XLog网络流量分析系统配合AR46收集NetStream日志的配置

王涛1　2007-01-04 发表

XLog网络流量分析系统配合AR46收集NetStream日志的配置

一　组网需求：

XLog网络流量分析系统支持与交换机、路由器等设备联合组网，接收并记录网络日志信息，为用户提供直观、准确的网络流量统计结果，用户可以从其中了解到网络流量的分布情况、历史趋势、网络应用的流量分布以及网络流量的异常信息等。

二　组网图：

XLog服务器操作系统为Windows 2003 Server，XLog版本2.10-R0120

三　配置步骤：

1　登陆XLog配置管理台

打开IE浏览器，在地址栏中输入XLog NTAS登录的URL，如下图：

图1 XLog配置管理台访问URL

XLog配置管理台安装完成时，会提示用户登录XLog的方式，如果配置管理台安装用的HTTP端口是默认的80端口，那么登录的时候只需要输入IP地址即可，例如：http://192.168.4.30 。如果选择的端口不是80端口，而是用户自己指定的端口，比如：8080，那么登录的时候就需要输入IP地址＋冒号＋端口号的形式，例如：http://192.168.4.30:8080。打开登录页面，如下图所示：

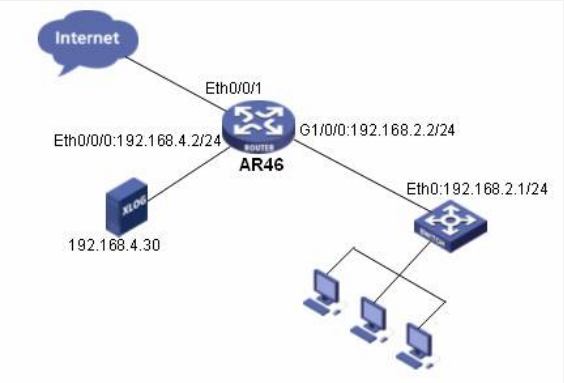

图2 XLog NTAS登录窗口

输入正确的用户名和密码，单击<登录>按钮进入XLog NTAS。（系统管理员admin的缺省密码为Admin）。

2　配置管理台窗口介绍

图3 配置管理台窗口介绍

为了便于后续的操作，需要说明配置台的窗口区域的划分。如上图所示左面的窗口区域为“导航菜单区”，右面的窗口区域为“主窗口”。在以下的配置过程中都按照这种术语来描述对应窗口区域。

3 配置设备信息

单击导航菜单区的[网络流量分析管理/设备信息管理]菜单项，进入设备信息管理主窗口，如下所示：

图4 设备信息管理主窗口

单击右上角的<增加>按钮，进入增加设备信息窗口，如下图：

图5 增加设备窗口

在增加设备窗口中，正确输入设备IP地址，设备描述（可选），SNMP团体字和SNMP端口。

设备IP地址就是所要监控的设备的地址；

设备描述可以不填，缺省会取设备的名称；

SNMP相关参数要和设备上的snmp的参数一致。

配置完设备参数后，单击<增加接口>按钮，进入设备接口选择的窗口，如下图：

图6 设备接口列表

选择要进行监控的设备接口，本文中监控和局域网连接的GigabitEthernet0/0/0 以及和Internet相连的Ethernet0/0/1。

选择接口后，点击<确定>，返回到增加设备窗口，再次单击<确定>按钮，完成增加设备操作，页面返回到设备信息管理页面，如下图：

图7 设备信息管理（增加设备后）

4 配置日志接收管理

点击导航菜单栏中[系统管理/日志接收管理]菜单项，进入日志接收管理页面。

图8 日志接收管理

单击右上角<配置>按钮（或点击“配置”链接），进行日志接收配置。如下图：

图9 日志接收配置

输入处理器IP（192.168.4.30），选择缺省的日志聚合策略。输入接收器IP，监听端口使用默认的9020,9021，单击<增加>，然后单击<确定>按钮，完成日志接收配置，页面返回到日志接收管理。然后单击右上角<下发>按钮，下发日志接收配置，显示如下信息时，表示下发配置成功，日志接收配置完成。

图10 日志接收配置下发成功

5 网络流量分析

设备信息和日志接收配置完成后，设备配置正确，大约10分钟就可以在网络流量分析查看报表，如下图所示，通过点击相应的接口链接，进入报表。

图11 网络流量分析

6 配置路由器AR46

6.1 根据2.1的组网需求，配置各接口IP地址和及路由

6.2 配置设备时间

clock datetime 08:00:00 2006/11/03

在用户视图下，配置正确的标准时间，不要配置时区。目前XLog和设备配套时存在时区问题，具体请参见2.3故障排除举例。

6.3 配置SNMP

```
#
 snmp-agent
 snmp-agent community read public
 snmp-agent sys-info version all
```

进入系统视图，配置SNMP相关命令。在设备信息管理，增加设备时，SNMP参数要和设备上配置的一致，否则无法获取到设备的接口列表。

6.4 配置NetStream日志导出

```
#
 ip netstream export source interface Ethernet0/0/0  //设备IP
 ip netstream export host 192.168.4.30 9020   //接收器IP 端口
```

进入系统视图，配置上述NetStream日志导出命令。其中source interface的IP地址要和XLog中设备IP一致，日志导出host 和监听端口要和XLog的接收器IP和监听端口一致。

6.5 使能NetStream统计

```
#
interface GigabitEthernet1/0/0
 ip address 192.168.2.2 255.255.255.0
 ip netstream inbound
 ip netstream outbound
```

进入接口视图，在该接口下使能NetStream日志统计功能。

6.6 查看NetStream日志导出信息

```
display ip netstream export
Version 5 export information
  Stream destination IP(UDP)              : 192.168.4.30(9020)
  Stream source interface                 : Ethernet0/0/0
  Exported stream number                  : 83577
  Exported UDP datagram number(failed number): 71281(0)
```

在用户视图或系统视图都可以使用该命令查看NetStream日志导出的情况。

四　　配置关键点：

4.1 接收器和处理器在同一台服务器上时，不需要配置FTP相关参数。XLog支持接收器和处理器的分布式安装，如果二者不再同一台服务器上时，需要在处理器所在的服务器上开启FTP服务，同时在日志接收管理配置相应的FTP配置信息。

接收器的监听端口，缺省为9020和9021，用户可以进行修改，但是要保证和设备上配置的日志导出端口一致。

4.2 设备IP地址就是所要监控的设备的地址，对于路由器（如AR46）可能存在多个IP，XLog中配置的设备IP要和设备上 配置的NetStream 日志导出的Source 接口IP相同，即和设备上配置的下面命令中的接口IP相同，本文中使用以太网接口Ethernet 0/0/0，IP为192.168.4.2。

[AR46]ip netstream export source interface Ethernet 0/0/0

XLog中的设备IP要和Eth0/0/0的IP一致。