



Product Mode: DRS-100 Series

日志管理系统操作手册

Release V3.1.5

Table of Contents

1. 系统安装.....	3
1.1. 操作系统及硬件平台.....	3
1.2. 系统软件安装.....	3
2. 日志系统简介.....	4
3. 日志系统管理.....	5
3.1. 访问管理界面.....	5
3.2. log 进程管理.....	6
3.3. log 日志管理.....	7
3.4. 分析结果导出.....	7

1. 系统安装

1.1. 操作系统及硬件平台

系统安装在Linux操作系统上，推荐使用RedHat AS4.2版本。如果没有该版本的系统，至少需要使用内核版本号在2.6.9-22之上的Linux系统。

系统硬件配置建议：

尽量使用两块硬盘，一块系统盘(大于10G)，一块数据盘（大于100G）；

CPU PIII500以上，内存512M以上，100/1000网卡

本文使用以下硬盘分区方案（文件系统均为 ext3）：

/	大于512M
/var	大于1G
/usr	大于4G
/home	大于4G
交换区 (SWAP)	大于256M（最好是内存的两倍）
/logserver	如果是一块硬盘则大于10G，否则分配剩余的所有空间
/a01	如果是一块硬盘则大于10G，否则分配第二块硬盘所有空间

1.2. 系统软件安装

在安装前确认系统没有这个用户帐号和用户组存在，如果有，则删除。

命令：

```
grep dlink /etc/passwd
```

如果存在dlink用户，则用下面命令删除：

```
/usr/sbin/userdel dlink
```

系统是一个rpm安装包，安装命令如下（**请向技术人员获得最新版本**）：

```
rpm -ivh DRS100-LOG-3.1.5-2007.04.25.i386.rpm
```

安装完之后会生成dlink用户，密码为空，需要管理员修改密码：

```
passwd dlink
```

重新启动机器，tomcat、logserver将会在系统启动的时候自动运行。

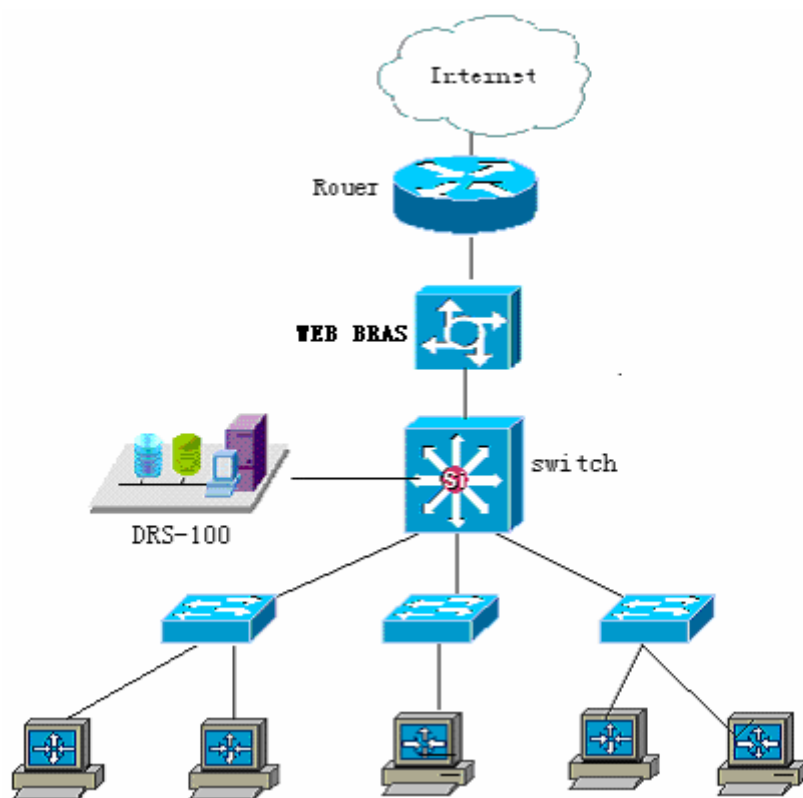
卸载命令如下（请注意卸载包的名字需与安装包相同，不包括“.i386.rpm”部分）

```
rpm -e DRS100-LOG
```

注：卸载会删除本软件的全部内容，请小心操作。

2. 日志系统简介

日志系统体系结构涉及到三方：用户计算机，WEB BRAS，Log_Receive Server。其中WEB BRAS与Log_Server之间采用友讯公司特有的通讯机制已保证能够采集到用户的实时上网信息，日志系统体系结构如下图所示：



WEB BRAS作为PSTN和Internet之间的网关设备，负责用户的接入和数据转发。用户接入的时候一般都需要一个帐号和密码，当帐号密码认证通过的时候用户才能够完成接入，之后WEB BRAS使得用户接入到Internet；用户从接入到Internet开始一直到离线，用户访问internet发生的所有数据流都流经WEB BRAS，因此用户在使用的时候WEB BRAS可以将用户的详细上网行为记录下来。同时，由于WEB BRAS上面没有大容量的存储设备，所以WEB BRAS要将用户的上网日志记录发向一个专门用于接收WEB BRAS发送用户上网日志的接收服务器。

该服务器没十分钟生成一个数据文件用来存放WEB BRAS送来得数据。同时，在接收服务器上，还可以对接收到的数据进行查询和分析。

3. 日志系统管理

3.1. 访问管理界面

Log Server的查询管理平台采用B/S管理结构，管理员只需打开浏览器，输入如下形式的URL：

<http://ip:8080>

系统默认的端口是8080, 如要修改，可以编辑：

```
[root@drs bin]# vi /logserver/tomcat/conf/server.xml
```

修改如下行的8080为目标端口，如为80即不需要在IE中输入端口。

```
<!-- Define a non-SSL HTTP/1.1 Connector on port 8080 -->
<Connector port="8080" maxHttpHeaderSize="8192"
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
    enableLookups="false" redirectPort="8443" acceptCount="100"
    connectionTimeout="20000" disableUploadTimeout="true" />
```

其中ip是系统安装所在机器的IP地址，即出现管理员的登录界面，如下图所示：

系统默认的用户名为：admin ，密码为：logadmin

如果想修改此用户名密码，请在服务器上修改

```
[root@dlink bin]# vi /logserver/tomcat/conf/tomcat-users.xml
```

修改下行中的logadmin保存即可修改登录密码。

```
Last login: Tue Apr 10 11:57:48 2007 from 192.168.1.236
[root@oracle ~]# vi /logserver/tomcat/conf/tomcat-users.xml
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <role rolename="manager"/>
  <user username="admin" password="logadmin" roles="manager"/>
</tomcat-users>
```

将看到如下的管理登录页面：



登录进去的页面如下：



3.2. log 进程管理

系统启动后，log进程自动启动。在这里可以查看接收程序的运行情况，可以在这里停止和重新启动接收程序。



3.3. log 日志管理

填写查询数据文件所要求的条件：用户ID、使用协议（tcp/udp/all）、源IP（用户IP）、目的IP、源端口、目的端口、开始时间、结束时间。**注：文件每10分钟生成一个**

The screenshot shows the 'Log Server' interface with a sidebar on the left containing 'Log Server', 'log进程管理', and 'log日志管理'. The main area is titled 'log日志管理' and includes a '查询' (Query) button and a '导出' (Export) button. Below these are input fields for various search criteria: '文件开始时间' (File Start Time), '文件结束时间' (File End Time), '用户姓名' (User Name), 'URL地址' (URL Address), '目标IP' (Target IP), '源IP' (Source IP), '协议' (Protocol), '目标端口' (Target Port), '源端口' (Source Port), '上网开始时段' (Online Start Time), and '上网结束时段' (Online End Time). Each time field has a format dropdown set to '2006-05-12' and a time dropdown set to '16:53:10'. A '说明' (Note) states: '可以导出所有查询记录，查询最多只能显示10000条记录' (All query records can be exported, but only 10,000 records can be displayed at a time). A '查询' (Query) button is at the bottom of the form. Below the form is a table header with columns: '用户姓名', '协议', '目标IP', '源IP', '目标端口', '源端口', '上网开始时间', '上网结束时间', and 'URL地址'.

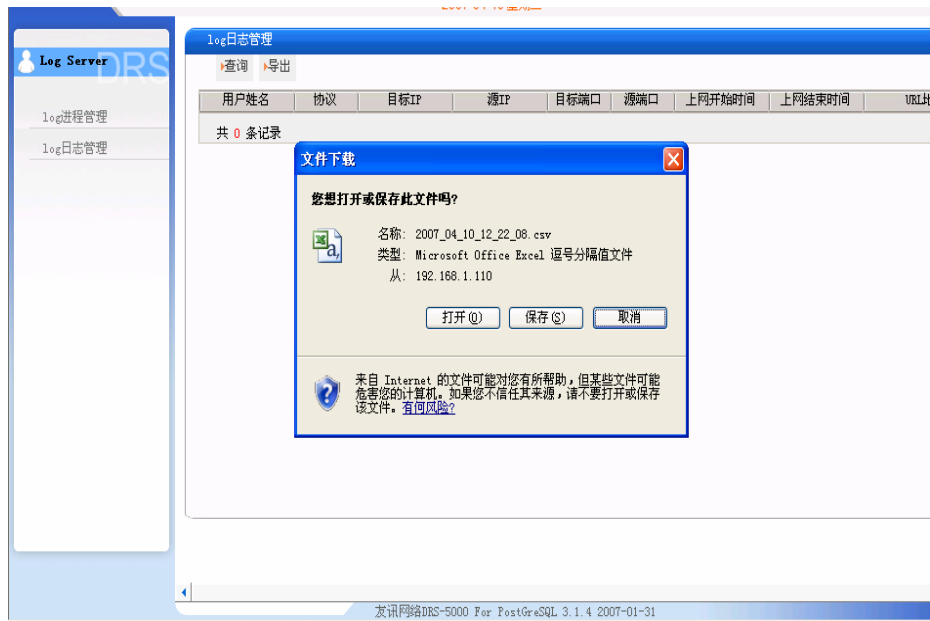
点击“查询”。根据输入查询的条件不同，所需要的时间不同。

The screenshot shows the 'Log Server' interface with the 'log日志管理' section. The '查询' (Query) button has been clicked, and a table of results is displayed. The table has columns: '用户姓名', '协议', '目标IP', '源IP', '目标端口', '源端口', '上网开始时间', '上网结束时间', and 'URL地址'. The table contains 10 rows of data. At the bottom of the table, there is a summary: '共 10000 条记录 全显 首页 上一页 下一页 尾页 共 834 页 当前第 50 页 每页 12 条记录 跳到 页'. The footer of the page reads: '友讯网络DRS-5000 For PostgreSQL 3.1.4 2007-01-31'.

用户姓名	协议	目标IP	源IP	目标端口	源端口	上网开始时间	上网结束时间	URL地址
lw	TCP	221.210.36.145	192.168.1.137	4247	3583	2006-09-02 13:25:58	2006-09-02 13:26:29	
lw	TCP	221.200.212.131	192.168.1.137	8669	3038	2006-09-02 13:25:58	2006-09-02 13:26:30	
lw	TCP	222.209.141.89	192.168.1.137	8274	1745	2006-09-02 13:25:58	2006-09-02 13:26:29	
lw	TCP	218.87.50.157	192.168.1.137	6488	1887	2006-09-02 13:25:58	2006-09-02 13:26:29	
lw	TCP	222.209.141.89	192.168.1.137	8274	1945	2006-09-02 13:26:40	2006-09-02 13:26:46	
lw	TCP	222.141.87.196	192.168.1.137	3599	1946	2006-09-02 13:26:40	2006-09-02 13:26:45	
lw	TCP	69.116.107.179	192.168.1.137	1775	1947	2006-09-02 13:26:40	2006-09-02 13:26:45	
lw	TCP	221.203.198.114	192.168.1.137	3432	1948	2006-09-02 13:26:41	2006-09-02 13:26:44	
lw	TCP	221.4.185.106	192.168.1.137	6654	1938	2006-09-02 13:26:33	2006-09-02 13:26:43	
lw	TCP	58.53.83.177	192.168.1.137	3306	1937	2006-09-02 13:26:32	2006-09-02 13:26:43	
lw	TCP	121.25.39.251	192.168.1.137	2009	1932	2006-09-02 13:26:30	2006-09-02 13:26:43	
lw	TCP	222.217.119.221	192.168.1.137	7525	1944	2006-09-02 13:26:38	2006-09-02 13:26:43	

3.4. 分析结果导出

分析结果可以以.csv格式保存，具体内容包括：用户ID、使用协议（tcp/udp/all）、源IP（用户IP）、目的IP、源端口、目的端口、开始时间、结束时间。



技术支持

办公地址：北京市朝阳区建国路 71 号惠通时代广场 C1 座
202 室 邮编: 100025

技术支持中心电话：8008868192/(028)85176977

技术支持中心传真：(028)85176948

维修中心地址：北京市朝阳区建国路 71 号惠通时代广场 C1 座
202 室 邮编: 100025

维修中心电话：(010) 58635800

维修中心传真：(010) 58635799

网址：<http://www.dlink.com.cn>

办公时间：周一到周五，早09:00到晚18:00





TO:

Three vertical lines for writing the recipient's address.

D-Link®