Ubuntu Server 从入门到精通

第九章：文件服务

文件服务

我的就是你的—你的还是你的

- 网络诞生最初的动因是去中心化和资源共享
- 文件是初期最主要的资源共享形式
  - 把文件存放在集中的位置供大家访问
- 去中心化是另外一个话题
  - 早期的军事需求
  - 现在的信任需求

文件服务

我的就是你的—你的还是你的

- File Transfer Protocol（FTP）
  - 早期互联网的重要服务
  - 产生于安全出现之前
  - 明文传输一切
  - 目前主要用于公开提供的文件下载服务
  - 使用简单、兼容性好
  - SFTP、FTPS

文件服务

我的就是你的—你的还是你的

- FTP 服务端软件
  - Server U、vsftpd、Proftpd
- 安全考虑
  - 独立布署于企业防火墙之外
  - 只读挂载存储或采用只读存储设备（CD / DVD）

文件服务

我的就是你的—你的还是你的

- Vsftpd
  - 灵活、安全的FTP服务端软件
- 安装
  - sudo apt install vsftpd
  - 安装过程中生成 ftp 帐号（anonymous）
- ftp 帐号
  - /etc/passwd # /bin/false
  - /etc/shadow # *
  - /srv/ftp # ftp用户主目录

文件服务

我的就是你的—你的还是你的

- 配置模式
  - anonymous　　# 匿名模式（适用于公开共享文件）
  - Standard　　# 认证模式
- 配置文件
  - /etc/vsftpd.conf　　# 主配置文件
- 匿名模式
  - Vsftpd默认禁止匿名登录
  - anonymous_enable=YES　　# 启动匿名帐号登录
  - local_enable=NO　　# 禁用认证用户登录

文件服务

我的就是你的—你的还是你的

- 开启匿名帐号上传
  - write_enable=YES　　# 全局设置（以下配置生效的依赖）
  - anon_upload_enable=YES　　# 允许匿名上传文件
  - anon_mkdir_write_enable=YES　　# 允许匿名创建目录
- 常见FTP客户端
  - 浏览器
    - ftp://anonymous@10.1.8.145
  - FTP 命令
  - FTP 客户端程序（Filezilla）
  - 文件同步客户端软件

文件服务

我的就是你的—你的还是你的

- 匿名上传
  - vsftpd 强制禁止在根目录下匿名上传
  - sudo mkdir /srv/ftp/upload　　# 创建上传目录
  - sudo chown ftp:ftp upload　　# 配置文件系统权限
  - anon_umask=022　　# 上传文件权限掩码
  - anon_other_write_enable=YES　　# 允许删除和重命名文件/目录
- 修改FTP主目录
  - sudo mkdir /srv/files/ftp

文件服务

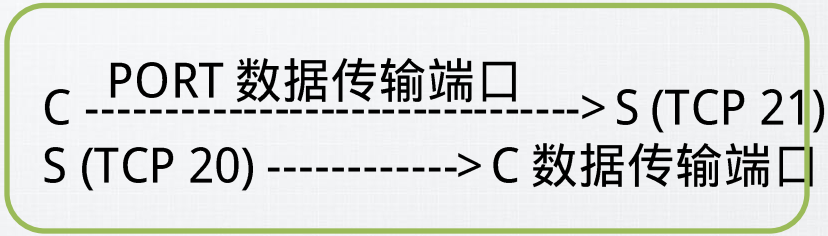
我的就是你的—你的还是你的

- 文件传输日志
  - xferlog_enable=YES　　# 默认开启
  - xferlog_file=/var/log/vsftpd.log　　# 默认日志目录（可修改）
- 其他配置
  - idle_session_timeout=600　　# 会话超时时长
  - no_anon_password=YES　　# 命令行登录禁用密码提示
  - hide_ids=YES　　# 显示属主/属组名称（默认UID）

文件服务

我的就是你的—你的还是你的

- TCP 21 # 会话指令通信端口
- 数据传输模式
  - 主动模式 # 受客户端防火墙影响
  - 被动模式 # 兼容性好（建议方式）
- ftp -p 10.1.8.128 # 被动模式连接



文件服务

我的就是你的—你的还是你的

- 限定被动模式数据通信端口
  - pasv_min_port=40001
  - pasv_max_port=40100
- 在服务器端边界防火墙上开放上述100个端口

文件服务

我的就是你的—你的还是你的

- 身份认证用户登录FTP
  - 默认配置
  - 不能上传
  - 可回溯到根目录（安全隐患）
- chroot 将登录用户锁定在自己的主目录里
  - chroot_local_user=YES
  - 默认主目录可写，vsftpd 禁止用户登录

文件服务

我的就是你的—你的还是你的

- 为FTP登录指定新的主目录
  - sudo mkdir ~/ftp && chmod -w fpt　　# 删除写入权限
  - sudo vi /etc/vsftpd.conf
    - local_root=/home/yuanfh/ftp
- 允许根目录写入
  - write_enable=YES
  - local_root=/home/yuanfh
  - allow_writeable_chroot=YES

文件服务

我的就是你的—你的还是你的

- 指定 chroot 的用户列表
  - chroot_list_enable=YES
  - chroot_list_file=/etc/vsftpd.chroot_list　　# 帐号列表
  - sudo vi /etc/vsftpd.chroot_list
- /etc/ftpusers　　# 默认禁止FTP登录帐号
  - root、daemon、sys、bin、nobody
- 上传文件权限掩码
  - local_umask=022
- 文件同步客户端

文件服务

我的就是你的—你的还是你的

- FTPS：FTP over Secure Socket Layer (SSL)
  - 帐号无需 shell 登录权限
- SFTP：基于SSH加密通道传输文件
  - 帐号需要 shell 登录权限（可设置禁止权限）
- 开启FTPS
  - ssl_enable=Yes # 启动 FTPS
  - rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem # 证书
  - rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key # 私钥

文件服务

我的就是你的—你的还是你的

- 替换默认证书
  - 安全考虑
- 生成密钥文件
  - openssl genrsa -des3 -out ftp.key 2048
- 生成不加密的密钥
  - openssl rsa -in ftp.key -out ftp.key.insecure
  - mv server.key server.key.secure
  - mv server.key.insecure server.key
- 生成证书请求文件
  - openssl req -new -key ftp.key -out ftp.csr #

文件服务

我的就是你的—你的还是你的

- 生成自签名证书
  - openssl x509 -req -days 365 -in ftp.csr -signkey ftp.key -out ftp.pem
- 部署证书
  - sudo cp ftp.key /etc/ssl/private/
  - sudo cp ftp.pem /etc/ssl/certs/
- 生产环境建议由证书颁发机构签名生成证书
- 一行命令
  - sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.key -out /etc/ssl/certs/vsftpd.pem

NFS — Network File System

我的就是你的—你的还是你的

- 最早由 SUN 公司开发
- 类 unix 平台最主要的文件共享方法
- 基于 RPC（Remote Procedure Call）协议
  - NFS 是一个RPC Server（v3 / v4）
- 协议本身不加密，可结合SSH、Kerberos实现加密
- 隐藏式身份验证
- 权限配置是关键
- 服务端口 TCP 2049

文件服务

我的就是你的—你的还是你的

- 安装
  - sudo apt-get install nfs-kernel-server　　# 服务端
  - sudo apt-get install nfs-common　　# 客户端
- 进程
  - rpcbind　　# RPC 服务进程
  - nfsd　　# NFS主进程（身份识别）
  - mountd　　# 根据 /etc/exports 配置验证权限
  - lockd　　# 锁定（需 C/S 同时启用）
  - statd　　# 一致性（需 C/S 同时启用）

文件服务

我的就是你的—你的还是你的

- 身份识别
  - 客户端提供 UID / GID　　# 与用户名、组名无关
  - 服务器按客户端UID / GID付权
  - 服务器无客户端UID / GID帐号，则将客户端映射为匿名帐号
    - nobody / nogroup　　# 65534
  - 客户端使用root帐号（UID 0），默认映射为匿名帐号
    - 可修改配置文件映射 UID 0 为服务器端 ROOT（存在安全隐患）
- 权限
  - 共享权限
  - 文件系统权限

文件服务

我的就是你的—你的还是你的

- 配置
  - sudo vi /etc/exports　　# 主配置文件
  - /export/public　10.1.1.0/24(rw,sync,no_subtree_check)　　# *.lab.com
    - no_root_squash　　# 禁用root默认映射为nobody
  - sudo mkdir /export/public -p　　# 创建共享目录
  - sudo chown nobody:nogroup /export/public　　# 设置权限
  - sudo systemctl restart nfs-kernel-server　　# 重启服务
  - sudo exportfs　　# 查看共享目录
- /var/lib/nfs/etab　　# 共享目录
- /var/lib/nfs/xtab　　# 客户端信息

文件服务

我的就是你的—你的还是你的

- 权限
  - ro / rw　　# 只读 / 读写
  - sync / async　　# 同步写入硬盘 / 暂存于内存中
  - all_squash　　# 所有用户全部映射为 nobody
  - anonuid / anongid　　# 指定匿名ID (默认 65534)
  - secure / insecure　　# 使用1024以下 / 以上端口
  - hide / no_hide　　# 共享 / 不共享NFS子目录
- 客户端挂载
  - sudo mount 10.1.8.135:/export/public /nfs/

文件服务

我的就是你的—你的还是你的

- 启动挂载
  - sudo vi /etc/fstab #
  - 10.1.8.135:/home /nfs/ nfs auto,nofail,noatime,nolock,intr,tcp,actimeo=1800 0 0
- 其他命令
  - rpcinfo -p 10.1.8.135 # 查询 RPC 服务注册状态
  - tail /var/log/kern.log # 服务器日志
  - Showmount -e localhost # 显示共享目录
  - df -h # 客户端查看挂载

文件服务

我的就是你的—你的还是你的

- 企业环境有统一域名和身份验证系统时
  - sudo vi /etc/idpamd.conf
  - Domain = lab.com
- Windows 客户端
  - 企业版

SAMBA文件共享

我的就是你的—你的还是你的

- SMB/CIFS 协议
  - Server message block / Common internet file system
  - 最早由IBM研发，后由微软采用并不断完善
  - Windows 文件和打印共享
  - TCP 139 445 / UDP 137 138
  - SAMBA 是开源世界逆向了SMB协议后打造的兼容微软SMB的文件共享服务
  - SAMBA 还有其他功能、用途和使用场景
- NFS只适用于类 Unix 系统环境
- 适用图 Windows 、Linux 混合环境的文件共享需要

SAMBA文件共享

我的就是你的—你的还是你的

- SAMBA实现了CIFS服务四个基本功能
  - 文件和打印共享
  - 认证和授权
  - 名称解析
  - 服务宣告（browsing）
- 传输协议
  - NetBIOS / NetBIOS over TCP/IP　　# 局域网 / 跨网段
- 后台进程
  - Smbd　　# 文件共享主进程 TCP 139 / 445
  - Nmbd　　# WINS通信、名称解析UDP 137 / 138
  - Winbindd　　# 同步系统帐号
  - 其他10多个进程

SAMBA文件共享

我的就是你的—你的还是你的

- 安装
  - sudo apt install samba libpam-winbind

SAMBA文件共享

我的就是你的—你的还是你的

- 配置文件 /etc/samba/
  - dhcp.conf　　# 指定 WINS 服务器
  - Smb.conf　　# 主配置文件
- smb.conf
  - workgroup = WORKGROUP　　# [global]
  - [Private]
  - comment = private　　# 描述
  - path = /srv/private/　　# 共享路径
  - browseable = yes　　# 可浏览（完整路径）
  - guest ok = no　　# 禁用来宾帐号
  - writable = yes　　# 可读写（ read only = yes ）
  - create mask = 0755　　# 新建文件权限
  - valid users = @samba　　# 可访问共享的用户组

SAMBA文件共享

我的就是你的—你的还是你的

- 用户/组/共享文件夹
  - sudo adduser user1
  - sudo groupadd samba
  - sudo gpasswd -a user1 samba
  - sudo smbpasswd -a user1 # 设置用户SMB密码（不同于系统帐号秘密）
  - sudo mkdir /srv/private/
  - sudo setfacl -R -m "g:samba:rwx" /srv/private/ # 设置组ACL权限（get）
  - testparm # 测试samba配置
  - sudo systemctl restart smbd nmbd # 重启服务
- 客户端访问
  - Linux、windows

SAMBA文件共享

我的就是你的—你的还是你的

- Windows客户端
  - net use \\host\private /user:user1 password
  - net use \\host\private /delete
  - net use s: \\host\private
  - net config workstation

SAMBA文件共享

我的就是你的—你的还是你的

- Linux 客户端
  - smbclient -L //10.1.8.135
  - smbclient -L //10.1.8.135 -U user1
  - mount -t cifs -o username=smb1 //10.1.8.135/public /mnt

SAMBA文件共享

我的就是你的—你的还是你的

- 开放共享文件夹
  - 将不提供登录帐号的用户映射为 guest，无须输入密码
  - [Global]
  - workgroup = WORKGROUP
  - security = user　　# share已废止、Domain、ADS、Server
  - map to guest = bad user　　# 映射为 guest
  - guest ok = yes

SAMBA文件共享

我的就是你的—你的还是你的

- 开放共享文件夹
  - [public]
  - comment = public share
  - path = /srv/public/
  - browseable = yes
  - writable = yes
  - guest ok = yes
- sudo setfacl -R -m "u:nobody:rwx" /srv/public/

SAMBA文件共享

我的就是你的—你的还是你的

- 服务器信息
  - smbd --version
  - sudo smbstatus

Questions?