server=192.168.2.100,192.168.2.5
都可以，方便自己使用zabbix_get测试

5.设置buffer的值，追寻什么规律吗？还是随便给吗?
buffer的值，需要看里面存的内容，不同的内容，大小不同
文件的buffer就看文件的大小，head的buffer可以看f12的信息，看有多大

北京天坛中心

6.nginx模块的功能，能不能扩展的讲解一下

nginx核心模块84项目，每个模块的选项5-10个，上百个选项，上课已经挑选了至少3个核心模块分别讲解，其他的可以参考下面的连接：

http://nginx.org/en/docs/

7.自动识别主机的时候，客户端zabbix_agentd都已经查到端口，但是无法识别到，只能开httpd。

无法识别说明软件他自己没找到，解决：可以附加使用ping检测，不需要启动任何服务，只要开机就能添加主机，识别率更高

8. /etc/php-fpm.d/.d/www.conf这个文件这个文件里面，关于控制进程数量，最大进程和最小进程，最小空闲进程，和最大空闲进程，是怎么算的?

一个进程25M左右，计算自己有多数内存就可以

9.企业中常用的加密算法有哪些！用在什么应用上?

md5,rsa,dsa,AES,DES都是企业常用算法，md5做数据校验，对称加密做数据加密

非对称加密应用在网络加密

成都金融街中心

1.iptables案例中写到"可以不指定链，默认为对应表的所有链"，但是在实际设置时不指定链就会报错，能再说明下吗
iptables -nL　　#不会报错，没有指定链，默认是所有链
你不可能写规则也说，不指定链啊

2.能否再说一下iptables nat表应用
只有2种SNAT，DNAT

3.老师，通过无线网怎样黑入连接的所有设备，可否演示一下。如果我们设备在之前已经被黑了，又需要采取何种措施解救?
不能，不会，自己的设备可以随时还原设置，重置密码

4.zabbix 邮件，动作这块创建，成功了，也没有发邮件。还有创建的图形。也没不能成功。没法远程，看不出错误，需要找项目经理排错（或者重置一次）

深圳龙岗中心

.

zabbix 怎么实现微信报警

需要添加插件，而且需要微信开发接口，微信对这个管理的非常严格，很麻烦，要实名认证，一般需要公众号

可以使用阿里的钉钉，第5个阶段张老师的课程内容有这个。

杭州西溪中心

1.案例上说使用私钥签名的文件是可以使用对应的公钥验证签名的，只要验证成功，则说明这个文件一定是出自对应的私钥签名。但最后的验证却使用签名文件对软件包进行签名认证:

gpg --verify log.tar.sig log.tar

而实际上也可以用公钥对数字签名进行签名认证:

gpg -d -r usera.key log.tar.sig

那么生产环境中的话是不是应该是建立信任的公钥库，拿公钥进行验证比较好

签名的意义是需要确保数据的安全，是验证签名和数据的

仅验证签名也不能保证数据的安全

杭州西溪中心

.
2.自定义监控中,想要将脚本和自定义监控配套给别人,能不能自定义变量代表目录?
如果能,
该怎么做?
场景模拟:
同时在/usr/local/etc/zabbix_agentd.conf.d/ 中创建目录shells(放nginx.status.sh执行脚本),
同时创建nginx.status自定义监控,此时,我需要将这两个文件用tar -czPf打包传给其他人,而
他将使用tar -xPf傻瓜式解包即用
那么此时在nginx.status文件中该如何定位到shells目录调用脚本?
写据对路径!!
/usr/local/etc/zabbix_agentd.conf.conf/shell/nginx.status.sh

上海云中心

1.iptables中什么情况下用drop拒绝，什么情况下用reject拒绝，各有什么优缺点?

drop不回应数据包省流量，reject给拒绝的回应包

2.grep和awk过滤后 有什么方法拍序，比如按照a到z首字排序或者数字？

sort命令可以排序（这个问题要在shell阶段的总结中就解决）

awk最后一天有这个命令sort

呼和浩特中心

1.shill脚本中，虚拟机有IP地址，可以用ecpect实现ssh远程登录的自动交互。
如果虚拟机没有IP，可不可以用virsh远程实现自动交互，如果可以，请指点一下。
以下是编写的脚本：

```
#!/bin/bash
#创建虚拟机
read -p “要创建几台虚拟机：” a
echo $a | clone-auto7 > /dev/null
echo “创建成功”          #开启虚拟机
read -p “输入虚拟机后的数字(空格隔开,如:1 2)，启动：” b
for i in $b
do
virsh start rh7_node$i &> /dev/null
done     #远程
for i in $b
do
virsh console rh7_node$i
done
```

之后我想用virsh远程自动交互。
没写过，可以自己测试下

呼和浩特中心(续1)

2.安装--with-http_stub_status_module模块，安装完成后nginx -V 发现模块没安装上，
第二次安装结果一样没装上。然后，rm -rf /usr/local/nginx/ 后重新安装，nginx -V 还是没有该
模块。百度后，又rm -rf /etc/nginx /usr/local/nginx/ 后重新安装，模块安装成功。 问题出在哪?
想从系统中完全卸载nginx怎么作?
应该是做了链接了，链接删了，或使用绝对路径看就对了

3.iptables中的转发规则具体在什么条件下应用。举个栗子。
这个是正课的练习内容，如果linux是网关，保护网关后面的服务器时，就用转发规则
4.我想请教以下丁老师，在运维的工作当中哪些是日常必做的事情，我们学习的高级运维知识
的先后性，哪些特别的重要哪些了解就好。
运维最终要的是排错，其他东西都可以在网上获取资料

5.工作中用到shell脚本比较多的地方有哪些?
只要能写出来，用在运维的哪里都可以（仅运维）

6.防火墙企业中都会常用到哪些策略?
过滤策略和地址转换

呼和浩特中心(续1)

7.通过网络传输的信息貌似可以被人轻易的抓包分析，如何让自己的通讯更安全并且简便？（GPG加密有点费事）

加密，没有好的方法，安全与便利性是互斥的

8.如何抓别人的包还不会被人发现？

可以百度

杭州西溪中心（续1）

.

3. 自定义监控要如何应用在主动监控中?
与被动监控一样

4./etc/sudoers里给一个普通用户加可以执行别名SERVICES的命令时，su到普通用户，用sudo+命令，执行的时候就不成功（比如systemctl提示命令在/bin/下），但配置文件里不用别名直接打命令路径的时候就成功了。
把start、stop去掉，仅保留systemctl就可以了

石家庄中山路中心

1.zabbix自动发现，不太明白

可以不用，可以手动添加500台主机，链接监控模板

手动发现和自动发现做的事一样，明白自动发现，先要明白手动添加主机

2.聚合图形只显示第一行内容，第二行有设内容，但是不显示

另，设置完后如何退出编辑模式，直接点聚合图形么

找项目经理给点击、演示一遍

3.zabbix仪表盘删除后，如何恢复

编辑仪表盘

4.今日的脚本变量调用不太明白过程.

再看看视频吧

长沙东塘中心

1.丁老师，我昨天在做zabbix的过程中，因为之前创建过用户，我在输入mysql的时候显示“Access denied for user 'root'@'localhost' (using password: NO)” 我用之前建立过的用户操作，没用。同桌跟我讲我没弄明白，卡了好久。最后我是在没办法重新做了一遍。您能不能帮我理清一下思路。

之前配置mysql密码了，没有密码就不能操作mysql

普通用户能进入mysql，也没权限操作数据库

2.用patch打补丁，p0，p1的运用还不是很清楚，丁老师能不能再讲一遍。

看视频吧（正课的内容不适合答疑）

西安省体中心

1.防火墙(firewalld)与iptables区别有哪些？以后在公司中用哪个？

正课里面说了区别的，可以看看视频，公司暂时用的iptables

2.SNAT通过真机实现虚拟机上网，这块还是有问题。

做错了，没有其他可能，正常一定是没问题的

3.装完zabbix后，在server上的agent不能被发现，没有绿怎么办？

没有就是没启动

4.有没有一键安装Zabbix的办法?

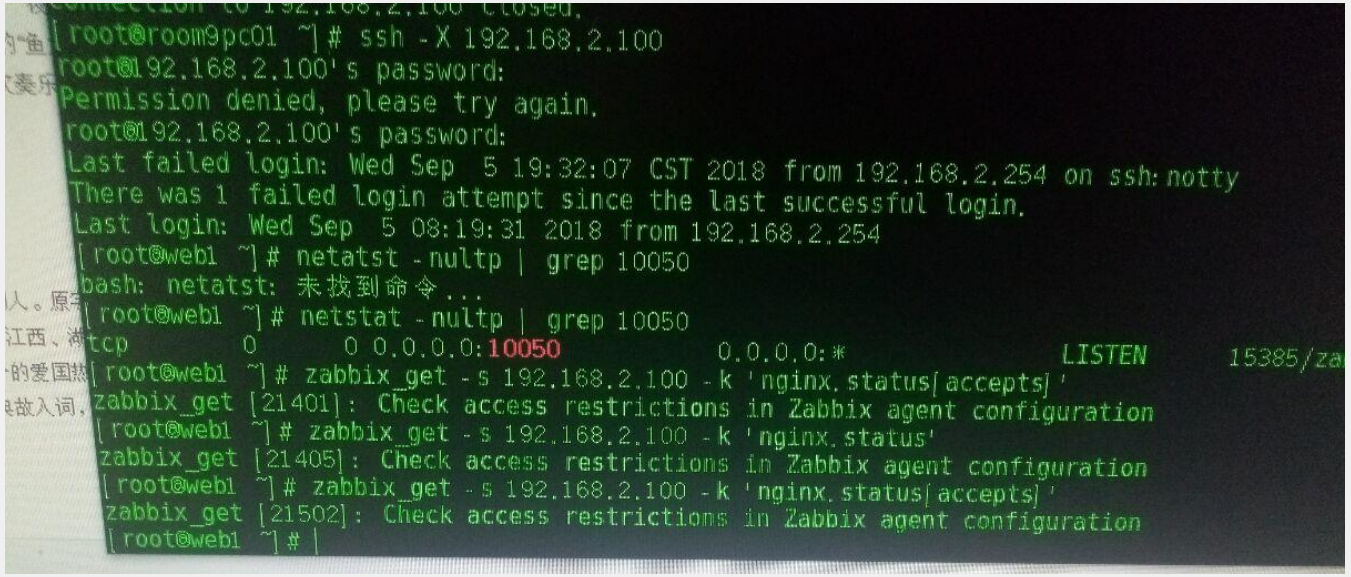
网上有别人写的脚本

5.zabbix配置报警邮件和触发器了，我停掉了nginx，但是没有给我发邮件，这是怎么肥四?

邮件配置错误

洛阳王城中心

1.zabbix在监控网页创建图形时，严格按照步骤操作，其它情况也检查过，但是图形却不显示，可能的原因有哪些，怎么解决
做错了，没有给足够的错误提示信息，无法排错，可以重新做
2.用192.168.2.100检测是报错，用127.0.0.1检测输出是空，是什么原因？（如下图）
配置文件控制这个有没有权限，看配置文件



谢谢各位！！