

FreeBSD 版日志系统安装教程 (V1.0)



广州网纵信息技术有限公司

2013 年 05 月

文档信息

文档名称			
保密级别	公开	文档版本编号	V1.0
制作人	马中杰	制作日期	2013 年 05 月 06 日
复审人		复审日期	
适用范围	本文档为广州网纵信息技术有限公司 (以下简称：广州网纵) 在 XX 项目中所制作的项目文档，供相关项目人员参考。		

分发控制

编号	读者	文档权限	与文档的主要关系
1	广州网纵信息技术有限公司	读取	项目组成员使用本规定
2		批准	项目的负责人，负责本文档的批准程序
3		读取，建议	本文档的使用者

版本控制

时间	版本	说明	修改人
2013-05-06	V1.0	修改	马中杰

目录

目录.....	3
1 概述.....	4
1.1 目的	4
1.2 适用范围	4
2 安装前准备.....	4
2.1 安装环境准备	4
2.2 安装文件及工具准备.....	4
3 安装步骤	5
3.1 进入流控大师控制台.....	5
3.2 查看格式化硬盘	5
3.3 上传安装文件	7
3.4 解压缩安装文件	9
3.5 编辑/etc/rc.local 文件.....	9
4 日志系统配置及使用	10
4.1 设置日志系统，将其与流控大师关联	10
4.2 导出日志报表	13

FreeBSD 版日志系统安装教程

1 概述

1.1 目的

本文编写旨在流控大师使用及管理人员，通过本文可以快速安装并熟练使用 FreeBSD 版日志系统，并排查基本的服务故障。

1.2 适用范围


本文档系广州网纵信息技术有限公司为 FreeBSD 版日志系统的安装和使用所制作的文档，供相关技术人员参考。

2 安装前准备

2.1 安装环境准备

首先，FreeBSD 版日志系统必须安装在 FreeBSD 系统环境中，一般和流控大师同时安装在同一个硬件设备上，然后相关联后才能正常使用。

2.2 安装文件及工具准备

- 1、准备好 FreeBSD 版日志系统安装包，如： log20130121_fb8x.tar.gz
- 2、如果原先的硬件上没有多余的硬盘，要添加一个硬盘，容量最好在 500G 以上。
- 3、在个人电脑上准备并安装 SSH 远程工具。

3 安装步骤

3.1 进入流控大师控制台

首先，使用 SSH 工具或者直接接显示器键盘进入流控控制台，如下图：

```

The Handbook and FAQ documents are at http://www.FreeBSD.org/ and,
along with the mailing lists, can be searched by going to
http://www.FreeBSD.org/search/. If the doc distribution has
been installed, they're also available formatted in /usr/share/doc.

If you still have a question or problem, please take the output of
'uname -a', along with any relevant error messages, and email it
as a question to the questions@FreeBSD.org mailing list. If you are
unfamiliar with FreeBSD's directory layout, please refer to the hier(7)
manual page. If you are not familiar with manual pages, type 'man man'.

You may also use sysinstall(8) to re-enter the installation and
configuration utility. Edit /etc/motd to change this login announcement.

Panabit8# ifconfig
em2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
    ether 08:00:27:31:41:19
    inet 192.168.1.222 netmask 0xfffff00 broadcast 192.168.1.255
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
    options=3<RXCSUM, TXCSUM>
    inet 127.0.0.1 netmask 0xff000000

Panabit8#

```

3.2 查看格式化硬盘

在控制台页面依次输入以下命令：

```

sysctl -n kern.disks 查看硬盘

dd if=/dev/zero of=/dev/ad4 bs=512 count=32

fdisk -qBI /dev/ad4

disklabel -B -w /dev/ad4

newfs ad4

mkdir /usr/logdata

mount /dev/ad4 /usr/logdata

```

以下是执行以上命令后的部分截图：

查看硬盘:

```
Welcome to FreeBSD!

Before seeking technical support, please use the following resources:

o Security advisories and updated errata information for all releases are
  at http://www.FreeBSD.org/releases/ - always consult the ERRATA section
  for your release first as it's updated frequently.

o The Handbook and FAQ documents are at http://www.FreeBSD.org/ and,
  along with the mailing lists, can be searched by going to
  http://www.FreeBSD.org/search/. If the doc distribution has
  been installed, they're also available formatted in /usr/share/doc.

If you still have a question or problem, please take the output of
'uname -a', along with any relevant error messages, and email it
as a question to the questions@FreeBSD.org mailing list. If you are
unfamiliar with FreeBSD's directory layout, please refer to the hier(7)
manual page. If you are not familiar with manual pages, type 'man man'.

You may also use sysinstall(8) to re-enter the installation and
configuration utility. Edit /etc/motd to change this login announcement.

Panabit8# sysctl -n kern.disks
ad1 ad0
Panabit8#
```

格式化硬盘:

```
Panabit8# sysctl -n kern.disks
ad1 ad0
Panabit8# dd if=/dev/zero of=/dev/ad1 bs=512 count=30
30+0 records in
30+0 records out
15360 bytes transferred in 0.049561 secs (309921 bytes/sec)
Panabit8# dd if=/dev/zero of=/dev/ad1 bs=512 count=32
32+0 records in
32+0 records out
16384 bytes transferred in 0.028591 secs (573044 bytes/sec)
Panabit8# fdisk -qBI /dev/ad1
***** Working on device /dev/ad1 *****
fdisk: invalid fdisk partition table found
Panabit8# disklabel -B -w /dev/ad1
Panabit8# newfs ad1
/dev/ad1: 5120.0MB (10485760 sectors) block size 16384, fragment size 2048
using 28 cylinder groups of 183.77MB, 11761 blks, 23552 inodes.
super-block backups (for fsck -b #) at:
160, 376512, 752864, 1129216, 1505568, 1881920, 2258272, 2634624, 3010976,
3387328, 3763680, 4140032, 4516384, 4892736, 5269088, 5645440, 6021792,
6398144, 6774496, 7150848, 7527200, 7903552, 8279904, 8656256, 9032608,
9408960, 9785312, 10161664
Panabit8#
```

检查格式化硬盘完毕：

```

Panabit8# sysctl -n kern.disks
ad1 ad0
Panabit8# dd if=/dev/zero of=/dev/ad1 bs=512 count=30
30+0 records in
30+0 records out
15360 bytes transferred in 0.049561 secs (309921 bytes/sec)
Panabit8# dd if=/dev/zero of=/dev/ad1 bs=512 count=32
32+0 records in
32+0 records out
16384 bytes transferred in 0.028591 secs (573044 bytes/sec)
Panabit8# fdisk -qBI /dev/ad1
***** Working on device /dev/ad1 *****
fdisk: invalid fdisk partition table found
Panabit8# disklabel -B -w /dev/ad1
Panabit8# newfs ad1
/dev/ad1: 5120.0MB (10485760 sectors) block size 16384, fragment size 2048
        using 28 cylinder groups of 183.77MB, 11761 blks, 23552 inodes.
super-block backups (for fsck -b #) at:
    160, 376512, 752864, 1129216, 1505568, 1881920, 2258272, 2634624, 3010976,
    3387328, 3763680, 4140032, 4516384, 4892736, 5269088, 5645440, 6021792,
    6398144, 6774496, 7150848, 7527200, 7903552, 8279904, 8656256, 9032608,
    9408960, 9785312, 10161664
Panabit8# mkdir /usr/logdata
Panabit8# mount /dev/ad1 /usr/logdata
Panabit8#

```

用“df-h”命令查看新装上去的硬盘是否识别出来：

```

Panabit8# df -h

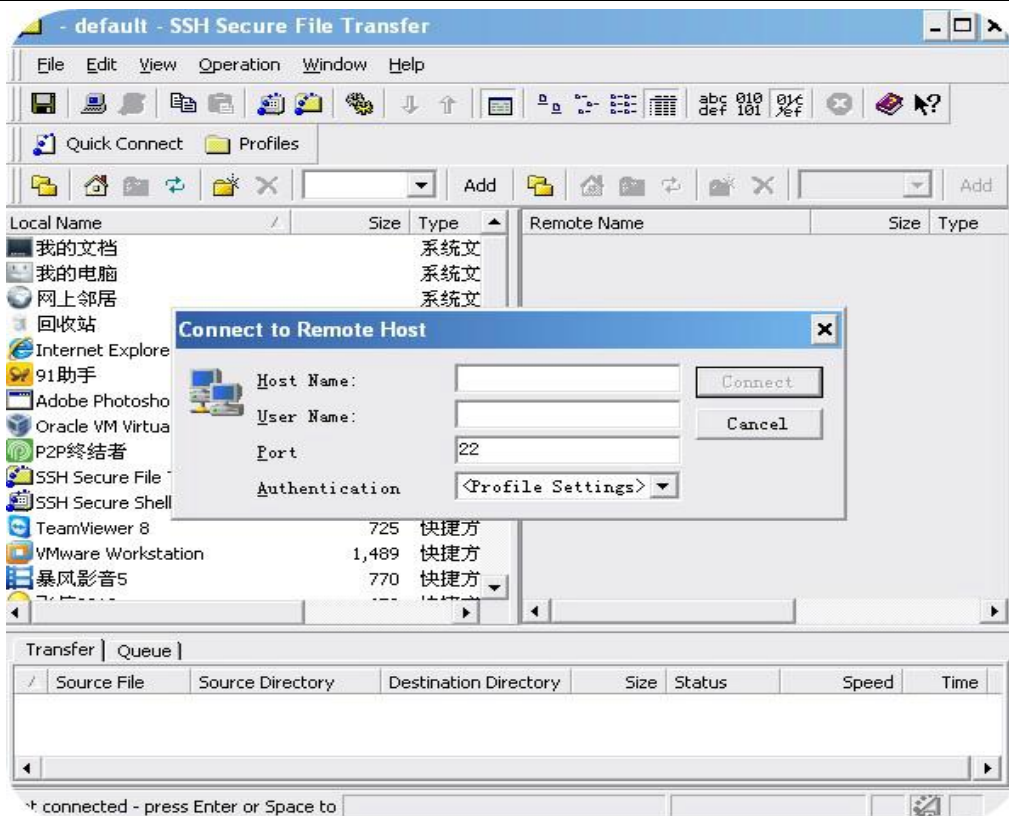
```

Filesystem	Size	Used	Avail	Capacity	Mounted on
/dev/ad0s1a	252M	22M	209M	10%	/
/devfs	1.0K	1.0K	0B	100%	/dev
/dev/ad0s2a	98M	7.3M	83M	8%	/usr/panabit
/dev/ad0s3a	28M	22K	26M	0%	/usr/panaetc
/dev/ad0s4a	1.6G	134K	1.4G	0%	/usr/panalog
/dev/md1	31M	7.4M	21M	26%	/usr/ramdisk
/dev/ad1	4.8G	4.0K	4.5G	0%	/usr/logdata

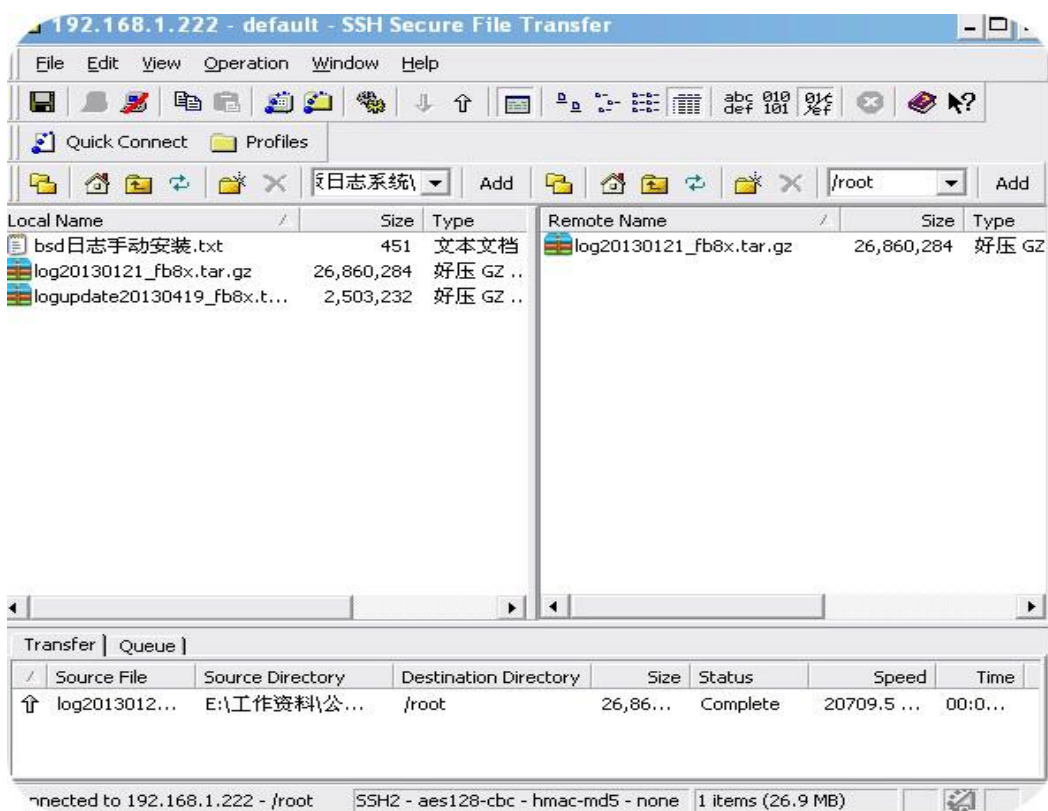
3.3 上传安装文件



- 1) 用这个 SSH 文件传输客户端上传 FreeBSD 版日志系统安装文件。打开客户端，输入 IP 和用户名 root 连接控制台。如下图：



2) 选中安装文件，手动拉入右边对话框上传，如下图：



3) 进入控制台，用“ls”查看安装文件是否已经上传成功。

```
you may also use sysinstall(8) to re-enter the installation and
configuration utility. Edit /etc/motd to change this login announcement.

Panabit8# ls
.cshrc                .k5login              .profile
.history              .login                log20130121_fb8x.tar.gz
Panabit8#
```

注：如上图，安装文件已经上传成功。

3.4 解压缩安装文件

命令为：tar zxvf log20130121_fb8x.tar.gz -C /，如下图：

```
x etc/appweb/ssl/server.req
x etc/appweb/conf/hosts/
x etc/appweb/conf/tune.conf
x etc/appweb/conf/log.conf
x etc/appweb/conf/doc.conf
x etc/appweb/conf/modules/
x etc/appweb/conf/modules/dir.conf
x etc/appweb/conf/modules/cgi.conf
x etc/appweb/conf/modules/ejs.conf
x etc/appweb/conf/modules/egi.conf
x etc/appweb/conf/modules/fcgi.conf
x etc/appweb/conf/modules/upload.conf
x etc/appweb/conf/modules/php.conf
x etc/appweb/conf/hosts/ssl-default.conf
x etc/appweb/conf/hosts/vhost-sample.conf
x etc/appweb/conf/hosts/named-vhost-sample.conf
x etc/my.cnf
x usr/filelist
x var/log/appweb/.log
x var/log/appweb/upload/
Panabit8#
```

3.5 编辑/etc/rc.local 文件

用“ee /etc/rc.local”命令进入可编辑模式，编辑如下：

```
fscck -y -t ufs /dev/ad0s2a >/dev/null
fscck -y -t ufs /dev/ad0s3a >/dev/null
fscck -y -t ufs /dev/ad0s4a >/dev/null
fscck -y -t ufs /dev/ad1 >/dev/null

mount /dev/ad0s2a /usr/panabit
mount /dev/ad0s3a /usr/panaetc
mount /dev/ad0s4a /usr/panalog
mount /dev/ad1 /usr/panalog

/usr/panabit/bin/iptctrl start
/usr/logd/bin/mysqld_safe --user=root &
sleep 10
/usr/logd/bin/logd &
```

注：ad1 是新增加硬盘的盘符。

设置后，reboot 重启流控。

4 日志系统配置及使用

4.1 设置日志系统，将其与流控大师关联

1) 登录日志系统的 Web 界面

http://192.168.1.221（流控大师的内网 IP）进入 web 界面，默认账号：admin，默认密码：admin。



2) 在“系统管理-设备管理”添加设备，如下图：



其中：流控设备编号 10 与图 6.1 流控中的设置要一致，流控设备名称任意，192.168.1.221 是流控地址，流量日志端口可为 0~65535（看个人习惯，一般惯用端口 60000），与图 6.2 流控中的设置保持一致，因为日志系统和流控都在一个 FreeBSD 系统中，故日志服务器 IP 就是本机 IP：127.0.0.1。



图 6.1



图 6.2

3) 在“系统管理-时间采集”添加事件采集器，如下图：



说明：名称任意，采集器端口，一般我们习惯用 5183 或 5184。

4) 在流控中添加要监控的应用流量，如下图：

The screenshot shows the 'System Maintenance' (系统维护) tab with the 'Event Log' (事件日志) configuration. The table lists various event types and their corresponding log formats and server IP/port settings.

事件类型	日志格式	接收服务器IP:端口	计数器(已记录/记录失败/已发送/发送失败)	操作
QQ上下线	不记录	0.0.0.0	0/0/0/0	编辑
MSN上下线	不记录	0.0.0.0	0/0/0/0	编辑
DNS请求	不记录	0.0.0.0	0/0/0/0	编辑
POP3登录	不记录	0.0.0.0	0/0/0/0	编辑
用户认证	不记录	0.0.0.0	0/0/0/0	编辑
共享用户检测	不记录	0.0.0.0	0/0/0/0	编辑
节点跟踪	不记录	0.0.0.0	0/0/0/0	编辑
URL访问	不记录	0.0.0.0	0/0/0/0	编辑
连接撤销	不记录	0.0.0.0	0/0/0/0	编辑
飞信登录	不记录	0.0.0.0	0/0/0/0	编辑
淘宝登录	不记录	0.0.0.0	0/0/0/0	编辑
新浪微博	不记录	0.0.0.0	0/0/0/0	编辑
腾讯微博	不记录	0.0.0.0	0/0/0/0	编辑

如下图，添加 URL 访问日志，接收服务器 IP 为：127.0.0.1，端口为：5183 和日志系统设置的采集器端口相同。

The screenshot shows the 'Event Log' configuration form for 'URL Access' (URL访问). The form includes fields for the event type, receiver server IP and port, and the log format.

事件类型	接收服务器IP:端口	日志格式
URL访问	127.0.0.1 : 5183 (格式为xxx.xxx.xxx.xxx:nnn)	syslog

Buttons: 提交 (Submit), 取消 (Cancel)

到此，即 FreeBSD 版日志系统与流控大师链接成功。

4.2 导出日志报表

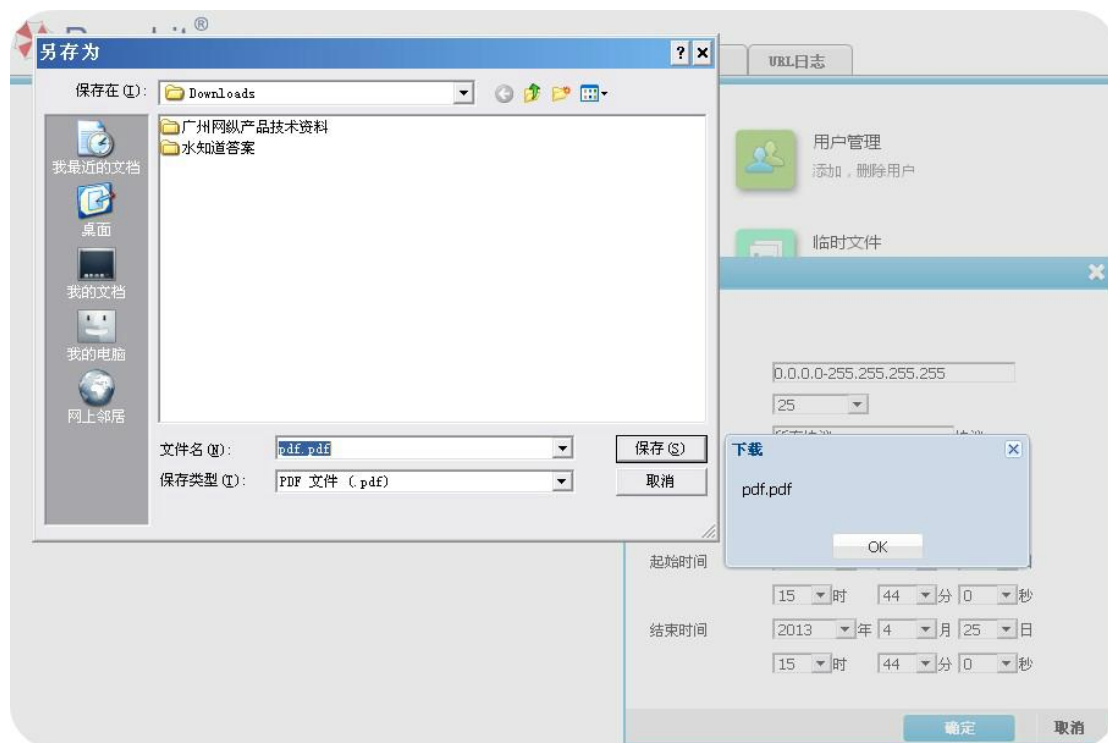
1) 点击“系统维护-系统报表”，出现如下对话框：



2) 点击“确定”如下:



3) 右击 pdf 文件，选“链接另存为”下载 pdf 报表。



4) 流控日志管理系统报表格式如下：

流控日志管理系统报表

(2013/04/25)



流控设备编号： 0

流控设备名称：

报表统计时间： 2013/04/22 15:58-2013/04/25 15:58

统计地址范围： 0.0.0.0-255.255.255.255

报表生成时间： 2013/04/25 15: 58