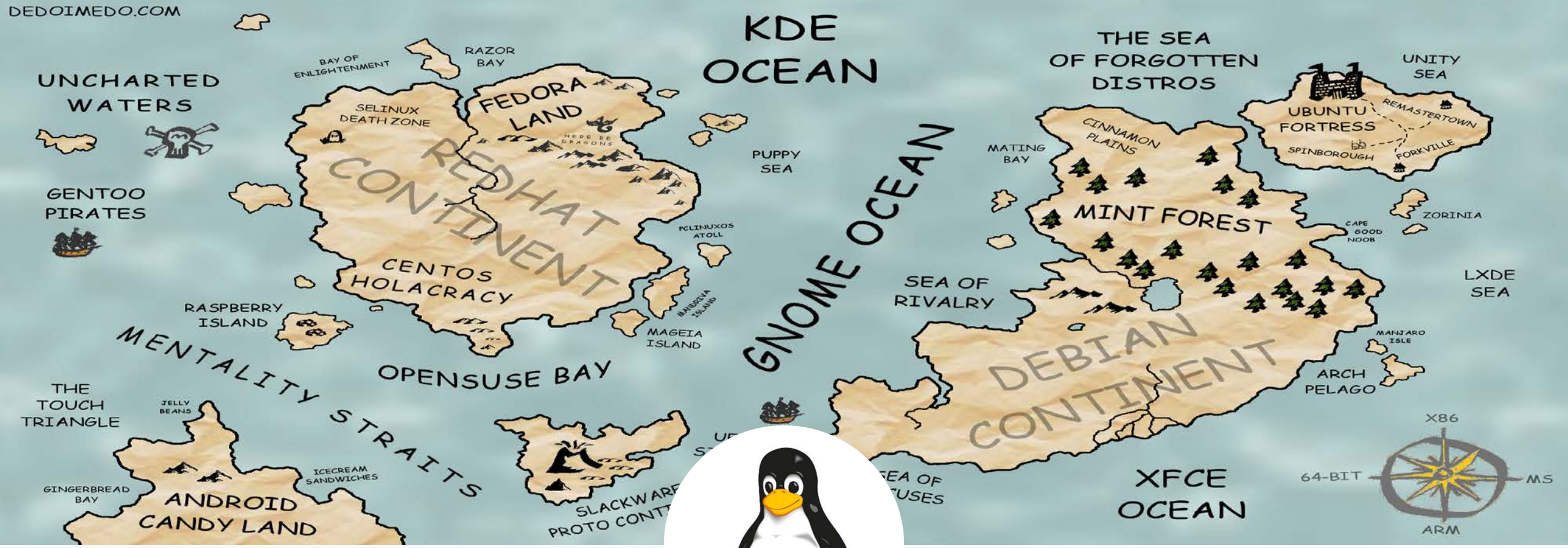


使用vsftpd服务传输文件

任课教师：刘遄 www.LinuxProbe.com

课程概述

01 **文件传输协议**
File Transfer Protocol

02 **vsftpd服务程序**
Vsftpd Service Program

03 **TFTP（简单文件传输协议）**
TFTP (Simple File Transfer Protocol)

前言

01 什么是文件传输协议（File Transfer Protocol，FTP），以及如何部署vsftpd服务程序，然后深度剖析了vsftpd主配置文件中最常用的参数及其作用，并完整演示了vsftpd服务程序3种认证模式（匿名开放模式、本地用户模式、虚拟用户模式）的配置方法。

02 还涵盖了可插拔认证模块（Pluggable Authentication Module，PAM）的原理、作用以及实用的配置方法。

02 进一步练习SELinux服务的配置方法，掌握简单文件传输协议（Trivial File Transfer Protocol，TFTP）的理论及配置方法，学习服务部署和排错方面的经验技巧，灵活应对生产环境中遇到的各种问题。

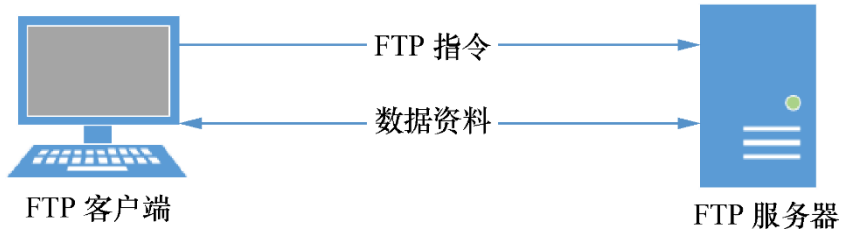
文件传输协议

File Transfer Protocol

文件传输协议

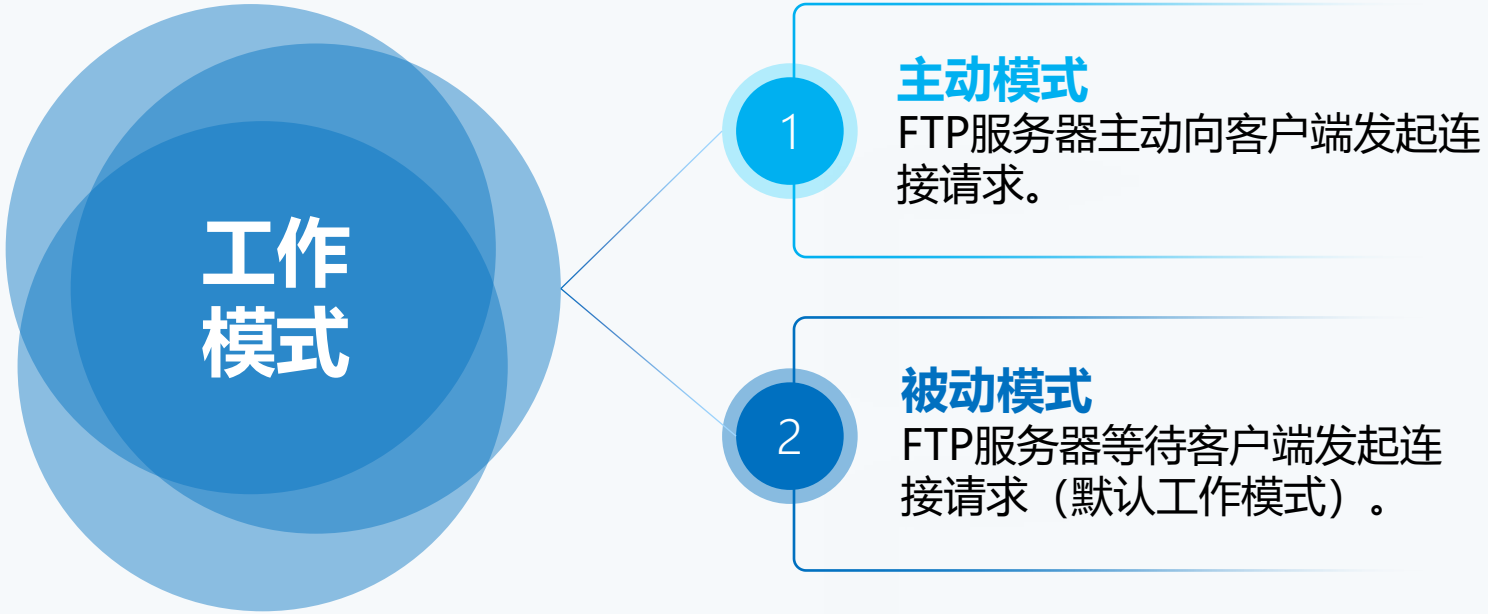
文件传输协议（FTP）

FTP是一种在互联网中进行文件传输的协议，基于客户端/服务器模式，默认使用20、21号端口，其中端口20用于进行数据传输，端口21用于接受客户端发出的相关FTP命令与参数。FTP服务器普遍部署于内网中，具有容易搭建、方便管理的特点。



FTP的传输拓扑

文件传输协议


工作
模式
1
主动模式
FTP服务器主动向客户端发起连接请求。
2
被动模式
FTP服务器等待客户端发起连接请求（默认工作模式）。

vsftpd服务程序常用的参数以及作用

参数	作用
listen=[YES|NO]	是否以独立运行的方式监听服务
listen_address=IP地址	设置要监听的IP地址
listen_port=21	设置FTP服务的监听端口
download_enable＝[YES|NO]	是否允许下载文件
userlist_enable=[YES|NO] userlist_deny=[YES|NO]	设置用户列表为“允许”还是“禁止”操作
max_clients=0	最大客户端连接数，0为不限制
max_per_ip=0	同一IP地址的最大连接数，0为不限制
anonymous_enable=[YES|NO]	是否允许匿名用户访问
anon_upload_enable=[YES|NO]	是否允许匿名用户上传文件
anon_umask=022	匿名用户上传文件的umask值
anon_root=/var/ftp	匿名用户的FTP根目录
anon_mkdir_write_enable=[YES|NO]	是否允许匿名用户创建目录
anon_other_write_enable=[YES|NO]	是否开放匿名用户的其他写入权限（包括重命名、删除等操作权限）
anon_max_rate=0	匿名用户的最大传输速率（字节/秒），0为不限制
local_enable=[YES|NO]	是否允许本地用户登录FTP
local_umask=022	本地用户上传文件的umask值
local_root=/var/ftp	本地用户的FTP根目录
chroot_local_user=[YES|NO]	是否将用户权限禁锢在FTP目录，以确保安全
local_max_rate=0	本地用户最大传输速率（字节/秒），0为不限制

vsftpd服务程序

Vsftpd Service Program

三种认证模式

匿名开放模式

最不安全的一种认证模式，任何人都可以无须密码验证而直接登录到FTP服务器。

本地用户模式

通过Linux系统本地的账户密码信息进行认证的模式，相较于匿名开放模式更安全，而且配置起来也很简单。但是如果黑客破解了账户的信息，就可以畅通无阻地登录FTP服务器，从而完全控制整台服务器。

虚拟用户模式

更安全的一种认证模式，它需要为FTP服务单独建立用户数据库文件，虚拟出用来进行密码验证的账户信息，而这些账户信息在服务器系统中实际上是不存在的，仅供FTP服务程序进行认证使用。

匿名访问模式

匿名访问模式

在vsftpd服务程序中，匿名开放模式是最不安全的一种认证模式。任何人都可以无须密码验证而直接登录FTP服务器。

这种模式一般用来访问不重要的公开文件（在生产环境中尽量不要存放重要文件）。

参数	作用
anonymous_enable=YES	允许匿名访问模式
anon_umask=022	匿名用户上传文件的umask值
anon_upload_enable=YES	允许匿名用户上传文件
anon_mkdir_write_enable=YES	允许匿名用户创建目录
anon_other_write_enable=YES	允许匿名用户修改目录名称或删除目录

向匿名用户开放的权限参数以及作用

本地用户模式

本地用户模式

相较于匿名开放模式，本地用户模式要更安全，而且配置起来也很简单。如果之前用的是匿名开放模式，现在就可以将它关了，然后开启本地用户模式。

参数	作用
anonymous_enable=NO	禁止匿名访问模式
local_enable=YES	允许本地用户模式
write_enable=YES	设置可写权限
local_umask=022	本地用户模式创建文件的umask值
userlist_deny=YES	启用“禁止用户名单”，名单文件为ftpusers和user_list
userlist_enable=YES	开启用户作用名单文件功能

本地用户模式使用的权限参数以及作用

unmask一般被称为“权限掩码”或“权限补码”，能够直接影响到新建文件的权限值。

虚拟用户模式

第1步

重新安装vsftpd服务。创建用于进行FTP认证的用户数据库文件，其中奇数行为账户名，偶数行为密码。

第2步

创建vsftpd服务程序用于存储文件的根目录以及用于虚拟用户映射的系统本地用户。vsftpd服务用于存储文件的根目录指的是，当虚拟用户登录后所访问的默认位置。

第3步

建立用于支持虚拟用户的PAM文件。PAM（可插拔认证模块）是一种认证机制，通过一些动态链接库和统一的API把系统提供的服务与认证方式分开，使得系统管理员可以根据需求灵活调整服务程序的不同认证方式。

虚拟用户模式

第4步

在vsftpd服务程序的主配置文件中通过pam_service_name参数将PAM认证文件的名称修改为vsftpd.vu。PAM作为应用程序层与鉴别模块层的连接纽带，可以让应用程序根据需求灵活地在自身插入所需的鉴别功能模块。

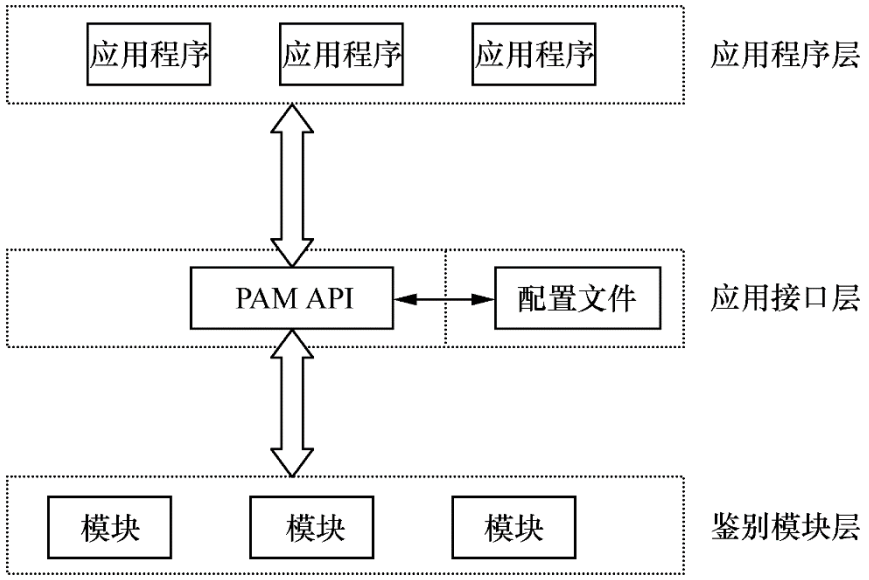
第5步

为虚拟用户设置不同的权限。虽然账户zhangsan和lisi都是用于vsftpd服务程序认证的虚拟账户，但是我们依然想对这两人进行区别对待。

第6步

设置SELinux域允许策略，然后使用虚拟用户模式登录FTP服务器。

vsftpd服务程序



PAM的分层设计结构

参数	作用
anonymous_enable=NO	禁止匿名开放模式
local_enable=YES	允许本地用户模式
guest_enable=YES	开启虚拟用户模式
guest_username=virtual	指定虚拟用户账户
pam_service_name=vsftpd.vu	指定PAM文件
allow_writeable_chroot=YES	允许对禁锢的FTP根目录执行写入操作，而且不拒绝用户的登录请求

利用PAM文件进行认证时使用的参数以及作用

使用不同方式登录后的所在的位置

登录方式	默认目录
匿名公开	/var/ftp
本地用户	该用户的家目录
虚拟用户	对应映射用户的家目录

TFTP（简单文件传输协议）

TFTP (Simple File Transfer Protocol)

TFTP（简单文件传输协议）

定义

简单文件传输协议（Trivial File Transfer Protocol，TFTP）是一种基于UDP协议在客户端和服务器之间进行简单文件传输的协议。顾名思义，它提供不复杂、开销不大的文件传输服务，可将其当作FTP协议的简化版本。

命令功能

TFTP的命令功能不如FTP服务强大，甚至不能遍历目录，在安全性方面也弱于FTP服务。而且，由于TFTP在传输文件时采用的是UDP协议，占用的端口号为69，因此文件的传输过程也不像FTP协议那样可靠。但是，因为TFTP不需要客户端的权限认证，也就减少了无谓的系统和网络带宽消耗，因此在传输琐碎（trivial）不大的文件时，效率更高。

一个带有独立开关的插线板

tftp命令中可用的参数以及作用

参数	作用
?	帮助信息
put	上传文件
get	下载文件
verbose	显示详细的处理信息
status	显示当前的状态信息
binary	使用二进制进行传输
ascii	使用ASCII码进行传输
timeout	设置重传的超时时间
quit	退出

复习题

✓ **1．简述FTP协议的功能作用以及所占用的端口号。**

答：FTP是一种在互联网中进行文件传输的协议，默认使用20、21号端口，其中端口20用于进行数据传输，端口21用于接受客户端发起的相关FTP命令与参数。

✓ **2．vsftpd服务程序提供的3种用户认证模式各自有什么特点?**

答：匿名开放模式是任何人都可以无须密码认证即可直接登录FTP服务器的验证方式；本地用户模式是通过系统本地的账户密码信息登录FTP服务器的认证方式；虚拟用户模式是通过创建独立的FTP用户数据库文件来进行认证并登录FTP服务器的认证方式，相较来说它也是最安全的认证模式。

✓ **3．使用匿名开放模式登录到一台用vsftpd服务程序部署的FTP服务器上时，默认的FTP根目录是什么?**

答：使用匿名开放模式登录后的FTP根目录是/var/ftp目录，该目录内默认还会有一个名为pub的子目录。

✓ **4．简述PAM的功能作用。**

答：PAM是一组安全机制的模块（插件），系统管理员可以用来轻易地调整服务程序的认证方式，而不必对应用程序进行过多修改。

✓ **5．使用虚拟用户模式登录FTP服务器的所有用户的权限都是一样的吗?**

答：不一定，可以通过分别定义用户权限文件来为每一位用户设置不同的权限。

✓ **6．TFTP协议与FTP协议有什么不同?**

答：TFTP协议提供不复杂、开销不大的文件传输服务（可将其当作FTP协议的简化版本）。

祝同学们学习顺利，爱上Linux系统。