

S3500-EA系列交换机日志信息发送到Linux日志主机功能的配置

一、组网需求：

交换机的日志信息发送到Linux日志主机上，日志主机的IP地址为202.38.1.10，只允许严重性高于errors的日志信息发送到日志主机上，允许输出信息的模块为所有模块。

二、组网图：



三、配置步骤：

(1) 交换机上的配置

开启信息中心。

```
<Sysname> system-view
```

```
[Sysname] info-center enable
```

将IP地址为202.38.1.10的主机用作日志主机，只允许严重等级高于errors的日志信息输出至日志主机，允许输出信息的模块为所有模块。

```
[Sysname] info-center loghost 202.38.1.10 facility local7
```

```
[Sysname] info-center source default channel loghost log level errors debug state off trap state off
```

(2) 日志主机上的配置

以超级用户（root）的身份执行以下命令。

```
# mkdir /var/log/Sysname
```

```
# touch /var/log/Sysname/information
```

以超级用户（root）的身份编辑文件/etc/syslog.conf，加入以下选择/动作组合（selector/action pairs）。

```
# Sysname configuration messages
```

```
local7.info /var/log/Sysname/information
```

当日志文件information建立且/etc/syslog.conf文件被修改了之后，应通过执行以下命令查看系统守护进程syslogd的进程号，杀死syslogd进程，并重新用-r选项在后台启动syslogd。

```
# ps -ae | grep syslogd
```

```
147
```

```
# kill -9 147
```

```
# syslogd -r &
```

四、配置关键点：

对Linux日志主机，必须保证syslogd进程是以-r选项启动。在编辑/etc/syslog.conf时应注意以下问题：

(1) 注释只允许独立成行，并以字符# 开头。

(2) 选择/动作组合之间必须以一个制表符分隔，而不能输入空格。

(3) 在文件名之后不得有多余的空格。

(4) /etc/syslog.conf中指定的设备名及接受的日志信息级别与交换机上配置的info-center loghost和info-center source命令中的相应参数应保持一致，否则日志信息可能无法正确输出到日志主机上。