

XLog UBAS系统与交换机配合采集DIG日志的典型配置

一 组网需求:

XLog服务器的操作系统为Windows Server 2003 + SP1 或 Windows 2000 Server + SP4), 数据库为SQL Server2000+SP3(或SP4), 客户端IE的版本应在5.5版本以上, XLog UBAS使用版本为XLog2.10-R0120。XLog采集器安装在FreeBSD系统上。交换机用S3952P-EI, 版本信息是VRP software, Version 3.10, ESS 1510ver。

二 组网图:

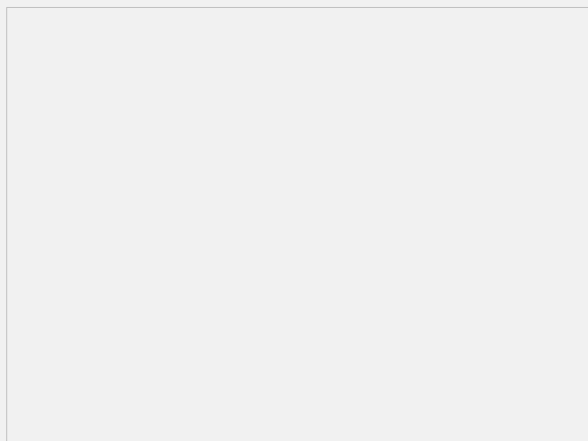


图1 组网图

采集器将生成的日志文件传给处理器, 是通过FTP方式实现的, 因此需要在处理器所在的计算机上搭建一个FTP服务器端。图 1为XLog UBAS系统配合采集器采集网络中的流量及摘要信息的组网图。其中采集器的网卡Inc1的IP地址不需要和局域网路由可达; 其他所有网卡的地址都需要和网络路由可达。局域网用户通过交换机上网, 产生的流量都镜像到一个以太网口上, 采集器的网卡Inc1就连接在这个以太网口上, 从而可以采集到本局域网所有用户的流量信息和部分应用的摘要信息; 采集器再利用另一块网卡Inc0将生成的日志文件通过交换机传给XLog服务器192.168.4.50供XLog管理员进行日志审计。

三 配置步骤:

1 S3952P-EI上的配置

首先, 根据图1的组网需求, 配置各个接口的IP信息, 接口IP配置和路由配置本文不再描述。确定了交换机的镜像端口和监听端口之后, 其他配置如下:

1) 创建镜像组:

```
#  
mirroring-group 1 local
```

在用户视图下, 配置正确的标准时间, 不要配置时区。

2) 将镜像端口加入镜像组

```
#  
//使用下面的命令, 可以将离散的端口加入到镜像组中, 其中'both'为同时镜像入方向和出方向的数据  
mirroring-group 1 mirroring-port Ethernet 1/0/1 Ethernet 1/0/3 both  
//下面的命令, 可以将连续的端口加入到镜像组中, 其中'both'为同时镜像入方向和出方向的数据  
mirroring-group 1 mirroring-port Ethernet 1/0/5 to Ethernet 1/0/10 both
```

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。

3) 指定监听端口

```
#  
mirroring-group 1 monitor-port Ethernet 1/0/48
```

配置的最终结果为: 所有经过Ethernet1/0/1、Ethernet1/0/3、Ethernet1/0/5到Ethernet1/0/10端口的入方向和出方向的数据都被镜像到Ethernet1/0/48。

2 配置FTP服务器

采集器将生成的日志文件传给处理器, 是通过FTP方式实现的, 因此需要在处理器所在的计算机上搭建一个FTP服务器端。FTP服务器端软件使用通用的FTP软件, 安装和

配置过程请参照FTP软件的安装配置指导说明书。注意，配置的FTP用户必须拥有写权限。配置完FTP Server后，请记住FTP用户名和密码，以及FTP的主目录路径，后面配置台下发配置将会用到。

3 配置XLog UBAS系统

1) 登陆XLog UBAS配置台

采集器将生成的日志文件传给处理器，是通过FTP方式实现的，因此需要在处理器所在的打开IE，在地址栏中输入XLog配置台的URL。在XLog安装配置台的最后界面窗口中的提示信息中有登录配置台的方式，如果配置管理台安装用的HTTP端口是默认的80端口，那么登录时只需输入IP地址即可，例如：<http://192.168.4.50>。如果HTTP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://192.168.4.50:8080/>。打开登录页面，如图2所示：



图2 设备信息管理主窗口

打开登录页面后，输入正确的用户名和密码后，点击<登录>按钮。安装后默认的登录用户名为“admin”，登录密码为“Admin”。

2) 增加被管理设备

在导航菜单区选择[系统管理->设备信息管理]，打开设备信息管理主窗口。点击设备信息管理窗口左上方的<增加>按钮，打开增加设备的窗口（图 3所示）。在“设备名称”输入框中输入设备名称，如“DIG_65”；在“设备支持的日志类型”选择框中选择“DIG日志”日志类型选项；在“设备IP地址”输入框中输入设备的IP地址，如“192.168.4.65”，本设备IP地址就是采集器的IP地址；在“设备描述”中，输入描述信息，设备描述一般用于描述该设备的用途和位置信息，以方便用户更好的区分设备。



图3 增加设备窗口

确认信息输入正确后点击<确定>按钮即可完成设备增加配置，增加设备主窗口将被自动导航到设备信息管理主窗口，并显示新增加的和已有的设备信息。如图4所示：



图4 增加设备成功

3) 服务配置

在导航菜单区选择[日志服务管理->服务配置]，打开服务配置主窗口。在初次登录时，服务配置中没有任何数据，并且服务配置页面是只读的，需要点击<修改>按钮来激活页面。点击<修改>按钮后，显示的服务配置的主窗口如图5所示：



图5服务配置主窗口

在处理器IP地址输入框中输入处理器所在的主机的IP地址（不要输入127.0.0.1）；根据上面配置的FTP Server的用户名、密码和主目录路径，依次输入到“FTP用户”、“FTP密码”和“FTP主目录”中；输入内网信息“IP地址”和“网络掩码”，然后点击<增加>按钮，IP地址和网络掩码可以计算出一个IP地址段。如图6所示：

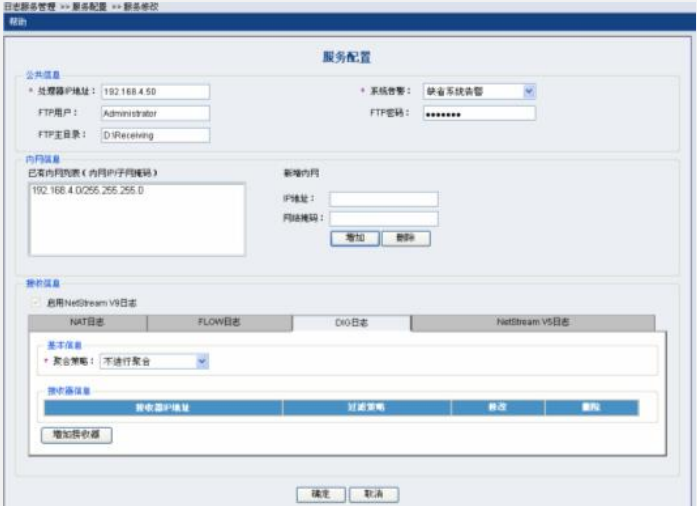


图6填写公共信息和内网信息

然后选中接收信息中的“DIO日志”，并点击<增加接收器>按钮，进入增加接收器页面。如图7所示：



图7增加接收器

选中‘接入设备’中的DIO设备，然后点击<确定>按钮即可保存接收器的配置信息，并返回到服务配置的主窗口中。确认配置的信息正确后，点击<确定>按钮，进入如图8所示的页面中：

日志服务管理 >> 服务配置

帮助

服务配置

公共信息

* 处理器IP地址: 192.168.4.50

FTP用户: Administrator

FTP主目录: D:\Recalving

* 系统告警: 设备系统告警

FTP密码: *****

内网信息

已启用内网连接《内网IP地址》

192.168.4.0/255.255.0

操作信息

启用NetStream V5日志

NAT日志 FLOW日志 DIO日志 NetStream V5日志

基本设置

* 聚合策略: 不进行聚合

接收器信息

服务器IP地址	发送行或流	发送策略
192.168.4.65		

修改 下发 删除

图8服务配置完毕

点击<下发>按钮，向采集器和处理器下发服务配置，进入如图9所示页面：

日志服务管理 >> 服务配置 >> 服务下发

处理器配置下发情况		
服务器IP地址	下发成功	下发结果
192.168.4.50		

接收器配置下发情况		
服务器IP地址	下发成功	下发结果
192.168.4.65		

告警配置下发情况		
服务器IP地址	下发成功	下发结果
192.168.4.65		
192.168.4.50		

确定

图9服务下发完成

这个页面中显示的是下发后的信息，通过这些信息可以得知下发给采集器、处理器的业务配置以及告警配置的成功与否，如果下发全部都是成功的，则点击确定按钮即可完成配置。如果下发有异常或者错误的提示信息，则需要对各个组件以及网络环境做检查。

四 配置关键点：

- 1) 必须查看监听网卡是否都配置了IP地址。采集器启动时会根据网卡名去获得网卡的IP地址，如果网卡没有配置IP地址，将会导致采集器获得不到IP地址，从而启动失败。
- 2) 查看XLog服务配置中的FTP的用户名、密码以及主目录配置和FTP Server中的这些配置是否一致；同时要确保这个FTP用户要有写权限。
- 3) 确保FreeBSD系统的时区和时间和XLog配置台的时区和时间一致。