

# 基于 Linux 的数据服务器在核能工程中的应用

史楠, 揭银先

(中国科学院等离子体物理所, 合肥 230031)

**摘要:** 介绍在核能科学领域, 基于 Linux 操作系统的稳定的数据服务器的搭建过程。通过安装和配置 Linux 系统的 Vsftpd, Apache HTTP 以及 OpenSSH 服务软件包完成对服务器 FTP 服务、Web 服务和 SSH 服务的搭建, 并对过程中需要注意的诸如主机访问控制、不同操作系统的字符集编码转化等问题进行分析和解决。

**关键词:** Linux 服务器; FTP 服务; Web 服务; SSH 服务; 主机访问控制

## 0 引言

核能通常包括裂变能和聚变能两种形式。目前, 裂变能已经实现商用化, 而聚变能仍处于实验研究阶段, 中国科学院等离子体物理研究所全超导非圆截面核聚变实验装置 EAST (Experimental Advanced Superconducting Tokamak) 是一个用于磁约束聚变实验研究的全超导托卡马克装置, 虽然它目前不能提供给我们聚变能, 但却是人类核聚变研究的重要环节, 必将为聚变堆的实现做出重要贡献。实验获得的大量诊断数据对了解和掌握磁约束聚变等离子体中的各种物理过程, 从而改善约束, 实现反应堆的稳态运行等具有很重要的意义。架构诊断数据服务器, 目的在于提供一个稳定的诊断数据服务平台, 方便实验数据的存储和传输下载。

## 1 数据服务器总体构想

为保证服务器的长久稳定运行, 在操作系统方面选择了稳定性良好的 RedHat Enterprise Linux 4.0 系统; 由于网页具有直观性, 所以借助 Web 服务, 在 Dreamweaver 中进行网页设计, 使用户通过网页方便的查找需要的数据; 而又因为数据的规模比较大, 所以后台选择 FTP 服务的方式方便管理员和用户上传和下载数据; 同时, 该数据服务器旨在保证内部使用, 故搭建时还要考虑到对 IP 地址的限制; 根据管理员要远程控制服务器的要求, 再采用 SSH 服务, 最终完成一个完整的服务器架构工作, 工作示意如图 1 所示:

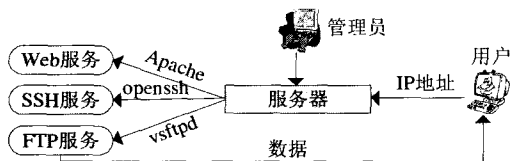


图 1 架构流程图

项目名称: EAST 托卡马克 DCN 激光偏振干涉仪

项目编号: 075ETYD30A

下面就架构服务器的各个部分分别加以说明。

## 2 FTP 服务器的架构

基于 Linux 系统的 FTP 服务器架构, 主要包括 vsftpd 服务器的安装、配置以及对用户权限设置、访问控制等等。

### 2.1 FTP 服务模型及两种数据传输模式

FTP 协议是用于在两台主机之间进行数据交换, 它在主机之间建立两条通信链路, 分别是控制连接和数据连接。控制连接主要负责传送在会话过程中用户发送的 FTP 命令和 FTP 服务的响应; 数据连接主要负责传输数据。

FTP 服务的数据传输模式有两种, 分别是 Port (主动)模式和 Passive(被动)模式。

在主动模式下, 服务器向客户端发起一个用于数据传输的连接, 客户端的连接端口是由服务器和客户端通过协商确定的; 而在被动模式下, 客户端向服务器发起一个用于数据传输的连接, 客户端的连接端口

收稿日期: 2008-01-24 修稿日期: 2008-02-25

作者简介: 史楠(1982-), 女, 河北石家庄人, 在读研究生, 研究方向为核能科学与工程、计算机控制

是发起这个数据连接请求时使用的端口号。

## 2.2 FTP 服务器的配置

在 RHEL 4.0 中,FTP 服务是靠 vsftpd(very secure FTP daemon) 来实现的。vsftpd 是一个受 GPL 版权协议保护的 FTP 服务实现。从名字可以看出,安全是它首要考虑的问题。通过系统的添加/删除应用程序来安装 vsftpd。

vsftpd 服务的配置文件为/etc/vsftpd/vsftpd.conf,是需要根据具体要求进行修改以实现不同功能的。下面表 1 所描述的配置主要是从对用户访问权限、连接时间、控制访问等方面来说明的。

表 1 vsftpd 配置文件部分说明

配置项	说明
anon_mkdir_write_enable=NO	不允许匿名用户创建目录
anon_upload_enable=NO	不允许匿名用户上传文件
anonymous_enable=YES	允许用户匿名登录
ascii_download_enable=NO	下载文件不能使用 ASCII 模式传输
ascii_upload_enable=YES	上传文件可以使用 ASCII 模式传输
chroot_local_user=YES	限制本地用户在登录后权限被设置在家目录
ftpd_banner=welcome to logging our FTP service	显示首次连入 vsftpd 时现实的欢迎字符
listen=YES	vsftpd 将以独立模式运行
local_enable=YES	允许本地登录
accept_timeout=60 (s)	用户以 PASV 模式建立数据连接的时间限制
connect_timeout=60 (s)	响应 PORT 方式的数据连接的时间限制
data_connection_timeout=300 (s)	设定空闲的数据连接所允许的最大时间
idle_session_timeout=600 (s)	用户最大 FTP 命令的间隔时间
xferlog_enable=YES	启用后,将维护一个日志文件,用于详细的纪录上传和下载
xferlog_std_format=YES	FTP 将使用标准的 ftp xferlog 日志格式
pam_service_name=vsftpd	设置 PAM 认证服务的配置文件名称
userlist_enable=YES	FTP 检查 userlist_file 设置文件中指定的用户是否可以访问 vsftpd 服务器
userlist_deny=YES	指定不可以访问 vsftpd 服务器的用户
tcp_wrappers=YES	实现对 IP 访问控制

注意,配置文件完成之后要重启 vsftpd 才可以得到更新。

## 2.3 配置主机访问控制

在 FTP 服务配置过程中,根据需要考虑到对 IP 地址段访问的限制,可以将 vsftpd 与 TCP\_wrapper 结合起来一起实现,这样连接请求转由 TCP\_wrapper 完成控制访问。如上在配置文件中首先设置 tcp\_wrappers=YES,而后分别设定/etc/hosts.allow 和/etc/hosts.deny 的内容。如只允许 IP 段在 111.22.33.4/

255.255.248.0 的用户访问,其余 IP 均受限制,则如下设定内容:

```
# vi /etc/hosts.allow //打开并编辑 hosts.allow 文件
vsftpd:111.22.33.4/255.255.248.0 //在 hosts.allow 文件中填写允许访问的 IP 段
```

```
# vi /etc/hosts.deny
```

```
ALL:ALL //在 hosts.deny 中阻止其他所有的 IP
```

## 2.4 设置访问权限

所设服务器管理员的账户名是 upload,下面对其访问权限进行设置:

```
# mkdir /var/ftp/pub //创建 FTP 服务目录
```

```
# useradd -g ftp -d /var/ftp -M upload //创建用户 upload 属于 ftp 组
```

```
# chown upload.ftp /var/ftp/ -R //设置/var/ftp 目录及其子目录的属主是 upload
```

```
# chmod 755 /var/ftp -R //设置/var/ftp 目录及其子目录的读写权限是只有 upload 具有可读可写权限,其他用户均只有读数据的权限
```

由于在 FTP 配置文件中设置允许用户的匿名访问,所以一般用户即可不需要用户名直接登录服务器,但只具有读数据和下载数据的权限,不可上传或者修改数据。

到此,FTP 服务器架构完毕,保证了对 IP 地址段的限制,同时为管理员和普通用户的权限进行了区别。

## 3 Web 服务器的架构

在 RHEL 4.0 中,Web 服务是靠 Apache HTTP 来实现的。Apache 是一个稳定、多平台的 Web 服务器守护进程,是 Linux 最常用的 Web 服务器。通过添加/删除应用程序来安装即可。使用 HTTP 配置工具可以方便的对 Apache HTTP 进行配置,根据需要在“主”选项卡中设置服务器名,在“调整性能”选项卡设置服务器最大连接数以及超时限制等。如果想添加 HTTP 配置工具中没有的额外模块或者配置选项,就需要修改相应的配置文件,这里均采用默认值。编写网页的过程中,通过超链接的方式把网页内容连接到 FTP 服务器上。

网页的设计是在 Dreamweaver 中进行的,DW 一般运行在 Windows 下,把编写好的网页代码拷贝到服务器相应的目录下,到此完成了对 Web 服务器的架构。

需要注意的一点是,在 DW 下编写的网页,字符集是 GB2312, 当其在 Linux 下运行时汉字全部为乱码。需要找到 apache 配置文件/etc/httpd/conf/httpd.conf 中的配置命令行 AddDefault Charset iso 8859-1, 将其改为 AddDefault Charset gb2312,再重启 Apache, 即可解决。

#### 4 SSH 服务器的架构与使用

由于传统的 rlogin、rsh、telnet 等远程登录方式在传输机制和实现原理方面都没有考虑到安全机制,使用明文进行传输,起本质是不安全的;另外出于维护运行 Linux 的 Web 和 FTP 服务器的需要,管理维护人员经常需要通过 Windows 系统来登录 Linux 主机进行备份、更新和删除工作。故在选择远程登录服务时,采用 SSH 技术。

首先在服务器端通过系统盘安装 OpenSSH,成功后,启动 OpenSSH,为了实现开机自启动功能,输入命令 #ntsysv,在弹出的窗口中选择 sshd。这里需要注意的问题是,如果 Linux 服务器开启了防火墙功能,则需关闭防火墙功能或者设置允许 TCP 端口 22 通过,远程连接才可正常开启;

其次在用户端 Windows 系统下,下载应用程序

PUTTY,进行简单的设置,输入 IP 地址或者网址,以及选择 SSH 服务,即可与服务器进行连接了。管理员通过 SSH 服务与服务器进行通话,管理 FTP 服务,方便的完成上传、下载以及修改数据、文件名等任务。至此,SSH 服务器架构完毕。

#### 5 结语

在建立内网使用的数据库服务器的时候,首先应该考虑的是对访问用户 IP 地址的限制,其次还应注意到对这种大数据量的服务器,使用 FTP 服务可以使管理员更加安全、方便的管理,用户下载数据也不会受网络不稳定等问题的干扰。FTP 服务器的架构过程中,要根据实际情况编写配置文件。再有,Windows 系统和 Linux 系统使用的是不同的字符集编码,所以在不同系统编写网页的时候要考虑到字符转化的问题。

#### 参考文献

- [1]林晓飞,万辉,张鑫金. RedHat Enterprise Linux 4.0 架设实务[M]. 北京:清华大学出版社,2007:35-95
- [2]余永洪. 用 SSH 技术远程管理 Linux 服务器[J]. 计算机与现代化,2007:96-98

## Application of Database Server Based on Linux in the Field of Nuclear Engineering

SHI Nan , JIE Yin-xian

(Institute of Plasma Physics ,Chinese Academy of Sciences ,Hefei 230031)

**Abstract:** Describes a structured process of database server based on Linux. Through the installation and configuration of the system's service packages such as Vsftpd, Apache HTTP, as well as OpenSSH, completed the structured process of FTP, Web and SSH server. Pays attention to some questions such as the host access control,the transformation of the different character sets which run on the Windows and Linux, and discusses the solutions.

**Keywords:** Database Server Based on Linux; FTP Service; Web Service; SSH Service; Host Access Control