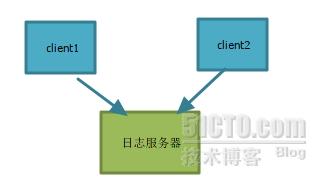
**rsyslog+mysql+loganalyzer构建日志服务器**

**一，背景**

服务器数量增量的情况下，需要建立一台日志服务器来查看每台服务器的异常情况。

[](http://img1.51cto.com/attachment/201303/180000287.jpg)

Server :centos 6.3 64bit,Server version: 5.1.67,Apache/2.2.15,PHP 5.3.3,rsyslogd 5.8.10

在centos6.0系列的系统已经是rsyslog记录日志。

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，可以是lamp,也可以是lnmp。根据自己的喜好来搭建。  
**二，安装好环境**

yum install rsyslog rsyslog-mysql mysql-server httpd mod\_ssl php php-gd php-mysql

如果有兴趣可以采用源码编译安装。

三，导入Syslog的数据库,并设置权限

[root@test1 ~]# mysql < /usr/share/doc/rsyslog-mysql-5.8.10/createDB.sql

Mysql> grant all privileges on Syslog.\* to log@localhost identified by ‘123456’;

Mysql>flush privileges;

Mysql>exit

四，编辑rsyslog.conf

#vim /etc/rsyslog.conf

#### MODULES ####

$ModLoad ommysql.so #这两行添加

\*.\* :ommysql:localhost,Syslog,log,123456 #localhost表示主机，Syslog数据库名，log管理这个数据库的用户，123456密码。

$ModLoad immark #下面三行取消注释

$ModLoad imudp

$UDPServerRun 514 #利用upd 514传递

#/etc/init.d/rsyslog restart

五，安装loganalyzer

目前最新版3.6.3

#wget <http://download.adiscon.com/loganalyzer/loganalyzer-3.6.3.tar.gz>

#tar xf 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/"

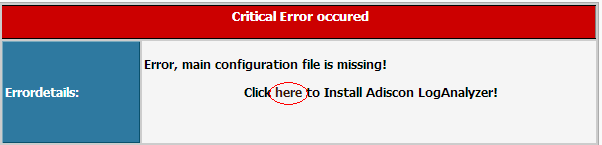
ServerName my.log.com:443

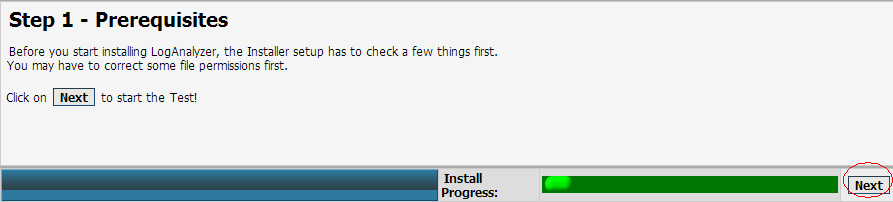
#/etc/init.d/httpd start

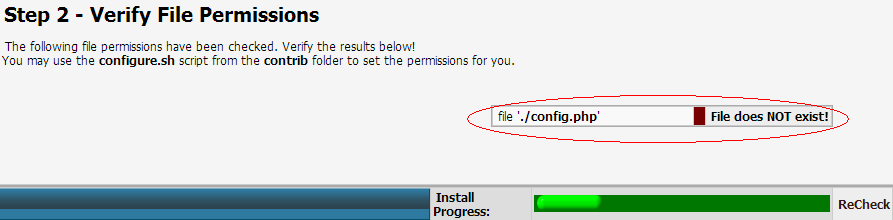
编辑windows上hosts文件，添加

192.168.1.26 my.log.server

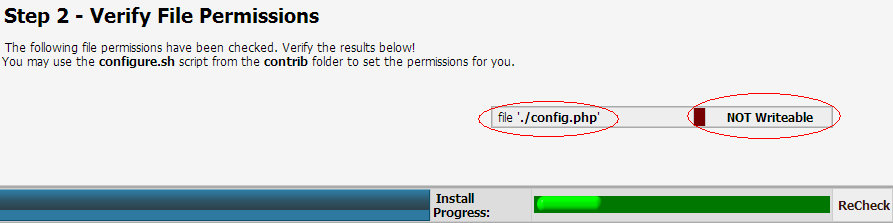
打开浏览器https://my.log.com,开始安装

[](http://img1.51cto.com/attachment/201303/180216801.png)

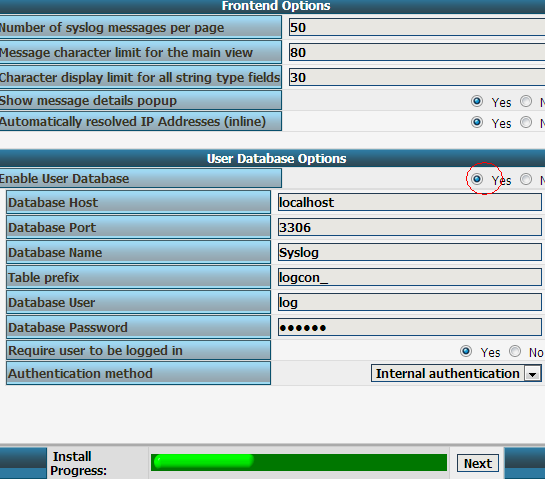
[](http://img1.51cto.com/attachment/201303/180235172.png)

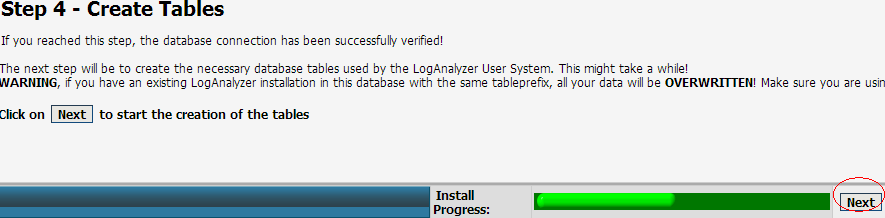
[](http://img1.51cto.com/attachment/201303/180252914.png)

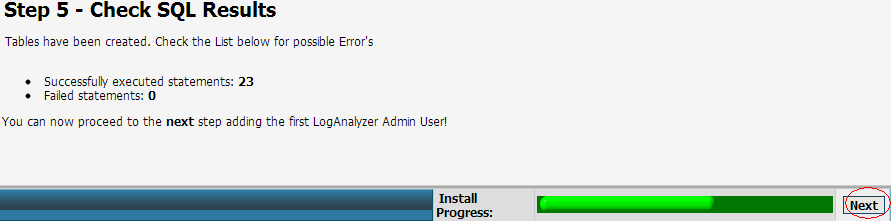
# touch /var/www/html/syslog/config.php 建立完后再点recheck

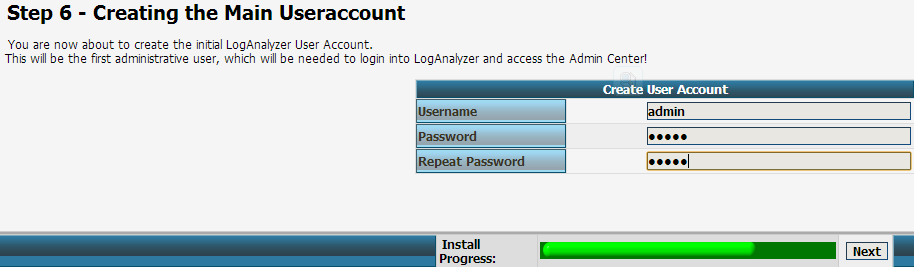
[](http://img1.51cto.com/attachment/201303/180432280.png)

[root@test1 ~]# chmod 666 /var/www/html/syslog/config.php

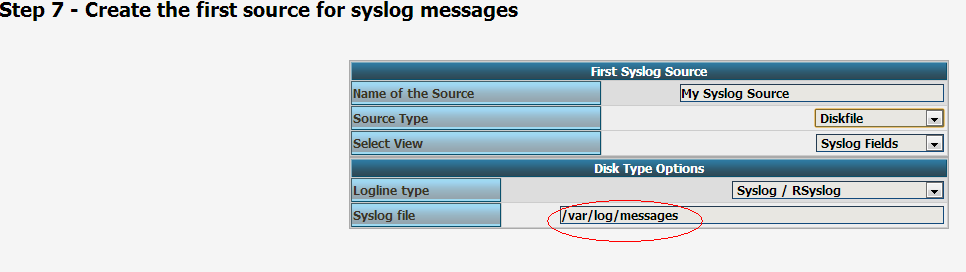
[](http://img1.51cto.com/attachment/201303/181057948.png)

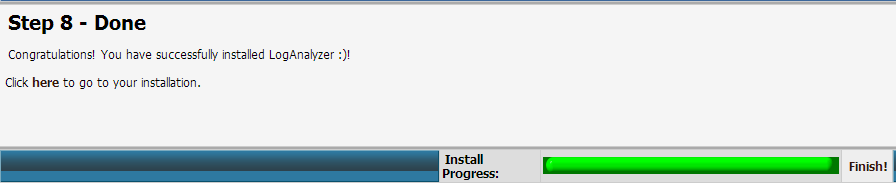
[](http://img1.51cto.com/attachment/201303/180500909.png)

[](http://img1.51cto.com/attachment/201303/181655383.png)

[](http://img1.51cto.com/attachment/201303/181612749.png)

 创建登录管理页面的用户

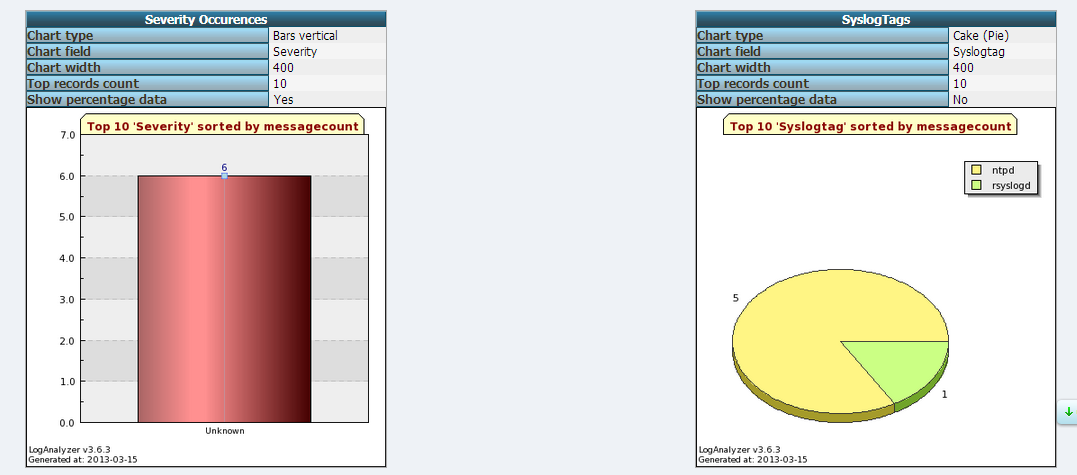
[](http://img1.51cto.com/attachment/201303/181715285.png)

[](http://img1.51cto.com/attachment/201303/181808952.png)

[](http://img1.51cto.com/attachment/201303/181737495.png)

[root@test1 ~]# chmod a+r /var/log/messages

成功后的图

[](http://img1.51cto.com/attachment/201303/181959546.png)

六，添加客户端

# yum install rsyslog  
# vi /etc/rsyslog.conf  
添加如下内容  
\*.\* @192.168.1.26:514  
注:192.168.1.26为日志服务器端IP地址,@表示用udp传输，514表示514端口，@@表示tcp。514可以省略，因为默认是514端口。

[](http://img1.51cto.com/attachment/201303/182123565.png)