**CentOS 6.3下利用Rsyslog+LogAnalyzer+MySQL部署日志服务器**

平时查看分析LINUX系统日志我觉得是我们每天必做的功课，但时间长了会发现每次查看站点日志都得挨个进后台，几台服务器还可以这么对付，但如果管理成百上千台线上服务器，这种方法就捉襟见肘了。

后来想了想能不能有一台日志服务器集中管理日志，并以WEB形式将日志显示到前台方便查看，顿时码字的想法油然而生，呵呵。

本文档是利用rsyslog+loganalyzer+mysql将网内所有LINUX服务器的系统日志集中到日志服务器进行管理，所有日志会保存在mysql数据库表中

注：loganalyzer在获取客户端日志会有两种保存模式，一种是直接读取客户端/var/log/目录下的日志并保存到服务端该目录下，一种是读取后保存到日志服务器数据库中，本文档推荐后者

一.环境部署

操作系统： centos6.3 x64

1、安装LAMP环境: httpd-2.4.4，mysql-5.6.10，php-5.4.13

需要的软件包：

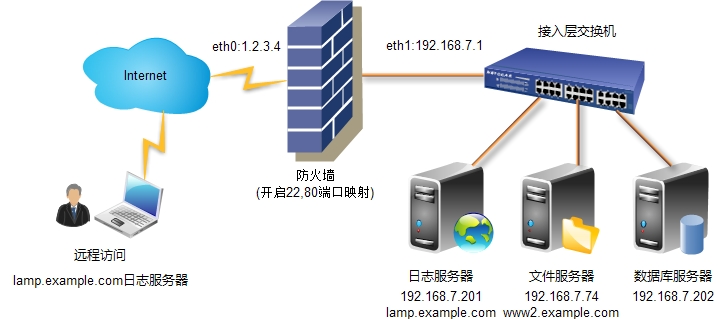
rsyslog: 系统默认yum源

loganalyzer: loganalyzer-3.6.3

rsyslog server: 192.168.7.201 lamp.example.com

rsyslog client: 192.168.7.74 www2.example.com

网络拓扑图：



2.关闭iptables和SELINUX

# service iptables stop

注：这里若要开启iptables服务增加系统安全性

服务端需添加rsyslog UDP 514端口以及loganalyzer TCP 80端口通过规则

# iptables -A INPUT -p udp --dport 514 -j ACCEPT

# iptables -P OUTPUT ACCEPT

# iptables -A INPUT -p TCP --dport 80 -j ACCEPT

客户端只需添加OUTPUT通过规则

# iptables -P OUTPUT ACCEPT

从规则可见，rsyslog server端为被动获取数据，client端为主动发送数据

关闭iptables的朋友可以无视。。

# setenforce 0

# vi /etc/sysconfig/selinux

---------------

SELINUX=disabled

---------------

3.同步时间

# ntpdate asia.pool.ntp.org

二.安装配置rsyslog

(rsyslog server)

# yum install rsyslog rsyslog-mysql -y

注：rsyslog-mysql为rsyslog将日志传送到mysql数据库的一个模块，这里必须安装

# cd /usr/share/doc/rsyslog-mysql-5.8.10/

# mysql -uroot -p123456 < createDB.sql

注：这里导入数据库操作其实博主最后研究了下，就是创建了Syslog库并在该库中创建了两张空表

创建rsyslog用户在mysql下的相关权限

# mysql -uroot -p123456

> grant all privileges on Syslog.\* to rsyslog@localhost identified by "123456";

> flush privileges;

> exit

配置服务端支持rsyslog-mysql模块，并开启UDP服务端口获取网内其他LINUX系统日志

# vi /etc/rsyslog.conf

在#### MODULES ####下添加这两行

------------------

$ModLoad ommysql.so

\*.\* :ommysql:localhost,Syslog,rsyslog,123456

------------------

注:localhost表示本地主机，Syslog为数据库名，rsyslog为数据库的用户，123456为该用户密码

取消下面三行注释

-----------------

$ModLoad immark

$ModLoad imudp

$UDPServerRun 514

-----------------

重启服务：

# service rsyslog restart

(rsyslog client)

# yum install rsyslog -y

配置rsyslog客户端发送本地日志到服务端

# vi /etc/rsyslog.conf

末行添加如下内容

-------------------

\*.\* @192.168.7.201

-------------------

注:192.168.7.201 为日志服务器端IP地址

重启服务：

# service rsyslog restart

三.安装loganalyzer

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

# tar zxvf loganalyzer-3.6.3.tar.gz

# cd loganalyzer-3.6.3

# mkdir -p /usr/local/apache2/htdocs/loganalyzer

复制loganalyzer源代码到apache的DocumentRoot下loganalyzer目录

# cp -r src/\* /usr/local/apache2/htdocs/loganalyzer

# cp -r contrib/\* /usr/local/apache2/htdocs/loganalyzer

# chown -R daemon.daemon /usr/local/apache2/htdocs/loganalyzer

通过web向导安装loganalyzer前，必须先执行以下两个脚本

# cd /usr/local/apache2/htdocs/loganalyzer/

# sh configure.sh

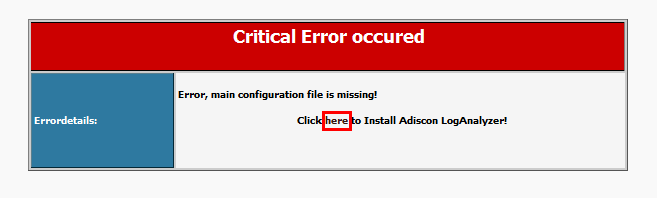
# sh secure.sh

注：该脚本实际上是创建该目录下的config.php，并配置该文件权限。

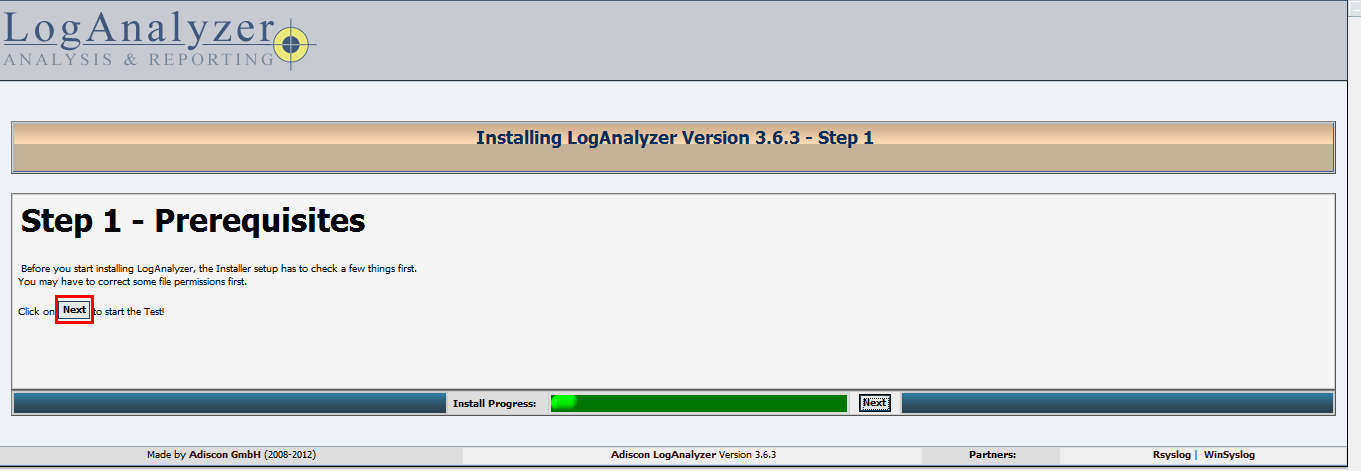
在浏览器输入网址，进入安装向导

http://192.168.7.201/loganalyzer

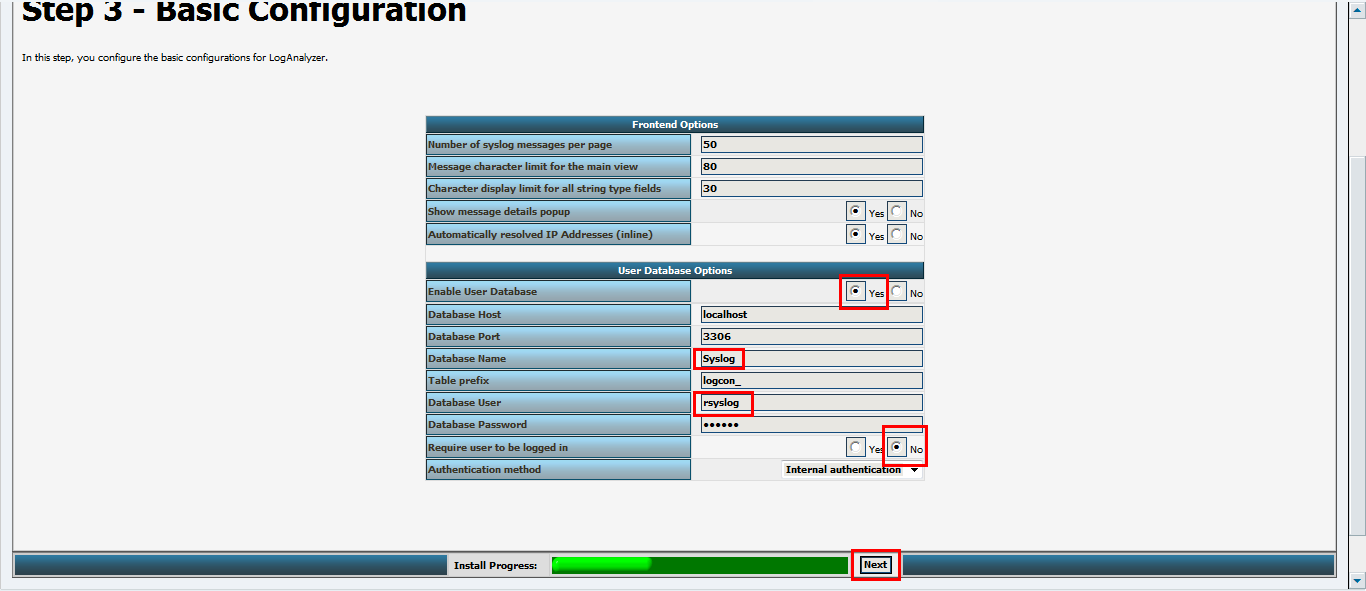
1. 提示没有配置文件，点击here利用向导生成



1. NEXT



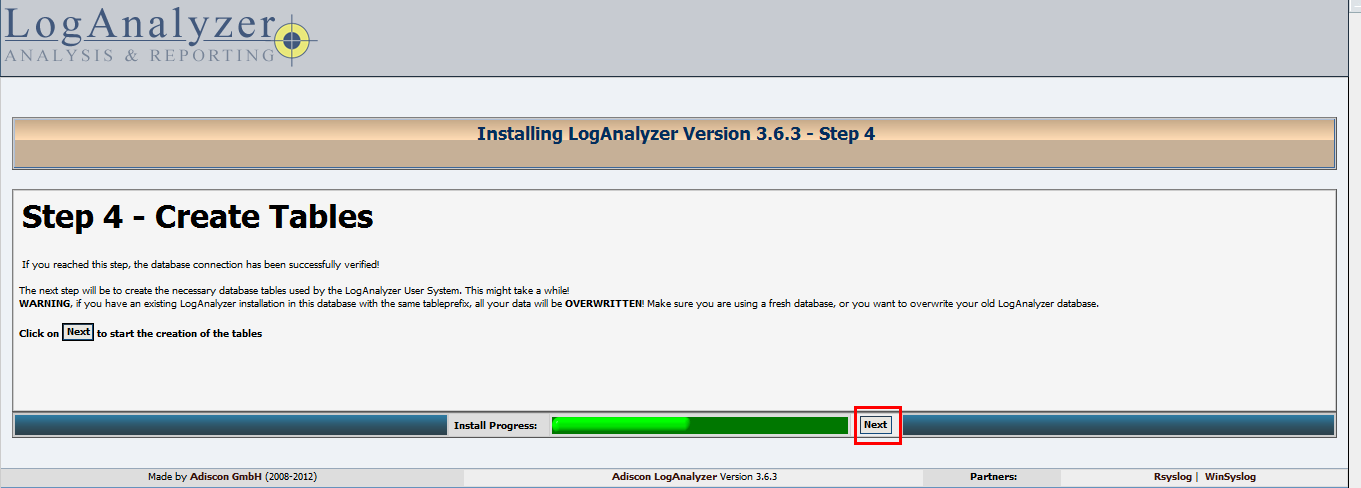
1. 按照如图输入配置，点击NEXT：



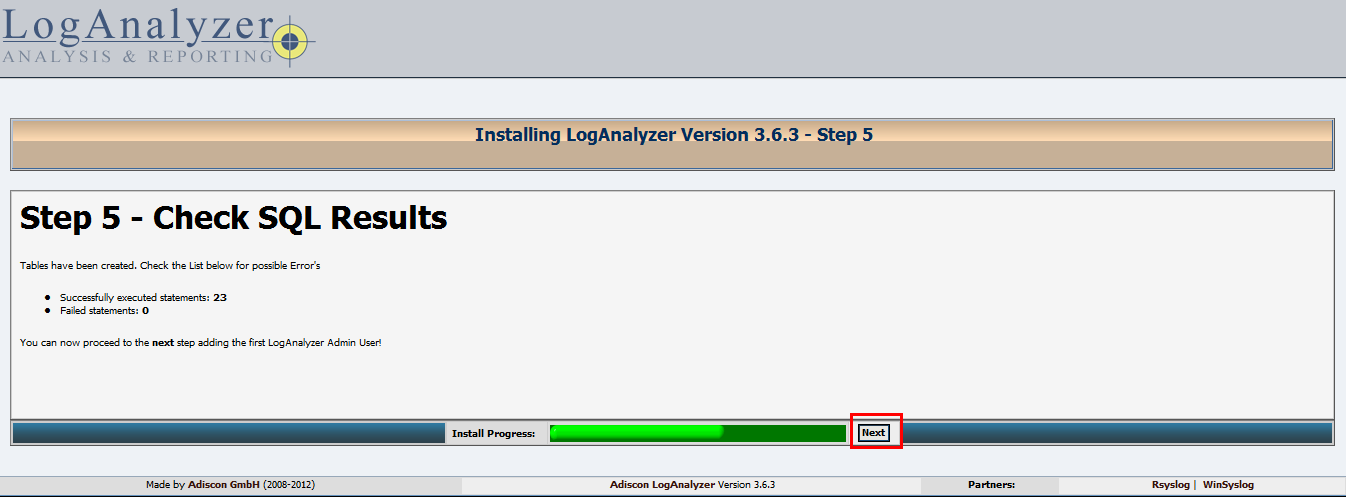
注：点击NEXT时若报错，后台执行如下命令后继续

# ln -s /var/lib/mysql/mysql.sock /tmp/mysql.sock

1. 开始写入数据库，NEXT



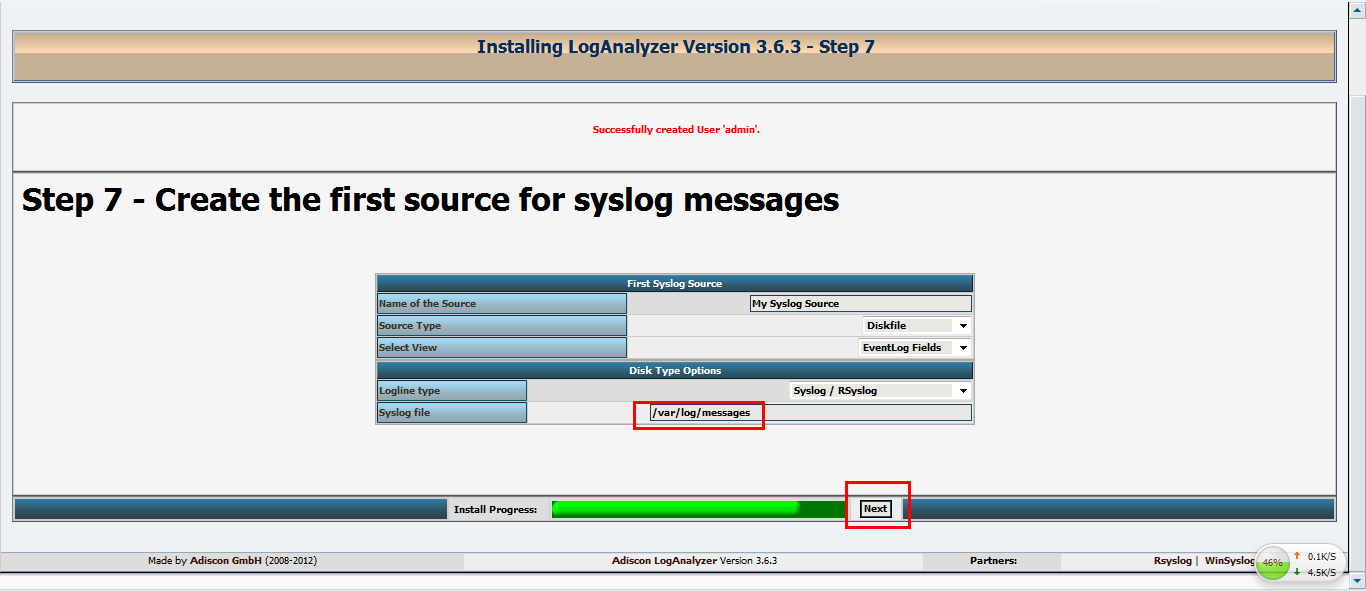
1. 提示写入成功，NEXT

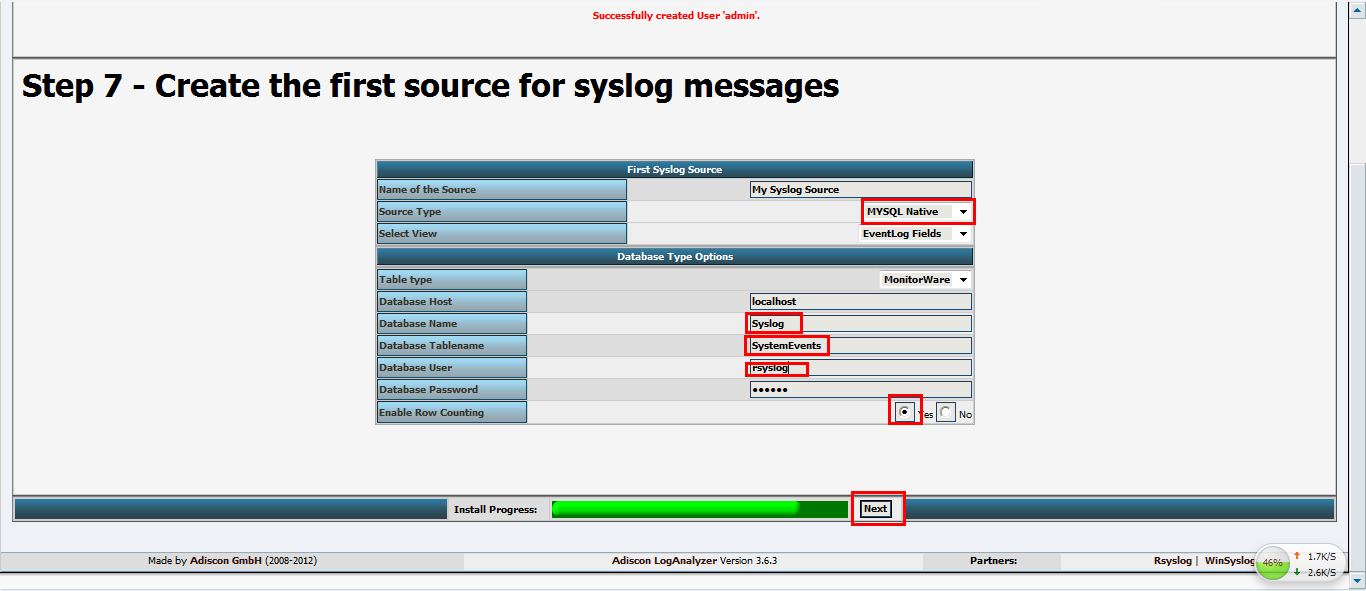


1. 设置管理员账户，配置完毕NEXT

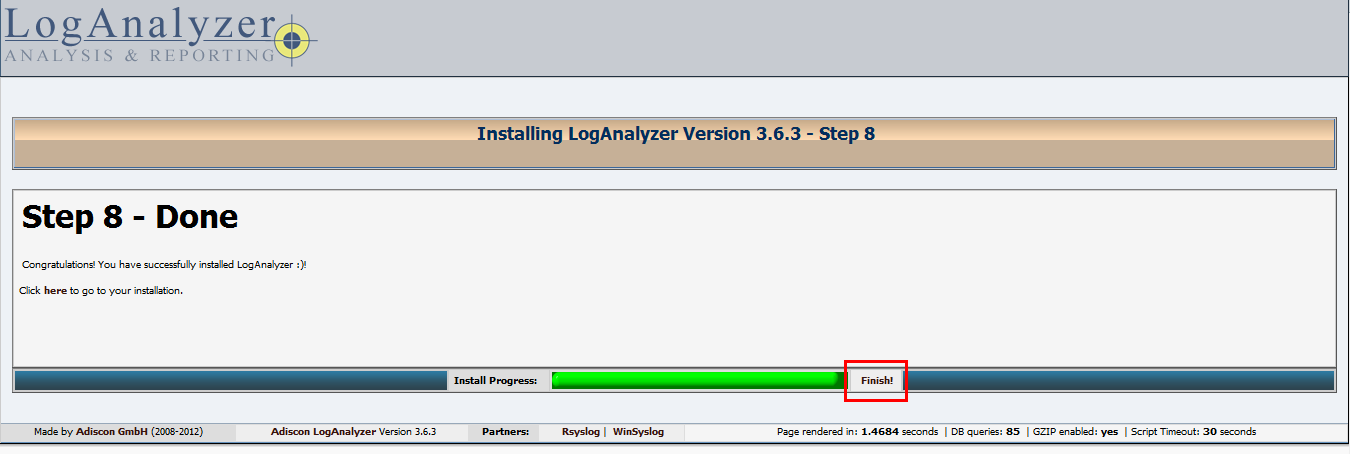


1. 设置监控日志保存到mysql数据库中，按照如图配置后NEXT





1. 完成配置,FINISH

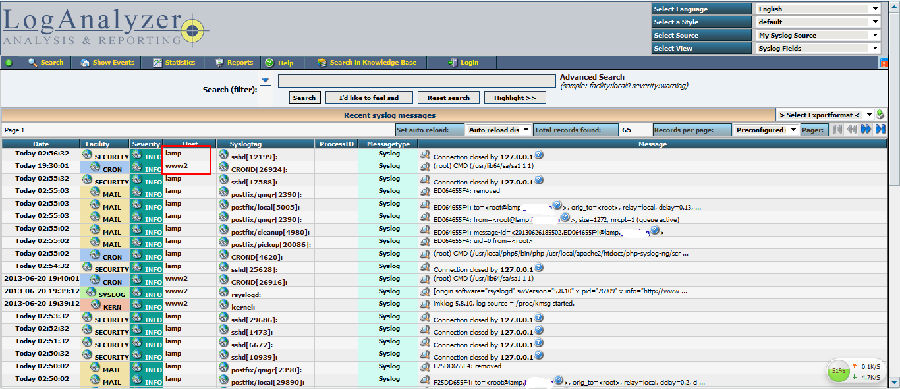


1. 进入登陆界面：

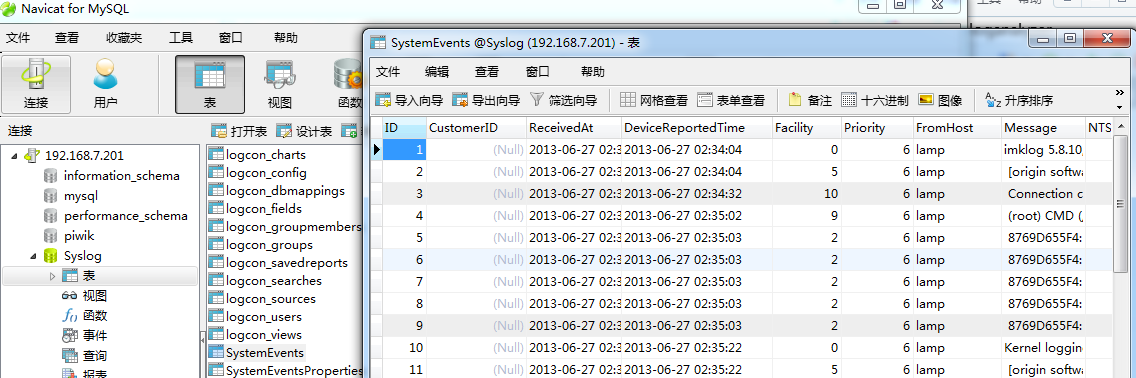


10.进入主界面：

查看loganalyzer是否获取192.168.7.201和192.168.7.74系统日志



利用navicat查看rsyslog服务端和客户端系统日志是否都写入数据库Syslog-SystemEvents表



**后记：**

1.本人在loganalyzer安装向导配置的web后台账户，在登陆界面无法登陆，提示账号或密码错误，不知道是什么原因？最后是在向导一处去掉登陆认证才勉强通过，有遇到相同问题的朋友望帮忙解答。经过一位朋友指点，终于找到了原因：

首先利用以下命令守株待兔

# tail -f /usr/local/mysql/log/mysql.log

然后在loganalyzer向导STEP6输入web后台账号密码后，点击NEXT

查看到mysql.log日志里出现了一条INSERT语句

130706112038551.png

然后将该语句复制到后台手动执行，看报什么错误

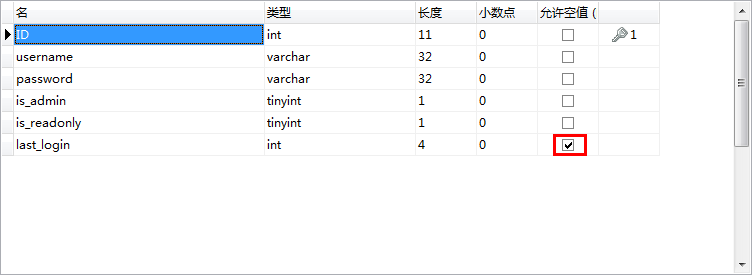
# mysql -uroot -p123456;

> INSERT INTO logcon\_users (username, password, is\_admin) VALUES ('admin', '00a1f187721cxxxxxxx6bf791e69382c', 1);

ERROR 1364 (HY000): Field 'last\_login' doesn't have a default value

提示'last\_login'栏不能为空值

OK，直接登录navicat,将这栏设置为允许空值保存即可。



从新执行这条语句

> INSERT INTO logcon\_users (username, password, is\_admin) VALUES ('admin', '00a1f187721cxxxxxxx6bf791e69382c', 1);

Query OK, 1 row affected (0.06 sec)

显示执行成功

利用navicat 查看后台该表，显示成功插入一条记录

130706112038553.png

重新利用该账号即可成功登录loganalyzer web后台

看来是mysql在执行该语句时，发现last\_login栏默认为非空，所以拒绝这条insert语句执行，解决办法就是将该栏设置为允许空值即可。

在线上老版本mysql-5.0.56无需进行上述手动操作，即可成功登录后台。但本篇出现的问题则是在mysql-5.6.10版本上。看来这应该不算是loganalyzer的BUG，应该是mysql在高版本执行insert语句提高了严谨性。这里给卡在这里的朋友点思路，仅供参考。

2.安装rsyslog可谓是过程曲折，之前本想全部编译安装，最后才发现网上的文档各种误导，编译rsyslog最后花了2个小时安装了其6个依赖包，全部找的老外的文档挨个测试，装完网上给出的文档又不能合理给出如何与系统自带的rsyslog共存保证不冲突，也就是编译的rsyslog的启动方法如何与系统自带的区别，索性就yum吧，实属无奈之举，还有吐槽下google各种间歇性抽风，至于原因，大家都懂的。。。

3.Windows客户端安装(win2008 server 64bit)

1.下载evtsys

http://eventlog-to-syslog.googlecode.com/files/Evtsys\_4.4.3\_64-Bit.zip

2.解压文件将包内64-Bit文件夹下的所有文件复制C:\Windows\System32下

3.开启evtsys服务

运行- cmd

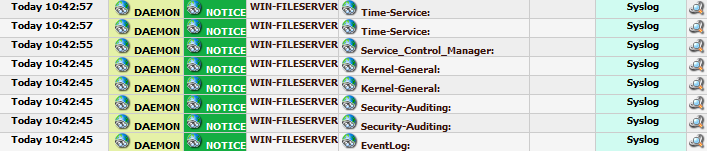
> cd c:\Windows\System32

> evtsys -i -s 10 -h 192.168.7.11 -p 514

> net start evtsys

4.验证效果

如图：



本文出自：<http://www.linuxidc.com/Linux/2013-07/86956.htm>

（完）