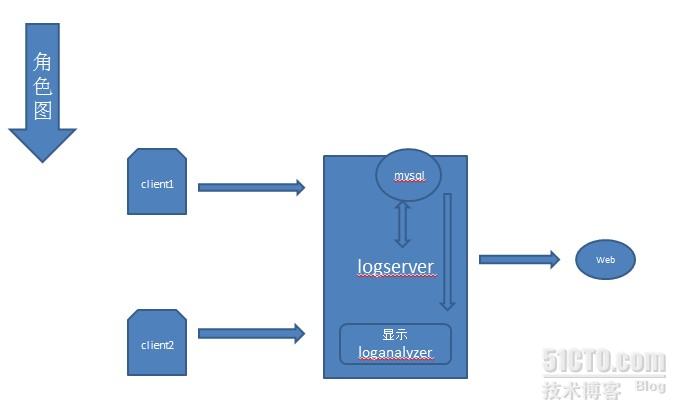
**Centos6.0之rsyslog部署日志服务器**

日志服务器，可以方便统一查看服务器上的日志，并且写入数据库，进行web显示,方便查看；也起到了一定的安全的作用，当黑客离开clear history的时候，我们这边也是可以看到的；废话少说了，直接正题

[](http://img1.51cto.com/attachment/201306/180509311.jpg)

Client1: 192.168.244.154

Client2: 略；一样的配置

logserver:192.168.244.132

LogAnalyzer是一个syslog和其他网络事件数据的Web前端工具，提供简单易用的日志浏览、搜索和基本分析以及图表显示。采用php开发的，因此需要php的运行环境，本文lamp

下面开始操作：

logserver:

|  |  |
| --- | --- |
| 1 | yum install httpd mysql\* php\* mod\_ssl rsyslog-mysql -y |

配置rsyslog;  vim /etc/sysconfig/rsyslog

|  |  |
| --- | --- |
| 1  2 | SYSLOGD\_OPTIONS="-c 2 -r -x -m 180"  KLOGD\_OPTIONS="-x" |

[](http://img1.51cto.com/attachment/201306/184043688.jpg)

各参数作用：

-c 指定运行兼容模式。

-r 指定监听端口。 默认514

-x 在接收客户端消息时，禁用DNS查找。需和-r参数配合使用。

-m 标记时间戳。单位是分钟，为0时，表示禁用该功能。

编辑rsyslog.conf 开启相关属性

|  |  |
| --- | --- |
| 1  2  3 | $ModLoad immark.so  $ModLoad imudp.so  $UDPServerRun 514 |

[](http://img1.51cto.com/attachment/201306/110135445.jpg)

Client1:

编辑rsyslog.conf  新增以下：

|  |  |
| --- | --- |
| 1 | \*.\*                 @192.168.244.132 |

/etc/init.d/rsyslog restart

编辑/etc/bashrc

|  |  |
| --- | --- |
| 1 | export PROMPT\_COMMAND='{ msg=$(history 1 | { read x y; echo $y; });logger "[euid=$(whoami)]":$(who am i):[`pwd`]"$msg"; }' |

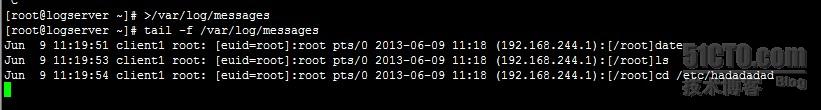
source/etc/bashrcce

测试Client执行命令，logserver是否可以正常接收

client1:

[](http://img1.51cto.com/attachment/201306/112011107.jpg)

logserver:tail -f /var/log/messages

[](http://img1.51cto.com/attachment/201306/112029989.jpg)

说明接收正常，包括你重启机器的一些Log都可以查看的。

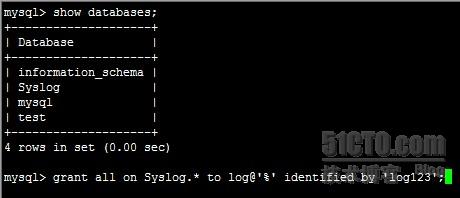
下面是导入数据库，借助loganalyzer进行web展示

logserver:

|  |  |
| --- | --- |
| 1 | [root@logserver ~]# mysql -u root -p < /usr/share/doc/rsyslog-mysql-5.8.10/createDB.sql |

mysql 授权；

|  |  |
| --- | --- |
| 1 | mysql> grant all on Syslog.\* to log@'%' identified by 'log123'; |

[](http://img1.51cto.com/attachment/201306/113746644.jpg)

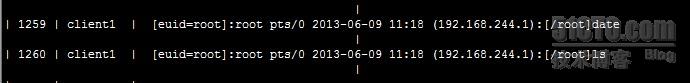
编辑rsyslog.conf  新增以下：

vim /etc/rsyslog.conf

|  |  |
| --- | --- |
| 1  2 | $ModLoad ommysql  \*.\* :ommysql:192.168.244.132,Syslog,log,log123 |

service rsyslog restart

|  |  |
| --- | --- |
| 1 | mysql> select ID,FromHost,Message from SystemEvents where FromHost like '%client1%'; |

[](http://img1.51cto.com/attachment/201306/114719197.jpg)

安装loganalyzer

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8 | wget http://download.adiscon.com/loganalyzer/loganalyzer-3.6.3.tar.gz  tar zxvf loganalyzer-3.6.3.tar.gz  mkdir -p /var/www/html/syslog  rsync -a loganalyzer-3.6.3/src/\* /var/www/html/syslog  # vi /etc/httpd/conf.d/ssl.conf  修改下面两行  DocumentRoot "/var/www/html/syslog/"  ServerName  www.lansgg.com:443  #/etc/init.d/httpd restart |

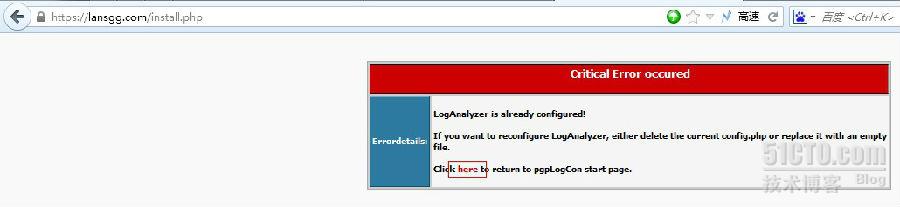
编辑Host

|  |  |
| --- | --- |
| 1 | 192.168.244.132 lansgg.com |

打开浏览器https://lansgg.com开始安装

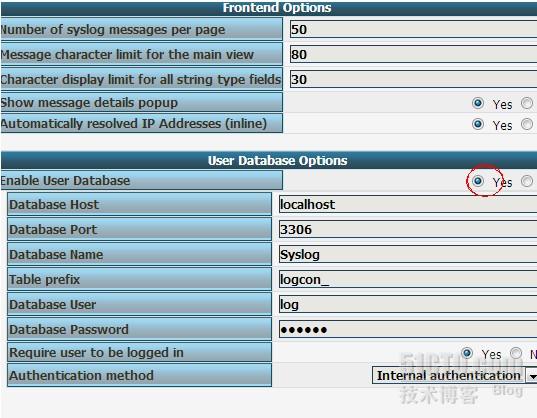
# touch /var/www/html/syslog/config.php  
# chmod 666 /var/www/html/syslog/config.php

# chmod a+r /var/log/messages

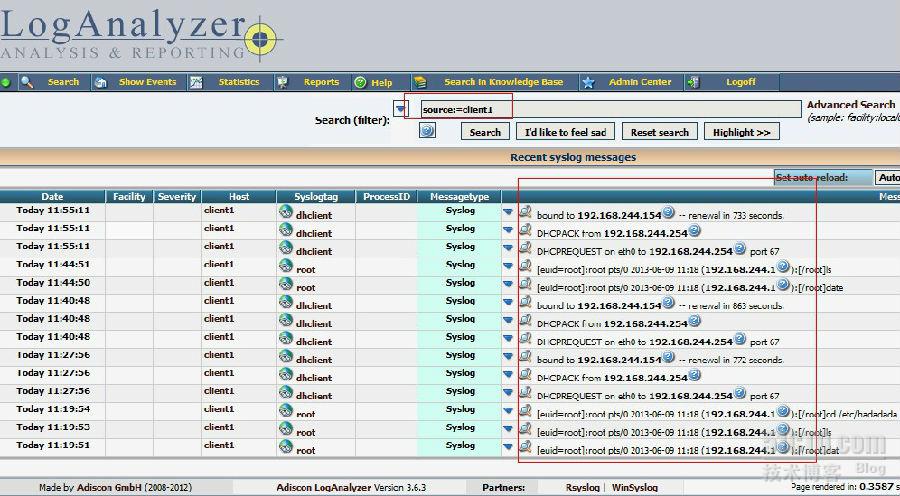
[](http://img1.51cto.com/attachment/201306/115523964.jpg)

下一步，下一步即可

到此步注意即可，其他的都easy

[](http://img1.51cto.com/attachment/201306/115932858.jpg)

安装完成，登录进入

[](http://img1.51cto.com/attachment/201306/123631540.jpg)

结束。